NUREG/CP-0027
Vol. 1
R1

Proceedings of the International Meeting on Thermal Nuclear Reactor Safety

Held at Chicago, IL
August 29-September 2, 1982

Date Published: February 1983

Sponsored by
American Nuclear Society
Nuclear Reactor Safety Division
Chicago Section

Cosponsored by
European Nuclear Society
Canadian Nuclear Society
Japan Atomic Energy Society

In Cooperation with
U.S. Nuclear Regulatory Commission
International Atomic Energy Agency

FOREWORD

The International Meeting on Thermal Nuclear Reactor Safety, held August 29-September 2, 1982, in Chicago, Illinois, is part of an ongoing series of meetings on the subject of nuclear reactor safety, jointly sponsored by the *American Nuclear Society* (through its *Nuclear Reactor Safety Division*) and the *European Nuclear Society*. The cosponsorship by the *Canadian Nuclear Society* and the *Japan Atomic Energy Society*, as well as the cooperation received from the *U.S. Nuclear Regulatory Commission* and the *International Atomic Energy Agency*, further attests to the importance and international character of the meeting.

The *Chicago Section* of the American Nuclear Society served as host of the meeting, having carried, through the Organizing Committee, the responsibility for the local arrangements and the financial aspects.

The safety of nuclear power reactors is a subject that, of necessity, has to be dealt with in an international framework. It is for this reason that the meeting organizers have also made a major effort to encourage participation from countries other than those represented by the cosponsoring professional societies. In this respect should be mentioned the valuable contributions, both in the organizational and the technical aspects of the meeting, made by representatives from countries with major nuclear power programs such as Argentina, Brazil, Mexico, the Republic of China (Taiwan), and the Republic of (South) Korea.

High distinction was bestowed on the meeting by three Honorary Chairmen, namely: James R. Thompson, Governor of Illinois; André Giraud, Professor at the University of Paris-Dauphine and Minister of Industry and Technology in the immediate-past government of France; and Joseph M. Hendrie, Senior Scientist at Brookhaven National Laboratory and past Chairman of the U.S. Nuclear Regulatory Commission, to whom the meeting organizers wish to express great appreciation for their support and valuable contributions.

It is not possible to individually acknowledge all persons who contributed to the meeting. As regards the *technical content* of the meeting, major contributions were made by those who accepted responsibility for organizing and coordinating the Special Sessions and Panel Discussions, namely: R. A. Bari (BNL), R. D. Cheverton (ORNL), R. S. Denning (BCL), J. W. Hickman (SNL), W. Y. Kato (BNL), D. A. Meneley (OHC), M. Rosen/E. Iansiti (IAEA), and E. Yaremy (AECL). An important contribution was also made by Annick Carnino (EdF), who accepted primary responsibility for coordinating the papers from France. We are greatly indebted to Long-Sun Tong, the Representative of the U.S. Nuclear Regulatory Commission on the Technical Program Committee, for his numerous and valuable contributions. Many thanks are also due to the members of the International Advisory Committee, the Technical Program Committee and the Paper Review Committee; in particular we wish to express our thanks to those members of the Paper Review Committee, who came from far to make an essential contribution, namely: Karel Brinkmann (ECN), Eric Hellstrand (Studsvik), Morris Rosen (IAEA), Wolfgang Schikarski (KFK), Jean Stolz (EdF), Roberto Treviño (CNSNS), and Hermann Unger (USt).

With respect to the *non-technical part* of the meeting organization, we wish to express our great appreciation to Miriam Holden (ANL) for her valuable advice and assistance concerning numerous aspects, including hotel arrangements and registration. Great appreciation is also due to Joyce Kopta (ANL) for her valuable advice and assistance in the preparation of the Meeting Program and Proceedings. Our special gratitude goes to Joan Cooley (ANL), Barbara Heineman (ANL), Beverly Korelc (ANL), Dena Rottner (NWU), Alice Townsend (ANL), Jill Wadas (ANL), Julia Wertelka (ANL), and Carol Whalen (ANL) for their numerous and valuable contributions made before, during, and after the meeting.

In the final analysis, the success or failure of a meeting depends on its attendees — authors, session chairmen, panelists, and others — they make the meeting. Therefore, last, but not least, we wish to thank all attendees for their participation in, and contributions to, this meeting which, it is hoped, has served a useful purpose by providing a forum for fruitful exchange of information, by promoting the safety of nuclear power reactors, and by contributing to international cooperation in the field of nuclear safety.

STEERING COMMITTEE

Donald T. Eggen (NWU)	General Chairman
Adolf Birkhofer (GRS)	General Co-Chairman
Norman C. Rasmussen (MIT)	Chairman, Technical Program Committee
Jan B. van Erp (ANL)	Co-Chairman, Technical Program Committee
Elmer E. Lewis (NWU)	Chairman, Publications Committee
André Gauvenet (EdF)	Chairman, International Advisory Committee
Dietrich Buenemann (GKSS)	Chairman, ENS Representatives on the Technical Program Committee
Wladimir Paskievici (EPM)	Chairman, CNS Representatives on the Technical Program Committee
Yasumasa Togo (UT)	Co-Chairman, JAES Representatives on the Technical Program Committee

REPRESENTATIVES OF COOPERATING ORGANIZATIONS

U. S. Nuclear Regulatory Commission: L. S. Tong

International Atomic Energy Agency: M. Rosen

HONORARY CHAIRMEN

The Honorable James R. Thompson,
Governor of Illinois

André Giraud, Professor at the University of Paris-Dauphine,
Minister of Industry and Technology of France

Joseph M. Hendrie, Senior Scientist Brookhaven National Laboratory,
Past Chairman US Nuclear Regulatory Commission

ORGANIZING COMMITTEE

Donald T. Eggen (NWU)	Chairman	Elmer E. Lewis (NWU)	Publications
Raymond M. Crawford (SAI)	Treasurer	Donald R. MacFarlane (ETA)	Publicity
Joseph Edelstein (Fluor)	Activities	John T. Madell (FAI)	Deputy Chmn.
Donald R. Ferguson (ANL)	Deputy Chmn.	Martin Plys (FAI)	Students
Mary Goodkind (ESCOR)	Guests	William J. Sturm (ANL)	Publications
James W. Henning	Audio/Visual	Bruce W. Spencer (ANL)	Poster Sessions
C. Daniel Henry (ETA)	Tours	Tom R. Tramm (CECo)	Registrar
Miriam L. Holden (ANL)	Arrangements	Jan B. van Erp (ANL)	Technical Program
Dennis J. Kilsdonk (ANL)	Audio/Visual	Norman Weber (S&L)	Publications
Joyce A. Kopta (ANL)	Publications		

AMERICAN NUCLEAR SOCIETY

Nuclear Reactor Safety Division

Executive Committee:

Joseph C. Turnage (SNR)	Chairman
Walter Y. Kato (BNL)	Vice Chairman
Dirk A. Dahlgren (SNL)	Secy.-Treas.
William Kerr (UM)	Past Chairman
Robert Avery (ANL)	Past Chairman

Program Committee:

Joseph A. Murphy (NRC)	Chairman
George F. Flanagan (ORNL)	Past Chmn.
Alan Waltar (HEDL)	Past Chmn.

Chicago Section

Brian R. T. Frost (ANL)	Chairman
Mary Goodkind (ESCOR)	Chairman-Elect
Dennis O'Boyle (CECo)	Secretary
F. O. (Whitey) Hurd (WEC)	Treasurer
Tom R. Tramm (CECo)	Past Chairman
Joseph Edelstein (Fluor)	Past Chairman
Donald R. MacFarlane (ETA)	Past Chairman

REPRESENTATIVES OF CO-SPONSORING SOCIETIES

Canadian Nuclear Society

W. Paskievici (EPM), Chairman
W. T. Hancox (AECL)
D. A. Meneley (OHC)
E. Yaremy (AECL)

European Nuclear Society

D. Buenemann (GKSS), Chairman
L. Bindler (BN)
K. Brinkmann (ECN)
A. Carnino (EdF)
A. Hassid (NIRA)
M. Israel (EdF)
W. Jeschki (Wuerenlingen)
P. Mostert (KEMA)
A. Rastas (TVO)
H. Teague (UK-AEA)
H. Unger (USt)
G. Volta (JRC)

Japan Atomic Energy Society

R. Kiyose (UT), Chairman
Y. Togo (UT), Co-Chairman

TECHNICAL PROGRAM COMMITTEE

N. C. Rasmussen (MIT), Chairman
R. A. Bari (BNL)
W. R. Corcoran (CE)
W. B. Cottrell (ORNL)
D. Dahlgren (SNL)
L. W. Deitrich (ANL)
R. S. Denning (BCL)
R. Duffey (EPRI)
D. T. Eggen (NWU)
H. K. Fauske (FAI)
G. Flanagan (ORNL)
E. Fuller (SLI)
J. W. Hickman (SNL)
J. F. Jackson (LANL)
R. J. Johnson (TVA)
J. A. Murphy (NRC)
E. O'Donnel (EC)
V. E. Schrock (UCB)
R. Seale (UA)
G. Sherwood (GE)
R. R. Stiger (EG&G)
J. C. Turnage (SNR)
J. B. van Erp (ANL), Co-chairman
L. J. Ybarrondo (EG&G)

INTERNATIONAL ADVISORY COMMITTEE

A. Gauvenet (France, EdF), Chairman
A. Alonso (Spain, JEN)
R. Avery (USA, ANL)
R. Bello (Mexico, CNSNS)
D. Beninson (Argentina, CNEA)
A. Birkhofer (FRG, GRS)
B. R. T. Frost (USA, ANL)
A. Gonzalez (Argentina, CNEA)
J. H. Jennekens (Canada, AECB)
W. Y. Kato (USA, BNL)
G. Kinchin (UKAEA)
L. Lederman (Brazil, CNEN)
S-H. Lee (Korea, KAERI)
S. Levine (USA, NUS)
W. Loewenstein (USA, EPRI)
M. Nozawa (Japan, JAERI)
D. Okrent (USA, UCLA)
M. Rosen (IAEA, Vienna)
D. Smidt (FRG, KFK)
K. Stadie (OECD)
J. Stolz (France, EdF)
W. Stratton (USA, LANL)
L-S. Tong (USA, NRC)
R. Treviño (Mexico, CNSNS)
W. Vinck (CEC, Brussels)

PAPER REVIEW COMMITTEE

N. C. Rasmussen (MIT), Chairman
S. Asselin (TEC)
L. Baker, Jr. (ANL)
R. Bari (BNL)
C. Bowers (ANL)
K. Brinkmann (ECN)
J. Buchanan (ORNL)
R. Christie (TVA)
D. Dahlgren (SNL)
R. S. Denning (BCL)
Z. Domaratzki (AECB)
D. T. Eggen (NWU)
H. K. Fauske (FAI)
G. Flanagan (ORNL)
B. R. T. Frost (ANL)
W. T. Hancox (AECL)
E. Hellstrand (Studsvik)
J. W. Hickman (SNL)
J. Ireland (LANL)
J. F. Jackson (LANL)
W. Y. Kato (BNL)
R. Lindsay (ANL)
D. A. Meneley (OHC)
C. J. Mueller (ANL)
L. Potash (INPO)
W. Quapp (EG&G)
M. Rosen (IAEA)
W. Schikarski (KFK)
B. W. Spencer (ANL)
J. Stolz (EdF)
L-S. Tong (NRC)
R. Treviño (CNSNS)
H. Unger (USt)
J. B. van Erp (ANL), Co-chairman
R. Vogel (EPRI)
E. Yaremy (AECL)
J. Young (CE)

COORDINATORS OF SPECIAL SESSIONS AND PANEL DISCUSSIONS

R. A. Bari (BNL)	Session 28
R. D. Cheverton (ORNL)	Sessions 7 and 11
R. S. Denning (BCL)	Sessions 17 and 21
J. W. Hickman (SNL)	Session 18
W. Y. Kato (BNL)	Session 6
D. A. Meneley (OHC)	Session 22
N. C. Rasmussen (MIT)	Sessions 1 and 32
M. Rosen (IAEA)	Session 2
E. Yaremy (AECL)	Session 10

ACRONYMS OF ORGANIZATIONS

AECB	Atomic Energy Control Board (Canada)
AEC-Greece	Atomic Energy Commission of Greece
AECL	Atomic Energy of Canada Limited
ANL	Argonne National Laboratory
ARL	Alden Research Laboratory (Worcester, MA)
AS	Anstalt fuer Stroemungsmaschinen GmbH (Austria)
ASA	Applied Science Associates, Inc.
ASEA	ASEA-Atom (Sweden)
BCL	Battelle Columbus Laboratories
BEC	Boston Edison Co.
BN	Belgonucléaire
BNL	Brookhaven National Laboratory
B&W	Babcock & Wilcox Co.
CE	Combustion Engineering Co.
CEA	Commissariat à l'Energie Atomique (France)
CEC	Commission of the European Communities
CECo	Commonwealth Edison Co.
CEGB	Central Electricity Generating Board (UK)
CMET	Center for Mineral and Energy Technology (Canada)
CNEA	Comision Nacional de Energia Atomica (Argentina)
CNEN	Comissão Nacional de Energia Nuclear (Brazil)
CNSNS	Comision Nacional de Seguridad Nuclear y Salvaguardias (Mexico)
COGEMA	Compagnie Generale des Matieres Nucleaires (France)
CPC	Consumers Power Co.
CSDL	Charles Stark Draper Laboratory
CU	Carleton University (Canada)
DE	Davis Engineering Ltd. (Canada)
DOE	Department of Energy
DPC	Duke Power Co.
EA	Empresarios Agrupados (Spain)
EC	Envirosphere Company/Ebasco Services, Inc.
ECN	Energy Research Center (The Netherlands)
EdF	Electricite de France
EERM	Etablissement d'Etudes de Recherches Météorologiques (France)
EES	Electrowatt Engineering Services (London or Zurich)
EG&G	EG&G Idaho, Inc.
EI	Energy Incorporated
ENACE	Empresa Nuclear Argentina de Centrales Electricas SA (Argentina)
EPM	Ecole Polytechnique de Montréal (Canada)
EPDC	Electric Power Development Co., Ltd. (Japan)
EPRI	Electric Power Research Institute
ESA	Engineering Science & Analysis
Escor	Escor, Inc.
ESI	Ebasco Services, Inc.
ETA	ETA Engineering, Inc.
FAI	Fauske & Associates, Inc.
FEPC	Federation of Electric Power Companies (Japan)
Fluor	Fluor Power Services, Inc.
Framatome	Framatome, SA (France)

ACRONYMS FOR ORGANIZATIONS (Contd.)

GA	General Atomic Co.
GE	General Electric Co.
GKSS	Gesellschaft fuer Kernenergieverwertung in Schiffbau und Schiffahrt mbH, Geesthacht (FRG)
GPC	General Physics Corporation
GRS	Gesellschaft fuer Reaktorsicherheit (FRG)
Halden	Halden Project (Norway)
HEI	Heat Engineering Institute (USSR)
Hitachi	Hitachi, Ltd. (Japan)
HTRB	Hochtemperatur-Reaktorbau GmbH (FRG)
IAEA	International Atomic Energy Agency
INEL	Idaho Nuclear Engineering Laboratory
INPO	Institute for Nuclear Power Operation
INS	Institute of Nuclear Safety (Japan)
IT	Intermountain Technologies, Inc.
IVO	Imatran Voima Oy (Finland)
JAERI	Japan Atomic Energy Research Institues
JBF	JBF Associates, Inc.
JEN	Junta de Energia Nuclear (Spain)
JRC	Joint Research Centre - Ispra (Italy)
KAERI	Korea Advanced Energy Research Institute
KEMA	N. V. Keuring van Electrische Materialen (The Netherlands)
KFK	Kernforschungszentrum Karlsruhe
KLA	Kernkraftwerk Leibstadt AG (Switzerland)
Ktech	Ktech Corp.
KWU	Kraftwerk Union AG (FRG)
LANL	Los Alamos National Laboratory
LLNL	Lawrence Livermore National Laboratory
LPL	Louisiana Power and Light
LU	Lehigh University
MESA	Studio MESA (Italy)
MIT	Massachusetts Institute of Technology
MU	McMaster University (Canada)
NAIG	Nippon Atomic Industry Group Co., Ltd. (Japan)
NEC	NucleDyne Engineering Corporation
NII	Nuclear Installations Inspectorate (UK)
NIRA	Nucleare Italiana Reattori Avanzati S.P.A. (Italy)
NRC	Nuclear Regulatory Commission (U.S.)
NSAC	Nuclear Safety Analysis Center
NU	Northeast Utilities
NUS	NUS Corporation
NWU	Northwestern University
OECD	Organization for Economic Cooperation and Development
OHC	Ontario Hydro Company (Canada)
ORNL	Oak Ridge National Laboratory
PLG	Pickard, Lowe and Garrick, Inc.
PNL	Pacific Northwest Laboratory

ACRONYMS FOR ORGANIZATIONS (Contd.)

RI	Rockwell International
Risø	Risø National Laboratory (Denmark)
S&A	Stevenson and Associates
SAI	Science Applications, Inc.
SEC	Sukegawa Electric Co., Ltd. (Japan)
S&L	Sargent & Lundy
SLI	S. Levy, Inc.
SNL	Sandia National Laboratories
SNR	Summit Nuclear Resources
SPB	State Power Board (Sweden)
Studsvik	Studsvik Energiteknik AB (Sweden)
SUNY	State University of New York
S&W	Stone & Webster Engineering Corp.
Sydkraft	Sydkraft (Sweden)
TAI	Tech. Aid Inc.
TC	Toshiba Corp. (Japan)
TEC	Technology for Energy Corporation
TEPC	Tokyo Electric Power Company (Japan)
TPC	Taiwan Power Company (Taiwan)
TRC	Technical Research Centre (Finland)
TUM	Technische Universitaet Muenchen (FRG)
TVA	Tennessee Valley Authority
TVO	Teollisuudon Voima Oy (Finland)
UA	University of Arizona
UCB	University of California at Berkeley
UCLA	University of California, Los Angeles
UdP	Universita di Pisa (Italy)
UFRJ	Universidade Federal Rio de Janeiro (Brazil)
UKAEA	UK Atomic Energy Authority
USt	University of Stuttgart (FRG)
UT	University of Tokyo (Japan)
UWa	University of Waterloo (Canada)
UW	University of Wisconsin
VEPCO	Virginia Electric and Power Co.
WEC	Westinghouse Electric Corp.
WLA	Wood-Leaver and Associates, Inc.
Wuerenlingen	Federal Nuclear Research Center (Switzerland)
YAEC	Yankee Atomic Electric Co.

VOLUME 1

SESSION 8

PRA-2; SYSTEMS APPLICATIONS OF RELIABILITY AND RISK METHODS

Chair: **L. Lederman** *(CNEN)*
I. Wall *(EPRI)*

SESSION 9

MAN/MACHINE INTERFACE - 1; HUMAN FACTORS

Chair: **Z. Sabri** *(LPL)*
A. Vuorinen *(IAEA)*

VOLUME 2

SESSION 13

FUEL PERFORMANCE EVALUATION

Chair: **M. Israel** *(EdF)*
W. Quapp *(EG&G)*

SESSION 14

RADIOLOGICAL SOURCE TERMS - 2

Chair: **B. W. Spencer** *(ANL)*

SESSION 15

SMALL-BREAK LOCA ANALYSIS

Chair: **B. W. Spencer** *(ANL)*

SESSION 16

DEGRADED CORE ANALYSIS - 1

Chair: **B. W. Spencer** *(ANL)*

Page

SESSION 22

NPP SAFETY-RELATED OPERATIONAL EXPERIENCE

Chair: **D. A. Meneley** *(OHC)*
J. Stolz *(EdF)*

SESSION 23

DEGRADED CORE ANALYSIS - 3

Chair: **Y. Togo** *(UT)*
A. Torri *(PLG)*

Page

VOLUME 3

SESSION 24

LICENSING CRITERIA: DEVELOPMENT AND COMPARISON

Chair: **Z. Domaratzki** *(AECB)*
R. Treviño *(CNSNS)*

SESSION 25

LOCA ANALYSIS

Chair: **B. W. Spencer** *(ANL)*

Page

SESSION 26

MAN/MACHINE INTERFACE - 3

Chair: **B. W. Spencer** *(ANL)*

SESSION 27

LOCA-RELATED EXPERIMENTS AND ANALYSIS

Chair: **B. W. Spencer** *(ANL)*

Page

SESSION 32

PANEL DISCUSSION: WHERE DO WE GO FROM HERE?

Chair: **N. C. Rasmussen** *(MIT)*
P. Tanguy *(CEA)*

* * * * * * *

WHAT ABOUT THE FUTURE OF NUCLEAR ENERGY?

André Giraud
COGEMA
Velizy Villacoublay, France

ABSTRACT

The future of nuclear energy, which looked bright in the first part of the seventies, is apparently dull today. However, facts remain.

Nuclear energy will be necessary. Oil will be scarce in the nineties, and will not compete with other energies on the heat market. Coal development meets a certain number of obstacles.

Moreover, it is demonstrated from American experience, but still more from European and French experience, that nuclear electricity is and will be the cheapest.

There remains a key problem: the nuclear debate, and its byproducts, the regulatory perfectionism and administrative red tape. From the author's experience, the following points are essential: a clear expression of why nuclear energy is needed and the corresponding political will, little arguing on technical issues in public (contrary to what is generally done), but achieving ways of convincing the public opinion that safety matters are handled with paramount care and competence.

Nuclear electricity production became economical at the end of the sixties. And although costs increased substantially after an initial underestimation, the 1974 oil shock and price increase changed the terms of reference to such an extent that from that date a tremendous development of nuclear energy seemed certain. The problem of those days was to cope with the expected rapidly increased needs in uranium and equipment production, enrichment capacity, and availability of competent staff.

Surprisingly enough, the situation of today is about the reverse, even after a second spectacular oil price increase. Where oil scarcity should be the norm, there is a large excess of oil. Nuclear orders have stopped for several years in most countries. In the U.S., instead of plant orders, we observe cancellations at the approximate rate of 10/year since 1975, and one can hardly predict any new order before 1990. Uranium and enrichment capacities are in excess. Reprocessing is questioned. The fast breeder program turns into a myth.

Has the situation basically changed? The answer is definitely no. Facts remain. And we will see that beyond the world recession nuclear electricity will have to play its part to fill the energy needs, all the more now that we have enough experience to state that it is indeed the cheapest base-load type of electricity. The only, but essential, problem that raises uncertainties is the nuclear debate and its byproducts--regulatory perfectionism and administrative red tape--which have led the programs to a stop. Nuclear opponents have been more clever than nuclear experts to tackle that political issue.

From the experience gained, and since we believe that this is a right cause, we must concentrate on the solution of this problem.

Unless the world experiences a longlasting depression unknown in history, one can predict that oil will be scarce in the nineties (or even before in certain political situations). The present oil glut must not deceive us. Three facts, among others, explain its existence:

1. The economic recession; the world was organized to supply every year 3% more energy. The impact resulting from the stop in economic growth has touched essentially the most expensive source: oil.

2. The panic inspired in 1979-80 by the situation in Iran and Iraq was responsible for an important increase in oil inventories throughout the world. This phenomenon appeared clearly only after the crisis (see Chart I), and the excess which now is being resorbed amounts to nearly 4 Mbbl/day during one year, or the equivalent of one-third to one-half of the Saudi Arabia production.

3. The United States, which represents one-third of the free world oil consumption, has dramatically decreased its consumption and, of course, the whole impact falls on imports (see Chart II), which are down to 4 Mbbl/d from 8.5 in 1979.

These phenomena and some others (Mexico and North Sea oil development for instance) explain that the OPEC production is presently at the level of 17.5 Mbbl/d compared to a capacity of 27, and even 31 including Iran and Iraq, which are almost shut down nowadays. But they are either limited in time (decrease in inventory, world recession) or limited in size (energy conservation).

On the contrary, the resumption of the world economic growth, even with a much increased energy efficiency pattern, would mean the addition of the equivalent of 2 to 3 Mbbl/d of energy supply. While there are good reasons to anticipate the disappearance of the oil glut, there are also good reasons to await a decrease in oil reserves and production.

Chart III shows that since the sixties the world oil discoveries are lagging widely behind what would be necessary to keep the reserves level. And in fact, if we credit the existing reserves to the year in which each field is originally discovered, we can see that it is since 1950 that, in years of current production, the situation is deteriorating (Chart IV).

We know for sure that no improvement will occur, due to the dramatic unbalance between the money invested in research and production of oil and the money needed. Due to the nationalization of oil, exploration has turned now toward less politically uncertain areas, but where, if taxes are lower, the unit investment has to be much higher than in OPEC areas. Say $12/bbl. Thus the amount spent in 1980 of $60 billion means 5 billion bbl, as compared to the free world consumption of five times as much. Hidden by the present mattress of reserves, the scarcity will no doubt appear. We already know that some OPEC countries will no longer be exporting in the nineties.

At the same time this will result in a very slow change in the world distribution of reserves, which will remain, as it is today, dominated by the Middle East (see Chart V).

The quantity of oil is not the only parameter to be considered. Its geographic distribution, which will not be essentially changed within years (see Chart V), commands the reliability of the supply, which in turn has an influence on the consumer's investment, which finally determines the oil share.

A look at the well-known Middle East map (Chart VI) reminds us of the number of issues that bring and will continue to bring uncertainty to the oil supply: Turkey is ruled by a military government, periodically arguing between neighbor countries that cut the pipe-lines; the Israeli-Palestinian war; the Kurdish dispute; the Iraq-Iran war; the Iranian internal situation; the Shi-ite outburst that tends to spread all over the Arabian Gulf; the Russian presence in Afghanistan; the division of Baluchistan; the risks of closing the Ormuz Strait; the communist penetration in South Yemen; the military presence in Aden, etc. No need to comment any more. From the above, I think that we can state that oil will become scarce, and remain unsafe. It is generally recognized that it cannot compete any longer--by far--on the heat market, and one can guess that it will not recover a competitive position.

Natural gas is not in a position to inherit this outlet, apart from very specific areas, for a number of reasons: similarities with oil as far as exploration and economics are concerned, lack of flexibility in transportation, domination of the reserves pattern by the Soviet Union and OPEC countries (see Chart VII).

More attractive seems coal, due to the large reserves, relatively low cost, and a favorable geopolitical pattern with a large part of the reserves in the U.S.A., Canada, Australia, and Europe.

However, even if we set apart for a while the economic competition with nuclear, even if we neglect the fact that South Africa is supposed to play an increasing part in the supply with corresponding uncertainties, three obstacles will prevent a too-rapid development of coal:

- The need for a tremendous development of loading and transportation facilities (Chart VIII).

- The environmental problems related with coal production, transportation and price rises that, if considered objectively, largely overtake the nuclear ones (Chart IX).

- And, mainly, the unavoidable difficulty to reach directly a part of the heat market that is, as of now, satisfied with heating oil and cannot or very hardly be attained by coal itself (Chart X).

Therefore, the electric wire is the proper distribution system and we come to the direct comparison between coal and nuclear for power production. This deserves careful consideration. The nuclear builders and operators, especially in this country, have suffered so many difficulties and disillusions, expected investment figures have been so dramatically increased, that scepticism is prevailing. The absence of plant orders for the last seven years makes economic calculations apparently unreal.

It is one of the merits of the healthy French program to give a real point of reference, observing that, if it is not presently the case, there is no basic reason why the same efficiency cannot be reached by other industrialized countries.

For the sake of comparison, we will use busbar costs, that is, costs at the busbar of the power plant, established in constant dollars, and levelized for the operating time of the plant. For that purpose we calculate the present value of the power plant costs, then divide that value by the number of kWh of energy the plant is expected to produce over its economic life. Although the figures do not identify with rate calculations, they have the merit of avoiding the speculation on future inflation. The chosen discount rate for the calculation of the present value can be considered as a real rate of interest, less inflation, on utility debt, preferred stock and common stock. Here it will be 5% or near it.

Then the French costs, as recently calculated within the Union of European Utilities (UNIPEDE), show that for base load, electricity costs 1 from nuclear, 1.74 from coal and 3.86 from oil (Chart XI).

The UNIPEDE study has the merit of giving, for the various European countries, figures established according to the same method. Chart XII shows that for the three more-nuclear European countries, the results are reasonably homogeneous, all the more that satisfactory explanations can be given to the remaining discrepancies; and this gives us a reliable European average figure. The same can be done for coal power plants where the homogeneity would be excellent indeed if we discarded the subsidy included in the price of the German coal.

Evaluating an American cost is, for the above-mentioned reasons, more hazardous. Among the available studies, I chose finally to refer to a recent paper issued by the Nuclear Energy Agency of the OECD because it seems to make a fairly comprehensive evaluation of what would actually be the cost of a plant ordered for 1990-1995 (Chart XIII), and because the busbar cost is calculated through a method very close to the UNIPEDE one.

The rough comparison of Europe-USA is shown in Chart XIV. It shows an advantage of nuclear against coal of 14% in USA (Illinois) against 75% in France (% of the nuclear cost) and 67% in Europe.

By adjusting some remaining discrepancies between the OECD and the UNIPEDE methods (Chart XV), we can finally compare what is or would be in the USA the cost of electricity produced from coal (the example chosen--coal quality, location--is rather favorable to coal) with the cost of nuclear electricity under the present American conditions (Chart XVI). But the purpose of this figure is to show also what the American economy would have to gain in reestablishing favorable conditions to the realization of nuclear plants as in Europe or France.

A more careful comparison would give detailed explanations of the difference. At first glance it seems that, upon a unit investment of 1770 $/kWe versus 1053 in France, the increase in lead time for construction (see Chart XVII) explains nearly $300, the instability of regulation $100, and the remaining being tied to lack of standardization, nongrouping of several (2 to 4) units on the same site and excess of so-called "safety" constraints.

If the cost superiority of nuclear for the production of base load power seems well-established, it remains that, for psychosociological reasons, the construction of nuclear plants is a difficult job in most of the countries where nuclear opponents came out victorious in the nuclear debate.

There is no need, in this room, to discuss the safety problems themselves. We all know at the same time that the matter deserves serious consideration, and that there is no safer way of satisfying the energy needs. The active debate that was held during the past few years has located the true and false problems. Thus we are facing an irrational situation, of which, however, it is essential to find our way out, for the benefit of our economies and of our fellow citizens.

On that problem, I would like to emphasize four points, derived from past years' experience, and which explain, I think, why the French program was not blocked by the nuclear debate. I will first express those points in a rather provocative way:

1. Know why you are developing nuclear energy. Express it clearly and loudly. Put a strong coherent political will on it.

2. Establish a safety pattern (I do not say regulation) of very high quality.

3. Avoid as much as possible any public discussion on safety technical matters.

4. Convince the public that the safety system is handled by people above any suspicion.

Before commenting on those points, I would like to remind you of the tactics used by the nuclear opponents: they base their action first on the frightening power of nuclear energy derived from the Hiroshima explosion and from the unknown effects of invisible radiations. Secondly, they use the lack of knowledge of the average citizen, because if he were knowledgeable, he would not be frightened.

If we are willing to play the game on these two grounds, we shall be lost. Whatever the efforts, all the citizens will not become nuclear experts: they will not be able to follow, by themselves, the technical discussions. If we do not do what is necessary for them to recognize the true experts, anyone who talks is an expert and the best trained in the public debate technique is the one who wins. All the more so, since a nonprofessional is not embarrassed with facts, whereas the true technician has the opposite weakness. Thus, the debate in front of Mr. Smith (who knows nothing about nuclear) deals first with the key question: Is nuclear energy perfectly safe? Everybody agrees on the fact that it is not perfectly safe. But it is said to be safe enough. But how safe is safe enough? Then comes a nonconclusive debate, clear like Chinese for Mr. Smith--or rather much worse than Chinese for him, because he picks up the existence of these frightening words and expressions: critical mass, chain reaction, vapor explosion, radioactive gaseous effluent, reference accident, etc. He notices that the expert is not firm and positive on everything, that he admits that nobody is perfect and that there remains a probability of an apocalyptic accident.

And he comes back home with the idea that after all, it would be better to avoid that damned nuclear energy. That will remain his very reasonable conclusion unless something is done to convince him that there is a sufficient incentive in the reverse direction.

A careful analysis of the process leads to the above-listed guidelines.

The first idea is to change the contents, the main flavor of the concept "nuclear energy". If we discuss only or mainly the safety of nuclear energy--even demonstrate that it is safe enough--it will remain in Mr. Smith's mind that the main issue concerning nuclear energy is safety, which means that it is unsafe.

We must on the contrary talk about the necessity, the low cost, the cleanness, the advantages of nuclear energy; emphasize all the benefits that can be derived from its use, or will be derived by others clever enough to use it. And let the opponents talk alone on safety since discussing with them, in any way, on that subject, will not bring any good.

Keeping in mind that the fuel of the antinuclear movement is fear, we must avoid feeding that fear through elementary blunders. The vocabulary in itself implies danger: "radioactive waste" is worse than "nuclear waste", which is more frightening than "used fuel" or "used fuel extract". A "uranium fast reactor" would be a better name than a "fast neutron reactor," either of which is preferable to a "plutonium breeder". It is the emotional load of the words which is important. Although a "plutonium dustbin" is objectively very attractive since it allows us to get rid of plutonium, the two words "plutonium" and "dustbin" make the thing unacceptable. Who would accept a "plutonium dustbin"?

The more the subject is controversial and delicate, the more it is necessary that the people in charge--central government, local authorities--hold a simple and coherent attitude instead of paying a tribute to the unjustified fears that have developed in the public. At the beginning of the Carter Administration it was difficult for the American people to be convinced that nuclear energy was necessary and safe when the American government itself was explaining that the Pakistani, Indian, or Argentine could do without it, and that it was unsafe to let them use it.

First there are matters, simple enough, which the average citizen is able to judge. We can and must help him through popularization of knowledge and communication of data. One example would be to understand the effect of cooling on the temperature of the river.

Beyond those accessible problems, the citizen does not want to be involved personally in the technical debate. He knows his limits. He knows he has to rely on experts to judge on behalf of him. I have used the word "judge". In fact, the technical experts appointed to act on behalf of the citizens in these important and delicate matters are true "magistrates" with all the attached rights and duties.

Among the rights, I want to insist on one, essential in my opinion, that has to be respected: the right to quiet, undisturbed and unpublished work. The judge or inspector on safety must keep the right to suspect anything or anybody without his suspicion being on the front page of the "Washington Post" until he releases himself the results of his inquiry and calculations if they lead to a real issue. Doing otherwise is not increasing democracy. It is demagogy. It mainly results in confusing the people with premature and superficial problems that will turn out 99 out of 100 times to be of no interest. And it will induce the experts to retain only the issues that they know in advance to be substantial, which will not favor safety.

The counterpart of this "zone of calm" is of course an increased responsibility. If the citizens accept to rely on a body of "technical magistrates", they expect them, of course, to work at least as seriously as if they were in the open light and they do not accept implicitly that the privilege of knowledge be used improperly. Some system must be provided so that some higher authority can at last resort overlook the experts. I experienced that once. Cracks had been discovered in some nuclear equipment, and studies were on the way to confirm the harmlessness of these imperfections, when an unexpected press release started a very emotional nation-wide controversy. The emotion approached the TMI fallout in our country. We were able to control it first because the technical work of the people in charge of controlling safety was beyond reproach, and secondly because we were able to call a panel of the Academy of Sciences as a guarantee of the quality of that work, the publication of which I authorized, but only when it was fully established.

Such general considerations explain the guidelines I was suggesting earlier.

Where the technical debate is useless and even harmless let us not feed it if we can avoid it. Let us, anyway, be very careful in the language we use in front of the nonspecialized people, in order to avoid giving any help to those who try to cultivate both their fears and their lack of expertise.

Let us on the contrary insist on the reasons that justify the development of nuclear energy and make it desirable. Consequently, the authorities' attitude must be completely in phase with these considerations, and they must apply firmly their political will toward this achievement.

As far as the safety problems are concerned, the basic duty is for the authorities to reach high standards and to establish an organization that gives the best guarantees. This does not mean the hardening of constraints and the development of regulations; but rather a sound and clear organization of responsibilities between builders, operators, regulators and inspectors with a high regard for the competence of the people involved.

This being done, the decisions must be the result of democratic choices, but demagogy would be as harmful as usual. The technical complexity of nuclear energy makes it necessary that the citizen rely on a body of experts to control the safety problems. These experts must be put in the most favorable work conditions which imply that normally their work be published only when they feel it deserves to be published; but the citizen has the right to ascertain that the mandate thus given

to these experts is properly fulfilled. Provisions have to be made so that their conclusions can be checked in important instances.

You are accustomed to discussing and solving technical matters. The quality of your work is a necessary condition to the development of nuclear energy. But this is not enough and it would be of little use if your fellow citizens were not convinced at the same time that you are achieving your goals and protecting them. This congress should be very useful in that respect.

Let me express the wish that the nuclear community be as successful in the nuclear debate as it has been in nuclear technology, so that mankind will be able to take advantage of this attractive source of energy.

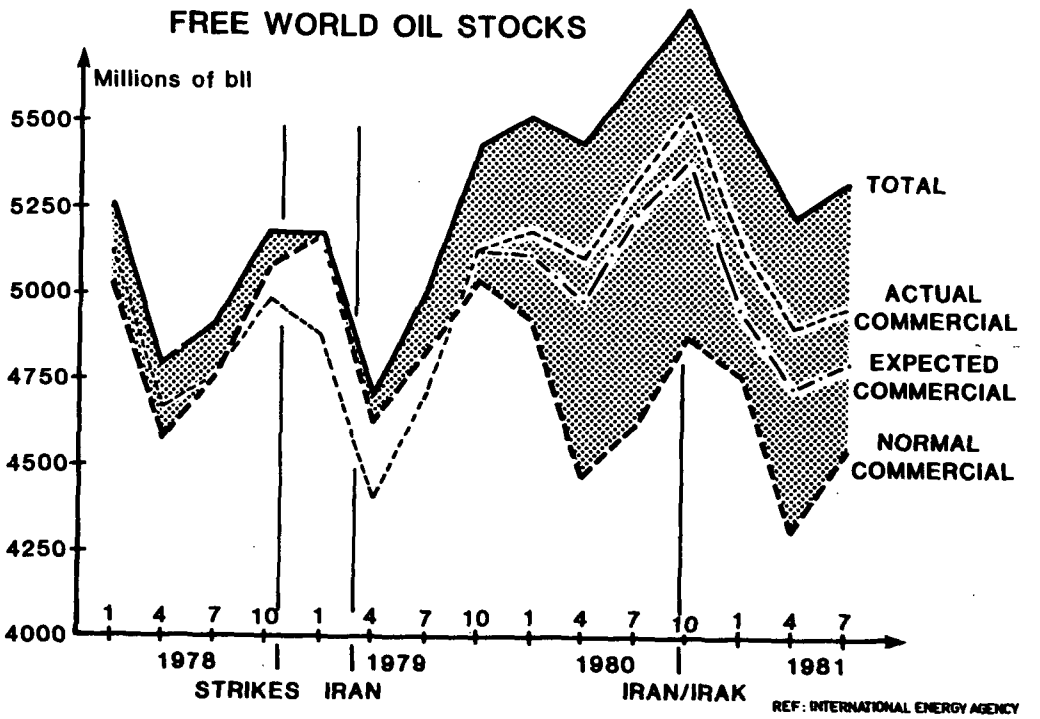


Chart I.

US. CRUDE OIL AND PETROLEUM PRODUCTS IMPORTS

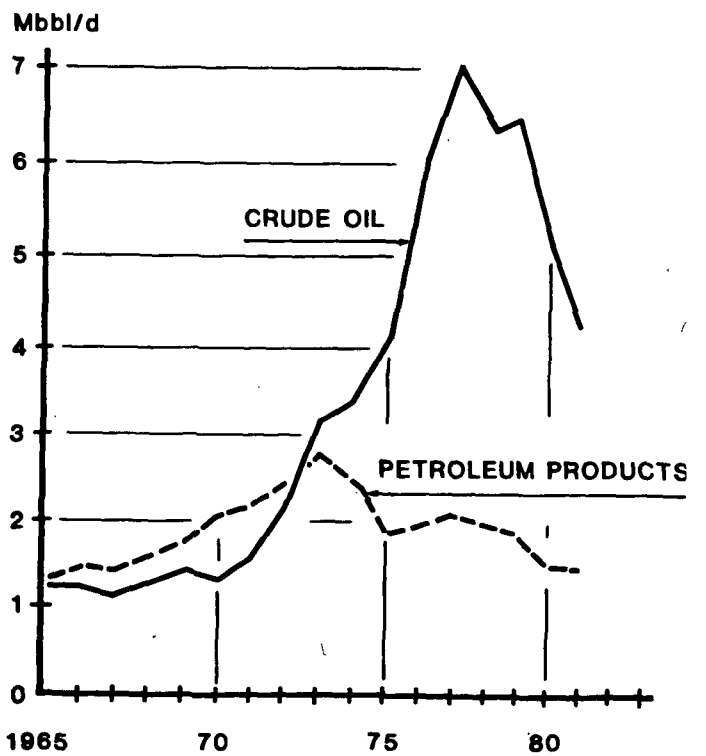


Chart II.

WORLD OIL DISCOVERIES

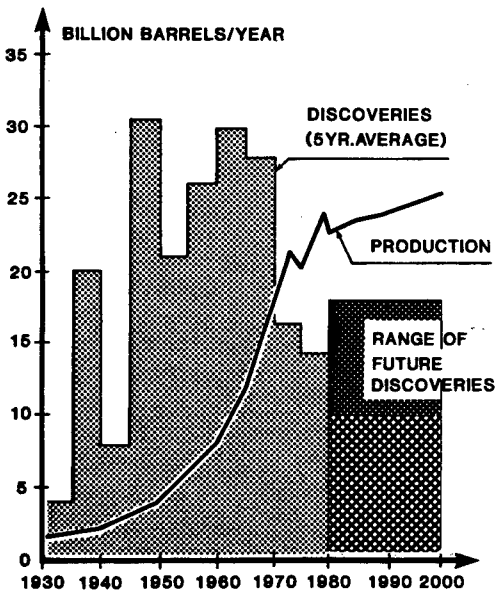
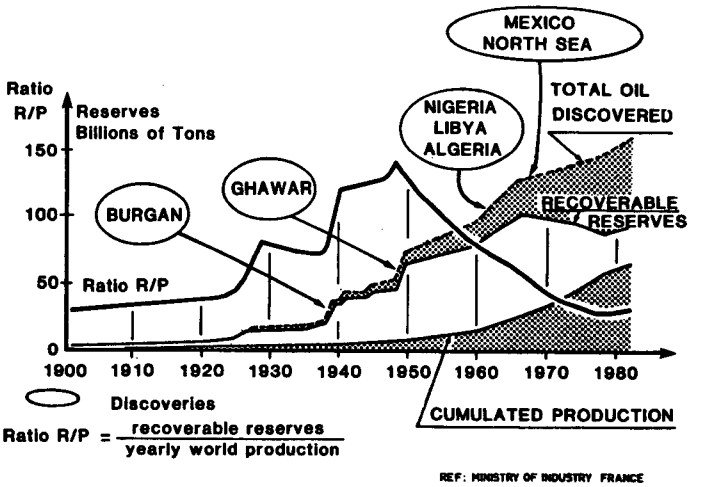


Chart III.

CRUDE OIL RESERVES EVOLUTION



REF: MINISTRY OF INDUSTRY FRANCE

Chart IV.

TOTAL DISCOVERED OIL

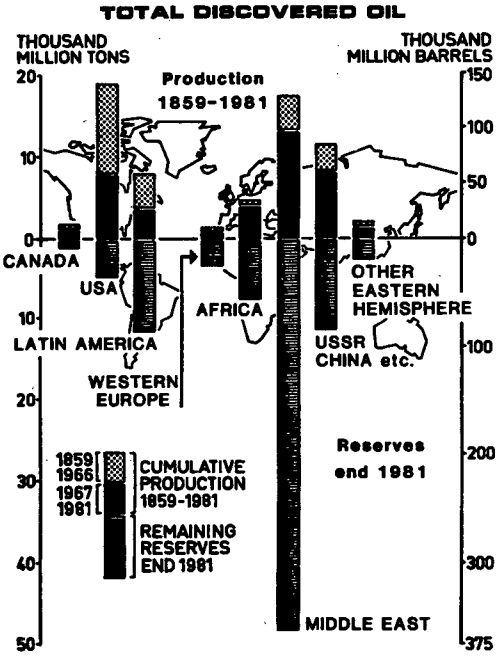


Chart V.

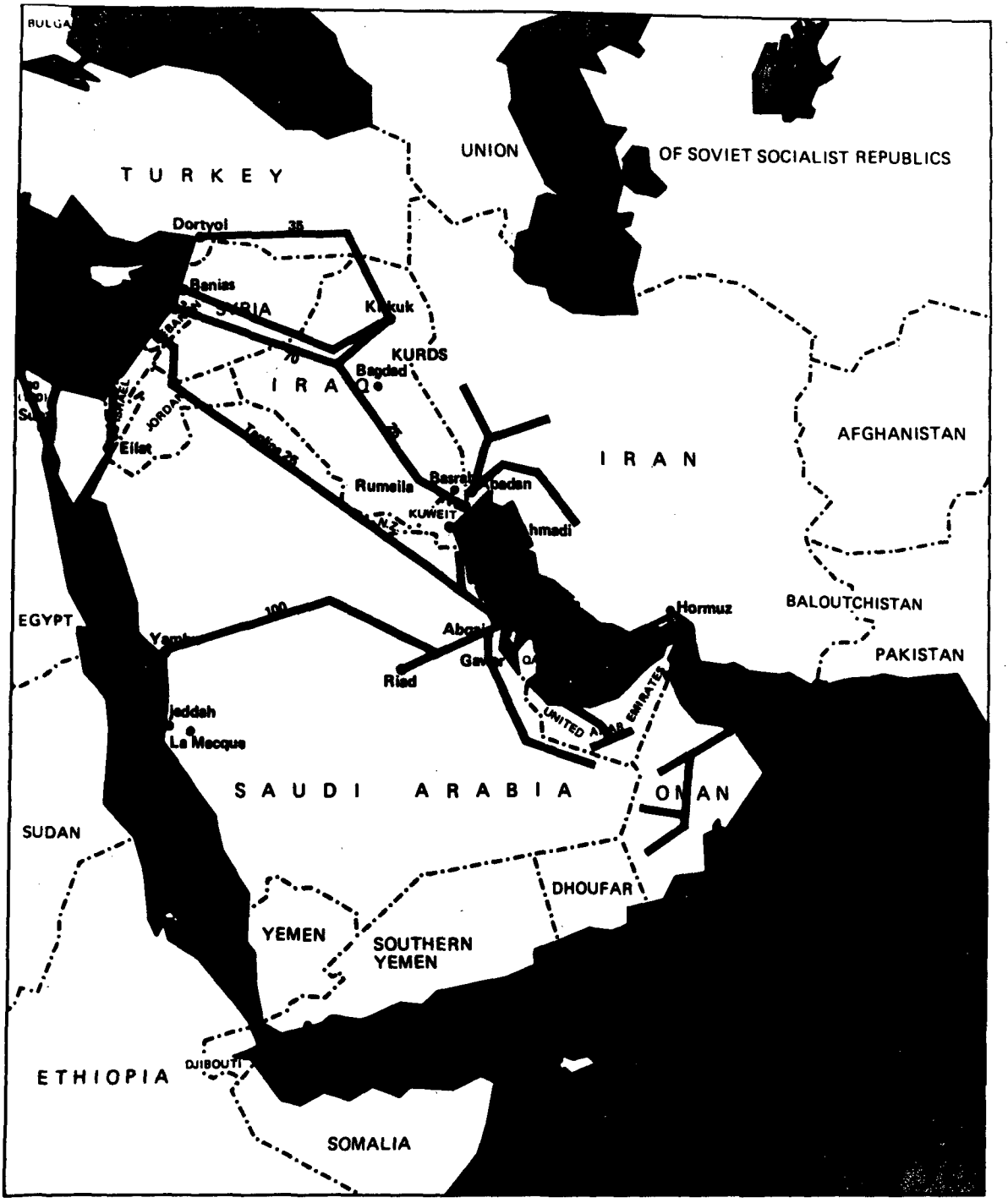

TURKEY
UNION
OF SOVIET SOCIALIST REPUBLICS
Dortyol
35
Banias
SYRIA
Kirkuk
KURDS
Bagdad
IRAQ
70
ISRAEL
JORDAN
Eilat
Rumeila
Basrah
Abadan
KUWEIT
Ahmadi
IRAN
AFGHANISTAN
BALOUTCHISTAN
PAKISTAN
Hormuz
EGYPT
100
Yanbu
Abqaiq
Riad
Jeddah
La Mecque
UNITED ARAB EMIRATES
SAUDI ARABIA
OMAN
SUDAN
DHOUFAR
YEMEN
SOUTHERN YEMEN
ETHIOPIA
DJIBOUTI
SOMALIA

Chart VI.

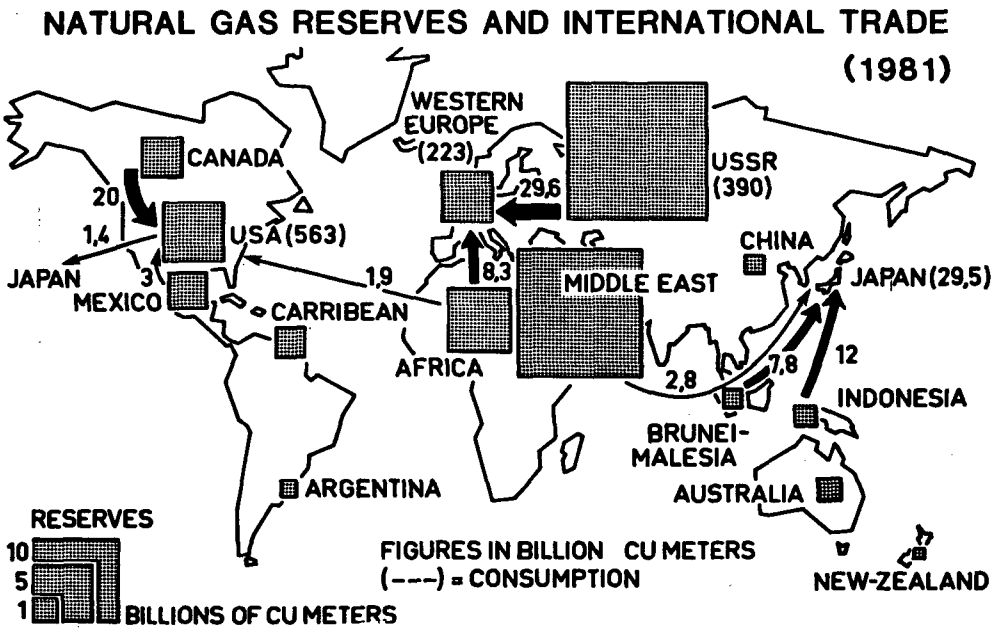


Chart VII.

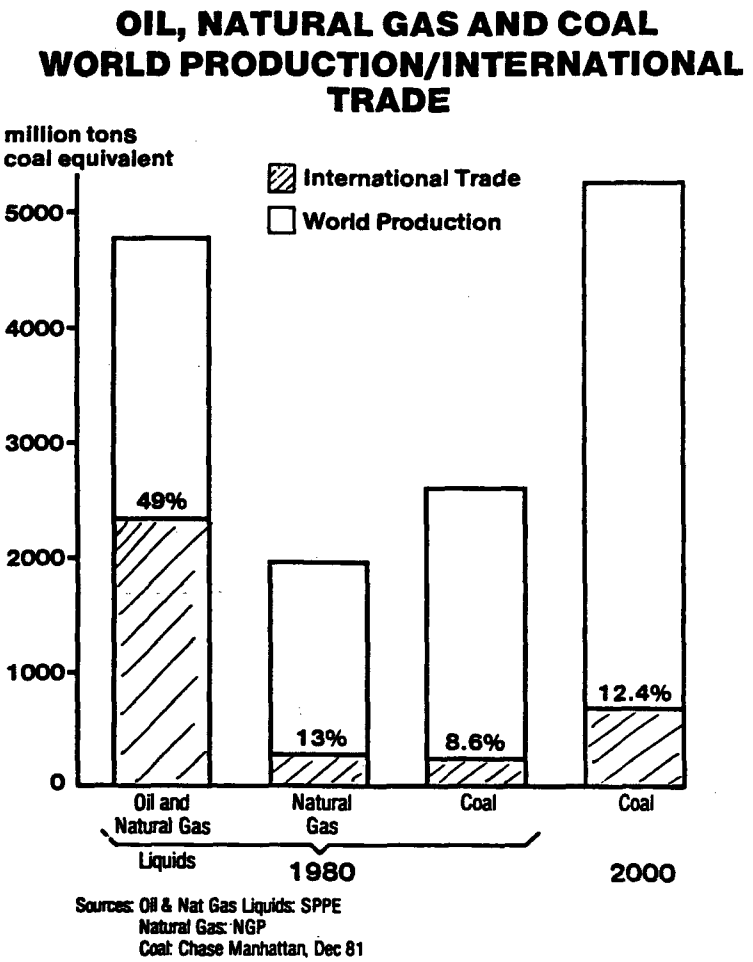


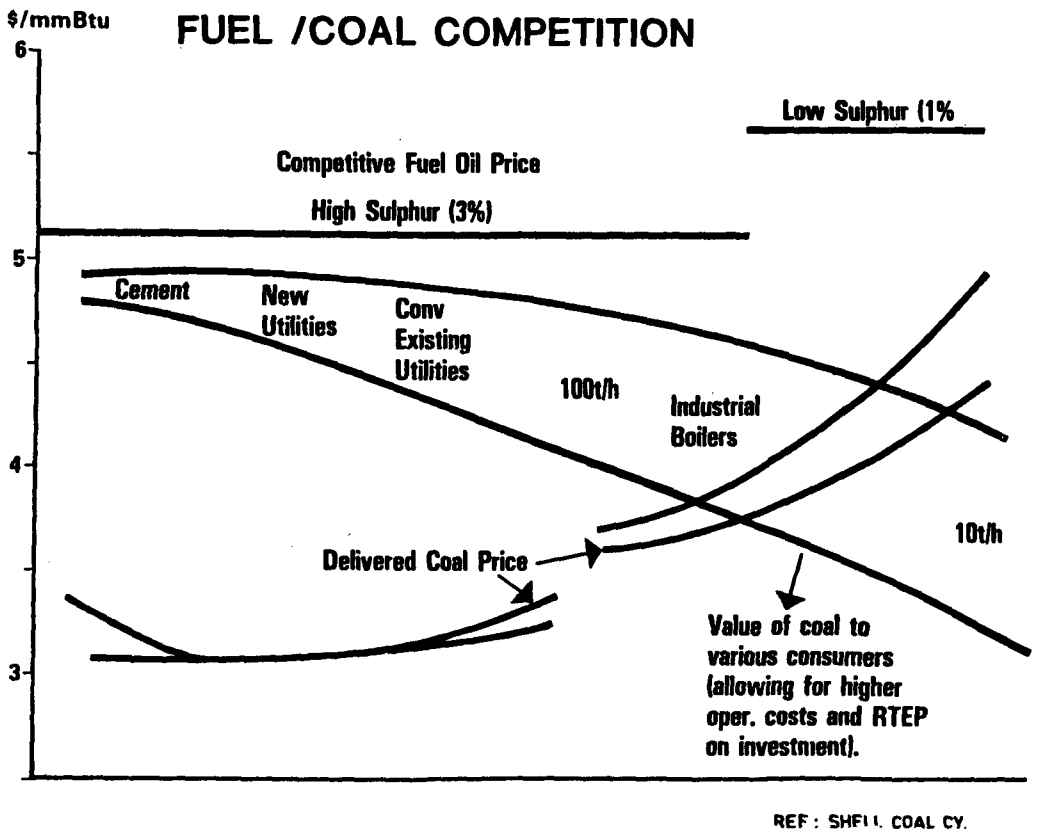
Chart VIII.

POWER PLANT NUISANCES (5000 Mw)

	COAL	NUCLEAR
CO_2 T/yr	40 000 000	0
SO_2 T/yr	200 000	0
NO_2 T/yr	50 000	0
FINES T/yr	30 000	0
FINES WITHOUT SCRUBBERS T/yr	2 000 000	0
ASHES T/yr	2 000 000	0
HIGH ACTIVITY WASTE m3/yr	0	70
MIDDLE & LOW ACTIVITY WASTE m3/yr	0	2 500
RADIOACTIVITY DILUTION		
AIR billions m3/yr	50 to 1 500	400
WATER m3/s	0	60
FUEL TRANSPORTATION	120 000 100 TONS CARS	A FEW TRUCKS

REF : EDF

Chart IX.



REF : SHELL COAL CY.

Chart X.

FRANCE
ELECTRICITY COST:M/kWh
(PLANT OPERATION 1990)

	NUCLEAR	COAL	OIL
CAPITAL	13,25	10,78	9,22
O & M	4,68	3,77	3,25
FUEL	8,96	32,47	91,32
TOTAL	26,89	47,02	103,79
RATIO VS NUCLEAR	1	1,74	3,86

"BUSBAR COSTS" : DISCOUNT RATE 5% - CONSTANT $ OF JANVIER 1981

REF : UNIPEDE JUNE 1982

Chart XI.

EUROPE

PLANT OPERATION 1990

NUCLEAR ELECTRICITY COSTS M/kWh

	FRANCE	BELGIUM	FRG	AVERAGE
CAPITAL	13,25	16,37	20,52	16,76
O & M	4,68	7,40	6,11	6,11
FUEL	8,96	8,83	10,65	9,48
TOTAL	26,89	32,60	37,28	32,35
RATIO/ AVERAGE	0,83	1,01	1,15	1

Chart XII.

COAL ELECTRICITY COSTS M/kWh

	FRANCE	BELGIUM	FRG	AVERAGE
CAPITAL	10,78	7,66	10,26	9,61
O & M	3,77	4,16	7,79	5,20
FUEL	32,47	33,64	52,22	39,49
TOTAL	47,02	45,46	70,27	54,30
RATIO/ AVERAGE	0,87	0,84	1,29	

Ref UNIPEDE june 1982

Busbar costs - Discount rate 5 % - Constant $ of jan 1981.

OECD STUDY (REYNOLDS)

CAPITAL RELATED COST =

BASE COST : EEDB(ENERGY ECONOMIC DATA BASE)

+ ADDITIONAL RESULTING FROM TMI
+ AVERAGE REAL ESCALATION : 2%/yr
+ CONTINGENCY 20%
+ INTEREST DURING CONSTRUCTION *
+ COST OF DECOMMISSIONNING

* LEADTIME : 98 TO 140 MONTHS

Chart XIII.

COMPARISON (NON ADJUSTED) EUROPE-USA

	NUCLEAR			COAL		
	FRANCE*	EUROPE*	USA**	FRANCE*	EUROPE*	USA***
INVESTMENT $/kWe	1053	1326	1770	851	757	1096
COSTS (MILLS/kWh)						
CAPITAL	13,25	16,76	30,21	10,78	9,61	19,66
O & M	4,68	6,11	2,78	3,77	5,20	8,60
FUEL	8,96	9,48	8,68	32,47	39,49	18,98
TOTAL	26,89	32,35	41,66	47,02	54,30	47,24

1,14

1,75

* UNIPEDE JUNE 1982
** OECD STEERING COMMITTEE FOR NUCLEAR ENERGY JUNE 1982
*** OECD " " : PLANT LOCATED IN ILLINOIS ; HIGH SULFUR BITUMINOUS COAL

Chart XIV.

BUSBAR COSTS PARAMETERS

	UNIPEDE	OECD
ECONOMIC LIFE yrs	20	30
DISCOUNT RATE %	5	4,3
HOURS OF FULL PRODUCTION	1st year 3000 2nd 5000 3rd-20th 6600	65% (5700H)
DATE OF OPERATION	1990	1995
$ OF	jan 81	jan 80

Chart XV.

BUSBAR COST OF ELECTRICITY IN THE USA

PLANT OPERATION 1990

CONSTANT $ JAN.1981

	NUCLEAR ASSUMING CONDITIONS OF			COAL
	FRANCE	EUROPE	USA (PRESENT)	USA*
INVESTMENT $/ kWe	1053	1326	1770	1096
CHARGES				
CAPITAL	13,25	16,76	23,80	14,73
O & M	4,68	6,11	2,78	8,60
FUEL	8,96	9,48	8,68	18,98
TOTAL	26,89	32,35	35,26	42,31
RATIO COAL/NUCLEAR	1,57	1,31	1,20	

* PLANT LOCATED IN ILLINOIS,HIGH SULFUR BITUMINOUS COAL

Chart XVI.

LEAD-TIME FOR THE CONSTRUCTION OF NUCLEAR PLANTS

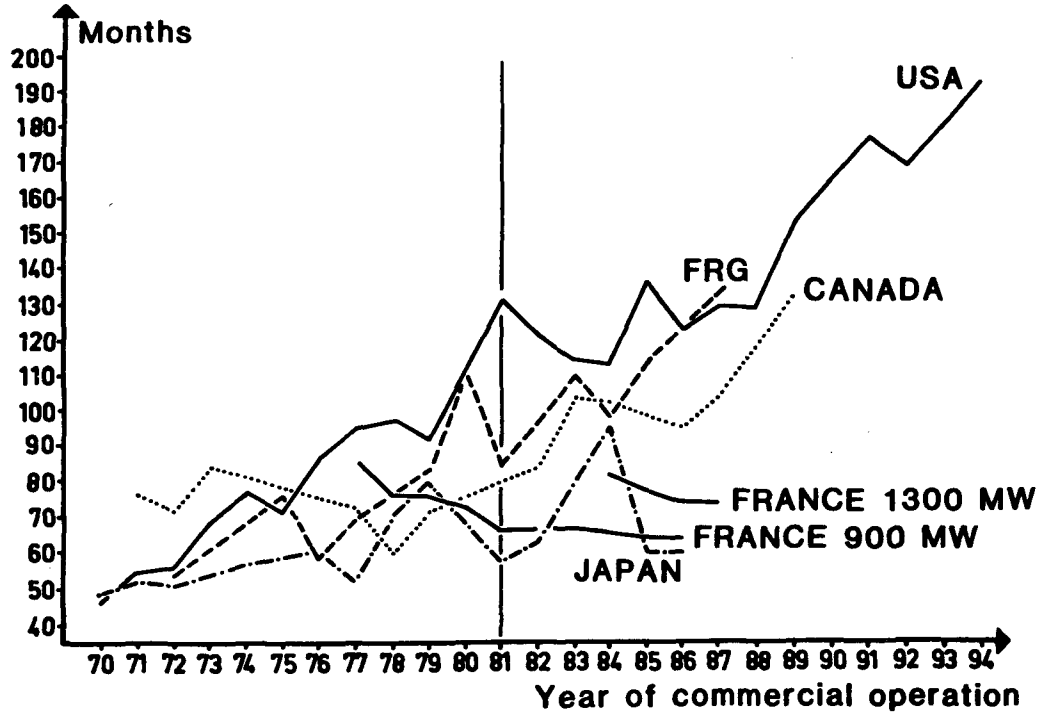


Chart XVII.

MAN-MACHINE RELATIONS IN NUCLEAR ENERGY--AND ELSEWHERE

André Gauvenet
Electricité de France
Paris, France

1. INTRODUCTION

Over the ages, man's relations with the machines he has created for his use have varied constantly and considerably. These relations have varied because the machines have evolved and because man's behavior has also changed, both in itself and in its relations with machines. It is interesting to note that, in its attitudes to nuclear reactors, human behavior has changed a great deal.

At the beginning it was a miracle machine, but one should not forget the initial calculations made by the Fermi team who were afraid that reactors would be inherently unstable, and that it would be necessary to be able to stop them by emergency action. Other scientists even felt, with regard to tests of nuclear explosive devices, that there would be instability that might be communicated to the whole of our planet.

Consequently, human behavior was not very rational with regard to this very special machine, which was endowed with divine (or maleficent) powers: some people erred in the direction of excessive optimism, and others in that of excessive pessimism. And this "equilibrium" has varied over the years.

In 1956, as Dyson recalls in his book "Disturbing the Universe," a working group was set up under the aegis of Frederic de Hoffmann and Edward Teller to build a nuclear reactor that would be safer than any other. Teller gave this group the task to design a reactor that would be so safe that it could be put in the hands of a group of "high-school" children. The idea here was to solve the human problem by eliminating it completely.

This led to the Triga reactor, which had great success as a research reactor and which is indeed extremely safe, so safe that some of its sponsors said that it could not only be entrusted to the high-school kids, but also to their teachers.

At this time, and even later on, the human problem was thus treated very globally.

It is significant in this respect that an official U. S. document on safety in nuclear power plants, published in April 1979 a few days after the accident at Three Mile Island (which means that it was written before), says nothing at all about the human factors. Was too much importance given then to technical problems? Too little to human problems?

Aerospace technology, which has often served as a model for nuclear safety, attached enormous importance to human problems right from the beginning. It must be said that to launch a man into space by a rocket, to make him orbit the earth and to send him to land on the moon, raise obvious human problems of physiology and psychology.

But "conventional" aeronautics has for a long time attached very great importance to these problems. It is only since the Three Mile Island accident that we have really become aware of the human factors in the reliability and safety of reactors and nuclear plants.

Have we done enough in this field? Have we perhaps done too much? The history of relations between men and machines is significant in this respect. We often move from one situation to its opposite, without really finding a balance.

2. MEN AND MACHINES IN THE PAST

The first form of machine was the tool: it was understandable, useful, but often dangerous. Between tools and weapons there was sometimes little difference, when we are talking about knives and picks, for example.

Tools sharpened man's senses and muscular strength; the true machine, whose development dates especially from the 18th century, amplified this strength by the use of power: steam.* In its initial form it replaced and multiplied the abilities of slave labor.

Man thus had the prospect of a tool that would do him great service: the mechanical slave, powerful, of doubtful reliability at the beginning, of course, but at any rate, obedient. There would be no more fears of strikes or revolts (at least when the machine was used by artisans, small businessmen or housewives).

But in factories--even in small factories--the workforce very soon began to worry that they would be replaced by the machine. Social and mental change did not keep pace with technical change. This has always been the case.

At different times, depending on the categories of people involved, machines have been an object of admiration or fear, and the two feelings have often been mixed. They have grown in intensity when the machine has developed firstly in the direction of great size (creating both power and danger), and secondly in the direction of intelligence.

These feelings have become stronger when the design and use of modern machines have been provoked by war and defense needs. The use of nuclear fission or fusion for peaceful purposes and sometimes for military purposes is not, strictly speaking, a question of machinery, but rather the use of an energy of inordinate proportions, hitherto locked up in the heart of matter, a kind of violation of nature. Einstein and Hahn were a new incarnation of Prometheus, who defied God, and acquired forbidden knowledge.

The Swiss mathematician, Weyl, wrote in 1923: "Matter conceals within itself--because of Einstein's formula ($E = mc^2$)--a prodigious source of energy. Thank heavens, man is not capable of liberating it." He, incidentally, eliminated this phrase from later editions, even before fission had been discovered.

Note, however, that the first philosophical revolts against technology, after that of Rousseau in the 18th century, occurred in Europe (particularly in Germany) at the beginning of the century. And Sigmund Freud in 1932 wrote a book on these anxieties (Malaise in Civilization) in which he used a phrase with a very modern connotation: "Humanity has acquired the power to destroy itself," at a time when atomic fission was not known.

This shows that the fears caused by technology are several decades old and that this heritage was passed on to the atom, when all anxieties linked to machines were added to the fear of an "explosive" energy.

*Obviously, the motive power of air and water had already been used, but in a way that was still peaceful and limited.

3. MEN AND MACHINES TODAY AND IN THE FUTURE

The technological revolution has taken place in all sorts of directions. Machines have become: much more powerful, much more complicated (understood by specialists only), and much more reliable (because of the astonishing progress made in electronics). The machine is in the course of becoming "intelligent": though sometimes it is given devices which look like sense organs, it has no emotions.

As an example of a modern machine, I shall quote a brochure dealing with the new 767 plane, to be put in operation quite soon in the United States:

> "From just after takeoff until after the landing rollout, the 'Flight Management System' controls the airplane with a precision impossible for the most capable pilot....And wherever possible, backup systems automatically handle inflight failures if a malfunction occurs. With the new systems, pilots have not surrendered an iota of control; in fact, they have gained a great deal."

This is a wonder machine that we wish we could use to operate a nuclear reactor. Its concept is certainly well-accepted by the public, as airplane flights are not felt the way nuclear energy is.

What can man do in the face of this new machine? How can man, who, it is said, still closely resembles his ancestor of 40,000 years ago in his emotions, his intelligence and fears, succeed in:

- -associating himself closely with a machine which a priori is so strange to him,
- -controlling it and if necessary correcting its faults,
- -ensuring that no advantage is taken of the machine's fragile nature to cause damage deliberately?

4. THE AREA OF INCIDENTS

Now that machines have become apparently so reliable if properly used, it is clear that, in modern technologies, the principal cause of incidents and of their aggravation becomes man himself. This is true on the roads, where automobile accidents are now usually due to human failure (alcoholism, sleepiness, errors of all kinds). It is true in flying, where, despite the theoretically critical aspect of the technical functions assumed by the aircraft's instruments, most of the accidents are due to human failure. It is probably becoming true in nuclear power stations, where incidents are likely to become more serious when operators are not alert or because of their wrong reaction.

It used to be said not so long ago that accidents were acts of God. After an era (which is not yet over) during which the blame was essentially placed on technology, we now see a time coming when accidents, apart from natural catastrophes, will be considered acts of man.

This belief is becoming so profoundly anchored in people's minds that we now tend to look for human responsibility even in the case of earthquakes or hurricanes, not in respect of the causes of such catastrophies, but in respect of their consequences, because it is felt, somehow, that man should be capable of predicting the catastrophe or at least giving an alarm or minimizing its consequences.

Let us get back to nuclear energy. I do not intend to lecture you on psychology or to elaborate on what is, in fact, one of the very subjects of this conference. I would just like to mention two points which I believe must be looked into; in doing so, I shall pass over all the problems of training, education, incident simulation, and the taking into consideration of human psychological states.

Here are the two examples:

1. What happens when there is an incident? Our aeronautical colleagues have some prescriptions. Imagine, they say, a pilot in the course of a routine flight. If something abnormal happens (to the engine, or in the sky: for instance a risk of collision), the machines must:

a) firstly act alone, because man is then not in a position to act quickly and intelligently;

b) give orders that the pilot can execute, without any explanation which would disturb him.

This probably applies also in a power station, with certain differences.

First we may note that in the case of a nuclear incident, while the first actions are extremely important in the development of this incident, one generally has some time before it reaches a critical state. This period may be used for thinking, if the situation does not correspond clearly to one which has already been predicted. This demands intelligent reasoning, and possibly putting aside certain established procedures.

The normal operator is there to apply the rules. Infringing them would constitute a fault: he is and must be like a part of the machine. It is therefore necessary to bring in someone else. The transition from the strict application of the rules to a new thinking is very delicate. The interplay of the operator and his counselor demands a specific study of the problems that may arise between the two men who are trying to control the machine. It is a three-component system with two men involved.

It should be noted that these new situations are rare and will become more and more so as time goes by and operating experience accrues, with the systematic operation of power stations on an international scale.

2. Just as I have mentioned a case in which two men are dealing with a machine, and with each other, I shall define the "operator-reactor" problem as follows: there is in actual fact one man (sometimes more) who is coping with two machines.

For the reactor itself is a complex machine, by its nature at one and the same time hydraulic, thermal, and mechanical; the nuclear part proper only plays a clearly limited role. As one of the pioneers of nuclear energy in France, Professor Yvon, used to say: "There is nothing nuclear in a nuclear reactor."

This first machine is, in fact, a machine just like earlier ones, with pumps, valves, joints, and fluid. None of that is very reliable and much time has to be spent to maintain all the elements of this complex whole in proper order.

The other machine is the instrumentation, the control mechanisms and the computer, whose role it is to understand and interpret the first one. This is of a quite different nature. It is reliable (though the operator must still be convinced of this reliability and be able to check it: how many incidents in the past have followed from a lack of confidence in the measuring instruments!). It is reliable in its data. Is it reliable in its interpretations?

It is, in any case, a machine of the second type. The limit between it and the man who serves it will evolve in the future towards greater speed, greater reliability, more thought, and in the last resort, more intelligence.

It is this machine that must provide (and very quickly) the immediate data about the incident and take the first action (dropping the control rods, to begin with). It is this machine that must then seek to explain and provide advice, and we may consider that it will go further and further in this direction in the future along a carefully planned route.

These dialectics between man and machine (the second machine) are comparable to the efforts made by science to understand life. The limits of the living organism that are accessible to science will be continually pushed back, though one will never be able to solve biological problems in their entirety. Similarly, the part played by the intelligent machine in the action and decisions to be taken will increase continuously, though the operator and his advisor will never be eliminated. They will remain the last resort.

We still have the problem of giving these men interesting work to do in the very long periods during which the two machines get along with each other and leave no place for human intervention.

5. CONCLUSION

I will not push any further this rapid and somewhat subjective analysis of the relations between man and machine. In the last resort, the problems seen from a certain point of view which leaves aside their more emotive aspects can be symbolized as follows:

> In what circumstances can the machine be considered sufficiently intelligent to act alone?
>
> In what circumstances must man be considered as subject to error?

On this last point, I would tend to reply: however well-trained and intelligent he is, man will always be prone to error. Our whole system must be based on this fact. Machines and men must constitute an integrated and self-correcting system. It is up to the specialists to know the system as well as possible, and to improve it. I hope we are now on the right road.

SESSION 1

CURRENT ISSUES IN NPP SAFETY

Chair: N. C. Rasmussen *(MIT)*

Panel Discussion on

CURRENT ISSUES IN NPP SAFETY

Chair: N. C. Rasmussen *(MIT)*

Panelists

A. Birkhofer *(GRS)*
G. L. Brooks *(AECL)*
H. R. Denton *(NRC)*
S. Hamaguchi *(FEPC)*
M. Rosen *(IAEA)*

THE USE OF PROBABILISTIC RISK ASSESSMENT FOR SAFETY EVALUATION

A. Birkhofer

Gesellschaft für Reaktorsicherheit (GRS) mbH
Garching, Federal Republic of Germany

ABSTRACT

Probabilistic methods to analyse performance aspects of complex systems have become a powerful tool for safety evaluations. Since a survey of the use of probabilistic risk assessment (PRA) on the nuclear field in the F.R. Germany has been given at the IAEA Conference in Stockholm in the fall 1980, this paper describes more recent developments and applications. This is the use of PRA on the nuclear field in licensing procedures, in studies aimed at comparisons, and in R&D activities. Especially the recently performed quantitative comparison of a PWR (type Biblis) with the fast breeder reactor SNR-300 will be discussed in more detail. Obviously, probabilistic methods will increasingly be incorporated into decision-making in various fields, especially in the nuclear field.

INTRODUCTION

Probabilistic methods to analyse performance aspects of complex systems have become a powerful tool for safety evaluation. Aircraft and space technology have pioneered in this area. However, the application in the nuclear field has promoted controversial discussions about its advantages and disadvantages. The discussion became very emotional when the probabilistic analysis was further developed into risk estimation, especially since the publication of WASH-1400 and later the German risk study [1, 2].

Nevertheless, since several years a tendency has become clear to increasingly incorporate probabilistic methods into decision-making in various fields, particularly in the nuclear field.

I refer to the ongoing discussions in a number of countries to use probabilistic risk assessment (PRA) for the evaluation of siting conditions, backfitting measures and safety goals.

A survey of the use of PRA in the F.R. Germany has been given at the IAEA Stockholm Conference on "Current Nuclear Power Plant Safety" in the fall 1980 [3]. Therefore, I will present only developments and applications that have been experienced during the last two years.

This paper will describe three lines of arguments as to how PRA can be used in the nuclear field: in licensing procedures, in studies aimed at comparisons, and some remarks within the framework of R & D activities.

PRA IN THE LICENSING PROCEDURE

The deterministic analysis of systems behaviour and effectiveness is an essential part of the safety evaluation in the licensing procedure. In addition, probabilistic methods to support safety decisions have already been used for quite a long time. Recently, probabilistic arguments, especially to estimate the reliability of complex systems under postulated accident conditions have been playing an increasingly important role.

Typical examples are analyses of small LOCAs and of transients such as loss of heat sink, loss of main feedwater and loss of off-site power. In many cases results from the German risk study were used as reference values.

Another example concerns the use of probabilistic analyses for the classification of incidents and accidents within the Radiation Protection Ordinance. In the F.R. Germany, there are some specialities of the Radiation Protection Ordinance compared to other countries. For example, the basis of planning and design of constructional safety measures and of the engineered safeguards of nuclear installations is such that in the case of design basis accidents a maximum of 5 rem whole body dose must not be exceeded in the environment of the plant.

Probabilistic arguments may help to define classes of events which are dealt with in the Radiation Protection Ordinance. Three types of events may to be distinguished:

- The operating license for normal operation covers events of moderately low frequencies with small fission product releases.
- Events of low to very low frequencies, which are not to be expected during the lifetime of either a single plant or of all plants which will be in operation sometime in the future. Typical examples are design basis accidents. These events may result in fission product releases leading to a maximum individual whole body dose of 5 rem.
- Events of extremely low frequencies where either typical or bounding accident sequences are very difficult to describe. Such events or sequences can better be described by scenarios. Examples are events like crashes of large commercial or military airplanes, degraded core cooling, partial or complete core melt.

  A consistent design against all major aspects of these events is extremely difficult - if not impossible. Cost-benefit arguments for this class of events play a substantial role. Also, design measures to mitigate a certain hypothetical accident may have neutralizing or even disadvantageous effects on other accidents.

  A typical example is the core catcher. One might design a structure to cool a molten core underneath the vessel for large guillotine breaks if emergency core cooling systems are considered non-functional. However, such a device could fail to cope with a different hypothetical accident, namely a small loss-of-coolant accident without ECCS or a severe transient event with loss of heat sink. In those cases core melt under high system pressure could happen and the impact of the thus failed vessel would destroy the structure of present design core catcher. In a probabilistic analysis, the pros and cons of safety devices to mitigate severe accidents can be assessed. However, one has to use expert's opinion to a large extent in order to generate the requested subjective probability distributions.

Very recently, results of risk analyses have been considered in legal decisions by administrative courts. It is typical for German nuclear licensing procedures, that objections have been raised against nearly every license. Administrative courts (Verwaltungsgerichte) of the individual states (Bundesländer) deal with these objections in the first instance. Courts of second instance are administrative courts of appeal (Oberverwaltungsgerichte bzw. Verwaltungsgerichtshöfe) of the states. These

administrative courts of appeal make the final decision on the facts. The last instance is the federal administrative court (Bundesverwaltungsgericht) as court of revision, which only deals with points of law.

In its decision on the law suit of nuclear opponents against the construction permit of the Whyl nuclear power plant the administrative court of appeal Mannheim has made use of results of the German risk analysis. This administrative court decision is of fundamental importance for the assessment of technical safety measures and for the risk definition, which has to be born by the general public. I will quote:

"At present possible estimations of the risk due to the operation of nuclear power plants do not indicate that the risk of accidents caused by the operation of a KWU-PWR of the 1300 MWe series is out of proportion and therefore unacceptable to the individual." End of quote.

Another quote is: "In order to convince the administrative court of appeal, importance lies not so much in the figures coming out of the individual investigations, but in the order of magnitude of the risk resulting from accidents of nuclear power plants, in comparison to other risks, as has been performed - at least partially - in the German Risk Study. Despite the uncertainties of individual results an order of magnitude risk estimation is possible." End of quote.

A third quote is: "There is no basis visible for objections against the fundamental results of the German Risk Study." End of quote.

Great efforts are being made to improve the data basis of nuclear power plants through field experience. By means of such improvements, the reliability of safety systems can be predicted more accurately.

For example, the surveillance of component failure can be used to monitor the quality of different components.

Continuous effort is made to improve the data basis for component failure rates by field experience. Component failure rates used in the German Risk Study were mainly based on literature data, taken from process industry and conventional power plants.

In figure 1, data for motor-operated valves and for pumps (including motor starters and control devices), as used in the German Risk Study, are compared with those from operating experience in the Biblis nuclear power plant. The data are mean values. As a result of this comparison one can see, that the received operating data fit well into the error bands of the data of the German Risk Study.

PRA FOR QUANTITATIVE COMPARISONS OF DIFFERENT REACTOR TYPES

PRA have also been used for quantitative comparisons of different reactor types. I would like to spend some time on this subject.

Recently, the fact-finding committee on "Future Nuclear Energy Policy" of the German Federal Parliament in July 80 recommended a study on the accidental risk of the SNR-300, the German fast breeder prototype reactor under construction in Kalkar, in order to facilitate a comparative safety evaluation between the SNR-300, and a modern pressurized water reactor of the type Biblis B.

The safety features of the SNR-300 make a core destruction highly unlikely. However, since the SNR-300 is a prototype reactor and since operating experience with sodium cooled breeder reactors is limited, the SNR-300 has been designed to prevent significant releases of mechanical energy.

Important safety features for the mitigation of core destructive accidents are as follows:

- Reactor tank and primary system are designed to withstand mechanical energy releases up to 370 MJ.
- Core internals are designed such that core debris can be cooled within the tank. In case of melt through, molten fuel is collected and cooled in the core catcher underneath the tank.
- Decay heat removal is possible by passive means.
- The plant wiil be equipped with a double containment system.

Let me now turn to the risk analysis.

Figure 2 identifies in form of a flow diagram six groups of accidents which may initiate core destruction. The core can be destroyed either through rapid nuclear power excursion, usually called "core disruptive accident", or through slow melt down.

Core destruction through nuclear excursion can occur if a failure to scram is postulated.

Potential causes for reactivity increases are

- displacement of sodium from core,
- unprotected reactivity addition, and
- fuel pin failure propagation.

Potential causes of displacement of sodium could be gas bubbles in the core area or sodium boiling. The introduction of gas bubbles into the core is prevented by passively acting devices. The prevention of sodium boiling requires active measures and therefore warrants a more detailed consideration.

Sodium boiling may occur in case of insufficient coolant flow through the core or insufficient heat removal to the heat sink, and if this combines with a failure of reactor scram. These events correspond to groups 1 and 2, designated as "Unprotected Loss of Flow" and "Insufficient heat removal without scram", which is similar to an "Unprotected Loss of Heat Sink".

Unprotected reactivity addition and fuel pin failure propagation have been analyzed in the study. Their effects are covered by the treatment of groups 1 and 2; they are not further discussed in this presentation.

The core could also be destroyed after reactor a scram, due to an imbalance between the decay heat generated in the core, and heat removed from the primary coolant. Possible causes are

- loss of active and passive decay heat removal capability without loss of coolant (which is group 5 on the slide), or
- loss of decay heat removal capability in case of primary coolant boundary leakage, which is group 6 on the slide.

These six groups of core destruction initiators comprise all conceivable courses, potentially leading to core destruction. Each of these core destruction initiators can themselves be caused by various accident initiators.

Expected frequencies of core destruction initiators have been calculated by reliability analyses. The most important results are shown on figure 3.

It shows frequencies of initiating events and failure probabilities of systems needed to keep the reactor in a safe state. From these, the expected frequencies of the core destruction initiators of group 1, 2 and 5 are determined. Other groups are not shown here, since their contribution is insignificant.

Dominant accident initiators for groups 1 and 2 are general transients, estimated to occur 12 times a year. With an estimated failure probability of 10^{-7} per year of the mechanical scram system, an expected frequency of $1{,}2 \cdot 10^{-6}$ is obtained for the unprotected loss of flow case. This case is used as the basis case of the subsequent accident analysis.

The following classes of accident initiators contribute to the frequency of group 5: loss of normal ac-power, steam generator failure, and the general case of decay heat removal. If the accident is initiated by a loss of normal ac-power or by a steam generator failure, the availability of the decay heat removal system is already impaired by the accident initiator.

The reliability analysis took into account the passive decay heat removal capability. A conditional probability of 10^{-2} has been estimated for a failure of passive decay heat removal. All together, an expected frequency of $3 \cdot 10^{-7}$ per year has been estimated for this core destruction initiator.This value comprises a small contribution from group 6.

The next step of the analysis deals with the course of core destructive accidents.

Core destruction may be accompanied by the release of significant amounts of mechanical energy. The primary coolant system of the SNR-300 is designed to withstand mechanical energy releases of up to 370 MJ. Other design features like the submerged heat exchangers make it possible to cool the molten core inside the reactor tank, so that melt-through of the tank can be prevented.

The accident analysis had to estimate the conditional probability that releases of mechanical energy beyond the design value of 370 MJ occur, and the conditional probability of reactor tank failure due to mechanical or thermal overload at energy releases below 370 MJ.

According to present understanding, the amount of mechanical energy possibly released in such accidents is expected to be far below the design value of 370 MJ. However, for the probabilistic risk assessment it was necessary to arrive at an estimation of probabilities of energy release exceeding certain values.

This part of the analysis had to incorporate expert judgement in a number of places. In order to put such estimates on as broad a basis as possible, an international expert questionning was conducted on phenomena influencing the release of mechanical energy after an unprotected loss of flow.

Incorporating the results of this action, subjective complementary cumulative probability distributions for a release of mechanical energy have been obtained (figure 4). The totality of these distributions reflects the degree of uncertainty exhibited in the experts' answers. On the slide several subjective confidence limits are shown. A reference complementary cumulative distribution was also generated.

These results represent the subjective judgement arrived at in the analysis. By no means should they be interpreted as results of a statistical analysis.

According to the reference curve B, there is a 0,95 conditional probability that the release of mechanical energy in an unprotected LOF is less than 50 MJ. The conditional probability for exceeding 400 MJ, which is about the design value, is three tenth of a percent. The analysis also showed that there is a conditional

probability of about one half that there is no mechanical energy release at all in an unprotected LOF.

Figure 5 shows the results of the plant systems analysis. Five release categories have been defined. They are distinguished by different release portions of the radionuclide inventory, by the release time after accident initiation, by the duration of the release, and by the thermal energy carried with the release. Their expected frequencies of occurence are obtained from the expected frequencies of core destruction and from conditional probabilities of tank failure modes and containment isolation failure.

Category 1 comprises the most severe release after a plug system failure and an overpressurization failure of the outer containment.

The main release occurs a few minutes after accident initiation and is combined with a considerable release of thermal energy. On the slide, only the released portions of noble gases, 100 percent, and actinides, five percent, are shown. For other radionuclides, released fractions of the inventory between five and fifteen percent have been calculated.

Category 2 comprises cases with failure of heat removal from the inner containment, while the outer containment is isolated for up to 22 hours. At that time, a hydrogen explosion occurs in the inner containment, destroying the integrity of the containment sytem.

For category 3 thermal tank failure, failure of containment isolaton and unfiltered exventing of containment atmosphere is assumed.

Categories 4 and 5 contain cases with lower releases, category 5 being quite similar to the design basis accident.

The slide shows that the released fraction of actinides is considerably lower for categories 2 to 5 than for category 1. Similar relations apply to other groups of isotopes, with the exception of noble gases, which are partially retained only for category 5.

Besides accidents caused by internal initiating events, possible effects of external events have been investigated. Flooding, tornadoes, lightning, gas cloud explosions, effects of hazardous materials and missile generation in the turbogenerator building have been analysed qualitatively. The analysis showed that no significant risk contribution is to be expected from such events.

Effects of airplane crashes and earthquakes have been analysed quantitatively. Due to design measures, and low probabilities of these events contributions from air plane crashes to the overall risk are small. Earthquakes, which may threaten the availability of the reactor scram systems, of the decay heat removal systems, and of containment isolation, contribute 50 percent to the expected frequency of the most severe release category 1 and about 40 percent to the expected frequency of category 3.

The reason for this significant contribution is not a particular sensitivity of the SNR-300 to earthquakes, but the fact that the expected frequency of core destruction caused by internal events is as low as the expected frequency of extremely strong earthquakes at the site Kalkar.

Since simultaneous core destruction and failure of containment structures have been assumed for a very high intensity earthquake, this event contributes mainly to release categories 1 and 3.

Using the release categories as input, accident consequences were calculated for the site Kalkar.

Early fatalities due to acute lethal radiation doses occur only above a threshold dose. This threshold is calculated not to be reached after accidents of the SNR-300 within populated areas around the reactor site.

Late fatalities have been determined on the basis of a linear dosis-effect relation without threshold. The maximum number of late fatalities has been estimated at 14000, resulting from release category 1.

The results most important for the comparison of PWR and SNR-300 are summarized on the figure 6.

The main risk contribution of a PWR comes from small leaks and loss of heat sink. Overall, the expected frequency of core melt of $9 \cdot 10^{-5}$/per year had been obtained in the PWR risk analysis.

The SNR-300 and more general a LMFBR is insensitive to those kinds of accidents. Due to the high boiling temperature of the coolant which facilitates low system pressure, and due to the high thermal capacity of sodium, complete evaporization of the coolant is ruled out provided that the reactor is scramed. Coolant loss by leakage is prevented by design features. Decay heat can be removed after a loss of the heat sink by passive means.

The main contribution to the risk of the SNR-300 is from the unprotected loss of flow accident. Overall, an expected frequency of core destruction of $2 \cdot 10^{-6}$/per year has been estimated. The smallness of this figure is mainly due to the highly reliable shutdown system.

For the PWR, the most severe consequences occur if the containment is destroyed by steam-explosion during core melt down. The expected frequency of this accident, which may cause up to 14000 early fatalities, has been estimated at $2 \cdot 10^{-6}$ per year.

The maximum number of late fatalities has been estimated at about 105000 but not for the same accident that causes the maximum number of early fatalities.

For the SNR-300, the most severe consequences occur if the mechanical energy release accompanying core destruction significantly exceeds the design value of 370 MJ. Though this accident does not cause early fatalities, up to 14000 late fatalities may occur.

Though the uncertainty bandwidths obtained in the SNR-300 analysis are much wider than in the PWR analysis, these figures indicate that frequencies of severe accidents, and their consequences should be smaller for the SNR-300.

However, before drawing final conclusions one has to remember that the analysis was performed for a prototype plant under construction. The data base is poorer than for a large commercial LWR. Therefore, subjective probabilities derived from expert opinions play a very important role.

PRA IN R&D ACTIVITIES

Results of PRA can be used as an aid to establish relevant priorities for R&D activities more effectively than has been done so far in the F.R. Germany. As in other studies indications to support this suggestion can be found in the SNR-300 risk analysis.

For example, the SNR-300 Fast Breeder Study showed that there is an uncertainty about the reactivity effect of material motion in case of fuel cladding failure. This is exhibited in the experts answers to one of the questions which, on the average, show that the experts are indetermined as to whether there is a positive, neutral, or negative reactivity effect.

Uncertainties also exist about the potential recriticality out of slow melt down. This may become important for larger reactors, where cooling conditions will be less favourable than for the SNR-300. Besides uncertainties about energetics due to nuclear excursions, it is unclear whether an interaction of large pools with sodium may lead to steam-explosion like phenomena.

The study also demonstrated the great importance of the containment for the retention of radioactive material. This suggests that more accurate transport calculations and a more detailed description of interactions between sodium, atmosphere and concrete should be achieved. Also, a more accurate simulation of the transport of expanding materials througl sodium is important, because the source terms depend on it.

In view of the low expected frequencies of plant internal accidents the treatment of failure probabilities of passive structures may become more important.

CONCLUSIONS

PRA has been accepted as a powerful tool for a variety of technical applications, such as the investigation of complex nuclear systems. Some of its more recent perspectives on the nuclear field are:

- Through the identification of possible weak points in the system design it serves to improve the system availability and to ensure that all parts of the reactor safety concept are well-balanced.
- Through an improved data basis by field experience the reliability of safety systems can be predicted more accurately.
- The assessment of the probability of severe accident scenarios requires substantial use of subjective probability distributions.
- The evaluation of accident precursors may serve to get a better understanding of failure mechanisms and of the influences on the uncertainties of the probability distributions.
- Through quantitative analyses different reactor types can be compared.

REFERENCES

[1] "Reactor Safety Study - An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants", United States Nuclear Regulatory Commission, WASH-1400 (NUREG-75/014), October 1975

[2] "Deutsche Risikostudie Kernkraftwerke", Gesellschaft für Reaktorsicherheit (GRS) mbH, Hrsg.: Bundesministerium für Forschung und Technologie, Verlag TÜV Rheinland, Köln, 1979, ISBN 3-921059-67-4

[3] A. BIRKHOFER, "The Expanding Role of Quantitative Risk Analysis in Germany", International Conference on Current Nuclear Safety Issues, International Atomic Energy Agency, Stockholm, 20 - 24 October 1980.

[4] "Risikoorientierte Analyse zum SNR-300, Bericht der GRS", Band 1 und 2, Gesellschaft für Reaktorsicherheit, GRS-A-700, F.R. Germany, Garching, April 1982.

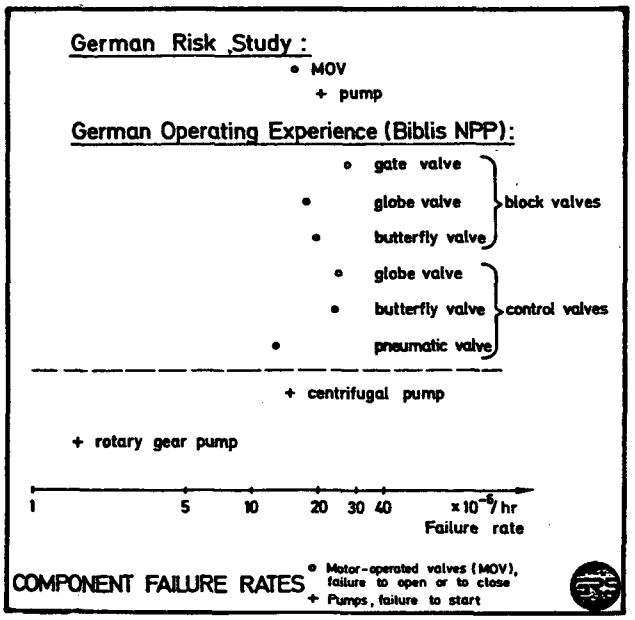


Figure 1

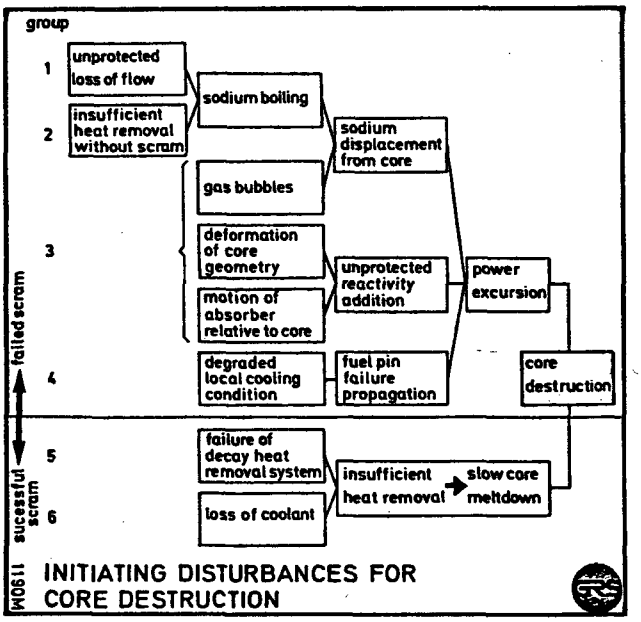


Figure 2

group	accident initiator frequency	failed system function conditional probability		core destruction initiator
1	transient 12/a	reactor scram system (mechanical) 10^{-7}		$1.2 \cdot 10^{-6}$/a
2	transient 12/a	manual shut down 10^{-1}	reactor shut down signal 10^{-7}	$1.2 \cdot 10^{-7}$/a
5	loss of power 0.07/a	decay heat removal system active 10^{-4}	passive 10^{-2}	$7 \cdot 10^{-8}$/a
	steam generator failure 1/a	decay heat removal system active $1.5 \cdot 10^{-2} \cdot 5 \cdot 10^{-4}$	passive 10^{-2}	$8 \cdot 10^{-8}$/a
	general case of decay heat removal 11/a	decay heat removal system active $1.7 \cdot 10^{-3} \cdot 5 \cdot 10^{-4}$	passive 10^{-2}	10^{-7}/a
sum	12/a			$3 \cdot 10^{-7}$/a

EXPECTED FREQUENCIES OF CORE DESTRUCTION INITIATORS

Figure 3

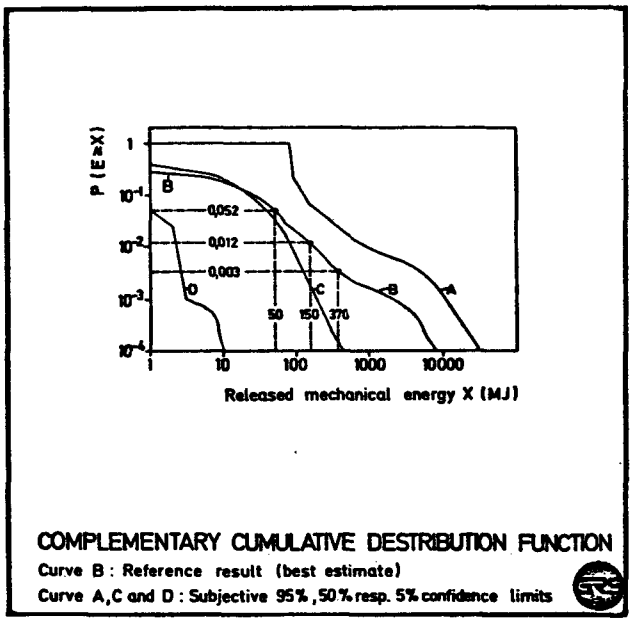


Figure 4

release category nr.	description	time of main release h	released thermal energy 10^6kJ/h	expected frequency of release per year	released portion of reactivity inventory	
					noble gases	actinides
1	core destruction, plug system failure, overpressurization failure of outer containment	0 - 1	530	10^{-8}	1	0.05
2	core destruction, mechanical tank failure, damaged core catcher, loss of power	22 - 33	15	$2 \cdot 10^{-7}$	1	$5.5 \cdot 10^{-4}$
3	core destruction, thermal tank failure, unfiltered exventing	0 - 48	-	$2 \cdot 10^{-8}$	1	$4.1 \cdot 10^{-4}$
4	core destruction, thermal tank failure, loss of power, containment isolated	48 - 100	-	$2 \cdot 10^{-7}$	1	$1.8 \cdot 10^{-5}$
5	core destruction, thermal tank failure, containment systems functioning	240 - 320	-	$3 \cdot 10^{-7}$	$2 \cdot 10^{-2}$	$1.4 \cdot 10^{-11}$

1198M DEFINITION OF RELEASE CATEGORIES AND EXPECTED FREQUENCIES

Figure 5

	PWR	SNR 300
EXPECTED FREQUENCY PER YEAR OF		
CORE DESTRUCTION	$9 \cdot 10^{-5}$	$2 \cdot 10^{-6}$
RELEASE CATEGORY 1 (FAST CONTAINMENT FAILURE)		
BEST ESTIMATE	$2 \cdot 10^{-6}$	$1 \cdot 10^{-8}$
SUBJ. 95 % CONF. LIM.	$7 \cdot 10^{-6}$	$5 \cdot 10^{-7}$
MAXIMUM OF EARLY FATALITIES	14 500	0
LATE FATALITIES	104 000	14 000

COMPARISON PWR - SNR 300

Figure 6

ISSUES AND TRENDS IN CANADIAN REACTOR SAFETY PRACTICE

G.L. Brooks
Vice-President, Design and Development
Atomic Energy of Canada Limited
Engineering Company

ABSTRACT

As in the case of other countries which have played lead roles in the development of commercial power reactor systems, the early evolution of Canadian reactor safety practice was strongly influenced by:

(i) early experience with domestic research and experimental reactors, particularly that gained from mishaps and accidents

(ii) the basic inherent characteristics of the power reactor system being developed

(iii) the perceptions and judgments of key individuals who established the safety practice basis.

In its early stages, the Canadian power reactor program was directed almost exclusively to the domestic market. As a result, a relatively unique set of safety practices could be evolved for the CANDU system. Subsequently and as Canada has moved into the international marketplace and as exchanges between regulatory bodies on an international level have increased, these safety practices have been subject to change. Practical safety-related experience in other countries has also had a significant influence. Perhaps unavoidably, this has led to a proliferation of safety requirements and a measure of loss of focus and consistency in applied safety practice with consequent adverse economic impact.

The paper summarizes this history and outlines initiatives being taken in Canada to deal with current safety issues and to rationalize Canadian safety practice.

1. HISTORICAL BACKGROUND

As in the case of other countries which have played leading roles in the development of commercial nuclear power systems, the early evolution of Canadian reactor safety practice was strongly influenced by a number of contemporary factors. The major of these were as follows:

(i) In 1952, and just prior to the start of feasibility studies which led to the CANDU system, a partial core melt accident occurred with the 20 MW(t) NRX research reactor at AECL's Chalk River Laboratory. The primary cause of the accident was a partial failure of the reactor shutdown system which permitted a relatively severe overpower transient to occur during a reactor physics experiment. As a result of this accident, reactor shutdown systems received

particular attention and prominence in the development of designs and safety criteria for CANDU reactors.

(ii) In optimizing the design of early CANDU reactors for a natural uranium fuel cycle, particular recognition was given to the question of the small but positive coolant void coefficient of reactivity. This characteristic necessitated a highly reliable means of achieving prompt reactor shutdown following a loss-of-coolant accident. Together with (i) above, this factor was to play a major role in shaping CANDU shutdown system criteria.

(iii) Since the natural uranium CANDU system does not possess an inherent negative power coefficient of reactivity, a highly reliable, closed-loop, reactor power regulation system is required. This characteristic, coupled with factors (i) and (ii) above, which relate to shutdown system criteria, led to an early requirement for total separation between the reactor power regulation and shutdown functions. This remains a hallmark of the CANDU system to this day.

(iv) At the outset of most novel human endeavours, the perceptions and views of a few key individuals establish a basic direction which fundamentally shapes subsequent developments. In the case of the CANDU system and the associated Canadian safety approach, two individuals played the key roles in this regard, viz., Dr. W.B. Lewis, widely recognised as the father of CANDU, and Dr. G.C. Laurence, who led the development of the Canadian safety approach during its formative years.

Having identified certain key factors which were to have a major influence on the early development of Canadian reactor safety practice, I will now briefly outline this development.

Following a series of basic feasibility studies, detailed design of the first CANDU plant, a 20 MW(e) demonstration unit (NPD), commenced in the mid-1950's. In order to guide the design, it was necessary that an overall safety target be established since no detailed explicit Canadian safety criteria existed at the time. The adopted target was that the plant should be at least 10 times safer than the norm of "good" established industries in Canada. Translated into more practical working terms, this target was restated as a probability of serious injury of $< 10^{-5}$ per year and of death of $< 10^{-6}$ per year. In parallel with design of the plant, an approximate probabilistic risk assessment was carried out to demonstrate that the plant, as designed, would satisfy this target.

This same basic approach was carried forward for the safety assessment of the next CANDU plant, a 200 MW(e) semi-commercial scale unit (Douglas Point).

With the commencement of preliminary work on the first fully commercial CANDU station in the early 1960's (the 4 x 500 MWe Pickering-A station), the safety assessment and criteria basis utilized for Douglas Point and NPD was reviewed in detail by the Canadian regulatory body, the AECB, under the leadership of its president, Dr. G.C. Laurence. This review took into account experience gained with the earlier prototype units, the much larger size of the proposed Pickering plant, and its proposed site which was close to metropolitan Toronto.

Two perceived difficulties with earlier Canadian practice were identified, viz., the lack of fully comprehensive component reliability data necessary to give high confidence in a solely probabilistic approach and the problems of cross-linked and common-mode failures which by their nature are difficult to handle in probabilistic assessments. In addition, the AECB was in close contact with the regulatory scene in other countries where comprehensive deterministic safety criteria were being established. I might note that in most of these countries little attention had, at the time, been given to probabilistic assessment methods.

As a result of these considerations, the Canadian approach turned towards a rather more deterministic methodology as embodied in what become known as the "single/dual failure" criterion. At this point I should note that this change was really one of practical expediency. It was not based on any preconception that deterministic approaches are inherently superior. The single/dual failure methodology was first applied in the case of Pickering-A and has become a cornerstone of Canadian safety assessment practice since that time. In applying this methodology, the plant is notionally divided into two groups of systems. The first, termed process systems, includes all those systems required for the production operation of the plant. The second, termed special safety systems, includes those systems required solely to mitigate the consequences of failures in the process systems. These are the reactor shutdown system(s), the emergency core cooling system, and the containment system.

The methodology embodies two basic steps. Firstly, a set of prescribed failures are considered in the various process systems with the special safety systems assumed operative. Each failure must be shown to result in an exposure to the individual most at risk of not more than 0.5 rem whole body*. Secondly, each such process failure must then be reanalyzed assuming, in turn, the complete unavailability of each of the special safety systems. Each such "dual" failure must be shown to result in an exposure to the individual most at risk of not more than 25 rem whole body*.

Returning to historical highlights, a further basic development occurred, commencing with the Bruce-A station (4 x 750 MWe). Prior to Bruce-A, CANDU reactors were provided with single fast shutdown systems. Within the single/dual failure methodology, it was therefore necessary to consider accidents involving positive reactivity transients coupled with failure of the reactor shutdown system to function (ATWS). In this scenario, reactor power would increase until terminated by core geometry disruption sufficient to render the reactor subcritical. Given the then current state of technology, such analysis was necessarily somewhat speculative. To avoid this difficulty, a second, totally independent, and functionally and geometrically diverse, shutdown system was added. With this addition, the action of at least one shutdown system could be credited in all analyzed accident scenarios.

To complete the historical highlights, a return has now been made to the earlier probabilistic approach in considering more complex possible failures in service systems (electrical power, service cooling water, compressed air supplies, etc), and in considering the consequences of earthquakes and longer-term failures of the special safety systems where they are required to function for extended periods following an accident. Such analyses augment the more "classical" single/dual failure analyses in that a rather wider spectrum of possible accident scenarios is considered.

In summary, the foregoing historical outline shows Canadian reactor safety assessment methodology moving from an initial probabilistic basis towards a substantially deterministic basis followed by augmentation through the adoption of probabilistic assessment methods for a class of accident scenarios where the method is particularly appropriate.

---

* Additional criteria are specified for thyroid dose and total population exposure.

2. CURRENT ISSUES

Time precludes my discussing all of the detailed issues currently under consideration in Canada at this time. I will, however, highlight a few which are of particular interest and significance from my perspective as a reactor designer.

2.1 Conservatism

Since the outset of safety analysis, arguments as to the nature and treatment of "adequate" conservatisms have arisen regularly between designers and regulators. We are well aware that this is not a uniquely Canadian problem. Equally, we do not have a uniquely Canadian solution. I would like, however, to offer an observation which, while hardly novel, bears repeating in my view. The stacking of conservatism on top of conservatism on top of conservatism takes us, inevitably, further and further away from reality. I have a very real concern that this widespread regulatory-decreed practice may well be counter-productive in that unsuspected adverse consequences can be masked by such a distortion of reality. The same basic argument applies to the selection of failure assumptions in accident analysis. What are commonly taken to be "worst case scenarios" are not necessarily "worst case" even though they may be more spectacular in terms of perception. A return to a collective best judgment of reality is, I believe, long overdue. Uncertainties must, of course, be considered but this should be done in such a way that realism is not lost.

2.2 Deterministic vs Probabilistic Criteria

As discussed in Section 1, the Canadian approach to reactor safety assessment and criteria has strong probabilistic roots. However, over the years, a number of somewhat arbitrary deterministic criteria have evolved, largely through what I will term "common law" licensing practice. Today we have what some might consider the best of both worlds while others might conclude the opposite. Be that as it may, there are inevitable (at this stage of development) inconsistencies between the two approaches which give rise to detail issues between designers and regulators. This question will be further discussed in the next section dealing with trends for the future.

2.3 ECCS Effectiveness

"Pure" application of the single/dual failure criterion would require consideration of a LOCA combined with unavailability of containment (one of the special safety systems). Given this "dual accident" secenario, it will be seen that ECCS must be highly effective in that very few fuel sheath failures could be tolerated if the dual failure exposure limit is to be satisfied (this limit translates to a total allowed I-131 release of about 10^3 Ci). Recent CANDU reactors are provided with a high capability, high pressure ECCS to minimize fuel overheating transients following a LOCA and, hence, to minimize the risk of fuel sheath failures. When analyzed using the latest transient thermo-hydraulic codes, the performance of the ECCS is predicted to be satisfactory over a wide range of possible LOCA scenarios (break size and location). Nevertheless, these analysis codes inevitably contain modelling simplifications and empirical correction factors which leave an element of question as to the veracity of their predictions. This is particularly true for a small range of break size and location where significant periods of low coolant flow are predicted, giving rise to periods of two-phase flow stratification.

The AECB has referred the basic question of the required effectiveness of the ECCS to a new independent advisory group, The Advisory Committee on Nuclear Safety, (ACNS), for recommendations as to appropriate further criteria. The ACNS subsequently fowarded its recommendations to the AECB Board. The Board accepted these recommendations in July 1982 and referred them to AECB Staff for implementation in the licensing process.

2.4 Fuel Channel Power Limitation

In CANDU reactors, the basic consideration in determining maximum allowable power from a fuel channel is protection of the integrity of the fuel channel pressure boundary, i.e., the pressure tube. Protection of fuel sheath integrity, per se, is not an important safety consideration since defective fuel can be readily detected, located, and replaced on-power in CANDU reactors. It is however important that fuel overrating be limited such that consequential pressure tube damage is precluded. Continuing research and evaluation is being directed to the determination of the allowable degree of fuel overrating in order that adequately (but not overly) conservative limits on fuel channel power can be established.

2.5 How Safe is Safe Enough?

I have deliberately left this issue to the last although, in my view as a designer, it is by far the most important. In Section 1, I made reference to the early Canadian target of nuclear plants being 10 times safer than the norm of "good" industries. A paper by Ernest Siddall, to be presented later to this conference (1), suggests that an optimum overall benefit to public safety might result were a less stringent standard adopted. In fact, however, the continuing escalation in regulatory requirements has taken us in just the opposite direction. As a result, capital costs and construction durations have increased to a point where the net benefit to society from nuclear power has been seriously undermined.

This is not a uniquely Canadian problem; it is being faced in several countries. Why has it arisen? The answer is, I believe, far from simple. Certainly, from an overall objective perspective, the record of nuclear power plants to date does not support a continuing escalation in requirements. However, to blame the regulatory agencies for this state of affairs is, I believe, unwarranted. Indeed, I would like to acknowledge that, given the imperatives and constraints under which it currently operates, the AECB in Canada has shown commendable restraint in limiting the rate of escalation of licensing requirements. I believe that the real source of the problem lies in the basic institutional structures and perspectives of priorities, roles and responsibilities which exist in Canada and, I believe, in other countries which are experiencing this problem. In free societies, our institutional structures generally perform best when there is an appropriate balance between the regulators and the regulated. A significant imbalance will inevitably lead to distortions such as we are currently encountering. Realistically, though, we cannot expect a rapid adjustment in the balance to occur. The nuclear industry has a formidable task ahead in convincing those who influence public and political opinion that nuclear power is both desirable and necessary to the health of our society. Until this task is accomplished, we can expect little relief from this escalation scenario.

3. TRENDS

In the current Canadian scene, clear trends are not yet apparent in our collective efforts to resolve certain of the issues discussed in the previous section. In these cases the task is ongoing.

Significant progress is, I am pleased to report, being made in resolving the issue of deterministic vs probabilistic criteria (Section 2.2). In Canada, and as discussed in a paper by Paskievici et al, being presented at this conference (2), the ACNS is taking a lead role in rationalizing current safety criteria. A clear move towards more emphasis on a probabilistic approach is evident in the Committee's work to date. As a designer, I welcome this trend. While recognizing that there remain definite limitations in current practical probabilistic assessment methods and in the underlying component reliability data base, our experience with this method, as discussed earlier in this paper, is very favourable. It has already lead to significant design improvements in some areas where "conventional" practice has been found lacking. Having said this, we do not see a total abandonment of deterministic criteria. We believe that there will be a continuing role for certain deterministic criteria to cover areas where the probabilistic assessment method and/or its underlying data base are not fully adequate. Finally, we believe that probabilistic methods, while a powerful assessment tool, will not replace the ultimate need for applying judgment in making licensing decisions. That need will remain.

With regard to the question of ECCS effectiveness and as noted in Section 2.3, AECB acceptance and publication of the ACNS recommendations should resolve this issue.

While not directly associated with the issues discussed in the preceeding section, two further trends are, I believe, of interest. The first relates to shutdown systems. Starting with the Darlington-A reactors of Ontario Hydro, we expect to see a major trend towards fully computerized trip logic in CANDU shutdown systems. In fact, a limited application of computerized logic is incorporated in the shutdown systems of the 600 MW(e) CANDU plants which are now coming into operation. This approach offers two advantages. Firstly, the frequency of spurious trips can be reduced and, secondly, plant safety will be enhanced through a more comprehensive capability to automatically diagnose plant transients.

The second trend, which will be on a longer time base, is towards providing plant operations with diagnostic tools to facilitate their handling of plant upsets and accidents. Termed AIDSS (Abnormal Incidents Decision Support Systems), such a system offers great potential in assisting operators to assimilate and diagnose large volumes of parameter information. The longer time base will be required since it is essential that such a system not inadvertently mislead the operators through incorrect diagnosis.

CONCLUSIONS

As in other countries, the safety record of Canadian power reactors has been excellent to date, demonstrating the clear adequancy of our overall safety practice. The question which remains is to what degree has our safety practice exceeded logical requirements, i.e. how safe is safe enough? In my opinion, and as I have stated earlier, the answer to this question is that the excedence is substantial in many areas. As probabilistic methods of safety assessment become more comprehensive and more widely accepted, it should become easy to identify the areas of these excesses as well as areas where further improvements are appropriate. The real challenge to all, including regulatory bodies, will then come. Will we collectively be able to progressively eliminate the excesses that are identified? I

believe our success or failure will hinge on our ability to influence key leaders of public and political opinion. Since success in this would lead to a significant improvement in the economies of nuclear power, we can expect a strong negative reaction from anti-nuclear forces. It will then be the task of all those knowledgable concerning nuclear power to effectively neutralize this emotional reaction. I am optimistic that we will, in the long term, succeed.

REFERENCES

1. E. SIDDALL, "Safety Policy in the Production of Electricity", presented to the International Meeting on Thermal Nuclear Reactor Safety, Chicago, August 29 - September 2, 1982.

2. V. PASKIEVICI, A. PEARSON, J.T. ROGERS, "Development of Risk Based Safety Related Criteria for Licensing CANDU Nuclear Power Reactors", presented to the International Meeting on Thermal Nuclear Reactor Safety, Chicago, August 29 - September 2, 1982.

OPERATING EXPERIENCE OF LIGHT WATER REACTORS IN JAPAN

S. Hamaguchi
Federation of Electric Power Companies
Tokyo, Japan

ABSTRACT

At present, 24 commercial nuclear power units in the total capacity of 17 GWe are in service and 10 units with the total capacity of 9.6 GWe are under construction in Japan. In the past, as for the problems mainly affecting nuclear power plant availability, PWR plants experienced the tube degradation of steam generator and the stress corrosion cracking of piping system affected BWR plants. The study for cause of the above mentioned problems and corrective actions taken will be explained, then, the measures for improvement of availability are also to be introduced.

PREFACE

In Japan where the supply of oil is so heavily dependent upon those oil-producing countries, it is an urgent task of Japan to develop nuclear power as an alternative energy source in order to curtail such dependency as well as to promote energy conservation program; therefore, we are standing together as a nation for the promotion of such activities. The development of nuclear power will demand us to win the people's understanding and to obtain a national concensus on this issue, which in turn implies how it is important for us to demonstrate the safety and reliability of the existing nuclear power generation facilities by dint of the betterment of their capacity factors.

First, this paper presents the current status of nuclear power generation plants in Japan, and then in the light of the operating experience to this data - in particular such major causes adversely affecting plant capacity factor as steam generator tube degradation on PWR and pipe stress corrosion cracking on BWR -, describes remedial actions taken against such major causes. Finally, this paper accounts for measures for improving the plant capacity factor in the years ahead.

STATUS OF NUCLEAR POWER GENERATION PLANTS IN JAPAN

In Japan, 24 units with the total capacity of 17 GWe are in service as of June, 1982, which consists of 11 PWR units, 12 BWR units and one GCR unit, and occupies about 12% of the total capacity of commercial power generation facilities in Japan (See TABLE I). In addition, 10 units with the total capacity of 9.6 GWe, namely, 5 units each of PWR and BWR, are under construction (See TABLE I), and the construction program of 5 units is under review.

In a year period from April 1981 thru March 1982, the operating nuclear power

TABLE I

Nuclear Power Plants in Japan

Status	Owner/Operation	Name of Plant		Type	Capacity (MWe)	Commercial Operation
In Operation	JAPC[a]	Tokai		GCR	166	7/25/66
	do.	Tokai Daini		BWR	1,100	11/28/78
	do.	Tsuruga	#1	BWR	357	3/14/70
	Tokyo Elec.	Fukushima Daiichi	#1	BWR	460	3/26/71
	do.	do.	#2	BWR	784	7/18//4
	do.	do.	#3	BWR	784	3/27/76
	do.	do.	#4	BWR	784	10/12/78
	do.	do.	#5	BWR	784	4/18/78
	do.	do.	#6	BWR	1,100	10/24/79
	do.	Fukushima Daini	#1	BWR	1,100	4/20/82
	Chubu Elec.	Hamaoka	#1	BWR	540	3/17/76
	do.	do.	#2	BWR	840	11/29/78
	Kansai Elec.	Mihama	#1	PWR	340	11/28/70
	do.	do.	#2	PWR	500	7/25/72
	do.	do.	#3	PWR	826	12/ 1/76
	do.	Takahama	#1	PWR	826	11/14/74
	do.	do.	#2	PWR	826	11/14/75
	do.	Ohi	#1	PWR	1,175	3/27/79
	do.	do.	#2	PWR	1,175	12/ 5/79
	Chugoku Elec.	Shimane	#1	BWR	460	3/29/74
	Shikoku Elec.	Ikata	#1	PWR	566	9/30/77
	do.	do.	#2	PWR	566	3/19/82
	Kyushu Elec.	Genkai	#1	PWR	599	10/15/75
	do.	do.	#2	PWR	559	3/30/81
		Subtotal (24 Units)			17,177	
Under Construction	JAPC	Tsuruga	#2	PWR	1,160	6/87
	Tohoku Elec.	Onagawa		BWR	524	6/84
	Tokyo Elec.	Fukushima Daini	#2	BWR	1,100	1/84
	do.	do.	#3	BWR	1,100	7/85
	do.	do.	#4	BWR	1,100	2/86
	do.	Kashiwazaki-Kariwa	#1	BWR	1,100	10/85
	Kansai Elec.	Takahama	#3	PWR	870	2/85
	do.	do.	#4	PWR	870	8/85
	Kyushu Elec.	Sendai	#1	PWR	890	7/84
	do.	do.	#2	PWR	890	3/86
		Subtotal (10 Units)			9,604	

[a] The Japan Atomic Power Co.

plants produced nearly 85 billion KWHs, which amounts to approximately 16% of about 525 billion KWHs generated as a whole.

Speaking of nuclear power plant availability, such factors of both PWR and BWR units were comparatively high in the early years. However, on PWR units mainly because of the implementation of remedial actions for steam generator tube degradation experienced in a period of 19/2 thru 1978 plus the forced outage resultant from the impact of TMI accident in 1979 and the inspection and corrective actions associated with the stress corrosion cracking on support pins of control rod cluster guide tubes, capacity factor went down to the neighborhood of 40-50%. On the other hand, BWR capacity factor was reduced to nearly 30% because of the implementation of remedial actions against pipe stress corrosion cracks and those against thermal fatigue cracks in such components as feedwater sparger nozzle which were experienced in a period of 1975-197/. Nevertheless, since 1980 there has been an advancing tendency in an average capacity factor of PWR and BWR units to exceed 60%.(See Fig. 1)

STEAM GENERATOR TUBE DEGRADATION AND ITS COUNTERMEASURES

It can be seen from Fig. 2a. showing the grand total of units outage hours by equipment in a period from 1970 thru 1980 at 7 PWR units of Kansai Electric Power Company that major factor attributable to a poor capacity factor was steam generator tube. Consequently, the following countermeasures were taken:

1. Tube wall thinning from OD surface:
   It has been designed to arrest the thinning of tube wall by dint of changing the secondary water chemistry from phosphates treatment to all volatile treatment (AVT) together with the removal of residual phosphates by means of hot water flushing and flushing out of secondary water under cyclic load fluctuation.

2. Intergranular stress corrosion cracking from OD surface:
   The local concentration of caustic soda produced from a trace amount of residual sodium phosphates left inside the respective steam generators initially treated with sodium phosphates resulted in intergranular stress corrosion cracking in the region of tube support plate or tube sheet crevice. In order to cope with this problem, either hot water flushing, or tube sheet crevice cleaning jointly developed by us has been applied to remove caustic-soda, and the degradation of tubes in the region of tube sheet crevice has been held back by means of the re-rolling of tubes to eliminate crevices in tube sheet as well as of the insertion of sleeves.

3. Intergranular stress corrosion cracking from ID surface:
   Stress corrosion cracking was found in the bend of small radius bend tubes processed under a certain bending technique, due to high residual stress. Accordingly, all the tubes in Row 1 or Row 1&2 of steam generators equipped with such small radius bend tubes, have been preventively plugged.

4. Others:
   Explosive tube plugs which had been installed as a countermeasure for many wall-thinned tubes were recently found leaking. Due to stress corrosion cracking developed from the primary side. It was learnt that oxygen contained inside the tube was dissolved into the coolant seeped into the tube through cracks to produce the oxygen-rich liquid, with resultant damage to tube integrity. Therefore, it is scheduled to replace those explosive plugs with the plugs of other type.

In addition to the foregoing remedial actions, the utilities in Japan have been paying careful attention to the secondary water chemistry, with meticulous care to specifically control the ingresses of oxygen by the installation of deaerator in FW system and condenser cooling sea water, which in turn has resulted in no occurance of tube denting and pitting.

Moreover, in the light of all the troubles experienced with steam generators at those domestic and oversea plants, the utilities and venders in this country have been working together to improve the integrity of new steam generators in its materials, structures and production processes.

STRESS CORROSION CRACKING OF BWR PIPING AND ITS COUNTERMEASURES

It can be seen from the total hours of forced outages by equipment on 6 units of Tokyo Electric Power Company in a period from 1971 thru 1981 that the stress corrosion cracking of piping was the primary factor adversely affecting the capacity factor (See Fig. 2b).

Up to the present, the affected regions of stress corrosion cracking were primary loop recirculation bypass piping, core spray system piping, residual heat removal system piping, reactor water clean-up system piping, reactor core isolation cooling system piping, primary loop recirculation system riser piping, and various instrumentation lines. Accordingly, we did conducted the study of stress corrosion cracking in the light of material, erection method of piping system, and environments, based upon the findings of which we have taken the following countermeasures:

1. Removal of such piping system as bypass piping of primary loop recirculation system.

2. Replacement of stainless steel with carbon steel for the pipe lines of core spray system, residual heat removal system, reactor water clean-up system, and reactor core isolation cooling system piping which have no possibility of bringing corrosion products over to core under normal operating conditions.

3. Replacement of stainless steel with 304 stainless steel of low carbon content for primary loop recirculation riser pipe, plus the application of solution heat treatment, corrosion resistance clading, and heat sink welding to replacement pipes.

4. Replacement of stainless steel instrumentation lines with 316 stainless of low carbon content.

5. Application of induction heating stress improvement technique to the welding of large main pipe of primary loop recirculation and headers.

6. For new plants, the adoption of 316 stainless steel pipe for primary loop recirculation system, and the reduction of weld lines by the adoption of large prefabricated pipe runs.

7. Betterment of system environment deaerating operation during the course of start-up or shutdown operation.

All the field works associated with the implementation of the foregoing countermeasures were accomplished by automatic equipment and tools specifically developed in the light of the radiation exposure reduction of worker as well as quality control.

MEASURES FOR THE BETTERMENT OF PLANT CAPACITY FACTOR

The following 3 measures have been taken to improve the plant capacity factor:

(a) Curtailment in the time span of annual inspection outage
(b) Extension of unit on-line hours between the annual inspection outages (which will be coordinated with each refueling schedule)

(c) Reduction in forced outage hours

1. Curtailment in the time span of annual inspection outage

(1) Re-examination of annual inspection work system in order to:
Adopt the around-the-clock work system for activities in the critical paths of annual inspection work schedule, and maintain the required number of well qualified workers.

(2) Fosterage of neutral inspection organization in order to:
Facilitate the orderly progress of ever-increasing inspection activities.

(3) Scheduling of annual inspection to:
Perform it simultaneously with refueling operation.

(4) Scope of annual inspection and inspection frequency of each equipment to be properly determined:
In the light of the records of operation and maintenance.

(5) Standardization of annual inspection manuals

(6) Filing with the authority concerned for any application of repair program in the most efficient and expeditious fashion.
Expeditions handling of such application for repairing any defect found in the course of annual inspection.

(7) Furtherance of standardization
.Betterment of maintenancebility.
.Improvement of plant facilities as well as equipment and tools in order to curtail the annual inspection schedule.
.Measures designed for reducing radiation exposure.

2. Extension of unit on-line hours between the annual inspection outages
.Development of an extended cycle core.

3. Reduction in forced outage hours

(1) Improvement of equipment and facilities in the light of the operation and maintenance records as well as the history of defects.

(2) Collection of data concerning abnormal occurances, troubles, and defects as well as the development of an utilization system of such data.
It is intended in this connection to enhance the exchange of information for those of foreign utilities through such organizations as EPRI.

(3) The programmed implementation of protective maintenance work during the course of annual inspection schedule.

CONCLUSIONS

In Japan, we have been endeavoring to develop nuclear power energy in the light of releaving us from heavy dependence on oil; however, the circumstances do not allow us to facilitate it.

In order for us to cope with this unfavourable situation, we find it an effective mean to cultivate the sense of nuclear power security on the part of general public by dint of reducing a number of forced outages toward the furtherance of nuclear power plant reliability and availability.

In this connection, we strongly feel it important, as stated in the foregoing chapter of "Measures for the Betterment of Plant Capacity Factor", to lay stress on

the positive action of preventive maintenance based upon the history of troubles by means of exchanging information thereon at international conferences such as the one at this time as well as of keep maintaining information exchange channels established among the utilities concerned.

RECENT NUCLEAR POWER SAFETY INITIATIVES AT THE INTERNATIONAL ATOMIC ENERGY AGENCY

M. Rosen

International Atomic Energy Agency
Vienna, Austria

ABSTRACT

The role of the International Atomic Energy Agency in the field of nuclear power safety is growing. New emphasis is being placed on the major effort to establish and foster the use of a comprehensive set of internationally agreed safety standards for nuclear power plants. New initiatives are in progress to intensify international co-operative safety efforts through the exchange of information on safety related operating occurrences, and through a more open sharing of safety research results. Emergency accident assistance lends itself to international co-operation and in addition to several new publications an important initiative is underway to encourage a programme of mutual emergency assistance between countries. Meetings to discuss current safety topics are being held on timely subjects such as accident fission product release and quantifying safety goals. To report on nuclear power plant safety world-wide, the Agency is planning to issue a regular annual publication.

INTRODUCTION

Through its capacity to co-ordinate world-wide nuclear safety efforts, the International Atomic Energy Agency (IAEA) makes available to each of its Member States knowledge gained from the experience of the others. The sharing of information and human resources can serve not only to further increase the level of safety of nuclear power plants, but also to help in assuring the public that these plants can provide a safe and reliable means of meeting the world's energy needs.

The Agency nuclear safety activities have grown considerably in recent years and its Division of Nuclear Safety now has a professional level staff of about 30 persons drawn from 16 countries. In addition 7 full-time experts have been seconded cost-free to the Agency, and about 7 man-years of services are provided annually by cost-free technical experts who participate in the many working groups and committee meetings. As many as 30 technical committee meetings, 4 or 5 conferences, symposia and seminars, and 15 safety advisory missions are held in a typical year, and 10 to 15 documents are published.

In the nuclear safety programme, recent initiatives include the new emphasis being placed on efforts to establish and foster the use of internationally agreed upon safety standards for nuclear power plants, for radiation protection and for the transport of radioactive materials. Efforts are in progress to intensify international co-operative safety efforts through the exchange of information on safety related operating occurrences, and through a more open sharing of safety research results. Emergency accident assistance lends itself to international co-operation and in addition to new publications which discuss detailed planning requirements

and a handbook providing examples of exercises and scenarios, an important initiative is underway to encourage a programme of mutual emergency assistance between countries. Meetings to discuss current safety issues are held on timely subjects such as evaluating fission product release following severe accidents and quantifying safety goals.

In addition to activities aimed at the safe operation of nuclear facilities, a limited risk assessment programme is in progress to assess and compare risks associated with various energy systems and to develop methods to more precisely quantify risk.

To regularly report on nuclear power plant safety world-wide and to highlight what is being done to improve it, the Agency is planning to issue a Nuclear Safety Review. This report will become a regular annual publication designed to provide member countries, news media and the interested public with an overview of major trends and developments in the field.

SAFETY STANDARDS AND REGULATIONS

The IAEA continues to play an important role in setting safety standards. A recent feature has been the strong emphasis on encouraging and assisting Member States to implement the guidance contained in the three major areas of this activity:

- The Nuclear Safety Standards Programme (NUSS) for power reactors
- The Basic Safety Standards for Radiation Protection
- The Regulations for the Safe Transport of Radioactive Materials.

The Nuclear Safety Standards Programme

In 1974 an ambitious programme, NUSS (the letters being an acronym for Nuclear Safety Standards), was initiated to establish internationally agreed safety standards for nuclear power plants in the five subject areas of governmental organization, siting, design, operation and quality assurance. Preparation of the basic NUSS documents is now nearing completion: all five Codes of Practice have been published in the Agency's four working languages (English, French, Russian and Spanish) and by year end 1981, 37 of 57 planned companion safety guides were completed (26 of them already published in English and many in the other working languages). When the development phase comes to an end during the next two years, some 250 one-week technical committee meetings, each attended by an average of 10 internationally drawn experts, will have been required to produce the 2200-page set of documents that is the final goal of the programme.

Although at present there are no plans for formalizing the acceptance of the NUSS standards by means of an international convention, a considerable effort is now underway to encourage their use. Training courses and seminars are being organized to promote them as the basis for preparing relevant national regulations, for the domestic development of nuclear industries and for use in international commerce. The Agency is arranging visits to Member States of special missions consisting of experts directly involved in the preparation of these documents. Such missions, during which discussions can be held with regulatory, utility and other appropriate personnel, should be particularly useful to countries in the early stages of nuclear power programmes. Fourteen countries have already requested missions and 5 visits were completed by year and 1981.

A principal goal of these codes and guides is to make available to developing countries starting a nuclear power programme a cohesive set of nuclear safety standards. Regulations developed elsewhere may not always be suitable and the development of new comprehensive technical regulations is an undertaking that a

developing country cannot perform itself. Many developing countries are now involved with the nuclear power option. At this time there are six with nuclear power plants under construction, seven with projects in an advanced planning phase or already in the plant procurement stage, and about ten considering nuclear power programmes.

These countries may utilize the NUSS documents for guidance in:

(1) organizing a Regulatory Body for nuclear safety,
(2) surveying for possible suitable sites,
(3) qualifying a specific site to demonstrate its acceptability,
(4) establishing the main plant design criteria and those of the principal safety-related systems,
(5) issuing guidance for safe operation, operator training, emergency preparedness and quality assurance.

The NUSS documents will be used by the Agency as a basis for giving assistance to Member States in safety-related matters. They will help recruited technical experts to assess and to make recommendations and ensure objective and consistent advice. These documents may also be useful when an internationally agreed approach to safety is indicated such as when nuclear power plants are located near national borders. In such cases NUSS standards may be useful as a reference for an agreed upon level of safety and as a basis for organizing an emergency plan for the countries involved.

The Basic Safety Standards for Radiation Protection

An important step to reduce the risks resulting from the use of ionizing radiation has been taken with the international agreement on revised Basic Safety Standards for Radiation Protection which will be published later this year. The revision was a joint project undertaken by the Agency with the World Health Organization (WHO), the International Labour Organization (ILO) and the Nuclear Energy Agency (OECD/NEA).

These new standards represent the culmination of efforts underway since 1977 to provide a world-wide basis for harmonized and up-to-date radiation protection standards. They reflect a considerable advancement over the previous Basic Safety Standards and they will in many circumstances substantially increase radiation protection for workers, and for the general public. It is the first instance where a consistent safety system has been developed for hazards where no threshold to risk can be demonstrated, and where the ultimate goal of absolute protection with zero risk can only be approached. They can serve as an example to other industrial activities which involve hazards to man.

The standards are based on the latest recommendations of the International Commission on Radiological Protection (ICRP), contained in its publication No. 26. One of the main features of the ICRP publication is the formulation of a dose-limitation system which requires as its first element that no source or practice involving exposure to radiation or radioactivity be authorized unless the resulting benefits are sufficient to justify the detriments resulting from the exposure. The second element of the system, optimization of protection, requires that justifiable sources and practices ensure that radiation protection is optimized so that economic and social factors are taken into account. The third element, establishes dose-limits beyond which no individual should be exposed.

In the practical application of the standards, some questions still remain.. One area where further clarification is needed is in the application of the principle that all radioactive exposures be "as low as reasonably achievable (ALARA)". A clearer understanding is needed of the meaning of procedures such as reduction of collective doses, reduction of individual doses, optimization (where this is a strict numerical technique), and how to integrate this input into making decisions. Guidance is also needed in evaluating the necessary trade-off between various

competing factors such as that between worker and public doses, between doses to the close-in population and the world population, between doses to critical groups and others, and between doses at present and in the future.

A topical seminar was convened in 1979 in Vienna on The Practical Implications of the ICRP Recommendations and the revised Basic Safety Standards for Radiation Protection. The aim, in addition to exchange of information, was to identify and deal with areas where practical difficulties might arise in application. This seminar was followed in 1981 by a symposium held in Madrid on Application of the Dose Limitation System in Nuclear Fuel Cycle Facilities and Other Radiation Practices whose aim was to gather data on current experience.

The Agency is publishing extensive recommendations to provide guidance in the application of the revised Basic Safety Standards for Radiation Protection and will continue to provide a forum for continued exploration and clarification.

The Regulations for the Safe Transport of Radioactive Materials

Transportation of fuel and waste is a critical aspect of reactor operation. Most radioactive materials are transported in routine commerce by regular means. Safety Standards based on the Agency's Regulations for Safe Transport of Radioactive Materials are applicable to such transport almost everywhere in the world. The standards require protective packaging and simple transport controls give assurance that radiation will add very little to the hazards normally associated with transport.

Although there is no international convention, standards based on the Agency's regulations are applied by more than 50 countries and all relevant international transport organizations. While all international and most domestic regulations are based on the 1973 Revised Edition, a few Member States, among them the United States, follow earlier versions. A comprehensive review of the regulations is underway for a new revision to be published in 1984. When published, Member States will be urged to adopt the revision within 5 years.

In 1977 a programme to offer assistance in implementing the standards was undertaken. A standing Advisory Group for the Safe Transport of Radioactive Materials was established in 1978. This November a group representing 16 countries and several international organizations will meet to identify and discuss specific operational problems encountered in applying the transport standards, and to exchange views on programmes to assure implementation including package design review, inspection, enforcement and quality assurance.

An updated version of Advisory Material on Application of the Transport Regulations first published in 1973, was issued early this year and work has started on a revision to be issued with the 1984 Regulations. Preparation of explanatory material on specific regulatory requirements is also planned for publication in the next two years. In May 1982, the first training course, attended by 21 trainees from 16 countries, was held on the background and implementation of the Regulations.

A system of probabilistic analysis for assessing the radiation and chemical risks from transporting radioactive materials was developed for the Agency by Sweden. Although necessarily simplified and somewhat limited because available data are inaccurate and incomplete, the results may identify major contributors to risk and encourage the development of better data. In 1979, a coordinated research programme on transport safety was established to encourage needed research and provide for exchange of results. Ten countries are now part of that programme and an initial report was issued in 1981.

Data on the hundreds of transport package designs in use in the world are being compiled in a computer programme established in 1980. A similar programme already in operation by the US Department of Transportation is linked with the Agency's data

bank. Reports are issued annually and in the next few months a computer link will facilitate ready access to data on all designs.

EMERGENCY PREPAREDNESS ACTIVITIES

Since early 1981, the IAEA has pursued the development and implementation of an accelerated and expanded programme in emergency planning and preparedness consisting of four main parts: (1) the upgrading of the Agency's capability to respond, along with its Member States, to a request for assistance in the event of a serious nuclear accident; (2) the development of new technical guidance publications; (3) the development of a training programme; and (4) the fielding of Special Assistance Missions to requesting Member States.

The most recent activity of the Agency relates to the first part of this expanded programme, what we have termed "Mutual Emergency Assistance in Connection with Nuclear Accidents". A nuclear power plant accident which could have serious radiological consequences would require a substantial response effort to mitigate these consequences and to effect the recovery of both the plant and the off-site situation. This effort could tax the resources of a country experiencing such an accident, and in many cases, might well be beyond the capabilities of a country. Even highly developed countries with many nuclear power facilities and a large technical supporting infrastructure could find themselves hard-pressed to cope effectively with a nuclear accident, especially if it involved significant off-site radiological consequences.

Additionally, a nuclear accident in border areas could have serious radiological effects in the territories of neighbouring countries and in cases where these countries have no nuclear installation the capability of dealing with the situation would be limited. Some kind of external assistance enhancing the response capability would, therefore appear to be desirable.

In February of this year, the Board of Governors of the Agency adopted a resolution jointly submitted by the Netherlands, Sweden and the United States calling for a group of experts to study the most appropriate means of responding to the need for mutual assistance in connection with nuclear accidents. The group, consisting of 54 participants and observers from 31 Member States and two international organizations, met 28 June - 2 July of this year.

Their report analyzes the need for establishing mutual emergency assistance, the constraints (such as political, liability, financial, logistics) and the means of overcoming them. It further identifies advance emergency planning requirements which would apply to both potential requesting and assisting parties, the Agency's role in this context and special planning considerations for nuclear power plants located in border areas. The report also considers how legal impediments to the provision of external emergency assistance might be overcome and it concludes in recommending the development by the Agency of a less formal document than a multilateral agreement. This, to be in the form of an information document (INFCIRC) that could be readily agreed to by the parties concerned in the event of a nuclear emergency and that could also facilitate the negotiation of bilateral or regional agreements for mutual assistance. It was the experts' view that the appropriateness of negotiating a multilateral agreement or convention might be considered at a later stage, after an INFCIRC document has been developed as a first step. The report will be submitted to the Board in September of this year for consideration, five months ahead of a February 1983 deadline.

In the area of technical guidance, the Agency published in 1981 and 1982 a set of emergency planning and preparedness documents. These have been well received by Member States and international organizations and they are now in wide use within the international nuclear community. Three of these publications are Safety Series documents dealing with emergency planning and preparedness for nuclear power

facilities and one publication is a Technical Document concerning emergency planning for transport accidents involving radioactive material.

One of the most important emergency planning concepts identified in these documents is the concept of establishing Emergency Planning Zones (EPZs) around power reactor sites. The EPZ concept was developed quite independently in the United States and in several European countries giving significant validity and credibility to this important idea.

To complement these publications, the Agency also is developing two new handbooks, the first dealing with the preparation, conduct and evaluation of emergency preparedness exercises and the second dealing with the practical aspects of assessing off-site consequences of an accident in a nuclear facility including decision-making in an emergency. These documents will be published in 1983 and 1984 respectively.

In the area of training, the Agency developed and conducted in February of this year at the Argonne National Laboratory, the First Interregional Training Course in Planning, Preparedness and Response to Radiological Emergencies. A second course to be offered in the spring of 1983 also at Argonne, will have a new added teaching module concerning the latest developments in "Computerized Aids for Accident Assessment".

Special assistance missions to Yugoslavia and Brazil were completed in 1981. Additional missions are planned in 1982 and 1983 to other interested Member States, with a primary objective of assisting in the development and improvement of emergency plans and response capability.

INCIDENT REPORTING SYSTEM

In the nuclear safety community, increasing importance is being given to collecting information on abnormal events at nuclear power plants. The IAEA is developing this activity along two directions:

(1) Preparing guidelines for national incident reporting systems so that systems organized in different countries are similar and that information may be more easily exchanged.

(2) Organizing a comprehensive incident reporting system that could include OECD countries, the countries of the CMEA (those with planned economies) and the developing countries.

Features of a national system should include the reporting, assessing and evaluating of information on abnormal events in order to identify those significant for safety, and to establish the corrective action that could be taken to avoid accidents or to mitigate their consequences. The system should also ensure ample dissemination of results. To facilitate the organization of national systems and to ensure that they are compatible, the IAEA has developed a draft guide which will be made available to Member States for a 2 year trial period. Comments on the guide will then be requested and a committee convened to formulate a new document which will be published as an Agency safety guide.

The draft now available comprises seven parts. The first part identifies seven categories of events to be reported. These are listed and explained in detail to facilitate the selection and classification of events. One of the more critical categories includes events that lead to exposure to radiation or release of nuclear material. Another includes events that involve the degredation of items important to safety and another covers events that lead to identifying design or operational deficiencies. An additional category concerns unusual events, i.e. man-made or natural events like earthquakes or explosions.

The guide describes in detail the collection and storage procedures necessary for easy data retrieval and guidance is given for screening large numbers of events to identify those that may be of significance to safety. The document then elaborates on the analysis of the event so that proper preventive and corrective actions can be identified.

The second component of the programme is the IAEA-IRS (Incident Reporting System). Currently, the largest international incident reporting system functioning is the NEA system for the OECD countries. Efforts have been initiated by the IAEA to organize a world-wide system which would include not only the OECD but also the CMEA and the developing countries. This broader incident reporting system may be more effective since a world-wide data base might offer an expanded opportunity to identify precursors of accidents.

The development of the IAEA-IRS has reached an advanced stage. The draft procedures for establishing the system have been already reviewed by a technical committee and will be sent shortly to Member States that have nuclear power programmes. Within a year, the draft will be revised to take into account comments received, and then published. Initial operation of the system is planned for the latter months of 1983. A few developing countries have already reported some details of abnormal events to the Agency and it is anticipated that other countries including those of the CMEA will also furnish reports at a meeting to be held in Spain later this year.

The IAEA-IRS system will include all Member States and this may present some initial difficulties. Nevertheless, international recognition of the need to give priority to safety should help in the resolution of any problems that may be encountered.

SAFETY RESEARCH

The potential advantage of international co-operation through shared resources, expertise, and costs is obvious for nuclear safety research undertakings. A Technical Committee on Thermal Reactor Safety Research which met in Moscow in December 1981, strongly supported closer world-wide co-operation and stressed the value of routine exchanges concerning the main objectives of national research programmes and the more significant results. Topics identified of particular interest include containment integrity, early failure diagnosis, hydrogen aspects, fuel behaviour under accident conditions, and fission product release. As a result of the Moscow meeting a Specialists' Meeting on Early Diagnosis of Failures in Primary System Components of Nuclear Power Plants was held in June 1982 in Prague, Czechoslovakia, with strong participation from CMEA countries and encouraging results. Of the 48 participants 29 were from Czechoslovakia, Hungary, German Democratic Republic, Poland and the Soviet Union, and 16 of the 25 papers were presented by experts from these CMEA countries. In a concluding discussion the participants strongly encouraged the Agency to continue holding such meetings.

A second meeting in October 1982, to which representatives from 22 countries and 3 international organizations will be invited, will identify subjects of particular interest and make recommendations on future activities including the subjects of two specialists' meetings which are foreseen for 1983. The topics are likely to relate to the containment area, and possible choices appear to be hydrogen aspects (e.g. generation, release, behaviour, control) and structural aspects (e.g. response to dynamic and thermal loads, internal missiles, leak tightness). The October meeting will also have discussions on other means of exchange, e.g. co-operating in research projects of common interest; the possibility of establishing a Research Project Index similar to those of NEA and CEC, but including CMEA and other countries; exchange of scientists; harmonizing national safety research programmes for better economy. It should be stressed here that these activities are carried out in close contact with OECD/NEA, CEC and CMEA, who are also represented at the research meetings.

CURRENT SAFETY ISSUES

Frequently, when a topic is of widespread current interest, the Agency can provide a forum for airing and perhaps reconciling differing opinions and points of view of safety-related topics. In 1981 a meeting on Fission Product Release Following Severe Accidents brougth together 26 experts from 15 countries and international organizations. The subject, which attracted considerable interest in countries with advanced nuclear programmes,has many controversial aspects and is highly complex. There was agreement that some reduction in the "source term", the postulated amount of radioactive fission products released in a reactor accident is indicated. Since the reduction for many significant postulated accidents might be of several orders of magnitude, this could affect siting and emergency planning, even though estimates of total risk would not be significantly altered at the present time. Several areas of major uncertainty that remain on this question were also highlighted, such as the ability to predict containment failure and the behaviour of aerosols in the primary circuit of a nuclear reactor. The subject is of such interest and is evolving so quickly that a second meeting has been planned for this year.

Another timely topic of interest to both developed and developing countries is that of quantifying safety goals so that a nation's resources can be allocated most effectively. To do so requires a synthesis of nuclear technology, probability theory, economics and sociology in order to arrive at a balanced system to avoid or mitigate the consequences of nuclear accidents. The Agency is planning a meeting in 1982 to discuss this subject. Since it will be the first international meeting on this topic, widespread interest with participation from many Member States is expected.

SESSION 2

NATIONAL PROGRAMS IN NPP SAFETY

Chair: M. Rosen *(IAEA)*
K. Stadie *(OECD)*

Panel Discussion on

NATIONAL PROGRAMS IN NPP SAFETY

Chair: M. Rosen *(IAEA)*

Panelists

R. Bello *(CNSNS)*
S. Bergström *(Studsvik)*
A. Gonzalez *(CNEA)*
L. Lederman *(CNEN)*
K. Stadie *(OECD)*
A. Vuorinen *(IAEA)*

REGULATORY ACTIONS DURING THE TRANSITION PERIOD FROM CONSTRUCTION TO OPERATION

Ruben Bello

CNSNS-MEXICO

ABSTRACT

The role of the regulator to progressively assure safety in order to arrive at the licensing stage without significant safety related issues is presented. Mexico considers such a role as a responsibility, especially when dealing with a utility that is building its first reactor. This concept may appear novel, however it is presented here as inherent in any regulatory scheme.

Based on the above mentioned considerations, the regulatory body of Mexico is prepared to provide assurance that during the transition period from construction to operation of the "Laguna Verde" facility, all possible errors and defects are detected and corrected.

In this manner Mexico will build its nuclear plant as safe as possible.

INTRODUCTION

Activities related to nuclear energy in Mexico began in 1956, with the creation of a National Commission for Nuclear Energy (CNEN). This body was entrusted with the responsibilities of promoting research and development in the fields of nuclear science and technology, plus activities related with exploration of uranium, as well as the establishment of regulatory measures.

In 1968, the Federal Commission of Electricity initiated a nuclear power program in response to the growth in the demand of electricity derived from the high rate of industrial development during that time. The program became a reality with the beginning of the Laguna Verde Nuclear Plant (LVNP) in 1972.

Although there have been delays and some periods of slow progress, Unit I is due to be concluded in 1985 and Unit II about two years later.

From the start of the project the CNEN was invited to participate. It was obvious, however, that the institution lacked the adequate manpower for a project of such magnitude. Furthermore, there was an enormous gap regarding the necessary licensing procedures.

The problem of the lack of a national nuclear legislation in this field was solved by adopting the regulations from the country of origin of the NSSS vendor.

In the case of LVNP, the General Electric Company was selected as the NSSS supplier, therefore the United States' licensing procedures have been applied.

In January 1979, a new law established three different bodies. The new entities were named Mexican Uranium (URAMEX), the National Institute for Nuclear Research (ININ) and the National Commission for Nuclear Safety and Safeguards (CNSNS).

The latter was assigned the responsibility of supervising safety in all nuclear related activities in the country, including, i.e., the control, nation-wide, of the use of radioactive materials and radiological protection. The new law granted the CNSNS the highest possible level of authority within the structure of the Mexican Government, a fact that, added to a decisive support from our authorities, has allowed the Commission to integrate a rather select group which, through intensive programs, has become technically qualified to perform its duties.

CNSNS APPROACH FOR DESIGN AND CONSTRUCTION ACTIVITIES

When the CNSNS was created, the construction of Laguna Verde Nuclear Project had advanced to about 30%.

A review indicated that it was necessary to hire personnel, train and qualify them as fast as possible and to conduct the required regulatory activities, since the utility would not hold up construction waiting for a qualified regulator. There was, at the time, a small group dedicated to regulatory activities within the predecessor agency, the National Institute of Nuclear Energy.

Effective results were obtained when the enthusiastic and dedicated group was augmented with new personnel and a program of training and qualification was implemented. It is recognized, that without the support of the Government authorities such effectiveness would not have been achieved.

As of today, CNSNS has the following personnel:

98 professionals
40 technicians, and
57 support personnel

making a total of 195

DESIGN. As a first approach, consideration was given to the fact that the most significant source of achievements and errors in the construction of any project is found in the design. Accordingly the CNSNS decided to establish a system which assured that the design complied with the applicable rules and regulations.

To this effect, the first joint inspection groups were established. Quality Assurance Personnel was integrated with personnel from the Safety Review Area; the latter were the specialists in the engineering areas of the systems being audited.

These groups conducted audits, not only of the processes and methodology of the design but also of the compliance with the design requirements and the manner in which good engineering practices were applied.

This concept resulted in some protests from the Utility as well as from the Arquitec Engineer and its suppliers; due to the depth with which the audits were made. They sustained that regulation was proceeding beyond what had been considered normal at the time.

The CNSNS had to demostrate that the reasons for reviewing the design in detail were valid and, in many ocassions, problems were prevented and solved as a result of the deficiencies and observations raised by the Commission's auditors.

With reference to this, it can be stated that a design verification effort is presently being finished that covers all the safety related systems, an effort which

was initiated by the audit findings of CNSNS.

CONSTRUCTION. To buy time and to be able to gain the necessary training, qualification and experience in conducting inspections as planned, the CNSNS established a group of "Observers" at the construction site.

The first Observers were referred to, in friendly terms, as the CNSNS spies. Their functions were limited to just observing and noting any event considered important. The Observers provided formal monthly reports which served as a basis for selecting inspection inputs for subsequent inspections. These observer activities were started in May 1979.

When the CNSNS personnel were considered to have sufficient training and experience, a group of resident inspectors was established at the site about mid 1980. These inspectors work on a schedule which includes an average of 2 to 3 inspections a month.

ITEMS TO BE CONSIDERED DURING THE TRANSITION FROM CONSTRUCTION TO OPERATION

The transition from construction to operation offers a great opportunity to perform an independent and detailed verification of the construction and the performance of each one of the safety related systems.

In order to carry out the regulatory activities during the design and construction phases, it was previously estimated that the personnel would be capable of developing its tasks if they were subjected to a relatively intensive training and had experience in other industries.

When dealing with the operation of a nuclear facility, the case is completely different. Consequently, it was then decided to analyze the experience of the regulatory bodies in other countries; specifically with regard to the approach taken during the turn-over from construction to operation and during the first years of commercial operation.

For this purpose, technical visits were arranged with the regulatory bodies of several countries. During these visits the Department Heads of the CNSNS investigated the trends, scope, types of activities, etc., in different areas, during the transition from construction to operation.

When the CNSNS personnel returned to Mexico, several meetings were held to comment and discuss the different approaches found in the countries visited and to establish a proper Action Plan.

From the analysis of the tasks of the various regulatory bodies, a consensus was established regarding the scope and depth the CNSNS should give to its activities. Evidence was obtained indicating that a detailed plan of these activities was required in order to achieve the assurance level necessary to issue the Operating Licence. With this in mind, each of the departments was requested to list the activities they should realize during this phase.

They should also establish patterns for their participation in the system testing, the preoperational test development and finally during the plant start-up.

Later, the tasks to be realized by the CNSNS were established, grouping the activities of all the departments involved. From this, tasks were assigned to the departments in such a manner that each one could develop plans, and establish the necessary resources and schedules.

CNSNS ACTION PLAN DURING THE TRANSITION FROM
CONSTRUCTION TO OPERATION

The activities, which make up the Action Plan are listed in 34 work programs de-- signed to adequately cover the transition phase. See annex.

The Action Plan objective is to determine, in the best possible manner, all the tasks the regulatory body must accomplish, so that each department within the CNSNS is fully conscious of its responsibilities and functions.

The general aspects included in the Action Plan are:

a) DESIGN AND CONSTRUCTION

DESIGN: The review of the Safety Evaluation Report and its complementary documents was made in order to verify that the design included all the requirements established by the CNSNS and that it was satisfactorily accomplished according to all the applicable codes and standards.

CONSTRUCTION: The aim of the activities included in this category, is to verify that the design has been faithfully interpreted during construction, and that all deviations have been clearly identified and will be taken into account in order to verify that the modifications, which must be made to comply with requirements established after the construction phase, have been adequately executed on the system already built.

b) TEST: The objective of the actions in this category is to verify that written procedures and the personnel qualified to execute them, will be available to develope the construction and preoperational tests according to the applicable Quality Assurance Programs. The results of some selected tests shall be evaluated independently by the CNSNS.

c) OPERATION: The target of this part of the plan is to verify that procedures for operation have been formally established, that the operation personnel training has been accomplished and that the Quality Assurance Programs, applicable for Plant operation, are being enforced. The CNSNS is being prepared to issue formal licenses to operators.

d) EMERGENCY PLANS: The activities in this group comprise the emergency plans that include conditions internal and external for the plant. In order to review the adequacy of the necessary procedures, drills are scheduled previous to fuel loading.

e) ENVIRONMENTAL MONITORING PROCEDURES: Our Action Plan also includes the evaluation of the adequate implementation of the environmental monitoring procedures. The monitoring plan should be in operation at least two years before fuel loading.

f) PHYSICAL SECURITY AND SAFEGUARDS: In our case the physical security for the plant as well as the accounting procedures and materials control have special significance. This is due to the fact, that the Unit II construction program shows that Unit I will go on stream at least 2 years before Unit II and will complicate the Physical Security aspects for the unit in operation. For this reason, a special category of activities has been included in the Plan.

g) EXPERIENCE OBTAINED FROM THE TMI-2 ACCIDENT: The Action Plan includes the establishment of the requisites derived from our evaluation of the causes and consequences of the TMI-2 accident. Also included, is the verification that said requisites will be complied with by the utility, by means of operating procedures, design changes and the analysis of critical events in relation to the new criteria. Special attention will be given to operator retraining and to the detailed design revision of the control

room.

An important activity not included in the Action Plan is the presentation to the utility of the "rules of the game" to be used during the transition period. It is also important to obtain an agreement relative to the responsibilities and functions of the Regulatory Body, as well as those of each one of the groups participating on behalf of the utility.

CONCLUSIONS

The analyses of the activities, developed by the Regulatory Bodies of other countries, constitute an element of judgement which we consider very important.

The selection of the activities to be developed by the CNSNS was made possible only after detailed analyses of: the problems detected during the review of the Final Safety Report, the problem identified during construction, and the points of view of other Regulatory Bodies.

The fact that an Action Plan was established several months previous to the LVNP final construction tests, covering all the activities which the CNSNS must develop in order to fulfill its functions, allows us to clearly define our activities, and the training and skill required in those areas where we lack the necessary experience.

To plan with foresight and to determine, together with the utility, the necessity of the exchange of information, limiting milestones and concrete commitments, will prevent that the regulatory activities cause undue delays in the start-up of the nuclear facility.

A N N E X

A C T I O N P L A N

Activities to be realized by the CNSNS during the preoperational phase of the LVNP.

DESIGN AND CONSTRUCTION

Fire Protection.

Radiological Protection.

Radioactive Wastes.

Conformance of the LVNP systems with the FSAR.

Comparison of FSAR Piping and Instrument Diagrams with as-built drawings.

Design review verification.

Plant construction completion certification.

Regulatory response to significant events.

Regulations for reporting events that jeopardize safety.

Verification of compliance with regulations during testing.

Follow-up of unresolved issues.

TESTS

Quality Assurance during preoperation test.

Verification of accomplishment of personnel responsibilities in preoperational test.

Evaluation of procedures.

Witnessing and evaluation of preoperational test results.

In-service inspections.

Preoperational test program records.

OPERATION

LVNP operating personnel training.

LVNP operating organization qualification and efficiency.

Evaluation of LVNP operating procedures.

Utilization of BWR operating experience.

Reports of abnormal events.

Technical Specifications.

Responsibility compliance of safety committees.

Evaluation of off-site organizations.
Licensing of operators.

EMERGENCY PLANS

Emergency plan.

ENVIRONMENTAL MONITORING PROGRAM

Environmental protection.

PHYSICAL SECURITY AND SAFEGUARDS

Physical security.
Accounting and control of nuclear material.
Industrial safety.
Fuel reception and storage.

EXPERIENCE FROM THE TMI-2 ACCIDENT

CNSNS position regarding the TMI-2 accident.

A REVIEW OF THE BRAZILIAN EXPERIENCE IN THE LICENSING OF NUCLEAR POWER PLANTS

L. Lederman [1] and J. J. Laborne

Comissao Nacional de Energia Nuclear
Rio de Janeiro, Brazil

ABSTRACT

In this paper a survey of the licensing of the Brazilian Nuclear Power Plants (NPPs) is presented. The organization and technical expertise of the Comissao Nacional de Energia Nuclear, the Brazilian Regulatory Body, is reviewed with regard to in-house experience, foreign consultants, agreements with regulatory bodies of other countries and research contracts with Brazilian universities. The application of the two-stage licensing process and the stage of development of Brazilian nuclear standards is described. Finally, the paper speculates about the future role of probabilistic risk assessment in the Brazilian licensing process.

INTRODUCTION

On October 10th, 1956, the Comissao Nacional de Energia Nuclear, or CNEN, as it is commonly referred to, was created under the Presidency of the Republic and assigned the responsibility for coordination and direction of the Nuclear Energy Policy in Brazil. [2]

In 1974, Nuclebras (Empresas Nucleares Brasileiras) was formed to coordinate the execution of nuclear activities, particularly on the industrial side. CNEN was kept as the adivsory body for planning and is responsible for the inspection of nuclear activities, as well as being entrusted with the promotion and execution of fundamental research and manpower preparation. Both CNEN and Nuclebras are under the Ministry of Mines and Energy.

According to CNEN's organization, the activities pertaining to reactor safety are carried out by the Department of Power Reactors. This department is responsible for the safety evaluation, inspection, and enforcement during the construction, pre-operational, and operational phases of nuclear power plants (NPP) and research reactors. It examines operator candidates for NPPs and research reactors and inspects the fabrication of NPP heavy components. Over fifty professionals including college graduates, M.Sc. and PhDs are presently staffing this Department.

THE LICENSING PROCESS

Standards And Regulations. [3]

Basically, the standards issuing duties of CNEN are depicted in the laws which form the basis of the monopoly established by the Federal Government for Nuclear En-

ergy in Brazil. It is the task of CNEN's Department of Standards and Specifications to propose regulations, standards, specification, methods, and administrative systems to assure the safe use of nuclear energy. A study group is formed including CNEN's staff and public and private organizations to issue each regulation, standard or specification. Upon being issued by CNEN they must, by law, be implemented throughout the country. On the other hand, those issued by private institutions are voluntary, i.e., without obligation. Over 20 standards are established or being established by CNEN, others are planned for study or review.

The National System of Metrology, Standardization and Industrial Quality (SINMETRO) was established in December 1973, aiming at the promotion of the Brazilian industry, consumer protection, and the establishment of a subsystem of quality certification so as to support the commercialization and competitiveness of Brazilian products in foreign markets. In 1979, the Brazilian Committee for Nuclear Energy, (COBREN), was set up to deal with voluntary standards and to conciliate the current position of the Brazilian industry with world standardization development under the rules and regulations issued by SINMETRO.

Overview Of The Brazilian Experience. [2], [4], [5], [6], [7]

Angra I

The Brazilian experience in the licensing of NPPs dates from 1970 when preparations started to review the Preliminary Safety Analysis Report (PSAR) of NPP Angra I. Angra I is a 627 MWe, Westinghouse PWR, located near the city of Angra des Reis, 133 km from Rio de Janeiro and owned by Furnas Centrais Eletricas, a subsidiary Company of Electrobras which is a government owned electric power holding company. The Angra I PSAR was received by CNEN in December 1972 and the construction permit was granted in May, 1974. In April of 1977, the Final Safety Analysis Report (FSAR) was submitted and on September of 1981 the Provisional Operating Permit was issued. Core loading took place in September 1981 and initial criticality was achieved in March 1982.

The CNEN staff reviewed the SARs based on the applicable standards and regulations. Substantial portions of the safety analysis reports have been independently recalculated using computer codes, either publicly available or developed by the CNEN staff with the support of Brazilian universities and research centers. Core physics, accident analysis, and stress analysis are some of the areas in which independent calculations have been made.

The pre-operational testing phase provided an excellent school for CNEN staff which closely monitored all safety related tests reviewing test procedures and witnessing test performances. The CNEN staff also had a major involvement during core loading and criticality operations through monitoring of these activities.

After revision and approval of the applicant's emergency plans, CNEN developed its own complementary emergency plans extending beyond the plant's exclusion area. Extensive training and drills were conducted under the coordination of CNEN prior to initial criticality.

Prior to issuing the Provisional Operation License, CNEN became aware of problems encountered in Westinghouse steam generators in plants of similar design. Upon detailed evaluation of the problem, CNEN decided to authorize plant operations up to 30% of full power, limiting feedwater flow to the auxiliary feedwater nozzles.

At present, the power ascencion tests up to 30% have been completed and a complete ultrasonic testing of the steam generator tubes is underway. Based upon the results of these tests, CNEN will evaluate whether or not the 30% power limit will be changed.

There is close cooperation going on between CNEN and the regulatory bodies of other countries facing similar problems.

Angra II

In May 1976, the site report for NPP Angra II, a 1245 MWe KWU PWR, located at the same site of Angra I and owned by Furnas, was filed. Site approval was given in November 1976 subject to the fulfillment of several conditions. In January 1977, the PSAR was submitted and on November 1981 the construction permit was issued. Several limited permits for site development were issued prior to issuance of the construction permit. A detailed dynamic structural analysis was developed at CNEN depicting a state-of-the-art model to handle the large number of underground piles and the soil-structure interactions.

Angra III

A site evaluation is being conducted by CNEN for licensing of NPP Angra III, a 1245 MWe KWU PWR owned by Furnas, at a site near Units I and II.

NPP Unit IV

A site evaluation has also started for NPP Unit IV,a 1245 MWe KWU PWR owned by Centrais Eletricas de Sao Paulo, at Peruibe, which is about 200 km from the city of Sao Paulo.

Fabrication Of Heavy Components

The fabrication of NPP heavy components started in Brazil in May 1980 by NUCLEP, a subsidiary of Nuclebras. Since then, CNEN staff has reviewed and approved their quality assurance program. A continuing CNEN inspection program is maintained at this plant to ensure compliance with the approved quality assurance program.

Operator's Qualification

All Angra I reactor operators and senior reactor operators have taken CNEN's required written and practical examination. These exams were prepared and graded by the CNEN staff. They covered all theoretical and practical knowledge deemed necessary for the assurance of safe operations.

Technical Assistance

Technical assistance to CNEN staff comes from agreements with several organizations and contracts with consulting companies. Of major importance is the support obtained from the International Atomic Energy Agency Technical Assistance Programs, the Arrangement for Exchange of Technical Information in the Area of Nuclear Safety between CNEN and the USNRC, and the Contract for Licensing Assistance maintained between CNEN and the German Institute of Reactor Safety (GRS).

Recent examples of technical assistance to the CNEN staff include IAEA Missions to Brazil for the Westinghouse Steam Generator Tube Failure Problem, for the Review of Emergency Preparedness and the participation of USNRC inspectors during the various phases of Angra I pre-operational testing.

FUTURE TRENDS

The safety evaluation of NPPs in Brazil has, so far, relied on a deterministic approach. Plant safety has been analyzed by verifying the ability to mitigate the

consequences of pre-selected design basis accidents, should they occur. This well established methodology limits the scope of the analysis since it assumes that, due to design redundancies, required safety systems will always be available. Thus possible propagation of accident initiator events throughout the sequences involving failures of various plant safety systems are not evaluated.

Probabilistic safety assessments, on the other hand, allowing for unbounded scenarios, have long been used as an alternative or as a complement to the deterministic approach in several countries.

Examples of the large-scale use of probabilistic risk evaluation in the licensing process are the National Reliability Evaluation Program (NREP) and the proposed safety goals of the US Nuclear Regulatory Commission.

It is the firm belief of the author [1] that the probabilistic methodology will play an important role in the Brazilian licensing process in the near future. The use of probabilistic analysis methods by CNEN is to be expected as an aid for licensing decisions based on comparative risk reduction and for the allocation of priorities for safety research.

A probabilistic risk assessment for NPP Angra I or Angra II, under the coordination of CNEN, should be the next step to develop the required familiarity with the technique. The evaluation of NPP fire protection and emergency planning are also areas to be reviewed by probabilistic methods in the near future.

Limited attempts to conduct probabilistic assessments have been developed by CNEN staff with the support of the Brazilian Universities.

The establishment of an adequate system for the licensees to report NPP operational experience data should have a priority consideration as the first plant has already started operation.

It is felt that the knowledge to be acquired by the CNEN staff in handling large probabilistic safety assessments will rapidly move beyond the nuclear sphere bringing real benefits to the country's technological development.

The establishment of numerical safety goals in Brazil is not to be expected until the country's nuclear experience and operational data base can support the consideration of absolute numerical limits for licensing decisions.

To conclude, it can be said, based on accomplished and future goals, that the Brazilian licensing process has the means to guarantee the country's safe use of nuclear power.

REFERENCES

1. currently on sabbatical at the Brookhaven National Laboratory, Upton, NY, 11973.

2. L. LEDERMAN, "The Licensing of NPPs in Brazil", European Nuclear Conference, Hamburg (1979).

3. R. N. ALVES, J. J. LABORNE, J. R. COSTA, "Nuclear Standardization in Brazil", Seminar on Selection and Implementation of Safety Standards for NPPs, IAEA, Vienna (1980).

4. L. LEDERMAN, "Nuclear Power Plant Safety in Brazil", Conference on Current NPP Safety Issues, Stockholm (1980).

5. C. ALMEIDA, "Licensing Requirements for Upgrading Angra I Design During Construction", Seminar on Safety of Two Loop PWRs, IAEA, Vienna (1981).

6. C. ALMEIDA, "Supplier Country Assistance in Safety Review and Inspection of NPPs in a Developing Country", Seminar on Safety Review and Inspection of NPPs, IAEA, Vienna (1981).

7. J. M. LIMA, "The Brazilian Experience in Licensing Reactor Operators for Angra I", Seminar on Safety of Two Loop PWRs, IAEA, Vienna (1981).

NUCLEAR POWER PLANT SAFETY-RELATED EXPERIENCE IN FINLAND

A.J. Rastas
Teollisuuden Voima Oy, Olkiluoto, Finland
and
B.A.O. Regnell
Imatran Voima Oy, Helsinki, Finland

ABSTRACT

Presently, four nuclear power plant units are in commercial operation in Finland. Imatran Voima Oy (IVO) operates two 440 MW PWR units of Soviet design at the Loviisa site. Teollisuuden Voima Oy (TVO) owns two 660 MW BWR units of Swedish design at the Olkiluoto site. The entire experience from the operation of these units until today is about 12 reactor years.

The radiological experience so far is very favourable. The ratios of the collective environmental and occupational doses to the electrical energy produced by the four units until the end of 1981 are 2.2 man mSv/GWa and 1.9 man Sv/GWa, respectively.

The Institute of Radiation Protection (STL) is responsible for full regulatory control and inspection with regard to safety of nuclear power plants in Finland. The number of events reportable to STL has a downward trend. The most significant events until now are discussed in the paper. A brief description of the utilization of operational experience and nuclear safety related research activities in Finland is also given.

INTRODUCTION

Presently, four nuclear power plant units are in commercial operation in Finland, at two different sites and operated by two utilities.

The state-owned Imatran Voima Oy (IVO) operates a nuclear power plant at the Loviisa site, about 100 km east of Helsinki. The plant comprises two PWR units of Soviet design, delivered by the Soviet organisation V/O Atomenergoexport. The net electric output of the units is 440 MW. The units are furnished with two turbine generators and are furthermore characterized by having six primary loops with horizontal steam generators. The containments are furnished with an ice condenser.

Teollisuuden Voima Oy (TVO) operates a nuclear power plant at the Olkiluoto site, on Finland's west coast. The plant comprises two identical BWR units, supplied by the Swedish company AB Asea-Atom. The net electric output of the units is 660 MW. There is one turbine generator for each unit. The units are characterized by the absence of external loops due to the use of internal circulation pumps. The containments are of the pressure suppression type, consisting of pre-stressed concrete structures.

The main commissioning dates and the capacity factors of the Finnish nuclear power plants are given in Table I and II, respectively.

Table I

Main Commissioning Dates of the Finnish Nuclear Power Plant Units

	Loviisa 1	Loviisa 2	TVO I	TVO II
Start of construction	May 1971	Aug 1972	Jan 1974	Aug 1975
Criticality	Jan 21 1977	Oct 17 1980	July 28 1978	Oct 13 1979
Synchronization	Febr 8 1977	Nov 11 1980	Sept 2 1978	Febr 18 1980
Full power	April 4 1977	Dec 12 1980	Jan 1 1979	Nov 11 1980

Table II

Capacity Factors (%)

Year	Loviisa 1	Loviisa 2	TVO I	TVO II
1977	81.2[a]	-	-	-
1978	78.1	-	-	-
1979	75.8	-	60.5[a]	-
1980	36.7	81.9[a]	73.9	65.0[a]
1981	80.6	70.5	79.4	60.8
1982 [b]	95.4	90.2	75.7 [c]	81.7

[a] from the date of full power
[b] until end of June
[c] refuelling outage included

The low capacity factor for Loviisa 1 in 1980 is due to the extensive inspection of steam generator welds and some repair work. The reductions of the TVO I and TVO II capacity factors are mainly caused by generator problems. The average capacity factor of the Finnish nuclear power plants, calculated from the dates of full power until the end of June 1982, is 72.2 %.

In 1981 one third of electricity consumed in Finland was produced by the nuclear power plants. The rather big nuclear share in the electricity production emphasizes the importance of the high availability of the plants.

Due to a declining rate of increase in the consumption of electrical energy and the large capacity now available, no need for new large power plants in Finland is foreseen before the beginning of the nineties. Two nuclear alternatives have been selected for closer study at this stage. These are a 1000 MW four loop PWR of Soviet design, modified for Finnish requirements and a 900 MW French PWR, also adapted to Finnish conditions. Also application of nuclear power for district heating purposes is being considered.

REGULATION OF NUCLEAR POWER PLANTS IN FINLAND

General guidelines for the supervising of the construction and operation of nuclear power plants in Finland are given in the Atomic Energy Act from the year 1957 and in later amendments to it. According to this act a construction license, an operating license and a fuel license are required for a nuclear power plant. These licenses are issued by the Ministry of Trade and Industry (KTM). The revision of the Atomic Energy Act is presently undergoing the legislative process. The main change proposed to the licensing process is a decision of principle needed from the Finnish government before the start of a nuclear power plant project. System of public hearing and parliamentary debate is also proposed for inclusion in the licensing process.

The regulatory review and assessment are conducted by the Institute of Radiation Protection (STL). Before the issuance of each license KTM asks STL for a statement. STL bases its statement about the construction or operational license on a thorough review of the preliminary or final safety analysis report, respectively, and additional design information supplied by the licensee. STL supervises the construction of the nuclear power plant by making so called preinspections, construction inspections, and start-up inspections for individual structures and components. During the commissioning period STL reviews the start-up test programmes, actual tests and test results. STL supervises the operation of the nuclear power plant by reviewing operational reports and by making audits.

The conduct of proper regulatory review and assessment, in a small country like Finland, is a very demanding challenge. The situation in Finland has been further complicated because plants based on different technologies have been built. STL adopted a very independent role already from the beginning. It started developing a guidance system of its own. In addition to that STL wanted itself to become assured of the acceptability of the design solutions. The acceptance given by a foreign safety authority has never been sufficient as such.

The level of the safety requirements has been rather high, already from the beginning. This, together with licensee specifications in some respects exceeding the minimum requirements has contributed to the avoidance of major back-fitting measures so far.

General design criteria for nuclear power plants are given in a document based on Appendix A of USNRC 10 CFR 50. STL is preparing a revision of this document and plans to include some new stricter requirements in it. Many of them have already been adopted in the design of the existing power plants.

For a more detailed guidance STL is developing and publishing so called YVL-guides (Nuclear Power Plant guides). Until now, STL has published 40 guides in the final form and 20 guides in a draft form. Because of limited resources there is no possibility to develop in a small country like Finland, a guidance system covering the whole area of the nuclear power plant safety. Therefore standards and guides from international organizations and foreign countries have been adopted, too.

So far the excessive bureaucracy typical for the licensing process in some larger countries has been avoided. The rather collaborative way to conduct regulatory review and assessment practiced in Finland allows to concentrate upon the issues most important for safety. This, in our opinion, is beneficial from the safety point of view.

RADIOLOGICAL EXPERIENCE

The radiological limits in force in Finland are based on international recommendations. The dose-equivalent limits for the individual in the environment of a power plant site are 100 μSv to the whole body and 300 μSv to a specific organ. In addition, the one year operation of a nuclear plant should not cause a collective dose (plant personnel excluded) exceeding 5 man mSv per MW of installed useable power.

The main data related to environmental doses are presented in Table III. Occupational doses are given in Table IV. The ratios of the collective environmental and occupational doses to the electrical energy produced by the four units until the end of 1981 are 2.2 man mSv/GWa and 1.9 man Sv/GWa, respectively.

Table III

Maximum Individual Whole Body Dose-Equivalent and
Collective Whole Body Dose-Equivalent in the Environment

Year	Loviisa 1 + Loviisa 2		TVO I + TVO II	
	Individual /uSv	Collective man mSv	Individual /uSv	Collective man mSv
1977	0.0011	0.000050	-	-
1978	1.0	1.3	0.0041	0.061
1979	1.2	1.7	0.085	0.11
1980	2.4	3.9	0.20	0.36
1981	0.23	0.77	0.22	0.34

Table IV

Collective Occupational Doses (man Sv)

Year	Loviisa 1	Loviisa 2	TVO I + TVO II
1977	0.006	-	-
1978	1.05	-	0.03
1979	1.40	-	0.23
1980	2.05	0.05	0.54
1981	0.90	0.54	0.62 [b]
1982 [a]	0.07	0.02	0.81

[a] until end of June
[b] refuelling outages included

The radiological experience obtained so far from the operation of the Finnish nuclear power plants is very favourable. The activity releases have been extremely low, and the environmental and occupational doses are well below allowed limits. One explanation of small dose values is a very low fuel failure rate. Loviisa 1 and TVO I have experienced one failed fuel rod each, Loviisa 2 and TVO II none. The exceptionally low occupational doses compared with international averages are also due to plant design, operational procedures and adopted radiation protection policies (1, 2, 3).

REPORTABLE EVENTS

STL expects to receive from the licensee following reports:

- daily, monthly and annual reports
- special reports
- reports on reactor trips
- reports on operating disturbances
- notifications and reports on damages in pressure vessels
- environmental radiation safety reports
- reports on personal radiation doses
- reports on nuclear materials
- reports on the results of inservice inspections
- reports on outages and individual work performances.

Submission and contents of the reports are specified in detail in an YVL-guide.

A special report is compiled on a safety-related event or observed deficiency. The annual numbers of the reported events are given in Table V.

Table V

Annual Numbers of the Special Reports

Year	Loviisa 1	Loviisa 2	TVO I	TVO II
1977	14	-	-	-
1978	32	-	26	-
1979	16	-	26	2
1980	14	-	10	3
1981	12	8	2	2
1982 [a]	1	0	2	0

[a] until end of June

The fairly large number of reports is partially due to the quite low threshold of reporting, especially during the first years. The downward trend in the number of the special reports is obvious.

From the body of reported events and deficiencies the most significant ones are described below.

Loviisa plant

Inadvertent opening of a steam generator safety valve

At the Loviisa 1 unit an inadvertent opening of a steam generator safety valve occurred in 1978. Due to a fault in a pressure signal conversion unit one safety valve was fed a continuous signal, indicating a pressure of 75 bars (opening pressure 56 bars). The level in the affected steam generator decreased and the primary pump in that loop was stopped manually. The isolation of the affected loop was initiated (stop valves in the loops are available). Within a few minutes it was determined that the valve had opened inadvertently. The valve was manually closed. In the meantime the steam generator level had decreased enough to start the auxiliary feed pumps. The transient was later evaluated from the point of view of thermal stresses. These were found to be insignificant. Thanks to the rapid and correct actions by the operators a more severe transient was avoided.

Primary circuit cool-down transient

In 1981 at the Loviisa 2 unit, due to a combination of two instrument malfunctions a situation arouse where a small increase in the secondary pressure opened a by-pass valve to the condenser. This in turn led to a cool-down transient on the primary side, initiating the safety injection system. Unfortunately, the by-pass valve did not work properly, but got stuck in its open position. By the time this was realized by the operators and corrective action was taken, the primary temperature had fallen to about 220°C. Before restart the thermal stress effects of this transient were carefully analysed and found to be quite small.

Pipe hanger attachment deficiencies

In 1979, alerted by reports from other plants, the quality of pipe hanger attachments to concrete walls were inspected. Because deficiencies were found in the first inspection, an extensive program for inspection and correction of defective attachments was carried out. This program caused a three week shut-down of Loviisa 1.

Pressure vessel embrittlement

In 1980 the first samples of pressure vessel steel irradiated in the Loviisa 1 reactor were tested for radiation embrittlement. The tests indicated a faster embrittlement than anticipated. As a preventive measure, to slow down the rate of embrittlement, it was decided to replace the 32 outermost fuel elements by dummies. In order to reduce the thermal stresses caused by safety injection water, the accumulator temperature and the refuelling water storage tank temperature were raised.

Steam generator weld indications

In connection with in-service inspection of Loviisa 1 steam generator, indications of faults in certain welds were observed in 1980. This led to an extensive program of inspection and, if needed, repairing of all suspected welds in the steam generators. The work was also extended to the loop stop valves. Highly sophisticated methods and instruments were used in this difficult work with good results. The work was difficult, because it involved personnel entering into the steam generators with very little working space available. Because of the radiation level, decontamination had to be carried out (2). For decontamination special equipment was developed, and the result was excellent. Because of this additional work the planned two month refuelling outage was streched out to seven months.

TVO plant

Rupture of a reactor water clean-up system pipe

At TVO I the most significant safety-related event so far has been a rupture of a stainless steel pipe in the reactor water clean-up system outside the containment in August 1979. The outer diameter and the wall thickness of the ruptured pipe were 168 mm and 14 mm, respectively. The length of the longitudinally oriented crack was 150 mm and it was 1.5 mm open. The crack was located about 0.5 m downstream from a T-junction in the piping. The reason of the rupture was thermal fatigue. It was caused by temperature fluctuations due to the mixing of water flows at different temperatures (130 ^{o}C and 280 ^{o}C) coming to the T-junction. The unfavourable flow conditions arouse from an erroneous valve position in the system.

The reactor protection, isolation and safety systems worked during the event without any faults. About 5 m^3 reactor water leaked out from the rupture. Radiological impact on the environment was negligible.

Reactor depressurization transient

A stuck open control valve in the reactor pressure relief system caused a couple of reportable events at TVO I in spring 1980. The reactor pressure decreased in one of these events to 4.5 MPa in seven minutes before the valve in series with the stuck open control valve was closed by operators. The transient was deemed quite harmless for the reactor pressure vessel. In the design bases of the vessel ten total depressurization transients through one relief valve have been assumed to happen during the life time.

The erroneous function of the control valve was caused by loose fixing screws of the drive motor.

Stress corrosion cracking in reactor pressure vessel internals

After having received information on cracked bolts in the core grid of the Forsmark 2 unit in Sweden the corresponding bolts were inspected by ultrasonic at TVO I during the refuelling outage in May 1982. About one tenth of the bolts were found to be almost broken. In addition to that about one third of the bolts had indications of cracks. The cracks were caused by intergranulal stress corrosion of bolt material (stainless steel SIS 2570-04, ASTM SA-453 Grade 660). The bolts are used to fasten vertical guide rails to the core grid plates which provide lateral support for the top ends of the fuel assemblies. The diameter and the length of the bolts are 65 mm and 10 mm, respectively. The number of bolts is 500.

As a provisional measure 37 fuel bundles in the core were provided with new top tie plates of modified design. The rails in the new top tie plates prevent the loosening of the broken bolts. In this way 148 bolts, including all bad ones, were secured. The final repair of the TVO I core grid will be carried out during the refuelling outage in 1983.

Cracks were found in corresponding bolts of TVO II, too. All bolts were replaced by new ones, made of different material. For the repair work the core grid was removed from the reactor vessel to the storage pool.

All reactor internal components made of same material were inspected at TVO I and TVO II. Cracks were found also in beam springs supporting the reactor internals from above. Seven beam springs are assembled in a polygon inside the reactor pressure vessel cover. They are elastically deformed by the internals when the pressure vessel cover is fitted. The length, maximum height and width of a beam are 2165, 150 and 70 mm, respectively. All beams of TVO I and TVO II were replaced by new ones, made of another material.

UTILIZATION OF OPERATIONAL EXPERIENCE

Operational safety of nuclear plants can be enhanced by efficient use of operational experience both from the own plant and other plants. Both at the Loviisa plant and the TVO plant operational occurrences, equipment failures and design deficiencies are reviewed by special safety groups and appropriate actions are implemented. In order to exchange safety-related experience the chairman of the IVO's group is a joint member of the TVO's corresponding group and vice versa.

In 1980 a group with members from STL, IVO, TVO and the Technical Research Center of Finland (VTT) was formed. The primary task of the group is to review reported occurrences in nuclear plants all over the world, to point out the lessons to be learned from these occurrences and to distribute the reports and the group's conclusions to designers and operating personnel who can take advantage of this kind of information. The organization and work of the group is still under development, but the results so far obtained are encouraging.

Speaking of lessons learned from experience at other plants, the accident of the Three Mile Island plant had a considerable impact in Finland, especially at the Loviisa plant with PWR reactors. A very thorough review of the accident itself, characteristic design features of the affected unit and the corresponding design features of the Loviisa plant was carried out. Even if a similar accident sequence turned out to be very improbable, a number of improvements and modifications in line with NRC's recommendations have been carried out. Some work is still going on, e.g. measures are taken to ensure safety of the plant in the case of a much more extensive metal-water reaction than originally assumed.

TRAINING, RESEARCH AND INTERNATIONAL COOPERATION

Nuclear engineering can be studied at the University of Technology in Helsinki and Lappeenranta. In connection with the former VTT operates a research reactor of the type Triga Mark II, also extensively used as an educational tool. A substantial part of the expertise needed for the design, construction and operation of the present nuclear power plants in Finland has been obtained from the research reactor laboratory.

Training of reactor operators has partly been undertaken by the reactor suppliers, partly by the utilities themselves and the above mentioned institutions. An important role of the continual training programs is played by simulators. For the Loviisa plant a full scope simulator, now in operation at the plant site, was designed and built as a joint Finnish project involving IVO, VTT and Nokia Electronics (4). In addition to operator training, the Loviisa simulator has been used for other tasks, e.g. testing of operating procedures, studying of transients occurred at the real plant and investigation of disturbance handling systems. TVO has made arrangements with the Swedish undertaking AB Kärnkraftutbildning (AKU) allowing their operators to use a training simulator in Sweden.

The limited resources of a small country like Finland do not permit extensive research in nuclear safety. Most of this work is carried out at VTT. Some experimental work on reflooding is being conducted at the Lappeenranta University of Technology (5). The work done at the hydraulic laboratory of IVO may also be mentioned.

An important activity of VTT is the acquisition, development and application of computer codes for evaluation of nuclear safety. Several wellknown codes, like RELAP, CONTEMPT, GAPCON and FRAP have been extensively used, among other things for the carrying out of confirmatory accident analysis as required by STL. VTT has also developed codes of their own like the transient codes TRAWA, TAPP and TRAB (6,7) tailored for the Finnish nuclear power plants, the fast small break code SMABRE (8), the hydraulic transient code TMOC (9), the pipe whip code PIPEBREAK (10), the environmental consequence code package ARANO (11), and the probabilistic fuel damage code ACCREL-2 (12). The cooperation between Nordic Countries has produced advanced NORCOOL codes specialized for the BWR ECCS analyses.

Nuclear power plant automation is an important safety-related research field of VTT. Results of these studies were extensively utilized in the design, commissioning and operator training for the Loviisa plant (13). The dynamic plant models on a hybrid computer was formerly in active use. The latest activities have mainly concentrated upon the control room design and the disturbance handling systems.

Activities on reliability methods and applications were started at VTT about ten years ago. VTT has carried out reliability analyses for safety systems of the nuclear power plants in connection with the licensing. Recent activities are concentrated upon reliability aspects in setting operational limits and requirements (14,15,16).

Safety related research at VTT concerning construction and fuel element materials has been concentrated on the evaluation of the structural integrity of reactor pressure vessel and other primary circuit components as well as fuel elements in normal and accident conditions (17). The main emphasis has been on the evaluation of the fracture and corrosion behaviour of materials as well as on irradiation damage. The reliability of various NDT-methods has also been studied.

To compensate for lack of resources, Finland is participating in a number of international projects, e.g. LOFT, PBF (Power Burst Facility) and HSST (Heavy Section Steel Technology) in USA, Marviken in Sweden and Halden in Norway. A joint project between VTT and the All Union Heat Engineering Institute (VTI) in Moscow has been completed (18). Outside these projects, extensive cooperation is taking place within the Nordic Countries.

CONCLUSIONS

Safety and reliability of nuclear power plants are primary goals for the efforts made during their design, construction, and operation. In countries like Finland, where the share of nuclear power is large, the achievement of high availability is of particular importance. Embarking on a nuclear power program is a challenge, especially for small countries with limited resources. Lack of resources can partly be compensated by international cooperation, especially in areas of utilization of regulatory requirements and operational experience, and in various research activities. However, it is essential that a substantial amount of domestic expertise is available to actively take part in the accomplishment of the nuclear projects, and to ensure the safe operation of the plants independently of the supplier. The important role of knowledgeable and dedicated regulatory bodies should be recognized.

REFERENCES

1. A.T. RUUSKANEN and R.O. SUNDELL, "Measures associated with the Dose Limitation System at TVO Power Company", presented at the International Symposium on the Application of the Dose Limitation System in Nuclear Fuel Cycle Facilities and Other Radiation Practices, IAEA/WHO/OECD/NEA/ICRP, Madrid, 19-23 October 1981.

2. J. HELSKE und R. JÄRNSTRÖM, "Erfahrungen im Kernkraftwerk Loviisa mit der Dekontamination von Dampferzeugern und Primärkreiskomponenten", VGB Kraftwerkstechnik 62, 223 (1982).

3. R.T. JÄRNSTRÖM, "Experience of Primary Circuit Water Chemistry in Loviisa 1 NPP", presented at the Second International Conference on Water Chemistry of Nuclear Reactor Systems, British Nuclear Energy Society, Bournemouth, 14-17 October 1980.

4. M. NEVALAINEN and J. SAASTAMOINEN, "Simulator for Loviisa", Nucl. Eng. Int. 25, 296 (1980)

5. T. KERVINEN, "Reflood Experiments with Simultaneus Upper and Lower Plenum Injection in the REWET-II Rod Bundle Facility", presented at the International Meeting on Thermal Nuclear Reactor Safety, ANS/ENS/CNS/JAES, Chicago, Aug. 29 - Sept. 2, 1982.

6. M. RAJAMÄKI, "TRAWA, A Transient Analysis Code for Water Reactors", Technical Research Centre of Finland, Nuclear Engineering Laboratory, Report 24 (1980).

7. M. RAJAMÄKI, "TRAB, A Transient Analysis Program for BWR, Part 1. Principles, Technical Research Centre of Finland, Nuclear Engineering Laboratory, Report 45 (1980).

8. J. MIETTINEN and M. HÄNNINEN, "Experience about a Two-Phase Model SMABRE in a Full Scale PWR Plant Simulator", presented at the International Meeting on Thermal Nuclear Reactor Safety, ANS/ENS/CNS/JAES, Chicago, Aug. 29 - Sept. 2, 1982.

9. T. SIIKONEN, "Computer Program TMOC for Calculating of Pressure Transients in Fluid Filled Piping Networks", presented at the Topical Meeting on Nuclear Power Reactor Safety, ENS/ANS, Brussels, 16-19 October 1978.

10. K. IKONEN, T. KUKKOLA and M. KANGAS, "Local Crush Rigidity of Pipes: Experiments and Application to the Pipe Whip Restraint Design", presented at the 5th International Conference of Structural Mechanics in Reactor Technology, Berlin, 13-17 August 1979.

11. I. SAVOLAINEN and S. VUORI, "ARANO- A Computer Program for the Assessment of Radiological Consequences of Atmospheric Radioactive Releases", Technical Research Centre of Finland, Nuclear Engineering Laboratory, Report 53 (1980).

12. R. SAIRANEN, L. MATTILA and J. VAURIO, "Probabilistic Analysis of Fuel Damage and Radioactivity Release during an LWR LOCA", presented at the Topical Meeting on Reactor Safety Aspects of Fuel Behaviour", ANS, Sun Valley, 2-6 August 1981.

13. I. EKMAN and P. HAAPANEN, "Experience on the Design and Start-up of the Instrumentation and Control Systems for Loviisa Nuclear Power Plant in Finland", presented at the Specialist Meeting on Acquisition of Control and Instrumentation Technology for Countries Embarking on Nuclear Power Programmes, IAEA, Madrid, Nov. 30- Dec. 3, 1981.

14. T. MANKAMO, P. AALTONEN, P. PORVARI and R. VIROLAINEN, "Allowable Repair Down-Time in Stand-by Safety Systems", presented at the Meeting on Probabilistic Risk Assessment, ANS/ENS, Port Chester, 20-24 September.

15. T. MANKAMO, "Optimizing Test Intervals of Stand-by Diesel Generators", Reliability in Electrical and Electronic Components and Systems, 786, North-Holland Publishing Company (1982).

16. T. MANKAMO and U. PULKKINEN, "Dependent Failures of Diesel Generators", Nuclear Safety, 23, 32 (1982).

17. K. TÖRRÖNEN (ed.), "Reliability of Reactor Materials Program, Semiannual Progress Report for Period ending June 30, 1981", Technical Research Centre of Finland, Metals Laboratory, Research Report 87 (1982).

18. V.I. KISINA, A.S. KONJKOV, D.L. PROZEROV, N.V. TARASOVA, K.L. EERIKÄINEN, O.M. TIIHONEN and T.A. VANTTOLA, "Experiments on Heat Transfer Crisis in Triangular Lattice Configuration", presented at the International Meeting on Thermal Nuclear Reactor Safety, ANS/ENS/CNS/JAES, Chicago, Aug. 29 - Sept. 2, 1982.

SCIENTIFIC/ENGINEERING JUDGEMENT IN SWEDISH REACTOR SAFETY ASSESSMENT

Stig O W Bergström
Studsvik Energiteknik AB
S-61182 NYKÖPING, Sweden

ABSTRACT

The Swedish nuclear energy program started in the late 1940's. For two decades the development proceeded in a climate of widespread scientific, political and public acceptance of nuclear energy as such. The debate that existed concerned the choice of reactor design and similar mainly technical/economical questions.

Since the early 1970's on the contrary there has developed an attitude of distrust towards the nuclear industry and often also the staff of the safety authorities and any level of decision makers where risk/benefit assessments are made. The author describes this change mainly by examples from governmental studies since 1959, focussing on source term and environmental consequences applied in siting decisions and emergency planning.

INTRODUCTION

This paper attempts to follow the way in which scientific and engineering judgement has influenced nuclear safety assessment in Sweden since the start of the nuclear energy program in the 1950's. It is focussed on the determination of accident source term and environmental consequences for use in siting decisions and emergency planning. The views are entirely those of the author and should not be taken as an official standpoint of the Swedish government or safety authorities or a STUDSVIK company policy declaration.

DECISION PROCESS

Laws and criteria governing nuclear energy are created in the same way as those connected with other activities in the Swedish society. Usually the government asks for a study to be performed by a commission or committee which reports back to the government. The report is then sent out for public review. After that the government submits its own proposal based on the report and the information supplied by individuals and organizations in the review. If the parliament accepts the proposal with or without changes the government then issues a law or directs its safety authorities to apply the criteria proposed. The result of the proposal might also be that a new authority is created or that the existing one is modified to comply with the findings of the commission. In the nuclear energy field both the types of study demanded by the government and the staffing of the main committees and their expert sub-committees has changed a lot during the thirty years since the different atomic acts in Sweden started to be issued.

Another thing that has changed a lot is the general climate in which the different committees have had to work while producing their reports. From 1946 and until 1970 there was a generally very positive attitude among the public, among politicians, and in the mass media for everything concerned with the development of peaceful nuclear energy. The situation became somewhat more touchy during the early 70's, when opposition against nuclear energy started to be more than refreshing incidents at public hearings. In the election 1976 Sweden got a new three party government, where the largest party, having the Prime Minister post, was declared against nuclear power. Finally, just before the election 1979 the TMI-2 incident created large resonance effects in Swedish political life. The commotion ended in a compromise to get rid of this awkward problem during the campaign for the parliamentary election. The future of the Swedish nuclear power program was then put to a referendum in the Spring of 1980 [1]. The outcome is well-known. There were three alternatives, none of them very clear-cut, all large political parties aware of having both proponents and opponents among their normal voters. Later on the parliament decided that the result of the referendum meant that Sweden should operate up to 12 reactors for 25 years per unit with the last reactor shut down AD 2010. Thus, Sweden, with the biggest per capita production of nuclear power in the world - at present and for a long time to come - is the only country in the world that has decided that it does not need any nuclear power 25-30 years from now.

THE ROARING FIFTIES AND SIXTIES

The first report from a commission investigating the emergency planning required to cope with credible nuclear accidents was delivered 1959 [2]. Investigator was the head of the Swedish Insurance Inspection who had at his side a couple of legal experts and three physicists coming from the safety authorities and the nuclear industry. The report refers to an expert study on the largest accident consequences, which it was reasonable to base an emergency organization upon. This expert study was actually using information from Wash-740 [3]. Already then it was realized that some of the assumptions in Wash-740 should be made more realistic to be useful in connection with practical emergency planning. The main report states the possibility of acute radiation effects up to 5 kilometers but points out that milk restrictions might be required out to very large distances - 120 km and an area of about 1000 km^2 is mentioned. Finally, the report states that theoretically it would be possible by utilizing extreme values for all parameters involved to define an accident with much greater consequences. The investigator, however, concludes that the figures given should be considered to give a representative picture of the size of the areas which might be involved in connection with severe accidents.

The comparison with WASH-740 shows that reactor size and population characteristics were fairly similar, but that dispersion characteristics and source term was judged differently by the Swedish experts at least from what was used in calculation of maximum consequences in the American report. A practical result of the study was that all Swedish nuclear power stations have an exclusion radius of about 2 km, and that regional authorities have been requested to keep population changes out to about 10 km from each site under observation. The report and the atomic emergency act that was simultaneously proposed were both accepted without much debate, and the act has been the basis for Swedish nuclear emergency organization until 1981.

During the 1960*s the assumed optimum reactor size increased steadily, so that from the 500 MW quoted in ref [2] the thermal power of units actually built ranged from 1500 to 3000 MW. To balance the larger radioactive inventory engineered safeguards of increasing sophistication were introduced to reduce the source term in case of an accident. In parallel, atmospheric dispersion and mechanisms like rainout and deposition, retention in the containment and so on, were subject to studies to establish safety margins which earlier had not been taken into account. During this time

the four power reactor sites in Sweden were approved after due consideration by the safety authorities and through decisions by the government. Even though the expression "design basis accidents" was substituted for the earlier "maximum credible accident", there was all the time a declared attitude, that an emergency organization and planned emergency counter measures in case of accidents should be based not on a maximum hypothetical accident but on a very severe and unlikely though still credible accident sequence. This called for a lot of careful consideration and judgement mainly among the safety authorities and the regional administrative authorities responsible for the emergency organizations.

THE INVESTIGATIVE SEVENTIES

Siting condensing units at the four sites thus did not give rise to much opposition, even though the Barseback site was only some 25 km from both the Swedish city of Malmö and from the Danish capital of Copenhagen. Around 1970 urban siting was attracting interest for several different reasons. Coastal areas suitable for industrial sites are getting scarce also in Sweden which otherwise is quite fortunate in that respect. Further one realized the advantage of shorter power transmission lines to highly populated areas and from utilizing reactors in large district heating systems. 1968-69 the Stockholm electricity authority proposed to locate a heat and power reactor in the rock only a couple of kilometers from the centre of Stockholm. After some deliberation the safety authorities suggested that the problems connected with such a localization should become subject of a thorough investigation. In 1970 the government appointed a committee to look into this problem. Later on, in 1971, the study was extended to treat also siting at intermediate distances from the city centre. This committee like the one in 1959 consisted mainly of specialists from the authorities and from the industry, but had also representatives from the ministries concerned.

The Urban Siting Study [4] was reported in August 1974, just before the US Reactor Safety Study, WASH-1400 [5] appeared in a draft version. The latter tried to estimate the total risk picture from the US nuclear power program. The former, instead, assumed that the already established siting decisions represented a risk that was accepted by the Swedish society and discussed only the additional risks introduced by choosing urban or near-urban sites for future power (and heat) reactors instead of conventional localizations. This difference was never acknowledged (or observed) by most critics in Sweden. In the wake of the debate around WASH-1400 and the Urban Siting Study a series of governmental studies on energy production and its environmental effects were launched from 1976 and through 1979, when the TMI-2 incident led to an intensification of public concern about nuclear safety issues.

The Urban Siting Study calculated only acute effects from large accidents and made the judgement that for these effects, releases of iodine and noble gas radionuclides were of dominant importance for a relative risk assessment between sites at different distances from large population centers. Further, the committee judged that source term assumptions had to allow for 100 % noble gas releases but that iodine releases used for internal and external exposure calculation could be limited at 3 to 30 % of the reactor inventory. Its conclusions also took into account an efficient thermal plume rise in connection with accidents leading to rapid release of as much as 30 % of the iodines. Finally, the atmospherique dispersion calculations were based on actual, observed statistics with a probability of down to 0.0015 which was the lower limit obtainable with acceptable confidence.

The opponents of course pointed out the much larger iodine releases used in WASH-1400 and the influence of the quite high release fractions of other fission products also assumed there. Further, dispersion conditions applied in WASH-1400 were studied to much lower theoretical (but not observed) frequencies than the ones used in the Swedish study.

In 1977 a new report "Energy, Health, Environment" [6] was published by a committee, also this one composed mainly by members of parliament, with subcommittees dominated by representatives from different health and safety authorities. This report quotes information from WASH-1400 but does not present a judgement of its own as to the absolute risk level from nuclear accidents or how this might compare with risks from other energy sources.

Already at the publication of the 1977 report, another study was well under way. It had been requested by the new non-socialistic government of 1976 and was launched in a very grand manner. This so-called "Energy Commission" included members of parliament and experts not concerned with the nuclear industry or nuclear safety authorities. Also the commission's subcommittees recruited its experts to a large extent from circles not involved with nuclear energy. For the first time representatives of the declared opposition against nuclear energy were included both in the main commission and in the subcommittees. The commission had a politically very difficult task as the three parties forming the new government were disagreeing on the nuclear issue and the dominant opposition party was mainly pro-nuclear.

The main report [7] concludes that the risks from (large) very improbable accident lie within acceptable limits. The commission also states that administrative and technical measures can be taken if the risks in the future should be found larger than expected. These statements apply to nuclear energy as well as other sources. One of the commission members, however, who served as chairman of the safety and environment subcommittee, filed a reservation on the grounds - among other things - that the knowledge about large accident consequences was insufficient. Both the main commission and the subcommittee quote WASH-1400 and the US debate on this study. The subcommittee had in its background material two different consequence analyses, one from a Swedish and one from a US consultant. Parameter values applied in the US analysis were extremely conservative as to dispersion and deposition and not coupled to actual observations. The Swedish analysis used the same concentration statistics approach as in the Urban Siting Study. The large consequence difference between these two calculations was taken as a measure of the general uncertainty by the sub-committee chairman.

The publication of the energy commission report early 1978 lead to a 75 % parliamentary majority supporting continued development of nuclear energy in Sweden. A year later the TMI-2 incident, about a month before the Parliament was supposed to approve this program, stopped the decision process and called for new investigations.

The reactor safety investigation [8] called its report "Safe nuclear power?", whereas the radiation protection institute delivered "More efficient (nuclear emergency) preparedness" [9] without any question-mark. The former committee had a very tough time table that did not allow for the production of much new information. Without detailed argumentation it criticizes the energy commission's judgement on the risks from large accidents and refers to the energy commission sub-committee report and to ref [6] as giving well-balanced accident analyses. Among other things this leads the reactor safety committee to stress development of new engineered safeguards for consequence mitigation. Its favourite among these is vent-filter arrangements which are supposed to be possible to add on to all existing Swedish power reactors. Such arrangements had been studied for some time - even before the TMI-2 incident - but no detailed design had yet been developed. It is remarkable that a committee with a dominance of non-engineering competence could feel so convinced about the positive

net safety effect of a quite complex addition to the very complicated system that a nuclear power plant represents.

The radiation protection institute had been asked by the government to look over the adequacy of the existing emergency organization based on ref [2]. This study is thus performed by one of the expert safety authorities concerned with nuclear safety. The report accepts the source strengths in WASH-1400 for accident types PWR 1A and BWR 1 as relevant for describing consequences which the emergency organization should be able to cope with. The report illustrates consequences with these source strengths and "artificial" weather conditions of extreme severity but unknown probability. The picture is summarized in quoting earlier reports ref [6], the sub-committee report of ref [7] and ref [8] besides WASH-1400 with the remark that the institute has found no reason to believe that the largest (relevant) accident consequences fall outside these ranges.

The figures given are:
- Acute deaths: hundreds to thousands
- Late cancer deaths: thousands to tens of thousands
- Contaminated land areas: thousands to tens of thousands km^2

Some reservations are listed but not quantified. This report was published a couple of months before the nuclear referendum.

Much less attention was attracted by a later report [10] by a small expert group with the task to evaluate the probability of the very large steam explosions which are included in the severe accident sequences postulated in ref [9] as a basis for emergency planning. The new report concludes that it is not necessary to take the effects of steam explosions into account when safety systems and emergency measures are determined. One of the committee members is still more explicit in a special comment included in the report. He admits that small steam explosions are possible but that they never will reach such strength that the integrity of reactor vessel or containment can be endangered. He further draws the conclusion that the consequences described in emergency study [9] can not be used as background for emergency planning at nuclear sites.

In the meantime, however, the Swedish government had decided that the two Barseback units should be provided with a vent-filter addition to their containments [11]. On the other hand, it seems as if the tune-up of the emergency organizations is aiming at a slightly lower ambition level than what could be congruent with the worst consequence pictures in ref [9].

CONCLUSION

This has necessarily been a very fragmentary (and mainly qualitative) description of the diminishing influence of technical and scientific judgement on the official attitude in Sweden towards risks from large nuclear accidents. It is the hope, and perhaps too optimistic, view of the author that we have reached the peak of simplistic overconservative parameter choice in accident calculations applied to nuclear siting and emergency planning.

It is amazing how little interest and effort have been directed towards studies on the possible overestimates of source term and exposure mechanisms. Studies aimed at defining realistic models for radioactive releases, for retention in the degraded core, in the primary system and in the reactor containment are now under way in several countries and in multinational cooperation. These studies will most likely establish significant reductions in the source terms to be applied in accident consequence calculations. The author is convinced that similar reductions can be de-

monstrated in the exposure models used at present and would welcome an international cooperation also in this field. The source term is, of course, easier to treat in a way that is universally applicable, but the fundamental mechanisms governing radioactivity transport in the environment should also be the same for most sites.

REFERENCES

1 S O W BERGSTRÖM, "Public Administration and Nuclear Safety," Lecture at a seminar in Barcelona, May 28, 1980.

2 "Beredskap mot atomenergiolyckor," SOU 1959:38, Industridepartementet, Stockholm, (1959).

3 "Theoretical possibilities and consequences of major accidents in large nuclear power plants," WASH-740, USAEC, (1957).

4 "Närförläggning av kärnkraftverk," SOU 1974:56, Industridepartementet, Stockholm, (1974).

5 "Reactor Safety Study. An Assessment of Accident Risks in US Commercial Nuclear Power Plants," WASH-1400, USNRC, (1975).

6 "Energi, hälsa, miljö," SOU 1977:67, Jordbruksdepartementet, Stockholm, (1977).

7 "Energi," SOU 1978:17, Industridepartementet, Stockholm, (1978).

8 "Säker kärnkraft?," SOU 1979:86, Industridepartementet, Stockholm, (1979).

9 "Effektivare beredskap " , Statens strålskyddsinstitut, Stockholm, (1979).

10 "Ångexplosioner i lättvattenreaktorer," DsI 1980:28, Industridepartementet, Stockholm, (1980).

11 K JOHANSSON et al, "Design considerations for implementing a vent-filter system at the Barseback nuclear power plant", to be presented at ANS Chicago meeting, August 29 - September 2, 1982.

THE REGULATORY USE OF PROBABILISTIC SAFETY ANALYSIS IN ARGENTINA

A. J. Gonzalez

Comision Nacional de Energia Atomica
Avda. del Libertador 8250
1429 Buenos Aires, Argentina

ABSTRACT

This paper describes the regulatory use of probabilistic safety analysis by the Argentine competent authority. A historical background of the use of probabilistic approaches in the Argentine nuclear safety programme is presented. A probabilistic safety criterion enforced by the authority for the purpose of licensing nuclear power plants is described. The logics of the criterion is based on probabilistic safety goals derived from the individual-related requirement of the dose limitation system used for radiation protection purposes. The use of the criterion in the licensing process of the Atucha II Power Plant is described. Finally, the paper analyzes the limitation of the criteria, as an individual-related requirement, to take appropriately into account the overall expected impact from the source and the theoretical difficulties involved in the complementation of the criteria.

1. INTRODUCTION

The Argentine nuclear safety programme is following the current world tendency, continuously improving the safety levels of nuclear power plants while still allowing the generation of energy by nuclear means. Notwithstanding, there are features in the programme that are particularly distinctive, considering the current world practices in this field. One of the relevant aspects of the programme is the full implementation of the radiation protection system of dose limitation; this feature has already been discussed in the bibliography.[1,2] Another distinctive feature of the programme is the regulatory use of probabilistic safety analysis in nuclear power plants. This paper is aimed at briefly summarizing the latter feature.

2. BACKGROUND

Probabilistic safety assessments were first performed by the Argentine authority for the evaluation of some engineering safety features of the Atucha I Nuclear Power Plant, at the beginning of the seventies. Although neither probabilistic safety goals nor specific probabilistic regulations were established at that time, probabilistic assessments were performed for analyzing some safety systems of the plant. The assessments were intended to detect possible weak points in the safety structure of the plant, rather than to ensure compliance with a given relevant regulation.

At the same time, local authors published suggestions on the use of probabilistic criteria for overall nuclear safety assessments and with the purpose of

licensing nuclear power plants. A proposal for a new safety criterion, based on a probabilistic approach and on the underlying philosophy of the dose limitation system used for radiation protection purposes, was presented at that time.[3]

The basic proposal was to use the available probabilistic tools, such as event and fault trees, for an a-priori overall safety analysis of the nuclear power plant. A comparison could, therefore, be performed between the probability of occurrence of a hypothetical chain of events leading to an unexpected human exposure, along with its consequences -in terms of doses incurred-, and a probabilistic regulatory criterion. The licensing authority would then be able to judge the safety level of the plant on the basis of a rational approach.

Contemporaneously with these local efforts, safety studies of light-water reactors, based on probabilistic methods, were published elsewhere.[4,5] These resulted, however, in a-posteriori assessments, intended to show that an already-built reactor would be sufficiently "safe" if compared with other sources of harm to the public. These studies were not regulatory-oriented, nor were they intended to feedback the reactor design with the purpose of increasing its safety level up to a given standard. Moreover, the value judgement on the study result was made from the current experience on conventional safety and sources of harm rather than from the reference framework provided by the radiation protection practice.

It should be emphasized that the proposals for using probabilistic safety criteria in Argentina were never aimed at performing the above type of "confirmatory" studies. Rather, their aim was encouraging the use of criteria liable to ensure a-priori the level of safety of the reactors by enforcing mandatory probabilistic safety objectives, derived from the system of dose limitation used for radiation protection purposes, and by obliging the license applicants to perform probabilistic safety analyses of the plant and confirm that those objectives were met.

The structure of the Argentine nuclear Programme facilitated the use of the suggested safety approach. The Programme is based on natural-uranium, heavy-water reactors, some of which were quasi prototypes at the time the decision of their construction was made. Since the reactors are not, in practice, fully designed when the licensing application is submitted to the authorities, feedbacking the design with the results of an a-priori probabilistic analysis is a feasible action in which both, the applicant and the regulatory authority, are interested. Unfortunately, this is not the regular case with world-spread reactors (e.g., PWR or BWR), in which the basic conceptual design usually reaches a frozen status before their licensing application is submitted, and introducing major changes in both, the reliability and the redundancy of systems, is difficult.

3. INDIVIDUAL-RELATED PROBABILISTIC SAFETY CRITERION

The Argentine authorities issued a probabilistic safety criterion as Norm Number 3.1.3., "Criterios radiologicos relativos a accidentes" (Radiological criteria in relation to accidents)[6] and further clarified it by issuing Norm Number 3.2.2., "Analisis de fallas para la evaluacion de riesgos" (Failure analysis for risk evaluation)[7] The main features of these norms are the following:

i) The applicant for a nuclear power plant license shall identify the failure sequences which, in case of occurrence, will deliver a radiation dose to members of the public.

ii) The probability of occurrence of each failure sequence, as well as the corresponding activity of released radionuclides, shall be assessed by using event and fault trees, while taking into account the following criteria:

- The failure analysis shall systematically encompass all foreseeable failures and failure sequences, including the common-mode failures, the failure combinations and the situations exceeding the design basis. (Failure in this context means an alleatory event preventing a component from performing its safety function, as well as any other event which may additionally occur as a necessary consequence of such defficiency. Failure sequence, on the other hand, means a sequential series of failures which can, although not necessarily, occur after an iniciating event.)

- A failure or a failure sequence may be selected as representative of a group of failures or of failure sequences. In such a case, the failure or failure sequence to be selected from the group shall be that delivering the worst consequences and the analysis shall take into account the sum of the probabilities of the failure or failure sequences in the group.

- The analysis shall consider that a protection function may have lost operativeness either before the occurrence of the failure or of the failure sequence or as a result of such occurrence.

- The analyses of failures, of failure sequences or of any part thereof shall be based on experimental data as far as it is possible. If this cannot be done, the valuation methods must be validated through appropriate tests.

- The levels of failure rate assigned to the safe-related components, in the evaluation of the failure probability of systems, shall be justified. In case that justifiable values were not available for some of the components, the applicant shall use levels of failure rate prescribed by the licensing authority. If a given failure rate is justified on the basis of quality assurance, this must be specified in detail.

- The failure analyses shall consider the maintenance and testing procedures, and the time interval between successive maintenance and testing actions.

- A failure rate postulated for human actions shall be justified taking into account the complexity of the task, the stress involved and any other factors which might influence that failure rate.

iii) The doses on the critical group, that would result from the release of radionuclides due to a failure or failure sequence, shall be assessed by accepted methods. (For the purpose of the norm, the critical group is defined as a group of people, neighbour to the nuclear power plant, sufficiently homogeneous with regard to the doses expected to be incurred, and representative of the most exposed individuals in case of an accident.) The assessment shall take into account the meteorological conditions of dispersion at the site and their probabilities. The assessment shall not take into account the eventual application of countermeasures, even if they are forecasted in emergency planning.

iv) The annual probability of occurrence of any failure sequence, if plotted as a function of the resulting effective dose equivalent assessed as indicated above, shall result in a point located in the acceptable area of Figure 1. (The boundary between acceptable and non-acceptable areas in Figure 1 is a criterion curve which is discussed hereinafter.)

The implicit basic safety goal of the above mentioned norms is a risk limit derived from the dose limitation system used for radiation protection purposes (the term risk is used in this paper to mean the probability of occurrence of an event and <u>not</u> the mathematical product of such probability times the consequences resulting from the event; in the context of this paper the individual risk is the probability that a given individual will incur a deletereous effect from radiation). This

system, recommended by the International Commission of Radiological Protection (ICRP) [8], is widely used by almost all national authorities and international agencies.[9] The system includes three major requirements: two of them are source-related (v.g., justification of any practice involving radiation exposure and optimization of the related radiation protection) and the other is individual-related (v.g., the limitation of the highest dose that the most exposed individual may incur). The latter implies that the risk level due to the individual radiation exposure from all sources should be low enough as to be automatically disregarded. Using the ICRP risk factor of approximately 10^{-2} Sv^{-1}, the current recommended dose limit of 1 mSv per year[8,9] implies an annual risk limit of 10^{-5} for any individual, even for the highest exposed one, as a result of performing all practices involving radiation exposure.

Since the dose limits relate to individuals, appropriate upper bounds for individual doses should be selected for each source of exposure. The dose upper bound must be sufficiently lower than the relevant dose limit, so as to prevent individual exposure due to several sources from exceeding such limit. Different upper bounds have been used for nuclear power plants in various countries by the local competent authorities. In Argentina, a regulation controlling the release of radioactive effluents from nuclear power plants establishes a dose upper bound of 0.3 mSv per year [10] (Optimization of radiation protection is an additional mandatory requirement in the Argentine regulations, so that -in practical cases- the actual highest individual dose has resulted to be far lower than the upper bound). Therefore, the de-facto annual limit of individual risk due to radiation exposure from nuclear power plant operations accepted by the Argentine authority became 0.3 10^{-5}.

On the basis of the above limit and taking into account the uncertainties usually involved in probabilistic safety assessments, the Argentine authority has estimated that an annual risk limit for accidental exposures from nuclear power plants of the order of 10^{-6} would be consistent with the philosophy involved in the currently enforced system of dose limitation. This limit came to be the safety goal for probabilistic safety analysis of nuclear power plants in Argentina.

Accidental exposures may arise from a theoretically infinite number of accidental sequences, each one having a given probability of occurrence and delivering a given expected dose to the most exposed individual. The actual risk incurred by this individual will then result from the integration of the tail distribution of doses (i.e., the complement of the probability function of doses) times the probability of death provided the dose is incurred. The safety objective should therefore be that the value of this integral be lower than the annual risk limit; i.e., lower than 10^{-6} $annum^{-1}$.

The assessment of all possible accidental sequences is extremely difficult and practically impossible. Therefore, the Argentine authority is satisfied if only a ten of the relevant sequences is identified, and has assigned them an annual risk limit of 10^{-7}. Since each sequence may result in different doses, a criterion curve was adopted, which is a relationship between the annual probability of sequence occurrence and the expected individual dose, each point of the curve representing a constant level of risk. The criterion curve enforced by the Argentine authority is shown in Figure 1.

Failure of a point to be under the criterion curve does not necessarily mean that the risk limit is not met. In fact, even in this case, the integral of the tail distribution could be lower than 10^{-6} $annum^{-1}$.

The logics behind the criterion curve is as follows. For the range of doses from which only stochastic effects of radiation can be incurred, the criterion curve must show a constant, negative, 45° slope in a -log annual probability versus log individual dose- coordinate axis plane. This would ensure that the annual probabi-

lity of incurring the dose times the probability of death provided the dose is incurred (the latter being in the order of 10^{-2} per sievert) will be kept constant. One of the coordinate points in this part of the curve would obviously be the following: {Annual probability = 10^{-5} annum^{-1}; Individual dose = 1 Sv}, because the product 10^{-5} annum^{-1} 1 Sv 10^{-2} Sv^{-1} results in an annual risk of 10^{-7} annum^{-1}, which is the safety goal. In the dose range where non-stochastic effects of radiation may occur (i.e., for individual doses higher than 1 Sv), the slope of the curve should increase, in order to take account of the higher risks of death at these levels of dose. For doses higher than a few sievert (say, approximately 6 Sv), the probability of death approaches unity. From this level to higher doses, the criterion curve should remain constant at an annual probability of 10^{-7} (because the exposed individual would inevitably die regardless the level of the dose). Between the coordinate points defined by {Annual probability = 10^{-5} annum^{-1}; Individual dose = 1 Sv} and {Annual probability 10^{-7} annum^{-1}; Individual dose = 6 Sv}, the criterion curve should show a shape similar to that of the relationship between the individual dose and the frequency of death (which, at that range, is S-shaped). However, for the sake of simplification, the authority has decided to approximate these two points by means of a linear-shaped relationship. Finally, the criterion curve has been truncated at an annual probability level of 10^{-2}, because the occurrence of incidents having a higher annual probability (regardless the dose) is unacceptable for the authority.

It should be emphasized that the Argentine Norm 3.1.3. is individual-related; i.e., it is intended to limit the risk-rate on the individual incurring the highest risk, but does not take into account the overall expected impact from accidental situations in the nuclear power plant. This problem will be further discussed later in this paper (see point 5).

The regulatory use of probabilistic analysis in nuclear reactor safety has been criticized on various grounds, among them on that of the potential lack of reliable statistical data for assessing probabilities. When statistical data are not available and cannot be extrapolated, the Argentine authority is using the concept of probability as one of subjective probability (or degree of believe) provided by "engineering judgement", rather than as a classical game of chance or as a frequency probability, provided that, in any case, the assessment complies with the requirement of coherence.[11] The probabilities used for the safety assessment would therefore not require symetry (i.e., the condition of existence of identical entities) nor the empirical experience giving a frequency estimate. As a matter of fact, these two requirements may not exist in practice. Nevertheless, for the purpose of decision-making, it is legitimate to rely upon subjective probabilities depending on the experience and knowledge of those who make the estimate.[12]

4. THE REGULATORY USE OF THE PROBABILISTIC SAFETY CRITERION

The probabilistic safety criterion is being regulatorily used in Argentina for the first time in the licensing process of the Atucha II Nuclear Power Plant. Atucha II will be equipped with a pressure vessel reactor, fueled with natural uranium and cooled and moderated by heavy water. Although the reactor is based on the Atucha I concept, its power would double that of Atucha I and reach a level of 747 MW(e). The basic engineering of the reactor, therefore, is not identical to that of Atucha I and was not definitely frozen when the the reactor was shown to be feasible.[13]

After consultation with the regulatory authority, the local responsible organization (i.e., the organization having overall responsibility of Atucha II[14] decided to include a clause requiring compliance with the probabilistic safety criterion in the contract with the supplier of Atucha II.[15] The supplier is contractually obliged to perform an appropriate risk analysis and responsible for accomodating the design of the reactor, feedbacking the result of the analysis, in order to meet the probabilistic safety goals.

A preliminary risk analysis was already prepared by the supplier and submitted by the applicant to the authority as a part of the preliminary safety analysis report of the plant.[16] The results were encouraging enough to ensure the release of the plant construction permit. The original predesign of the plant has already been modified as a result of the analysis, and some engineering safety features are still being improved.

Accidental sequences, or "categories of releases", have been preliminary selected by the applicant, in consultation with the authority, and are the following: (1) Core meltdown followed by steam explosion; (2) core meltdown and large leak in containment; (3) core meltdown and meium leak in containment; (4) core meltdown and small leak in containment; (5) core meltdown, overpressure failures, and failed filter system; (6) core meltdown and overpressure failure; (7) design basis loss-of-coolant accident, large leak in the containment; and, (8) design basis loss-of-coolant accident.[16]

The annual probabilities of occurrence of the various failure sequences and the expected releases of radioactive materials were assessed following the requirements of the relevant norms (see Table I[16]). Also, the probabilities of incurring a dose, given a release, were determined taking into account the expected dispersion for different Pasquill's conditions and their chances of occurrence. Finally, both probabilities were appropriately combined.

After several attempts and successive design feedbacking, the latest result of the risk analysis was attained and is shown here in Figure 2.[16] The figure clearly shows that the accidental sequences (6) and (7) are the most compromised ones and, under Pasquill's condition (F-G), they lie on the criterion curve. The figure also shows that, as it could be expected, the plant is overdesigned for the so-called "design basis loss-of-coolant accident".

Currently, the analysis is being consolidated as the design of the plant is being finished. Improvements in the reliability and redundancy of components and systems are being introduced so that the points can lie in the region of acceptability, sufficiently far from the criterion curve. So, a definitive risk analysis is being performed on a continuous basis under the authority's surveillance. It should be finished and submitted to the authority before the plant is authorized to operate. The final analysis shall demonstrate that the plant meets the probabilistic safety criterion.

5. A COMPLEMENTARY PROBABILISTIC CRITERION. THE LIMITATION OF THE MATHEMATICAL EXPECTATION OF HARM FROM THE SOURCE

The probabilistic safety criterion presented before assures a level of safety which is sufficient to ensure that an individual risk limit, compatible with the philosophy of the dose limitation system, will not be exceeded. It fails, however, to answer positively the old question of the safety engineers; v.g., is such safety level safe enough as to preclude further safety improvements? A nuclear power plant complying with the criterion would be licenciable, both if it is sited in a desertic region, where it would impose risks (lower than the "acceptable" one) to few individuals, and if it is sited in a densely populated area where many individuals would incur such risks. If an accident does occur, however, the overall radiological impact will be very different in each case, suggesting that the safety level might be lower in the second than in the first one. Further safety improvements would be necessary in the second case if an equal expected impact is required. But, is this equalization really necessary, providing the individual-related criterion is met? and, if so, on what basis can the equalization be determined? The answers to these questions will allow for complementing the probabilisitc criterion based on individual risk considerations alone.

After the ICRP recommended the use of the concept of detriment to quantify the impact from a source of radiation exposure, there was a temptation to use a similar concept for measuring the expected impact from accidental exposures. [3,17,18] The detriment is an extensive quantity introduced by the ICRP to quantify the combined impact of deleterous effects resulting from exposure to a given radiation source. [19] It is defined as the expectation of the harm to be incurred, taking into account the expected frequency and severity of each type of deletereous effect. The detriment incurred by one individual receiving a dose in the range of stochastic effects is proportional to the effective dose equivalent incurred; the proportionality factor being the probability that the individual will incur a deleterous effect as a result of the exposure. Therefore, in cases of actual exposures to low levels of dose, the total detriment is proportional to the sum of all individual effective dose equivalents incurred, i.e., is proportional to the collective dose commitment (this latter quantity results from the time integration of the collective dose rate, which, in turn, results from the integral of the population spectrum in terms of effective dose-equivalent rate incurred).

For potential exposures, the concept of detriment should keep its theoretical meaning although it would become a quantity of a second order of stochasticity. In such case, the probability of a given exposure, i.e., the combined probabilities of both, an accidental release and an environmental condition (dispersion, deposition), should be introduced in the formulation, and integrated over all possibilities. Then, if low doses were expected, the detriment should be proportional to the resulting mathematical expectation of the collective dose commitment. For higher doses, another component of the detriment should be added in order to take into account the non-stochastic effects of radiation.

The idea of using the detriment of a second order of stochasticity, and the related mathematical expectation of collective dose commitment, for quantifying the impact from accidental exposures is really appealing. The concept would allow for optimizing safety[17,18], increasing it to a sufficiently high level that further improvement would not be worthwhile taking into account both, the benefits achieved in terms of expected collective dose commitment reduction and the cost of obtaining such reduction. However, it has been demonstrated[12] that, at very low probabilities, the detriment will lose its usefulness as a basis for decision-making. In fact, in such cases the standard deviation of the result may be orders of magnitude higher than the actual expectation and the coefficient of variability would become very large. The detriment is then no longer a central measure of the distribution of harm and, in addition, the uncertainty of the detriment becomes too large to make it meaningful, even if the probability as such could be estimated by safety assessments with an accurate degree of certainty.

On the other hand, the use of the expected total impact, for safety optimization purposes, requires the assignment of a certain cost to the resulting detriment. This would be a very controversial issue. For the reasons stated above, if the postulated failure is of a stochastic nature and not very unlikely, the product of probability times the cost of the consequences could be used as a reasonable quantity in the optimization procedure. At very low failure probabilities, the inherent uncertainty of the product of probability and consequences makes the use of this quantity rather doubtful. In the general case, the value assigned should follow an utility function of probability and consequence. The utility function should probably give more weight to larger accidents than would be implied by the direct product probability times consequence.

If the use of the above mentioned utility functions were enforced, the safety of nuclear power plants could be further improved on a rational basis by optimizing the nuclear safety systems. This problem is being carefully studied by the Argentine authority. However, the authority has not yet issued any norm, criteria or rule on this matter.

CONCLUSION

The use of probabilistic safety analysis in the regulatory process of licensing nuclear power plants is a reality in the Argentine nuclear power programme. The approach has shown to be feasible and practical. Furthermore, it allows for a rationalization of the regulatory decisions on the safety level of the plant.

For judging the acceptability of the analysis result, the Argentine authority had to enforce a regulatory probabilistic safety criterion, which is based on a limitation of individual risks. This criterion is consistent with the philosophy of the dose limitation system used for radiation protection purposes and therefore allows for an equalized measure of the radiological risk on individuals resulting from the generation of nuclear energy.

The criterion presented, however, fails to take into account the expected overall radiological impact from the plant. Whether or not this complementation needs to be introduced and in what way this should be done are matters under current debate, and no firm conclusion on this point can be given yet.

REFERENCES

1) D.J. BENINSON and A.J. GONZALEZ, "Application of the dose limitation System to the control of releases of Carbon-14 from heavy water moderated reactors" In International Symposium on the Application of the Dose Limitation System in Nuclear Fuel Cycle Facilities and other Radiation Practices organized by IAEA, WHO, OECD/NEA, ICRP. Madrid, Oct. 19-23, 1981. 20 p. IAEA-SM-258/53.

2) D.J. BENINSON, "Application of the dose limitation system to design". In International Conference on Nuclear Power Experience. Vienna, Sep. 13-17, 1982. IAEA CN-42/87 (in press)

3) A.J. GONZALEZ, "Un criterio para la evaluacion de la seguridad nuclear". In Proceedings of a Symposium on Siting of nuclear facilities, jointly organized by the International Atomic Energy Agency and the OECD Nuclear Energy Agency. Vien na, Dec. 9-13, 1974. p. 265-281. IAEA-SM-188/52. STI/PUB/384.

4) GESELLSCHAFT FUR REAKTORSICHERHEIT, "German risk study - main report. A study of the risk due to accidents in nuclear power plants". A translation of phase A of the Deutsche Risiko studie Kernkraftwerke. A study sponsored by the Federal Ministry for Research and Technology. Palo Alto, California, Electric Power Research Institute, 1981. Technical editors Arthur W. Barsell and Ian B. Wall. EPRI NP-1804-SR.

5) NUCLEAR REGULATORY COMMISSION, Washington, DC, (USA). Office of Nuclear Regulatory Research. Probabilistic Analysis Branch. "Reactor Safety Study, an Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants" U.S., NRC, Oct. 1975. Main Report and 11 App. WASH-1400 (NUREG 75/014) . PB-248.201 to 248.209

6) COMISION NACIONAL DE ENERGIA ATOMICA, Buenos Aires. (Argentina). Consejo Asesor para el Licenciamiento de Instalaciones Nucleares. "Criterios radiologicos relativos a accidentes". Buenos Aires, CNEA, 1979. 2 p. NORMA CALIN N° 3.1.3.

7) COMISION NACIONAL DE ENERGIA ATOMICA, Buenos Aires. (Argentina). Consejo Asesor para el Licenciamiento de Instalaciones Nucleares. "Analisis de fallas para la evaluacion de riesgos". Buenos Aires, CNEA, 1980. 1 p. NORMA CALIN N° 3.2.2.

8) INTERNATIONAL COMMISSION ON RADIOLOGICAL PROTECTION, "Recommendations of the International Commission on Radiological Protection. Adopted January 17, 1977".

ICRP Publication 26. Oxford, Pergamon Press, 1977. 53 p. Annals of the ICRP. v.1: N°3, 1977.

9) INTERNATIONAL ATOMIC ENERGY AGENCY, Vienna (Austria). "Normas Basicas de seguridad en materia de proteccion radiologica". Informe de un grupo asesor patrocinado conjuntamente por OIEA/OMS/OIT/AEN. Aprobado por GOV/2044 - 28 Jul. 1981. (in press).

10) COMISION NACIONAL DE ENERGIA ATOMICA, Buenos Aires. (Argentina) Consejo Asesor para el Licenciamiento de Instalaciones Nucleares. "Limitacion de efluentes radiactivos" Buenos Aires, CNEA, 1974. 2 p. NORMA CALIN N° 3.1.2.

11) G. APOSTOLAKIS, "Probability and risk assessment: The subjectivistic viewpoint and some suggestions". Nuclear Safety v. 19: 305-315, 1978, N° 3.

12) D.J. BENINSON and B. LINDELL, "Critical views on the application of some methods for evaluation of accidents probabilities and consequences." In Proceedings of an International Conference on Current Nuclear Power Plants Safety Issues organized by the International Atomic Energy Agency. Stockholm, Oct. 20-24, 1980. Vienna, IAEA, 1981. Vol. 2, p. 325-341 IAEA-CN-39/4. STI/PUB/566.

13) KRAFTWERK UNION AG, "Feasibility study for Comision Nacional de Energia Atomica, Buenos Aires, Argentina". Development of a D_2O - Reactor System for a Nuclear Power Plant in the range of 350 to 600 MWe based on the Reference Plant Atucha I. Jul. 1978. 4 vol.

14) INTERNATIONAL ATOMIC ENERGY AGENCY, Vienna (Austria) "Design for safety of nuclear Power Plants. A Code of Practice" Vienna, IAEA, 1978. Safety Series N° 50-C-D. 43 p. STI/PUB/516. "Governmental Organization for the regulation of Nuclear Power Plants. A code of practice". Vienna, IAEA, 1978. Safety Series N° 50-C-G. 43 p. STI/PUB/502.

15) ARGENTINA, Decreto N° 1337, 8-7-1980. "Se aprueban diversos contratos suscriptos entre CNEA y una empresa extranjera KWU para la construccion de la Central Nuclear Atucha II". Contrato de Suministros. Contrato de Servicios. Contrato de Garantia. Acuerdo de Accionistas. In Boletin Oficial. 23 Jul. 1980.

16) COMISION NACIONAL DE ENERGIA ATOMICA, Buenos Aires. (Argentina) Direccion de Centrales Nucleares. "Nuclear Power Plant. Atucha II. Preliminary safety analysis, Report." 1981. 11 vol.

17) A.J. GONZALEZ, "Criterios de optimizacion para los sistemas de Instrumentacion y control de centrales nucleares". In: IAEA-IWG/NPPCI Specialists' Meeting on The Effect of Regulatory Requirements on Nuclear Power Plant Control and Instrumentation Systems. Madrid, Oct. 4-6, 1977. Buenos Aires, CNEA, 1977. 23 p. CNEA-NT 28/77.

18) D.J. BENINSON and A.J. GONZALEZ, "Optimization of Nuclear Safety Systems". In Proceedings of an International Conference on Current Nuclear Power Plants Safety Issues organized by the International Atomic Energy Agency. Stockholm, Oct. 20-24, 1980. Vienna, IAEA, 1981. Vol. 2, p.449-456. IAEA-CN39/211 STI/PUB/566

19) INTERNATIONAL COMMISSION ON RADIOLOGICAL PROTECTION, "Cost-benefit analysis in the optimization of radiation protection." Adopted by the Commission in June 1982. (in press).

TABLE I - ACCIDENTAL SEQUENCES (CATEGORIES OF RELEASES) FOR ATUCHA II NPP

Release category No.	Description	Time of release h	Duration of release h	Release height m	Energy release 10^6 KJ/a	Frequency**) of release 1/a	Fraction of core inventory released							
							Xe-Kr	J_{org}	J_2-Br	Cs-Rb	Te-Sb	Ba-Sr	Ru	La
1	Core meltdown followed by steam explosion	1	1	30	540	$2\cdot10^{-6}$	1.0	$7.0\cdot10^{-3}$	$7.9\cdot10^{-1}$	$5.0\cdot10^{-1}$	$3.5\cdot10^{-1}$	$6.7\cdot10^{-2}$	$3.8\cdot10^{-1}$	$2.6\cdot10^{-3}$
2	Core meltdown, large leak in containment (ϕ 300 mm)	1	3	10	15	$6\cdot10^{-7}$	1.0	$7.0\cdot10^{-3}$	$4.0\cdot10^{-1}$	$2.9\cdot10^{-1}$	$1.9\cdot10^{-1}$	$3.2\cdot10^{-2}$	$1.7\cdot10^{-2}$	$2.6\cdot10^{-3}$
3	Core meltdown, medium leak in containment (ϕ 80 mm)	2	3	10	1	$6\cdot10^{-7}$	1.0	$7.0\cdot10^{-3}$	$6.3\cdot10^{-2}$	$4.4\cdot10^{-2}$	$4.0\cdot10^{-2}$	$4.9\cdot10^{-3}$	$3.3\cdot10^{-3}$	$5.2\cdot10^{-4}$
4	Core meltdown, small leak in containment (ϕ 25 mm)	2	3	10	–	$3\cdot10^{-6}$	1.0	$7.0\cdot10^{-3}$	$1.5\cdot10^{-2}$	$5.1\cdot10^{-3}$	$5.0\cdot10^{-3}$	$5.7\cdot10^{-4}$	$4.0\cdot10^{-4}$	$6.5\cdot10^{-5}$
5 *)	Core meltdown, overpressure failure, failed filter system	0 1 25	1 1 1	10 10 10	– – 200	$2\cdot10^{-5}$	$2.0\cdot10^{-5}$ $2.3\cdot10^{-2}$ $9.8\cdot10^{-1}$	$1.8\cdot10^{-7}$ $1.6\cdot10^{-4}$ $6.8\cdot10^{-3}$	$1.8\cdot10^{-7}$ $9.6\cdot10^{-4}$ $9.6\cdot10^{-3}$	$4.7\cdot10^{-5}$ $6.7\cdot10^{-4}$ $4.5\cdot10^{-4}$	$3.6\cdot10^{-7}$ $6.7\cdot10^{-4}$ $7.7\cdot10^{-4}$	$5.5\cdot10^{-9}$ $8.0\cdot10^{-5}$ $4.7\cdot10^{-5}$	– $5.5\cdot10^{-5}$ $5.3\cdot10^{-5}$	– $8.8\cdot10^{-6}$ $9.5\cdot10^{-6}$
6 *)	Core meltdown, overpressure failure	0 1 25	1 1 1	150 100 10	– – 200	$7\cdot10^{-5}$	$2.0\cdot10^{-5}$ $2.3\cdot10^{-2}$ $9.8\cdot10^{-1}$	$1.8\cdot10^{-9}$ $1.6\cdot10^{-4}$ $6.8\cdot10^{-3}$	$1.8\cdot10^{-8}$ $9.6\cdot10^{-7}$ $9.6\cdot10^{-3}$	$4.7\cdot10^{-8}$ $6.7\cdot10^{-7}$ $4.5\cdot10^{-4}$	$3.6\cdot10^{-10}$ $6.7\cdot10^{-7}$ $7.7\cdot10^{-4}$	$5.5\cdot10^{-12}$ $8.0\cdot10^{-8}$ $4.7\cdot10^{-5}$	– $5.5\cdot10^{-8}$ $5.3\cdot10^{-5}$	– $8.8\cdot10^{-9}$ $9.5\cdot10^{-6}$
7	Design basis loss-of-coolant accident, large leak in the containment	0	1	10	9	$1\cdot10^{-4}$	$1.7\cdot10^{-2}$	$3.7\cdot10^{-5}$	$5.3\cdot10^{-3}$	$1.3\cdot10^{-2}$	$2.5\cdot10^{-5}$	$2.5\cdot10^{-7}$	0.	0.
8	Design basis loss-of-coolant accident	0	6	100	–	$1\cdot10^{-3}$	$4.6\cdot10^{-4}$	$1.0\cdot10^{-3}$	$1.2\cdot10^{-8}$	$2.1\cdot10^{-8}$	$4.1\cdot10^{-11}$	$4.1\cdot10^{-13}$	0.	0.

*) The released fractions of activity are specified for three intervals of time, because the release extends over a longer period of time.

**) Probabilities are calculated including 10 % contributions from adjacent release categories

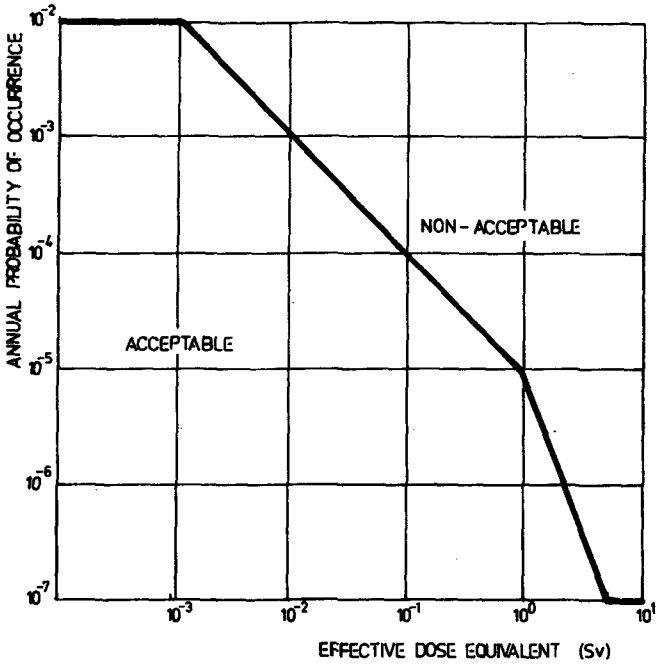


Fig. 1. Criterion Curve.

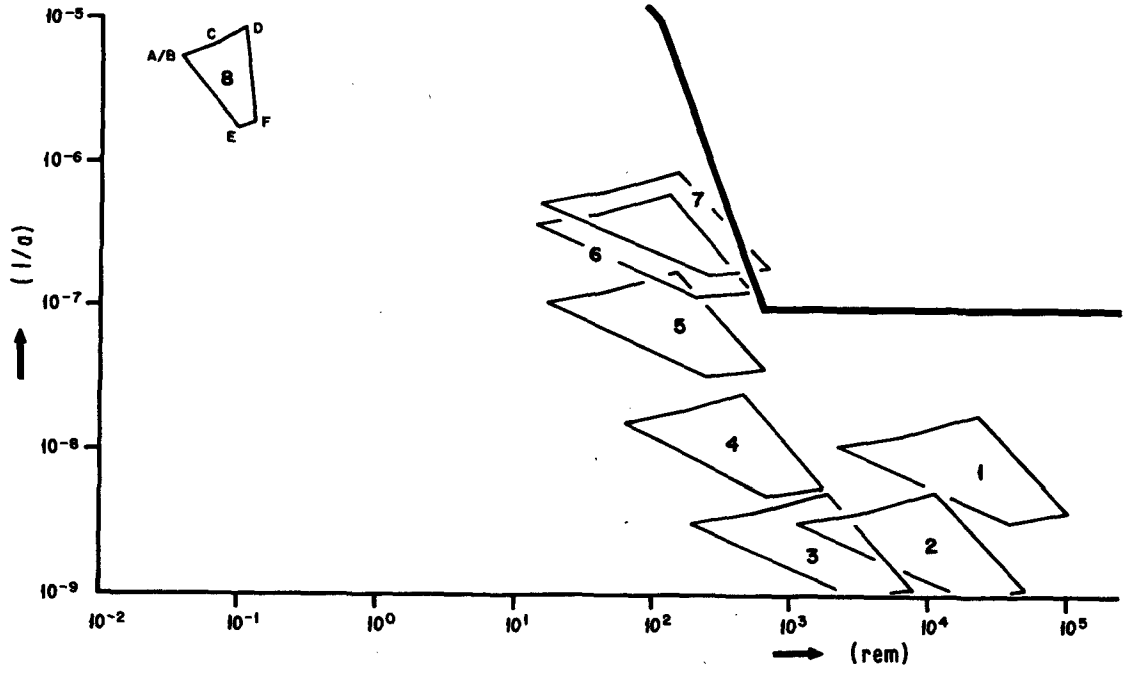


Fig. 2.

SESSION 3

RADIOLOGICAL SOURCE TERMS - 1

Chair: C. Devillers *(CEA)*
J. Griffith *(DOE)*

EFFECT OF CORE CHEMISTRY ON FISSION PRODUCT RELEASE

S. W. Tam, P. E. Blackburn, and C. E. Johnson

Argonne National Laboratory
Argonne, Illinois 60439, U.S.A.

ABSTRACT

To obtain reliable estimates of volatile fission-product release from oxide fuels for various accident conditions, an accurate description of the internal fuel-rod chemistry is required. Unlike release processes involving inert fission gases such as Xe and Kr, volatile fission products participate in strong chemical interactions with one another as well as with the UO_{2+x} fuel matrix. On the other hand, their release processes from oxide fuels are closely tied to those of the fission gases. Based on this knowledge, a model has been developed to describe the release rates and the chemical states of three volatile fission products (I, Cs, and Mo) released from oxide fuels as functions of operating temperature, burnup, and oxygen-to-metal ratio. The results are consistent with a wide range of data. The model is very flexible, easily applied, and can be readily extended to include a large number of volatile fission products.

INTRODUCTION

Fission product release during operation of a light water reactor (LWR) has been under active investigation for many years.[1] Extensive data related to noble fission-gas release have been accumulated,[2] and important advances have been made towards understanding and modeling the physical processes involved during both steady-state and transient conditions.[3,4,5] In contrast, comparable efforts made towards understanding the behavior of volatile fission products (such as Cs and I) are of relatively recent undertaking.[1] The experience of TMI-2 has indicated the importance of understanding the volatile fission product (VFP) release behavior.

The work reported here is concerned with deriving source terms for the volatile fission products, from which a model for estimating VFP release rates was developed. We believe that VFP release is governed by two factors. The first factor is the chemical interaction that occurs among fission products, between fission products and fuel, and between fission products and cladding and coolant. These interactions serve to reduce the thermodynamic activity of a given fission product, thus limiting its release. For the chemical interactions, local equilibrium was assumed to exist so that the compounds and their concentrations could be calculated from thermodynamic considerations. The second factor is the migratory processes of the fission gases (Xe and Kr), which transport the volatile fission products and their compounds through the fuel. Our model takes into account core chemistry as well as thermal transport of the volatile fission product.

INTERNAL FUEL CHEMISTRY

For the chemically active fission products, the formation of chemical compounds vastly complicates the model development. In particular, unlike the case of noble gas release, the oxygen potential of the fuel is a crucial factor.

In its present stage of development, the model focuses on the fission products Cs, I, and Mo in the UO_{2+x} fuel matrix. The following equilibria have been considered:

$$Cs(g) + I(g) \rightarrow CsI(g) \quad (1)$$

$$CsI(g) \rightarrow CsI(l) \quad (2)$$

$$2I(g) \rightarrow I_2(g) \quad (3)$$

$$2Cs(g) + UO_2 + O_2 \rightarrow Cs_2UO_4(c) \quad (4)$$

$$2Cs(g) + Mo + 2O_2 \rightarrow Cs_2MoO_4(c) \quad (5)$$

$$Cs_2MoO_4(c) \rightarrow Cs_2MoO_4(g) \quad (6)$$

The resulting equations are:

$$a_{Cs}a_I = \frac{1}{K_1} a_{CsI(g)} \quad (7)$$

$$a_{CsI(g)} = \frac{1}{K_2} a_{CsI(l)} \quad (8)$$

$$a^2_{I(g)} = \frac{1}{K_3} a_{I_2(g)} \quad (9)$$

$$a^2_{Cs}a_{UO_2}P_{O_2} = \frac{1}{K_4} a_{Cs_2UO_4(c)} \quad (10)$$

$$a^2_{Cs}a_{Mo}P^2_{O_2} = \frac{1}{K_5} a_{Cs_2MoO_4(c)} \quad (11)$$

$$a_{Cs_2MoO_4(c)} = \frac{1}{K_6} a_{Cs_2MoO_4(g)} \quad (12)$$

where a_i = activity of the ith species, K_j = equilibrium constant for the jth reaction, and P_{O_2} = oxygen pressure.

All condensed-phase activities are assumed to be of unit activity except that for the condensed phase of Mo, which is assumed to be an alloy phase containing Mo, Tc, Ru, Rh, and Pd. The vapor phase above each condensed phase is assumed to possess ideal gas behavior. The oxygen pressure, P_{O_2}, is derived from the Blackburn model.[6] The following mass balance equations describe the condition for release of Cs, Mo, and I:

$$Cs + CsI(l) + CsI(g) + 2(Cs_2UO_4 + Cs_2MoO_4) = 0.1882\ BU \quad (12)$$

$$Mo + Cs_2MoO_4 = 0.2348\ BU \quad (13)$$

$$CsI(l) + CsI(g) + I + 2I_2 = 0.011\ BU \quad (14)$$

The total amount of Cs, Mo, and I generated depends upon burnup (BU).

The effective oxygen-to-metal (O/M) ratio used in the P_{O_2} calculation is based on the following consideration. The O/M ratio changes during fission because uranium is lost and a fraction of the available oxygen is consumed in forming stable oxides of the rare earths, Y, Sr, Ba, Zr, and Nb. Since these oxides are much more stable [7] than the compounds given in Eqs. (1-6), they were not included when we estimated the effective O/M ratio through mass-balance considerations. No separate equilibria are invoked.

The choice of the compounds given in Eqs. (1-6) was guided by WASH-1400 [8] and relevant core chemistry. Expansion of the present model to include other fission products (Te, Ba, and Ru [8]) should further illustrate the effect of core chemistry on fission product behavior. The choice of compounds will be guided by stability considerations.

A number of calculations with the model have been performed over a wide temperature range at different levels of burnup and starting O/M ratios (i.e., temperatures from 1000-3000°C, burnups from 0-3%, and stoichiometry changes from 0.0 to 0.1). The analysis predicts that, within the irradiated fuel, the dominant chemical form of iodine is CsI in both the condensed and vapor form. This is consistent with the observation that during the TMI-2 accident only a very small fraction of the iodine inventory was released into the environment.

In this study, we examined the VFP release rates rather than vapor pressures because the VFP release rates are crucial in any analysis of reactor safety. The scaling model, given below, is formulated to relate the fuel chemistry to the VFP release rates.

SCALING MODEL

We shall now examine the effect of internal fuel chemistry on the release of various volatile fission products from LWR fuels. To this end, we have developed a scaling model that predicts VFP release rates which depend upon the internal fuel chemistry. The basic thesis of this model is that the VFP release rates correlate with the Xe and Kr release rates. The precise forms of the correlation (or scaling factors) are obtained from the fuel chemistry discussed previously.

To appreciate the physical basis of the scaling model, one needs some understanding of the microscopic processes through which both the fission gases and the volatile fission products are released from LWR fuels. Within the last decade, intensive experimental and theoretical efforts have been undertaken towards understanding fission gas release. The fission gas atoms, within the grain interior, arrive at the grain boundary via several processes.[2-5] They are:

1. Atomic Migration: The Xe and Kr atoms migrate individually towards the grain boundary. External driving forces such as a temperature gradient may also be operating.

2. Bubble Migration: The low solubility of the noble gas atoms in the ceramic fuels leads to bubble formation. These bubbles move towards the grain boundary via mechanisms such as surface diffusion and ledge/step nucleation.

3. Grain Boundary Sweeping: At high temperatures, sintering and grain growth processes take place. The fission gases, in atomistic form or within bubbles, will be swept onto the expanding grain surfaces by the moving grain boundary.

Conflicting points of view [5] have been presented on the relative importance of the above processes in contributing to the arrival rate of the gas atoms at the grain boundary. There are, in fact, uncertainties concerning even some of the individual processes themselves. However, the general validity of the scaling model is independent of the mechanism through which fission gas atoms migrate to the grain boundary. The scaling model is valid as long as the average arrival time, t_{VFP}, of the VFP atoms onto the grain boundary is comparable or smaller than the corresponding average arrival time for the fission gas, t_{FG}.

The mechanism through which VFP atoms arrive at the grain boundary is similar to that of the fission gas. They may (1) migrate as individual atoms, (2) be swept up by the fission gas bubbles on their way to the grain boundary, or (3) be picked up via grain boundary sweeping. For the last two processes, t_{VFP} is the same as t_{FG}. In the case of the first process, the relative mobility of both the VFP and fission-gas atoms depends on their respective atomic diffusion coefficients. Although the mechanism for Xe and Kr diffusion is not rigorously known, available evidence suggests the possibility that Xe and Kr diffuse via association of higher-order vacancy complexes, which include a cation (e.g., U) vacancy.[3] It is known that, for materials of the fluorite structure (of which UO_2 is an example), the cation is the slowest diffuser.[10] Therefore, one would expect the following order-of-magnitude relationship to hold:

$$D_{Xe} \lesssim D_U \tag{14}$$

where D_{Xe} and D_U are the bulk Xe and U diffusion coefficients, respectively. This is consistent with experimental data over a wide temperature range.[11]

There is even less understanding on VFP atom diffusion within UO_2. However, if the VFP migration mechanism (e.g., substitutional, interstitial, defect complexes, etc.) does not involve the cation (i.e., U) defect, then it is reasonable to assume that the following approximate relations are true:

$$D_{VFP} \gtrsim D_U \gtrsim D_{Xe} \tag{15}$$

where D_{VFP} is the VFP atom diffusion coefficient. On the other hand, if the bulk diffusion mechanism for the VFP atom does involve the U defect (e.g., vacancy complexes similar to the one discussed above for the fission gas atoms), then one would have,

$$D_{VFP} \simeq D_{Xe} \tag{16}$$

Equations (15) and (16) can be condensed into one single estimate,

$$D_{VFP} \gtrsim D_{Xe} \tag{17}$$

Equation (17) is consistent with the most recent experimental data.[12] Thus, irrespective of the involvement or noninvolvement of a U defect in the VFP atom bulk migration, the t_{VFP} at grain boundaries is comparable or shorter than t_{FG}. This result, taken together with the previous discussion, leads to the conclusion that, regardless of whether the dominant transport mechanism is atomic migration, bubble migration, or grain boundary sweeping, t_{VFP} at the grain boundary is comparable or shorter than t_{FG}.

The most favorable sites where VFP compound formation can take place are the fission-gas bubble interior, bubble/UO_2 matrix interfaces, and grain boundaries. For these sites,the VFP compounds have an arrival time [t_{VFP} (compound)] which is comparable to t_{FG}. Where VFP compounds are formed "in place" (i.e., in the grain interior away from the above-mentioned favorable regions), they may still reach the grain boundary via fission-gas bubble sweeping and/or moving grain boundaries during grain growth. In these cases one would still have t_{VFP} (compound) $\lesssim t_{FG}$. To summarize, the average arrival time of the VFP (whether elemental or compound form) from the grain interior onto the grain boundary is roughly comparable or shorter than t_{FG}. The next stage is for the fission gas bubbles at the grain boundary to grow "in place" via absorption of the incoming fission gas flux from the grain interior. Similar situations also develop along the grain edges.

While the detailed dynamics of this development of grain-surface and grain-edge porosity are complex [4], the scaling model is independent of these details. It depends only on the fact that the fission gas bubbles at the grain face and grain edge grow and overlap. In time, this leads to the establishment of a network of open channels across the grain faces and along the grain edges, ultimately ending in some region in the fuel matrix. These regions are themselves connected to the fuel exterior via a tortuous but open path of interconnected pores and cracks. Through these open channels and pathways, the fission gases are transported to the fuel exterior via the relatively rapid process of gaseous diffusion. Given enough time at high temperature, sintering will close off these open pathways at various "choke" points and thereby reduce greatly this migration process. After that, the whole cycle will repeat itself.

The central thesis of the scaling model is that the volatile fission products (whether elemental or compound form) that have arrived onto the grain face through processes previously described will be transported to the fuel exterior via vapor diffusion along the same open channels and pathways established by the fission gases. Thus, the volatility of the VFP species is an important factor in determining their release rate from the fuel. Qualitatively, this is well supported by recent data.[1] Quantitatively, this is determined with the scaling model as follows.

The present analysis identifies two key physical facts. They are:

1. Several of the important migration mechanisms, as well as the actual physical-escape pathways from the fuel interior for the volatile fission products, are closely associated with the fission gases. This determines the mechanistic aspect of the VFP release processes. The VFP fractional release rate, μ_{VFP} (units of fraction of total inventory released per unit time), should then be approximately the same as the fission-gas fractional release rate, μ_{FG}. However, unlike the fission gases, the volatile fission products are not necessarily all in vapor form. (In this work, we have utilized the most-recent experimental "best estimate" [1] for μ_{FG} as a function of temperature.)

2. To obtain μ_{VFP}, one needs only to scale μ_{FG} with a scaling factor, α_{VFP}. This scaling vapor, α_{VFP}, takes into account the fact that only a fraction of a given VFP species, out of its total inventory, exists in vapor form and thus can participate in the release processes. In other words, within the scaling model, one has

$$\mu_{VFP} = \alpha_{VFP}\, \mu_{FG} \tag{18}$$

The scaling factor, α_{VFP}, reflects the effect of chemical interaction in a multi-component system and depends upon temperature, burn-up, and the O/M ratio in the fuel. It is easily obtained from the chemical model discussed previously. The effect of fuel chemistry on VFP release rates from reactor fuel is plainly illustrated by Eq. (18).

The advantages of the scaling model are twofold:

1. The impact of core chemistry on the release process is separately considered in the scaling factor, α_{VFP}. As a result, the model can incorporate, with minimal difficulty, the complex chemistry of a large number of volatile fission products (elements and compounds) in both vapor and condensed state. The present work serves to illustrate the power of this approach in relating core chemistry to the release process.

2. The physical aspects of the VFP release process are contained in μ_{FG}, the fractional fission-gas release rate. Within the scaling model, this quantity bears some similarity to the scaling length in various theories of localization and phase transition. In practice, μ_{FG} provides a pivotal link between fuel chemistry and release rates. Thus, the scaling model is in the best position to draw upon the significant theoretical understanding and the empirical data that have been accumulated.

RESULTS AND DISCUSSION

Figure 1 shows the fractional release rate of elemental iodine, μ_I (i.e., atomic plus molecular iodine), as a function of temperature. Note the extremely low release rate even at the high temperature regime (1800-2800°C) considered. For comparison, the empirical μ_{FG} taken from Ref. [1] is also shown. At 2000°C μ_I is five orders of magnitude below μ_{FG}. Even at 2800°C, these two rates still differ by 3-4 orders of magnitude. This illustrates a central point being emphasized in the present work. A volatile fission product (in this case iodine) can have a very low release rate if the fuel chemistry dictates that a large fraction of this fission product exists in some other stable, but less volatile, chemical form (in this case CsI). The results shown in Fig. 1 are consistent with the TMI data, which indicate that fission-gas radioactivity exiting the plant is orders of magnitude above that due to iodine.[1]

Comparison of the scaling-model predictions were made with data obtained by methods involving primarily nuclear rather than chemical species identification. The μ_{VFP} shown in Figs. (2-8) reflects a composite quantity that takes into consideration the volatile fission product in all its chemical forms. For example, the iodine fractional release rate, μ_I, in Fig. 2 denotes the sum of the elemental iodine and the CsI fractional release rates. The scaling-model results for μ_I show reasonable agreement with the data, which are considered to be accurate to within plus or minus an order of magnitude.[1] The figure indicates that above about 1300°-1400°C μ_I is practically the same as μ_{FG}. The reason is that, above 1300-1400°C, CsI, the principal contributor to μ_I, primarily exists in the vapor form.

The Cs fractional release rate, μ_{Cs}, depicted in Fig. 3 includes contributions from pure Cs, CsI, and Cs_2MoO_4. Once again, the calculated result is consistent with the data. Here the convergence to μ_{FG} at higher temperature is much slower. Even at 1800°C μ_{Cs} is still about a factor of two to three below that of μ_{FG}. At that temperature, a nontrivial amount of the Cs_2MoO_4 is still in a condensed state. However, given the uncertainty in the existing data base [1], such lack of convergence between μ_{FG} and μ_{Cs} at the higher temperature may be difficult to resolve.

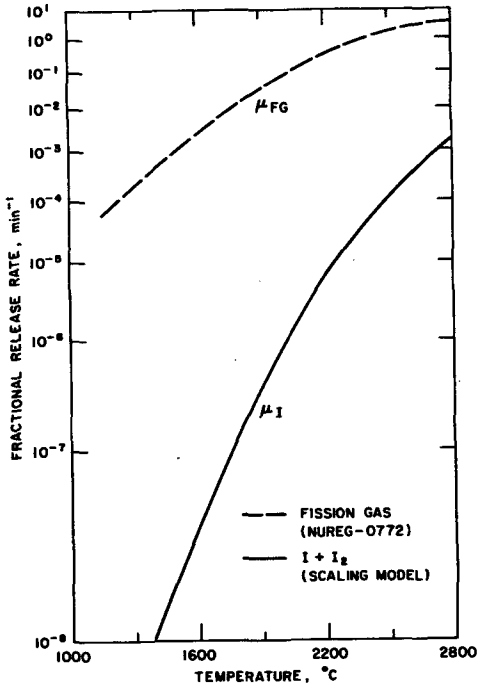


Fig. 1. Iodine Release Rate Constant Versus Temperature.

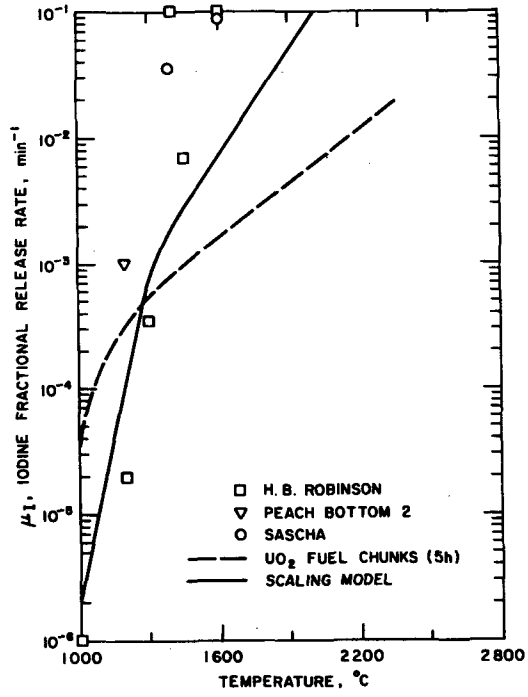


Fig. 2. Iodine Release Rate Constant Versus Temperature.

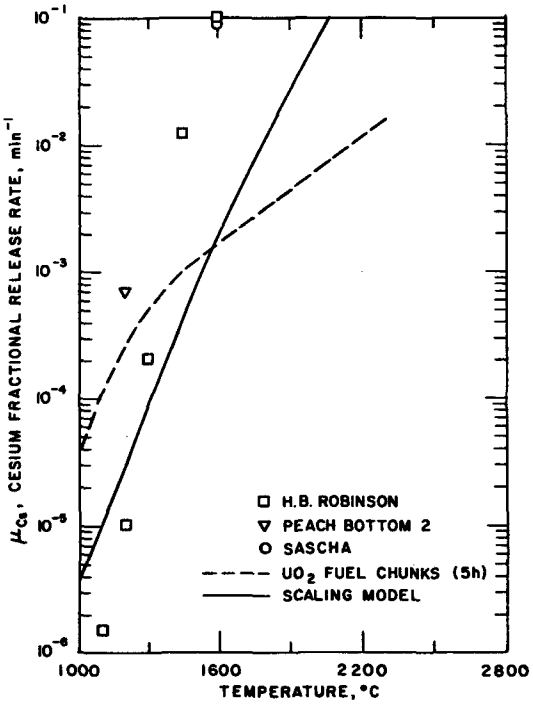


Fig. 3. Cesium Release Rate Constant Versus Temperature.

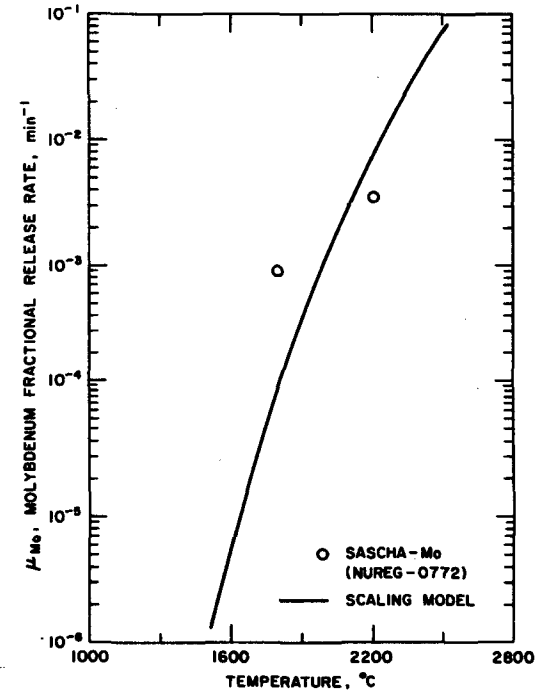


Fig. 4. Molybdenum Release Rate Constant Versus Temperature.

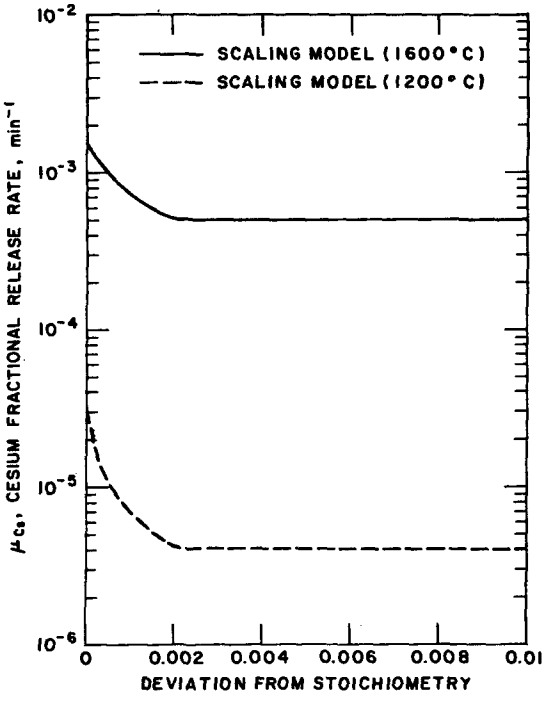


Fig. 5. Cesium Release Rate Constant Versus Deviation from Stoichiometry.

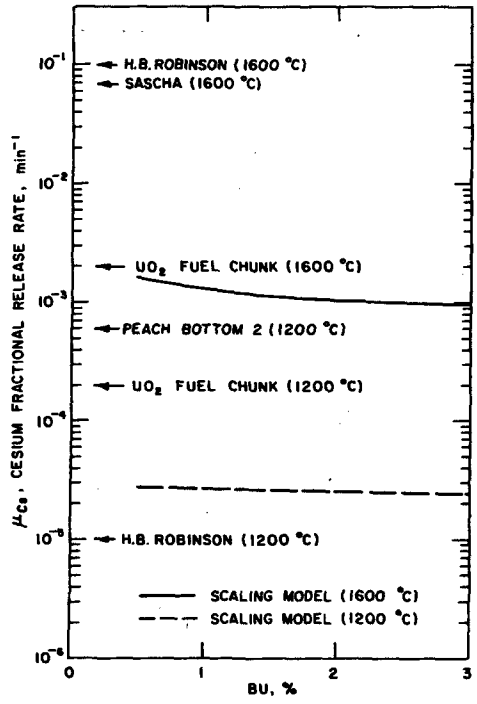


Fig. 6. Cesium Release Rate Constant Versus Burn-up.

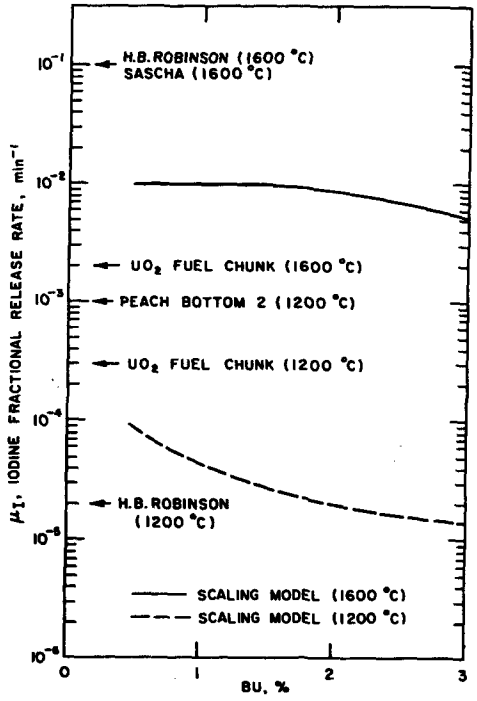


Fig. 7. Iodine Release Rate Versus Burn-up.

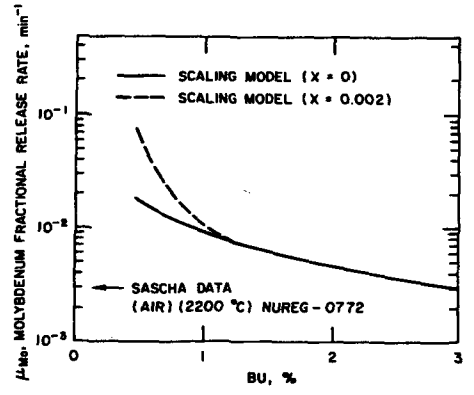


Fig. 8. Molybdenum Release Rate Constant Versus Burn-up.

Figure 4 contains the Mo fractional release rate, μ_{Mo}, for which Cs_2MoO_4 is the only species contributor. Again the calculation is consistent with the data. However, the trend predicted by our theory can only be rigorously tested when more data of improved accuracy become available.

The effect of the initial deviation of fuel stoichiometry, x, on μ_{Cs} is shown in Fig. 5. Note that μ_{Cs} is the same composite quantity as in Fig. 3. The effect of changes in stoichiometry on the release rate is dramatic for small x (< 0.002) but is negligible for larger x. This is easily understood since the oxygen potential is known to vary extremely rapidly for small changes in stoichiometry near the stoichiometric composition.[6] Changes in oxygen potential will affect the internal fuel chemistry, which, in turn, according to the argument given for our scaling model, will impact upon the VFP release rates.

Figures 6, 7, and 8 illustrate the effect of burn-up (in atom %) on μ_{Cs}, μ_I, and μ_{Mo}, respectively. The results shows that μ_{Cs} is only marginally sensitive to burn-up. The μ_I curves in Fig. 7 undergo a qualitative change in shape between 1200°C and 1600°C. Actually, this reflects a dependence of the temperature at which μ_I merges with μ_{FG} with burnup ($\sim$1600°C with burn-up of 1.5%). The μ_{Mo} curve in Fig. 8 shows the same qualitative change with burn-up as the μ_I curve (1200°C) in Fig. 7.

CONCLUSION

In conclusion, we have developed a scaling model for estimating VFP release rates. This model incorporates sophisticated concepts on microscopic mechanisms for VFP and fission-gas migration in the fuel via simple arguments. The model is flexible in the sense of being able to include increasingly complex aspects of fuel chemistry with no conceptual difficulty and only moderate computational effort. It utilizes the theoretical understanding and empirical data on fission gas release accumulated over the last two decades. In its most general form, it does not require any adjustable parameter beyond that necessary for obtaining fission gas release rates themselves and is relatively easy to use.

In the present work, the model has been employed to examine the impact on VFP release rates due to a limited but representative subset of the fuel chemistry. The results are in broad agreement with the available data. However, many of the detailed predictions of this model will have to wait for testing against future experimental data of improved accuracy. Meanwhile, generalization of the scaling model to include more complex fuel chemistry is in progress. It is expected that the model will be very useful to a broad area of activities concerned with reactor safety.

ACKNOWLEDGEMENT

This work is supported by Sandia National Laboratory under purchase order 61-6792A-3.

REFERENCES

1. Technical Basis for Estimating Fission Product Behavior During LWR Accidents, Nuclear Regulatory Commission NUREG-0772, June 1981.

2. C. A. FRISKNEY and J. A. TURNBULL, J. Nucl. Mat. 79, 194 (1979).

3. See e.g., Hj Matzke, Rad. Effects 53, 219 (1980).

4. M. O. TUCKER, Rad. Effects 53, 251 (1980).

5. C. C. DOLLINS and M. JURSICH, J. Nucl. Mat. 101, 192 (1982).

6. P. E. BLACKBURN, Fuels and Materials Chemistry Annual Report, Argonne National Laboratory Report ANL-75-48, 14 (1975).

7. P. E. BLACKBURN and C. E. JOHNSON, Argonne National Laboratory, private communication (1981).

8. WASH-1400 (NUREG-75/014) Table 5.1 and Appendix VII.

9. W. NIXON and D. A. MACINNES, J. Nucl. Mat. 101, 192 (1981).

10. A. B. LIDIARD, Chapter 3 in Crystals With the Fluorite Structure, W. Haynes (ed.), Clarendon Press (1974).

11. D. R. OLANDER, Fundamental Aspects of Nuclear Reactor Fuel Elements, TID-26711-P1 (1976).

12. J. A. TURNBULL, C. A. FRISKNEY, J. R. FINDLAY, F. A. JOHNSON, and A. J. WALTER, J. Nucl. Mat. 107, 168 (1982).

VOLATILE FISSION-PRODUCT SOURCE TERM EVALUATION USING THE FASTGRASS COMPUTER CODE*

J. Rest

Materials Science Division
Argonne National Laboratory
Argonne, Illinois 60439

ABSTRACT

As the noble gases play a major role in establishing the interconnection of escape routes from the interior to the exterior of nuclear reactor fuel, a realistic description of the release of volatile fission products (VFPs) must a priori include a realistic description of fission-gas release and swelling. The steady-state and transient gas release and swelling subroutine, FASTGRASS, has been modified to include a mechanistic description of behavior of VFPs (I, Cs, CsI, Cs_2MoO_4, and Cs_2UO_4). Phenomena modeled are the chemical reactions between the VFPs, VFP migration through the fuel, and VFP interaction with the noble gases. This paper will describe calculations performed with FASTGRASS to describe the release of noble gases, I, Cs, and CsI from LWR fuel during steady-state and power-ramping conditions. Key issues that are addressed in the analysis are the effects of (a) VFP chemistry, (b) various assumptions concerning mechanisms of VFP migration through solid UO_2, (c) fission-gas behavior, and (d) accident scenario on the chemical form of iodine and the rate of iodine release from water-reactor fuel.

I. INTRODUCTION

The accident that occurred at TMI-2 in March 1979 has underscored the necessity of understanding the behavior of volatile fission products (VFPs) in order to predict the radiological consequences of various nuclear reactor accident scenarios. In addition, fission-product (e.g., iodine) source term evaluation is required for the analysis and understanding of the so-called "stress-corrosion cracking" of nuclear reactor fuel cladding.

To date, the analysis of VFPs has, for the most part, utilized simple Booth-type diffusion models and has concentrated on conditions present in nuclear fuel rods during normal or steady-state irradiations.[1-4] The relative success of this technique[1] (at low temperatures) can be attributed to the employment of "effective diffusion coefficients" that have been determined and

*Work supported by the U. S. Nuclear Regulatory Commission. The initial phase of this work was supported by the Nuclear Safety Analysis Center.

utilized over a relatively small range of operating conditions, and the choice of an appropriate fuel surface-to-volume ratio for the determination of the surface area from which the fission products are released. Although the use of diffusion-type models to describe VFP release during normal, low-temperature fuel rod irradiations may be justified, the successful extension of such models to higher-temperature regimes and transient conditions is questionable in that these models totally ignore the chemical interactions between the various fission products, and, except for a partial treatment in Ref. 4, ignore the interaction between the VFPs and the noble fission-gas bubbles. In turn, the inappropriateness of describing the behavior of fission gases during transient conditions with models developed for steady-state operation has been demonstrated.[5]

As the noble gases play a major role in establishing the interconnection of fission gas and VFP escape routes from the interior to the exterior of the fuel,[5] a realistic description of VFP release must a priori include a realistic description of fission-gas release and swelling. The mechanistic steady-state and transient gas release and swelling subroutine, FASTGRASS, has been modified to include a mechanistic description of the behavior of VFPs (I, Cs, CsI, Cs_2MoO_4, and Cs_2UO_4). Phenomena modeled are the chemical reactions between the VFPs, VFP migration through the fuel, and VFP interaction with the noble gases. This paper will describe calculations performed with FASTGRASS to describe the release of I, Cs, and CsI from LWR fuel during steady-state and severe core accident conditions. The effects of a steam environment[6] and gross fuel melting on fission gas and VFP behavior are not considered in this paper.

Key issues that are addressed in the analysis are the effects of (a) VFP chemistry, (b) various assumptions concerning mechanisms of VFP migration through solid UO_2, (c) fission-gas behavior, (d) and accident scenario on the chemical form of iodine and the rate of iodine release from water-reactor fuel.

II. DESCRIPTION OF FASTGRASS

The mechanistic computer code FASTGRASS has been used for predicting fission-gas behavior in UO_2-base fuels during steady-state and transient conditions. (See Ref. 5 for a detailed discussion of the FASTGRASS code.) This code represents an attempt to develop an efficient predictive capability for the full range of possible reactor operating conditions. Fission gas released from the fuel is assumed to reach the fuel surface by successively diffusing (via atomic and gas-bubble mobility) from the grains to grain faces and then to the grain edges, where the gas is released through a network of interconnected tunnels of fission gas-induced and fabricated porosity.

FASTGRASS uses only one bubble size class to characterize the fission gas bubble distribution. Whereas the behavior of fission gas bubbles at the grain face and grain edge in FASTGRASS is based entirely on this single-size-class description, the description of intragranular fission gas behavior includes the kinetics of fission gas atom generation and migration and fission-gas-bubble/gas-atom interactions. In FASTGRASS, with only one bubble size class available, separate descriptions of the size classes are necessary for the intragranular, grain-face, and grain-edge bubbles. In addition, the evolution in time of these average bubble sizes is calculated. The intragranular single gas atoms are characterized by number density; the intragranular, grain-face and grain-edge bubbles are characterized by number density and the average number of atoms per bubble, $S_i(t)$. (The index "i" identifies a particular intra- or intergranular bubble.)

Models are included for the effects of the key variables (production of gas from fissioning nuclei, bubble nucleation and re-solution, bubble migration, bubble coalescence, gas-bubble/channel formation on grain faces, temperature and temperature gradients, interlinked porosity on grain edges, nonequilibrium effects, microcracking, and fission-gas interaction with structural defects) on both the distribution of fission gas within the fuel and on the amount of fission gas released from the fuel. The FASTGRASS code uses these models, together with an equation of state for xenon, experimentally derived steady-state bubble mobilities, and phenomenological modeling of bubble mobilities during transient nonequilibrium conditions,[5,7] to calculate the swelling due to retained fission-gas bubbles in the lattice, on grain faces, and along the grain edges. It also calculates the fission-gas release as a function of time for steady-state and transient thermal conditions.

III. MODELING THE BEHAVIOR OF VFPs WITH THE FASTGRASS COMPUTER CODE

A. Introduction

Modifications for the inclusion of a mechanistic description of VFP behavior consisted of incorporating in the FASTGRASS fission-gas analysis the effective production rates of the relevant VFPs, the chemical interactions between the various VFPs, the interaction of the VFPs with the fission-gas bubbles, and the migration of the VFPs through the solid UO_2 fuel. In the present treatment, only the VFPs I, Cs, and their major reaction products, CsI, Cs_2MoO_4, and Cs_2UO_4 have been included. The formation of Cs_2MoO_4 and Cs_2UO_4 can have a crucial effect on the reactions involving CsI, which are of major concern for deducing the form of the iodine released in LWR power plant accident scenarios.[8-10]

B. VFP Chemistry

The available data are not sufficient to describe the kinetics of VFP chemical reactions. Therefore, the approach to modeling VFP chemistry in FASTGRASS is to assume that the kinetics of the relevant VFP chemical reactions occur fast enough that chemical equilibrium is maintained.

Assuming local equilibrium for the CsI system under consideration (i.e., I, Cs, CsI, Cs_2MoO_4, Cs_2UO_4) and utilizing mass balance and the law of mass action, the chemical reactions model, based on the work of S. W. Tam, P. E. Blackburn, and C. E. Johnson,[11] leads to the following set of coupled nonlinear equations:

$$C_{Cs}^{T} = C_{Cs} + 2C_{Cs_2UO_4} + C_{CsI} + 2C_{Cs_2MoO_4} , \tag{1a}$$

$$C_{Cs}^{2}(1 - \beta - C_{Cs_2UO_4})\, P_{O_2} = \frac{1}{K_1} C_{Cs_2UO_4} , \tag{1b}$$

$$C_{Cs}(C_{I}^{T} - C_{CsI}) = \frac{1}{K_2} C_{CsI} , \tag{1c}$$

$$C_{Cs}^{2}(C_{Mo}^{T} - C_{Cs_2MoO_4})\, P_{O_2}^{2} = \frac{1}{K_3} C_{Cs_2MoO_4} , \tag{1d}$$

$$C_{Cs}^{T} = 0.1882\ \beta\ , \tag{1e}$$

$$C_{I}^{T} = 0.011\ \beta\ , \tag{1f}$$

$$C_{Mo}^{T} = 0.2348\ \beta, \tag{1g}$$

where

$$\beta = \dot{F}t/N_{f}^{o}, \tag{1h}$$

and

$$p_{O_2} = p_{O_2}(x, \beta, C_{Cs_2UO_4}, C_{Cs_2MoO_4})\ . \tag{1i}$$

Here, C_i is the concentration of chemical species i; C_i^T is the total concentration of chemical species i that has been generated by fission at time t; p_{O_2} is the oxygen pressure; x is the initial stoichiometry; K_1, K_2, and K_3 are equilibrium constants for the reactions leading to the formation of Cs_2UO_4, CsI, and Cs_2MoO_4, respectively; β is the fractional burnup, related to the fissioning rate $\dot{F}$ per unit volume; N_f^o is the initial density of heavy-metal atoms in the fuel; and t is the irradiation time.

All condensed phases are assumed to be of unit activity except for Mo, which may be found distributed between an oxide phase and an alloy phase. The vapor phase above each condensed phase is assumed to possess ideal gas behavior. The oxygen pressure, p_{O_2}, is derived from the Blackburn model,[11,12] which has previously been shown to correlate well with oxygen potential data for UO_{2+x}.

The Cs_2MoO_4 and Cs_2UO_4 that are included in the present model can provide strong competitive traps for the available Cs. In fact, since more Mo than Cs is produced at radioactive equilibrium, and each Mo atom takes up two Cs atoms in forming Cs_2MoO_4, the latter species can provide a very efficient sink for the available Cs.

C. VFP Migration and Interaction with Fission-gas Bubbles

The chemical reactions model described by Eqs. (1a-i) is coupled to the FASTGRASS models for the migration of the VFPs through the fuel and for the interaction of the VFPs with the fission-gas bubbles. The set of equations (1a-i) are solved with a non-linear system solver at each code time step and for each morphological fuel region (intragranular, grain face, and grain edge) as functions of VFP concentrations, temperature, burnup and starting O/M.

The VFPs and the fission gases are generated via the fissioning of uranium within the UO_2 grains. The gases and VFPs then migrate to the grain faces and subsequently to the grain edges where they can be released to the exterior of the fuel if a network of long-range interconnected grain-edge porosity exists, and/or if grain boundary separation (microcracking) has occurred.[5,7]

Elemental iodine is assumed to have the same diffusion coefficient as atomic xenon.[13] This assumption is consistent with the findings of Friskney and Turnbull[3], who reported that the diffusion coefficients calculated for krypton, xenon, and iodine were similar in magnitude and temperature dependence; the derived diffusion coefficients for iodine showed good agreement with those obtained from direct measurements of ^{133}I and ^{131}I. Above ~1250°C, the atomic diffusivity of iodine is assumed thermally activated and

$$D_{iodine} = 2.1 \times 10^{-4} \exp[-91{,}000/(RT)], \quad (2)$$

in cm^2/s.[14] Here R is the gas constant in cal/mole·K and T is the temperature in K. At lower temperatures, the diffusion coefficient is enhanced by irradiation[15] and

$$D_{iodine} = 2.0 \times 10^{-30} \dot{F}, \quad (3)$$

where $\dot{F}$ is the fission rate in fissions/cm^3/s. The diffusion coefficient of atomic cesium is taken from Oi and Takagi[16] and is given by

$$D_{Cs} = 8.53 \times 10^{-9} \exp(-6100/RT)\ cm^2 s, \quad (4)$$

where T is the absolute temperature and R is the gas constant. In addition, it is assumed that CsI is formed mainly near fission-gas bubbles and migrates through the fuel primarily within these gas bubbles. Cs_2UO_4 and Cs_2MoO_4 are assumed to be immobile.

Atomic iodine (and cesium) may also migrate to the grain boundaries in fission-gas bubbles. The effect of this particular migration mechanism is discussed in Sections IV and V.

IV. FISSION-PRODUCT RELEASE DURING STEADY-STATE IRRADIATIONS

Figure 1 shows FASTGRASS-predicted fractional release of iodine (^{131}I + ^{133}I) as a function of irradiation time, and compares these results with the data of Turnbull and Friskney.[2] To reflect the experimental uncertainty in temperature reported in Ref. 2, three predicted curves are given in each figure, corresponding to irradiation temperatures of 1733 ± 40 K. The circles in Figs. 1a and 1b represent the fractional release of iodine (^{131}I + ^{133}I) calculated from the data by taking into account the respective fission yields of ^{131}I and ^{133}I. The predictions of Fig. 1a are based on the assumptions that (1) atomic iodine (i.e., iodine that is not predicted to be bound up as CsI) diffuses intragranularly through the solid UO_2 and (2) CsI migrates in fission-gas bubbles; in Fig. 1b, the atomic iodine is assumed to migrate intragranularly with the CsI in fission-gas bubbles, instead of diffusing through the solid as an individual species. A comparison of the curves in Figs. 1a and 1b shows that the latter assumption leads to higher total iodine release predictions than calculations performed with the assumption that the atomic iodine diffuses intragranularly independent of the fission gas. The reason for this result is that the xenon (and krypton) gas bubbles (predicted average-size bubble diameter ≃ 25 Å) diffuse to the grain boundaries at a faster rate than the diffusing iodine atoms and, hence, provide a relatively faster iodine release rate to the grain faces. The iodine atomic species diffuses to the grain faces at a slower rate than these smaller gas bubbles because the effective iodine generation rate is about a factor of 30 less than that for the noble gases. Presumably, the real situation is somewhere in between the curves in Figs. 1a and 1b (i.e., a certain fraction of atomic iodine is captured in intragranular fission-gas bubbles). However, the assumption that both atomic iodine and CsI diffuse predominantly in gas

bubbles gives the best overall agreement with the data. In addition, this particular assumption is more consistent with the general assumption of quasi-chemical equilibrium. Because of the much higher diffusivity of atomic cesium as compared to the noble gases, it is assumed that the predominant intragranular migration mechanism for atomic cesium is solid-state diffusion as an individual species.

The iodine release data shown in Figs. 1a and 1b do not provide any information on the chemical form of the released iodine. The FASTGRASS calculations shown in Figs. 1a and 1b represent the sum of the released atomic iodine and the iodine released as the compound CsI.

Figures 2a and 2b show FASTGRASS-predicted fission product release at 1733 K for Xe, Cs, atomic iodine (I), and total iodine, based on the assumptions of Figs. 1a and 1b, respectively. As is shown in Figs. 2a and 2b, the release of iodine is predicted to occur mainly as CsI (i.e., the difference between I_{TOT} and I). This result indicates that at the average operating temperature of 1733 K utilized for the calculations shown in Figs. 1a and 1b, serious error is introduced when the formation of CsI is neglected in the analysis.

Again, the assumption that atomic iodine migrates intragranularly with CsI in fission-gas bubbles results in a higher total-iodine release at 1733 K than the assumption that the iodine atoms diffuse as an individual species through the solid UO_2. In fact, under the assumption of Fig. 2b (iodine migrates with CsI in fission-gas bubbles), total iodine fractional release is almost identical to the fractional release of the stable fission gases. This result is in agreement with the observation of Appelhans and Turnbull[1] that the total-iodine release is similar to the noble gas release at relatively low temperatures and burnup. It is interesting to note that in Turnbull and Friskney's analysis of these experiments, no account of the chemical form of the iodine was included. Based on the FASTGRASS analysis, it can be concluded that neglecting fission product chemistry (e.g., the formation of CsI) in the interpretation of the data shown in Fig. 1 could result in quite misleading conclusions about the mechanisms of VFP release. Subsequent analyses (e.g., Refs. 3 and 4) have also neglected to include the effects of fission product chemistry.

The calculations shown in Figs. 1 and 2 were repeated, but with the effects of the formation of Cs_2UO_4 and Cs_2MoO_4 neglected. The resulting CsI formation will then be independent of the starting O/M and, consequently, of the oxygen potential. The results showed that in the temperature and burnup range utilized in Figs. 1 and 2, neglecting Cs_2MoO_4 and Cs_2UO_4 formation has very little effect on the predicted form and amount of iodine release. Thus, the growing instability of Cs_2MoO_4 and Cs_2UO_4 at these temperatures decreases the efficiency of these compounds as strong sinks for Cs. At 1733 K, 3% of the retained cesium is predicted to occur as Cs_2MoO_4 and Cs_2UO_4 compounds.

V. FISSION-PRODUCT RELEASE DURING TRANSIENT HEATING CONDITIONS

Previous FASTGRASS studies on the behavior of fission gases during transient conditions have resulted in the identification of the as-irradiated condition of the fuel (e.g., fuel burnup), the fuel microstructure (e.g., grain size), and the transient scenario (e.g., the fuel heating rate) as the key variables affecting fission gas response. Well-characterized data on VFP release during transient conditions are not currently available. In this study the FASTGRASS code was used to examine the effect of as-irradiated fuel burnup and transient temperature on the chemical form (e.g., I, Cs, CsI) of the released fission products, as well as on the relative magnitude of the VFP

release during transient heating conditions. Based on the analyses presented in section IV of this paper, it is assumed that atomic iodine and CsI migrate intragranularly in fission-gas bubbles, and that atomic cesium diffuses intragranularly through the solid UO_2 as an individual species.

Figures 3a-c show FASTGRASS predictions for VFP and noble gas release during a 1 K/s heatup from 1500 K for as-irradiated burnups of 0.1, 1, and 3 at. %, respectively. A comparison of Figs. 3a-c shows that transient fission product release increases with increasing burnup. The increased transient fission product release with increased as-irradiated burnup is due, in part, to the more extensive netowrk of pathways which result, in general, from increased fuel burnups. Figure 4 shows the predicted grain-boundary separation vs transient temperature for the three burnups under consideration. The predicted microcracking increases dramatically with burnup. In addition, the temperature at which the microcracking initiates decreases with an increase in burnup. Again, the reason for this behavior is linked to the increased development of fission-gas bubbles on the grain boundaries at the higher fuel burnups.

The fraction of iodine released as CsI during the transient also increases with burnup. Because enhanced release begins at lower transient temperatures for higher values of as-irradiated burnup (Figs. 3a-c), and because the relative amount of iodine present as CsI is greater at the lower temperatures, the higher burnup fuel releases the available CsI earlier in the transient before the higher temperatures are reached, and the CsI availability has been appreciably reduced.

Note also that for 0.1 at. % burnup, the total iodine release is substantially less, and follows qualitatively different kinetics, than the noble gas release, in contrast to the results at higher burnup values. This is because at this low burnup value, gas atom diffusion to the grain boundaries is dominating the intragranular fission-gas transport during the transient. At the higher values of burnup, the intragranular fission-gas transport is dominated by the migration of small fission-gas bubbles, and because of the assumption that both atomic iodine and CsI migrate within these bubbles, the fractional total-iodine release is qualitatively and quantitatively similar to the noble gas values.

Figures 5a and b show FASTGRASS-calculated transient fission product release during a heatup at 0.1 K/s from 1200 K for two values of fuel burnup (3 and 5 at. %, respectively). The dotted lines in Figs. 5a and b are the results of the calculations without the effects of Cs_2UO_4 and Cs_2MoO_4 formation included. In general, Figs. 5a and b indicate that the effect of Cs_2UO_4 and Cs_2MoO_4 formation increases with as-irradiated fuel burnup and results in relatively more fractional CsI release than would occur if these Cs compounds were not present. The reason behind the increased fractional CsI release in the presence of Cs_2MoO_4 and Cs_2UO_4 formation can be traced to the reduced release of Cs, and thus its higher availability to form more CsI (i.e., as dictated by chemical equilibrium). This effect would also increase with a decrease in the as-irradiated fuel temperatures (as well as with an increase in fuel burnup as shown in Figs. 5a and b).

VI. SUMMARY

The mechanistically based computer code FASTGRASS has been modified to include a description of the VFPs I, Cs, CsI, Cs_2UO_4, and Cs_2MoO_4, as well as the stable fission gases. Phenomena modeled are the chemical reactions between the VFPs, VFP migration through the fuel, and VFP interaction with the noble gases.

As the noble gases play a major role in establishing the interconnection of escape routes from the interior to the exterior of the fuel, a realistic description of VFP release must a priori include a realistic description of fission-gas release and swelling.

Key issues that are addressed in the analysis are the effects of (a) VFP chemistry, (b) various assumptions concerning mechanisms of VFP migration through solid UO_2, (c) fission-gas behavior, and (d) accident scenario on the chemical form of iodine and the rate of iodine release from water-reactor fuel.

Two different assumptions concerning the mode of atomic iodine transport from within the grains to the grain boundaries were examined: (1) atomic iodine diffuses through the solid UO_2 as an individual species, and (2) atomic iodine diffuses with the CsI in fission-gas bubbles. Assumption (2), above, provided a higher rate of release of the iodine to the grain boundaries, and better overall agreement with the data of Turnbull and Friskney.[2] In addition, assumption (2) is more consistent with the assumption of thermodynamic equilibrium, combined with the assumption that CsI migrates in gas bubbles.

The iodine release data of Turnbull and Friskney (shown in Fig. 1) do not provide any information on the chemical form of the released iodine. The FASTGRASS calculations shown in Fig. 1 represent the sum of the iodine released as an atomic species and as the compound CsI. FASTGRASS predicts that iodine will be released predominantly as CsI in these experiments. (The formation of the compounds Cs_2UO_4 and Cs_2MoO_4 were found to have a minimal effect on cesium and iodine release during these experiments.)

Fission-product release during transient conditions is dependent on the accident scenario (e.g., fuel temperatures and heating rates), on the as-irradiated history of the fuel (e.g., fuel temperatures and burnup), and on the degree of grain-boundary separation (microcracking) that occurs during the transient.

In general, transient fission product release is increased with increased as-irradiated fuel burnup. This is due, in part, to the more extensive network of pathways (microcracking and/or bubble interlinkage) produced at higher fuel burnups. The fraction of iodine released as CsI during the transient also increases with burnup. Because enhanced release begins at lower transient temperatures for higher values of as-irradiated burnup (Figs. 3a-c), and because the relative amount of iodine present as CsI is greater at the lower temperatures, the higher burnup fuel releases the available CsI earlier in the transient, before the higher temperatures are reached and the CsI availability has been appreciably reduced.

Finally, the effect of Cs_2UO_4 and Cs_2MoO_4 formation is to increase the fractonal release of CsI; the magnitude of the effect increases with as-irradiated fuel burnup.

The reason behind the increased fractional CsI release in the presence of Cs_2MoO_4 and Cs_2UO_4 formation can be traced to the reduced release of Cs, which makes more Cs available for CsI formation (i.e., as dictated by chemical equilibrium). This effect would also increase with a decrease in the as-irradiated fuel temperatures, as well as with an increase in fuel burnup.

VII. ACKNOWLEDGMENTS

The author would like to thank Drs. C. A. Johnson and S. W. Tam for stimulating discussions and S. Zawadzki for his diligence and expertise in implementing the VFP modifications to FASTGRASS and in FASTGRASS optimization. Finally, many thanks to M. Piasecka for her assistance in performing the FASTGRASS calculations.

VIII. REFERENCES

1. A. D. Appelhans and J. A. Turnbull, "Measured Release of Radioactive Xenon, Krypton, and Iodine from UO_2 at Typical Light Water Reactor Conditions, and Comparison with Release Models," NUREG/CR-2298 (1981).

2. J. A. Turnbull and C. A. Friskney, "The Release of Fission Products from Nuclear Fuel During Irradiation by Both Lattice and Grain-boundary Diffusion," J. Nucl. Mater. 58, 331 (1975).

3. C. A. Friskney and J. A. Turnbull, "The Characteristics of Fission-gas Release from Uranium Dioxide During Irradiation," J. Nucl. Mater. 79, 184 (1979).

4. M. O. Tucker and R. J. White, "Unstable Fission-product Release from UO_2 Irradiated at High Temperature," J. Nucl. Mater. 98, 157 (1981).

5. J. Rest, "The Prediction of Transient Fission-gas Release and Fuel Microcracking under Severe Core-Accident Conditions," Nucl. Technol. 56, 553 (1981).

6. D. Cubicciotti, "A Model for Release of Fission Gases and Volatile Fission Products from Irradiated UO_2 in Steam Environment," Nucl. Technol. 53, 5 (1980).

7. J. Rest and S. M. Gehl, "The Mechanistic Prediction of Transient Fission-gas Release from LWR Fuel, Nucl. Eng. and Des. 56, 233 (1980).

8. J. Rest and C. E. Johnson, "A Prediction of TMI-2 Core Temperatures from the Fission Product Release History," NSAC-12 (1980).

9. D. O. Campbell, A. P. Malinauskas, and V. R. Stratton, "The Chemical Behavior of Fission-product Iodine in Light Water Reactor Accidents," Nucl. Technol. 53, 111 (1981).

10. "Technical Basis for Estimating Fission Product Behavior During LWR Accidents," Nuclear Regulatory Commission NUREG-0772, June 1981.

11. S. W. Tam and C. E. Johnson, to be published.

12. P. E. Blackburn, "Fuels and Materials Chemistry Annual Report," Argonne National Laboratory Report ANL-75-48 (1975) 14-15.

13. J. K. Dawson and R. G. Somden, "Chemical Aspects of Nuclear Reactors, Vol. 1: Gas-Cooled Reactors," Butterworth, London (1963).

14. R. M. Cornell, "The Growth of Fission Gas Bubbles in Irradiated Uranium Dioxide," Philos. Mag. 19, 539 (1969).

15. A. Holt and J. H. Matzke, "Fission-Enhanced Self-Diffusion of Uranium in UO_2 and UC," J. Nucl. Mater. 48, 157 (1973).

16. N. Oi and J. Takagi, "Diffusion of Non-gaseous Fission Products in UO_2 Single Crystals," Z. Naturforsch. 19A 1331-1332 (1964).

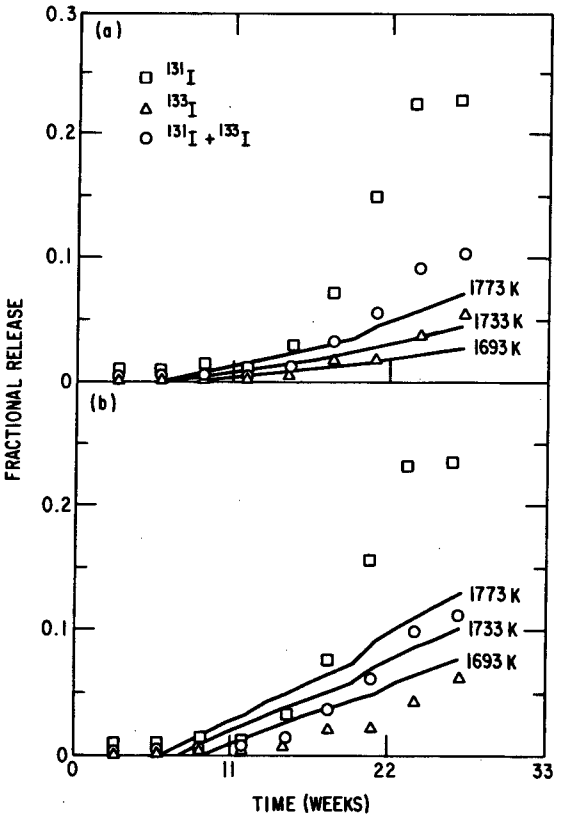


Fig. 1. FASTGRASS-predicted fractional release of $^{131}I + ^{133}I$ at 1733±40 K (solid curves), compared with data of Turnbull and Friskney[2] (symbols). Figures 1a and b were generated utilizing the assumption that (1) atomic iodine diffuses intragranularly through the solid UO_2, and (2) atomic iodine diffuses with CsI in fission-gas bubbles, respectively.

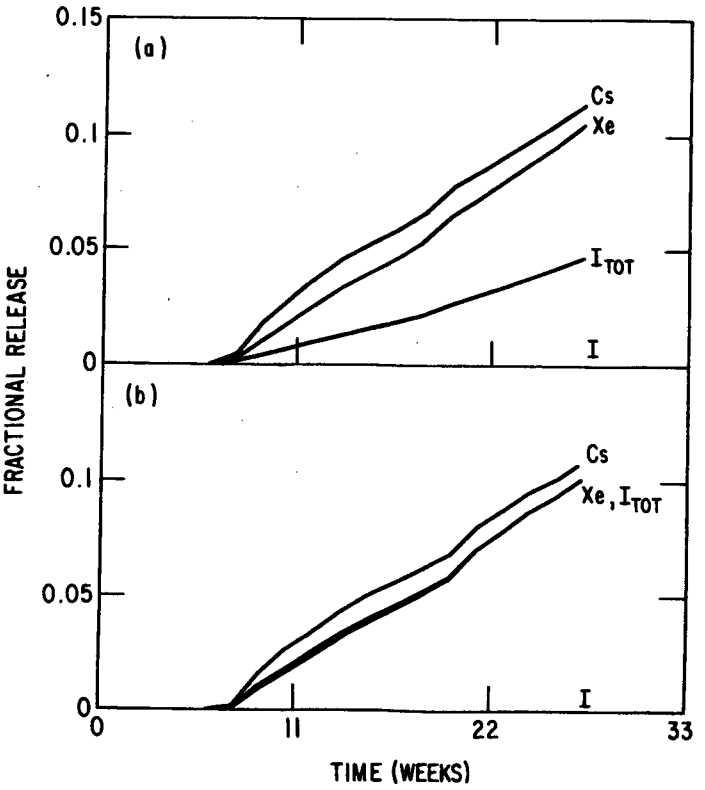


Fig. 2. FASTGRASS-predicted fission-product release at 1733 K. Figures 2a and b were generated utilizing the assumption that (1) atomic iodine diffuses intragranularly through the solid UO_2, and (2) atomic iodine diffuses with CsI in fission-gas bubbles, respectively.

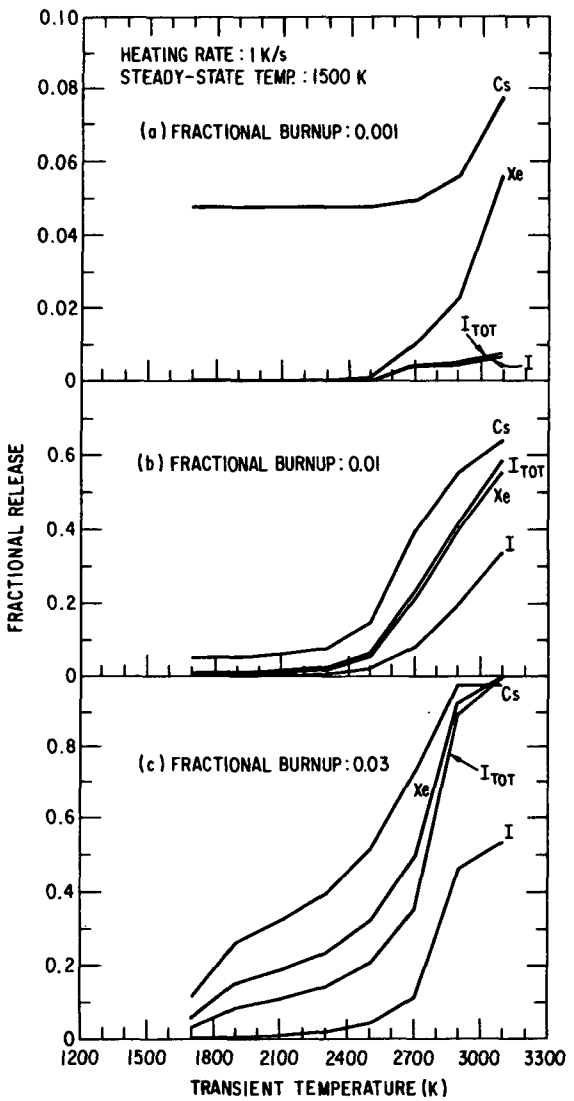


Fig. 3. FASTGRASS-predicted Transient Fission-product Release.

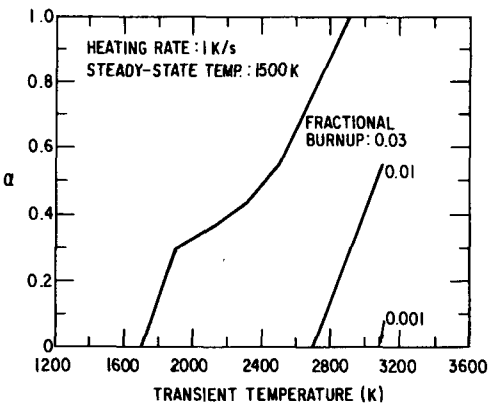


Fig. 4. FASTGRASS-predicted Fraction of Total Grain-boundary.

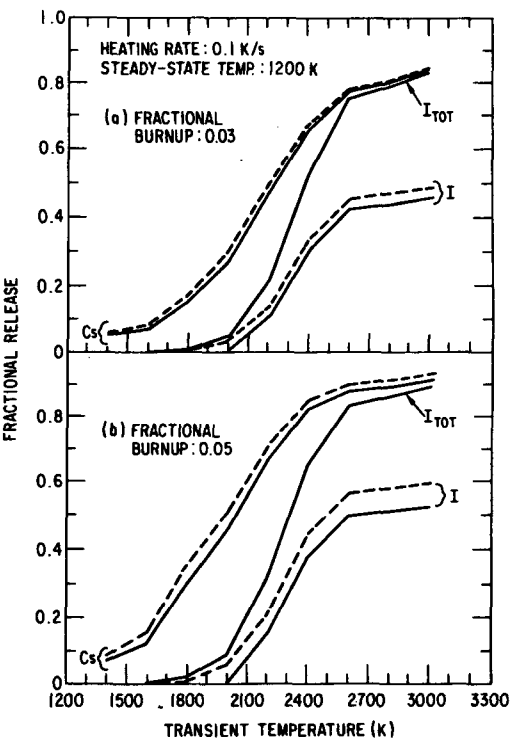


Fig. 5. FASTGRASS-predicted Transient Iodine and Cesium Release.

A GENERALIZED MODEL FOR PREDICTING RADIONUCLIDE SOURCE TERMS FOR LWR DEGRADED CORE ACCIDENTS

Stephen L. Nicolosi and Paul Baybutt

Battelle's Columbus Laboratories
505 King Avenue
Columbus, Ohio 43201, USA

ABSTRACT

The generalized source term code, START, is a semi-mechanistic code which gives a quantitative and time dependent description of the release of radionuclides, and structural materials, from the core region to the primary system of light water reactors during degraded core and meltdown accidents. Results of START analysis are presented for several degraded core accident sequences. These sequences include one of the type analyzed in the Reactor Safety Study and others which involve fuel leaching, core meltdown, and solidified corium leaching. Some of the START results are used to calculate time-dependent release rates.

INTRODUCTION

We have developed a generalized source term code that quantifies the time dependence and the magnitude of the release of radionuclides from degraded reactor fuel. This code, named START (Source Term Analysis for Radionuclide Transport), was developed as a module to provide a radionuclide source term for the TRAP[1] (Transport of Radionuclides in Primary Systems) code. The development of a time-dependent source term code was undertaken because previous source term descriptions, such as that used in the Reactor Safety Study,[3] do not adequately quantify the magnitude of the time dependence of the radionuclide release. Additionally, uncertainty analyses[2] showed that the magnitude of the radionuclide release to the environment is dependent on both the magnitude and the timing of the radionuclide release from fuel. The START code, which uses both semi-empirical and semi-mechanistic models, provides an improved description of LWR source terms. START can also be used as a source term module for reactor safety codes other than TRAP such as CORRAL[3] and MATADOR[4] which describe the transport of radionuclides through reactor containments. The generalized nature of START makes it applicable to the analysis of many types of LWR accidents which involve fuel degradation.

In this paper, we describe the START code and the radionuclide release models which it uses. We also show results of analyses of several degraded core accidents which proceed through several radionuclide release processes. These include clad rupture, diffusion, leach, and melt release processes. The START results, which give the time dependence of the radionuclide releases for these scenarios, show that the time dependence of the release rate is sensitive to the scenario as well as the fuel temperature. The cumulative time at temperature can affect the release rate in the START models.

COMPUTER CODE

START is a generalized source term code which has been assembled in a modular fashion.[5] The code is composed of a main routine, an input routine, a separate subroutine for each radionuclide release model, and an output routine. The radionuclide release processes treated are clad rupture, diffusion, fuel rod leach, melt, corium leach, vaporization, and oxidation. The clad rupture release processes is modeled semi-empirically. All other START radionuclide release processes are modeled semi-mechanistically. This semi-mechanistic description leads to a time-dependent and quantitative description which is an improvement over previous source term models.[3] Each of the radionuclide release models will now be described.

RELEASE PROCESSES AND MODELS

In START, the clad rupture release model assumes fuel rupture by clad weakening and overpressurization in the temperature region 1000-2300 K. Internal pressures can range from approximately 10^3-10^5 kPa. Physically, cladding rupture allows the rapid release of the high pressure gas which has accumulated in the gap at the fuel-clad interface. This escaping gas, whose major components are noble gases and volatile radionuclide species, also entrains some particulates.[6] In meltdown accidents, the clad rupture component comprises only a small fraction of the total source term. In our generalized model, the clad rupture release is described by a semi-empirical model developed at Oak Ridge National Laboratory.[7] This model assumes two release mechanisms. The dominant of these is the burst release at the time of cladding rupture. The secondary release is by gas phase diffusion through interconnected voids and eventually through the opening in the ruptured cladding.

The diffusion release model describes the release of radionuclides from the exposed fuel matrix or from fuel rods with oxidized cladding. It is applied to fuel at temperatures from approximately 2100 K to the fuel liquefaction temperature (which may be lower than the melting point of UO_2). This model uses effective diffusivities to take account of volume diffusion, grain boundary diffusion, and porosity. A readily variable effective diffusivity for the fuel surface resistance is necessary since the fate of the cladding depends on particular accident scenarios. If the heatup rate is rapid, zircaloy melting may dominate cladding oxidation. Under other conditions, the cladding is subject to extensive oxidation through the zircaloy-steam reaction. The zirconia reaction product may either spall and expose the fuel, or it may form a ceramic cladding and act as a crucible to contain and support the fuel until temperatures approaching the melting point of the zirconia (approximately 3000 K) are reached.[9]

In START, the diffusion release can be described through either of two distinct models. One diffusion model is cast in cylindrical geometry and other in spherical geometry. The model in cylindrical geometry can be used to describe the migration of radionuclides through stacked fuel pellets and through stacked fuel pellets surrounded by oxidized cladding. This model however, requires appropriate effective diffusivities. Most radionuclide diffusivities in the laboratory, for UO_2, have been evaluated with the assumption of an equivalent sphere model. To make use of this data START also has an equivalent sphere model available as an alternative to the fuel rod diffusion model.

The melt release model used in START is based on a boundary layer diffusion model similar to that developed by Miller.[10] In this model, the melt surface is exposed to a sweep gas which transports the radionuclides from the molten mass. It is assumed that transport of the radionuclides to the sweep gas is limited by diffusion through the boundary layer. The driving force for diffusion through the boundary layer is the partial vapor pressure of the radionuclide over the surface of the melt. The radionuclide vapor pressure is determined from a Henry's law model

relating the vapor pressure to the mole fraction of the dissolved radionuclide species in the melt.

A semi-mechanistic vaporization release model is used in START to describe the release resulting from concrete decomposition gases sparging through the melt after the molten corium reaches the reactor cavity. It is believed that when the corium melt contacts the reactor vessel cavity, the concrete decomposes releasing gases which sparge up through and around the molten corium.[3] The rate of gas generation is initially rapid and decreases with time. Initially, H_2O and CO_2 are formed, but they react rapidly with the corium to generate a gas mixture composed primarily of H_2, CO, and CO_2. During this process, the sparge gas presents an oxidizing environment to the corium which changes the effective vapor pressures of several radionuclides in the melt. Most radionuclides will form less volatile oxides while the volatility of some species, such as Ru, may be enhanced. Our model assumes that as the decomposition gases sparge through the melt, the sparge gas bubbles equilibrate with the radionuclide species dissolved in the melt. Distribution coefficients are used to determine the ratio of radionuclide concentration in the molten fuel to that in the gas bubbles. Since the bubbles are assumed to equilibrate with the melt, the total volume of gas which sparges through the melt determines the magnitude of the vaporization release.

The oxidation release results from the expected reaction with air of UO_2 particles generated by a steam explosion or other energetic event. When UO_2 oxidizes, it undergoes lattice expansion which causes a change in morphology that enhances radionuclide release. Previously, this release process was modeled empirically.[3] In START, this release process is treated semi-mechanistically as a diffusion release from a spherical UO_2 particle. As in the diffusion release model, effective diffusivities are employed to accommodate competing mechanisms in the diffusion process. The diffusion coefficients from the diffusion release model are required as input data and are adjusted by a multiplicative constant so that the calculated rare gas oxidation release matches benchmark experimental data.[11] This also accounts for the effects of burnup which may be significant.

Leach release models are used to describe the radionuclide release to the primary system fluid when the water level is restored. One set of leach release models can be applied to fuel rods (cylindrical geometry) after the water level is restored following the diffusion release process. Another set of leach release models (variable geometry) can be applied to solidified corium when the water level is restored, terminating the melt release process. Both leach release processes can be described by either an effective diffusivity model or a model using leach rates. Leach rates for several radionuclides in fuel rods have been measured at Battelle's Pacific Northwest Laboratories.[12]

RESULTS AND DISCUSSIONS

The models described above have been used in the START code to predict the magnitudes and time dependences of the release of radionuclides from fuel during several degraded core accidents. These scenarios include a meltdown sequence of the type modeled in the Reactor Safety Study,[3] a degraded core accident involving fuel leaching and liquefaction, and a sequence involving fuel overheating without liquefaction. Since details of the physical processes of core degradation are not completely known, some parameters necessary to describe these processes are not yet available. Among these parameters are surface-to-volume ratio and physical parameter of the molten fuel. These and other parameters were estimated so that these analyses could be performed to demonstrate some of the capabilities of the START code.

For the sequence, similar to that modeled in the Reactor Safety Study,[3] the radionuclide release was initiated at 1070 K when clad rupture was assumed to occur. After 540 seconds, the fuel temperature reaches 2070 K and the cladding melts. A diffusional radionuclide release during the time period between clad melting and fuel melting was included in the analysis. At 750 seconds after clad rupture, the fuel temperature is ∿2600 K. Meltdown is assumed to be complete at 9480 seconds into the accident. Vaporization and oxidation releases then occur. A fraction of the corium (0.15 in our case) is assumed to be dispersed by a steam explosion and is subjected to radionuclide release by oxidation. The remainder of the core is subjected to vaporization release of radionuclides. These two release processes continue for 7200 seconds (2 hours). The accident sequence is terminated at the completion of the vaporization and oxidation releases. The surface-to-volume ratio assumed for the melt in this analysis was ∿.1 cm^{-1}. These assumptions are consistent with those for a typical meltdown accident of WASH-1400. START results for this analysis are shown in Figure 1 alongside the equivalent results for the WASH-1400 source term model. In this analysis, the agreement between the two models is quite good because of the choice of surface-to-volume ratio for the melt. Had a larger surface-to-volume ratio been chosen, the release would have been faster and vice-versa. The sensitivity of the melt release process to surface-to-volume ratio for this scenario is shown in Figure 2. Here the analysis was performed with a range of surface-to-volume ratios of ∿.001 -1.15 cm^{-1}. Results are shown for the Cs release fraction calculated at the end of the melt release. The very low values of the surface-to-volume ratio (∿.001) represent an extreme bounding case where the entire core is present as a single molten mass. These cases naturally give relatively low releases due to the small surface area available for evaporation. More reasonable values of A/V fall in a range of 0.1-5 cm^{-1} which is representative of small pools and single pellet sized drops. With this assumption, the melt release fraction can be expected to vary from 50-100% for cesium. The WASH-1400 Cs release fraction (∿82%)[2] corresponds to an A/V value of ∿0.1 cm^{-1}. This value is equivalent to a drop diameter of ∿60 cm. Any cesium which remains through the end of the melt release process is subject to release by the vaporization and oxidation release processes. Our models for these processes predict complete removal of the remaining cesium in the case studied. In Figure 1, the vaporization release process (∿9480 sec) of the generalized source term model gives a much faster release than that predicted by the Reactor Safety Study model.[2] This can be attributed to the shorter effective release half time (∿.08 min) corresponding to the sparge gas flow rate (2.47 x 10^6 cm^3/sec) used in the calculation. The Reactor Safety Study vaporization release process uses a 30 minute release half time.

A START analysis using the code's multi-species capability was also performed for a degraded core accident involving fuel leaching and liquefaction. These results are shown in Figure 3 for CS, I, and Te. In this case, the radionuclide release was initiated at 1100 K (0 seconds) with failure of the fuel rods. The fuel temperature increased until 1620 seconds into the accident attaining a temperature of 2400 K. At 1620 seconds, the water level was regained bringing the fuel temperature down to 600 K until 5580 seconds at which time the core cooling capability was again compromised. The fuel temperature then increased gradually causing the fuel to liquefy at 2600 K (7380 seconds). The fuel then stayed in this state until 7980 seconds at which time the accident was terminated with restoration of adequate core cooling. Results shown in Figure 3 indicate that 30-40% of the selected radionuclides are released by diffusion processes before fuel melting or liquefaction. In this accident sequence, most of the remaining Cs and I were released from the molten corium.

Since START is a semi-mechanistic code, the radionuclide release rates which it predicts are dependent upon several factors. Among these are temperature, concentration, and surface-to-volume ratio. For example, the START code was used to calculate the cesium release rate from reactor fuel which was quickly heated to 2300 K

and maintained at that temperature for ∿30 minutes. Results of this calculation are shown in Figure 4. Here the cesium release rate is seen to vary from $\sim 2 \times 10^{-2}$ to $\sim 5 \times 10^{-3}$ fraction release per minute of the current fuel inventory of cesium. The actual release rates predicted by START would however be dependent on the burnup and thermal history of the fuel as well as on the accident scenario.

CONCLUSIONS

START (Source Term Analysis for Radionuclide Transport) is a semi-mechanistic code that was developed to quantify the time dependence of the radionuclide release from LWRs during meltdown and other degraded core accidents. This code has the capability to model radionuclide releases by leaching and diffusion, as well as by release mechanisms which have been identified in other source term models.

The analyses performed with the START role demonstrate the importance of surface-to-volume ratio in quantifying the radionuclide release from liquified corium. These calculations also show that the diffusion release mechanism may be important in describing the release of radionuclides during certain accident sequences. It is also shown that the release rates predicted by START are not necessarily constant. These release rates will depend upon a number of factors, including the accident scenario.

ACKNOWLEDGEMENT

This work was performed under the auspices of the U.S. Nuclear Regulatory Commission.

REFERENCES

(1) Hans Jordan, James A. Gieseke, and Paul Baybutt, "TRAP-Melt Users Manual", NUREG/CR-0632 (BMI-2017) (1979).

(2) R. Kurth, P. Baybutt, and D. Cox, "Determination of Environmental Radionuclide Release Uncertainties for LWR Meltdown Accidents", ANS Trans., 34, 144 (1980).

(3) Reactor Safety Study, "An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants", WASH-1400 (NUREG-76/014) (October, 1975).

(4) P. Baybutt and S. Raghuram, "Radionuclide Behavior in LWR Containments During Degraded Core Accidents: MATADOR, A Replacement for the CORRAL Code", presented at the Ninth Water Reactor Safety Research Information Meeting, The National Bureau of Standards, Gaithersburg, Maryland (October 26-30, 1981).

(5) P. Baybutt, S. L. Nicolosi, and S. Raghuram, "Radionuclide Source Terms for Degraded Core Accidents in Light Water Reactors", Proceedings of the ANS Topical Meeting on Reactor Safety Aspects of Fuel Behavior, Sun Valley, Idaho, (August 2-6, 1981).

(6) R. A. Lorenz, et al, "Fission Product Release from Highly Irradiated LWR Fuel", NUREG/CR-0722 (ORNL/NUREG/TM-287/R2) (June, 1979).

(7) A. P. Malinauskas, et al, "Fission Product Release During Loss of Coolant Accidents", Trans. Am. Nucl. Soc., 32, 651 (June, 1979).

(8) R. A. Lorenz, et al, "Fission Product Release from Highly Irradiated LWR Fuel Heated to 1300-1600 C in Steam", NUREG/CR-1386, ORNL/NUREG/TM-346 (November, 1980).

(9) Louis Baker, Jr., and Richard O. Ivins, "Analyzing the Effects of a Zirconium-Water Reaction", Nucleonics, 23, No. 7, 70-74 (July, 1965).

(10) C. E. Miller, Jr., "A Boundary-Layer Diffusion Model of Fission Product Release from Reactor Fuels", Nuclear Application, 5, 198-205, (October, 1968).

(11) G. W. Parker, et al, in "Nuclear Safety Program Semiannual Progress Report for period ending June 30, 1962", ORNL-3319, 11 (August, 1962).

(12) Y. B. Katayama, D. J. Bradley, and C. O. Harvey, "Status Report on LWR Spent Fuel Leach Tests", PNL-3473 (November, 1980).

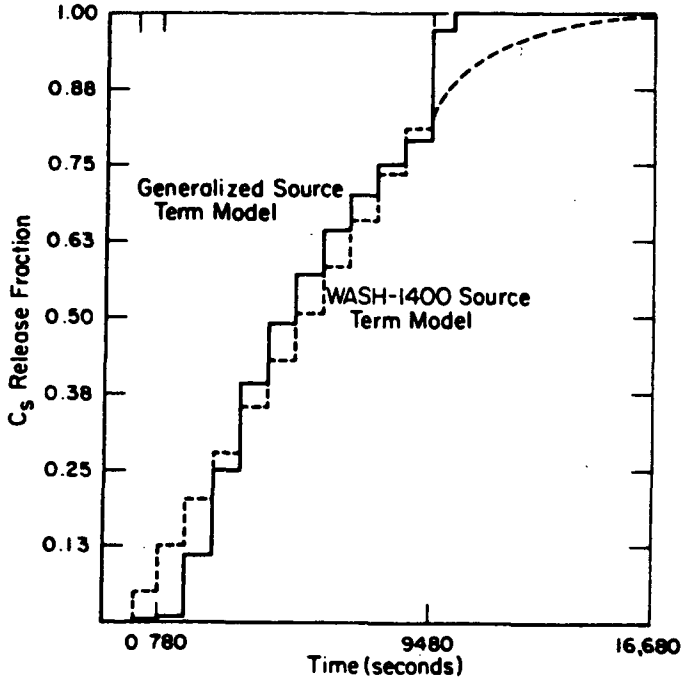


Fig. 1. Comparison of the Generalized Source Term Model with the Reactor Safety Study Source Term Model.

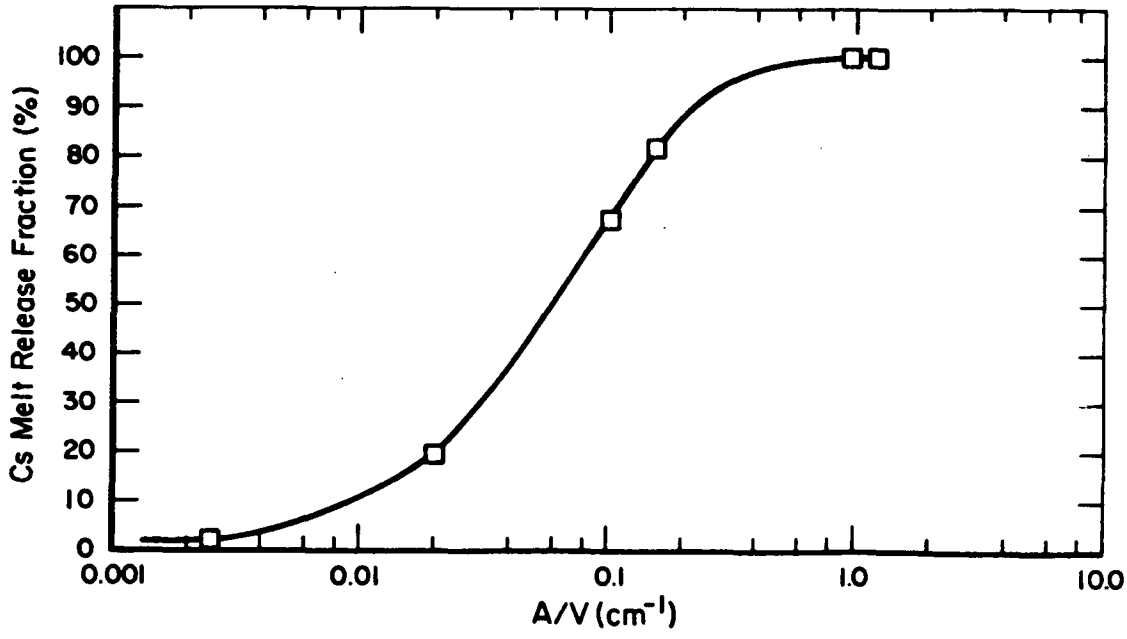


Fig. 2. Effect of Melt Surface/Volume Ratio on the CS Release Fraction.

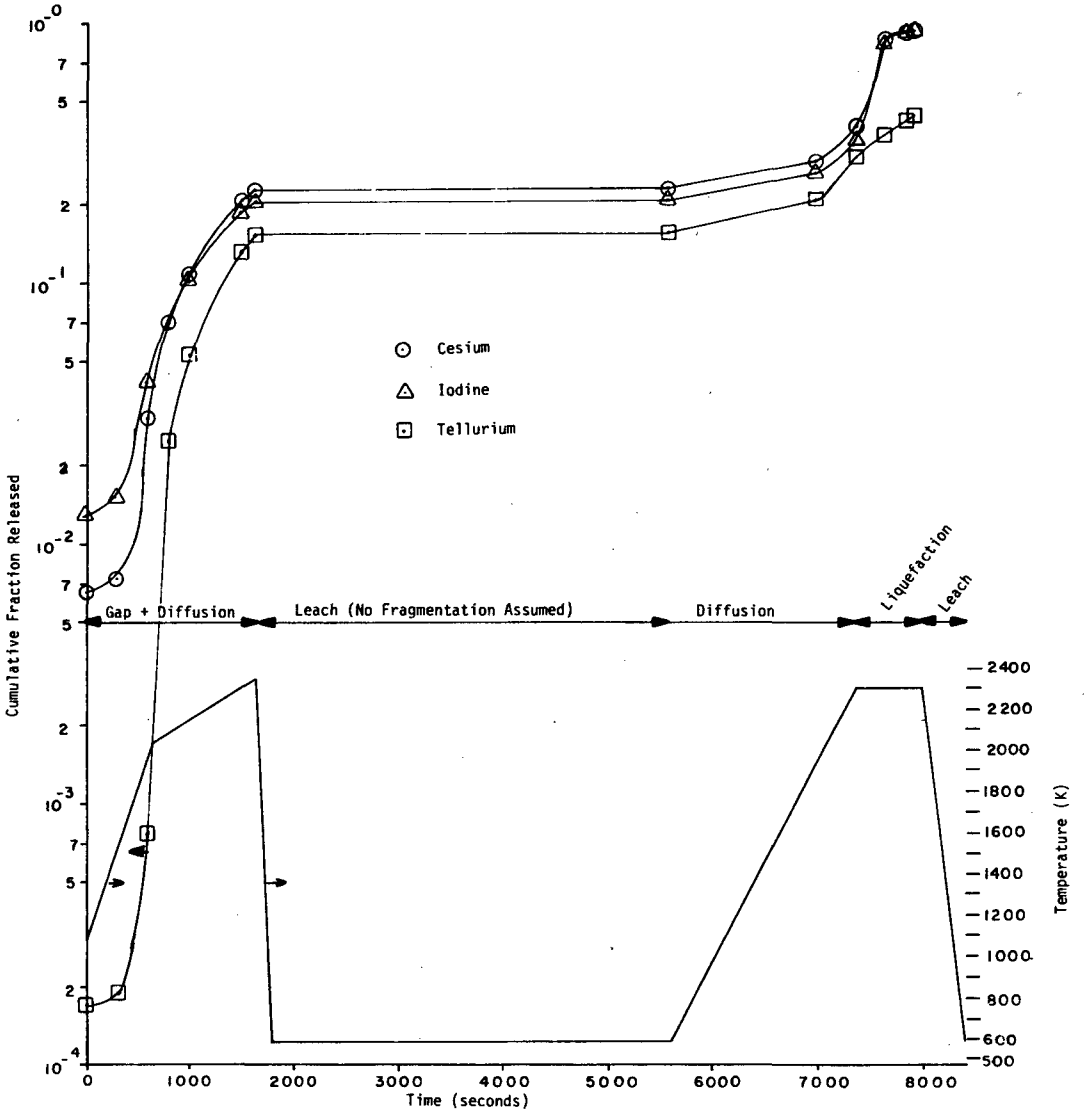


Fig. 3. Cumulative Fraction Release for Selected Radionuclides during a Hypothetical Sequence.

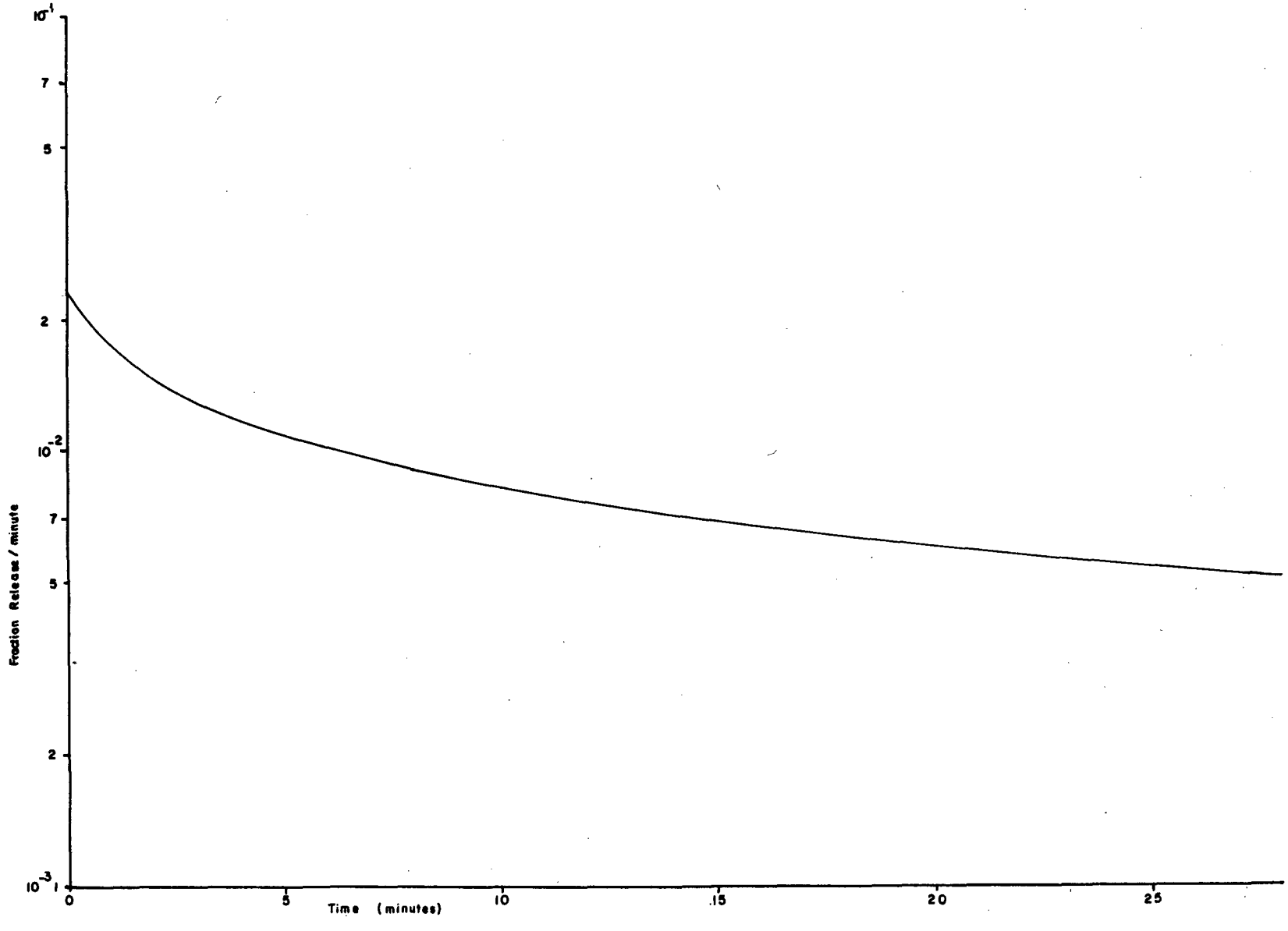


Fig. 4. Time Dependence of a Release Rate Calculated from Results of a START Analysis.

PLATE-OUT MODELLING IN ASSESSING FISSION PRODUCT RETENTION IN ADVANCED GAS-COOLED REACTOR PRIMARY CIRCUITS

E M Hood, A R Taig and P N Clough

Safety and Reliability Directorate, UKAEA,
Culcheth, Warrington, UK

ABSTRACT

The consequences of releases of activity from gas-cooled reactors, both in routine operation and in abnormal conditions, can be substantially mitigated in the case of iodine and caesium due to their retention by primary circuit surfaces. Analysis of the plate-out processes is important in order to construct a validated model for assessing safety-related questions in operating such reactors. The plate-out behaviour of iodine is discussed in this paper, and development of a computer code AGRIPA for modelling the plate-out in Advanced Gas-cooled Reactors in a variety of normal and transient conditions is described.

INTRODUCTION

Analysis of fission product behaviour in the coolant circuit plays a key role in the safety assessment of British Advanced Gas-cooled Reactors (AGRs), both in normal operation and in hypothetical accident conditions. In these reactors the reactor building is not designed to act as a secondary containment and may be only partially effective in retaining fission products and mitigating environmental releases following an abnormal occurrence. The effectiveness of the coolant circuit surfaces for trapping fission products which might escape from the fuel pins is therefore important. A basic commercial AGR (CAGR) design is shown in Fig 1. The graphite-moderated core is some 12 times the volume typical for a PWR core of equivalent power, and itself provides extensive surfaces for plate-out. There are 12 heat-exchangers in the circuit presenting further large areas of steel pipework for fission product deposition from the CO_2 coolant.

Because of their volatility and radiological importance, radioisotopes of iodine and caesium are of prime concern in AGR safety analysis. This paper considers iodine behaviour, specifically I 131. Measurements on reactors of AGR type [1-3] have demonstrated that iodine released into the coolant rapidly plates out onto circuit surfaces. We describe here developments of models of iodine plate-out behaviour which have been incorporated in a computer code, AGRIPA. The code is flexible in its approach to handling the interacting problems of chemistry and mass transport, making it suitable for analysing both steady operation and abnormal transient conditions for a range of AGR designs. In combination with information on the escape of fission product iodine from fuel, the code can define the magnitude and time-behaviour of environmental release associated with specific accident scenarios, for use in consequence assessment.

THE MODELLING APPROACH

A range of diverse information is required for the development of a useful and

flexible code, as illustrated schematically in Fig 2. This can be subdivided into two broad categories, one concerned with handling the coolant flow and mass transport for the event sequence under scrutiny, the other with the chemistry and kinetics of the plate-out process. The former is essentially independent of the latter, since fission product iodine does not significantly perturb the overall flow and thermal conditions. In the first modelling stage, a framework for handling the thermal and fluid flow conditions is required. Most of the information here is well-defined, either by input, or in terms of accepted correlations for the description of mass transport in various flow regimes. By contrast, the chemistry and kinetics of plate-out were initially undefined and interact strongly with mass transport effects in determining overall plate-out behaviour. Moreover, since the timescales of the flow and chemical process are widely different, ability to handle stiff differential equations is needed. For this reason, the numerical integration package FACSIMILE, developed at AERE Harwell [4] proved an excellent framework for the AGRIPA code.

Reactor description The current AGR design is depicted in Fig 1; the core and the heat exchangers are contained within a massive pre-stressed concrete pressure vessel, cylindrical in shape. The graphite moderator contains two types of vertical channel - fuel channels and re-entrant channels, through which a fraction of the 'cool' gas from the exit of the heat exchangers is passed to cool the graphite before re-entering the fuel channels. In the annular space between the core and the vessel wall are 12 heat exchangers (3 per quadrant), manufactured from materials ranging from austenitic stainless steel at the top (hot) to 1% Cr steel at the base (cool). Eight gas circulators (2 per quadrant), situated underneath the heat exchangers, propel the gas round the circuit. The carbon dioxide (roughly 160te) is at ~ 40 bar pressure and contains small controlled amounts of CO, CH_4, H_2O and H_2. The prototype Windscale AGR (recently decommissioned) was a smaller experimental AGR, with coolant loading 14.7te, and four heat exchangers separated from the core enclosure. WAGR operating conditions were sufficiently close to those for a CAGR that conclusions on basic iodine behaviour from experiments there are considered to be directly transferable to a CAGR.

The complex reactor design must be simplified in order to represent it in the computer code. The two main reactor components with large, relatively cool surface areas (where iodine is likely to plate out) are the heat exchanger tube banks and the graphite re-entrant channels. It is assumed that iodine only deposits in compartments representing these two regions. The remainder of the reactor is divided up into appropriate compartments, within which the gas is well-mixed. A schematic representation of one quadrant of the latest CAGR design is shown in Fig 3 and an appropriately simplified version is used for modelling WAGR. Each quadrant is essentially separated from the others, except in the large volumes above and beneath the core and beneath the gas baffle dome, where mixing of gas between quadrants is allowed for, based on plant measurements. [5]

The compartments representing the heat exchangers and re-entrant channels must be further subdivided, since temperatures and pressures may vary within them. Each sub-compartment is then assumed to be homogeneous with respect to gas and surface temperatures, pressure and fission product concentration. Such compartments must be characterised by an effective flow diameter and area, which determine the mass transfer coefficients, and a surface area to free gas volume ratio. Gas flow is expressed as a mass flow-rate, which is uniform round the circuit in steady operation. Gas densities are calculated for each compartment from developed correlations [6] with pressure and temperature. Representation of the reactor as a series of interconnected compartments is extremely flexible and can be adapted to any particular AGR design.

The FACSIMILE package facilitates the treatment of time-dependent changes in temperature, pressure and flow rate associated with transients, by use of a special code block, called every time an update of the time derivatives is required. Temperature and flow rate variations are input as a series of points on a time-ramp profile. The AGRIPA code then interpolates linearly between each pair of points to evaluate the temperature or flow rate at any particular time. Pressure variation may also be

expressed in this way or as an exponential decay appropriate to a blowdown or depressurisation accident. The decay constant is evaluated from the breach area, temperature and pressure using the standard equations for sonic and sub-sonic flow out of an orifice. In this way, therefore, steady operating conditions or any combination of event sequences can be handled fairly simply using temperature, pressure and flow data from a thermal-hydraulic response code as input.

Plate-Out Modelling The amount of iodine in each compartment is expressed as a quantity (eg curies) rather than a concentration. Thus, if Qg_i and Qs_i are the quantities of iodine in the gas and on the surface of compartment i respectively, their derivatives are given by:-

$$\frac{dQg_i}{dt} = -J_i + Um\left[\frac{Qg_{i-1}}{M_{i-1}} - \frac{Qg_i}{M_i}\right] - \lambda Qg_i \qquad (1a)$$

$$\frac{dQs_i}{dt} = J_i - \lambda Qs_i \qquad (1b)$$

where J_i is the flux from the gas to the surface, Um is the gas flow rate (kg/s), M_i is the mass of gas in the compartment, and λ is the radioactive decay constant. Designating a gas-phase iodine species which plates out as X, and assuming that first-order kinetics are obeyed, then for the processes represented by

$$X(g) \underset{k_r}{\overset{k_f}{\rightleftharpoons}} X(s)$$

it can be shown that

$$k_f = \frac{A}{V} \cdot \mu \ s^{-1} \text{ and } k_r = \frac{k_b}{k_a} \cdot \mu \ s^{-1} \qquad (2)$$

where A/V is the surface area to the gas volume ratio for the compartment (m^{-1})

$$\mu = k_t . k_a / (k_t + k_a)$$

k_a = surface adsorption rate constant ($m\ s^{-1}$)

k_b = surface desorption rate constant (s^{-1})

and k_t = mass transfer coefficient ($m\ s^{-1}$) appropriate to the flow and geometry conditions for the compartment, calculated from suitable correlations relating the Sherwood to the Schmidt and Reynolds numbers. The form of the flux J_i in equation (1) is then:-

$$J_i = k_f\ Qg_i - k_r\ Qs_i \qquad (3)$$

IODINE CHEMISTRY AND SURFACE DEPOSITION

Ideally, the surface deposition and resuspension rate constants k_a and k_b should be obtainable from independent sources, such as laboratory measurements. Such measurements of deposition velocities [7, 8] and iodine gas-surface equilibria [9, 10] have established that iodine is absorbed onto a range of steel surfaces in chemically reactive processes. However, no measurements have been made for high pressure CO_2 atmospheres appropriate here, and the reactor steels are in any case contaminated, notably with caesium deposits. It has therefore been necessary to rely on plant measurements,

principally from WAGR, to develop chemistry and surface deposition models. This is feasible because the flow and mass transport aspects of the complex conditions in the reactor can be handled quite accurately in AGRIPA.

Measurements on elemental iodine injected into the Chinon reactor [1], of similar basic design to AGRs but lower operating temperature, have shown that iodine disappears from the coolant rapidly, with an initial half-life of a few minutes, presumably by surface plate-out. Rapid conversion of a proportion of the elemental iodine to organic form was demonstrated, although the completeness of the conversion was not determined. Investigations of iodine species at WAGR [2] have shown similar rapid plate-out of the iodine released from defected fuel, with a calculated half-life of about 2.5 min. for normal operating conditions. Estimates of total iodine deposited on the heat exchangers, from sample measurements, correlated well with estimates of the total released from the fuel. Species analysis of the coolant showed more than 90% of the iodine to be in organic form, principally methyl iodide (MeI), although loss of other forms by deposition in the long sampling pipes could not be excluded. A subsequent series of methyl iodide injection experiments at WAGR [3] showed that for normal operation, this species disappeared with a half-life close to that for defected-fuel iodine. For lower operating temperatures (~250°C), the initial disappearance rate was a little reduced, but for shutdown and cool conditions (~60°C) it decreased markedly ($t_{\frac{1}{2}} \simeq 30$min). These observations suggest that organic iodine (MeI) is an important form in AGR circuits, and that its plate-out behaviour is representative of iodine species generally. We assume in this work that the underlying physical and chemical processes operating in WAGR are common to all AGRs.

Modelling of WAGR iodine plate-out The most directly relevant data are provided by the time-resolved measurements of concentrations in the coolant following MeI injection at WAGR, by Hillary and Taylor [3]. Results of a second, recent series of MeI injection measurements over more varied operating conditions [11] have also been utilised. The general agreement in observed behaviour between the two series is good except for low temperature conditions (60°C) with the reactor shut down. Here, the second experiment shows a disappearance rate for MeI much faster ($t_{\frac{1}{2}}$ ~ 1.5 min) than the original results. The stages in development of a chemistry and surface deposition model are now described:-

(a) Single species model

The simplest starting point was to treat MeI as the only iodine species of importance in the coolant and suppose that it plates out directly onto surfaces. General considerations of gas-surface equilibria suggest that activated adsorption and desorption processes might be involved, with no dependence of rate on surface coverage at the low coverages concerned. Arrhenius - type trial forms of the rate constants k_a and k_b in equations (2) were therefore adopted:-

$$k_a = a \exp(-E_a/RT) \text{ - adsorption}$$

$$k_b = b \exp(-E_b/RT) \text{ - desorption}$$

By trial-and-error fitting, initially allowing plate-out only on the steel heat exchanger surfaces, it proved possible to find Arrhenius parameters which reproduced the main features of the behaviour found in the first MeI injection series reasonably well. The fit was somewhat refined by introducing surface plate-out reactions, again of Arrhenius rate-form, in the re-entrant channels of the graphite moderator. Fig 4 illustrates the stages of fitting for the original 'high temperature' injection experiment [3]. The parameters employed in the final curve shown, given in Table I were derived from an overall fitting to the first and second series injection results, excluding the low temperature conditions.

Table I

Fitting parameters for the single species model

Process	a or b	E_a or E_b, kJ mol^{-1}
Adsorption on steel	3.8×10^{2} ms^{-1}	45.0
Desorption from steel	1.5×10^{8} s^{-1}	140.0
Adsorption on graphite	2.96×10^{-2} ms^{-1}	17.3
Desorption from graphite	6.45×10^{-1} s^{-1}	33.4

Fits to individual experiments are reasonably satisfactory, but some anomalies remain. The experimental results show less temperature sensitivity of the initial MeI disappearance rate than predicted by the model, and the discrepancy in the low temperature results remains unexplained. More seriously, the parameters of Table 1, when applied to the steel sampling pipes employed in the experiments, predict retention of > 99% of the sampled MeI on the pipewalls. There is no reason to suppose these steel surfaces are less effective in trapping than the boiler steels. However, the experimentally-measured coolant burdens of MeI 131 extrapolate quite closely back to the known quantities injected (~100 mCi) at time zero. This provides good evidence that large attenuation factors for MeI in the sampling pipes did not infact exist. The observed rapid disappearance rate of MeI in the WAGR coolant, but minimal retention of this species on the sample-line steel surfaces, seems incompatible with a single species model.

(b) Two-species model We are currently investigating a two-species model which may overcome the inconsistencies noted above. In this, MeI does not plate-out directly, but is converted in the reactor into another iodine species, designated X, which is the form responsible for plate-out. The overall reaction scheme is then

$$\text{MeI (g)} \underset{k_g}{\overset{k_d}{\rightleftharpoons}} \text{X(g)} \underset{k_r}{\overset{k_f}{\rightleftharpoons}} \text{X(s)}$$

where k_d is the rate constant for the reaction which decomposes MeI to form X, and k_g that for regeneration of MeI from X. k_f and k_r are related to k_a and k_b for the surface reactions of X by equations (2), as before. Species X is unidentified, but is likely to be elemental iodine, an organic radical, or a volatile iodide. The reaction forming X is presently undefined, and it may be homogeneous, or involve heterogeneous processes, but some evidence suggests that it is radiation-induced. There is ample evidence [12] that MeI suffers γ radiolysis, and it is likely to be substantially decomposed on passage through the reactor core. The widely disparate removal rates for MeI between the low temperature WAGR injections could be explained by the much lower core γ-fields after prolonged reactor shut down in the first experiment than were present after the shorter shut down in the second case.

For this reason, early trials of the two-species model have confined MeI decomposition and reformation to the core region of the circuit, with rate constants chosen to establish equilibrium in one pass under normal operating conditions. Only the ratio k_d/k_g is then important. Deposition of species X has been limited to the heat exchanger surfaces. Preliminary results of fitting the WAGR MeI injection measurements, shown in Fig 5, demonstrate that this model can reproduce the main features of the experimental observations fairly satisfactorily. The fitting parameters are given in Table II. An Arrhenius temperature dependence has been retained for k_b, since this is the most plausible form for a resuspension process. Both k_a and k_b show much weaker temperature dependence than for the single species model, a consequences of discounting the original low temperature result.

Table II

Fitting parameters for the two-species model

$k_d = 10\ s^{-1}$ $\quad k_a = 0.1 \exp(-12\ kJ\ mol^{-1}/RT)\ ms^{-1}$

$k_g = 1.5\ s^{-1}$ $\quad k_b = 10^5 \exp(-100\ kJ\ mol^{-1}/RT)\ s^{-1}$

CONCLUSIONS

A two-species model appears necessary for simulating all features of the observed methyl iodide disappearance behaviour in the WAGR injection experiments, and thus for understanding of the plate-out of iodine in AGRs generally. Our work with this model is at an early stage, and much further work is needed, especially in defining the chemical reaction and radiation processes involved in interconversion of iodine species in the coolant. However, we believe that the plate-out behaviour deduced for the intermediate species will be generally applicable to AGRs. The form and flexibility of the AGRIPA code ensures that when reliable rate parameters for the surface deposition processes have been derived, application of these to steady-state and accident transient situations for a CAGR will be straightforward.

ACKNOWLEDGEMENTS

We thank collegues in UKAEA, particularly those concerned in the Windscale Nuclear Laboratory experiments on WAGR, for their help and co-operation.

REFERENCES

1. J BARBIER et al, "Piegeage et desorption de l'iode dans les reacteurs graphite gas", paper presented at IRPA Congress, Washington, USA, 1973. International Radiation Protection Association, Paris.

2. J J HILLARY, "Behaviour of iodine species in the Windscale AGR", J Br Nucl Energy Soc., 12,443 (1973)

3. J J HILLARY and J C TAYLOR, "Behaviour of methyl iodide in the Windscale AGR", J Br Nucl Energy Soc, 14,159 (1975)

4. E M CHANCE et al, "FACSIMILE - a computer program for flow and chemistry simulation and general initial value problems" AERE Report R8775 (1977)

5. E J HIGHAM, Windscale Nuclear Laboratories, Private Communication (1982)

6. UKAEA, "CO_2 Properties", TRG Report 680 (R) (1969)

7. J M GENCO et al, "Fission product deposition and its enhancement under reactor accident conditions: deposition on primary-system surfaces". Report BMI-1863 (1969)

8. S L NICOLOSI and P BAYBUTT, "Vapour deposition velocity measurements and correlations for I_2 and CsI". Report NUREG/CR-2713 (1982)

9. E HOINKIS, "A review of the adsorption of iodine on metals and its behaviour in loops". Report ORNL-TM-2916 (1970)

10. R P WICHNER et al, "Iodine sorption and desorption from low-allow steel and graphite", Summary Report, Specialist Meeting on Coolant Chemistry, Plate-out and Decontamination in Gas-cooled Reactors, Julich, F R Germany, December 1980, p55

11. E J HIGHAM et al, "Methyl iodide deposition in WAGR". Windscale Nuclear Laboratories, Unpublished work.

12. L F PARSLY, "Chemical and physical properties of methyl iodide and its occurrence under reactor accident conditions", Report ORNL-NSIC-82 (1971)

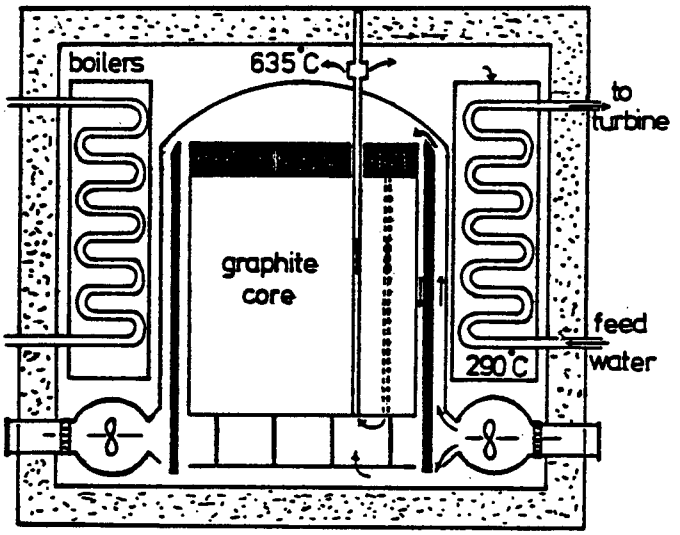


FIG 1 - Illustration of the current CAGR design.

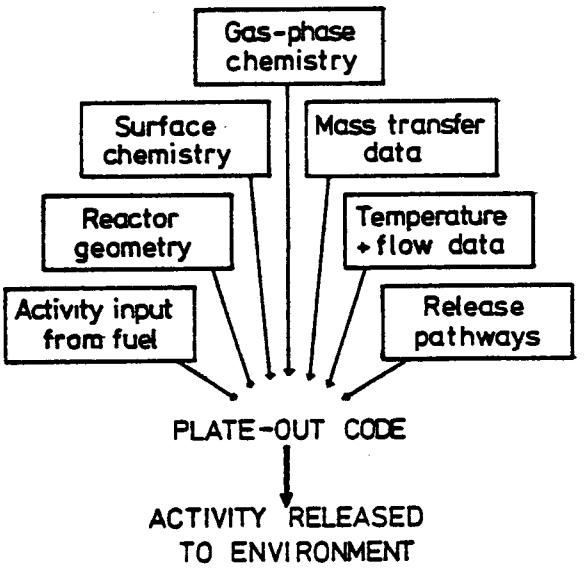


FIG 2 - Inputs to a plate-out modelling code

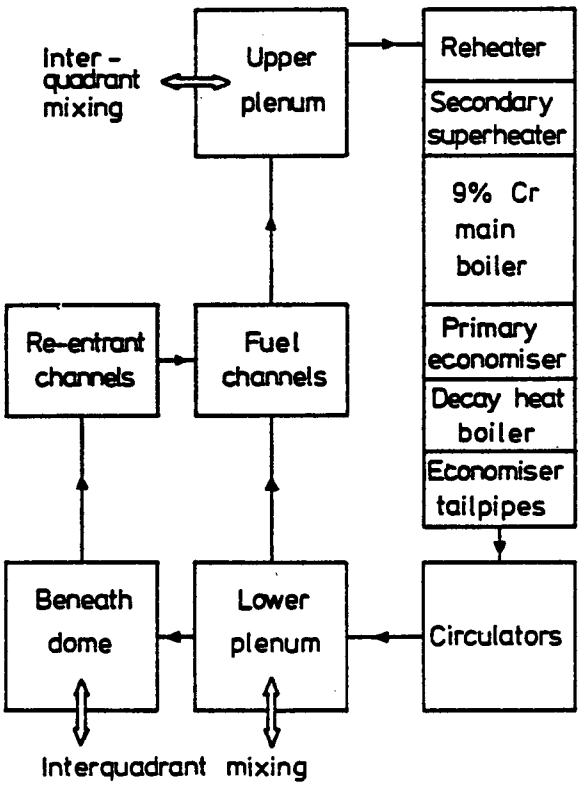


FIG 3 - Schematic of one quadrant of a CAGR as modelled in AGRIPA

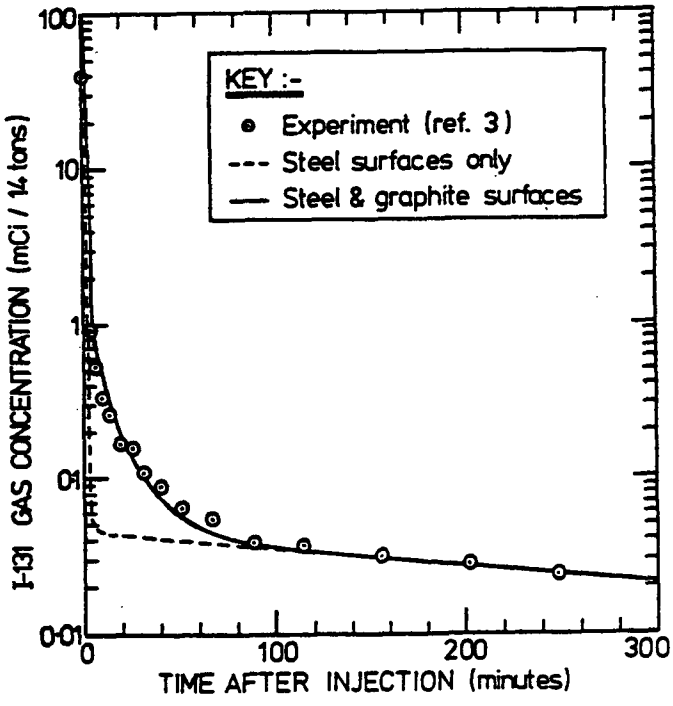


FIG 4 - One-species model - fits to the high temperature MeI injection experiment (ref 3)

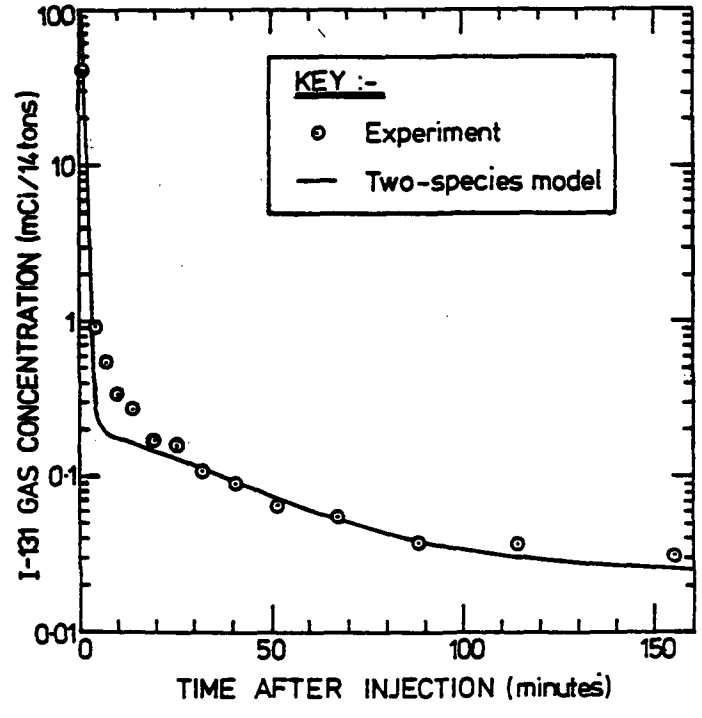


FIG 5 - Two-species model - preliminary fit to the high temperature MeI injection experiment (ref 3)

UNCERTAINTIES IN LWR MELTDOWN ACCIDENT CONSEQUENCES

R. E. Kurth and P. Baybutt

Battelle's Columbus Division
Risk Assessment Group
505 King Avenue
Columbus, Ohio 43201

ABSTRACT

The development of guidelines for estimating uncertainties in radionuclide releases during LWR meltdown sequence is important for the probabilistic risk assessment of nuclear power systems since comparison of nuclear power risk with other engineered systems risks, or the implementation of safety goals, requires a consideration of uncertainties. This paper provides guidelines for estimating uncertainties in the radionuclide release for risk-dominant LWR meltdown sequences. These guidelines are obtained by a method for extrapolating a set of results of uncertainty analyses for selected LWR meltdown sequences, in which the dominant sources of uncertainty in the radionuclide release were examined, to a set of uncertainties which cover a class of LWR meltdown sequences. The results of these analyses were modified to include all sources of uncertainty and then extrapolated to form guidelines for uncertainties for category one through four releases as identified in WASH-1400.

GENERIC GUIDELINES FOR UNCERTAINTIES IN LWR ACCIDENT CONSEQUENCES

INTRODUCTION

The objective of this work is to develop approximate guidelines for the uncertainty in LWR accident consequences so that present and future probabilistic risk assessments (PRA) of nuclear power plants can include the effects of these uncertainties in their evaluations. The purpose of this discussion is thus threefold: one, to summarize previous uncertainty analyses work; two, to extrapolate these results, to the extent possible, to other accident sequences; and finally, to make recommendations for uncertainty values and additional research.

The value of risk used in PRA is comprised of two components, probability and consequences. The variability of the risk value is caused by stochastic variations in the consequences and uncertainty, due to a lack of knowledge, in both the probability and consequences. The guidelines to be developed during this discussion address only the variability in consequence values. Further, no distinction is made between variation due to the stochastic nature of the consequence measure and that due to a lack of knowledge, thus the term uncertainty encompasses both sources of variation in this paper.

The sources of uncertainty in accident consequences arise from the stochastic nature of the variables and a lack of knowledge about parameter values and physical processes. Estimates for these uncertainties can be extrapolated, to an extent, from the results of previous analyses. The existing models and computer codes for calculating the health effects from a given radionuclide release introduce another source of uncertainty which cannot be estimated from previous uncertainty results. In addition, models and variables from the meltdown and radionuclide transport models which were not included in the previous uncertainty analysis and the uncertainty methodology (see reference 1) itself introduce uncertainties. These uncertainties will be included in the guidelines by developing multiplicative factors for the uncertainty values generated from the previous results.

UNCERTAINTY ANALYSES RESULTS TO DATE

Uncertainty analysis of each of three LWR meltdown accident sequences[2,3] have been performed using statistical designs and response surface methodologies.[1] Two accident sequences for a PWR, TMLB′-δ and ACDF-α, and one for a BWR, TC-γ, were analyzed. The TMLB-γ sequence involves a transient followed by the complete loss of on-site power in which the containment fails due to overpressurization while the ACDF-α sequence is a large LOCA sequence with the loss of ECC and containment spray injection where the containment failure occurs due to a steam explosion. The TC-γ sequence starts with a transient event requiring a reactor scram, however, the plant continues to operate at 30 percent of full power. Since the heat removal capabilities cannot handle this amount of heat, the containment fails due to overpressurization causing all pumps to cavitate.

The uncertainty analyses were performed by fitting a response surface to the results of runs of the MARCH[4] and CORRAL computer codes. The points through which the response surface was fit were determined by a statistical design, specifically a fold-over fractional factorial design.[5] The results of the analyses are summarized below, after which the guidelines are developed.

Uncertainty Analyses Procedure

The selection of the variables to be included in the uncertainty analysis was based on a priori judgment of which variable will determine the uncertainty of the accident consequences. In the case of the PWR study, results from a smaller design[2] coupled with engineering judgment provided the means for the choice of variables to use in the analysis. The BWR sequence was the first analysis done for this reactor type, and thus the variables were selected using engineering judgment.

The full set of inputs to and models contained in MARCH/CORRAL contains hundreds of values. In fact, only a portion of this set will determine the uncertainty in the accident consequences since either the variable has a negligible uncertainty or the response is insensitive to some variable. In such cases, there is no need to include the variable in an uncertainty analysis. It is useful then to construct a set of variables which may control the uncertainty in LWR meltdown sequences. This set is denoted the critical variable set. This set of variables may be further reduced since not all variables are important for a specific accident sequence. The design set of variables, i.e., those actually chosen for analysis, are shown in Table I.

Variable ranges, also shown in Table I, were assigned based upon a polling of expert opinion and data in the available literature. Values of the 5th and 9th percentile in addition to the mean values of each continuous variable were used to define the range. For models, or discrete variables, extreme cases were arbitrarily, but consistently, set to high and low values.

TABLE I

VARIABLES INCLUDED IN UNCERTAINTY ANALYSES

Acronym[a]	Variable Description	Variable Range Low	(Best Estimate)	High
FMP	Fuel Melting Point	1800°C	(2277°C)	2880°C
CFM	Containment Failure Mode	0.0065 m^2	(0.65m^2)	0.65m^2
FPSM	Fission Product Source Term--Melt Component	Low RSS	(RSS)[b]	High RSS
FPSV	Fission Product Source Term--Vaporization Component	Low RSS	(RSS)	High RSS
FPSX	Fission Product Source Term--Steam Explosion	Low RSS	(RSS)	High RSS
FPD	Fission Product Deposition--Natural			
	Vapor Radionuclides	1/2λ	(λ)[c]	2λ
	Particle Radionuclides	1/5λ	(λ)	5λ
FPDA	Fission Product Deposition Annulus			
	Vapor Radionuclides	1/3λ	(λ)	3λ
	Particle Radionuclides	1/5λ	(λ)	5λ
HTC	Heat Transfer Coefficient Between Corium Metal-Oxide Layer	0.002	(0.01)	0.05 w/cm^2/K
CFW	Core Fragmentation in Water Model	Particle	(Particle)	Slab
MM	Meltdown Model	A	(A)[d]	C
FCR	Fraction of Clad Reacting	0.5	(0.75)	1.0
FDROP	Fraction of Core Which Must be Molten for Slumping	0.4	(0.75)	6.9

[a]The acronyms are provided for the sake of conciseness during the discussion.

[b]RSS represents the best estimate value given in the Reactor Safety Study (RSS) WASH-1400. Similarly, the lower and upper bounds given in WASH-1400 for the radionuclide source terms were used.

[c]These factors represent a multiplier on the deposition velocity calculated by CORRAL.

[d]Models A and C represent discrete and continuous slumping models, respectively, in MARCH.

The choice of the statistical design to be used was based upon the number of variables to be included in the analysis, the requirement that the design be of resolution IV and the condition that the number of computer code runs be minimized. The selection of variables for both the PWR and BWR analyses has defined eight variables for inclusion in the analysis in both instances. A standard, well-known design (see reference 5), a 2^{8-4} "fold-over" design was selected for this study. Using the acronyms given in Table I, the variable assignment was made.

This statistical design was used to define 16 runs, for each accident sequence, of the MARCH and CORRAL codes to obtain the uncertainty information. The results of the analyses are given below.

TMLB'δ Sensitivity and Uncertainty Analysis Results

For the I_2 group, the meltdown model is the variable to which the response demonstrates the second largest amount of sensitivity while it is the CFM variable for Cs, CFW for Te, FPSM for Sr, and FPSV for both Ru and La. In all groups, other than Cs, the next most sensitive variable is a two-factor interaction, whereas in the Cs group the response is slightly more sensitive to the CFW variable than it is to an interaction. It is important to note that two-factor interactions are important according to this sensitivity ranking.

The response surface coefficients were used to calculate each variable's contribution to the total uncertainty using variance as the measure of uncertainty. The results of these calculations demonstrate that for the particulate radionuclides FPD is the dominant term in determining the uncertainty in the release of each group while for the vapor release group the containment failure mode is the dominant variable. The decreased importance of FPD for the iodine release group is due to the fact that the uncertainty in the FPD variable is 60 percent less for iodine than it is in the remaining radionuclide groups, and the fact that the iodine is deposited in the containment by a different physical mechanism than the particulate groups.

The MM and CFW variables are also somewhat important in determining the uncertainty in the iodine release, although much less important than the CFM variable. The low value of MM indicates that the discrete slumping model, Model A, is being used to model the core melt. Model A drops a large amount of molten material into the bottom head at or near the end of the core melt release and boils off the remaining water in the vessel head. By contrast, however, the continuous slumping model, Model C, is continuously boiling water out of the vessel head and, in fact, close to the end of the core melt the vessel head is dry. Thus, the MM variable controls the flow rate during the release of the melt component of the radionuclide release. The CFW variable affects the magnitude of the flow rate during the vaporization phase of the release. The HOTDROP model assumes the debris fragments into particles 1 inch in diameter, and thus the heat transfer area is increased over the slab model causing a greater rate of flashing and steam generation. The HOTDROP model thus causes a larger flow rate throughout the containment over a shorter period of time than the SLAB model predicts. The effect of MM and CFW on the magnitude and timing of the flow and leakage rates accounts for the contribution to the uncertainty for the I_2 group.

In the Cs and Te groups, FPD is the only variable of consequence which affects the releases, although CFM and CFW do contribute in a nonnegligible way to the release uncertainty. The radionuclide source terms are unimportant for the I_2, Cs, and Te groups since there is always a 100 percent release of these nuclides. For the Sr, Ru, and La groups, FPD is the key variable controlling the release uncertainty, however, the source terms are almost as important in determining the uncertainty. For the Ru and La groups, in which the varporization component of the release is large relative to the melt component, CFW is somewhat important also.

TC-γ Sensitivity and Uncertainty Analysis Results

For all radionuclide groups, one of the two deposition terms is the variable to which the radionuclide release is most sensitive, except in the La group where FPSV is equivalent to the FPD term.

The response surface coefficients were used to calculate each variable's contribution to the total uncertainty in the equilibrium release. The results of these calculations demonstrate that for all of the radionuclide groups, the deposition terms control the majority of the release uncertainty. Since the two deposition terms dominate the results, further analyses were performed to obtain additional uncertainty information about the TC-γ sequence.

The results of these analyses confirmed that FPD and the source terms, FPSM and FPSV, are the major contributors to the uncertainty in the release of radionuclides during the TC-γ sequence. Additionally, it was found that there are several important interactions involving FPDA, including FPDA x HTC, FPDA x FPSM, and FPDA x MM. Further analysis of the effect of two-factor interactions on the overall release uncertainties using an alternate measure of uncertainty confirms the fact that the FPD x HTC and FPDA x HTC interactions are important and demonstrates that the deposition terms and source terms interact together and amongst themselves to contribute a significant amount to the release uncertainty.

ACDF-α Uncertainty Analyses Results

The variance analysis of the full design demonstrates that, as in the previous uncertainty analysis results for TMLB'-δ and TC-α , the fission product deposition and source terms are clearly the variables controlling the uncertainty in the radionuclide releases. For the particulate groups, the uncertainty in the deposition variable contributes more than 90 percent to the total uncertainty except in the Sr group where the FPSM contributes 40.6 percent and FPD 53.8 percent and the La group in which FPSV contributes 31.8 percent and FPD 54.9 percent.

The vapor group, represented by I_2, presents a interesting result. In this group, the FPSM term makes up 49.8 percent of the total uncertainty, FMP 26.4 percent, and FPSX contributes 1.0 percent. The contribution of the FPSM term is not surprising, however, the contribution of the FMP term is surprisingly large. The large contribution of FMP contribution to the uncertainty may be explained by noting that the actual value of the oxidation source term, FPSX, is controlled by the fraction of the core which is molten when the core collapses. Thus, if the value of FPSX is 0.5 but only 40 percent of the core is molten at the time of the core collapse, then the source term for the oxidation release is 20 percent of the remaining fission products rather than 50 percent.

The contribution of FMP and FDROP to the response uncertainty is due to their interaction with the melt and oxidation release fission product source terms. A lower melting point will shorten the duration of the melt release while a higher melting point will lengthen the duration of the melt release. A long release time for the melt component will mean that radionuclides are being released later in the sequence when the intercompartmental flow rates have decreased. Smaller flow and leakage rates allow more deposition of the fission products to occur. Conversely, a shorter melt release period implies that more of the radionuclide release will occur during high flow rates when the deposition mechanism is less effective. The FDROP term is important in the sensitivity of the radionuclide release since it directly affects the oxidation release source term. If only 40 percent of the core is molten at the time of core collapse, then only 40 percent of the oxidation release for each

radionuclide group may occur. In addition, the value of FDROP will also affect the duration of the melt release.

Conclusions Reached From Uncertainty Analyses

The major conclusion drawn from these results is that there are four key mechanisms which control the uncertainty in the environmental release of radionuclides during meltdown sequences. These are the deposition velocity of radionuclides, the radionuclide source term modeling, the intercompartmental flow and leakage rate, and, for the I_2 release group, the temperature difference between the containment atmosphere and walls. This ranking of the physical mechanisms is as important as the variable ranking, since, while the variable ranking for these sequences is significant in determining priority areas for research to reduce the overall uncertainty in these accident consequences, certainly a more general ranking is necessary. For example, one would not presuppose that the same variables which were determined to control the uncertainty in the radionuclide release for the TMLB-δ sequence would also control the uncertainty in the release for the ACDF-α sequence. Thus, the identification of those physical mechanisms which cause the most significant variation in the radionuclide release is necessary in determining a priori which parameters and models are important in controlling the uncertainty in the release. It is also necessary for the development of generic guidelines for uncertainty.

Estimating the Uncertainty Contribution Not Included in Previous Analyses

The uncertainty in the radionuclide release fractions given in Table II to IV does not represent the complete uncertainty in accident consequences for several reasons. First, not all variables and models in the meltdown and radionuclide transport processes were included in the analyses because either they did not exist in the MARCH and CORRAL II computer code or they were inadequate. Secondly, no dispersion and health effect model was included in the analyses because of the incompatabilities of such consequence codes with MARCH/CORRAL results. In this section, multiplicative factors will be assigned to the results given in Tables II to IV in order to include such uncertainties. The derivation of these factors will proceed by examining each of the major physical processes which must be modeled.

In the meltdown modeling code, MARCH, several models not included in the previous analyses could affect the uncertainty in the accident consequences. These are discussed below.

The present model for head failure in MARCH assumes that the vessel always fails catastrophically. Localized head failure would probably change the location of the release, e.g., through the pressure relief valves, to a higher location decreasing deposition effects. On the other hand, the duration of the releases may be lengthened causing an enhancement of the deposition effect. These differences could cause a 10 percent variation.

The core debris particulation model in MARCH assumes a uniform distribution of particle sizes small enough to use a lumped heat capacity analysis. These are conservative assumptions in that they lead to the largest possible flow rates. Since changes in this model can only reduce the flow, and thus leakage rate, it is assigned a factor of 0.9.

The containment failure model in MARCH does allow for varying break area sizes. However, this effect was only included in the TMLB- sequence. Since a smaller break area can dramatically reduce the radionuclide release fraction, and vice-versa, this effect is included as a factor of 1.6.

TABLE II

UNCERTAINTY ESTIMATES FOR THE ENVIRONMENTAL RADIONUCLIDE RELEASE FRACTIONS FOR THE TMLB-δ SEQUENCE

Radionuclide Group	Best Estimate Value	Average Release Fraction	Standard Deviation
I	.59	.18	.08
Cs	.55	.38	.17
Te	.18	.35	.16
Sr	.07	.05	.03
Ru	.02	.06	.03
La	.003	.01	.006

TABLE III

UNCERTAINTY ESTIMATES FOR THE ENVIRONMENTAL RADIONUCLIDE RELEASE FRACTION FOR THE TC-α SEQUENCE

Radionuclide Group	Best Estimate Value	Average Release Fraction	Standard Deviation
I	.04	.08	.05
Cs	.15	.25	.11
Te	.11	.27	.12
Sr	.02	.03	.02
Ru	.01	.05	.03
La	.001	.01	.006

TABLE IV

UNCERTAINTY ESTIMATES FOR THE ENVIRONMENTAL RADIONUCLIDE RELEASE FRACTIONS FOR THE ACDF-α SEQUENCE

Radionuclide	Best Estimate Group	Average Release Value	Standard Fraction
I	.49	.38	.06
Cs	.36	.38	.16
Te	.19	.34	.15
Sr	.04	.06	.03
Ru	.19	.29	.12
La	.002	.01	.006

There are several engineered safeguard systems which have not been included in the previous uncertainty analyses. Of these, the containment spray systems for the PWR and the suppression pool for the BWR are considered to be the major contributors to the uncertainty and are assigned a factor of 1.1.

The important contributors to the uncertainty in the radionuclide transport code CORRAL are the radionuclide release and deposition models, and the coagulation models. These models in the present version of CORRAL are somewhat simplistic and, in fact, are being updated in a new version of CORRAL. Since the source term is important in determining the uncertainty, it has been assigned a factor of 1.3. The coagulation model will interact with the deposition model to have a significant effect on the uncertainty and thus is assigned a factor of 1.2. It is believed that any inadequacy in the deposition model has already been included in the previous analyses, and thus it is assigned a value of 1.0.

It is difficult to assess the uncertainty which would be introduced by a dispersion and health effect code without any formal analysis. However, based on informal discussions with CRAC code users, it is believed that the use of CRAC would involve a factor 2.5 change on the uncertainty in the accident consequences.

The effect of uncertainties in variables and physical processes not included in previous uncertainty analyses on the uncertainty in accident consequences is believed to increase the uncertainty estimates from previous analyses by a factor of 3.0. If the response is given in terms of health effects, e.g., initial fatalities, the uncertainty should be increased by a factor of 7.5.

RECOMMENDATIONS FOR GUIDELINES FOR LWR ACCIDENT UNCERTAINTIES

In order to extrapolate the results of the previous uncertainty analyses to other accident sequences, it is necessary to compile a list of appropriate sequences. This list is given in Table V where the sequences are identified by the nomenclature developed in WASH-1400.[6] The list excludes sequences in which the ESS operate in the injection mode but fail during recirculation or any sequences in which the containment failure occurs due to floor meltthrough. It is not possible to extrapolate the previous results to such sequences since no data exists from the previous analyses.

TABLE V

ACCIDENT SEQUENCES FOR WHICH
UNCERTAINTIES CAN BE ESTIMATES

PWR Sequences	BWR Sequences
TMLB′-δ	ADE-β
TMLB′-γ	ADE-γ
TMLB′-α	ADF-β
SB-δ	ADF-γ
SB-γ	AC-α
SB-α	S_1DE-β
AB-δ	S_1DE-γ
AB-γ	S_1DE-β
AB-α	S_1DF-γ
ACD-α	S_1C-β
AG-α	S_1C-γ
AG-δ	TW-γ
AG-γ	AW-γ
SG-δ	AW-β
SG-α	S_1W-γ
SG-γ	S_1-β
SCD-α	
SCD-δ	
SCD-γ	

The recommended values for the uncertainty in accident consequences, in terms of the standard deviation, are given in Table VI for category 1 through 4 releases as identified in WASH-1400. Lower category radionuclide release uncertainties cannot be estimated from the data in Tables II to IV without introducing significant uncertainty due to the extrapolation process.

TABLE VI

RECOMMENDED UNCERTAINTY GUIDELINES
FOR CATEGORY 1-4 RELEASE FOR
ACCIDENT SEQUENCES IN TABLE 4

Category	I_2	Cs	Standard Deviation			
			Te	Sr	Ru	La
1	0.20	0.50	0.40	0.10	0.10	0.02
1	0.20	0.50	0.40	0.10	0.10	0.02
3	0.15	0.40	0.40	0.05	0.05	0.03
4	0.10	0.10	0.10	0.02	0.01	0.003

It is recommended that future work include additional uncertainty analyses for low consequence accidents and accident sequences in which some ESS operate, the development of a methodology to quantify the extrapolation of the results of uncertainty analyses of several accident sequences to additional sequences not previously analyzed and an uncertainty and sensitivity analysis of the CRAC code.

ACKNOWLEDGEMENT

This work was supported by the Nuclear Regulatory Commission under Contract No. MPO B-87930-A-S.

REFERENCES

1. P. Baybutt, D. Cox, R. Kurth, "Methodology for Uncertainty Analysis of Light Water Reactor Meltdown Consequences, report to NRC, NRC FIN No. 44067, 1981.

2. P. Baybutt and R. Kurth, "Uncertainty Analysis of Light Water Reactor Meltdown Consequences: Methodology Development", Topical Report from BCL to NRC, 1978.

3. P. Baybutt, D. Cox, and R. Kurth, "Further Uncertainty Analysis of Light Water Reactor Consequences and the Development of Accident Sequence Uncertainty Signatures", in preparation, to be submitted to NRC.

4. R. O. Wooton and H. Auci, "MARCH (Meltdown Accident Response Characteristics) Code Description and User's Manual", NUREG/CR-1711 (BMI-2064), 1980.

5. G.E.P. Box and J. S. Hunter, "The 2^k-p Fractional Factorial Designs Part I", Technometrics, 3, 1961.

6. Reactor Safety Study, "An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants", WASH-1400 (NUREG-75/014), 1975.

TRANSIENT FISSION PRODUCT RELEASE DURING DRYOUT IN OPERATING UO_2 FUEL

I.J. Hastings, C.E.L. Hunt, J.J. Lipsett and R.G. Gray

Atomic Energy of Canada Limited - Research Company
Chalk River Nuclear Laboratories
Chalk River, Ontario K0J 1J0

ABSTRACT

We have irradiated an instrumented stainless-steel-clad UO_2 fuel element, with upper and lower gas lines attached, at a linear power of about 55 kW/m to about 80 MW.h/kg U. During normal operation, fuel central, peripheral and sheath temperatures were about 1700, 800 and 300°C, respectively. During three transients initiated during the test, the corresponding ranges of temperatures were 2000-2300, 1100-1400 and 500-700°C, for dryout times up to 40 min.

During normal and transient operation, short-lived xenons and kryptons were swept from the element by a carrier gas and measured by gamma-ray spectrometry. During the most severe transient, fission product release was about 1.8% of inventory, with maximum release during re-wet and a concurrent reactor trip. Despite the thermal shock, the fuel pellets maintained reasonable integrity. No iodines were measured at the spectrometer during normal or transient operation.

INTRODUCTION

The release of activity from UO_2 fuel elements, as a result of sheath failure, is an important consideration in reactor safety programs. Therefore, there is a need to determine the inventory of active species released from the fuel to the fuel-to-sheath gap, and subsequently available for escape. Such data are also necessary for code verification. The periods of short-lived fission product release to the fuel-to-sheath gap are:

(i) release during normal operation of the fuel, including periods of power changes, startups and shutdowns, and

(ii) release during temperature transients resulting from off-normal or accident conditions.

Most studies reported in the literature refer to normal fuel operation. Generally, reported tests have been carried out on small single crystal and sintered UO_2 samples heated by an in-reactor furnace; the temperature range covered is typically 150-2000°C. Useful data on the diffusion behaviour of the short-lived xenons, kryptons and iodines have been obtained [1,2]. More recent tests have used

short operating elements containing UO_2 pellets. For example, U.K. work [3] utilized a stainless-steel-clad three-pellet capsule with a maximum fuel central temperature of about 1200°C. Early French studies [4] and more recent ones in the CONTACT series [5,6] have used elements at linear powers up to 40 kW/m to 350 MW.h/kg U. In a Halden experiment [7] 1.28 m long fuel rods have been irradiated at up to 30 kW/m. Recent experiments [8,9] at Chalk River Nuclear Laboratories (CRNL) have examined directly the short-lived fission product release from operating, full-length (500 mm) CANDU-type elements at linear powers of 45 and 60 kW/m.

Data on transient release are less common. Some initial work was carried out at CRNL [10]. However, transient and accident fission product releases have usually been studied by out-reactor simulated transients on irradiated UO_2 fuel (for example, [11-13]), as well as simulated and in-reactor work on mixed-oxide LMFBR fuel (for example, [14-16]).

In this paper we give results of an experiment in which we directly measured the release of short-lived fission products within an operating, intact UO_2 fuel element during normal and dryout operation, and during subsequent re-wet/reactor trip conditions.

EXPERIMENTAL

We have irradiated an instrumented stainless-steel-clad UO_2 element, with upper and lower gas lines attached, at a linear power of about 55 kW/m to about 80 MW.h/kg U in the X-4 experimental loop of the NRX Reactor at CRNL. The experimental designation is FIO-133. Table I gives fuel characteristics and operating conditions. Thermocouples measured temperatures at the fuel centre and periphery, sheath, flow tube, and coolant.

The test operated normally for about two months, during which time the fuel assembly was cooled with pressurized water. We then initiated three dryout transients over a one month period. Prior to and following each dryout test, stable steam-water (fog) cooling was established. During the transients, the element was cycled into dryout for times up to about 40 min by controlling the coolant water flow. Re-wet was achieved by re-introducing coolant water flow. During the final dryout test, re-wet was accompanied by a planned reactor trip.

During normal and dryout operation, the gaseous fission products released from the fuel were swept from the element by a He-2% H_2 stream via the upper gas line to a sample chamber outside the loop, where they were measured directly by gamma spectrometry. Note that the fuel pellets were grooved to permit easy gas flow. The resultant data were then processed to obtain activity concentrations and hence release rates from the fuel. The gas mixture was stored in delay tanks to allow decay of fission products, and released via the stack exhaust system. We have previously used the technique successfully in normal operation tests [8].

RESULTS AND DISCUSSION

Normal Operation

During normal operation at about 55 kW/m, we measured fuel peripheral and sheath temperatures of 800 and 300°C respectively. The central thermocouple was not

operative during this period, but we calculated a temperature of about 1700°C from a fuel performance model. During steady state operation, we only observed release of short-lived xenons and kryptons.

To obtain the data, release rates were averaged over 24 h at steady state. Corrections were made to release, R, for recoil and precursor effects. Release for Xe-135 was plotted against effective decay constant (λ), which accounts for loss due to neutron capture. We did not directly observe any iodines or bromines. In our experimental arrangement, the limit of detectability for iodines is about 1% of the release to the fuel-sheath gap. Since no iodines were directly measured, we conclude that less than 1% of the gap inventory was released as a volatile, such as CH_3I. As previously [8,9] we have deduced the iodine behaviour from the decay of I-133 and I-135 to Xe-133 and Xe-135, respectively during reactor shutdowns. The shutdown behaviour is characterized by a prompt decrease in release, followed by a decay period. The initial drop is due to xenon, and the decay is characteristic of iodine, presumed to be deposited on fuel or sheath surfaces.

Figure 1 shows results with release fraction R/B (released/born) plotted against λ or effective λ for xenons and kryptons observed during steady state operation of the test at 55 kW/m. During normal operation, release followed a $\lambda^{-0.5}$ relationship. Gap inventories inferred for I-133 and I-135 were 8 and 4 GBq (0.2 and 0.1 Ci), respectively. R/B for I-131 inferred from extrapolation is about 3×10^{-4}, corresponding with an equilibrium gap inventory of 10 GBq (0.3 Ci). We believe the straight-line extrapolation produces a conservative result for I-131. The $\lambda^{-0.5}$ relationship corresponds with diffusion kinetics, and is consistent with results from previous steady state experiments [8], also shown in Figure 1. These suggest release by athermal diffusion from the fuel surface, with only a weak dependence of fuel rating up to about 55 kW/m. In addition, Figure 1 shows the increase in R/B which accompanied establishment of fog cooling prior to the dryout transients, with a concurrent linear power increase from 55 to 60 kW/m.

Transient Operation

The first temperature transient was restricted to moderate fuel temperatures to assess the impact of changes in temperature on release rates. The transient lasted approximately 20 min, with a maximum sheath thermocouple temperature of 510°C and a maximum peripheral fuel temperature of 1120°C. We calculated a central temperature of about 2000°C. Transient release results were complicated by two reactor trips which accompanied the approach to the transient. We have thus concentrated our analysis on the two subsequent transients. Activity release rates during the first transient were about 20-30% above those measured during steady operation.

The second transient was more severe, and was of about 50 min duration. Of this time, about 40 min was under dryout, with sheath temperatures above 350°C. The sheath and peripheral fuel temperatures reached maxima of 700 and 1400°C respectively. The fuel central thermocouple also operated intermittently, registering a maximum temperature of 2300°C, close to the value we predicted for this type of transient. Figure 2 shows the spectrometer count rate combined with representative curves of the sheath and peripheral fuel temperatures as functions of time during the transient. The data can be divided into three stages. In the initial stage, which extended from about 1350 h to about 1410 h, the loop coolant conditions were changed to establish fuel dryout and thus to obtain the desired fuel temperatures. In this stage there was a series of transient releases superimposed on a generally rising count rate. During the second stage, which extended from about 1410 h to about 1425 h, the fuel temperature was held approximately constant. The release rate, about an order of magnitude higher than that for normal operation, peaked early in this stage and then decreased monotonically. The initial increase in

release rate is attributed to the fission product gases diffusing to the swept volume more rapidly with increasing temperature. Since, however, the fission product production rate is constant, the release rate eventually decreases.

The major releases occurred as transient pulses in the third stage of the test during the re-wet and cooling of the fuel, with release rates about three orders of magnitude higher than normal over a five min period. These pulses correlated well with the temperature reduction steps. At the last stage of re-wet, there was a major release that caused the spectrometer to saturate. Following this, the count rate decayed to a new steady-state value that was 30 times greater than the original steady-state count rate. Typical steady-state conditions were re-established after three days of further operation.

Figure 3 shows total spectrometer count rate combined with representative curves for sheath and peripheral fuel temperatures for the third transient. Temperatures achieved were comparable with those in the second, but time to maximum temperature was reduced from 20 min to five min. In the 27 min transient, about 25 min was under dryout conditions. The three-stage release process was again observed, with initial release pulses in the shorter temperature rise time at rates about 100 times that just prior to the transient. A major activity release, with a rate about four orders of magnitude greater than that prior to the transient, accompanied the re-wet and reactor trip, which would have induced a more severe thermal shock than that of the second transient re-wet alone.

Though we had a significant iodine inventory at the fuel-sheath gap, only short-lived xenons and kryptons were observed during all three transients, as for normal operation. No iodine or bromines were measured at the spectrometer. We infer that the iodine is securely bound on fuel surfaces, or on the internal sheath surface. Data for the gaseous fission products from the second (constant temperature) stage of the second and third transients suggest that R/B changed to a λ^{-1} relationship, which is the release of a stored inventory. Table II gives the isotopic releases during the two transients, obtained by integration of the measured release rates over the indicated time periods. We define the transient release as a percentage of the isotopic inventory within the fuel element. In our isotopic release data we consider three periods during the transients: (i) temperature increase, (ii) steady temperature and (iii) re-wet or re-wet with a concurrent reactor trip. From Figures 2 and 3, dryout coincided with the initial rapid increases in sheath temperatures above 350°C. This increase occurred about four min into transient 2, and less than one min into transient 3. All period (ii) was under dryout. The criterion for completion of transient 2 was when the short-lived kryptons stabilized to their new steady-state value; in transient 3 the completion criterion was when the short-lived kryptons ceased to be released. During the dryout portion of the second transient, release was about 0.1% of inventory; release during re-wet was about 0.6% of inventory. During the third transient, the corresponding releases were 0.1% and 1.5% of inventory, respectively. From Table II, all individual releases in transients 2 and 3 are consistent, except that for Xe-135m, where the values are higher. We attribute this anomaly to the contributing effect of the comparatively long-lived I-135 precursor. Note that activity release during a normal reactor shutdown is typically about a factor of five to 10 less than measured during the transients.

During the shutdown following the final reactor trip we again followed the decay behaviour of the iodine daughters Xe-133 and Xe-135. I-133 and I-135 gap inventories obtained from the delayed shutdown component of these xenons were 500 GBq and 250 GBq (15 and 8 Ci), respectively. The I-131 inventory extrapolated from these values is 650 GBq (20 Ci). We infer this increase in iodine inventory accompanied the fuel cracking from thermal shock; however no iodines were measured at the spectrometer. Following removal of the test section a germanium spectrometer was used to measure for iodine deposits on 0.5 m of gas-line, 2 m downstream of the fuel element. An insignificant 0.02 GBq (500 μCi) was measured [9].

Figure 4 shows the as-sectioned fuel after the final re-wet and reactor trip, (a) fuel bottom (first area re-wet), and (b) fuel mid section (later re-wet). Despite the severe thermal shock of re-wet and a concurrent reactor trip, with a temperature of about 300°C achieved in about 30 s from dryout, the fuel pellets have maintained reasonable integrity. Vigorous tapping of the as-sectioned element did not dislodge the fuel. Cracking in Figure 4(a) is more severe, particularly circumferentially, than normally observed following a reactor shutdown; that in 4(b) is closer to that normally observed. Detailed metallographic examination is continuing. Preliminary post-irradiation O/U values of pellets close to the carrier gas inlet, and at the fuel stack mid-section were 2.030 $\pm$ 0.005 and 2.005 $\pm$ 0.005 respectively; starting O/U of the fuel was 2.005 $\pm$ 0.005. We do not believe this degree of localized oxidation contributed significantly to our release values; further analysis is planned.

CONCLUSIONS

1. During normal operation at about 55 kW/m, fuel central, peripheral and sheath temperatures were about 1700, 800 and 300°C, respectively. Under these conditions, steady-state release followed a $\lambda^{-0.5}$ relationship and was consistent with that observed in previous tests.

2. Three dryout transients, up to 40 min in duration, were completed during the test; ranges of fuel central, peripheral and sheath temperatures achieved were 2000-2300, 1100-1400 and 500-700°C.

3. Only xenons and krytons were measured at the spectrometer during normal, dryout and rewet/trip operation; no iodines or bromines were observed.

4. Maximum release occurred during the re-wet and reactor trip stages; integrated release during the third transient with re-wet and reactor trip was about 1.8% of inventory.

5. Despite thermal shock accompanying the final re-wet and reactor trip, the fuel pellets maintained reasonable integrity.

ACKNOWLEDGEMENTS

This study was funded by CANDEV, a co-operative development program funded by Atomic Energy of Canada Limited, Ontario Hydro and other Canadian utilities with Nuclear Programs.

We acknowledge significant contributions to the program from P. Anderson, L.R. Bourque, R.D. Delaney, A. English, P.J. Fehrenbach, R. Lavoie, D.H. Rose, C.A. Wills and A.R. Yamazaki.

We also acknowledge excellent co-operation from NRX Reactor Branch Staff.

REFERENCES

[1] C.A. FRISKNEY, et al., "The Characteristics of Fission Gas Release From Monocrystalline Uranium Dioxide During Irradiation", J. Nucl. Mater. 68, 186 (1977).

[2] C.A. FRISKNEY and J.A. TURNBULL, "The Characteristics of Fission Gas Release From Uranium Dioxide During Irradiation", J. Nucl. Mater. 79, 184 (1979).

[3] C.J. GREATLY and R. HARGREAVES, "The Measured Emission of Fission-Product Gases From Operating UO_2 Fuel", J. Nucl. Mater. 79, 235 (1979).

[4] P. CHENEBAULT and R. DELMAS, "Emission Des Gaz De Fission Par L'Oxyde D'Uranium Dans Les Elements Combustibles", IAEA Publication, IAEA-PL-463/196, p. 337 (1974).

[5] M. BRUET, et al., "CONTACT 1 and 2 Experiments: Behaviour of PWR Fuel Rod up to 15000 $MW.d.tU^{-1}$", IAEA Specialists' Meeting on Water Reactor FUel Element Computer Modelling, Blackpool, U.K., 1980 March 17-21, IAEA Report IWGFPT/7(1980).

[6] M. CHARLES, et al., "Utilization of 'CONTACT' Experiments to Improve the Fission Gas Release Knowledge in PWR Fuel Rods", IAEA Specialists' Meeting on Water Reactor Fuel Element Performance Computer Modelling, Preston, U.K., 1982 March 15-19.

[7] A.D. APPELHANS and J.A. TURNBULL, "Measured Release of Radioactive Xenon, Kryton and Iodine From UO_2 During Nuclear Operation and a Comparison with Release Models", Eighth Water Reactor Safety Research Information Meeting, Gaithersburg, Maryland, 1980 October 27-31.

[8] I.J. HASTINGS, C.E.L. HUNT, J.J. LIPSETT, and R.D. MacDONALD, "Behaviour of Short-Lived Fission Products Within Operating UO_2 Fuel Elements", IAEA Specialists' Meeting on Water Reactor Fuel Element Performance Computer Modelling, Preston, U.K., 1982 March 15-19, to be published Res. Mechanica.

[9] J.J. LIPSETT, I.J. HASTINGS, and C.E.L. HUNT, "Behaviour of Short-Lived Iodines in Operating UO_2 Fuel Elements", 3rd Annual Meeting Canadian Nuclear Society, 1982 June 8-9, to be published in Proceedings. Also available as Atomic Energy of Canada Limited, report AECL-7721 (1982).

[10] F.R. CAMPBELL, R. DESHAIES and M.J.F. NOTLEY, "Transient Fission Gas Release Rates Within UO_2 Fuel Elements Following Power Changes", Atomic Energy of Canada Limited, report AECL-4912 (1974).

[11] G. BANDYOPADHYAY, "Fuel and Fission Gas Response to Simulated Thermal Transients: Experimental Results and Correlation with Fission Gas Release and Swelling Model", Nucl. Tech. 40, 62 (1978).

[12] G. BANDYOPADHYAY, "Response of Oxide Fuel to Simulated Thermal Transients", Nucl. Tech. 41, 349 (1978).

[13] J. REST, "The Prediction of Transient Fission Gas Release and Fuel Microcracking Under Severe Core Accident Conditions", Nucl. Tech. 56, 553 (1982).

[14] R.A. LORENZ, D.O. HOBSON and G.W. PARKER, "Fuel Rod Failure Under Loss-of-Coolant Conditions in TREAT", Nucl. Tech. 11, 502 (1971).

[15] E.R. FISHER, "Analysis of Experimental Fission Gas Behavioural Data in Fast Reactor Fuel Under Steady State and Transient Conditions", EURFNR-1464 (1977).

[16] E.H. RANDKLEV and C.A. HINMAN, "Fission Gas Behaviour in Mixed Oxide Fuel During Transient Overpower and Simulated Loss-of-Flow Tests", Int. Conf. Fast Breeder Reactor Performance, Monterey, CA, 1979 March.

FUEL DESCRIPTION	
Sintered UO_2 density (Mg/m^3)	10.64
Enrichment, U-235 in U(wt%)	1.38
Pellet diameter (mm)	18.06
Pellet length (mm)	19.05
Pellet grooves	
Number	three
Depth (mm)	1.5
Width (mm)	1.0
Stack length (mm)	378.0
End Discs	
Material	304L Stainless Steel
Thickness (mm)	1.09
Diameter (mm)	18.06
SHEATH DESCRIPTION	
Material	304L Stainless Steel
Outside diameter (mm)	19.81
Wall thickness (mm)	0.81
INSTRUMENTATION	
Thermocouples	6 Sheath 3 Fuel Periphery (1.5 mm from fuel surface) 1 Fuel Central 2 Flow tube 2 Coolant
IRRADIATION CONDITIONS (NORMAL)	
NRX Test Loop	X-4
Coolant Condition	Pressurized Water
Coolant Pressure (MPa)	8.5
Coolant Flow (kg/s)	0.24
Inlet Temperature (°C)	260.0
ELEMENT OPERATION (NORMAL)	
Linear heat output (kW/m-Av.)	55.0
$\int \lambda d\theta$ (kW/m)	4.5
Heat output (kW)	22.4
Surface heat flux (kW/m^2)	960.0
Discharge burnup (MW.h/kgU)	80.0

TABLE I Fuel characteristics and operating conditions, test FIO-133.

PERIOD	INCREASING TEMPERATURES	STEADY HIGH TEMPERATURE	REWET*
Integration Time(s)	810	1520	1130
Isotope (% Release)			
Xe-133	0.03	0.08	N.A.
Xe-135	0.03	0.11	0.70
Xe-135m	0.09	0.35	1.15**
Xe-138	0.03	0.09	0.44
Xe-137	0.05	0.15	0.22
Kr-85m	0.03	0.09	0.57
Kr-88	0.02	0.08	0.40
Kr-87	0.04	0.11	0.70
Average	0.04	0.13	0.60

(a)

PERIOD	INCREASING TEMPERATURES	STEADY HIGH TEMPERATURE	REWET PLUS REACTOR TRIP*
Integration Time(s)	190	1090	480
Isotope			
Xe-133	0.14	0.06	1.2
Xe-135	0.14	0.11	1.4
Xe-135m	0.19	0.42	2.5
Xe-138	0.10	0.09	1.3
Xe-137	0.10	0.17	1.2
Kr-85m	0.16	0.07	1.4
Kr-88	0.11	0.10	1.0
Kr-87	0.15	0.10	1.6
Average	0.14	0.14	1.5

(b)

*These values include 47% and 54% corrections for transients 2 and 3, respectively, to account for the period of spectrometer saturation.
**Long-lived precursor.

Table II Isotopic releases for transients (a) 2 and (b) 3.

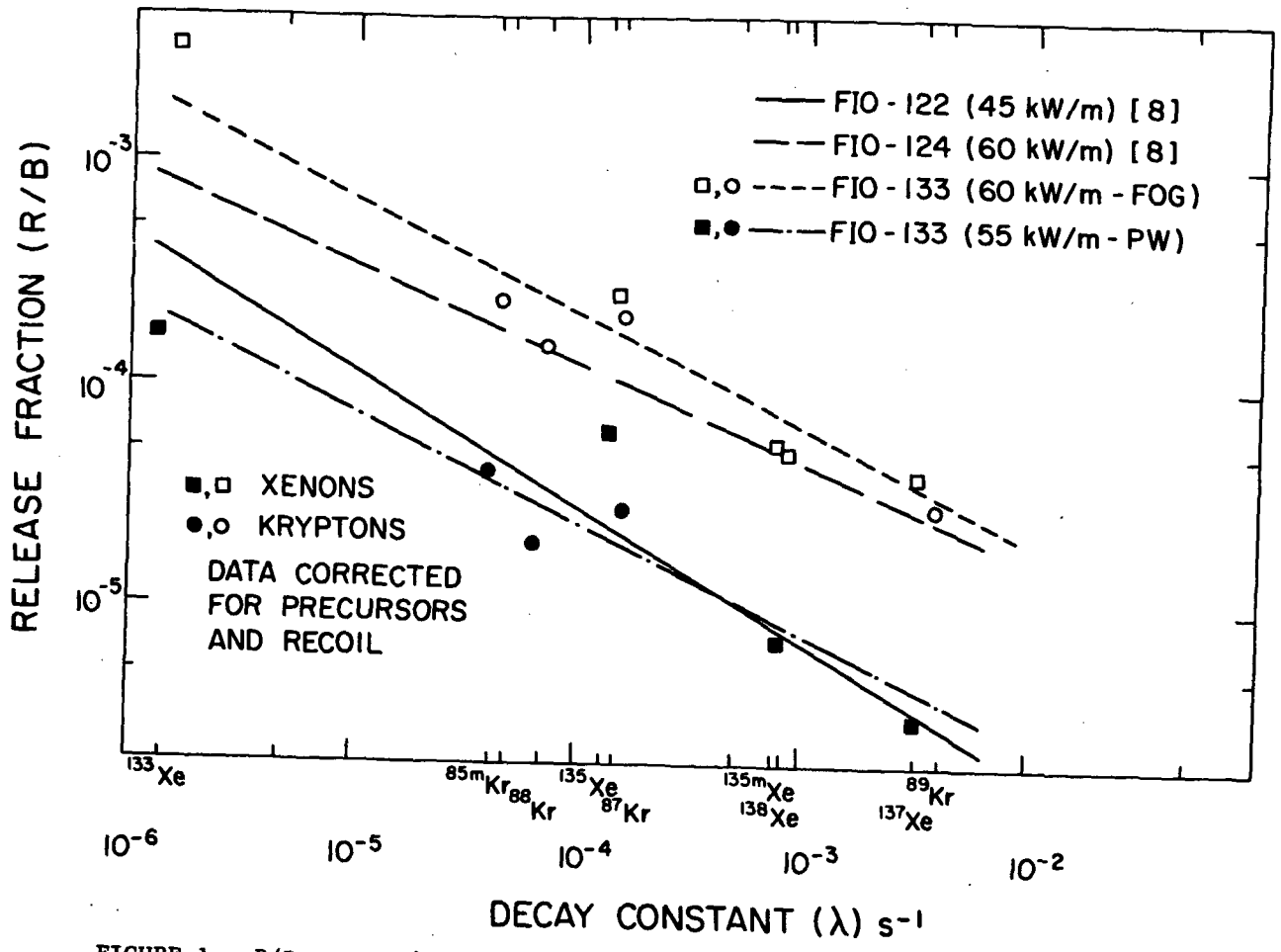


FIGURE 1 R/B versus λ or effective λ for observed xenons and kryptons during normal pressurized water (PW) operation at 55 kW/m, and for fog operation at 60 kW/m. Best fit results from previous tests [8] at 45 and 60 kW/m are included for comparison.

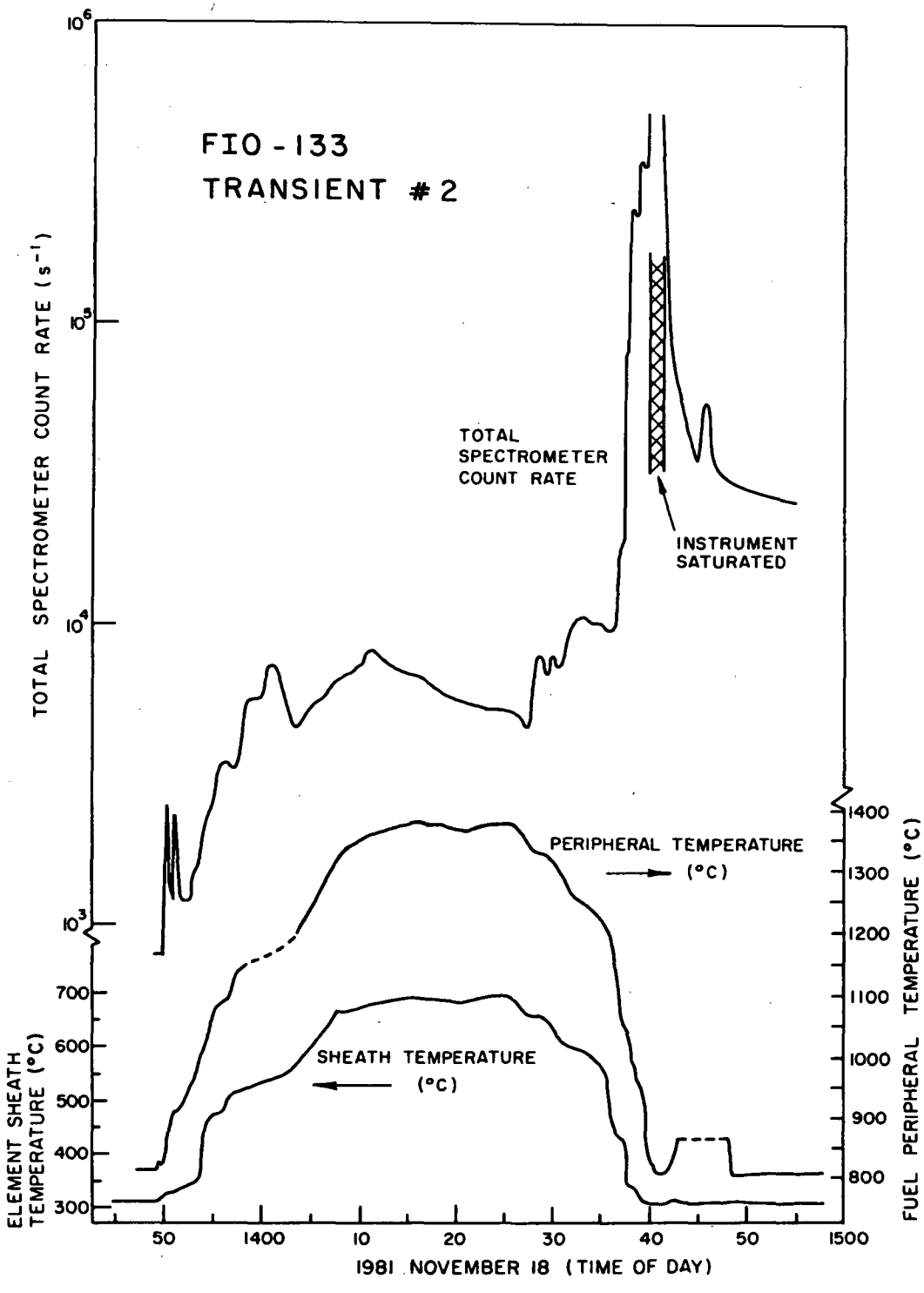


FIGURE 2 Spectrometer count rate with sheath and fuel temperatures for the second transient.

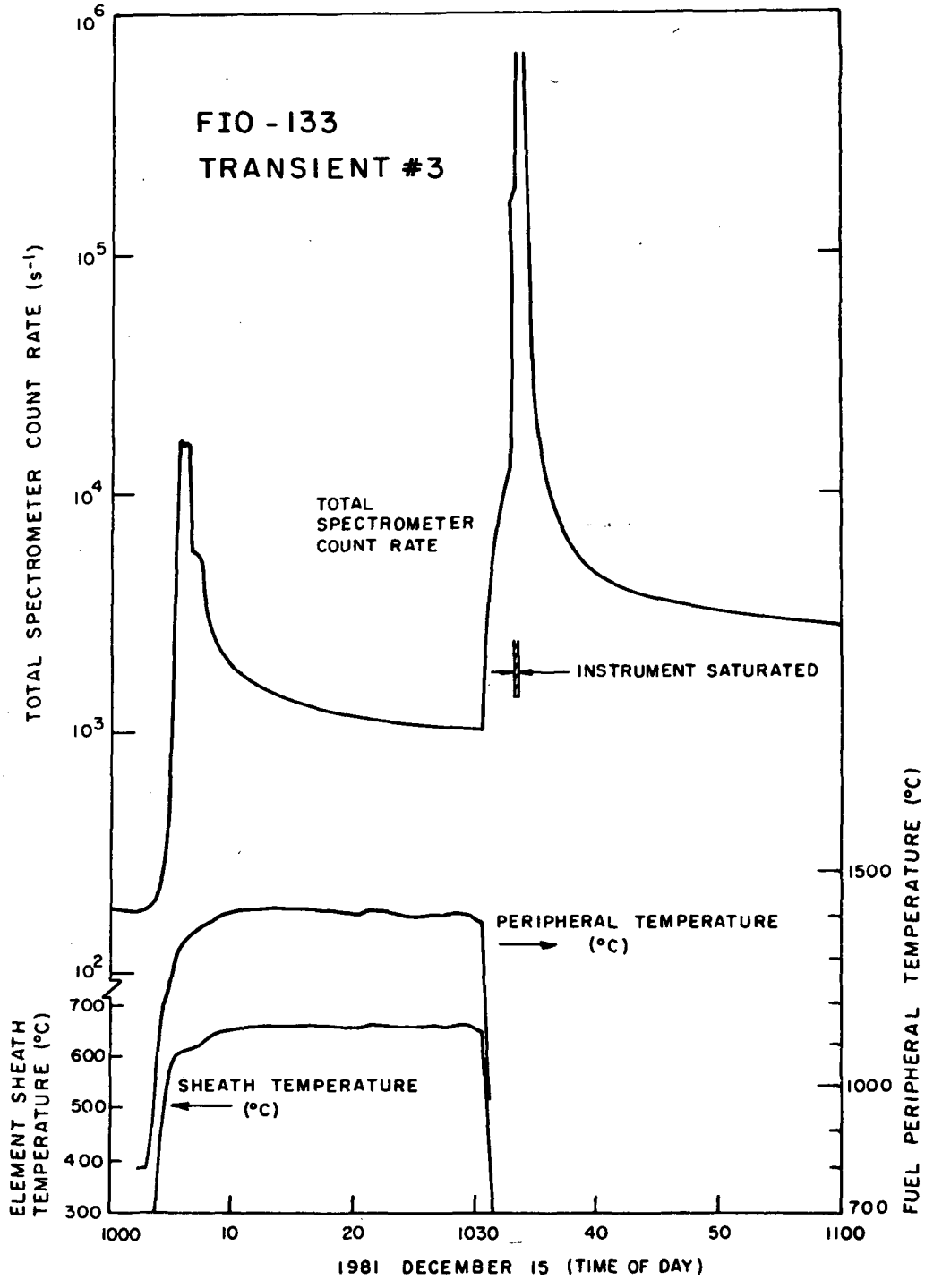
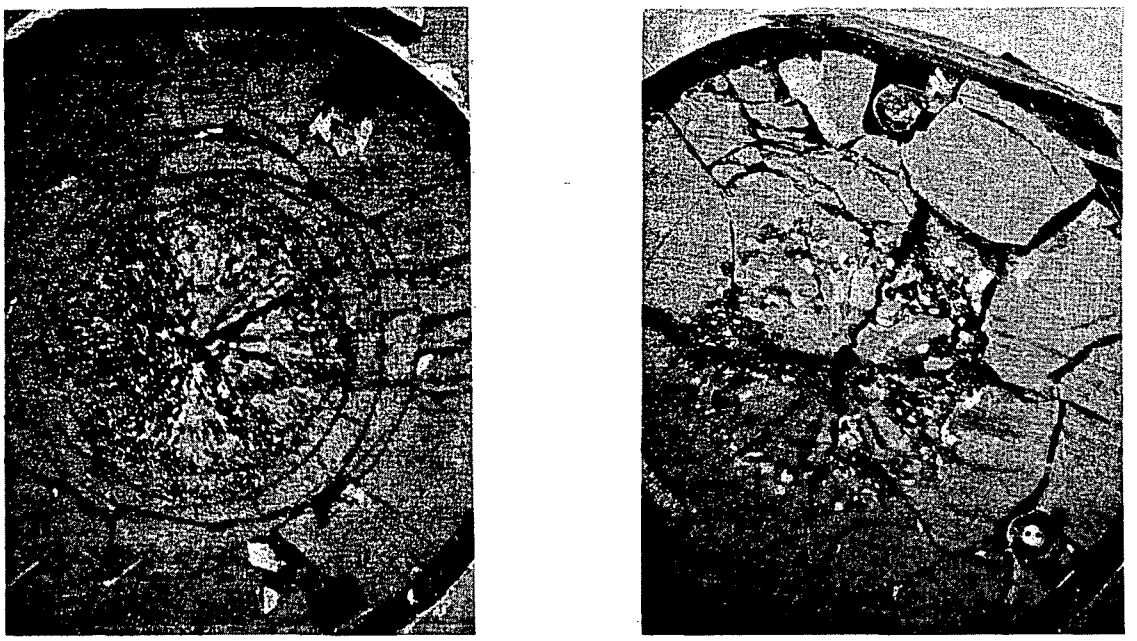


FIGURE 3 Spectrometer count rate with sheath and fuel temperatures for the third transient. Note that scales differ from those in Figure 2.



(a) (b)

FIGURE 4 As-sectioned fuel following final re-wet and reactor trip, (a) fuel bottom (first area re-wet), (b) fuel mid-section (later re-wet).

FISSION PRODUCT SOURCE TERMS MEASURED DURING FUEL DAMAGE TESTS IN THE POWER BURST FACILITY[a]

D. J. Osetek, J. J. King, and R. M. Kumar

EG&G Idaho, Inc.
Idaho Falls, Idaho 83415 U.S.A.

ABSTRACT

Fission product release from light-water-reactor-type fuel rods to the coolant was measured during eight fuel damage tests in the Power Burst Facility. On-line gamma spectroscopic measurements of short-lived fission products, and important aspects of fission product behavior observed during the tests, are discussed. The fission product source terms were found to be very time dependent, requiring 1 to 3 hours for equilibrium levels to be established. Estimates of the release rate constants generated during certain tests are provided. A comparison is made between calculated and measured release signatures for selected isotopes. Iodine behavior is discussed, and fuel fracturing is identified as a strong release mechanism that may substantially contribute to fission product source terms during light-water-reactor accidents where the core is damaged but the fuel does not melt.

INTRODUCTION

One of the greatest uncertainties remaining in reactor safety analysis is the magnitude and timing of fission product release during severe accidents. Definition of accident source terms requires an understanding of the release and transport processes that control fission product behavior. Measurements during simulated accident tests at the Power Burst Facility (PBF) are contributing to the fission product behavior data base.[1-3] Some important out-of-pile experiments are also being conducted to define fission product behavior.[4,5]

This paper summarizes the fission product release from eight severe transient experiments with light-water-reactor-type fuel performed in the PBF. Five of the tests were reactivity initiated accident (RIA) experiments[6-8] in which the test fuel was exposed to a range of natural power bursts representative of control rod ejection accidents. Two of the tests were power cooling mismatch (PCM) experiments[9,10] in which the test fuel was operated at power in film boiling for extended periods. The eighth test (Test PR-1) was a combination PCM-RIA experiment[11] in which the test fuel was exposed to three power bursts following a series of film boiling transients. Most of the tests were conducted with fresh fuel rods; however, two of the four rods in Test RIA 1-1 and all nine rods in Test RIA 1-4 were previously irradiated to ∿5400 MWd/t in a prototype pressurized water reactor. Each test included a fuel

a. Work supported by the U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, under DOE Contract No. DE-AC07-76ID01570.

preconditioning period of several hours. Fuel rod failure and fission product release were noted in each of the tests. Table I summarizes the important test parameters and resulting fuel conditions for each test. The measured fission product behavior is described below in terms of release fraction histories, equilibrium release fractions, and best-estimate release rate constants.

FISSION PRODUCT RELEASE FRACTIONS

Fission product concentrations measured in the test loop coolant with the on-line gamma spectrometer increased rapidly upon fuel failure in each test, and then continued to increase for 1 to 3 h after failure. Since the concentration of most fission products is dependent on parent decay in the coolant as well as release from the fuel, it is useful to convert the measured concentrations to the release quantities and relate these to the total quantity of the fission products present in the test. Thus, the release fraction and its time dependence can be used to describe fission product behavior independent of the test specific inventories. Use of the release fraction accounts for the complicating factors of parent decay and varying total inventory, and permits quantitative comparison between the different isotopes and between different experiments.

The time-dependent behavior of 15 to 30 isotopic release fractions have been documented for each of the eight PBF tests. The ORIGEN[12] code was used to calculate the total, time-dependent fission product inventories for each test. Although the time dependent release is important for estimating dynamic source terms, the equilibrium or maximum release fractions can be used to describe the general results. The results are divided into two groups. Relative equlibrium release fractions measured during Tests PCM-1, RIA ST-1, RIA ST-2, and RIA ST-4 are reported in Table II. Absolute equilibrium release fractions measured during Tests RIA 1-1, RIA 1-4, PR-1, and PCM-7 are reported in Table III. The relative release fractions were developed by dividing each measured release fraction by the largest value determined in each test. This was necessary because there was a large uncertainty in the efficiency of the spectrometer during these first four tests.

The relative equilibrium release fractions listed in Table II indicate the qualitative behavior of fission products during the four tests listed. Noble gas isotopes were released in large fractions in these tests, but iodine isotopes behaved differently in tests with and without fuel melting. Larger fractions of iodine were measured in the coolant following Tests RIA ST-1 and RIA ST-2, in which extensive fuel fracturing was produced. Much smaller fractions of iodine were found in the coolant following Tests PCM-1 and RIA ST-4, in which higher temperatures were achieved and fuel melting was prevalent. This result suggests that iodine is held up by deposition or reaction during high temperature, fuel melt conditions. Large fractions of alkali metal isotopes were measured following each test listed in Table II. The release fractions of the less volatile alkaline earth and rare earth isotopes measured during the RIA tests range widely over approximately three orders of magnitude. This variation is the result of strong precursor influences on the behavior of daughter isotopes during burst-type tests with fresh fuel. Less variation is noted in the nonvolatile fission product release fractions measured during Test PCM-1, because the longer duration of the PCM transients diminishes the influence of precursors on fission product release.

The absolute equilibrium release fractions measured during the four tests listed in Table III indicate generally larger release fractions for most isotopes in the RIA tests. The release fractions measured during Tests PR-1 and PCM-7 are generally smaller. Again, this phenomenon is believed to be due to the influence of precursor isotopes, which are generally more volatile and present in larger percentages during RIA transients than during PCM transients. Closer agreement exists among the isotopic release fractions of the low volatility elements (Ba, La, Ce).

TABLE I. PBF TEST PARAMETERS AND FUEL DAMAGE CHARACTERISTICS

Test	Transient	Number of Failed Rods	Rod[a] Fragmentation (%)	Fuel[b] Fracturing	Fuel Loss[c] (%)	Fuel Melt (%)
PCM-1	15 min in film boiling	1	38	Extensive	24	25
RIA ST-1	250 cal/g power burst[d]	1	17	Extensive	10	0
RIA ST-2	260 cal/g power burst[d]	1	28	Extensive	15	0
RIA ST-4	350 cal/g power burst[d]	1	90	Extensive	1	90
RIA 1-1	285 cal/g power burst[d]	4	48	Extensive	8.5	1
RIA 1-4	262 cal/g power burst[d]	9	1	Limited	0	1
PR-1	$\leq$26 min in film boiling plus three power bursts of 107,144 and 212 cal/g[d]	3	20	Extensive	6	1-10
PCM-7	$\leq$27 min in film boiling	7	20	Limited	1	1

a. Portion of failed rod's length sustaining visible fracturing.

b. Separation of fuel grains at grain boundaries.

c. Portion of test fuel washed out of test train and potentially influencing gamma spectroscopic measurements.

d. Radial average fuel enthalpy at the axial flux peak.

The effect of prior irradiation on fission product release cannot be conclusively determined from the PBF results. Test RIA 1-4 with irradiated fuel produced release fractions slightly smaller than the other RIA tests and data less scattered in magnitude. The mean value for noble gas release fractions in Test RIA 1-4 with irradiated fuel is 0.25 ± 0.11, and for other RIA tests with previously unirradiated fuel the mean value is 0.53 ± 0.27. However, the Test RIA 1-4 irradiated rods were not damaged nearly as much as the previously unirradiated rods were during the other RIA tests.

FISSION PRODUCT RELEASE RATES

The equilibrium release fractions reported in Tables II and III were determined at long times following fuel failure and are limited in usefulness because they are quite unique to the fuel behavior developed during the PBF tests. Single-valued, equilibrium release fractions are not sufficient to describe the dynamic source terms expected during reactor accidents. Time dependent release rate constants are not well known, and the only data base available[13] consists of smoothed curves describing temperature-dependent release rate constants determined in simple out-of-pile tests. The dependence of release rate constants on fuel fracturing, liquifaction, oxidation, and other parameters is not known. The PBF in-pile tests can be used to assess the magnitude of these release rate constants under typical accident conditions and, thus, estimate the combined effect of all parameters on release rate constants.

Realizing that the release rate constants are time dependent and that the radioisotope inventory in a reactor changes rapidly following scram, prediction of the dynamic source terms is a very complex calculation. Available computer codes, such as ORIGEN2,[14] separately track each decay chain and partition the fission product inventory into released and retained fractions using release rate constants. As

TABLE II. FISSION PRODICT RELEASE FRACTIONS TO THE PBF TEST LOOP COOLANT

Isotope	Relative Release Fraction			
	Test PCM-1	RIA ST-1	RIA ST-2	RIA ST-4
^{85m}Kr	1.00 ± 0.07	--[a]	--[a]	--[a]
^{87}Kr	$9.2 \pm 0.8 \times 10^{-1}$	$5.5 \pm 1.5 \times 10^{-1}$	$4.4 \pm 0.6 \times 10^{-1}$	$2.6 \pm 0.3 \times 10^{-1}$
^{88}Kr	$9.3 \pm 0.7 \times 10^{-1}$	$4.9 \pm 0.6 \times 10^{-1}$	$4.6 \pm 0.8 \times 10^{-1}$	$6.2 \pm 0.8 \times 10^{-1}$, [b]
^{88}Rb	$9.0 \pm 0.7 \times 10^{-1}$	$6.4 \pm 0.9 \times 10^{-1}$	$6.3 \pm 1.2 \times 10^{-1}$	$8.1 \pm 1.0 \times 10^{-1}$, [b]
^{89}Rb	$2.0 \pm 0.1 \times 10^{-2}$	$5.6 \pm 1.1 \times 10^{-1}$	$6.7 \pm 1.0 \times 10^{-1}$	$1.8 \pm 0.2 \times 10^{-1}$, [b]
^{131m}Te	--[a]	--[a]	--[a]	--[a]
^{132}Te	--[a]	--[a]	--[a]	--[a]
^{133}Te	--[a]	--[a]	--[a]	--[a]
^{134}Te	--[a]	--[a]	--[a]	--[a]
^{131}I	--[a]	$2.3 \pm 0.3 \times 10^{-1}$	--[c]	$4.8 \pm 0.9 \times 10^{-2}$
^{132}I	$1.2 \pm 0.1 \times 10^{-2}$	$2.3 \pm 0.2 \times 10^{-1}$	--[c]	$5.3 \pm 0.7 \times 10^{-2}$
^{133}I	$1.7 \pm 0.1 \times 10^{-2}$	$2.1 \pm 0.2 \times 10^{-1}$	$3.4 \pm 0.8 \times 10^{-1}$	$4.2 \pm 0.6 \times 10^{-2}$
^{134}I	$1.5 \pm 0.1 \times 10^{-2}$	$3.2 \pm 0.4 \times 10^{-1}$	$3.6 \pm 0.6 \times 10^{-1}$	$6.4 \pm 0.8 \times 10^{-2}$
^{135}I	$2.4 \pm 0.7 \times 10^{-2}$	$6.2 \pm 0.9 \times 10^{-1}$	--[c]	$5.6 \pm 0.7 \times 10^{-2}$
^{133}Xe	--[a]	--[a]	--[a]	--[a]
^{133m}Xe	--[a]	--[a]	--[a]	--[a]
^{135}Xe	$8.6 \pm 0.5 \times 10^{-1}$	$1.5 \pm 0.2 \times 10^{-1}$	$3.0 \pm 0.6 \times 10^{-1}$	$8.2 \pm 1.0 \times 10^{-1}$, [b]
^{138}Xe	$8.6 \pm 0.7 \times 10^{-1}$	$7.5 \pm 1.1 \times 10^{-1}$	1.00 ± 0.14	$8.5 \pm 1.1 \times 10^{-1}$
^{137}Cs	--[a]	--[a]	--[a]	--[a]
^{138}Cs	$1.5 \pm 0.4 \times 10^{-1}$	$4.3 \pm 0.4 \times 10^{-1}$	$5.5 \pm 0.8 \times 10^{-1}$	$4.5 \pm 0.6 \times 10^{-1}$
^{139}Cs	$2.0 \pm 0.4 \times 10^{-2}$	$7.5 \pm 1.5 \times 10^{-1}$	1.3 ± 0.3[d]	$1.9 \pm 0.2 \times 10^{-1}$
^{139}Ba	$7.5 \pm 1.3 \times 10^{-3}$	$6.2 \pm 0.4 \times 10^{-1}$	$8.7 \pm 1.6 \times 10^{-1}$	$5.2 \pm 0.7 \times 10^{-1}$
^{140}Ba	--[a]	$1.3 \pm 0.2 \times 10^{-1}$	--[c]	$2.1 \pm 0.3 \times 10^{-2}$
^{141}Ba	$2.4 \pm 0.3 \times 10^{-3}$, [e]	$3.2 \pm 0.4 \times 10^{-1}$	$6.7 \pm 0.8 \times 10^{-1}$	$4.0 \pm 0.4 \times 10^{-1}$
^{142}Ba	--[a]	$3.1 \pm 0.6 \times 10^{-1}$	$6.6 \pm 1.0 \times 10^{-1}$	$4.7 \pm 0.6 \times 10^{-1}$
^{140}La	--[a]	$1.3 \pm 0.2 \times 10^{-1}$	--[c]	$2.1 \pm 0.2 \times 10^{-2}$
^{142}La	$1.9 \pm 0.4 \times 10^{-3}$, [e]	1.00 ± 0.13	$6.9 \times 0.8 \times 10^{-1}$	1.0 ± 0.12
^{141}Ce	--[a]	--[a]	--[a]	--[a]
^{143}Ce	--[a]	--[a]	--[a]	$1.2 \pm 0.3 \times 10^{-2}$

a. Coolant concentrations below detectable levels.

b. In the time interval of the equilibrium release fraction, the values of the data points were generally monotonically increasing.

c. Background coolant concentrations for these nuclides released during RIAST-1, seven days earlier, overwhelmed the magnitude of nuclide releases occurring during RIAST-2.

d. These release fractions appear to represent a situation in which mixing was not complete.

e. These values should be interpreted as statistically marginal upper limits, since their presence was observed in only a few spectra.

f. Not corrected for ^{141}La interference.

g. Not corrected for ^{239}Np interference.

TABLE III. FISSION PRODUCT FRACTIONS TO THE PBF TEST LOOP COOLANT

Isotope	Absolute Release Fraction			
	RIA 1-1	RIA 1-4	PR-1	PCM-7
^{85m}Kr	$1.00^{+0}_{-0.15}$[e]	$2.9 \pm 0.4 \times 10^{-1}$	$8.1 \pm 0.9 \times 10^{-2}$	$2.1 \pm 0.3 \times 10^{-2}$
^{87}Kr	$2.8 \pm 0.5 \times 10^{-1}$	$3.2 \pm 0.4 \times 10^{-1}$	$1.6 \pm 0.1 \times 10^{-1}$	$2.3 \pm 0.3 \times 10^{-2}$
^{88}Kr	$3.0 \pm 0.6 \times 10^{-1}$	$2.9 \pm 0.4 \times 10^{-1}$	$6.1 \pm 0.8 \times 10^{-2}$	$1.7 \pm 0.3 \times 10^{-2}$
^{88}Rb	$3.3 \pm 0.6 \times 10^{-1}$	$2.7 \pm 0.4 \times 10^{-1}$	$6.3 \pm 0.8 \times 10^{-2}$	$1.9 \pm 0.3 \times 10^{-2}$
^{89}Rb	$3.4 \pm 0.6 \times 10^{-1}$	$1.3 \pm 0.2 \times 10^{-1}$	--[a]	$1.7 \pm 0.5 \times 10^{-2}$
^{131}Te	--[a]	--[a]	--[a]	$6.7 \pm 1.2 \times 10^{-2}$
^{131m}Te	--[a]	$8.6 \pm 1.5 \times 10^{-2}$	$1.3 \pm 0.2 \times 10^{-1}$	$8.8 \pm 1.2 \times 10^{-2}$
^{132}Te	--[a]	$2.1 \pm 0.3 \times 10^{-2}$	$2.0 \pm 0.3 \times 10^{-1}$	$9.3 \pm 1.2 \times 10^{-2}$
^{133}Te	--[a]	$9.3 \pm 1.3 \times 10^{-3}$	--[a]	$8.9 \pm 1.2 \times 10^{-2}$
^{134}Te	--[a]	$1.4 \pm 0.2 \times 10^{-2}$	$2.9 \pm 0.4 \times 10^{-1}$[g]	$4.8 \pm 0.7 \times 10^{-2}$
^{131}I	$4.5 \pm 0.8 \times 10^{-1}$	$2.8 \pm 0.4 \times 10^{-1}$	$9.1 \pm 1.1 \times 10^{-2}$	$2.9 \pm 0.4 \times 10^{-2}$
^{132}I	$4.3 \pm 0.7 \times 10^{-1}$	$1.4 \pm 0.2 \times 10^{-1}$	$9.7 \pm 1.2 \times 10^{-2}$	$3.9 \pm 0.5 \times 10^{-2}$
^{133}I	$3.9 \pm 0.8 \times 10^{-1}$	$9.5 \pm 1.3 \times 10^{-2}$	$6.8 \pm 0.8 \times 10^{-2}$	$2.8 \pm 0.4 \times 10^{-2}$
^{134}I	$2.4 \pm 0.5 \times 10^{-1}$	$5.3 \pm 0.7 \times 10^{-2}$	$9.2 \pm 1.2 \times 10^{-2}$	$2.1 \pm 0.3 \times 10^{-2}$
^{135}I	$2.7 \pm 0.5 \times 10^{-1}$	$1.5 \pm 0.2 \times 10^{-1}$	$6.1 \pm 0.7 \times 10^{-2}$	$2.4 \pm 0.3 \times 10^{-2}$
^{133}Xe	--[a]	$3.7 \pm 0.5 \times 10^{-1}$	$7.3 \pm 0.9 \times 10^{-2}$	$2.7 \pm 0.4 \times 10^{-2}$
^{133m}Xe	--[a]	$6.6 \pm 1.0 \times 10^{-2}$	--[a]	--[a]
^{135}Xe	$2.9 \pm 0.5 \times 10^{-1}$	$2.9 \pm 0.4 \times 10^{-1}$	$6.4 \pm 0.8 \times 10^{-2}$	$2.4 \pm 0.3 \times 10^{-2}$
^{138}Xe	$4.0 \pm 0.7 \times 10^{-1}$	$1.3 \pm 0.2 \times 10^{-1}$	--[a]	$2.0 \pm 0.3 \times 10^{-2}$
^{137}Cs	$6.5 \pm 1.4 \times 10^{-1}$[f]	$2.4 \pm 0.3 \times 10^{-1}$	$1.9 \pm 0.3 \times 10^{-1}$	--[a]
^{138}Cs	$2.7 \pm 0.5 \times 10^{-1}$	$1.1 \pm 0.2 \times 10^{-1}$	$5.6 \pm 0.7 \times 10^{-1}$	$1.7 \pm 0.3 \times 10^{-2}$
^{139}Cs	$3.2 \pm 0.6 \times 10^{-1}$	$1.5 \pm 0.2 \times 10^{-1}$	--[a]	$1.7 \pm 1.1 \times 10^{-2}$
^{139}Ba	$1.00^{+0}_{-0.33}$[d]	$1.0 \pm 0.2 \times 10^{-1}$	$5.1 \pm 0.9 \times 10^{-2}$	$1.2 \pm 0.4 \times 10^{-3}$
^{140}Ba	$1.5 \pm 0.3 \times 10^{-1}$	$6.1 \pm 1.0 \times 10^{-1}$	$5.1 \pm 0.7 \times 10^{-2}$	$4.9 \pm 0.7 \times 10^{-3}$
^{141}Ba	$5.2 \pm 1.0 \times 10^{-1}$	$3.1 \pm 0.4 \times 10^{-2}$	--[a]	--[a]
^{142}Ba	$1.5 \pm 0.4 \times 10^{-1}$	$1.8 \pm 0.3 \times 10^{-2}$	--[a]	--[a]
^{140}La	$2.2 \pm 0.4 \times 10^{-2}$	$2.6 \pm 0.3 \times 10^{-3}$	$3.7 \pm 0.4 \times 10^{-2}$	$5.9 \pm 0.8 \times 10^{-3}$
^{142}La	$2.0 \pm 0.4 \times 10^{-1}$	$1.2 \pm 0.2 \times 10^{-2}$	$9.3 \pm 1.5 \times 10^{-3}$	$8.1 \pm 1.1 \times 10^{-4}$
^{141}Ce	--[a]	$9.2 \pm 1.2 \times 10^{-3}$	$7.1 \pm 1.1 \times 10^{-4}$	$1.3 \pm 0.3 \times 10^{-3}$
^{143}Ce	$6.8 \pm 1.6 \times 10^{-3}$	$2.4 \pm 0.4 \times 10^{-3}$	$1.1 \pm 0.1 \times 10^{-4}$	$1.1 \pm 0.1 \times 10^{-3}$

Notes for Table II apply to Table III.

described in the recent NRC document[13] on fission product behavior during LWR accidents, dynamic source terms can be developed from equations of the form

$$\frac{dN_i^R}{dt} = -k_i(T)\, N_i^R \qquad (1)$$

where

N_i^R = inventory of nuclide i in a fuel element

$k_i(T)$ = temperature-dependent release rate constant of species i.

Equation (1), however, is strictly valid only for stable fission products with no radioactive parents. The important concern in reactor safety is the behavior of the radiologically significant fission product species which are born as members of radioactive decay chains. The inventory of fission products in a linear radioactive decay chain subsequent to reactor scram is given by the following coupled equations:

$$\frac{dN_i^R}{dt} = \alpha_{i-1}\,\beta_{i-1}\,\lambda_{i-1}\,N_{i-1}^R - (\lambda_i + k_i)\,N_i^R \qquad i = 2,3, \ldots \ell \qquad (2a)$$

where

α_{i-1} = decay branching factor of nuclide i-1 (parent of nuclide i)

β_{i-1} = release branching factor of nuclide i-1 = $\dfrac{\lambda_{i-1}}{\lambda_{i-1} + k_{i-1}}$

λ_{i-1} = decay constant of isotope i-1

N_{i-1}^R = inventory of nuclide i-1 in a fuel element

λ_i = decay constant of isotope i

k_i = release rate constant of nuclide i

ℓ = number of nuclei in a linear decay chain.

For i=1, Equation (2) reduces to

$$\frac{dN_1^R}{dt} = -(\lambda_1 + k_1)\,N_1^R \qquad (2b)$$

Prior to scram, Equation (2) is further complicated by the presence of generation-depletion terms due to fission and nuclear reactions; e.g., (n,γ), (n,α), (n,p), etc.

Using the exact analytical solutions of this set of equations and the appropriate physical constants for the various decay chains, release signatures were calculated for the same fission products measured during four PBF tests: RIA ST-4, RIA 1-1, RIA 1-4, and PCM-7. The input data were developed from the ORIGEN-generated inventories and assumed release rate constants, the latter of which were selected on the

basis of fuel temperatures produced during the tests, and the NUREG-0772[13] data base. Enhancement of the constants due to fuel fracturing was deemed necessary in certain instances. As a general rule, release rate constants were required to be largest for noble gases and decrease incrementally for the less volatile fission products. All isotopes of a given element were required to observe the same release rate constant in any time step and release rate constants were decreased exponentially in time. The inventory fractions remaining in the rod and accumulated in the coolant were calculated iteratively. Release rate constants were adjusted between calculations to force better agreement between the calculated and measured equilibrium release fractions. When convergence was established between the calculated and measured signatures, the results were considered to be best-estimate.

The release rate constants of the more volatile fission products (Kr, Xe, I, Cs) are larger than those of the lower volatility fission products (Ba, La, Ce) as expected. Figure 1 illustrates the time dependence of the best-estimate release constants for noble gases using data from Test RIA 1-1. The release rate constants estimated for the PBF tests include the result of fuel fracturing, fission product dissolution, and other fission product release processes in addition to the temperature-driven release rate constants reported in NUREG-0772. More accurate fission product release modeling will require better quantitative information on the effects of fracturing and the other processes on fission product release.

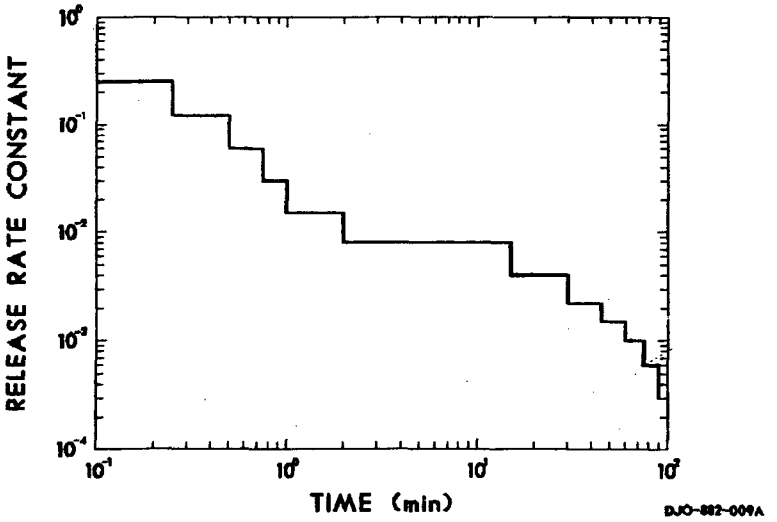


Fig. 1. Comparison of release rate constants for noble gas isotopes from NUREG-0772, and PBF Test RIA 1-1.

A comparison of calculated and measured release fractions for a few selected isotopes in Test RIA 1-1 is shown in Fig. 2. At longer times (>30 min), the calculated equilibrium release fractions agree reasonably well with the measurements. The disagreement between the predicted and measured release fractions during the first ∿30 min after fuel failure may be due to the hydrodynamic characteristics (incomplete mixing) of the PBF loop, which were not modeled in the calculated signature. This calculational technique is useful for order-of-magnitude estimates of release rate constants and can be beneficial for assessment of the fission product behavior data base and accident source term estimtes.

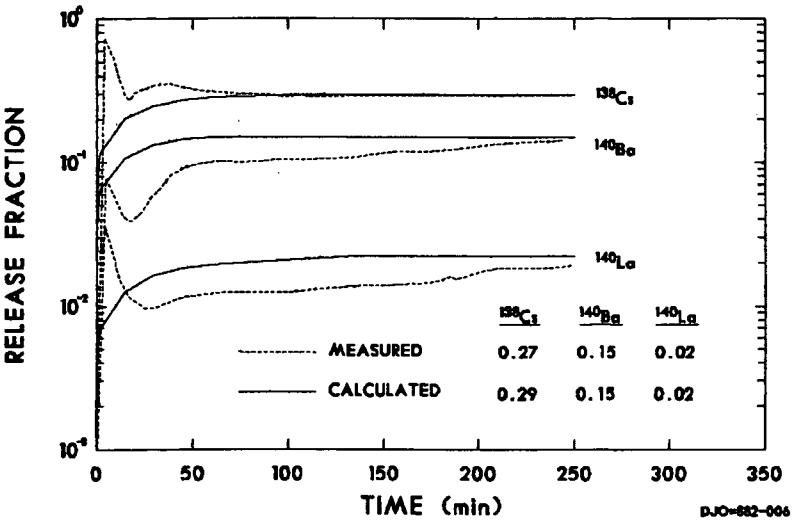


Fig. 2. Comparison of calculated and measured release fractions for PBF Test RIA 1-1.

CONCLUSION

Time-dependent fission product release has been measured during eight severe transient tests at the Power Burst Facility. A computer routine has been established to allow the fitting of calculated signatures to measured fission product data, and the best-estimate release rate constants developed using this model can be used to assess the current out-of-pile release rate data base.

Analysis of the fission product release measurements from the PBF tests indicate:

1. Large fractions of fission products can be released from nuclear fuel due to quench-induced fragmentation

2. Iodine appears to react or deposit during tests that produce fuel melting so that it is removed from the coolant and not measurable

3. Alkaline earth and rare earth isotopes, not expected to be volatile during most accidents, can be released during RIA tests because of the volatile nature of parent isotopes

4. By comparing calculated and measured release signatures, release rate constants were determined from the PBF data and were estimated to be larger than those predicted by fuel temperature alone. The difference is believed to be due to the influence of fuel fragmentation, fission product dissolution, and other controlling parameters.

The technique described in this paper for calculating dynamic source terms offers an improvement over previous methods of accident analysis. The time dependence of the inventory is important for tracking changes in the source term resulting from radioactive decay. The dependence of release rate on parameters other than temperature must be better defined, but the continued development of more accurate release rate constants will greatly improve accident analysis and source term definition.

REFERENCES

1. D. J. OSETEK and J. J. KING, "Fission Product Release from LWR Fuel Failed During PCM and RIA Transients," NUREG/CR-1674, EGG-2058, EG&G Idaho, Inc. (1980).

2. D. J. OSETEK, J. J. KING, and D. W. CROUCHER, "Fission Product Release Signatures for LWR Rods Failed During PCM and RIA Transients," in Proc. ANS/ENS Topical Meeting on Reactor Safety Aspects of Fuel Behavior, Am. Nucl. Soc., Sun Valley, Idaho, (1981) Vol. 2, pp. 446-457.

3. B. J. BUESCHER, D. J. OSETEK, and S. A. PLOGER, "Power Burst Facility Severe Fuel Damage Test Series," in Proc. ANS Conference on Fast, Thermal, and Fusion Reactor Experiments, Am. Nucl. Soc., Salt Lake City, Utah (1982).

4. R. A. LORENZ et al., "Fission Product Release from BWR Fuel Under LOCA Conditions," NUREG/CR-1773, ORNL/NUREG/TM-388, Oak Ridge National Laboratory (1981).

5. H. ALBRECHT, V. MATSCHOSS, and H. WILD, "Release of Fission and Activation Products During Light Water Reactor Core Meltdown," Nucl. Tech. 01, 46 (1979).

6. R. S. SEMKEN et al., "Reactivity Initiated Accident Test Series, RIA Scoping Tests Fuel Behavior Report," NUREG/CR-1360, EGG-2024, EG&G Idaho, Inc. (1980).

7. S. L. SEIFFERT et al., "Reactivity Initiated Accident Test Series, Test RIA 1-1 (Radial Average Fuel Enthalpy of 285 cal/g) Fuel Behavior Report," NUREG/CR-1465, EGG-2040, EG&G Idaho, Inc. (1980).

8. R. K. MCCARDELL, Z. R. MARTINSON, and P. E. MACDONALD, "Damage and Failure of Previously Irradiated Fuel Rods During a Reactivity Initiated Accident," in Proc. ANS/ENS Topical Meeting on Reactor Safety Aspects of Fuel Behavior, Am. Nucl. Soc., Sun Valley, Idaho, (1981) Vol. 1, pp. 509-524.

9. B. A. COOK, "Fuel Rod Material Behavior During Test PCM-1," NUREG/CR-0757, TREE-1333, EG&G Idaho, Inc. (1979).

10. F. S. GUNNERSON and D. T. SPARKS, "In-Pile Power-Cooling-Mismatch Testing of a Nine-Rod Fuel Assembly--Results of Test PCM-7," NUREG/CR-2303, EGG-2126, EG&G Idaho, Inc. (1981).

11. D. T. SPARKS et al., "Nuclear Fuel Rod Behavior During Normal and Abnormal Operating Conditions--Results of Test PR-1," NUREG/CR-2126, EGG-2102, EG&G Idaho, Inc. (1981).

12. M. J. BELL, "ORIGEN--The ORNL Isotope Generation and Depletion Code," ORNL-4268, Oak Ridge National Laboratory (1973).

13. U.S. Nuclear Regulatory Commission, "Technical Bases for Estimating Fission Product Behavior During LWR Accidents," NUREG-0772 (1981).

14. A. G. CROFF, "A Users Manual for the ORIGEN2 Computer Code," ORNL/TM-7175, Oak Ridge National Laboratory (1980).

SESSION 4

PRA-1; METHODS AND TECHNIQUES

Chair: W. Vinck *(CEC)*
W. Paskievici *(EPM)*

ASSEMBLING AND DECOMPOSING PRA RESULTS: A MATRIX FORMALISM

by

D. C. Bley, S. Kaplan, and B. J. Garrick
Pickard, Lowe and Garrick, Inc.
Irvine, California 92714

ABSTRACT

A matrix formalism has been an effective tool for the systematic assembly of the results of several U.S. PRAs--Zion, Indian Point, Midland, Oyster Creek, and Seabrook. Similarly, this same formalism has provided a comprehensive structure for decomposing final risk results into specific risk contributors. The contributors are examined at various levels of detail from release categories to systems and components including event sequences and administrative controls. The paper highlights the decomposition process with specific examples from a completed PRA.

Our approach to risk assessment begins with a deductive line of thought that leads to identification of possible initiating events. Next, we use the event tree method for organizing the possible scenarios which can emanate from any given initiating event. The "plant" event tree follows the scenarios up to the point where either the reactor is stabilized or plant damage has occurred. Now, as suggested in Fig. 1, a coalescence of scenarios or a "pinch point" in the analysis occurs (i.e., given that a certain state, y_j, of plant damage exists, the remainder, or downstream portion of the scenarios, is the same irrespective of how we arrived at that state).

The next portion of the scenarios is modeled by a "containment event tree" which follows their progress through the containment from the plant state to the occurrence or nonoccurrence of a release of radioactivity to the environment. The entry states to the containment event tree are the plant states; i.e., the exit states from the plant event tree.

The exit states from the containment are called "release categories," p_k, each of which specifies a certain quantity and mix of radioisotopes released. At this point, another coalescence occurs in that the effects in the environment of a given category of release are the same irrespective of the particular scenario that led to that release category.

The environmental effects are then studied by a "site model" which takes the release category as its input event, follows the movement of the radioactivity, and computes the final damage state, x_ℓ, in terms of public health impacts and property damage.

A matrix formalism [1] has been developed for the systematic assembly of the results from each phase of the analysis. It has been effectively applied in the quantification of several U.S. probabilistic risk assessments (PRAs)--Zion, Indian Point, Midland, Oyster Creek, and Seabrook. The formalism provides a simple and convenient method for revising final risk curves when modifications within any part of the analysis are being evaluated. An extension of the formalism yields a comprehensive diagnostic structure for decomposing final risk into specific risk contributors.

A key idea which makes the assembly process easy to understand is the recognition that an event tree may be regarded as equivalent to a transition matrix in the sense that the tree defines the likelihood of moving from various input conditions, or states, to various output states.

For example, in the plant event tree the entry states represent the various possible initiating events. The exit states represent various combinations of plant conditions, mainly pressure at time of core melt, containment conditions (spray, fan coolers, leakage paths), and time of core melt (measured from initiation of the incident). From the event tree itself, we may calculate the numbers

$$m_{ij} = \text{the conditional frequency of leaving the plant event tree in exit state } j \text{ given that initiating event } i \text{ has occurred.} \quad (1)$$

The set of these m_{ij} may now be regarded as constituting a matrix

$$M = \begin{bmatrix} m_{11} & m_{12} & m_{13} & \cdots \\ m_{21} & m_{22} & & \\ \vdots & & & \end{bmatrix} \quad (2)$$

which we call, naturally, the "plant matrix."

In a similar way from the containment event tree we can obtain a "containment matrix"

$$C = \left[c_{jk}\right] \quad (3)$$

where

$$c_{jk} = \text{the conditional frequency of emerging from the containment tree in exit state } k, \text{ given that we enter it in entry state } j. \quad (4)$$

Now the exit states from the containment tree are the various release categories, ρ_k. The entry states for the containment tree are by definition the exit states of the plant tree. Therefore, the matrix product MC gives the frequencies of transition from initiating event i to release category ρ_k. The site model, may be regarded as resulting in a "site matrix," S

$$S = [s_{k\ell}] \quad (5)$$

where

$$s_{k\ell} = \text{conditional frequency of damage level } x_\ell \text{ or greater occurring, given that a release in category } \rho_k \text{ has occurred.} \quad (6)$$

The variable x here stands for any of the damage indices, e.g., early deaths, thyroid cancers, etc. We presume in Eq. (5) that this variable has been discretized and in Eq. (6) use x_ℓ to denote one of the discrete values.

Now multiplying MC by S, we see that the product matrix, MCS, gives the frequencies of transition from initiating event i to damage state x_ℓ or greater.

We now introduce the row matrix

$$\phi^I = \left[\phi_1^I, \phi_2^I, \ldots \phi_i^I \ldots\right] \tag{7}$$

where

$$\phi_i^I = \text{the frequency of occurrence of initiating event i (measured in occurrences per reactor year).} \tag{8}$$

ϕ^I is called the "initiating event vector." The product of this row matrix ϕ^I by the rectangular matrix M yields a new row matrix ϕ^y.

$$\phi^y = \left[\phi_1^y, \phi_2^y, \ldots \phi_j^y\right] \tag{9}$$

related to ϕ^I by

$$\phi^y = \phi^I M \tag{10}$$

In expanded form, this relationship is

$$\phi_j^y = \sum_i \phi_i^I m_{ij} \tag{11}$$

Thus, in light of Eqs. (1) and (8),

$$\phi_j^y = \text{the frequency of plant damage state } y_j \text{ (in occurrences per reactor year).} \tag{12}$$

ϕ^y is therefore called the "plant state vector."

If this vector, in turn, is now multiplied by the containment matrix, we obtain the row matrix ϕ^o:

$$\phi^o = \phi^y C \tag{13}$$

$$\phi^o = \left[\phi_1^o, \phi_2^o, \ldots \phi_k^o \ldots\right] \tag{14}$$

where, by Eqs. (12) and (4),

$$\phi_k^o = \text{the frequency of release category } o_k \text{ (in occurrences per reactor year).} \tag{15}$$

ϕ^O is therefore referred to as the "release vector."

Finally, multiplying ϕ^O by S we obtain

$$\Phi^X = \phi^O S \tag{16}$$

where the row vector Φ^X

$$\Phi^X = \left[\Phi^X_1, \Phi^X_2, \ldots \Phi^X_\ell \ldots\right] \tag{17}$$

has in its ℓth position the quantity

$$\Phi^X_\ell = \text{the frequency, occurrences per reactor year, of occurrence of damage level } x_\ell, \text{ or greater.} \tag{18}$$

Φ^X is, in effect, a risk curve in frequency format, equivalent to the more familiar risk curve format of Fig. 2.

Substituting Eqs. (10) and (13) into Eq. (16), we obtain the relationship between Φ^X and ϕ^I as follows:

$$\Phi^X = \phi^I MCS \tag{19}$$

This equation shows how the results of the plant, containment, and site models are assembled with the initiating event frequencies to yield the risk curve. It is therefore called the "Master Assembly Equation." A diagram is given in Fig. 3 of the overall assembly process, showing the relationships between the various matrixes, the event trees, and the pinch points.

For a specific example of the matrices and the assembly process, we turn to the results of a recent PRA [2]. The ϕ^I, M, C, and S matrices are given in Tables I through IV. Then, the matrix products for the frequencies of plant states, release categories, and early fatalities are given in Tables V, VI, and VII. Note that the core melt frequency is the sum of the plant state (or release category) frequencies, 4.21×10^{-5} per reactor year.

An interesting set of diagnostic matrices can now be developed. First, we introduce diagonal forms of the row vectors ϕ^I, ϕ^Y, ϕ^O, and ϕ^S of frequencies as follows:

$$\phi^I_D = \begin{bmatrix} \phi^I_1 & & \\ & \phi^I_2 & \\ & & \ddots \end{bmatrix}$$

We can now form the product

$$\phi^I_D M = i \left[\quad \overset{j}{\downarrow} \quad \right]$$

The i,jth element of this matrix is the frequency of occurrence of plant state j as a result of initiating event type i. The column sums of this matrix lead to the vector ϕ^{Y}, which gives the frequency of entering each plant state. Thus, ϕ_D^{IM} is a diagnostic matrix for each plant state j; i.e., from it we can see exactly which initiating events i are contributing to the frequency ϕ_j^Y of plant state j.

A complete set of similar diagnostic matrixes can be constructed:

- $\phi_D^{I}MC$ - gives the contribution of each initiating event i to the frequency of each release category ρ_k.
- $\phi_D^{I}MCS$ - gives the contribution of each initiating event i to the frequency of exceeding damage level x_e.
- $\phi_D^{Y}C$ - gives the contribution of each plant state Y_j to the frequency of each release category ρ_k.
- $\phi_D^{Y}CS$ - gives the contribution of each plant state Y_j to the frequency of exceeding each damage level x_e.
- $\phi_D^{\rho}S$ - gives the contribution of each release category ρ_k to the frequency of exceeding each damage level x_e.

This set of diagnostics provides a powerful tool for decomposing and understanding the contributors to each risk measure: early fatalities, core melt, etc. It is possible to use many different combinations of the diagonal matrices in the decomposition process. We outline one rather straightforward approach below, identifying the contributors to early fatalities and core melt.

Let us begin by identifying the important release categories. Referring to Table VI, the core melt frequency is 4.21×10^{-5} per reactor year. Furthermore, the frequency of release category 8B is 4.17×10^{-5} or 99.1% of the total. Thus, sequences leading to category 8B are the dominant contributors to core melt.

Next, we examine health effects through the diagnostic matrix, $\phi_D^{\rho}S$ of Table VIII. If we take several cuts, say at 10, 100, 1,000, and 10,000 (or greater) fatalities, we find that categories 2 and 2R dominate the results.

Now for the dominant release categories 2, 2R, and 8B, we can identify the contributing plant states by scanning the diagnostic matrix $\phi_D^{Y}C$ (Table IX). For those plant states, we can find the dominant initiating events from ϕ_D^{IM} (Table X). From these displays, we identify the dominant contributors as follows:

Release Category	2	ϕ_V^I
	2R	ϕ_{11b}^I - TE
	8B	ϕ_3^I - SLFC, ϕ_1^I - ALFC, ϕ_2^I - ALFC, ϕ_7^I - SEFC, ϕ_{11a}^I - SEFC

It is now a simple matter to return to the particular plant event trees and identify the key sequences contributing to the important plant states. For example, ϕ_3^I - SLFC, the leading contributor to core melt, is a small LOCA with failure of high pressure recirculation cooling. Also, ϕ_{11b}^I - TE, an important contributor to early fatalities is due to loss of offsite power (and load), failure of onsite AC power, failure to recover power, and failure of auxiliary feedwater. The details of the plant analysis are preserved in simple summary tables. For the ϕ_S^I (small LOCA - SLFC contribution), Table XI shows that the dominant sequence is sequence 2 in which all AC buses are available and failure occurs at branch point R-2. From Table XII we see that R-2 stands for failure of high pressure recirculation.

This sequence occurs 4.55×10^{-4} for every small LOCA event and leads to core damage state SLFC, which is a symbol for a late melt with fan coolers and containment sprays working. To dig deeper, we consult the cause table (Table XIII) and find that approximately 40% of the unreliability of the recirculation system results from possible failure of the operator to initiate switchover. Only about 25% comes from hardware problems.

Thus, the real value of a risk assessment lies in uncovering the contributors to risk and establishing a basis for controlling and thereby managing risk. The ultimate reason for doing a risk analysis is that there is an underlying decision (or many decisions) to be made. The decision analysis then forms the context for the risk analysis. The risk analysis provides vital input to the decision analysis but is not itself the same as the decision analysis. A complete decision requires not only an assessment of risk but also an assessment of costs and benefits. Most importantly, these assessments must be done for each available option.

Thus, if the decision is whether to grant an operating license, the benefits of the plant must be considered, its contribution to the health and well being of the people in its service area, its contribution to the economy of the region, and its potential contribution to cleaning up the environment. Similarly, the costs and risks of doing without electric power, or of replacing it with another source, must also be considered.

Areas of opportunity for reduction of risk may take the form of specific plant components, personnel training, procedures, safeguards, or containment, or they may be site related such as evacuation routes or emergency plans. The plant and site specific risk models are designed to accommodate the next level of analysis--the decision analysis of candidate fixes.

REFERENCES

1. Kaplan, S., "A Matrix Theory Formalism for Event Tree Analysis - Application to Nuclear Risk Analysis," Reliability Engineering, August 1981.

2. "Zion Probabilistic Safety Study," Commonwealth Edison Company, "Internal Events" and early fatalities only, September 1981.

TABLE I

Initiating Event Frequency Vector ϕ^I

1 Large LOCA	2 Medium LOCA	3 Small LOCA	4 Steam Generator Tube Rupture	5 Steam Break Inside Containment	6 Steam Break Outside Containment	11c Turbine Trip, Loss of Service Water	12 Spurious Safety Injection	13 Reactor Trip	V Interfacing System LOCA
ϕ^I = [9.4E-4	9.4E-4	3.5E-3	2.4E-2	9.4E-4	9.4E-4	9.4E-4	6.3E-1	3.7	1.0E-7]

TABLE II

Plant Matrix M

Initiating Event	Plant Event Sequence Category SE/C	SEF	SEC	SE	SLF/C	SLF	SLC	SL	TEF/C	TEF	TEC	TE	AEC	AL	VE
1 Large LOCA:	0	0	0	0	0	0	0	0	0	0	0	0	3.77-7	2.6E-10	0
2 Medium LOCA:	0	0	0	0	0	0	0	0	0	0	0	0	4.6E-8	8.1E-12	0
3 Small LOCA:	8.5E-7	2.8E-8	2.8E-7	3.6E-9	6.8E-8	3.0E-8	2.3E-6	2.7E-8	0	0	0	0	0	0	0
4 Steam Generator Tube Rupture:	4.2E-13	2.0E-17	8.6E-17	2.1E-10	1.9E-14	1.5E-13	1.0E-16	8.8E-10	6.6E-6	4.5E-9	2.3E-6	2.0E-7	0	0	0
5 Steam Break Inside Containment:	7.4E-7	5.2E-11	1.5E-10	4.6E-12	2.6E-6	3.9E-9	2.2E-6	1.9E-8	6.6E-7	2.3E-10	1.1E-7	1.0E-8	0	0	0
6 Steam Break Outside Containment:	7.4E-7	5.2E-11	1.1E-10	2.0E-11	2.6E-6	3.1E-9	1.1E-6	1.5E-8	6.4E-7	1.6E-10	5.7E-6	6.5E-8	0	0	0
7 Loss of Main Feedwater:	7.5E-7	4.9E-11	3.1E-10	2.0E-11	2.6E-6	6.1E-12	2.6E-10	2.0E-10	6.5E-8	1.0E-10	5.9E-8	1.7E-9	0	0	0
8 Trip of One MSIV:	0	0	0	0	1.7E-9	3.1E-12	1.3E-10	1.0E-11	1.4E-8	1.0E-10	5.9E-8	6.4E-8	0	0	0
9 Loss of RCS Flow:	6.7E-7	4.4E-11	2.8E-10	2.5E-11	2.5E-6	2.8E-9	1.1E-6	2.2E-8	3.3E-6	9.3E-11	5.4E-6	5.0E-8	0	0	0
0 Core Power Excursion	9.8E-14	6.8E-10	4.0E-17	3.7E-10	4.0E-15	8.1E-10	3.4E-17	1.4E-17	4.6E-15	1.3E-17	7.5E-16	8.4E-15	0	0	0
11a Turbine Trip:	7.4E-7	5.2E-11	3.1E-10	2.0E-11	2.5E-6	6.3E-12	2.6E-10	2.1E-10	6.6E-8	1.0E-10	6.2E-8	7.2E-9	0	0	0
11b Turbine Trip, Loss of Offsite Power:	1.0E-7	5.6E-12	1.3E-12	6.3E-9	1.1E-8	6.4E-12	7.1E-14	8.9E-10	1.0E-7	9.9E-12	2.5E-13	3.4E-6	0	0	0
11c Turbine Trip, Loss of Service Water:	0	0	7.4E-7	5.2E-8	0	0	3.5E-8	2.4E-8	0	0	2.4E-8	3.5E-7	0	0	0
12 Spurious Safety Injection:	7.5E-7	5.1E-11	1.5E-10	6.8E-12	2.6E-6	3.8E-9	2.2E-6	3.0E-9	3.9E-8	1.6E-10	1.1E-7	1.0E-8	0	0	0
13 Reactor Trip	0	0	0	0	1.7E-9	3.3E-12	1.3E-10	1.0E-11	6.5E-8	1.0E-10	6.2E-8	1.2E-8	0	0	0
V Interfacing Systems LOCA:	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1.0

NOTES: 1. Mean values for conditional frequency of entering each Plant Event Sequence Category given that a specific initiating event has occurred

2. The Plant Event Sequence Categories are defined in Section 1.3.4.0, briefly:

A - Large LOCA behavior
S - Small LOCA behavior
T - Transient behavior
E : Early Melt
L : Late Melt
F - Fan Coolers are operating
C - Containment Sprays are operating

TABLE III

Containment Matrix C

Plant State	Release Category Z-1	2	2R	Z-3	5R	Z-5	6	7	8A	8B	2RV
SEFC	0.	1.000E-04	0.	1.781E-07	1.309E-04	8.985E-35	0.	1.740E-04	3.	9.998E-01	0.
SEF	1.781E-07	1.899E-04	1.309E-04	0.	0.	0.	1.740E-04	0.	9.998E-01	9.	0.
SEC	0.	1.000E-04	0.	1.781E-07	1.309E-04	8.985E-35	0.	1.740E-04	3.	9.998E-01	0.
SE	2.186E-06	1.997E-04	9.998E-01	0.	0.	0.	1.300E-04	0.	1.300E-04	3.	0.
SLFC	0.	1.000E-04	0.	9.084E-06	1.309E-04	8.985E-35	0.	1.740E-04	0.	9.995E-31	0.
SLF	9.084E-06	1.899E-04	1.309E-04	0.	0.	0.	1.740E-04	0.	9.995E-01	0.	0.
SLC	0.	1.003E-04	0.	9.084E-06	1.309E-04	8.985E-35	0.	1.740E-04	0.	9.995E-31	0.
SL	2.186E-06	1.997E-04	9.998E-01	0.	0.	0.	1.300E-34	0.	1.000E-04	3.	0.
TEFC	0.	1.000E-04	0.	9.797E-08	1.027E-04	9.982E-35	0.	1.899E-04	3.	9.995E-01	0.
TEF	9.797E-06	1.999E-04	1.027E-04	0.	0.	0.	1.899E-04	0.	9.995E-01	3.	0.
TEC	0.	1.000E-04	0.	9.797E-08	1.027E-04	9.982E-05	0.	1.899E-04	0.	9.995E-01	0.
TE	2.186E-06	1.999E-04	9.998E-01	0.	0.	0.	1.300E-04	0.	1.300E-04	0.	0.
AEFC	0.	1.000E-04	0.	1.979E-06	1.499E-04	1.998E-10	0.	1.499E-04	3.	9.998E-31	0.
AEF	1.979E-06	1.000E-04	1.499E-04	0.	3.	0.	1.499E-34	0.	9.998E-01	3.	0.
AEC	0.	1.000E-04	0.	1.979E-06	1.499E-04	1.998E-10	0.	1.499E-04	3.	9.998E-01	0.
AE	1.000E+00	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.
ALFC	0.	1.000E-04	0.	1.979E-06	9.993E-05	2.204E-10	3.	1.899E-04	3.	9.995E-01	0.
ALF	1.979E-06	1.003E-04	9.999E-05	0.	3.	0.	1.893E-34	3.	9.995E-01	3.	0.
ALC	0.	1.000E-04	0.	1.979E-06	9.993E-05	2.204E-10	0.	1.899E-04	0.	9.995E-01	0.
AL	1.000E+00	0.	0.	0.	0.	0.	0.	0.	3.	3.	0.
VE	0.	1.000E+00	0.	0.	0.	0.	3.	0.	0.	3.	0.

TABLE IV

Site Matrix S^T (S Transposed) for Early Fatalities

Number of Fatalities	Release Category Z-1	2	2R	Z-3	5R	Z-5	6	7	8A	8B	2RV
1.083E+00	1.067E-01	3.472E-02	1.042E-02	2.083E-02	0.				3.	0.	0.
2.000E+00	1.563E-01	1.477E-02	2.042E-02	2.292E-02	0.				0.	0.	0.
3.030E+00	1.563E-01	3.472E-02	1.042E-02	2.083E-02	0.				0.	0.	0.
5.000E+00	1.133E-01	1.472E-02	1.042E-02	2.083E-02	0.				0.	0.	0.
7.000E+00	1.458E-01	2.778E-02	1.042E-02	2.083E-02	0.				0.	0.	0.
1.033E+01	1.354E-01	2.778E-02	1.042E-02	2.083E-02	0.				0.	0.	0.
2.000E+01	2.135E-01	2.431E-02	1.042E-02	2.083E-02	0.				0.	0.	0.
3.053E+01	9.375E-02	1.431E-02	1.042E-02	2.083E-02	0.				0.	0.	0.
5.000E+01	6.771E-02	2.431E-02	1.042E-02	2.083E-02	0.				0.	0.	0.
7.000E+01	6.250E-02	1.042E-02	1.042E-02	2.083E-02	0.				0.	0.	0.
1.000E+02	4.514E-02	1.389E-02	1.042E-02	2.083E-02	0.				0.	0.	0.
2.033E+02	5.167E-02	1.389E-02	1.042E-02	2.083E-02	0.				0.	0.	0.
3.000E+02	4.167E-02	1.389E-02	6.944E-03	2.083E-02	0.				0.	0.	0.
5.033E+02	3.125E-02	1.389E-02	6.944E-03	2.083E-02	0.				0.	0.	0.
7.000E+02	3.125E-02	1.389E-02	6.944E-03	2.083E-02	0.				0.	0.	0.
1.000E+03	2.083E-02	6.944E-03	6.944E-03	2.083E-02	0.				0.	0.	0.
2.033E+03	1.389E-02	6.944E-03	6.944E-03	2.083E-02	0.				0.	0.	0.
3.000E+03	1.042E-02	6.944E-03	3.472E-03	1.042E-02	0.				0.	0.	0.
5.000E+03	1.000E-03	1.000E-03	0.		0.				0.	0.	0.
7.000E+03	2.000E-04	1.000E-03	1.000E-03		0.				0.	0.	0.
1.020E+04	2.000E-04	1.000E-04	1.000E-04		0.				0.	0.	0.
2.000E+04	2.000E-04	1.000E-04	0.		0.				0.	0.	0.
3.082E+04	0.	0.	0.		0.				0.	0.	0.
5.020E+04	0.	0.	0.		0.				0.	0.	0.
7.000E+04	0.	0.	0.		0.				0.	0.	0.

TABLE V

$\phi^{Y} = \phi^{I}_{M}$

Plant State	Frequency
SEFC	7.41-6
SEF	1.28-9
SEC	1.76-8
SE	6.53-10
SLFC	1.91-5
SLF	4.76-9
SLC	1.93-6
SL	1.25-8
TEFC	8.43-7
TEF	1.61-9
TEC	9.32-7
TE	2.27-7
AEFC	1.75-6
AEF	1.87-10
AEC	8.23-9
AE	1.05-11
ALFC	9.76-6
ALF	7.27-10
ALC	3.98-10
AL	2.52-13
V	1.05-7
Total (Core Melt)	4.21-5

TABLE VI

$\phi^{\rho} = \phi^{I}_{MC}$

Release Category	Frequency
Z-1	1.132E-11
2	1.092E-7
2R	2.401E-7
Z-3	2.153E-10
5R	5.147E-9
Z-5	2.734E-11
6	4.714E-11
7	7.405E-9
8A	8.494E-9
8B	4.173E-5
2RV	0.0
Total (Core Melt)	4.21E-5

TABLE VII

$\phi^{x} = \phi^{I}_{MCS}$

Number of Fatalities	Frequency
1.000E+00	6.332E-09
2.000E+00	6.332E-09
3.000E+00	6.332E-09
5.000E+00	6.332E-09
7.000E+00	5.574E-09
1.000E+01	5.574E-09
2.000E+01	5.195E-09
3.000E+01	5.195E-09
5.000E+01	5.194E-09
7.000E+01	4.814E-09
1.000E+02	4.057E-09
2.000E+02	4.056E-09
3.000E+02	3.217E-09
5.000E+02	3.217E-09
7.000E+02	2.458E-09
1.000E+03	2.449E-09
2.000E+03	2.449E-09
3.000E+03	1.608E-09
5.000E+03	3.506E-10
7.000E+03	3.506E-10
1.000E+04	3.506E-11
2.000E+04	1.093E-11
3.000E+04	2.273E-15
5.000E+04	0.0
7.000E+04	0.0

TABLE VIII

$\phi^{\rho}_{D}S$ (Transposed)

Number of Fatalities	Total	Release Category										
		Z-1	2	2R	Z-3	5R	Z-5	6	7	8A	8B	2RV
1.000E+00	9.331E-07	1.695E-12	3.791E-07	2.314E-09	4.469E-12	0.	1.699E-11	0.	0.	0.	0.	0.
2.000E+00	9.331E-07	1.695E-12	3.791E-07	2.314E-09	4.469E-12	0.	1.699E-11	0.	0.	0.	0.	0.
3.000E+00	9.331E-07	1.695E-12	3.791E-07	2.314E-09	4.469E-12	0.	1.699E-11	0.	0.	0.	0.	0.
5.000E+00	9.331E-07	1.695E-12	3.791E-07	2.314E-09	4.469E-12	0.	1.699E-11	0.	0.	0.	0.	0.
7.000E+00	9.331E-07	1.695E-12	3.791E-07	2.314E-09	4.469E-12	0.	1.699E-11	0.	0.	0.	0.	0.
1.000E+01	9.331E-07	1.695E-12	3.791E-07	2.314E-09	4.469E-12	0.	1.699E-11	0.	0.	0.	0.	0.
2.000E+01	9.331E-07	1.695E-12	3.791E-07	2.314E-09	4.469E-12	0.	1.699E-11	0.	0.	0.	0.	0.
3.000E+01	9.331E-07	1.695E-12	3.791E-07	2.314E-09	4.469E-12	0.	1.699E-11	0.	0.	0.	0.	0.
5.000E+01	9.331E-07	1.695E-12	3.791E-07	2.314E-09	4.469E-12	0.	1.699E-11	0.	0.	0.	0.	0.
7.000E+01	9.331E-07	1.695E-12	3.791E-07	2.314E-09	4.469E-12	0.	1.699E-11	0.	0.	0.	0.	0.
1.000E+02	9.331E-07	1.695E-12	3.791E-07	2.314E-09	4.469E-12	0.	1.699E-11	0.	0.	0.	0.	0.
2.000E+02	9.331E-07	1.695E-12	3.791E-07	2.314E-09	4.469E-12	0.	1.699E-11	0.	0.	0.	0.	0.
3.000E+02	9.331E-07	1.695E-12	3.791E-07	2.314E-09	4.469E-12	0.	1.699E-11	0.	0.	0.	0.	0.
5.000E+02	9.331E-07	1.695E-12	3.791E-07	2.314E-09	4.469E-12	0.	1.699E-11	0.	0.	0.	0.	0.
7.000E+02	9.331E-07	1.695E-12	3.791E-07	2.314E-09	4.469E-12	0.	1.699E-11	0.	0.	0.	0.	0.
1.000E+03	9.331E-07	1.695E-12	3.791E-07	2.314E-09	4.469E-12	0.	1.699E-11	0.	0.	0.	0.	0.
2.000E+03	9.331E-07	1.695E-12	3.791E-07	2.314E-09	4.469E-12	0.	1.699E-11	0.	0.	0.	0.	0.
3.000E+03	9.331E-07	1.695E-12	3.791E-07	2.314E-09	4.469E-12	0.	1.699E-11	0.	0.	0.	0.	0.
5.000E+03	9.331E-07	1.695E-12	3.791E-07	2.314E-09	4.469E-12	0.	1.699E-11	0.	0.	0.	0.	0.
7.000E+03	9.331E-07	1.695E-12	3.791E-07	2.314E-09	4.469E-12	0.	1.699E-11	0.	0.	0.	0.	0.
1.000E+04	9.331E-07	1.695E-12	3.791E-07	2.314E-09	4.469E-12	0.	1.699E-11	0.	0.	0.	0.	0.
2.000E+04	9.331E-07	1.695E-12	3.791E-07	2.314E-09	4.469E-12	0.	1.699E-11	0.	0.	0.	0.	0.
3.000E+04	9.331E-07	1.695E-12	3.791E-07	2.314E-09	4.469E-12	0.	1.699E-11	0.	0.	0.	0.	0.
5.000E+04	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.
7.000E+04	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.	0.

TABLE IX

$\phi^{Y}_{D}C$

Plant State	Release Category						
	Z-1	2	2R	Z-3	8A	8B	2RV
SEFC	0.	7.417E-10	0.	1.321E-12	0.	7.414E-06	0.
SEF	2.273E-16	2.623E-13	1.670E-13	0.	1.279E-09	0.	0.
SEC	0.	1.756E-12	0.	3.127E-15	0.	1.755E-08	0.
SE	1.417E-15	1.296E-13	8.480E-10	0.	8.402E-14	0.	0.
SLFC	0.	1.912E-09	0.	1.737E-10	0.	1.711E-05	0.
SLF	1.263E-14	9.912E-13	8.143E-13	0.	9.691E-09	0.	0.
SLC	0.	1.926E-10	0.	1.750E-11	0.	1.925E-06	0.
SL	2.023E-14	2.579E-12	1.209E-08	0.	1.290E-12	0.	0.
TEFC	0.	9.314E-11	0.	8.465E-13	0.	9.313E-07	0.
TEF	1.577E-16	3.218E-15	1.653E-15	0.	1.609E-09	0.	0.
TEC	0.	9.318E-11	0.	9.129E-14	0.	9.313E-07	0.
TE	9.962E-13	9.594E-11	2.870E-07	0.	2.279E-11	0.	0.
AEFC	0.	1.752E-08	0.	3.467E-12	0.	1.751E-04	0.
AEF	1.701E-15	1.979E-14	2.041E-14	0.	1.849E-10	0.	0.
AEC	0.	9.225E-13	0.	1.620E-14	0.	9.222E-09	0.
AE	1.094E-11	0.	0.	0.	0.	0.	0.
ALFC	0.	9.779E-10	0.	1.925E-11	0.	9.772E-06	0.
ALF	1.438E-15	7.266E-14	7.265E-14	0.	7.263E-10	0.	0.
ALC	0.	1.962E-14	0.	3.868E-15	0.	1.958E-10	0.
AL	2.521E-13	3.	0.	0.	0.	3.	0.
V	0.	1.958E-07	0.	0.	0.	0.	0.
TOTAL ϕ^{ρ} =	1.130E-11	1.349E-07	2.414E-07	2.153E-10	0.913E-09	4.176E-05	0.

TABLE X

$\phi_D^{I_M}$

ϕ \ Y	SEFC AEFC	SEF AEF	SEC AEC	SE AE	SLFC ALFC	SLF ALF	SLC ALC	SL AL	TEFC V	TEF	TEC	TE
1	0. 1.315E-06	0. 1.034E-10	0. 2.106E-09	0. 3.666E-12	0. 4.888E-06	0. 3.638E-10	0. 3.544E-13	0. 2.444E-13	0. 0.	0.	0.	0.
2	0. 4.362E-07	0. 8.357E-11	0. 6.119E-09	0. 6.871E-12	0. 4.888E-06	0. 3.628E-10	0. 4.380E-11	0. 7.661E-13	0. 0.	0.	0.	0.
3	3.016E-08 0.	7.788E-10 0.	1.391E-08 0.	1.292E-10 0.	1.621E-05 0.	1.090E-09 0.	8.461E-08 0.	9.735E-10 0.	0. 0.	0.	0.	0.
7	3.893E-06 0.	2.533E-10 0.	1.608E-09 0.	1.468E-10 0.	1.778E-07 0.	3.164E-11 0.	1.365E-09 0.	1.339E-09 0.	2.337E-07 0.	5.377E-10	3.081E-07	6.514E-09
8	0. 0.	0. 0.	0. 0.	0. 0.	4.410E-10 0.	8.392E-13 0.	3.427E-11 0.	2.570E-12 0.	2.478E-08 0.	2.621E-11	1.489E-08	3.152E-10
9	2.427E-07 0.	1.579E-11 0.	1.005E-10 0.	9.165E-12 0.	9.022E-07 0.	1.010E-09 0.	4.045E-07 0.	7.912E-09 0.	3.251E-08 0.	3.340E-11	1.940E-08	4.045E-10
10	2.241E-15 0.	1.566E-19 0.	9.234E-19 0.	8.436E-20 0.	1.069E-16 0.	1.867E-23 0.	7.820E-19 0.	3.283E-19 0.	1.052E-16 0.	3.101E-19	1.728E-16	1.923E-16
11a	2.784E-06 0.	1.940E-10 0.	1.144E-09 0.	1.041E-10 0.	1.321E-07 0.	2.328E-11 0.	9.815E-10 0.	9.359E-10 0.	1.694E-07 0.	3.948E-10	2.251E-07	4.613E-09
11b	5.933E-09 0.	3.272E-13 0.	7.891E-14 0.	2.511E-10 0.	6.739E-10 0.	3.721E-14 0.	4.095E-15 0.	5.126E-20 0.	1.043E-38 0.	5.708E-13	1.457E-14	1.993E-07
V	0. 0.	0. 0.	0. 0.	0. 0.	0. 0.	0. 0.	0. 0.	0. 0.	0. 1.050E-07	0.	0.	0.
TOTAL = ϕ_Y	7.417E-06 1.752E-06	1.274E-09 1.870E-10	1.758E-08 8.225E-09	6.483E-10 1.054E-11	1.912E-05 9.776E-06	4.693E-09 7.266E-10	1.926E-06 3.982E-13	1.290E-08 2.521E-13	8.314E-07 1.050E-07	1.613E-09	9.318E-07	2.279E-07

TABLE XI

Small LOCA Event Tree
Dominant Sequences

Plant Event Sequence Category	Conditional Frequency	Dominant Sequences			
		Sequence and AC Buses Available		Failed Branch Points	Conditional Frequency
		Bus No. 14	Seq.		
SEFC	4.38-8	7,8,9 7,8,9 7,8	35 62 35	L-1, OP-1 HH-2 L-1	2.52-8 7.29-9 9.46-9
SEF	2.20-8	7,8,9	147	TK	2.17-8
SEC	3.93-7	7,8,9 7	116 54	SA-1 L-1	2.76-7 1.06-7
SE	1.88-7	None	88		1.77-7
SLFC	4.58-4	7,8,9	2	R-2	4.55-4
SLF	3.08-8	7,8,9	4	R-2, CS	2.50-8
SLC	2.39-6	7	10		2.06-6
SL	2.75-8	9 7	14 91	CC, CS CS	6.72-9 1.81-8
ATWS	1.78-4	7,8,9	146	K-3	1.78-4

TABLE XII

System Unavailabilities for Small LOCA - All Electric Power and Support Systems Available

Code	Description	5th Percentile	Median	95th Percentile	Mean	Source
ET-3	Small LOCA	1.3-2	3.1-2	7.4-2	3.5-2	1.5.2
TK	Refueling Water Storage Tank	1.0-10	2.8-9	7.8-8	2.4-8	1.3.3
K-3	Reactor Trip	2.1-5	1.1-4	5.5-4	1.8-4	1.5.2
SA-1	Safety Injection Actuation Signal	6.8-9	8.6-8	1.1-6	2.8-7	1.5.2
HH-2	High Head Pumps	2.1-9	5.8-9	1.9-8	7.4-9	1.5.2
L-1	AFWS Actuation and Secondary Cooling	1.0-6	3.9-6	7.1-6	4.2-6	1.5.2
OP-1	Primary Cooling Feed and Bleed	3.6-3	5.9-3	9.4-3	6.1-3	1.5.2/1.3.3
SW	Service-Water	1.0-10	2.8-9	7.8-8	2.2-8	1.5.2
CF-1	Containment Fan Coolers	1.6-8	1.5-7	2.3-6	6.1-7	1.5.2
CC	Component Cooling Water	4.6-7	2.0-6	8.5-6	2.9-6	1.5.2
R-2	Recirculation Cooling	1.1-4	2.6-4	9.3-4	4.6-4	1.5.2/1.3.3
CS	Containment Spray	6.6-6	7.4-5	6.5-4	2.2-4	1.5.2/1.3.3
HA	Sodium Hydroxide Addition	1.0-4	6.1-4	1.2-3	7.6-4	1.5.2
RS	Recirculation Spray	9.0-5	7.3-4	4.3-3	1.6-3	1.5.2

TABLE XIII

Recirculation System Cause Table

Cause	System Failure Frequency (Mean)	Effects			
		Component	System	Other Systems	Initiating Event
Operator Error					
• Failure to initiate Switchover	1.3 x 10^{-4}	All	Fails	No effect	No effect
• Operators fail to stop all running pumps at RWST lo-lo level alarm	3.3 x 10^{-5}	All four ni-head pumps	Fails	No effect	No effect
Hardware Failures					
Single Failures					
• Containment sump blockage	5.0 x 10^{-5}	Containment sump	Fails	No effect	No effect
Multiple Failures (1)	2.9 x 10^{-5}	(1)	Fails	No effect	No effect

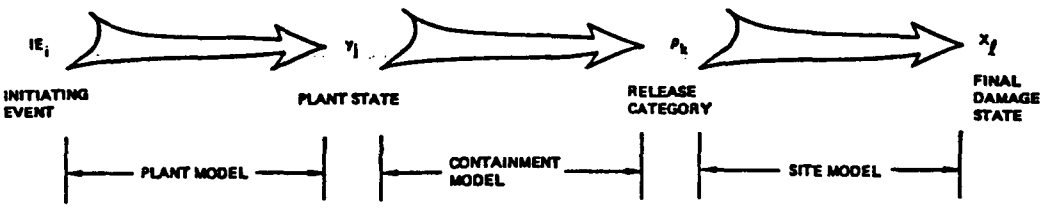


Figure 1. Structuring of Scenarios - Relationship of Pinch Points

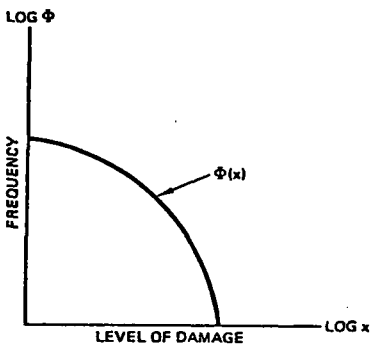


Figure 2. Risk Curve in Frequency Format

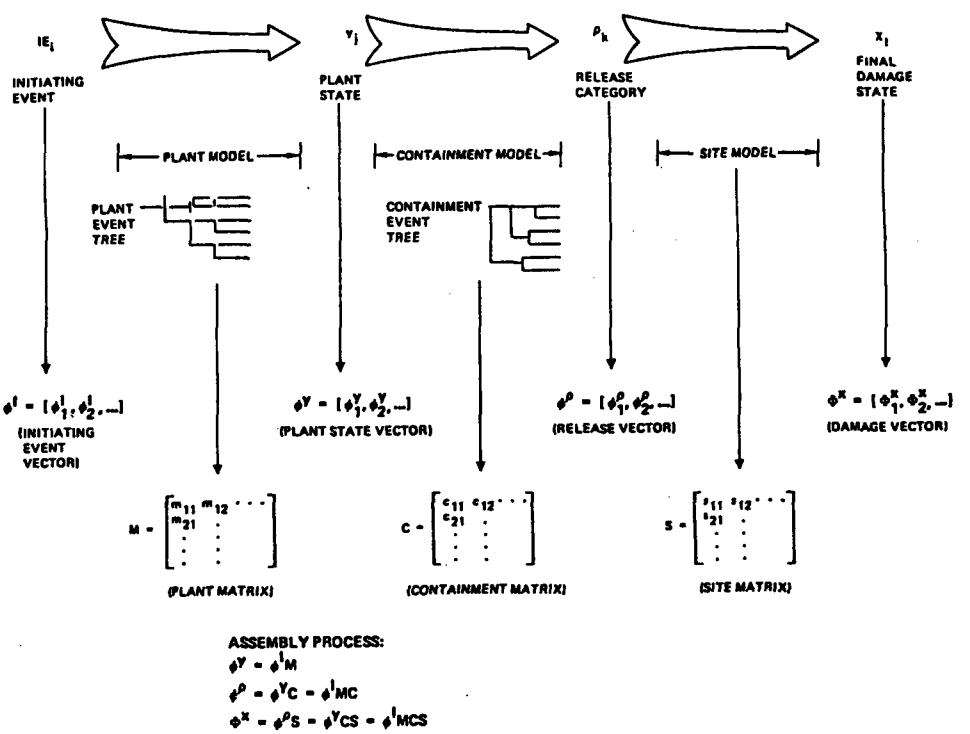


Figure 3. Overview of the Assembly Process Showing Relationship of Pinch Points, Frequency Vectors, Event Trees, and Transition Matrices

A METHODOLOGY FOR SEISMIC RISK ANALYSIS OF NUCLEAR POWER PLANTS

S. Kaplan, H. F. Perla, and D. C. Bley

Pickard, Lowe and Garrick, Inc.
Irvine, California 92714

ABSTRACT

This methodology begins by quantifying the fragility of all key components and structures in the plant. By means of the logic encoded in the plant event trees and fault trees, the component fragilities are combined to form fragilities for the occurrence of plant damage states or release categories. Combining these, in turn, with the seismicity curves yields the frequencies of those states or releases. Uncertainty is explicitly included at each step of the process.

INTRODUCTION

The purpose of this paper is to describe a methodology for calculating the risk to nuclear power plants from seismic events. The methodology is an outgrowth, or further development, of ideas described in [1]. Other aspects of the methodology have been discussed in [2,3]. A comparison with other approaches and a more complete bibliography was prepared by Ravindra for the PRA guidebook [4]. Although the methodology has been used so far, to our knowledge, mainly in nuclear power plants [5-7], it is equally applicable to other types of facilities and to other types of "external" events; e.g., high winds [6] and floods, where the severity of the event is characterized by one or more parameters. For simplicity, however, our presentation will be cast only in terms of seismic events in nuclear plants and will make use of the definition of risk and the matrix formulation described in [3,5,6,8,9].

STEPS IN A SEISMIC RISK ANALYSIS

A seismic risk analysis of a nuclear plant consists of the following steps:

1. Seismicity. Description of the seismic activity; i.e., of the likelihood of various sized ground motions at the location of the plant in question.

2. Fragility of Components. Identification of key components (equipment, systems, people, and structures) in the plant and description of the vulnerability of these items; i.e., the likelihood of their failure under various postulated ground motions.

3. Plant Logic. Identification of the combinations of component failures which would lead to plant level failures; e.g., core melt or radioactivity release. This is done from the logic of the plant's design and the physical phenomena involved.

4. Plant Level Fragilities. From the component fragilities and combination logic, compute the fragility of the plant level events (melt, release, etc.) being analyzed.

5. Initial Assembly of Results - Plant Level Failures. Combination of the seismicity and plant level fragility information to determine the frequency of seismically induced plant level failures.

6. Final Assembly - Further Consequences. Combine the results of step 5 with analyses of downstream consequences (e.g., public health impacts) of plant level failures. Thus, obtain an expression of the risk of such consequences stemming from seismic events.

The following sections describe each of these steps in turn.

SEISMICITY (STEP 1)

To discuss the seismic activity of a given location on the earth's surface, we must, as when discussing anything else, adopt some sort of model. Any model is, of course, only an approximation to the real world phenomena; yet it is necessary to choose in order to make any progress at all. For the present methodology, we shall, following [1,10], adopt a model which, though simple, is eminently workable, and thus enables us to give a definitive quantification of the seismic risk to any specific plant at any specific location. This, in turn, allows us to make progress towards making more rational and timely decisions about the design and location of such plants.

In this model, we characterize an earthquake by a single parameter, a, called the "effective peak ground acceleration." The seismicity of the location is then characterized by a seismicity curve, or frequency of exceedance curve, as sketched in Fig. 1.

The ordinate of this curve, $\Phi(a)$, at any point, a, gives the frequency, occurrences per year, with which earthquakes of acceleration a, or greater, occur at the location.

The curve $\Phi(a)$ for the site is supplied by seismologists from whatever recorded history and knowledge of crustal dynamics is available. Now since records have been kept for only a short time geologically speaking, this history and knowledge is limited. Thus, seismologists do not know the curve $\Phi(a)$ with great accuracy. To tell the truth, then, about our state of seismic knowledge and in keeping with the overall philosophy and "Level Two" format of risk analysis [9], we need to quantitatively express our uncertainty about the curve $\Phi(a)$. The most convenient format for this expression is to put forth a family of curves, $\Phi_i(a)$, and assign a probability, p_i, to each. Thus we obtain Fig. 2.

We may express this family of curves as a set of doublets:

$$\Phi = \{<p_i, \Phi_i>\} \qquad (1)$$

where Φ_i stands for the whole curve $\Phi_i(a)$, and

$$\sum_{i=1}^{J} p_i = 1.0 \tag{2}$$

Observe that the set of doublets in Eq. (1) is nothing more than a discrete probability distribution (DPD) on the space of curves $\Phi(a)$ [2]. Note also that this is an instance of usage of the "probability of frequency framework" [3,9].

In this methodology, the DPD of Eq. (1) is the format in which we express our state of knowledge of the seismicity of the location. This format is all we need for the present paper. For examples and information on how these curves Φ_i are actually developed from more basic information, see [4,11,12], and the references therein.

FRAGILITY OF COMPONENTS (STEP 2)

By fragility, we mean the likelihood of failure as a function of effective peak ground acceleration for plant structures, equipment, and other components. Let us focus, therefore, on a specific structural component of the plant, say for example, a particular "shear wall." We wish to know if this wall will fail under earthquake size a. We first must assign a clear and definite meaning to the word "fail." That being done, it is now a question of structural analysis--analyzing the movements and stresses in the wall when subjected to earthquake size a. The problem is that there are many different earthquakes, all having the same peak acceleration a. Thus, when we say earthquake "a," we really define thereby a whole category of ground motions with different time histories, frequency content, etc.

Thus, when we ask if the wall will fail under quake "a," we are really envisioning a series of thought experiments in which we subject the wall to quakes randomly selected from the category "a." We wish to know in what fraction, F, of these experiments did the wall fail [13]. This fraction, F, of course, will be a function of earthquake size a. Plotting this function, we obtain the fragility curve, Fig. 3.

This curve characterizes the seismic performance of the wall. If we had run the above series of experiments, we would know this curve. Since we have not, we have uncertainty about what this curve is and, again, express our uncertainty in the form of a family of curves, Fig. 4.

To each such curve, $F_k(a)$, we assign a probability, q_k, and thus obtain the DPD

$$F = \{<q_k, F_k>\} \tag{3}$$

Note that this is another instance of the probability of frequency format.

The family of fragility curves is developed by structural dynamicists for each component in the plant deemed important with respect to determining the plant's response to seismic motion. This set of fragility families constitutes step 2 and is the structural dynamics input to the analysis. When this input is received, the items are sorted and listed in order of increasing strength. Thus, the most fragile elements--those most vulnerable to seismic action--come first on the list. This ordering is a key step which makes it possible to handle the plant logic step (step 3) in a computationally feasible form.

PLANT LOGIC AND PLANT LEVEL FRAGILITIES (STEPS 3 AND 4)

If we have the fragility family for each structural and equipment component in the plant, we need next to aggregate these into fragility families for the plant as a whole. This is done within the context of the matrix formalism and the master assembly equation in probabilistic risk analysis [3,6,9]. Specifically, let y represent a certain plant damage state, one of the exit states from the plant matrix M. From the fault and event trees for the plant, we identify the set(s) of structural and equipment components whose failure in combination leads to state y. These combinations are stated in the form of Boolean expressions. For example, the expression

$$y = (1) \wedge [(4) \vee (8)] \tag{4}$$

would say that state y occurs if and only if component (1) fails and, in addition, either component (4) or component (8) fails.

Next, by means of the logic of these combinations, the fragility families for these components can be aggregated [14] into a single fragility family, which again can be written in the form of a DPD as follows:

$$F^y = \{<q_k^y, F_k^y>\} \tag{5}$$

This DPD represents the fragility family for the plant state y. The set of these DPDs for all plant states characterizes the seismic response of the plant and determines, therefore, the seismic M Matrix.

ASSEMBLY (STEP 5)

It remains next to assemble the seismicity and fragility information into a statement of the frequency of plant states due to earthquake. To explain how this is done, consider first the case of no uncertainty. Thus, we have a single curve, $\Phi(a)$, and a single fragility curve, $F^y(a)$, for damage state y. In this case, we can say that the frequency with which state y occurs due to earthquake is

$$\phi^y = -\int_0^\infty \left[\frac{d\Phi(a)}{da}\right] F^y(a)da \tag{6}$$

To understand this integral, note that

$$-\left[\frac{d\Phi(a)}{da}\right] da \tag{7}$$

is the frequency with which quakes occur in the size range da about a and $F^y(a)$ is the fraction of such quakes which result in plant state y.

FINAL ASSEMBLY (STEP 6)

Once the numbers ϕ^y are obtained, giving the frequency of plant states as a result of seismic activity, the combination of these results with the containment

and site matrices (C and S) proceeds as dictated by the master assembly equation; i.e.,

$$\phi^{O} = \phi^{y} C \tag{8}$$

and

$$\Phi^{x} = \phi^{O} S \tag{9}$$

The results of these operations can be plotted directly as risk curves against the various damage indices. These curves express the seismic risk. They may then be combined with those from other initiating events to obtain the total risk.

To include uncertainty, we apply the basic idea of DPD arithmetic as follows. Write

$$\phi^{y}_{jk} = -\int_{0}^{\infty} \left[\frac{d\Phi_j(a)}{da}\right] F^{y}_{k}(a)da \tag{10}$$

The probability that goes along with this value of frequency is the product of the probability of curve Φ_j and that of F^{y}_{k}:

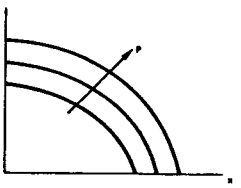
$$p^{y}_{jk} = p_j \, q^{y}_{k} \tag{11}$$

Thus, we have the DPD for each ϕ^{y}:

$$\phi^{y} = \{<p^{y}_{jk}, \phi^{y}_{jk}>\} \tag{12}$$

These DPDs constitute a probabilistic statement of the row matrix for plant states resulting from seismic events.

The DPDs in Eq. (12), propagated through the matrix operations of Eqs. (8) and (9), along with the DPDs for the matrices C and S, yield final risk curves in "Level Two" format.



SEISMIC EFFECTS ON CONTAINMENT

The above discussion on final assembly assumed that the C Matrix itself is not affected by the seismic event. This is sometimes not so since the containment itself may be damaged in an earthquake. To handle this case, we write the master assembly equation for seismic events in the form

$$\Phi^{x} = \phi^{s} (MC)^{s} S \tag{13}$$

thus thinking of the product matrix MC as a unity giving the transition from ground motions to release categories. The plant logic step (step 3) is now replaced by a plant and containment logic in which Boolean expressions are written for release

categories. Thus, for example, if (6) denotes the containment structure, the expressions

$$\rho_k = (1) \wedge [(4) \vee (8)] \wedge \bar{(6)}, \quad \rho_{k+1} = (1) \wedge [(4) \vee (8)] \wedge (6)$$

would say that release category k occurs if component (1) fails along with component (4) or (8) and also the containment, (6), does not fail. If (6) does fail along with the components, then we get a release of category k+1.

SEISMIC EFFECTS ON THE SITE MATRIX

For a complete analysis, one should also consider the effects of the earthquake on the site matrix S itself. The effects will be to raise the numbers in S, reflecting first, the casualties resulting directly from the earthquake without any reactor involvement, and second, reflecting the fact that earthquake damage to transportation facilities may make evacuation more difficult in the event of a radioactive release. Full systematic studies of these effects have not yet been done. However, initial calculations indicate that the former effect far outweighs the latter.

WIND AND FLOOD

We observe that wind, flood, and any other initiating events having a magnitude parameter can be treated within the same formalism as seismic events. Thus, for example, in the case of wind, the seismicity diagram, Fig. 1, is replaced by an equivalent set of curves showing the frequency at the site of winds exceeding, say, "w" miles per hour. The fragility families are then drawn similarly against the parameter w, Booleans are written, and everything proceeds just as before.

EXAMPLE

The following numerical example is taken from the Zion study [5]. The family of seismicity curves is shown in Fig. 5, each with a probability assignment. Fragility information for key components is given in Table I and typical families of fragility curves are shown in Fig. 6. In this figure, the median fragility curve is plotted as a solid line; the 10 and 90 percentile curves are dashed.

Table I gives for each component three parameters, $\tilde{\tilde{a}}$, β_R, and β_U. These describe the fragility family of the component according to the "double lognormal" format [1]. In this format, each sigmoid curve in Fig. 4 is a lognormal and can be written in parametric form as

$$F = N(z), \quad a = \tilde{a}\, e^{\beta_R z} \tag{14}$$

where z is the standard normal variate and N(z) is the area under the normal curve up to z. The family of sigmoid curves is then described by making the median, $\tilde{a}$, itself lognormal; i.e.,

$$\tilde{a} = \tilde{\tilde{a}}\, e^{\beta_U \zeta} \tag{15}$$

where ζ is another standard normal variate and $\tilde{\tilde{a}}$ is now the "median median"; i.e., the median value of the medians, $\tilde{a}$, of the individual curves.

As an example of the plant logic step, we reproduce as follows the Boolean expression for core melt in terms of the components of Table I:

$$\text{Melt} = (4) \vee (8) \vee (10) \vee [((12) \vee (22) \vee (26)) \wedge (9)] \vee (14) \vee (17) \vee (21) \quad (16)$$

Combining the individual fragility families through the logic of this expression, we obtain a fragility family for the event "core melt." This is shown in Fig. 7 in the form of five discrete curves, each with a probability of 0.20.

The assembly step is done using Figs. 5 and 7 along with Eq. (10). The resulting DPD, after smoothing, is presented in Fig. 8. This curve thus expresses our state of knowledge about the frequency of seismically induced core melt.

Finally, it is of interest to examine the contributions of the individual components to this melt frequency. From Eq. (16) and Table I, we see that out of those components whose failure leads to melt, the service water pumps, (4), are probably the first to fail. Component (4) is therefore the single most important contributor to the final probability of frequency curve, Fig. 8. The second largest contributor is (8), followed by (10), then the bracketed combination, and finally by (14), (17), and (21). Fig. 9 shows how the melt frequency curve changes as we build Eq. (16) incrementally.

Thus, curve I is the frequency of failure of the service water pumps alone. When a melt is possible via (4) or (8), we obtain the curve II, and so on. The higher numbered components contribute steadily less since an earthquake large enough to fail them will most probably have already failed the lower numbered components.

REFERENCES

1. R. P. Kennedy, et al, "Probabilistic Seismic Study of an Existing Nuclear Power Plant," Nuclear Engineering and Design, 59, (1980), 315-338.

2. S. Kaplan, "On the Method of Discrete Probability Distributions in Risk and Reliability Calculations - Application to Seismic Risk Assessment," Risk Analysis, Vol. 1, No. 3 (1981).

3. S. Kaplan, et al, "Methodology for Probabilistic Risk Assessment of Nuclear Power Plants," PLG-0209, Pickard, Lowe and Garrick, Inc., June 1981.

4. U.S. Nuclear Regulatory Commission, "PRA Procedures Guide," draft report, NUREG/CR-2300, Vol. 2, Chapters 10 and 11, April 1982.

5. "Zion Probabilistic Safety Study," prepared for Commonwealth Edison Company, September 1981.

6. "Indian Point Probablistic Safety Study," prepared for Consolidated Edison Company of New York, Inc., and the Power Authority of the State of New York, March 1982.

7. B. J. Garrick, et al, "OPSA, Oyster Creek Probabilistic Safety Analysis," draft report, PLG-0100, Pickard, Lowe and Garrick, Inc., August 1979.

8. S. Kaplan, "A Matrix Theory Formalism for Event Tree Analysis," Risk Analysis, Vol. 2, No. 1, 1982.

9. S. Kaplan, and B. J. Garrick, "On the Quantitative Definition of Risk," Risk Analysis, Vol. 1, No. 1, 1981.

10. A. C. Cornell, "Engineering Seismic Risk Analysis," Bulletin of the Seismological Society of America, Vol. 58 (1968), 1583-1606.

11. "Zion Probabilistic Safety Study," op. cit., Section 7.9.1.

12. "Indian Point Probabilistic Safety Study," op. cit., Sections 7.9.1 and 7.9.2.

13. In assessing the fraction of experiments in which failure occurs, we include not only direct failure of the component in question, but also "indirect" failures. For example, if another component falls on the component in question causing its failure, this would be an indirect failure, also known as a "systems interaction" effect.

14. In this aggregation process, attention must be paid to the notion of "dependence."

TABLE I

FRAGILITY OF KEY ZION STRUCTURES AND EQUIPMENT

Symbol	Structure/Equipment	$\tilde{a}$	β_R	β_U
①	Offsite Power Ceramic Insulators	0.20	0.20	0.25
②	125 VAC Distribution Panel*	0.60	0.37	0.50
③	125 VDC Buswork*	0.60	0.37	0.50
④	Service Water Pumps	0.63	0.15	0.36
⑤	4,160V Switchgear (chattering)*	0.72	0.35	0.47
⑥	480V Switchgear (chattering)*	0.72	0.36	0.47
⑦	480V Motor Control Centers (chattering)*	0.72	0.36	0.47
⑧	Auxiliary Building-Failure of Concrete Shear Wall	0.73	0.30	0.28
⑨	Refueling Water Storage Tank	0.73	0.30	0.28
⑩	Interconnecting Piping/Soil Failure Beneath Reactor Building	0.73	-	0.33
⑪	Impact Between Reactor and Auxiliary Buildings	0.78	0.28	0.41
⑫	Condensate Storage Tank	0.83	0.28	0.29
⑬	4,160V Diesel Generators*	0.86	0.35	0.37
⑭	Crib House Collapse of Pump Enclosure Roof	0.86	0.24	0.27
⑮	Safety Injection Pumps	0.90	0.20	0.37
⑯	Containment Ventilation Ductwork and Dampers	0.97	0.20	0.62
⑰	125 VDC Batteries and Racks	1.01	0.28	0.63
⑱	Core Geometry	1.16	0.25	0.42
⑲	Reactor Coolant System Relief Tank	1.19	0.20	0.63
⑳	4,160V Transformer	1.39	0.25	0.60
㉑	Service Water System Buried Pipe 48"	1.40	0.20	0.57
㉒	CST Piping 20"	1.40	0.20	0.57
㉓	Auxiliary Building-Failure of Concrete Roof Diaphragm	1.40	0.31	0.33
㉔	Failure of Masonry Walls	1.70	0.50	0.26
㉕	Containment Ventilation System Fan Coolers	1.74	0.49	0.23
㉖	Collapse of Pressurizer Enclosure Roof	1.80	0.39	0.34

*Fragility values indicated are for chatter, relay trip, or other intermittent or easily recoverable conditions. Unrecoverable failure is expected to occur at about three times the indicated fragility value.

FIGURE 1. SEISMICITY CURVE

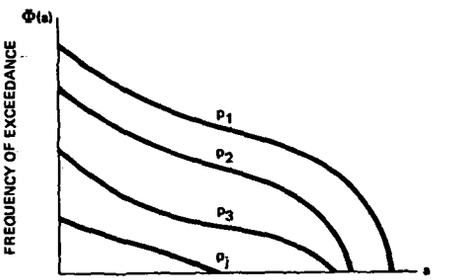


FIGURE 2. FAMILY OF SEISMICITY CURVES

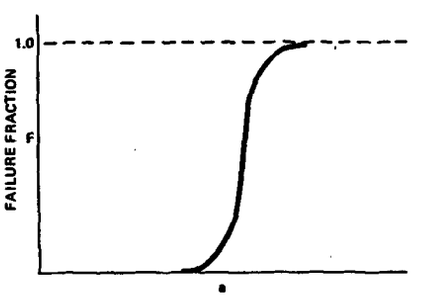


FIGURE 3. FRAGILITY CURVE FOR TYPICAL COMPONENT

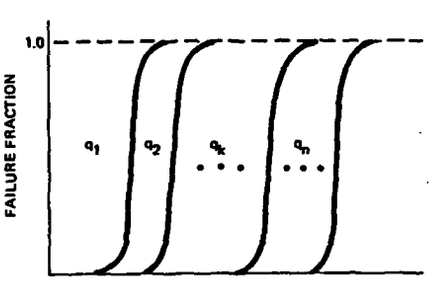


FIGURE 4. FAMILY OF FRAGILITY CURVES FOR A TYPICAL COMPONENT, C

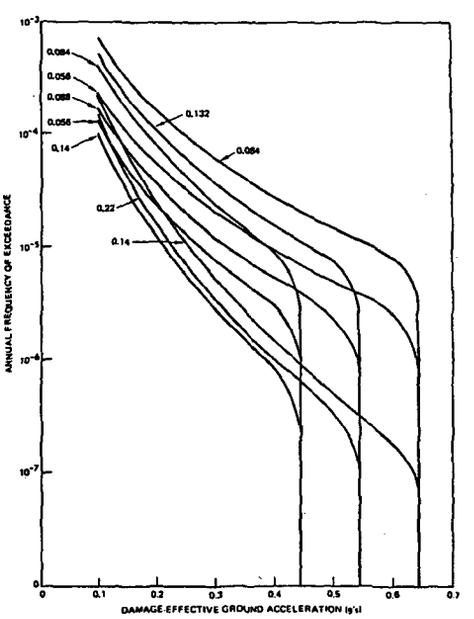


FIGURE 5. SEISMICITY FAMILY

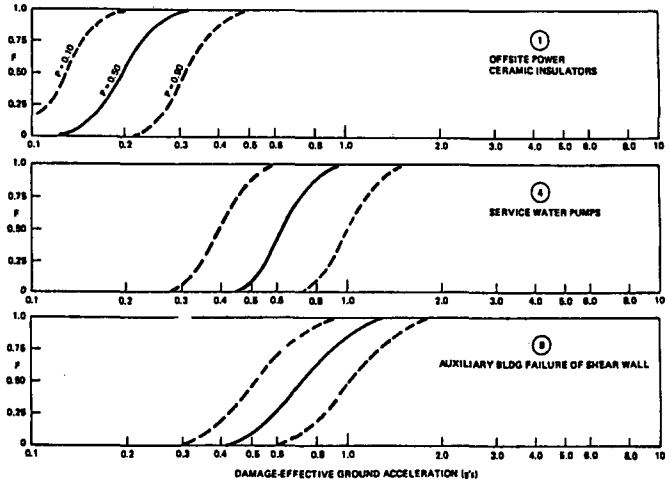


FIGURE 6. FRAGILITY FAMILIES FOR KEY COMPONENTS

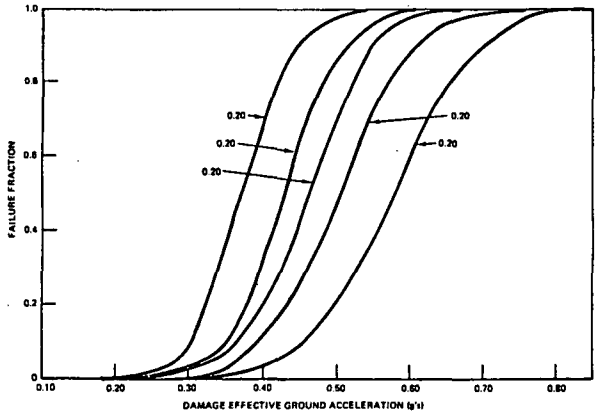


FIGURE 7. ZION PLANT LEVEL FRAGILITY FAMILY

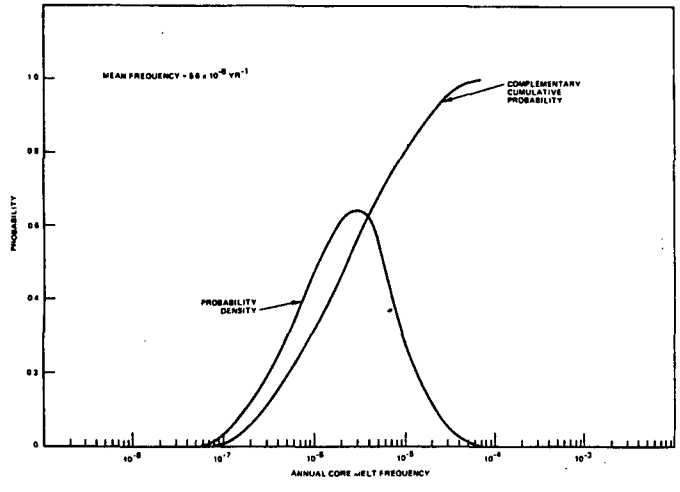


FIGURE 8. ZION ANNUAL CORE MELT FREQUENCY

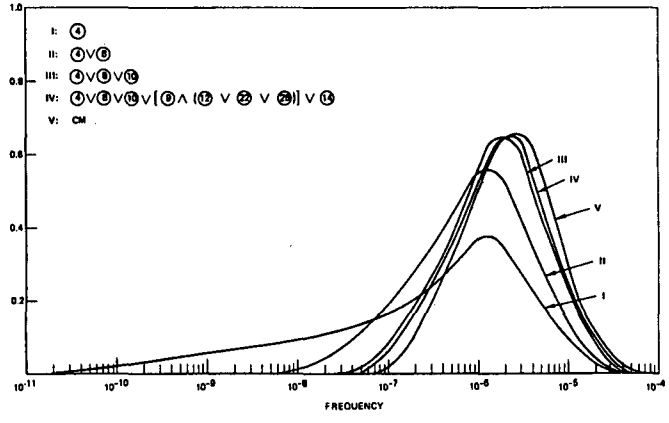


FIGURE 9. SEISMIC CORE MELT FREQUENCY SHOWING CONTRIBUTIONS FROM VARIOUS COMPONENTS

ACCIDENT SEQUENCE BINNING: A METHOD TO INTEGRATE THE INDIVIDUAL ANALYSES OF A PROBABILISTIC RISK ASSESSMENT

Blake F. Putney, Jr. and William J. Parkinson

Science Applications, Inc.
Palo Alto, California

ABSTRACT

A probabilistic risk assessment (PRA) for a nuclear power plant is composed of separate but dependent analyses. Completing a PRA requires that those analyses are properly integrated. Since each analysis can be almost unlimited in scope, the integration process should optimize the resources for each analysis. Examining the parameters which significantly affect public health and/or plant damage consequences and by focusing each analysis on those parameters, the accident sequence binning technique can be used to optimize and integrate a PRA. This paper outlines the rationale for the binning technique and its advantages for use in PRAs.

INTRODUCTION AND SUMMARY

A probabilistic risk assessment (PRA) for a nuclear power plant is composed of many separate but dependent analyses. Completing a PRA requires that those analyses are properly integrated. Since each analysis can be almost unlimited in scope, the integration process should optimize the available resources for each analysis. This paper outlines a technique known as accident sequence binning and illustrates how it can facilitate the integration of a PRA.

The overall risk model created for a PRA is composed of four basic modeling efforts:

- Accident sequence definition and system modeling;
- Physical processes;
- Radionuclide release and transport; and
- Environmental transport and consequence analysis.

Problems occur when a model does not contain enough detail to allow subsequent models to uniquely address consequences, i.e., early and late core melting and its impact on evacuation warning time. The accident sequence binning technique focuses each analysis on consequences. Each analysis effort, as shown in Figure 1, begins by examining those parameters that have unique effects on risk. The effort begins by identifying the risk sensitive parameters in the consequence model. An excellent guide to the sensitive parameters in the consequence model can be found in the PRA Procedures Guide [1]. Table 1 lists some of those sensitive parameters most commonly influenced by the other parts of a PRA.

Table 1
IMPORTANT PARAMETERS FROM THE CONSEQUENCE MODEL
INFLUENCED BY AN ACCIDENT'S CHARACTERISTICS

- Frequency of release
- Source term characteristics: magnitude and isotopic content
- Energy of release
- Particle size
- Warning time
- Duration of release

It is then determined specifically how those sensitive parameters are influenced by the other analyses. The radionuclide release and transport and the physical processes analyses are examined to determine their own specific consequence parameters which affect the source term characteristics, the particle size, and the duration of release. Parameters affecting the source term characteristics are the most important. The physical processes analysis is also examined for its influence on the energy, duration, and frequency of release as well as evacuation warning time. Consequence parameters stem from phenomena concerned primarily with containment failure models and timing.

The ultimate goal of this process is to develop a list of consequence parameters affected by events in the accident sequence development and systems modeling task. Therefore, at each point in the process an attempt is made to identify consequence parameters whose values are changed by the occurrence of a specific event. For example concern over the source term magnitude resulting from containment failure identified hydrogen burning as a key physical process consequence parameter. Spray system operation can reduce the pressure of a complete hydrogen burn [4]. Therefore heat removal by sprays during a hydrogen burn is identified as a consequence parameter. The amount of spray flow must be established to set a range, or ranges, for this parameter. In this way a list of important consequence parameters and ranges is developed. Table 2 is an example of such a list. It is similar to the one used to bin accident sequences for the Oconee PRA.

Given a list of important consequence parameters and ranges, the accident sequence development and system modeling task can be organized. Since an extremely large number of component failure combinations could lead to a nuclear power plant accident, some optimization and organization must be done. The first step in this process is event tree development. Event trees are formulated by grouping combinations of components (systems, subsystems, or groups of systems) whose failure results in a similar range of values for consequence parameters. This similarity is determined by examining the operation of the components in question and determining whether important consequence parameters are affected. If so, these components must be grouped as a separate top event in the event tree. If not, the components could be grouped with others performing a similar function. This process tailors the event tree development to the consequence analysis early in the risk assessment. Simultaneously, the possible consequence parameter combinations are identified.

The event tree process results in a set of accident sequences. Accident sequences with similar consequence parameter combinations can be further grouped into plant damage bins (PDBs). Oconee PRA experience indicates that six types of core melt

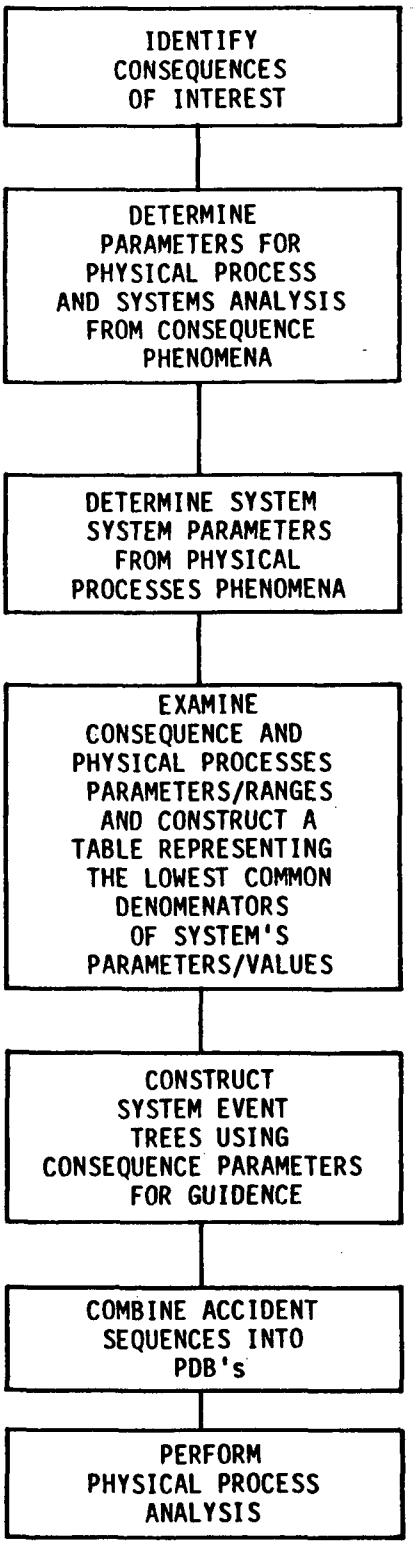


Figure 1: Plant Damage Binning Methodology.

Table 2

Important Consequence Parameters and Ranges

Critical Parameter	Parameter Range	Comments on Phenomena of Importance
Containment pressure	<110 psia	No containment overpressure failure
Containment pressure	>110 and <190 psia	Possible containment over-pressure
Containment pressure	>190 psia	Certain containment over-pressure
Steam partial pressure	Steam concentration >50 volume percent	Hydrogen (H_2) not flammable[4]
Heat removal during hydrogen burning	Any sprays operating	Lower H_2 burn pressures[4]
Turbulence during burning	Any fans or sprays	More complete H_2 burn[4]
RCS leakage to containment prior to RPV failure	Large LOCA leakage rates	Less likely H_2 burn before RPV failure with decreasing break size. Lower source term with decreasing break size.
RCS leakage to containment prior to RPV failure	Small LOCA leakage rates	Less likely H_2 burn before RPV failure with decreasing break size. Lower source term with decreasing break size.

Table 2 Cont'd

Important Consequence Parameters and Ranges

Critical Parameter	Parameter Range	Comments on Phenomena of Importance
RCS leakage to containment prior to RPV failure	Cycling relief valve leakage rates	Less likely H_2 burn before RPV failure with decreasing break size. Lower source term with decreasing break size.
Sudden spray initiation when high steam partial pressure exists.	After RPV failure	Could result in H_2 burning conditions leading to high containment pressures.
Radiation removal by sprays	Any sprays operating	Excellent radiation removal
Time from shutdown to start of boiloff of core inventory	<2 hours	Longer evacuation warning time with increasing time from shutdown.[2]
Time from shutdown to start of boiloff of core inventory	>2 hours and <12 hours	Longer evacuation warning time with increasing time from shutdown
Time from shutdown to start of boiloff of core inventory	>12 hours	Longer evacuation warning time with increasing time from shutdown
Water on containment floor	<100,000 gallons	No water in reactor cavity. No steam explosion or coolability possible.[6]
RCS pressure	> 400 psia	In-vessel steam explosion less likely.[5]

bins and five containment safeguard system states resulting in 24 PDBs were sufficient to adequately represent the various combinations of the important parameters and ranges identified. The number of bins is much smaller than the total number of possible consequence parameter combinations. This reduction occurs because many of the parameters are coupled (i.e., RCS leakage rate and RCS pressure) and because there are a limited number of systems involved (i.e., only containment sprays and fans affect most containment related phenomena).

In addition to providing an efficient management tool for coordinating the system and consequence analyses, this accident sequence binning technique has a number of advantages. A limited number of accident sequence consequence calculations are required, thus simplifying, focusing, and reducing the resources of the consequence efforts. The fault tree/event tree models are grouped into bins that are more efficiently quantified than large numbers of sequences. A framework for success criteria definition is formed for all systems. Completeness is enhanced by starting the analysis from the consequence end of the problem. The smaller number of accident sequence states improves communication and integration between the various groups working to complete the PRA. The PRA can be more clearly tailored to meet specific goals (i.e., for plant damage analysis or emergency response planning, various types of scenerios with unique outcomes can be clearly and separately defined).

In summary, by starting from the consequence end of a PRA, a series of consequence parameters affected by system responses are developed. The accident sequence development and system modeling effort is then tailored to reflect important variations in those parameters. Accident sequence bins are formed and used as a basis for simplifying the consequence analysis effort and the quantification effort, and the bins are used to enhance communication and improve integration of the individual tasks of the PRA. A description of this methodology follows.

DESCRIPTION OF METHODOLOGY

This section describes in more detail the application of the accident sequence binning technique, to a PRA. A flow diagram for this technique was illustrated in Figure 1. Each of the following subsections represents an important step in the flow diagram. Examples are provided to illustrate the use of the technique.

Identify Consequences of Interest

Identifying the consequences of interest is the first step in any probabilistic risk analysis. This step requires focusing the PRA in its initial stages. In the previous discussion, the focus of the PRA was public risk, more specifically early fatality risk. The focus could just have easily been utility economic risk. In the case of utilty economic risk, an important consequence parameter might be steam generator damage. Including these consequences with the ultimate utility consequence, core damage, a traditional risk assessment could be expanded in scope. Focusing early on important consequences, the PRA manager is likely to prevent modeling a hodgepodge of system states and attain a targeted, goal oriented product.

Determine Parameters for Physical Processes and Systems Analyses from Consequences Phenomena

The Introduction and Summary included in Table 1 a list of consequence phenomena which are important to the determination of early fatality risk. Translating the identified consequence phenomena into parameters expressed in terms of system operation is the next step in the binning technique. In the case of public health

consequences, intermediate steps may be required such as determining parameters for the physical processes analysis.

The previous discussion of spray effects on hydrogen burning is an example. A direct translation of an economic consequence parameter, steam generator repair, into a system oriented parameter would be actuation of a system that would inject untreated water into the steam generator.

Determine Parameters for Systems Analysis From Physical Processes Phenomena

A final list of parameters for a systems analysis focused on public health risk was presented earlier in Table 2. That list was obtained by a careful study of all potential containment failure modes (physical processes phenomena) which could lead to radionuclide releases (consequence phenomena) and therefore early fatalities (identified consequence).

Use Parameters and Their Ranges to Construct a Table Representing the Least Common Denominators of System Parameters and Values

Table 2 contains sets of ranges for each consequence parameter. In addition to the knowledge that a system affects a consequence parameter, the systems analyst must be aware of important variations in system operating parameters such as flow rate. For example while it is known that a containment spray system will remove radionuclides from the containment atmosphere, how much spray flow exists could also be important. Additionally, the same could be true of a containment spray system's effect on hydrogen burn pressures. Therefore the success criteria for the containment spray system as well as other systems must be established with respect to the consequence parameters identified for the study. Upon identification of system operating parameter requirements, the lowest common denominator of those values can be assigned.

Event Tree Construction Using Consequence Parameters

Traditionally, PRAs have used systemic event trees to model the plant response to initiating events. These event trees were drawn using a set of "functions" as guidelines for the structure of the event tree. While these sets of functions are arbitrary and vary from analyst to analyst, the plant configuration forces event trees to be similar. However, problems can occur when the plant model is merged with the consequence analysis. These problems involve accident sequences containing system failure modes not uniquely defining parameters used in the physical processes or consequence analyses. By identifying consequence parameters prior to systemic event tree construction, these problems can be avoided .

Construction of systemic event trees using consequence parameters is similar to the process used to derive systemic event trees from functional event trees. The difference stems from the criteria used to identify event tree branches. Using consequence parameter for guidelines, the analyst chooses branch points by identifying system requirements to prevent a certain undesired event, such as core melting. Once the systems have been identified, grouping systems under event tree headings begins. This grouping takes place using the consequence parameters as a guide. Some required systems can be combined in a single event tree top, while others must be broken into two events. The examples shown in Figure 2 illustrate this process. Event trees I and II illustrate portions of a typical PWR small LOCA event tree. These trees represent high pressure injection followed by recirculation when the injection water source is exhausted. The difference in the event trees arises when the time of core melt is considered, core melt accident sequence I-B can occur at either 2 hours or 24 hours depending whether the operator allows the containment sprays to deplete the injection water source. The consequences of the accident sequences differ because the evacuation warning time differs for early and late core melt. Introducing an intermediate event into Event Tree II, the time of core melt for a recirculation sequence can be identified separately for sequences II-B, and II-D.

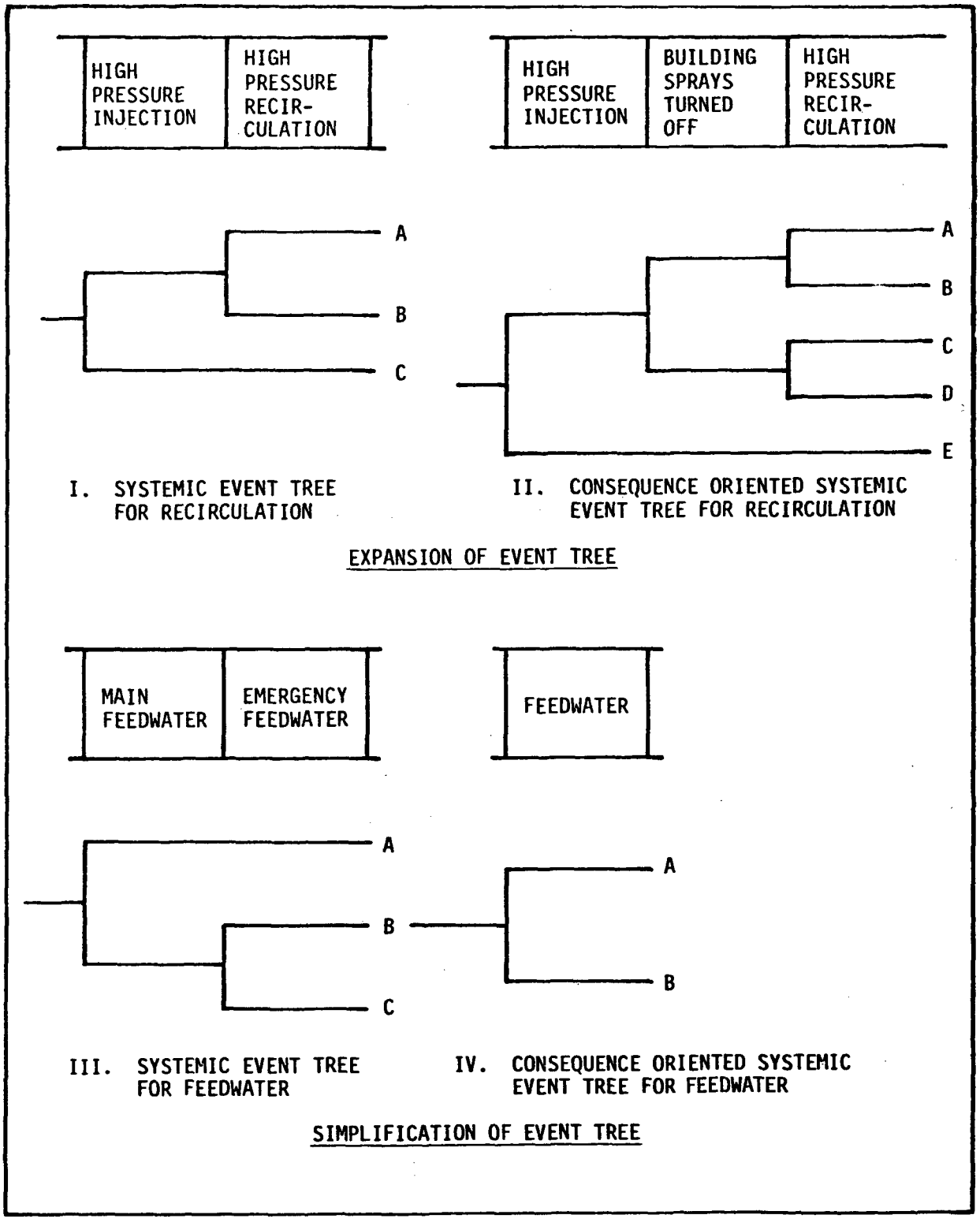


Figure 2: Event Tree Comparison.

The second example illustrates how this concept can be used to simplify systemic event trees. Event Tree III contains choices for both feedwater and emergency feedwater. Sequence C is the only sequence leading to core melt. If the consequence parameters of interest are not affected by the success states III-A and III-B, the event tree systems may be combined into one event, thereby simplifying this analysis. (On the other hand, however, if steam generator damage was also an important consequence, the event tree might require distinguishing between chemically controlled and uncontrolled emergency feedwater water sources in the top events.)

Create Plant Damage Bins

Plant damage bins are created upon conclusion of event tree construction. The effect of each accident sequence on the consequence parameters is identified. Accident sequences that result in similar values for the consequence parameters are grouped together in a PDB. A PDB is defined by the values of the consequence parameters that it contains. The analysis teams will determine if accident sequences with slightly different parameter values can be combined into a single PDB, and if so, what appropriate parameter values are to be used.

The number of plant damage bins will be reduced from the maximum number (all possible combinations of parameter values) to a smaller subset, depending on the particular plant configuration's limits on the possible combination of consequence parameter values. By using the consequence parameters and PDBs to rigorously define the interface between the plant system analysis, and the consequence analysis, the potential for miscommunication within the analysis team is reduced.

Perform Physical Processes Analysis

After the PDBs have been defined, the physical processes analyst has a list of unique consequence states to analyze. If the quantification process for those bins has been completed, the analyst has an ordered set of unique consequence states to aide in his planning process. The analyst can simplify his analysis to single sequences from a PDB and therefore optimize the resources of the physical processes analysis. Probably most important however is a clearer understanding by all participating, the systems analyst, the physical processes analyst, and the manager; and, of course with a clearer understanding, a higher probability that the overall analysis is correct.

REFERENCES

1) PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants, Review Draft, September 28, 1981, NUREG/CR-2300.

2) Reactor Safety Study, An Assessment of Accident Risk in U. S. Commercial Nuclear Power Plants, U. S. Nuclear Regulatory Commission, 1975, WASH-L400, NUREG-75/0L4.

3) L. T. RITCHIE, W. D. BROWN, and J. R. WAYLAND, 1976. Effects of Rainstorms and Runoff on Consequences of Nuclear Reactor Accidents, SAND 76-0429, Sandia National Laboratories.

4) Zion Probabilistic Safety Study, Commonwealth Edison Company, 1981.

5) L. S. NELSON, and P.M. DUDA, Steam Explosion Experiments With Single Drops of CO_2 Laser-Melted Iron Oxide. ANS Transactions, Miami, 1981.

A MATHEMATICAL FRAMEWORK FOR QUANTITATIVE EVALUATION OF SOFTWARE RELIABILITY IN NUCLEAR SAFETY CODES

by

C. J. Mueller, E. E. Morris, and C. C. Meek*
Argonne National Laboratory

W. E. Vesely**
Nuclear Regulatory Commission

ABSTRACT

This paper describes and illustrates a mathematical framework designed to establish quantitative predictions of reliability for the computer software used in the nuclear industry. The framework consists of four parts: 1) a classification system for software errors and code failure; 2) probabilistic modeling for selected reliability characteristics; 3) multivariate regression analyses to establish predictive relationships among reliability characteristics and generic code property and development parameters; and 4) the associated information base. Illustrations of the role that these supporting models can play in assessing codes relevant to nuclear safety are also presented.

INTRODUCTION AND SUMMARY

This paper describes and illustrates an analytic framework developed as part of a research program sponsored by the Nuclear Regulatory Commission (NRC) that is designed to establish quantitative predictions of reliability for the computer software used in the nuclear industry. The framework relies on Poisson modeling and is more readily adapted to the analysis of codes which operate in the batch mode than are the failure rate models [1] currently used in the aerospace and communications industry. The importance of quantitative predictions of software reliability has been discussed in Ref. 1. The increasingly important role of computers in reactor design and safety analysis as well as the need for improved on-line information processing were cited as reasons why software reliability should be taken into account in the assessment of risks associated with nuclear power plants. Fabic [2] has noted that both programming errors and a variety of plant and modeling uncertainties affect the accuracy of a safety code in predicting the response of a plant to a nuclear accident. The consequences of software errors in reactor analysis codes include such things as unsafe hardware design, unsafe operational and safety parameters (e.g., trip settings), and erroneous predictions of plant lifetime related parameters. The presence of software errors in on-line systems can lead to delayed or erroneous control and operator actions, and even to unnecessary forced outages.

*Present Address: Exxon Production Research Company
**Present Address: Battelle Columbus

PUBLISHED QUANTITATIVE SOFTWARE RELIABILITY MODELS

Published software reliability models were first developed in the military, aerospace and communications industries where they are used in nearly all phases of software development, testing, and quality assurance. In a recent paper [1] representative models were applied to common software failure data bases for comparison and evaluation. The results of these studies pointed out existing model highlights and deficiencies. In general, these models assume various functional forms for the code failure rate λ. These functions are then fit to failure data to estimate, generally using maximum likelihood, values for the model parameters so as to arrive at the reliability

$$R(t) = \exp\left[- \int_0^t dt'\lambda(t') \right]. \qquad (1)$$

These models have been used almost exclusively for estimating the failure rate of continuous-running codes.

However, analysis codes which comprise a major fraction of the computer codes relevant to nuclear safety, are discrete task codes. So long as errors occur infrequently, it should be possible to apply failure rate models to these codes provided the time is the accumulated CPU time for all runs, and provided the codes are run on identical computers with identical compilers. However, detection rates obtained for a code operation on one computer are not necessarily the same as detection rates for operation on another computer. This is especially important in the case of nuclear safety analysis codes which are often developed on a single computing system but are then exported to different computing systems throughout the country. In addition, if errors are detected too frequently, as might be the case for a code undergoing a new phase of testing, the run time assigned to an individual task might impose a structure on the error detection time which has little to do with the actual error occurrence rate. These reasons, as well as the nonconservative aspects of the existing models [1] made it necessary to develop the more comprehensive modeling described herein which is more naturally applied to discrete task codes and which can also be applied conservatively to continuous running codes.

THE COMPREHENSIVE FRAMEWORK WITH ILLUSTRATIONS

The ultimate goals of the framework herein are to:

1. Allow NRC to make an a priori estimate of a computer code's probability of successful operation given the code's general properties and its intended application. These properties include not only physical characteristics such as size, complexity and programming language but development and quality assurance parameters such as testing history and operational history after testing. It is to be emphasized that the usage or application of a code can be a strong determinant of its probability of successful operation.

2. Provide information for NRC to determine quantitative criteria for the acceptability of software relevant to nuclear safety for eventual use in the licensing arena.

With these goals, and the limitations of existing software reliability modeling as described above, a comprehensive framework was developed with four major components: (1) a categorization scheme(s) for classifying errors; (2) a Poisson model for the occurrence of software errors; (3) a multivariate regression analysis to establish the

role of code design, development, and testing parameters on error rates; and (4) sufficient data to make the first three components meaningful.

Error Classifications

To develop correlations between probability-of-failure characteristics and code properties, it is desirable to classify errors according to error type using one or more classification systems. A code error will be regarded as synonymous with a software error and is here defined as any defect in a line of code or in the input data which can cause the computer code to fail. Code failure includes abnormal termination, normal termination with erroneous results, or any other unacceptable departure of program operation from the required operation.

Table I shows one method of categorizing errors, failure, and code properties. In this table code execution failures are categorized according to their consequences and their software-error causal mechanisms; the controlling code properties and software development characteristics that are assumed to affect the failure frequency are categorized as shown. The detail in the table is presented for completeness--actual failure data are not detailed enough to support estimates of failure probabilities due to a specific faulty code unit, for example. However, by coarsely segregating the failure data according to potential consequence and probable cause, probability-of-failure characteristics may be categorized. For example, assuming sufficient failure data can be obtained, the probability of either a random (e.g., keypunch) or logical (e.g., incorrect implementation of an equation) error causing an execution failure of a specified type may be obtained. Although the current paucity of data precludes anything but gross estimates of such probabilities, even these can be used to make bounding estimates relevant to nuclear safety.

In general, two or three classification systems should probably be used simultaneously. In setting up error classification systems, the following general rules should be followed. First, error types should be mutually exclusive within a single classification system. Second, the number of errors of one type should be independent of the number of errors of other types within the same classification system. Third, ground rules should be clearly stated regarding how to count errors. Finally, when more than one classification system is in use, each system should result in the same total number of errors being counted.

Although, in general, it may be desirable to set up classifications that are not programming language specific, the following example illustrates how a single classification system for a program written in FORTRAN might be set up. Error types are defined according to whether they occur in

1. Input Data,
2. Arithmetic or Logical Assignment Statements,
3. Input or Output Statements,
4. Data Initialization Statements,
5. Specification Statements,
6. Subprogram Statements,
7. Control Statements.

A specific FORTRAN manual would be identified to resolve questions as to what FORTRAN statements fall into each of these types. In addition, one might stipulate that statements that are out of order or misnumbered would be counted as control statement errors and that more than one error in a single statement would be counted as a single

error. The question as to whether the number of errors of one type is independent of the number of errors of other types with this classification system is not obvious. One may simply have to assume independence with the understanding that whenever possible, statistical tests will be performed to test the assumption.

Probabilistic Modeling - A Poisson Model

Let X_{jk} be a random variable defined as the number of errors of type k in classification system j detected as the result of a given run. The expected value of X_{jk} will be denoted by Λ_{jk}. The probability distribution for X_{jk} is assumed to be Poisson, i.e.

$$P(X_{jk} = x) = \frac{\Lambda_{jk}^{x}}{x!} e^{-\Lambda_{jk}} \qquad (2)$$

where x is a non-negative integer. If the values for X_{jk} are independent for each error type k and if the error types are mutually exclusive, then it can be shown that the probability distribution for the total number of errors X, defined as

$$X = \sum_{k} X_{jk} , \qquad (3)$$

is also Poisson, i.e.

$$P(X = x) = \frac{\Lambda^{x}}{x!} e^{-\Lambda} , \qquad (4)$$

where

$$\Lambda = \sum_{k} \Lambda_{jk} . \qquad (5)$$

With this model, the reliability is

$$R = P(X = 0) = e^{-\Lambda} \qquad (6)$$

The use of the Poisson distribution has certain mathematical advantages. First, the Poisson distribution is often used to approximate the binomial distribution. There may be instances where it is useful to model the detection of errors of type k in terms of M_{jk}, the number of code units (lines of code, instructions, or some other unit) capable of producing type-k errors, and the probability q_{jk} that an error of type k is detected in a given unit during a given run. If q_{jk} is the same for each unit and if error detection in each unit is independent of error detection in other units, then the probability distribution for X_{jk} will be binomial with parameters M_{jk} and q_{jk}. In general, M_{jk} is likely to be large and q_{jk} small. The binomial distribution can then be approximated by the Poisson distribution in (2) with

$$\Lambda_{jk} = M_{jk} q_{jk} . \qquad (7)$$

In (7) failure data may be used to estimate Λ_{jk} or q_{jk} directly; some other source such as expert opinion or the human error literature, using analogous error probabilties to estimate q_{jk}, may also be used. Of course, the value of M_{jk} is provided from the code properties or specifications.

A second advantage arises for codes that are conveniently described in terms of error detection rates as in (1). For runs of duration t, the probability distribution for X_{jk} is seen to be given by the Poisson distribution in (2) with

$$\Lambda_{jk} = \int_0^t dt' \, \lambda_{jk}(t') \, . \tag{8}$$

The reliability estimates (1) and (6) become identical in this case.

Finally, for a given error type and classification system, only one parameter needs to be estimated for the Poisson distribution in (2). The accumulation of appropriate failure data is needed to verify whether values of Λ_{jk} obtained for a code operating on one computing system can be applied to the same code when it operates on a different computing system.

This model can be manipulated to provide estimates of various pertinent reliability characteristics such as the expected number of errors or the number of errors per machine language instruction. Once these have been made for several codes, correlation of these values with other code characteristics can be explored using the multivariate regression analysis capabilities found in many standard statistical analysis code packages.

Multivariate Regression Analyses

Tabulating the controlling variables associated with each code and its failure history must be done to obtain the dependencies among the probability-of-failure characteristics and the code properties. A statistically meaningful number of codes must be investigated so that these characteristics can be correlated. Obtaining these failure data is considered the most difficult part of implementing this framework and is discussed below. Given that the appropriate failure data can be obtained and probability characteristics calculated, then regression analyses can be performed to identify the most important properties and controlling variables in software development. This knowledge can be used as a basis for defining development or quality assurance criteria for codes used or proposed for the licensing arena.

To illustrate the use of regression analyses to correlate failure probability characteristics with code properties and development variables, a log-linear form for error content per line of instruction was assumed as follows:

$$\ln (N-n)/I + a_0 + a_1 t + a_2 I + a_3 P. \tag{9}$$

where N = the estimated number of total errors, available from existing failure rate modeling,
and n = the observed number of errors,
t = time in working days,
I = number of lines of instruction,
and P = number of code programmers,

all of which were available from published [3] software failure data for several codes.

Fits of the log-linear expression were then made to the data using the BMDP statistical analysis system [4]. Although the analysis was done solely for illustration of the methods and using very sparse data from only several codes the effects of the variables on error content satisfied "reasonableness". For example, error content decreased with time due to debugging, increased with number of programmers (suggesting inefficient coordination of the programming effort), and decreased with increasing number of lines of instruction.

Software Failure Data

Regarding the implementation of this framework, several conclusions relating to data needs and efforts to acquire these data are as follows:

(1) All data obtained to date and collected comprise only a small part of the information base needed to fully realize the goals of this framework.

(2) The acquisition and appropriate categorization of nuclear software failure data is a time-consuming but necessary component of this program. Categorizing the bugs according to the types of code defect consequence and cause categories is required as discussed earlier. To accomplish this will undoubtedly require some subjective categorization. Extended categorizations come to mind: for example, an important concern for nuclear safety is the probability with which an operational failure of a code or a documented code bug result in a misleading code result upon which an unsafe design decision or incorrect safety conclusion is made. No data to estimate this propagation probability have been found or indeed can be assumed to exist. Thus, expert opinions would have to be solicited and factored in to assign such a probability.

(3) Existing data are largely from testing phases of codes. Post-release or production status data must be sought. Clearly the aforementioned goals relate to production codes, not test versions. Drawing comparisons between the failure probabilities of pre- and post-release codes must be done to obtain the benefits of a large pre-release data base. However, the mathematical approach to treating the data is the same.

CONCLUSIONS

A general mathematical framework for predicting reliability characteristics has been established. At the core of this framework is a Poisson model for the number of code errors of a specified type in a given computer application. Methods of implementing this framework have been developed and include both mathematical modeling and the proper specification, classification, and handling of failure data. The product of this framework includes predictions of reliability characteristics such as expected number of errors and probability of failure in a given computer run. By accumulating failure data and specifying the code characteristics associated with each data set, multivariate regression techniques can be used to identify the important code parameters and controlling developmental parameters. Illustrations of such analyses were presented.

Specific areas within the framework that must be dealt with include the proper classification of software errors, and failures both for data organization and subsequent regression analysis. With respect to the regression, the optimum choice of dependent variables needs to be established. For example, in the Poisson model, the

expected number of errors may be amenable to regression. However, regression analysis may be performed directly on the reliability. Investigation of the number of errors per instruction in a code is useful since this quantity is a convenient figure of merit with which to measure the developmental progress of a code.

Although these concepts bear investigation, an overriding factor is that the data that will become available in the near term, say several years, simply do not justify the development of sophisticated mathematical modeling. Thus, a pragmatic approach dictates that in the near term, data acquisition efforts dominate future research.

ACKNOWLEDGEMENTS

This work was performed under the auspices of the U. S. Nuclear Regulatory Commission.

REFERENCES

1. H. KOMORIYA, C. MUELLER, and E. E. MORRIS, "Quantitative Software Reliability Analysis in Nuclear Safety," Proc. ANS/ENS International Meeting on Probabilistic Risk Assessment, September, 1981.

2. S. FABIC, "Code Assessment for Nuclear Reactor Accident Analysis Programs," Trans. Am. Nucl. Soc., 35, 254 (1980).

3. C. J. Mueller, H. KOMORIYA, C. C. MEEK, E. E. MORRIS and W. E. VESELY, "Quantitative Software Reliability Analysis of Computer Codes Relevant to Nuclear Safety," NUREG/CR-2186, also ANL-81-84, December, 1981.

4. W. J. DIXON and M. B. BROWN, ed., BMDP-79 Bio-medical Computer Programs P-Series, University of California Press, Berkeley, 1979.

Table I. Categories[1] of Operational Failures, Causal Mechanisms, and Controlling Properties and Development Variables in Software Reliability

Operational Failures		Causal Mechanism	Controlling Properties and Developmental Variables		
Type of Consequence	Faulty Code Unit	Faulty Modeling Unit	Type of Cause		
			In-Code[2]	Testing	Programming
1. No output (i.e. a crash)	1. Symbol	1. Constant	1. Random (e.g. key punch)	1. Quality assurance methods	1. Size
2. Absurd output (detectable)	2. Operand	2. Variable	2. Logical or decisional (incorrect or poor programming to implement modeling) analytic	2. Size of QA effort	2. Complexity
3. Misleading output (may propagate failures in nuclear plant design or operation)	3. Constant	3. Equation	Ex-Code	3. Capability for benchmarking or verification	3. Language
	4. Variable	4. Model (set of equations)	3. Documentation leading to misuse of code (e.g. design, safety assessment, monitoring, control)	Operational	4. Structure and method of coding
	5. Line (statement)	5. Table (e.g. property values)	2. History (time, numbers of runs and failures since release)	1. Application	
	6. Storage byte or array (e.g. common block)				
	7. Logic block (subroutine)				
	8. Logical directive (e.g. IF statement)				

[1]This table illustrates a plausible way of categorizing failures, their causes, and dominant variables. Other ways could be chosen.

[2]In-code causes could also be subdivided as follows: 1) "Pure" programming causes such as syntax errors or incorrect transfers of program control, logic, or data; 2) Program modeling causes such as incorrect algorithm approximations or improper treatment of singular points or critical parameters leading to overflow and roundoff errors.

COMPARISON OF DETERMINISTIC AND STOCHASTIC TECHNIQUES FOR ESTIMATION OF DESIGN BASIS FLOODS FOR NUCLEAR POWER PLANTS

S.I. Solomon and K.D. Harvey

Department of Civil Engineering
University of Waterloo
Waterloo, Ontario, Canada N2L 3G1

G.J.K. Asmis

Atomic Energy Control Board
Ottawa, Ontario, Canada K1P 5S9

ABSTRACT

The IAEA Safety Guide 50-SG-S10A recommends that design basis floods be estimated by deterministic techniques using probable maximum precipitation and a rainfall runoff model to evaluate the corresponding flood. The Guide indicates that stochastic techniques are also acceptable in which case floods of very low probability have to be estimated. The paper compares the results of applying the two techniques in two river basins at a number of locations and concludes that the uncertainty of the results of both techniques is of the same order of magnitude. However, the use of the unit hydrograph as the rainfall runoff model may lead in some cases to non-conservative estimates. A distributed non-linear rainfall runoff model leads to estimates of probable maximum flood flows which are very close to values of flows having a 10^6 - 10^7 years return interval estimated using a conservative and relatively simple stochastic technique. Recommendations on the practical application of Safety Guide 50-SG-10A are made and the extension of the stochastic technique to ungauged sites and other design parameters is discussed.

1. INTRODUCTION

The IAEA Safety Guide 50-SG-S10A[1] recommends that design basis floods be estimated by deterministic techniques using probable maximum precipitation (PMP)and a rainfall runoff model to evaluate the corresponding probable maximum flood (PMF) as the design basis flood for nuclear facilities. The Guide indicates that stochastic techniques are also acceptable, in which case floods of very low probability have to be estimated. World Meteorological Organization[2] made recently similar recommendations. AECB has initiated during the last three year studies[3,4] through an engineering consulting firm having the objective of developing the techniques required for the application of these recommendations and of comparing their results when applied to two Canadian rivers. Additional objectives of these studies were to estimate the intrinsic (and generally not recognized) uncertainty related to the application of the deterministic technique, to investigate the possibilities of applying the techniques to ungauged river sites, and of extending it to other design parameters. The main results obtained so far in these studies, based on the application of the two techniques to two river basins at several locations, are presented in this paper.

2. DETERMINISTIC TECHNIQUES

The application of deterministic techniques to the estimation of the design basis flood involves three stages: the development (or adaptation) of a so called deterministic rainfall runoff model to the basin under consideration, the estimation of the PMP for that basin, and the simulation of the PMF as an output of the rainfall runoff model when the PMP is used as input. All three stages involve significant uncertainties.

The two river basins which were used as testing grounds for the analysis are those of the Grand River and the Serpent River. Their location is shown in Figure 1. The basins present significant differences from the viewpoint of climate, surficial geology, and vegetation. Both river basins are in a temperate climate zone, but the Grand River has a relatively moderate temperature variation, whereas in the Serpent River this variation is extreme. The Grand River basin is covered by relatively thick soil, whereas the soil cover in the Serpent River, which is located in the Canadian Shield, is thin. Most of the Grand River has been deforested for agricultural and urban development and, except for three relatively small man made lakes, there are no lakes of significance in this river basin. Most of the Serpent River basin is covered by forest, and a significant portion (20%) by lakes, which reduce to a very large extent the variation of flow.

In both river basins two different rainfall runoff models were used, as well as two different values of PMP, as obtained from two different sources. This was done to illustrate the uncertainties of the so called deterministic techniques.

The first rainfall-runoff model is the unit hydrograph (UH) technique, since it is the one specifically mentioned in IAEA[1] and is widely used. The major assumptions of the unit hydrograph technique is that the river basin response to a precipitation input is linear, i.e. that precipitation and flow vary according to a linear relationship. In fact it is well known that this assumption is not supported by experience or theoretical analysis, and - from the viewpoint of estimation of design basis flood - is non-conservative. The shape and peak value of a unit hydrograph may vary greatly with the characteristics of the generating storm. To illustrate this, two different unit hydrographs were considered in the study of the Grand River, at the Galt gauging station (drainage area 3495 Km^2). The first was the "official" one, i.e., the one accepted at an official inquiry on a flood event by the Grand River Commission Authority, the second was based on a recent (1975) storm in the basin. The peak flow value of the second unit hydrograph is about 2.5 times larger than that of the first. The shape was accordingly different (Figure 2).

The two sources for estimating PMP were Bruce[6] and Soil Conservation Service[7]. The value estimated by the latter in the area of interest is about 37% larger than that recommended by the former in the Grand River basin and 50% in the Serpent River basin. Probable maximum flood peak values obtained by applying the two techniques and the two values of PMP in the Grand River basin at the Galt gauging station lead to the results shown in Table I. Similar results were obtained in the Serpent River basin (Table II).

3. STOCHASTIC METHOD

Stochastic methods are techniques of combined deterministic and statistical analysis and synthesis of time (space) series of data with the purpose of extending such series and defining from the extended series the magnitude of rare events. To put stochastic methods in proper relation to the deterministic ones, one may state that the former attempt to determine by the analysis-synthesis process the asymptote of the frequency curve that is directly estimated by the latter. The application of stochastic methods in hydrology has been discussed by Kisiel[8], Kotegoda[9] and Yevjevich[10,11], etc.

TABLE I

Comparison of PMF Estimates
Obtained Using Two Different Rainfall-Runoff
Models and Two Different PMP Estimates

Model	PMP Estimate According to	PMF Peak Value (m^3/s)
Official UH	Bruce	11,499
	Soil Conservation Service	15,746
1975 UH	Bruce	22,175
	Soil Conservation Service	30,303
Distributed rainfall-runoff model	Bruce	41,348
	Soil Conservation Service	67,969

Because of the combined deterministic-statistical treatment of the time series of data, it is possible to estimate the error or the confidence limits affecting the results obtained from a stochastic method. This provides a basis for estimating the risk related to the use of certain design basis values.

In contrast to the deterministic methods, the stochastic methods do not provide a continuous flood hydrograph and related information on rate of change in flow (levels). Therefore, when stochastic methods are applied it is necessary to make additional hydrologic computations to estimate a reasonably conservative set of hydrologic parameters required for NPP siting and design. Such parameters include at least: discharge peak and variation during the flood event; and velocities, average and variation in the cross section for important discharge values including the peak one. As these hydrological characteristics are easier to obtain when deterministic methods of flood estimation are used, it appears advisable to apply both techniques and use the stochastic technique to evaluate the probability of the deterministically estimated peak flood. This was in fact the approach used in the studies reported in this paper.

3.1 Stochastic Analysis

Stochastic methods of analysis of time (space) series proceed from the assumption that such series represents a numerical expression of a process generated by a limited number of definable and significant causes, and an infinite number of small causes. The first type of causes are initially identified in the analysis and their effect removed from the data series. In fact, in some actual cases of time series analysis it may happen that the effect of a significant cause is identified, but the cause itself can not be clearly defined. The residual component, which presumably represents the effects of a large number of small causes is then subject to statistical analysis. As a result of this analysis, one obtains a series of parameters of the time series that define the significant causes and the statistical characteristics of the residual component. If the hypothesis that the residual component represents the result of a large number of small causes is valid, then the corrollary is that its distribution is normal and can be defined by two parameters (mean and standard deviation). Tests of normality of the residual distribution can be thus used to indicate if the hypothesis is acceptable or not. In case of significant departure of residuals from normality the analysis must be iterated and the search for important factors leading to non-normality of the residuals expanded. It should be pointed out that the parameters defining the significant causes as well as the residual distribution are

only estimates of the actual values since they are defined on the basis of a limited number of data (a sample) belonging to an infinite population. Thus, all parameters of the series are affected by time sampling errors and this must be recognized in the stochastic synthesis.

3.2 Stochastic Synthesis

Having determined the time series parameters, it is in theory possible to express the flood of a given probability of exceedance in terms of these parameters. However, in some instances the sequence of flood values in time is required for simulation purposes. In such cases a long sequence of flows is generated by a Monte Carlo technique and the probability of the extreme estimated from it. In order to account for the time sampling errors of the time series parameters, the synthesis by Monte Carlo techniques has to be extended not only to the synthetic generation of the random component, but also to the generation of the other parameters of the series.

As in other cases of hydrologic models with uncertainties regarding basic assumptions, the model should be validated using split sampling techniques. The errors of the validation sample are the ones that should be used to make statistical or judgemental inferences about the validity of the model. Such inferences made on the basis of the errors of the calibration sample may be misleading since in some cases the model represents an exercise in curve fitting, rather than a mathematical formulation of valid physical and statistical relationships.

3.3 Application of Stochastic Methods

Stochastic methods require for practical application, the availability of computer technology. Nevertheless, such application should be made by means of techniques that can be readily understood and checked at each step in the course of the computation. The method suggested is believed to possess these qualities. In addition, it has been successfully tested in a large scale study carried out a few years ago in Canada.[12]

The stochastic technique suggested can be applied both to gauged and ungauged sites. When applied to an ungauged site, the technique involves the synthesis of time series parameters which have larger errors, resulting from the interpolation involved to estimate them.

3.3.1 Gauged site

A site is considered gauged in the following circumstances:

(a) If there is a long period of record at the site. A long period of record is defined for middle and higher latitudes (north of 40°N and south of 40°S) as 30 years and for lower latitudes as 50 years of record, provided there have been no extreme meteorological events in the region that have not affected the relevant basin; otherwise 50 and 70 years respectively.

(b) If the period of record can be extended by correlation with one or two other gauges to a period of record equivalent to that indicated above. The computation of the equivalent number of years should be carried out as indicated by Fiering.[13]

(c) If it can be demonstrated that the period of record provides a time series of data having an error variance less than the error variance obtained from a regional analysis. This check should be made in accordance with the methodology developed by Matalas and Gilroy[14].

The time series to be used consists of the series of maximum instantaneous or maximum daily flows within a selected time interval Δt. The use of instantaneous

maximums would be preferred if data are available in this form. However, in most cases maximum daily flows will be considered and relationships between maximum dailies and instantaneous maximums used to correct the final results. The time interval Δt is selected by considering various successively longer time intervals selecting the corresponding maximum flows, eliminating the seasonal component as shown below and computing the autocorrelation coefficients for the various intervals. The time interval selected would be the last but one for which the autocorrelation coefficient becomes insignificant.

The effect on flows of various causes is multiplicative rather than additive. In view of this, time series of flows are analyzed after a logarithmic transformation of the data.

The time series with the selected time interval is then analyzed for definable significant causes and their effect eliminated. The usual definable significant causes that should be considered are:

(a) seasonal variation of meteorological conditions
(b) causes that may produce trends (e.g. urbanization, deforestation)
(c) causes that may produce jumps (construction of large reservoirs, diversions)
(d) effect of storage.

The seasonal effect is removed from the time series by subtracting from each value the mean value corresponding to the given season. Obviously, where Δt is one year or longer the seasonal effect does not exist. Thus for each Q_{ij}, where i represents the year and j the season the value:

$$\Delta_{ij} = Q_{ij} - \bar{Q}_i$$

is calculated where Q_{ij} is the logarithm of the flow for the given i season, j year, and $\bar{Q}_i$ is the mean for the i season.

Trends can be detected by graphical and statistical analysis (Yevjevich,[10,11]) of the time series and search of causes. Graphical analysis can be carried out by means of moving - average graphs. Detected trends should be removed only if statistically significant at the 95% confidence level and supported by evidence of physical activity in the basin, or significant at the 99% level. Trends are considered in the computation by their linear approximation. Where a trend in the mean has been detected for a period starting from Δ_{kl} and ending at Δ_{gt} which are m Δt apart, and and at the last point Δ_{gt} represents a total departure from the average up to Δ_{kl} of δ_1, each value A_{ij} in the interval is corrected as follows

$$\Delta'_{ij} = \Delta_{ij} - \frac{\delta_1 \cdot b}{m} \qquad (a)$$

where b is the number of time intervals separating Δ_{ij} from Δ_{kl}.

Jumps (steps) are also identified by graphical and statistical analysis (Yevjevich,[10,11]) and their existence accepted using conditions equivalent to those set up for trends. Attention has to be paid to temporary jumps that may occasionally occur particularly in connection with the filling of large reservoirs. If a positive jump δ_2 occurs in the mean starting from value Δ_{mn} the value Δ_2 is added to all values Δ_{ij} preceding Δ_{mn}

$$\Delta''_{ij} = \Delta_{ij} + \delta_2 \qquad (b)$$

The effect of storage is removed by computing the autocorrelation coefficient r for the series Δ_{ij} corrected for trends and jumps as shown above. The removal of the effect is made by computing ε_{ij} values from the relationship:

$$\varepsilon_{ij} = \Delta_{ij} - r\Delta_{i,j-1} \qquad (c)$$

ε_{ij} time series represents the random component of the time series.

Tests of normality of the distribution of ε_{ij}'s are carried out (Yevjevich[15]). If the distribution of ε_{ij} is found to be significantly different from a normal one a search for outliers is carried out. If outliers are found to be the cause of non-normality, they are considered as one additional special significant cause (e.g., hurricanes in areas with infrequent occurrences of hurricanes, ice jams of exceptional size, etc.) and treated as such, i.e., removed and introduced at random intervals equivalent to intervals of their observed occurrence. The statistical characteristics of outliers are synthesized on the basis of the observed statistics by Monte Carlo techniques as shown further for other parameters of the time series.

If after consideration and removal of outliers ε_{ij} is not normally distributed the analysis is iterated. In iteration the following additional possible causes of non-normality are investigated:

- seasonal variation in storage leading to a seasonal variable r
- changes with time of the storage characteristics of the basin leading to trends and/or jumps in the value of S.

After obtaining a normally distributed series of ε_{ij}'s their standard error S is estimated. The latter, together with the values Q_i and S constitute the parameters of the time series. The standard error (E_p) of each of the time series parameters "P", (i.e. $\bar{Q}_i$, r, S) is computed using the formulas shown in Yevjevich[15] and N sets of values of each parameter are obtained by means of appropriate Monte Carlo techniques. The number N is obtained by dividing the number of years for which synthesis is intended by the number of years of record. For each of the above parameters P a number N of P_k values is calculated using the formula

$$P_k = \bar{P} + \eta_k E_p$$

where P_k is one of the N values of P, $\bar{P}$ is the estimated value of P, η_k is normally distributed random variate with zero mean and standard deviation equal to one.

Each value of S_k is used to synthesize a time series sample of ε_{ij} having a size equal to that of the recorded sample by means of the equation.

$$\varepsilon_{ij} = S_i \eta_{ij}$$

Each set of ε_{ij} is used to synthesize a corresponding set of Δ_{ij} by means of a synthesized value of r equation

$$\Delta_{ij} = \varepsilon_{ij} + r\Delta_{i-1,j}$$

If applicable, effects of trends and jumps are introduced by reversing equations (a) and (b).

For each set of Δ_{ij} a set of Q_{ij} is computed by means of synthesized $\bar{Q}_i$ values and the formula

$$Q_{ij} = \Delta_{ij} + \bar{Q}_i$$

Effects of causes related to outliers is introduced using Monte Carlo techniques as for any parameter.

A number of samples of time series can then be combined to give samples of the length required for the analysis. These samples can be analyzed for maximum annual flows and probability curves obtained from the synthesized data arrays in the same manner as in the case of the analysis of recorded data (Yevjevich,[10,11]).

By creating 100 samples of same length and analyzing as indicated above each sample separately, one obtains for each probability of interest 100 values. When arranged in a decreasing (or increasing) array these provide values the most probable estimates for the given probability (the median value) and confidence limits corresponding to various percentages (obtained by selecting the data on the 100 synthetic array corresponding to the given confidence limit percentage).

The mean daily maximum flows of one of the rivers studied (Grand River at Galt) were analyzed as indicated above. The analysis showed that the length of a season for this river basin is three months. The results obtained by analyzing mean daily flows were used to synthesize 100 samples of 10,000 years of maximum flows. For this purpose it was necessary to generate over 4 million random normally distributed numbers to be used in the process of synthesis.

Each 10,000 year series was synthesized by generating 167 series of 60 years. For each of the latter series the four seasonal mean values and the standard deviation of the second order component, and the auto-correlation coefficient were synthesized separately adding to their mean recorded values a random component. Each random component was obtained by multiplying a different random number from a normal distribution (0 mean, standard deviation equal to one) by the standard error of the corresponding parameter.

Each of the 100 samples was examined to establish the probability of exceedance of a number of 15 given (reference) flows ranging from 2,000,000 to 800 cfs. In addition the largest and the smallest generated seasonal maximum mean daily flow was also extracted from each 10,000 year synthetic series. The results are summarized in Table III.

The flow exceedance data shown in Table III were used to calculate the maximum flow with a probability of exceedance of 10^{-4} and the 5, 10, 90 and 95% confidence limits. The maximum mean daily flow with probability of exceedance of 10^{-4} years has a value of about 661,300 cfs (18,728 m^3/s) with lower and upper 95% confidence limits of 468,700 and 1.071,900 cfs, cfs (13253 and 30300 m^3/s) respectively. Furthermore, if all 100 samples of 10,000 years are considered together, it follows that the maximum mean daily flow with a probability of exceedance of 10^{-6} years is about 1,442,000 cfs (40,837 m^3/s).

To obtain an estimation of the corresponding maximum instantaneous flows, a graphical relationship between maximum instantaneous and maximum mean daily flows for the period of record was developed (Figure 3). This relationship indicates that the ratio between the two sets of flows is on average 1.4 but may be occasionally higher (up to 1.8). The analysis of the results of the non-linear distributed model indicates that this ratio may be for very large flows slightly over 2. Given that most instantaneous flows are affected by errors that are much larger than those affecting the maximum mean daily flow, it is considered conservative to assume that the ratio of the maximum instantaneous flows with a return probability of 10^{-4} and 10^{-6} years are about 1,300,000 and 2,900,000 cfs (36,916 and 82,128 m^3/s) respectively. In other words, the flows estimated by means of the PMP-PMF distributed model have a return probability varying between 10^{-4} and 10^{-6} years.

3.3.2 Ungauged Sites

When a site is ungauged but there are gauges in the region, it is still possible to apply the stochastic technique . This is done by synthesizing time series parameters at the site from relationships between the time series parameters and the

corresponding physiographic characteristics of the respective beams.

The application of the technique in this case requires that stochastic analysis is carried out as shown in 3.3.1 at each gauged site and the values of the time series parameters ($\bar{Q}_i$'s, r, and S) defined. The mean standard error of each parameter is also estimated as the mean of the standard error at each site.

Correlations between each of the time series parameters as dependent variable and the corresponding physiographic characteristics of each basin which may have a bearing on the maximum flow, such as drainage area, percent lake area, percent forest area, percent urban area, slope, and others as independent variables are developed (Solomon and Jolly[12]). The values required to calculate the standard error of each estimate (Solomon[15]) are retained for each of these correlations.

The correlations are then used to estimate the time series parameters at the ungauged site. The error of each parameter is calculated as the square root of the sum of the square of the average error of time sampling of the parameter and the square of the error of estimate from the correlation between the given time series parameter and the corresponding physiographic characteristics of the river basin. Once the time series parameters and their error of estimate have been calculated, the time series synthesis proceeds exactly as for gauged sites (3.3.1).

This technique was used in the second river basin studied (Serpent River). Results of validation of the technique when applied to a neighbouring river basin (Aux Sables et Massey) which was not used in the model development (are shown in Figure 4). The frequency curve obtained (average curve) is very consistent with the empirical frequency curve obtained on the basis of 65 years of record. The wide spread of the 90% confidence limits reflect the large uncertainty resulting from the combined error of time sampling and error of estimates by correlation.

The application of the stochastic technique was refined in this case to take into account the influence on maximum flows of changes in basin conditions due to man's activity, in particular filling of some of the lakes with tailings. The technique was used in parallel with deterministic models which were adapted in the framework of the study to estimate the design basis floods in three basins of interest before and after development including the effect of filling of a large lake with tailings. The results are summarized in Table II. They indicate that values of PMP calculated using deterministic techniques are of the same order of magnitude as flows with a return probability of 10^{-6} to 10^{-7} years, at the 50% and 90% confidence levels.

4. STOCHASTIC TECHNIQUES APPLIED TO WIND TIME SERIES

The stochastic technique can be readily extended to other time series with or without seasonal components. As an illustration of such extension the time series of winds located in or near the Serpent River basin were analysed as discussed in Chapter 3. As a result of time series synthesis it was concluded that maximum wind speed with a return probability of 10^{-6} to 10^{-7} years is of the order of 160-167 km/h. This compares well with estimates made by means of deterministic considerations.

5. CONCLUSIONS

Stochastic and deterministic techniques lead to comparable estimates of the design basis flood provided that the probability of exceedance for estimating the design basis flood by the stochastic technique is 10^{-6} to 10^{-7} years.

Conservation requires that a distributed non-linear model is used as the deterministic technique and that the values corresponding to the upper 90 to 95% confidence

limit values are selected when applying the stochastic technique.

The stochastic technique can be extended into a regional stochastic technique applicable to ungauged sites. Such regional model can be adjusted to reflect the influence of man-induced changes on the maximum flows with various probabilities of exceedance.

Both the rainfall runoff model and the unit hydrograph technique can be readily applied to ungauged sites and can be further extended to incorporate the influence on the PMF or other floods generated by severe storms of changes in percent area of lakes. However, the absolute values of the PMF obtained by means of the unit hydrograph technique are significantly lower than those obtained using the two other techniques. This result indicates that the use of the unit hydrograph technique in estimating PMF values is not conservative.

The stochastic technique can be used to estimate maximum wind speed values of extremely low probability of exceedance. The application of the technique in the Serpent River basin area, indicates that the maximum wind speed with a probability of exceedance of $1/10^7$ years in this area is about 160 km/h. The extension of the technique to other design parameters is also possible.

REFERENCES

1. International Atomic Energy Agency (1980) Determination of design basis floods for nuclear power plants on river sites - a safety guide, Draft of Safety Series No. 50 SG-S10A, Vienna, Austria.

2. World Meteorological Organization (1981) Meteorological and Hydrological Aspects of Siting and Operation of Nuclear Power Plants, Volume II, Hydrological Aspects, by S.I. Solomon in collaboration with G.E. Evans, Technical Note No. 170, WMO Publication No. 550, Geneva, Switzerland.

3. Shully I. Solomon & Associates Limited (1980) Development and Comparison of Techniques for Estimating Design Basis Flood Flows for Nuclear Power Plants - Phase I, Report for Atomic Energy Control Board of Canada.

4. Shully I. Solomon & Associates Limited (1982) Development and Comparison of Techniques for Estimating Design Basis Flood Flows for Nuclear Facilities, Phase II - Application to Serpent River Basin, Report for Atomic Energy Control Board of Canada.

5. Shully I. Solomon & Associates Limited (1974) A Hydrologic Model for Environmental Impact Assessment in the Rouge, Petticoat, and Duffins Watersheds, Report for North Pickering Project, Ontario Ministry of Housing, Toronto.

6. Bruce J.P. (1957) Preliminary estimates of Probable Maximum Precipitation over Southern Ontario, Engineering Journal, Vol. 40, No. 7, July pp. 978-984.

7. Soil Conservation Service (1974) Design of Small Dams, U.S. Department of the Interior, Bureau of Reclamation, A Water Resources Technical Publication, U.S. Government Printing Office, Washington.

8. Kisiel, C.C. (1969) Time series analysis of the hydrologic data, Advances in Hydrosciences, Vol. 5, V.T. Chow Editor, Academic Press, New York.

9. Kottegoda N.T. (1980) Stochastic Water Resources Technology, MacMillan Press, London.

10. Yevjevich, V. (1972) Stochastic Processes in Hydrology, Water Resources Publications, Fort Collins, Colorado.

11. Yevjevich, V. (1976) Chapters 1 to 4 in Stochastic Approaches to Water Resources, H.V. Shern, Editor and Publisher, Fort Collins, Colorado.

12. Solomon, S.I. and Jolly, J.P. (1976) Regional Analysis of Maximum Flows for Streams crossed by the Proposed Arctic Gas Pipeline. Report prepared by Shawinigan Engineering Co. Ltd. for Northern Engineering Services Limited.

13. Fiering, M.B. (1963) Use of Correlation to Improve the Mean and Variance, U.S. Geological Survey Prof. Paper 434 C.

14. Matalas N.C. and E.F. Gilroy (1968) Some comments on regionalization in hydrologic studies, Water Resources Research, Vol. 4, No. 6.

15. Solomon, S.I. (1966) Statistical association between hydrologic variables, in Statistical Methods in Hydrology, Proceedings of Hydrology Symposium No. 5. McGill University, published by National Research Council of Canada, Queen's Printer, Ottawa.

16. Yevjevich V. (1972) Probability and Statistics in Hydrology, Water Resources Publications, Fort Collins, Colorado.

TABLE II

PMF Values and Flows With Low Probability of Exceedance at Sites of Interest in the Serpent River Basin (m^3/s)

Site	PMF by unit hydrograph		PMF by rainfall-runoff model		Flows with low probability of exceedance (years)			
	Can PMP	US PMP	Can PMP	US PMP	50% confidence level 10^{-6}	50% confidence level 10^{-7}	90% confidence level 10^{-6}	90% confidence level 10^{-7}
Crotch Lake Outlet								
a) before development	25	42	112	190	31	40	136	195
b) after development	42	70	300	455	23	30	136	196
Stroth Lake								
a) before development	16	27	51	91	9	12	45	64
b) after development	22	36	73	129	17	21	76	109
Poppy Lake								
a) before development	18	28	38	65	8	11	49	71
b) after development	23	39	81	140	19	24	85	122

TABLE III
Probability of exceedance of given peak flows in 100 synthetic samples of 10,000 years

NUMBER OF YEARS THE FOLLOWING FLOWS WERE EXCEEDED

SET	MAX FLOW	$2x10^6$	$1x10^6$	$7x10^5$	$4x10^5$	$2x10^5$	$1x10^5$	$7x10^4$	$4x10^4$	$2x10^4$	10^4	$7x10^3$	$4x10^3$	$2x10^3$	$1x10^3$	$8x10^2$	MIN FLOW
1	645577.	0	0	0	2	55	407	817	2198	5184	8214	9189	9841	9990	10000	10000	1317.
2	802360.	0	0	2	8	65	394	842	2279	5243	8237	9196	9820	9988	10000	10000	1004.
3	965346.	0	0	1	3	64	366	796	2187	5146	8165	9177	9820	9988	10000	10000	1107.
4	549618.	0	0	0	4	56	368	806	2251	5098	8134	9138	9814	9989	10000	10000	1483.
5	457234.	0	0	0	5	47	343	781	2156	5098	8165	9106	9812	9989	9998	10000	894.
6	525692.	0	0	0	4	43	378	867	2286	5279	8215	9186	9840	9985	10000	10000	1105.
7	890908.	0	0	1	6	70	361	792	2177	5189	8196	9177	9839	9987	10000	10000	1067.
8	568763.	0	0	0	8	46	352	794	2165	5153	8232	9191	9819	9993	9999	10000	922.
9	931633.	0	0	1	6	55	391	848	2214	5128	8152	9130	9816	9990	10000	10000	1540.
10	908048.	0	0	1	7	58	380	824	2200	5176	8191	9124	9820	9994	10000	10000	1374.
11	796960.	0	0	3	7	59	419	843	2247	5164	8172	9184	9824	9994	10000	10000	1229.
12	976765.	0	0	2	5	51	339	763	2238	5193	8230	9198	9848	9985	10000	10000	1210.
13	430779.	0	0	0	2	46	363	825	2239	5183	8207	9169	9841	9996	10000	10000	1615.
14	497281.	0	0	0	5	57	376	796	2187	5146	8109	9118	9832	9994	10000	10000	1495.
15	1071934.	0	1	1	5	58	356	828	2226	5220	8266	9181	9832	9988	9999	10000	977.
16	912181.	0	0	1	3	42	370	831	2233	5271	8163	9169	9805	9987	10000	10000	1055.
17	622513.	0	0	0	3	51	348	795	2184	5217	8204	9120	9820	9995	10000	10000	1272.
18	640614.	0	0	0	4	56	368	829	2197	5208	8189	9152	9821	9980	9999	10000	934.
19	661549.	0	0	0	6	58	391	798	2191	5161	8184	9181	9867	9994	10000	10000	1588.
20	848435.	0	0	1	8	68	349	782	2256	5217	8223	9171	9845	9992	10000	10000	1511.
21	635767.	0	0	0	9	61	382	841	2267	5224	8222	9203	9827	9987	10000	10000	1083.
22	513746.	0	0	0	6	51	358	801	2208	5138	8173	9173	9836	9996	10000	10000	1637.
23	684107.	0	0	0	3	59	383	807	2236	5186	8175	9129	9840	9989	10000	10000	1533.
24	494215.	0	0	0	4	55	385	876	2292	5332	8192	9197	9843	9991	9999	10000	863.
25	511071.	0	0	0	5	61	379	836	2155	5205	8215	9169	9853	9992	10000	10000	1350.
26	663288.	0	0	0	6	62	360	807	2223	5261	8189	9199	9831	9990	10000	10000	1207.
27	672576.	0	0	0	8	58	354	761	2162	5270	8227	9158	9855	9989	9998	10000	853.
28	504933.	0	0	0	5	59	366	796	2206	5193	8226	9152	9829	9989	9999	10000	818.
29	753886.	0	0	1	6	63	362	789	2206	5278	8255	9189	9824	9991	10000	10000	1193.
30	590064.	0	0	0	9	60	378	840	2224	5241	8231	9179	9825	9991	10000	10000	1579.
31	544515.	0	0	0	3	76	341	804	2142	5110	8165	9141	9821	9993	10000	10000	1566.
32	789178.	0	0	2	5	63	371	818	2210	5228	8167	9196	9816	9986	10000	10000	1264.
33	601976.	0	0	0	3	52	364	768	2162	5079	8222	9194	9846	9995	9999	10000	822.
34	743934.	0	0	2	8	62	376	811	2195	5157	8042	9050	9804	9987	10000	10000	1239.
35	839522.	0	0	2	11	59	386	820	2234	5207	8240	9200	9853	9998	10000	10000	1569.
36	1009512.	0	1	1	5	63	351	769	2176	5165	8246	9175	9843	9993	10000	10000	1475.
37	773564.	0	0	2	9	54	391	878	2310	5194	8235	9139	9842	9992	10000	10000	1272.
38	522245.	0	0	0	5	59	379	835	2205	5154	8212	9132	9828	9996	10000	10000	1264.
39	511711.	0	0	0	4	57	355	807	2242	5214	8187	9157	9828	9991	10000	10000	1148.
40	1100150.	0	1	1	9	72	389	799	2243	5199	8148	9168	9826	9989	9999	10000	923.
41	593297.	0	0	0	2	59	367	810	2145	5143	8228	9191	9844	9991	10000	10000	1209.
42	522914.	0	0	0	12	76	367	790	2229	5211	8178	9207	9836	9990	10000	10000	1124.
43	690056.	0	0	0	1	58	414	852	2265	5181	8197	9168	9821	9991	10000	10000	1279.
44	754962.	0	0	1	3	35	352	760	2157	5186	8176	9160	9821	9988	10000	10000	1288.
45	836027.	0	0	1	3	64	416	858	2241	5297	8233	9186	9833	9994	10000	10000	1457.
46	886899.	0	0	1	8	60	379	801	2172	5232	8154	9160	9845	9990	9999	10000	842.
47	755452.	0	0	1	4	45	328	795	2150	5135	8134	9108	9841	9994	10000	10000	1252.
48	883231.	0	0	1	5	63	392	869	2225	5200	8165	9149	9821	9993	10000	10000	1374.
49	927178.	0	0	1	6	62	379	824	2179	5254	8151	9126	9834	9986	10000	10000	1154.
50	928938.	0	0	1	4	50	382	842	2263	5216	8216	9153	9850	9991	10000	10000	1521.
51	661064.	0	0	0	10	61	362	819	2172	5143	8213	9162	9825	9994	10000	10000	1547.
52	687047.	0	0	0	3	57	355	795	2166	5046	8126	9115	9843	9987	10000	10000	1293.
53	866891.	0	0	1	6	64	360	829	2282	5164	8171	9158	9830	9996	10000	10000	1243.
54	611893.	0	0	0	5	54	339	795	2187	5118	8131	9116	9832	9992	10000	10000	1514.
55	656425.	0	0	0	4	50	378	845	2273	5233	8169	9158	9846	9991	10000	10000	1014.
56	980657.	0	0	1	5	58	353	784	2165	5214	8155	9179	9846	9993	10000	10000	1034.
57	501692.	0	0	0	7	43	337	791	2142	5141	8174	9152	9847	9991	10000	10000	1279.
58	1175122.	0	1	2	6	59	359	821	2196	5178	8215	9120	9852	9986	9999	9999	694.
59	1274098.	0	2	2	7	50	356	803	2177	5153	8213	9191	9854	9993	10000	10000	1430.
60	867860.	0	0	1	5	52	370	850	2275	5279	8195	9171	9848	9992	10000	10000	1195.
61	551536.	0	0	0	7	48	361	784	2191	5185	8187	9128	9813	9983	10000	10000	1356.
62	529726	0	0	0	4	55	371	785	2146	5170	8175	9154	9834	9992	10000	10000	1376.
63	571136.	0	0	0	3	50	356	776	2145	5136	8165	9157	9845	9992	10000	10000	1509.
64	474395.	0	0	0	4	47	347	807	2229	5144	8126	9109	9831	9986	10000	10000	1401.
65	675452.	0	0	0	5	53	366	824	2163	5246	8208	9170	9843	9988	10000	10000	1215.
66	424947.	0	0	0	2	49	364	839	2199	5198	8174	9134	9842	9992	10000	10000	1021.
67	660977.	0	0	0	5	55	386	825	2246	5286	8233	9152	9832	9989	10000	10000	1473.
68	690711.	0	0	0	8	65	381	865	2217	5229	8217	9181	9821	9993	10000	10000	1218.
69	411254.	0	0	0	1	46	369	828	2170	5151	8155	9132	9819	9990	10000	10000	1232.
70	655072.	0	0	0	10	62	354	797	2218	5193	8179	9164	9844	9994	9999	10000	942.
71	663865.	0	0	0	5	49	354	786	2206	5161	8129	9146	9851	9989	10000	10000	1188.
72	591622.	0	0	0	7	69	382	847	2242	5206	8178	9123	9852	9992	10000	10000	1465.
73	933359.	0	0	3	7	56	368	843	2199	5190	8215	9191	9841	9995	10000	10000	1452.
74	678074.	0	0	0	4	48	376	809	2177	5093	8125	9122	9849	9990	10000	10000	1489.
75	983240.	0	0	1	7	66	382	805	2205	5179	8252	9205	9846	9988	10000	10000	1224.
76	670553.	0	0	0	4	50	378	777	2210	5202	8163	9185	9835	9988	10000	10000	1089.
77	671617.	0	0	0	11	57	369	801	2230	5175	8199	9147	9831	9991	9999	10000	823.
78	597403.	0	0	0	4	53	359	775	2163	5142	8167	9148	9844	9993	10000	10000	1031.
79	468716.	0	0	0	1	42	335	802	2211	5225	8165	9156	9837	9986	9999	10000	943.
80	1441886.	0	1	2	6	47	384	789	2148	5120	8185	9162	9845	9992	10000	10000	1478.
81	793944.	0	0	2	5	40	342	770	2153	5130	8149	9157	9846	9991	10000	10000	1506.
82	633948.	0	0	0	5	43	329	759	2146	5163	8207	9151	9824	9988	10000	10000	1524.
83	646857.	0	0	0	6	50	366	795	2242	5219	8192	9157	9827	9989	10000	10000	1033.
84	565915.	0	0	0	7	44	371	810	2177	5160	8181	9149	9825	9987	10000	10000	1555.
85	572323.	0	0	0	5	51	352	828	2209	5154	8149	9151	9827	9991	10000	10000	1440.
86	633641.	0	0	0	10	66	362	805	2186	5201	8194	9138	9842	9989	10000	10000	1095.
87	1143601.	0	1	3	8	63	384	831	2233	5238	8254	9143	9825	9991	10000	10000	1030.
88	654237.	0	0	0	4	59	374	808	2205	5229	8163	9115	9840	9988	10000	10000	1262.
89	538747.	0	0	0	2	43	339	766	2200	5143	8176	9160	9844	9990	10000	10000	1234.
90	609050.	0	0	0	7	58	376	817	2233	5304	8206	9161	9843	9995	10000	10000	1081.
91	513344.	0	0	0	5	59	356	817	2248	5230	8212	9142	9818	9979	9998	10000	916.
92	655771.	0	0	0	6	67	359	822	2181	5086	8162	9147	9823	9980	10000	10000	1095.
93	499810.	0	0	0	3	57	355	801	2216	5230	8237	9227	9874	9994	10000	10000	1303.
94	565316.	0	0	0	3	60	376	806	2234	5226	8159	9151	9820	9994	10000	10000	1465.
95	858480.	0	0	1	7	63	360	785	2140	5148	8211	9146	9840	9993	10000	10000	1241.
96	551618.	0	0	0	8	46	343	755	2147	5194	8183	9157	9823	9989	10000	10000	1344.
97	673821.	0	0	0	3	37	353	792	2221	5223	8183	9164	9822	9991	9999	10000	991.
98	852736.	0	0	1	6	56	349	825	2199	5265	8190	9123	9834	9989	10000	10000	1210.
99	656856.	0	0	0	2	54	348	761	2211	5194	8187	9148	9820	9989	10000	10000	1303.
100	889213.	0	0	3	9	52	382	836	2242	5204	8219	9175	9834	9994	10000	10000	1602.

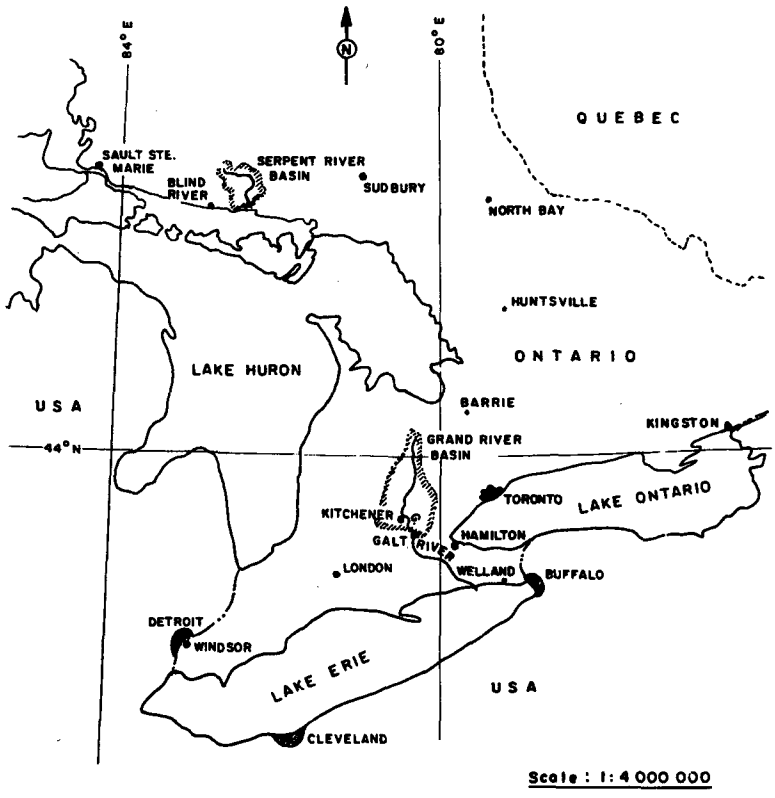


Fig. 1. Location Map.

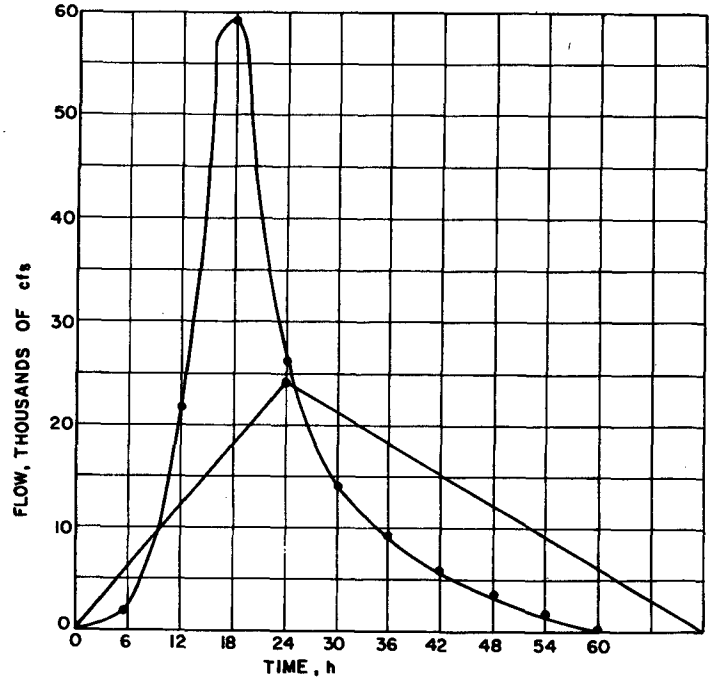


Fig. 2. "Official" and Up-dated Unit Hydrograph (Produced by 1 inch in 6 hours) of Grand River at Galt.

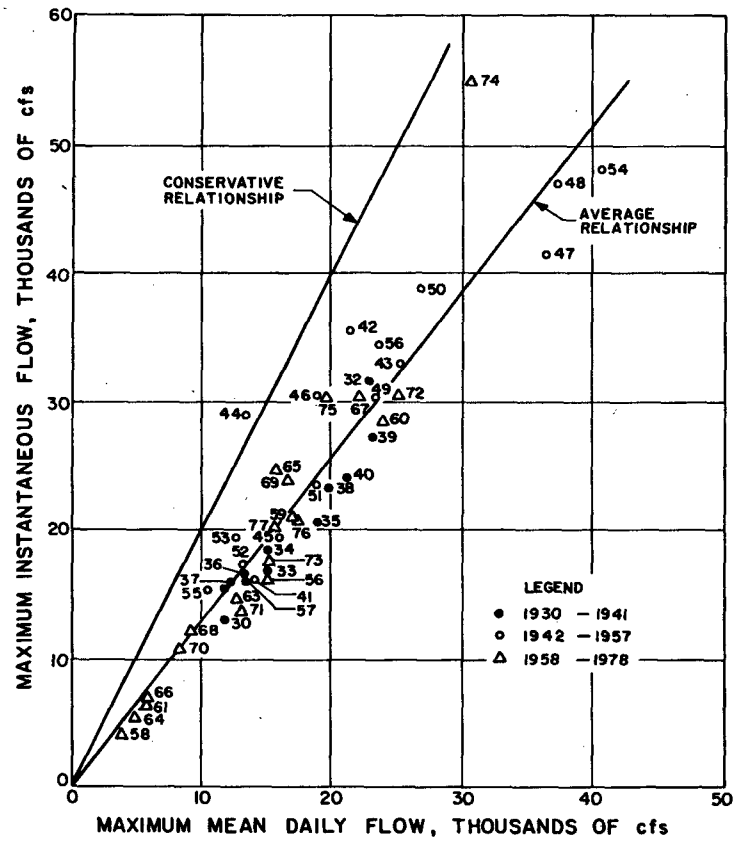


Fig. 3. Relationship between Maximum Mean Daily and Maximum Instantaneous Flow of Grand River at Galt.

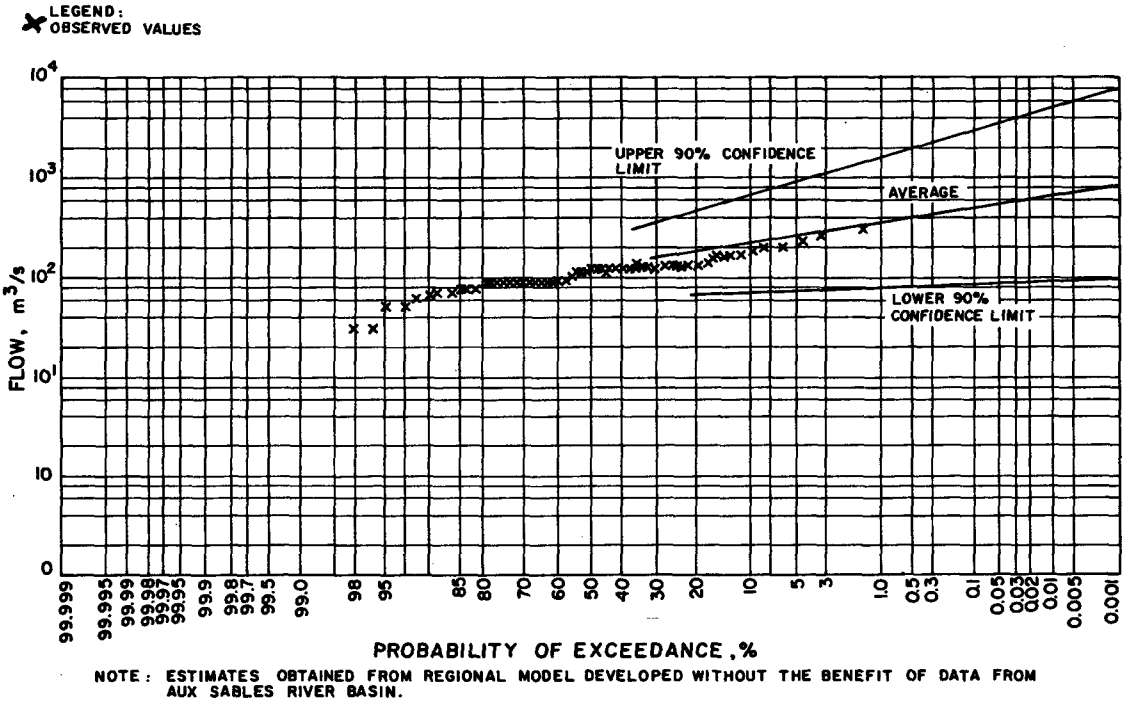


Fig. 4. Frequency Curve of Maximum Daily Flows of Aux Sables River at Massey.

ANALYTIC METHODS FOR UNCERTAINTY ANALYSIS IN PROBABILISTIC RISK ASSESSMENT

David C. Cox and Paul Baybutt

Risk Assessment Group
Battelle Columbus Laboratories
505 King Ave., Columbus, Ohio 43201, U.S.A.

ABSTRACT

This paper describes a new method for uncertainty analysis of the output of a model with uncertain inputs. The method uses variance as a measure of uncertainty and permits the calculation of output variance and its partitioning among effects due to the various input variables and their interactions. The partitioning allows one to evaluate an importance measure for each contributor to output uncertainty and, hence, to find cost-effective ways to reduce that uncertainty. The paper gives a brief description of the underlying theory and then develops the detailed formulas needed for its application to fault trees. A simple tree is used to illustrate the concepts and to compare our importance measure to an alternative based on partial derivatives. Finally, the implementation of the method in computer code CUTSE is described and results for a fault tree of moderate size presented. It is shown that the new method represents a significant increase in efficiency over existing techniques for evaluating the variance of the top event of a fault tree.

1. INTRODUCTION

This paper describes a new method for uncertainty analysis of the output of a model with uncertain inputs. The method uses variance as a measure of uncertainty and permits the calculation of output variance and its partitioning among effects due to the various input variables and their interactions. The partitioning allows one to determine the most important contributors to output uncertainty and, hence, to devise cost-effective ways to reduce that uncertainty.

Section 2 presents a brief description of the theory underlying the method, illustrating the concepts by means of a simple response-surface problem. In Section 3, the detailed formulas needed to apply the method to the uncertainty analysis of fault trees are developed. For a fault tree, the method calculates the variance of the top event and partitions that variance among the basic events and their interactions. The partition of variance is used to determine an uncertainty-importance-measure for each basic event and for interactions between basic events. We compare our importance measure to an alternative, based on partial derivatives, which has been developed by Bier [1]. We also show that, in evaluating top-event variance for large trees, our method can be expected to be significantly faster than conventional techniques. Section 4 contains numerical examples, together with a brief discussion of computer code CUTSE [2], which is under development at Battelle's Columbus Laboratories. CUTSE is a cut-set evaluation code which employs the method of this paper in carrying out uncertainty analysis of fault trees. Finally, Section 5 contains our conclusions.

2. THE METHOD

Let Y denote an output which is a function of input variables $X_1,\ldots X_m$. Write $Y = f(X_1,\ldots X_m)$. We employ variance as a measure of uncertainty, and assume throughout that $X_1,\ldots X_m$ are independent random variables. As shown in [3], we may write

$$\mathrm{Var}(Y) = \sum_{i=1}^{m} V_i + \sum_{i<j} V_{ij} + \sum_{i<j<k} V_{ijk} + \ldots + V_{12\ldots m} \quad . \tag{1}$$

The terms in (1) are defined as follows. First, $V_i = \mathrm{Var}\,[E(Y|X_i)]$, $i = 1,..m$. Since $E(Y|X_i)$, the conditional expectation of Y given X_i, is the unique function of X_i closest to Y in a mean-square sense [4], it is reasonable to call V_i the contribution of X_i to Var (Y). Next,

$$V_{ij} = \mathrm{Var}(E(Y - \sum_{k=1}^{m} E(Y|X_k)|X_i, X_j))$$

This may be regarded as the contribution to Var (Y) due to interaction between X_i and X_j. Higher-order terms in (1) are interpreted analogously. For more details on the basic decomposition formula (1), see [3].

As an illustration, consider the simple output function

$$Y = A_0 + \sum_{i=1}^{m} A_i X_i + \sum_{i<j} A_{ij} X_i X_j \quad . \tag{2}$$

Response surfaces of this type have been employed [5] in uncertainty analyses of large computer codes used in nuclear reactor safety analyses. In (2) assume that each X_i has expected value zero; this can always be achieved by a suitable translation. Then, $E(Y|X_i) = A_0 + A_i X_i$, so that $V_i = A_i^2\,\mathrm{Var}(X_i)$, $i = 1, \ldots m$. Next,

$$E(Y - \sum_{k=1}^{m} E(Y|X_k)|X_i, X_j) = A_{ij} X_i X_j - (m-1)A_0 \quad ,$$

so that $V_{ij} = A_{ij}^2\,\mathrm{Var}(X_i)\,\mathrm{Var}(X_i)$, for $i < j$. Higher-order terms are zero in this example. Thus, the decomposition (1) is

$$\mathrm{Var}(Y) = \sum_{i=1}^{m} A_i^2\,\mathrm{Var}(X_i) + \sum_{i<j} A_{ij}^2\,\mathrm{Var}(X_i)\,\mathrm{Var}(X_j)$$

An uncertainty-importance-measure for each variable X_i can be written down as $100A_i^2\,\mathrm{Var}(X_i)/\mathrm{Var}(Y)$. The uncertainty importance of interaction between X_i and X_j is, analogously, $100A_{ij}^2\,\mathrm{Var}(X_i)\mathrm{Var}(X_j)/\mathrm{Var}(Y)$.

3. UNCERTAINTY ANALYSIS OF FAULT TREES

Consider a fault tree with basic events $A_1,\ldots A_m$, and minimal cut-sets

$$C_i = \prod_{j=1}^{k_i} A_{i_j}, \quad i = 1, \ldots n \tag{3}$$

By definition, each A_i is a zero-one variable. Thus, $A_i = 1$ if the i^{th} basic event occurs, while $A_i = 0$ otherwise. Let $P_i = Pr\ (A_i = 1) = E(A_i)$. The randomness of occurence of the basic events is reflected in the random nature of the variables A_i. However, we are also interested in uncertainty in the basic event probabilities, due to lack-of-knowledge on the part of the fault-tree analyst. This uncertainty is modeled here by treating the P_i also as independent random variables, with means μ_i and variances σ_i^2. The probability polynomial corresponding to (3) is

$$\begin{aligned} P &= \sum_{i=1}^{n} Pr(C_i) - \sum_{i<j} Pr(C_iC_j) + \ldots + (-1)^{n-1} Pr(C_1 \ldots C_n) \\ &= \sum_{i=1}^{n} \prod_{j \epsilon S_i} P_j - \sum_{i<j} \prod_{\ell \epsilon S_i \cup S_j} P_\ell + \ldots + (-1)^{n-1} \prod_{j \epsilon S_1 \cup \ldots \cup S_n} P_j \ . \end{aligned} \tag{4}$$

Here P is the top-event probability, while S_i denotes the set of indices from $\{1, 2, \ldots m\}$ present in cut-set C_i. From (4) and the assumed independence of the P_i, the expected value E(P) of the top-event probability can be obtained by replacing each P_i by μ_i. We are interested in the variance of P. Let $P_j^* = P_j - \mu_j$, so that $E(P_j^*) = 0$. Now (4) can be rewritten

$$\begin{aligned} P = \sum_{i=1}^{n} \prod_{j \epsilon S_i} (P_j^* + \mu_j) - \sum_{i<j} \prod_{\ell \epsilon S_i \cup S_j} (P_\ell^* + \mu_\ell) + \ldots \\ + (-1)^{n-1} \prod_{j \epsilon S_1 \cup \ldots \cup S_n} (P_j^* + \mu_j) \ . \end{aligned} \tag{5}$$

On expanding the products in (5) one obtains a sum of signed products of P^*'s and μ's. Two such terms are uncorrelated unless they contain identical P^*'s. To evaluate Var(P), then, one only needs to collect all terms with identical P^*'s, and use the fact that the variance of a product of P^*'s is the product of the variances of the factors. This holds because the P^*'s are independent with mean zero. The calculations are facilitated by introducing a partial derivative operator as follows. Consider the probability polynomial (4) and let

$$I_j = \frac{\partial P}{\partial P_j} \Bigg|_{P_i = \mu_i,\ i=1,\ldots n}$$

Then, the sum of all terms in (5) containing only P_i^* is exactly $I_i P_i^*$. The corresponding term in Var (P) is $I_i^2 \sigma_i^2$. By arguing as in the response-surface example in Section 2, one can show that the quantity $I_i^2 \sigma_i^2$ is in fact the contribution V_i of P_i to Var(P), as defined in Section 2. Higher-order contributions to Var(P) can be evaluated similarly. For example, the contribution from interaction between P_i and P_j is $I_{ij}^2 \sigma_i^2 \sigma_j^2$, where $I_{ij} = \partial P / \partial (P_i P_j)$. Here, the product $P_i P_j$ is treated as a single variable for purposes of differentiation. In practice the main-effect terms $I_i^2\ \sigma_i^2$ usually dominate. By starting with these and including only the significant terms, Var(P) can be evaluated to any desired accuracy. As in the response-surface example

in Section 2, the uncertainty-importance-measures are evaluated as percentages of Var (P). Thus, the importance of P_i is $100I_i^2\sigma_i^2/\mathrm{Var}(P)$, that of P_iP_j is $100I_{ij}^2\sigma_i^2\sigma_j^2/\mathrm{Var}(P)$, etc. An example of the method is presented in Section 4.

It is interesting to compare the importance measure suggested here to one developed by Bier [1]. Bier's measure of the uncertainty importance of P_i is $100[\partial \mathrm{Var}(P)/\partial\sigma_i^2][\sigma_i^2/\mathrm{Var}(P)] = 100\partial[\ell n \mathrm{Var}(P)]/\partial \ell n\sigma_i^2$. In our notation, this quantity is the sum

$$(I_i^2\sigma_i^2 + \sum_{j\neq i} I_{ij}^2\sigma_i^2\sigma_i^2 + \ldots)/\mathrm{Var}(P)$$

Thus, Bier's measure of the uncertainty importance of P_i is the sum of our main-effect of P_i and all higher-order interaction effects which involve P_i. Our procedure, then involves a finer breakdown of the structure of the uncertainty contributions. As shown by example in Section 4, this can be used in assessing the effect on the top-event variance of changes in the basic event variances. In practical problems, however, the higher-order contributions are often negligible and the methods are more-or-less equivalent. This is also illustrated in Section 4.

Finally, we point out that the procedure described above provides a very efficient method for evaluating Var(P), the top-event variance, for large trees, as compared with more conventional approaches. To illustrate this, consider a typical term in the probability polynomial (4). Let $Y = \sum_{i=1}^{N}\prod_{j=1}^{M_i} P_{ij}$ with mean value $E(Y) = \sum_{i=1}^{N}\prod_{j=1}^{M_i}\mu_{ij}$. The method of evaluating Var(Y) described above involves writing $Y = \sum_{i=1}^{N}\prod_{j=1}^{M_i}(P^*_{ij}+\mu_{ij})$. This may be expanded into a sum of $\sum_{i=1}^{N} 2^{M_i}$ terms each consisting of a product of M_i factors. Terms containing the same P^*'s must be collected. It follows that the maximum number of multiplications required to evaluate Var(Y) is $\sum_{i=1}^{N}(M_i - 1)2^{M_i}$, given values of μ_i and σ_i^2. The conventional method of evaluating Var(Y) is as follows. Write $\mathrm{Var}(Y) = E(Y^2) - E(Y)^2$. Evaluation of E(Y) requires $\sum_{i=1}^{N}(M_i - 1)$ multiplications. Next, we have

$$Y^2 = \sum_{i=1}^{N}\prod_{j=1}^{M_i} P_{ij}^2 + 2\sum_{i<k}\prod_{j=1}^{M_i}\prod_{\ell=1}^{M_k} P_{ij}P_{k\ell} \quad ,$$

so that

$$E(Y^2) = \sum_{i=1}^{N}\prod_{j=1}^{M_i}(\sigma_{ij}^2 + \mu_{ij}^2) + 2\sum_{i<k}\prod_{j=1}^{M_i}\prod_{\ell=1}^{M_k}\mu_{ij}\mu_{k\ell}$$

The number of multiplications required to evaluate $E(Y^2)$ depends on the degree of repetition of individual elements among the terms. The first extreme occurs when there are no common elements between any pairs of terms. In that case, the number of multiplication is $\sum_{i=1}^{N}(M_i - 1) + \sum_{i<k}(M_i + M_k - 1) + 1 = N\sum_{i=1}^{N} M_i - N(N+1)/2 + 1$. The other extreme occurs when each pair of terms overlaps to the greatest extent possible i.e. terms of length M_i and M_j have $\min(M_i,M_j)$ elements in common. Then $\sum_{i=1}^{N}(M_i - 1) + \sum_{i<k}(\max(M_i,M_j) - 1) + 1$ multiplications are needed.

Consider a simple case where all $M_i = M$, say. Our method requires a maximum of $N(M-1)2^M$ multiplications. The conventional procedure requires between $MN^2 - (1.5M-2)N + 2$ and $(M-1)N^2 + (M-1)N + 2$ multiplications. Thus, we require $O(N)$, while the usual method requires $O(N^2)$, multiplications. The above calculations have not considered differences between the two algorithms which might also affect the computation times. However, the calculations do indicate that our procedure should be considerably faster, at least for sufficiently large trees. The larger the tree, the greater the difference in speed between the two methods since the running-time of our algorithm is roughly proportional to the number N of cut sets while the conven-

tional procedure has a running-time proportional to N^2. An actual numerical example is discussed in Section 4.

4. EXAMPLES

Our first example is a small tree, shown in Figure 1, which can be analyzed by hand and used to illustrate the technique described in Section 2.

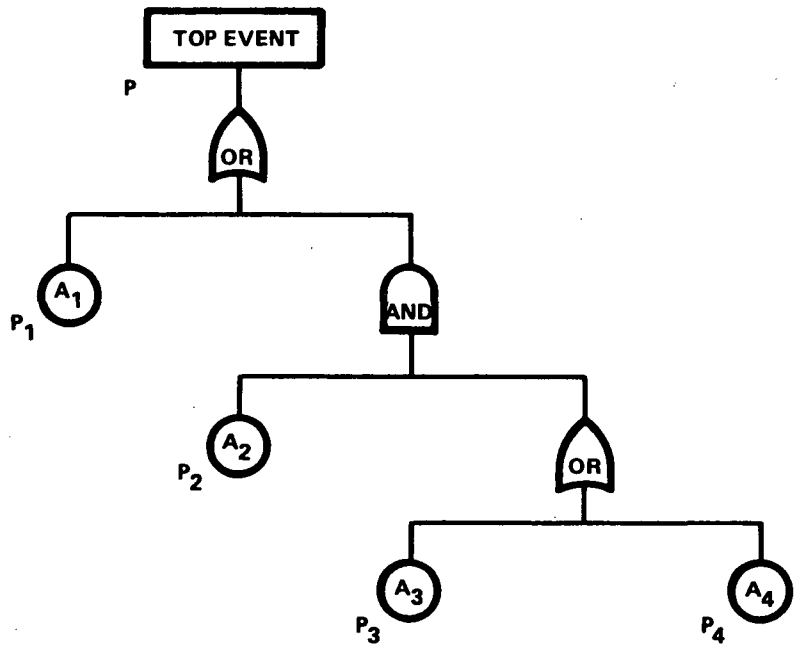


FIGURE 1. EXAMPLE FAULT TREE

Here, the minimal cut-sets are A_1, A_2A_3, and A_2A_4 so that the probability expression is

$$P = P_1 + P_2P_3 + P_2P_4 - P_1P_2P_3 - P_1P_2P_4 - P_2P_3P_4 + P_1P_2P_3P_4 \quad . \tag{6}$$

In the notation of Section 3, we have $I_1 = 1 - P_2P_3 - P_2P_4 - P_2P_3P_4$, where we have written p_i for $\mu_i = E(P_i)$. The contribution of A_1 to Var(P) is $I_1^2\sigma_1^2$. As a second example, $I_{23} = \partial P/\partial(P_2P_3) = 1 - P_1 - P_4 + P_1P_4$ so that the contribution of the A_2-A_3 interaction to Var(P) is $I_{23}^2\sigma_2^2\sigma_3^2 = (1 - p_1 - p_4 + p_1p_4)^2\sigma_2^2\sigma_3^2$. Similarly, the A_1-A_2-A_4 interaction contributes $(p_3 - 1)^2\sigma_1^2\sigma_2^2\sigma_4^2$. Adding all contributions gives Var(P). The main effect contributions are:

$$A_1: \quad (1 - p_2p_3 - p_2p_4 + p_2p_3p_4)^2\sigma_1^2$$

$$A_2: \quad (p_3 + p_4 - p_1p_3 - p_1p_4 - p_3p_4 + p_1p_3p_4)^2\sigma_2^2$$

$$A_3: \quad (p_2 - p_1p_2 - p_2p_4 + p_1p_2p_4)^2\sigma_3^2$$

$$A_4: \quad (p_2 + p_1p_2 - p_2p_3 + p_1p_2p_3)^2\sigma_4^2$$

As a numerical example, let $p_1 = \sigma_1 = 10^{-3}$; $p_2 = \sigma_2 = 10^{-2}$; $p_3 = p_4 = \sigma_3 = \sigma_4 = 10^{-1}$. Then Var(P) = 7.8×10^{-6} with the following major contributions, all others being neglible:

A_1	A_2	A_3	A_4	A_2-A_3	A_2-A_4
13%	46%	10%	10%	10%	10%

By comparison, Bier's method leads to the following important measures:

A_1	A_2	A_3	A_4
13	66	20	20

For each A_i, the Bier measure is obtained by summing all contributions involving A_i. Thus, because of overlap, the quantities above sum to more than 100, and are not to be interpreted as percentages of Var(P).

In this example, both importance measures indicate that A_2 is the dominant contributor to the uncertainty in the top-event probability. Note that $Pr(A_2)$ does not have the greatest inherent uncertainty; the uncertainty contribution of A_2 is enhanced by its level in the tree and by its interaction with A_3 and A_4. The Bier measure increases the importance of A_2, A_3, and A_4 as compared to our measure, because it includes all interactions in the main-effect of a variable. For this reason, the Bier measure is more accurate as a measure of the individual importance, but less accurate as a predictor of the effect on Var(P) of simultaneous changes in the σ_i. For instance, suppose, in the example, that each σ_i is reduced by 90% i.e., one order of magnitude. The Bier measure predicts a reduction in Var(P) of (13 + 66 + 20 + 20)90% = 107%, which is unrealistic. Our measure predicts a reduction of 13 + 46 + 10 + 10)90%+(10 + 10) x 99% = 91%, which is exact.

Our second example involves a tree of moderate size which arose in an actual study. The tree had 61 components with 65 minimal cut-sets (23 singles, 37 doubles, and 5 triples). The cut-set evaluation code CUTSE [2], which is under development at Battelle Columbus Laboratories, was used to evaluate top-event variance and uncertainty-importance-measures (for main-effects only) by our method. CUTSE represents an important advance over existing codes in that it considers the full probability polynomial (4) rather than just the "rare-event" approximation $P = \sum_{i=1}^{n} Pr(C_i)$. This is important in many practical problems where basic event probabilities are not very small. The complete expression (4) contains a prohibitively large number of terms whenever n is reasonably large. Most of the terms, however, are negligibly small in practice. Thus, CUTSE employs a user-specified cut-off to keep the number of terms retained in (4) within reasonable bounds. It should be emphasized that the code considers <u>all</u> terms and does not eliminate any arbitrarily. Thus, approximation errors are controlled. In performing the variance evaluation and importance-measure calculations by the "partial derivative" algorithm described in Section 3, CUTSE employs a second user-specified cut-off on the variance of the terms. This, again, reduces computation time while allowing any desired degree of accuracy to be attained. A further feature of CUTSE is its special treatment of cut-sets consisting of a single event. The singles are treated as a separate module in the calculation. Because the singles often contribute a large part of the variance, this reduces computation time and increases accuracy. CUTSE permits evaluation of both of the uncertainty-importance-measures we have discussed.

The ranking of the components by the two importance measures was, as expected, somewhat different. The major discrepancy was that the component ranked first by Bier's method ranked seventh by ours. This was because this component was present in many doubles in the tree. In general, the two methods led to similar groupings of components, with fine-tuning within groups produced by the Bier method. Our measure is considerably easier to calculate than Bier's and seems to give reasonable results. Its utility will be much increased when the capability of calculating interaction contributions is added to CUTSE.

To compare our method of top-event variance-evaluation to the conventional technique, we also calculated the top-event variance using the latter method. Running-time comparisons for the two are shown in Table I. We have used normalized costs as a measure of running time. Results for various cut-offs used in forming the probability polynomial are presented. The smaller the cut-off, the larger the effective

size of the problem. It is clear that the new method is considerably faster than the conventional one, with savings increasing steadily with the size of the problem. It appears likely that large fault trees cannot be handled by the conventional method. Whether our technique works in such cases requires further exploration.

TABLE I
Comparison Of Conventional And New Methods
For Evaluating Top-Event Variance

CUTOFF	CONVENTIONAL	NEW
10^{-3}	4.5	1.0
5×10^{-4}	7.9	1.0
10^{-4}	83.7	1.0
5×10^{-5}	----	1.5
10^{-5}	----	4.2

5. CONCLUSIONS

A new analytic method for uncertainty analysis of the output of a complex model whose inputs are uncertain has been described. Variance is used as a measure of uncertainty for both input and output variables. Assuming that the input uncertainties are statistically independent, the technique calculates output variance and, in addition, evaluates measures of the uncertainty importance of the input variables and their interactions. Uncertainty-importance-measures can be used to rank the inputs and their interactions in order of importance for output uncertainty and to devise efficient ways of reducing output uncertainty.

Although the technique we have developed is, in principle, applicable to any model where output is represented as an analytic function of input, its most important application to date has been to the uncertainty analysis of fault trees. Detailed formulas for this case have been developed and are being implemented in the computer code CUTSE [2], which is under development at Battelle's Columbus Laboratories. Preliminary calculations with the code indicate that the method of this paper is considerably more efficient than existing methods for calculating the variance of the top-event. This finding is reinforced by theoretical analyses based on calculations of the number of multiplications required in each method.

Two types of uncertainty-importance-measure capability are being included in the code, representing a further advance over existing fault-tree uncertainty-analysis codes. In many problems of practical interest, the two important measures are essentially equivalent. In general, however, one, due to Bier [1], provides a good measure of uncertainty-importance of the main-effects of the basic events, while the other, due to the authors, leads to efficient methods for calculating the change in top-event varience resulting from given changes in the basic-event variances.

ACKNOWLEDGMENTS

The support of Corporate Technical Development of Battelle Memorial Institute under Contract No. 587-K-7241 is gratefully acknowledged. Thanks to Fred Leverenz for providing the second example in Section 4 and for several stimulating discussions, and to Iverson Gary for making the CUTSE runs.

REFERENCES

1. V. BIER, "An Exploration and Extension of Analytic Methods for Propagation of Variances in Fault Trees", Thesis Proposal, MIT (1981).

2. F. L. LEVERENZ, "CUTSE: A Computer Code for Cut-Set Evaluation and Uncertainty Analysis of Fault Trees", under development at Battelle's Columbus Laboratories (1982).

3. D. C. COX, "An Analytic Method for Uncertainty Analysis of Nonlinear Output Functions, with Applications to Fault-Tree Analysis", submitted for publication (1982).

4. P. J. BICKEL and K. A. DOKSUM, "Mathematical Statistics: Basic Ideas and Selected Topics", Holden-Day, San Francisco (1977).

5. P. BAYBUTT, D. C. COX, and R. E. KURTH, "Method for Uncertainty Analysis of Large Computer Codes, with Application to Light-Water Reactor Meltdown Accident Consequence Evaluation", submitted for publication (1982).

A METHODOLOGY FOR ASSESSING UNCERTAINTIES IN THE PLANT-SPECIFIC FREQUENCIES FOR INITIATING EVENTS IN THE PRESENCE OF POPULATION VARIABILITY

I. A. Papazoglou

Department of Nuclear Energy
Brookhaven National Laboratory
Upton, New York 11973

ABSTRACT

This paper presents a derivation and some extensions of a technique for the assessment of the uncertainties in the frequency of accident initiators in nuclear power plants. The assessment is based on limited information coming from a number of plants belonging to a population that exhibits an inherent variability. The technique describes the use of Bayes theorem for updating, in the light of experiential data, the assessment of the uncertainties in both the generic (i.e., characterizing the whole population) and plant-specific frequencies of an accident initiator. The technique is demonstrated by assessing the uncertainties in the frequency of the loss of offsite power initiator for a population that exhibits inherent variability.

1. INTRODUCTION

The principles of the technique outlined in this paper were first introduced by Kaplan[1] and used in the Zion PRA[2]. The procedure for obtaining updated population and plant-specific distributions presented in this paper, is derived from a rigorous application of Bayes' theorem and the basic probability laws. Two new significant results are obtained. First, it is shown that the evidence from a specific plant must be excluded from the population evidence used in the plant-specific assessment of the same plant. Second, it is shown how the posterior distribution obtained by a first application of the technique, i.e., from a prior not based on any specific evidence, can be further updated in the light of additional experiential data. The results show that the proposed technique exhibits the "noninformative sampling stopping" property that characterize the "conventional" Bayesian approach[3]. To demonstrate the use of the methodology the uncertainties in the frequency of the loss of offsite power (LOOP) initiator were assessed for a generic plant (representing the whole population), as well as for two specific plants. All the necessary calculations have been computerized.

2. NOTATION AND ASSUMPTIONS

Let λ be the frequency (e.g., incidents/year) with which a particular accident initiator occurs. This initiator can occur in any one of a number of plants that are similar in behavior but not identical. Thus, there is no single value for the frequency λ that corresponds to all the plants in the population. Instead, the plant-to-plant variability is expressed by assuming that the frequency λ is a random

variable distributed according to a pdf $\phi(\lambda)$. Given perfect information, all that can be said about λ, as far as the population is concerned, is included in the pdf $\phi(\lambda)$, where $\phi(\lambda)d\lambda$ provides the percentage of the plants that are characterized by a frequency between λ and $\lambda+d\lambda$. For the purposes of this paper, $\phi(\lambda)$ has been assumed to be a lognormal pdf, i.e., of the form

$$\phi(\lambda) = \phi(\lambda|\mu,\sigma) = \frac{1}{\sqrt{2\pi}\,\sigma\lambda} \exp\left[\frac{-(\ell n\lambda-\mu)^2}{2\sigma^2}\right] \tag{1}$$

Given perfect information, the values of the parameters μ and σ would be exactly known. Due to limited information, however, the values of these parameters are not exactly known, and we quantify this uncertainty by assuming that they are random variables distributed according to a joint pdf $g(\mu,\sigma)$. Everything that is known about $\phi(\lambda)$ is incorporated in the pdf $g(\mu,\sigma)$ in such a way that $g(\mu,\sigma)d\mu d\sigma$ gives the probability that $\phi(\lambda)$ is the specific function $\phi(\lambda|\mu,\sigma)$. Since $g(\mu,\sigma)$ expresses our state of knowledge about the true value of $\phi(\lambda)$, the best pdf that characterizes the population is the expected value of $\phi(\lambda)$ over the measure $g(\mu,\sigma)$, i.e.,

$$\overline{\phi}(\lambda) = \iint \phi(\lambda|\mu,\sigma)g(\mu,\sigma)d\mu d\sigma \tag{2}$$

The second major assumption of the technique, is that the incidents occur randomly in time according to a Poisson random process. The intensity of the process (or frequency of the event), λ, has no unique value but exhibits the population variability discussed above and described by Eq. (1). Experiential data becomes available from various plants as incidents of loss of offsite power occur. The form of the data is: number of observed incidents (k) during a total period of operation (T). If there are N plants for which experiential data exists, the plant-specific evidence has the form

$$E_r = (k_r, T_r) \quad r = 1,2,\ldots,N \tag{3}$$

while the total evidence E from the population as a whole, is the union of the individual evidences

$$E = E_1 U E_2 U \ldots U E_N \tag{4}$$

3. POSTERIOR DISTRIBUTION FOR THE FREQUENCY OF AN ACCIDENT INITIATOR FOR THE PLANT POPULATION, GIVEN NO PRIOR EXPERIENTIAL EVIDENCE

The uncertainties about the exact value of the function $\phi(\lambda)$ that describes the plant-to-plant variability of the frequency λ are quantified by the measure $g(\mu,\sigma)$ that provides the probability that the parameters μ,σ (see Eq. 1) have the values μ and σ respectively. Given the evidence E (see Eqs. 3 and 4), the measure $g(\mu,\sigma)$ can be updated using Bayes' Theorem as follows:

$$g''(\mu,\sigma) = g(\mu,\sigma|E) = \frac{1}{C_1} L(E|\mu,\sigma)g'(\mu,\sigma) \tag{5}$$

where g″ is the posterior distribution of μ and σ given the evidence E, g' is the prior distribution, $L(E|\mu,\sigma)$ is the likelihood of obtaining the evidence E conditional to the fact that μ,σ have the values μ,σ and C_1 is a normalizing constant.

It can be shown [4] that

$$L(E|\mu,\sigma) = \left\{ \prod_{r=1}^{N} \int (\lambda^{k_r} e^{-\lambda T_r}) \phi(\lambda|\mu,\sigma) d\lambda \right\} \tag{6}$$

and that

$$C_1 = \iint L(E|\mu,\sigma) g'(\mu,\sigma) d\mu d\sigma \tag{7}$$

After calculating g" according to Eqs. (5-7), the posterior distribution for the frequency of the LOOP initiator that characterizes the total population is calculated by (see Eq. 2)

$$\overline{\phi}''(\lambda) = \iint \phi(\lambda|\mu,\sigma) g''(\mu,\sigma) d\mu d\sigma \tag{8}$$

It should be emphasized that Eqs. (5-7) are based on the assumption that g' does not depend in any way on experiential data coming from the N specific plants that provide evidence E (see Eqs. 3, 4).

4. PLANT-SPECIFIC POSTERIOR DISTRIBUTION FOR THE FREQUENCY OF AN ACCIDENT INITIATOR GIVEN NO PRIOR EXPERIENTIAL EVIDENCE

Before obtaining the evidence E, all we know about the frequency of LOOP for a specific plant m is contained in the measure g' and eventually in the unconditional distribution $\phi(\lambda)$ (see Eq. 2). The evidence E contains information that concerns both the behavior of the population as a whole and the specific plant in question (see Eq. 3). Careful application of Bayes' Theorem results in the following expression for the distribution of the plant-specific frequency

$$f''(\lambda_m) = f(\lambda_m|E) = \frac{1}{C_2} L(E,\lambda_m) \tag{9}$$

where $L(E,\lambda_m)$ is the likelihood that the evidence E will be obtained <u>and</u> that the frequency for the mth plant is λ_m, and given by (see [4])

$$L(E,\lambda_m) = (\lambda^{k_m} e^{-\lambda T_m}) \left\{ \prod_{\substack{r=1 \\ r\neq m}}^{N} \int (\lambda^{k_r} e^{-\lambda T_r}) \phi(\lambda|\mu,\sigma) d\lambda \right\} \phi(\lambda|\mu,\sigma) g' d\mu d\sigma \tag{10}$$

and C_2 is the normalizing constant equal to

$$C_2 = \int L(E,\lambda_m) d\lambda_m \tag{11}$$

It is noteworthy that if the evidence from the mth plant were not excluded from Eq. (10), then the double integral in the same equation provides the population posterior pdf (see Eqs. 5-8). If that were the case the procedure for obtaining the plant-specific posterior distribution would have been equivalent to an "one-stage conventional" Bayesian procedure, using as a prior the population posterior.

5. POSTERIOR DISTRIBUTION FOR THE FREQUENCY OF AN ACCIDENT INITIATOR FOR THE PLANT POPULATION GIVEN ADDITIONAL EXPERIENTIAL EVIDENCE

Let us assume that after applying the technique described in Section 3 and obtaining the posterior measure g", additional experiential data (E*) become available. In trying to incoporate this new evidence in the assessment of uncertainties one might be tempted to extrapolate from the customary practive in the conventional Bayesian analyses and apply again the procedure outlined in Seciton 3 using g" as a prior and evidence E*, to obtain a new posterior g'''. As it is shown elsewhere [4], this procedure leads into the wrong answer in the sense that g''' is not the same with the posterior g* that is obtained by updating the original prior (g') only once, using the original evidence E and the new evidence E* together. The derivation of the correct approach for incorporating the new evidence E* is briefly outlined here and in detail in Ref. [4].

The new evidence E* will contain in general, data obtained from plants that contributed into evidence E as well as "new" plants. The form of E* is

$$E^* = (k_r^*, T_r^*) \quad r = 1,2,\ldots,N,N+1,\ldots,N' \tag{12}$$

where the "old" plants have been indexed from 1 to N (as in Eq. 3) and the new plants from N+1 to N'.

Using Bayes' theorem we can write the conditional distribution of $g(\mu,\sigma\,|E,E^*)$ as follows:

$$g^* \equiv g(\mu,\sigma|E,E^*) = \frac{1}{C_3}\; L(E^*|E,\mu,\sigma)\; g(\mu,\sigma|E) \tag{13}$$

where $L(E^*|E,\mu,\sigma)$ is the likelihood of the new evidence E*, <u>given</u> the old evidence E and particular values of μ and σ, $g(\mu,\sigma|E)$ is the conditional measure g" given evidence E (see Eq. 5) and C_3 is a normalizing constant. It can be shown [4] that careful applicatin of Bayes' theorem leads to the following form for Eq. (13)

$$g^* = \frac{1}{C_4} \prod_{r=1}^{N'} L(E_r,E_r^*|\mu,\sigma)\, g'(\mu,\sigma) \tag{14}$$

where g' is the distribution of μ and σ <u>prior</u> to obtaining evidence E, C_4 is a normalizing constant, and $L(E_r,E_r^*|\mu,\sigma)$ is the joint likelihood of plant specific evidence E_r,E_r^* given μ,σ but unconditional on λ or

$$L(E_r,E_r^*|\mu,\sigma) = \int \left[\lambda^{k_r+k_r^*}\, e^{-\lambda(T_r+T_r^*)}\right] \phi(\lambda|\mu,\sigma)\,d\lambda, \qquad (k_r=T_r=0 \text{ if } r>N) \tag{15}$$

Operationally, Eq. (14) means that if additional evidence E* becomes available from "new" plants as well as from plants that have contributed in the original evidence E, then the distribution g" as obtained by Eq. (5) can not be used as the new prior but instead, the old evidence should be combined with the new and the procedure described in Section 3 should be repeated. The only time the posterior g" can be used as a new prior is if the additional evidence comes from plants that have not contributed to the assessment of g". This is of course rarely the case since as new plants are coming on line some of the old plants are still operating providing additional evidence.

It is also noteworthy, that as it follows from Eq. 15 the sufficient statistics for the evidences $E_r(r=1,2,...N,...,N')$ are the <u>total number</u> of failures $(k_r+k_r^*)$ and the <u>total time</u> $(T_r+T_r^*)$. Thus, the proposed technique exhibits the "noninformative sampling stopping" property. In other words, it leads to the same results whether the evidence is provided in one step (i.e., $k_r+k_r, T_r+T_r^*$) or in several steps [e.g., (k_r, T_r) and then (k_r^*, T_r^*)].

6. PLANT-SPECIFIC POSTERIOR DISTRIBUTION FOR THE FREQUENCY OF AN ACCIDENT INITIATOR GIVEN ADDITIONAL EXPERIENTIAL EVIDENCE

Let us assume that after obtaining evidence E and assessing the plant specific distribution of the frequency of an initiator as described in Section 4, additional evidence E* (see Eq. 12) becomes available. Here again care must be taken <u>not</u> to consider $f''(\lambda_m)$ given by Eq. (9) as prior and further update it using evidence E* in a conventional one-step Bayesian approach. The right procedure for incorporating the additional evidence E* into the plant-specific distribution is briefly outlined in the remaining of this section.

Using Bayes' theorem we can write the conditional distribution of the plant-specific frequency $f(\lambda_m|E,E^*)$ as follows

$$f(\lambda_m|E,E^*) = \frac{1}{C_5} L(E^*|E,\lambda_m)\, f(\lambda_m|E) \tag{16}$$

where $L(E^*|E,\lambda_m)$ is the likelihood of the new evidence E* <u>given</u> the old evidence E and that the frequency for the mth plant is λ_m, $f(\lambda_m|E)$ is the conditional distribution of λ_m <u>given</u> the evidence E (see Eq. 9), and C_5 a normalizing constant. It can be shown [4] that careful application of Bayes' theorem leads to the following form for Eq. 16.

$$f(\lambda_m|E,E^*) = \frac{1}{C_6}\left[\lambda^{k_m+k_m^*} e^{-\lambda(T_m+T_m^*)}\right] \prod_{\substack{r=1 \\ r\neq m}}^{N'} L(E_r,E_r^*|\mu,\sigma)\phi(\lambda|\mu,\sigma)g'\,d\mu d\sigma \tag{17}$$

where (k_m^*, T_m^*) is the new evidence from the specific plant m, $L(E_r$ is the joint likelihood of plant specific evidences (E_r,E_r^*) given μ,σ but unconditional on λ (see Eq. 15), $\phi(\lambda|\mu,\sigma)$ is the conditional distribution of λ (see Eq. 1), g' is the distribution of μ,σ <u>prior</u> to evidence E and E*, and C_6 a normalizing constant.

Operationally, Eq. 7 means that the distribution $f''(\lambda_m)$ obtained using evidence E can be used as a prior for further updating only if the new evidence E* originates from the specific plant m alone (see Eqs. 9 & 17). If the new evidence E* contains information from plants other than the mth, then, the procedure described in Section 4 must be repeated using the combined evidence (E,E*) and the prior measure g'.

7. THE FREQUENCY OF THE LOSS OF OFFSITE POWER ACCIDENT INITIATOR

As a demonstration of the methodology, the uncertainties about the frequency of the Loss of Offsite Power (LOOP) accident initiator have been assessed.

The variability of the frequency of the LOOP initiator within the site population has been quantified by assuming that the frequency of the initiator is a random variable distributed according to a lognormal pdf (see Eq. 1). To facilitate the numerical calculations, the random variables μ,σ were discretized. They have been assumed statistically independent, ranging over a "grid" of values. The unconditional distribution of the frequency λ as calculated from Eq. 2 has the characteristics given in Table II. This distribution characterizes the population variability prior to any experiential data.

The evidence used for this example is given in Table I and is based on the data presented by Scholl [5]. Using the prior distribution for μ,σ and the evidence in Table I, Eqs. 5-7 provide the posterior distribution g". The posterior distribution of the frequency λ for the population of plants, calculated according to Eq.(8), has the characteristics given in Table I. It is noteworthy that the evidence from the plants reduces the prior 90% interval of the frequency [0.001, 18], by two orders of magnitude to [0.025, 1.15] and the mean value from the prior value of 1.24 yr^{-1} to a posterior of 0.34 yr^{-1}. It is also noteworthy that the medians of the two distributions (prior and posterior) do not differ significantly.

If the prior measure g' and the evidence of Table I is specialized to plants #10 and #21, the plant-specific distributions have the characteristics given in Table II. Plant #10 has the "best" record and plant #21 has the "worst", thus the corresponding distributions "bracket" the distributions of the 21 plants of the sample.

For comparison purposes, the posterior distributions for plants #10 and #21 have been recalculated using only plant specific data and the unconditional population prior (see Table II) as prior. The results are displayed in Table III. It is noteworthy that the conventional Bayesian approach (i.e., neglecting the population variability) results in a posterior distribution for plant #21 (see Table III) that it is very similar to the one obtained taking the population variability into account (Table II). This is due to the fact that the evidence from plant #21 is very "strong" and thus the posterior is not affected by evidence from other plants. The opposite is the case, however, for plant #10. If the population variability is neglected and only the plant specific data are assumed relevent, the resulting posterior distribution (Table III) differs significantly from the one obtained if the plant-to-plant variability is taken into account (Table II).

Significally different results are obtained also for the population posterior. If for example, the plant-to-plant variability is neglected and all the evidence of Table I is assumed to come from exact replicas of the same plant (pooling of the data), the conventional Bayesian approach results in the posterior given in Table III. If on the other hand a plant-to-plant variability is assumed, then the posterior distribution is characterized by a much wider spread (Table II) although the median and mean values do not change significantly.

ACKNOWLEDGEMENT

The author wishes to thank Dr. A. Buslik for enlightning discussions at the first stages of the development of this technique. This work was performed under the auspices of the U. S. Nuclear Regulatory Commission.

REFERENCES

1. S. Kaplan, "On a two stage Bayesian Procedure for determining failure rates from the experiential data", PL6-0191, June 1981.

2. "Zion Probabilistic Safety Study", NRC Docket Nos. 50-295 and 50-304.

3. H. Raiffa and R. Schlaifer, "Applied Statistical Decision Theory", M.I.T. Press, Cambridge, Mass. (1961).

4. I. A. Papazoglou, et. al., "Assessment of the Uncertainties About the Plant-Specific Frequencies for Initiating Events In The Presence of Population Variability", BNL-NUREG-31794, Sept. 1982.

5. R. F. Scholl, Jr., "Loss of Offsite Power, Survey Status Report, Revision 3", Report of the Systematic Evaluation Program Branch, Division of Licensing, U. S. Nuclear Regulatory Commission.

TABLE I

Population Time and Event Data
Loss of Offsite Power

Plant No.	Number of Failures	Years in Operation
1.	1	15
2.	7	12
3.	4	12
4.	4	8
5.	3	11
6.	1	9
7.	4	9
8.	6	9
9.	1	8
10.	0	8
11.	1	6
12.	2	7
13.	1	7
14.	1	6
15.	0	6
16.	3	6
17.	0	5
18.	1	11
19.	1	5
20.	0	6
21.	7	8
22.	0	7
Totals	53	167

TABLE II

Unconditional Prior And Posterior Distribution Of The Population Frequency Of The LOOP Initiator (Yr^{-1})

	5% Percentile	Median	Mean	95% Percentile
1. Population Prior	1.00-03	1.46-01	1.24+00	1.79+01
2. Population Posterior	2.50-02	2.30-01	3.41-01	1.15+00
3. Plant #10	1.54-02	8.42-02	1.17-01	2.63-01
4. Plant #21	5.63-01	1.03+00	1.21+00	1.74+00

TABLE III

Results Of "Conventional" Bayesian Analysis

	5% Percentile	Median	Mean	95% Percentile
1. Population Prior	1.00-03	1.46-01	1.24+00	1.79+01
2. "Pooled data" Population Posterior	2.23-01	2.80-01	3.18-01	3.56-01
3. Plant #10	6.21-04	8.24-03	2.97-02	1.16-01
4. Plant #21	7.75-01	1.29+00	1.49+00	2.07+00

METHODOLOGY AND CODE FOR SPECIFYING PROBABILISTIC RISK COEFFICIENTS

D. E. Fields

Health and Safety Research Division
Oak Ridge National Laboratory
Oak Ridge, Tennessee 37830

ABSTRACT

Successful probabilistic risk assessment depends heavily on knowledge of the distribution of model parameters. We have developed the TERPED computer code as a versatile methodology for determining with what confidence a parameter set may be considered to have a normal or lognormal frequency distribution. Several measures of central tendency are computed. Other options include computation of the chi-square statistic, the Kolmogorov-Smirnov non-parametric statistic, and Pearson's correlation coefficient. Cumulative probability plots are produced either in high resolution (pen-and-ink or film) or in printer-plot form.

INTRODUCTION

Knowledge of the distribution of values characterizing an observable quantity is crucial for discussing and utilizing these values. Such knowledge is especially valuable in risk assessment analyses in which mathematical models are used to simulate system performance. One may arrive at widely varying estimates of risk, based upon differing choices of input parameters. If the statistical distributions of these parameters are well characterized, representative model input values may be intelligently chosen so as to yield more representative model predictions.

Accurate specification of the distribution of model input parameters is perhaps even more important if Monte Carlo techniques are to be applied. Furthermore, predictions of Monte Carlo models may often be examined and compared by characterizing their statistical distribution.

The importance of knowing the statistical distribution of model parameters and a desire for a convenient methodology for its generation have been expressed by several investigators [1,2,3]. The SAS [4] methodology, for example, is useful but not sufficiently versatile, as will be discussed below.

We have developed and implemented an interactive computer code, TERPED [5], to aid in analyzing a set of data and determining whether these data may be considered to be samples from either a normal or lognormal population. The code user assumes a normal or lognormal distribution, and the code linearizes the scales and plots the data in cumulative probability distribution format. Data linearization is by a spline

fit [6] of computed probability of occurrence values to a set of tabulated values representing the number of standard deviations away from the median value (50% cumulative probability value). Plots are generated consistent with the initial normal or lognormal assumption. The user may assess the validity of his assumption before plotting by specifying that a chi-square goodness of fit test [7] or a Kolmogorov-Smirnov (KS) one sample test analysis [8] be performed. The degree of linearity of the cumulative probability plot is quantized as Pearson's correlation between points corresponding to input data and equivalent values of the results of a least-squares fit to the data. In either case (normal or lognormal) the assumed distribution is tested versus a normal distribution with the same mean and standard deviation as the input data set.

Data input may be by named data file or via the user's terminal keyboard. The code is written in FORTRAN and runs on a Digital Equipment Corporation PDP-10 computer; typical central-processor-unit execution time is about 0.32 seconds, exclusive of plotting time. The code size is about 1500 card images.

STATISTICAL TESTS PERFORMED BY TERPED

TERPED assists the program user in deciding whether a given set of data may be considered to be samples from a normal or a lognormal distribution. The user may request several types of numerical or graphic output.

The frequency distribution of normally distributed parameters is the familiar "bell-shaped" curve. For a set of normal measured variables $x_{i;\ i=1,m}$ the mean value, $\underline{x}$, is computed by

$$\underline{x} = m^{-1} \sum_{i=1}^{m} x_i \quad , \tag{1}$$

and the variance about the mean, S^2, by

$$S^2 = (m - 1)^{-1} \sum_{i=1}^{m} (\underline{x} - x_i)^2 \tag{2}$$

If the data are lognormally distributed, the frequency distribution of logarithms of the data lie along a bell-shaped area, and there are several relevant statistical parameters (shown in Table 1). These include the mean of the logs $\hat{u}$, the most probable value x_p, the median value x_m, the arithmetic mean value $\bar{x}$, the 99th quantile value x_{99}, and the log variance $\hat{\sigma}^2$.

The calculated "expectation" value <x> of an observable quantity is $\underline{x}$ or x_p if the distribution is normal or lognormal, respectively. The value <x> would not be expected to be either $\underline{x}$ or x_p if the distribution is otherwise.

Table 1. Some useful statistical parameters for lognormally distributed data [10]

$$\hat{\mu} = m^{-1} \sum_{i=1}^{m} \ln x_i$$

$$\hat{\sigma}^2 = (m - 1)^{-1} \sum_{i=1}^{m} (\ln x_i - \hat{\mu})^2$$

$$x_p = \exp (\hat{\mu} - \hat{\sigma}^2)$$

$$x_m = \exp (\hat{\mu})$$

$$\bar{x} = \exp (\hat{\mu} + \hat{\sigma}^2/2)$$

$$x_{99} = \exp (\hat{\mu} + 2.326\hat{\sigma})$$

For a set of m values ordered by increasing magnitude with index i, the cumulative probability may be computed [9] by the following equation:

$$p_i = (i - 0.375)/(m + 0.25) \ . \qquad (3)$$

The TERPED user may choose to invoke a number of numerical algorithms to test his hypothesis of the distribution of his data. The user assumes either a normal or lognormal distribution, and the code first calculates cumulative probability values using Eq. (3). The user's data are then transformed into a linear function of cumulative probability assuming the hypothesized normal or lognormal distribution. Data linearization is by a spline fit [6] of computed probability of occurrence values to a set of tabulated inverse error functions values representing the number of standard deviations away from the mean value (50% cumulative probability value). If the user's assumption is a normal distribution, $\underline{x}$ and S^2 are computed and output, whereas if the choice is a lognormal distribution, the calculated values of $\hat{\mu}$, $\hat{\sigma}^2$, x_p, x_m, $\bar{x}$, and x_{99} are printed. The user may assess the validity of his assumption before generating a plot data set by specifying that a chi-square goodness of fit test [7] or a Kolmogorov-Smirnov (KS) one sample test analysis [8, 11] be performed. The degree of linearity of the cumulative probability plot is quantized as Pearson's correlation [12] between points corresponding to input data and equivalent values of the results of a

least-squares fit to the data. In either case (normal or lognormal), the assumed distribution (given or log-transformed) is tested versus a normal distribution with the same mean ($\underline{x}$ or $\hat{\mu}$) and standard deviation (S^2 or $\hat{\sigma}^2$) as the input data set.

The agreement between the data and the least-squares fit is quantified by calculating Pearson's correlation coefficient. If $x_{i,i=1,m}$ are data ordinates with mean $\bar{x}$, and $y_{i,i=1,m}$ least-squares fit ordinates with mean $\bar{y}$ at the abscissa of point i, then the correlation coefficient is defined by [12]

$$r = \frac{\sum_{i=1}^{m} (\bar{x} - x_i)(\bar{y} - y_i)}{\left[\sum_{i-1}^{m} (\bar{x} - x_1)^2 \sum_{i=1}^{m} (\bar{y} - y_1)^2\right]^{1/2}} \qquad (4)$$

Values of r^2 will range from 0 for a very poor fit to 1.0 for a perfect correlation.

The goodness of fit between data and the assumed distribution may be calculated using a chi-square test. Performance of this test by TERPED is a user option. The normalized data are represented as lying in n cells, where n may be chosen by the user to be equal to or less than the number of data points. The "observed" value for each cell is either the data value x_i, or $\ln x_i$. We count s_i, the number of data points lying in each of the n cells distributed either normally or lognormally, and compare this to t_i, the expected number for a distribution having the same mean and variance. The comparison is made by calculating the observed chi-square statistic, defined as,

$$\chi^2 = \sum_{i=1}^{n} (s_i - t_i)^2/t_i \ , \qquad (5)$$

which is based on (n-3) degrees of freedom, and from which is computed the "significance level" for rejecting the "null hypothesis" that the two sets of numbers have the same distribution. The greater the likelihood that the data are distributed as assumed, the greater the significance level calculated numerically in TERPED using an IMSL [13] alogrithm. The significance level can be considered to be the probability of calculating, based on random fluctuations alone, a greater value of χ^2 than the one calculated here. Frequently, the 0.05 level of significance is used to make a decision about the assumed distribution. If the significance level is greater than 0.05, the user can reasonably conclude that in using a χ^2 test he cannot show his data to be different from a normal or lognormal distribution with the same mean and variance as his data.

A second TERPED user option is choice of the KS one-sample test [11]. The KS test considers the hypothesis of equality between the actual distribution of data and the assumed normal or lognormal distribution. The KS test is based on the maximum difference between corresponding terms of the value ranked sets x_i and y_i. We define $D = \max_{i=1,m} |x_i - y_i|$. This value is compared to an expected statistic valid for

that number of points, and a "confidence level" is determined. The KS confidence level is the probability of Z being exceeded if the hypothesis of equality of the two distributions is true and if the alternative is "two sided," i.e., if a given measurement has equal chance of lying above or below the expected value.

In summary, TERPED computes several measures of central tendency, the chi-square probability, the correlation coefficient, and the KS statistic.

TERPED GRAPHICS OPTIONS

Several TERPED options relate to the generation of plots of user-supplied data versus cumulative probability. The cumulative probability axis is scaled so the data will lie along a straight line if the data are distributed as hypothesized. A least-squares fit of the linearized values is plotted on the same graph to permit visual evaluation of the distribution hypothesis.

Plots may be of either a printer-plot form or high-resolution form. The user makes his selection based on program generated prompts. If his choice is for a high-resolution plot, plot information is routed to a disk file, which is called a compressed plot data set. This compressed plot data set may be viewed on a graphics terminal using PDP-10 system utility programs, or it may be routed to a remote Calcomp pen-and-ink plotter to obtain a high resolution paper copy. A third option consists of routing the data set to a film plotter to obtain a 35-mm film plot suitable for use as a projection slide.

SUMMARY

The TERPED code is a versatile methodology for determining with what confidence a parameter set may be considered to have a normal or lognormal frequency distribution. TERPED should prove beneficial even to the users having access to SAS. TERPED produces high quality graphics, whereas SAS generates only printer plots. TERPED is portable, fast, interactive, requires significantly less computer memory for execution, and is designed for a file-oriented timesharing computer environment.

ACKNOWLEDGEMENTS

Research sponsored by the Office of Reactor Research and Technology, U. S. Department of Energy, under contract W-7405-eng-26 with the Union Carbide Corporation.

REFERENCES

1. Shaeffer, D. L., A Model Evaluation Methodology Applicable to Environmental Assessment Models, Oak Ridge National Laboratory Report ORNL-5507 (1979).

2. Hoffman, F. O. and C. F. Baes III, editors, A Statistical Analysis of Selected Parameters for Predicting Food Chain Transport and Internal Dose of Radionuclides. U. S. Nuclear Regulatory Commission Report NUREG/CR-1004 (1979).

3. Schwartz, G., Chairman of workshop on "General Aspects of Accuracy in Dose Calculations," in Proceedings of a Workshop on Accuracy in Dose Calculations for Radionuclides Released to the Environment, held in Aachen, Federal Republic of Germany, September 1979. Report ISBN-3-88668-000-2 (1980).

4. Proprietary software distributed by SAS Institute, Inc., Raleigh, N. C.

5. Fields, D. E., TERPED: A Versitile Code for Examining the Distribution of Experimental Data, Oak Ridge National Laboratory Report ORNL-5689 (1981).

6. Ahlberg, J., Nelson, E., and Walsh, J., The Theory of Splines and Their Applications, Academic Press, New York (1967).

7. Kendal, M. G., and Stuart, A., The Advanced Theory of Statistics, Vol. 2, Hafner Publishing Co., New York (1961).

8. Bradley, J. V., Distribution-Free Statistical Tests, Prentice-Hall, Inc., New Jersey (1968), pp. 367-69.

9. Gosslee, D. G., Statistics Department, Mathematics Division, Oak Ridge National Laboratory, Personal Communication, June 12, 1972.

10. Aitchison, J., and Brown, J., The Lognormal Distribution, Cambridge Press, New York (1969).

11. Siegel, S., Nonparametric Statistics for the Behavioral Sciences, McGraw-Hill Publishing Company, New York (1956).

12. Snedecor, G. W., and Cochran, W. G., Statistical Methods (Sixth Edition), Iowa State University Press, Ames, Iowa (1972).

13. Software distributed by International Mathematical and Statistical Libraries, Inc., Houston, Texas.

A FAST ANALYTICAL METHOD FOR THE ADDITION OF RANDOM VARIABLES

V. Senna and R. L. Milidiú
Instituto de Matemática - UFRJ
Rio de Janeiro, RJ, Brasil

P.V. Fleming, M.R. Salles and L.F.S. Oliveira
Programa de Engenharia Nuclear, COPPE/UFRJ
Rio de Janeiro, RJ, Brasil

ABSTRACT

Using the minimal cut sets representation of a fault tree, a new approach to the method of moments is proposed in order to estimate confidence bounds to the top event probability. The method utilizes two or three moments either to fit a distribution (the normal and lognormal families) or to evaluate bounds from standard inequalities (e.g. Markov, Tchebycheff, etc.) Examples indicate that the results obtained by the lognormal family are in good agreement with those obtained by Monte Carlo simulation.

INTRODUCTION

The propagation of uncertainties in the evaluation of fault trees has been recognized |1| as a very important aspect of any significant risk assessment. It requires that the inherent uncertainties associated with basic events be combined, so as to give the top event probability (system failure) as a function, $Q_T = f(X_1, X_2, \ldots, X_n)$, of the basic events probabilities $X_1, X_2, \ldots, X_n$. Until now, three different methods have been applied for uncertainty propagation namely, Monte Carlo, discrete probability distribution (DPD) and the method of moments.

The Monte Carlo method |2| obtains the shape of the top event distribution from the basic events distributions through a simulation procedure.

For the DPD method |3-4| each basic event distribution is approximated by a discrete distribution, presented as a histogram. The top event distribution is then obtained by a combination of these histograms using the Q_T function.

The usual approach to the method of moments consists of expanding the function $f(X_1, X_2, \ldots, X_n)$ around the mean values of its arguments by a multivariate Taylor series |5-6|. Recently, suggestions |7| have been made both to improve the accuracy of the results and to reduce the computational effort required. Nevertheless, this approach is still limited in the number of moments it can handle within reasonable processing time.

A NEW IMPLEMENTATION OF THE METHOD OF MOMENTS

If a fault tree has r minimal cut sets (K_1, K_2, ..., K_r) and the probability of occurrence of the ith cut set is $P(K_i)$ then the top event probability expression can be written as

$$P(TOP) \cong \sum_{i=1}^{r} P(K_i) \tag{1}$$

using the rare event approximation as given in the WASH-1400 |2|.

Now, each $P(K_i)$ is the product of the probability of occurrence, X_j, of the basic events in K_i, and therefore

$$P(TOP) \cong \sum_{i=1}^{r} \prod_{j \epsilon K_i} X_j \tag{2}$$

Taking each X_j also as an independent random variable with known moments, we can determine the corresponding moments of the distribution of P(TOP). In this case we say that the top event is represented by its minimal cut sets |8|.

The first moment (mean) can be easily obtained by replacing each X_j by its mean-value ($E|X_j|$) in Eq.(2). Higher order moments can be evaluated by attempting to the fact that the kth moment of a distribution is the expected value of the kth power of the variate, and that the function given by Eq. (2) is multilinear. We have

$$M_k(TOP) = E\left|\left(\sum_{i=1}^{r} \prod_{j \epsilon K_i} X_j\right)^k\right| \tag{3}$$

The moments calculated via Eq. (3) are exact and there is no restriction as to the appearance of the same basic event in more than one cut set. Thus, the problem boils down to correctly performing the calculations as indicated by Eq. (3), within reasonable time limits, for a typical fault tree.

The computer code ADORAVA, written in FORTRAN IV, was developed according to the procedure outlined above. In its current version it assumes the basic events to be lognormally distributed and the input data consist of the cut sets, and the median and error factor of each basic event.

The example below may help to clarify the implementation of the method.

Suppose we have,

$$P(TOP) = X_1 + X_2X_3 + X_4X_5 \tag{4}$$

The evaluation of the first moment of P(TOP) requires the calculation of $E|X_i|$ for each basic event. Using properties of the expected value of independent random variables the first moment of P(TOP) is:

$$E|P(TOP)| = M_1 = E|X_1| + E|X_2|\ E|X_3| + E|X_4|\ E|X_5| \tag{5}$$

In order to evaluate the second moment we square the P(TOP) function, obtaining:

$$P(TOP)^2 = X_1^2 + X_1X_2X_3 + X_1X_4X_5 + X_1X_2X_3 + X_2^2X_3^2 + \\ + X_2X_3X_4X_5 + X_1X_4X_5 + X_2X_3X_4X_5 + X_4^2X_5^2 \quad (6)$$

Care should be taken when squaring the right-hand side of Eq. (4) as $E|X_iX_i|$ is not $E|X_i|E|X_i|$. Thus, we can determine the second moment M_2 by taking the expected value of Eq. (6).

$$M_2 = E|P(TOP)^2| = E|X_1^2| + E|X_1|E|X_2|E|X_3| + E|X_1|E|X_4|E|X_5| \\ + E|X_1|E|X_2|E|X_3| + E|X_2^2|E|X_3^2| + E|X_2|E|X_3|E|X_4|E|X_5| \\ + E|X_1|E|X_4|E|X_5| + E|X_2|E|X_3|E|X_4|E|X_5| + E|X_4^2|E|X_5^2| \quad (7)$$

The same procedure outlined above is repeated for the third moment and higher moment, as needed.

At present the computer code ADORAVA will only go up to the third moment due to storage limitations.

Once the moments are evaluated, they may be used directly to determine confidence bounds for the top event probability through the use of inequalities such as Markov, Tchebycheff, Cantelli, etc. |5|

Alternatively, a subroutine will fit a distribution (chosen at present from the normal and lognormal families) to the given moments and compute selected percentiles from this distribution.

APPLICATIONS

Three examples are given here, comparing the results obtained through the ADORAVA computer code with those given by Monte Carlo simulation and other moment methods.

Example 1

The first example is from WASH-1400 |2| (Appendix II, Ch.3). It consists of seven minimal cut sets: three cut sets of first order (single failures) and four cut sets of second order. The top event function is written as

$$P(TOP) \cong X_1 + X_6 + X_7 + X_2X_5 + X_2X_4 + X_3X_4 + X_3X_5$$

The input data are given in Table I, and the results obtained with ADORAVA code are presented in Table II.

For the COMMODE and BOUNDS codes see reference |5|.

TABLE I

Input data for example 1

BASIC EVENT	MEDIAN	ERROR FACTOR	BASIC EVENT	MEDIAN	ERROR FACTOR
X_1	1.0×10^{-3}	3	X_5	1.0×10^{-2}	3
X_2	3.0×10^{-2}	3	X_6	3.0×10^{-2}	3
X_3	1.0×10^{-2}	3	X_7	1.0×10^{-6}	10
X_4	3.0×10^{-2}	3			

TABLE II

Example 1: Comparison of Mean, Variance and Upper Bound Estimates obtained with Monte Carlo and Method of Moments Codes

	METHOD OF ESTIMATION	MEAN	VARIANCE	90% BOUND	95% BOUND
ADORAVA (2 MOMENTS)	DIRECT RESULTS	7.50×10^{-3}	1.39×10^{-5}	-	-
	FITTED NORMAL	7.50×10^{-3}	1.39×10^{-5}	1.23×10^{-2}	1.36×10^{-2}
	FITTED LOG-NORMAL	7.50×10^{-3}	1.39×10^{-5}	1.23×10^{-2}	1.46×10^{-2}
	MARKOV (1 MOMENT)	-	-	7.502×10^{-2}	1.50×10^{-1}
	TCHEBYCHEFF	-	-	1.93×10^{-2}	2.42×10^{-2}
	IMPROVED TCHEBYCHEFF	-	-	1.87×10^{-2}	2.37×10^{-2}
ADORAVA (3 MOMENTS)	DIRECT RESULTS	7.50×10^{-3}	1.39×10^{-5}	-	-
	FITTED NORMAL	7.25×10^{-3}	1.99×10^{-5}	1.29×10^{-2}	1.46×10^{-2}
	FITTED LOG-NORMAL	7.47×10^{-3}	1.47×10^{-5}	1.23×10^{-2}	1.47×10^{-2}
	MARKOV (3 MOMENTS)	-	-	1.77×10^{-2}	2.04×10^{-2}
SAMPLE	MONTE CARLO (1200 TRIALS)	7.65×10^{-3}	1.49×10^{-3}	1.24×10^{-2}	1.49×10^{-2}
COM MODE	MONTE CARLO (2400 TRIALS)	7.61×10^{-3}	1.37×10^{-5}	1.26×10^{-2}	1.49×10^{-2}
BOUNDS	METHOD OF MOMENTS (2 MOMENTS) FITTED S_B	7.56×10^{-3}	1.39×10^{-5}	1.23×10^{-2}	1.45×10^{-2}

We can see from Table II that the values of the mean and variance given by the ADORAVA code are in good agreement with those given by Monte Carlo simulation (SAMPLE and COMMODE codes) and by another approach to the method of moments (BOUNDS). The confidence bounds obtained from the values of ADORAVA mean and variance by a fitted distribution are also in good agreement with those for Monte Carlo simulation, mainly for a log-normal distribution. A comparison of the results for the 90% and 95% upper bounds (shown in Table II) indicates that the Tchebycheff, the Improved Tchebycheff, and the Markov (3 moments) inequalities give values which are reasonably close to the Monte Carlo results.

Example 2

This example uses the reduced fault tree of the reactor protection system as given in Appendix II of WASH-1400. Here we have assumed the same approximations as Apostolakis and Lee [5]. The results is the function with nine minimal cut sets

$$P|TOP| = X_1 + X_2X_4 + X_2X_5 + X_2X_9 + X_3X_4 + X_3X_5 +$$

$$+ X_3X_9 + X_8X_4 + X_8X_5 + X_8X_9 + X_8X_7 + X_9X_6$$

The input data for this example are given in Table III and the results obtained are summarized in Table IV.

TABLE III

Input data for example 2

BASIC EVENT	MEDIAN	ERROR FACTOR	BASIC EVENT	MEDIAN	ERROR FACTOR
X_1	1.7×10^{-5}	10	X_6	6.1×10^{-3}	4
X_2	3.6×10^{-4}	3	X_7	6.1×10^{-3}	4
X_3	1.0×10^{-3}	3	X_8	9.7×10^{-4}	10
X_4	1.0×10^{-3}	3	X_9	9.7×10^{-4}	10
X_5	3.6×10^{-4}	3			

Again the 90% and 95% bounds obtained by ADORAVA are in good agreement with those of the Monte Carlo simulation codes, despite the difference in the values of the variance obtained by the two methods.

Among the four inequalities used in this work the result of the Improved Tchebycheff gave the best estimate to the 90% and 95% confidence bounds.

Computer time comparison

Table V is a comparison of the computational time required by the codes ADORAVA and SAMPLE in our Burroughs 6700 computer. The codes were run for a set of functions consisting of sums of N identical cut sets of first order, N varying from 10 to 200. All cut sets were assumed to be lognormally distributed with the same median and error factor values, respectively, 1.0×10^{-3} and 10.0.

TABLE IV

Example 2 : Camparison of Mean, Variance and Upper Bound Estimates obtained with Monte Carlo and Method of Moments Codes.

	METHOD OF ESTIMATION	MEAN	VARIANCE	90% BOUND	95% BOUND
ADORAVA (2 MOMENTS)	DIRECT RESULTS	1.08×10^{-4}	3.54×10^{-8}	-	-
	FITTED NORMAL	1.08×10^{-4}	3.54×10^{-8}	3.50×10^{-4}	4.18×10^{-4}
	FITTED LOG-NORMAL	1.08×10^{-4}	3.54×10^{-8}	2.45×10^{-4}	3.76×10^{-4}
	MARKOV (1 MOMENT)	-	-	1.08×10^{-3}	2.17×10^{-3}
	TCHEBYCHEFF	-	-	7.04×10^{-4}	9.50×10^{-4}
	IMPROVED TCHEBYCHEFF	-	-	6.73×10^{-4}	9.29×10^{-4}
ADORAVA (3 MOMENTS)	DIRECT RESULTS	1.08×10^{-4}	3.54×10^{-8}	-	-
	FITTED NORMAL	1.85×10^{-4}	4.69×10^{-8}	4.63×10^{-4}	5.42×10^{-4}
	FITTED LOG-NORMAL	9.49×10^{-4}	4.41×10^{-8}	2.16×10^{-4}	3.50×10^{-4}
	MARKOV (3 MOMENTS)	-	-	1.33×10^{-3}	1.65×10^{-3}
SAMPLE	MONTE CARLO (1200 TRIALS)	1.02×10^{-4}	1.58×10^{-8}	2.22×10^{-4}	3.46×10^{-4}
COMMODE	MONTE CARLO (2400 TRIALS)	- [a]	- [a]	2.43×10^{-4}	3.76×10^{-4}
BOUNDS	METHOD OF MOMENTS (2 MOMENTS) FITTED S_B	- [a]	- [a]	2.46×10^{-4}	3.76×10^{-4}

[a] The values of the mean and variance for this example were not given in Ref. 5.

TABLE V

Comparison of B6700 CPU time (in sec) required by SAMPLE and ADORAVA

CODE \ N	10	20	30	50	70	100	150	200
SAMPLE	87	95	116	173	230	299	426	505
ADORAVA (2 MOMENTS)	3	4	6	7	10	15	24	34
ADORAVA (3 MOMENTS)	6	15	32	115	300	880	-	-

We can see from Table V that when only two moments are specified by the user, the ADORAVA code is very fast compared to SAMPLE. When three moments are specified, the time required by ADORAVA is competitive with that of SAMPLE for N less than fifty.

SUMMARY AND CONCLUSIONS

In this paper we have presented a new approach to the propagation of uncertanties by the method of moments. This approach, implemented in the ADORAVA computer code, utilizes the fact that the kth moment of a distribution is the expected value of the kth power of the variate. Once the moments have been determined the program evaluates confidence bounds to the top event probability by fitting a log-normal or a normal distribution to these moments or by using standard inequalities (such as Markov, Tchebycheff, etc.). The Improved Tchebycheff inequality gave the most reasonable estimates in the cases tested. The procedure of fitting a distribution to the calculated moments gave the best result as compared to those obtained by Monte Carlo simulation. We see from the examples that the utilization of the third moment does not improve the estimates, despite giving more information about the top event distribution. Thus, we think that the best results may be obtained by using two moments and fitting a lognormal distribution (or a Johnson S_B distribution as suggested in Ref. 5).

REFERENCES

1. G.W. PARRY and P.W. WINTER, "The Characterisation and Evaluation of Uncertainty in Probabilistic Risk Analysis", Report SRD R190, Safety and Reliability Directorate, UKAEA (1980)

2. USNRC, "Reactor Safety Study: An Assessment of Accident Risk in US Commercial Nuclear Power Plants", WASH-1400, Washington DC, (1975)

3. A.G. COLOMBO and R.J. JAARSMA, "A Powerful Numerical Method to Combine Random Variables", *IEE Trans. Rel.* R-29, 126 (1980)

4. S. KAPLAN et al, "Methodology for Probabilistic Risk Assessment of Nuclear Power Plants", Report PLG-0209, Pickard, Lowe and Garrick,

Inc., June (1981)

5. G. APOSTOLAKIS and Y.T. LEE, "Methods for the Estimation of Confidence Bounds for the Top-Event Unavailability of Fault Trees", *Nucl. Eng. Des.* 41, 411 (1977)

6. P.S. JACKSON et al, "Comparison of the Monte Carlo and System Moments Methods for Uncertainty Analysis", in *Proc. of th International ANS/ENS Topical Meeting on Probabilistic Risk Analysis*, Sept 20-24, Port Chester, NY, p 973 (1981)

7. K. TAKAGARI, R. SASAKI and S. SHINGAI, "An Improved Moment-Matching Algorithm for Evaluating Top-Event Probability Bounds", *IEEE Trans.* Rel. R-31, 45 (1982)

8. R.E. BARLOW and F. PROSCHAN, *Statistical Theory of Reliability and Life Testing*, Holt, Rinehart and Winston, Inc. (1975)

9. L. AITCHISON and J.A.C. BROWN, "*The Lognormal Distribution*", Cambridge University Press (1957)

SESSION 5

NON-LOCA AND SMALL-BREAK-LOCA TRANSIENTS

Chair: W. Hancox *(AECL)*
E. Hellstrand *(Studsvik)*

ASSESSMENT OF CALCULATIONAL METHODS AND RESULTS FOR LARGE PWR FEEDWATER LINE BREAK AND STEAM LINE BREAK ACCIDENTS

K. S. Chung, M. F. Kennedy, and P. B. Abramson

Argonne National Laboratory
Argonne, Illinois 60439, U.S.A.

ABSTRACT

The main feedwater line break (FLB) and steam line break (SLB) accidents are two major system transients originating from secondary side pipe breaks whose potential seriousness has received considerable attention in recent years. This paper investigates trends and results of FLB and SLB accidents in a large pressurized water reactor, and provides a comparison with the typical bounding calculational approach used by reactor manufacturers in their Final Safety Analysis Reports (FSARs). This paper discusses the applicability of the RELAP series codes for analysis of severe accidents and, from results of parametric studies, highlights the problems which one might expect in using these computer codes and in interpreting the obtained results.

INTRODUCTION

A pipe break downstream of the feedwater line check valves occurring concurrently with inoperability of the main feedwater supply system is a typical initiating event scenario for FLB accident analysis. Until the turbine steam admission valves close, the liquid inventories in the steam generators continue to decrease as flow discharges through the break and liquid boils off, thereby reducing the primary-to-secondary heat transfer. In a SLB transient, a steam line pipe break at the exit of the steam generator creates a major cooldown event, due to excessive mass and energy removal from the steam generator and the accompanying heat removal from the primary. Reactor power increases due to the increase in moderator density and could result in fuel damage. Finally, when the cold High Pressure Safety Injection (HPSI) water hits the vessel it could cause the thermal shock which characterizes the Pressurized Thermal Shock problem now being widely investigated.

The current study focuses on the following aspects of accident analyses, designed to meet audit requirement: i) identify the most conservative initial plant conditions and accident scenario; ii) assess the thermal-hydraulic modeling of computer codes. The reactor system used in this study was the C-E system 80 plant, which has a capacity of 3800 MWt, and RELAP4 and 5 analyses performed by the authors are compared to those published in the CESSAR.

CODE INPUT MODEL DESCRIPTION

Figure 1a shows the ANL CE System 80 plant input model for RELAP5/1 [1]. Similar computations were performed with RELAP4/MOD6 [2] using a very similar noding diagram with a slightly reduced number of hydraulic volumes. Results obtained are used to distinguish the effects of different codes used for audit calculations (i.e., HEM vs. two-fluid model). To see the effects of different hydraulic nodalization on the transient results, a more detailed steam generator model illustrated in Fig. 1b employed,

and a split vessel model shown in Fig. 1c was utilized to maximize the SLB overcooling effects in evaluating the reactivity coefficient of moderator density feedback. (This model was important in describing the impact of multi-dimensional affects of reactor kinetics and flow motion upon calculations with one-dimensional codes.

A transient-specific steady-state initialization is necessary prior to each type of accident calculation [3].

RESULTS OF PARAMETRIC STUDY

The focus of the parametric study is on the determination of the accident condition which will lead to the highest RCS peak pressure for FLB cases (undercooling) and the highest reactor power for SLB cases (overcooling). Many different factors contribute to the severity of the calculated results; for instance, the plant thermal-hydraulic modeling, the assumed plant operating conditions at the initiation of the accident, the availability of the reactor protection systems, and the accident event scenario. These studies indicate that the initial reactor primary loop condition, feedwater conditions, and the break flowrate are the dominant variables which determine the severity of secondary side initiated accidents.

Conservative analysis for FLB accident cases is obtained by delaying reactor scram thereby increasing the potential for continuous heat-up and pressurization after the reactor scram. There appear to be two major interrelated mechanisms affecting the peak RCS pressure: the liquid mass inventory of the secondary side (M_L) and the rate of RCS pressurization ($\dot{P} = dP/dt$) at the time of a reactor trip. The RCS pressurization rate is determined by the primary to secondary heat transfer through the steam generators, which is strongly dependent on the quality (void) profile, which is also directly related to the liquid mass inventory, M_L.

The rate of RCS pressurization ($\dot{P}$) affects the RCS peak pressure in two ways: the reactor trip time (t_t) is determined by the pressure trip setpoint, but the RCS pressure may continue to rise after trip by an amount strongly affected by $\dot{P}$. One of the analysts task is to seek out the combination of M_L and $\dot{P}$ which gives the most conservative results.

Conservative analysis for SLB accident cases requires assumptions which are opposite to those of FLB accident cases. The worst SLB accident scenario is the one which leads to the largest RCS temperature drop from initial conditions and at the fastest rate. However, the thermal shock problems and the DNBR and fuel failure problem are made worse through different details of the SLB accident scenario.

The following parametric studies were performed to investigate how these variables are affected by input conditions.

Effects of Feedwater Condition

In order to determine the effects of FW conditions on the RCS peak pressure and the reactor power return, two extreme feedwater conditions were chosen, representing the upper and lower limits of FW enthalpy (430 Btu/lb and 376 Btu/lb). These lead to two distinctively different RCS operating conditions. The feedwater condition with the 376 Btu/lb enthalpy gives a RCS pressurizer pressure 1920 psia and cold leg temperature 560°F, while the higher feedwater enthalpy case yields a 2400 psia pressurizer pressure and 570°F cold leg temperature.

Table 1 shows the event sequence and the corresponding time at which each event occurred for both FW conditions. The high FW enthalpy case resulted in an earlier reactor scram at 20.35 sec compared to 47.15 sec for the low FW enthalpy case. Because of this earlier reactor scram, the mass inventory at SG is high and the pressurization rate was much smaller than that of the high FW enthalpy case. Note that the loss of heat sink, i.e., the substantial loss of heat transfer capability from the

primary to the secondary side did not occur until 60 seconds compared to 33.8 seconds and 50 seconds for the low enthalpy FW case and the reported CESSAR results, respectively. It took two seconds for this case to increase the RCS pressure from the high pressurizer reactor scram set point (2475 psia) to the pressurizer safety valve setpoint (2525 psia), while the low enthalpy FW case took only 0.6 seconds. From this parametric study, it can be concluded that a higher initial FW enthalpy pressure will result in an earlier reactor trip time (t_t), thus, M_L becomes larger and P is smaller. Consequently, a milder transient response and a lower peak RCS pressure are expected.

The rate of RCS overcooling in SLB computation, is maximized by choosing the high enthalpy FW conditions. This results in higher initial RCS pressure and temperature causing a larger RCS temperature drop accompanied by a large moderator density (reactivity) change.

Effects of Break Sizes and the Critical Flow Model

The break flowrate affects the steam generator mass loss rate and therefore plays a lead role in the amount of overcooling obtained. In this study, break sizes were varied from 0.05 to 0.5 ft^2 as well as using both RELAP4 and RELAP5 and varying the details of nodalization of the steam generators. RELAP4 predicts that a break size 0.05 ft^2 yields the highest maximum pressure, whereas RELAP5 and the CESSAR respectively predict 0.3 ft^2 and 0.2 to be the most conservative break areas.

However, those differences are probably attributable to the different code models and capabilities. For a given break area, the break flowrate varies significantly with the choice of critical flow model. A series of parametric study has been performed by using various critical flow models. Two interesting results are found:

1. There exist a factor of two to three differences in the break flowrate predicted by the various choking models (Fig. 2a). This variation in choked flow models causes the break flowrate to vary from 2500 lbs/sec to 800 lbs/sec during the first five seconds of the transient.

2. Given the same critical flow model, the calculated critical flowrates vary significantly with the choice of nodalization (Fig. 2b). For similar nodalization (i.e., one node SG model), CESSAR and RELAP4 predict a similar critical flowrate. However, a more detailed nodalization results in quite different break flow behavior from that of a one-node SG model. The larger break flowrate for the RELAP4 input model with the one-node SG model seems to be due to the fact that by lumping the entire secondary inventory in one node it takes a relatively long time to bring up the average quality high enough to trigger the change of the critical flowrate.

The critical flow model also affects safety and relief valve flowrates, which are also very important for accident simulation. Therefore, in order to maintain consistency between the audit calculation and FSAR results, the following are suggested:

1. To perform audit calculations, the critical break flow model used in the codes should be comparable to those used in the FSAR.

2. The nodalization used in the steam generator appears to have a larger influence than whether one uses a two fluid model or an HEM model, implying that which code is used is less important than how it is used in predicting the critical flowrates.

Effects of Heat Transfer Characteristics

One of the major uncertainties in analyzing the feedwater line break accident is the steam generator primary to secondary heat transfer characteristics. In the CESSAR calculation, the conservative assumption was made that the heat transfer rate from the

primary to the secondary side stays constant until the secondary side liquid inventory completely drys out.

In Fig. 2c we compare the average effective heat transfer rate between the primary and secondary side of a SG as calculated by RELAP5/1 with 9 boiling nodes, and two RELAP4/6 runs with a 1 boiling node and 5 boilings node on the secondary. As expected, the net heat transfer rate decreases as the inventory decreases. However, RELAP4/6 and RELAP5/1 exhibit similar behavior when many nodes are used, while the use of a single node secondary exhibits a step change in heat transfer rate. This latter results is similar to that shown in for CESSAR and appears to be simply due to the choice of nodalization (CESSAR also has a single volume secondary on the steam generator). No significant differences were obtained by using a more detailed steam generator model (Fig. 2c, 2d).

A similar heat tranfer behavior as predicted by RELAP5 and RELAP4 with the multi-volume SG model was calculated by using RETRAN and LOFTRAN codes [4].

Experimental data obtained from the Semi-Scale feedwater line break experiment shows a rather rapid loss of heat sink [5]. In this experiment the heat transfer rate was evaluated by measuring the primary flow temperature drop across the steam generator. The semi-scale test data shows a smooth and monotonic decrease of the heat transfer rate, and no significant spikes were observed in the total heat transfer rate. In other words, the transitions of boiling modes expected under the boil-off condition do not exert any signficant impact on the total heat transfer rate. However, the individual thermocouple behavior exhibited considerable oscillation. The thermocouple behaviors for the 100% break feedwater line break cases consistently show that all thermocouples experienced a modest drop in the heat transfer rate before a sudden increase and a subsequent plunge into a near zero heat transfer rate. These changes in local heat transfer are due to changes in flow regimes, which cause local changes that do not show up in the global measurement of primary side temperature drop. It took only 4-5 seconds to reach the near-zero heat transfer as shown by the last ramp of heat transfer rate for RELAP5/1 calculation. Therefore, a notion that there exists a slow slope linear relationship between the mass inventory and the heat transfer rate is not acceptable from the semiscale test data as well as the RELAP series code results.

The second major point addressed by the semiscale test is that the onset of the heat transfer degradation starts at the early stage of transients. From the semi-scale test, heat transfer degradation began at the 85% (100% break size), 75% (50% break size) and 50% (14% break size) initial mass inventory.

The third important observation in these semiscale test results is that, even though the intact side volume is three times larger than the broken side SG volume, the onset of heat transfer degradation for both intact and broken steam generators occurred approximately at the same time.

AUDIT RESULTS

FLB Audit Results

In the FLB analysis RELAP5 predicted a somewhat slower transient response (Table 1) resulting in a lower maximum pressure than that predicted in the CESSAR, primarily due once again to the difference in break flow rates caused by the different break flow models. The pressure relief in the primary side is largely caused by the steam line safety valve opening which enhances a very large heat removal from the primary to the secondary side (Fig. 3a). As the steam line safety valve starts to close (CESSAR 73.8 seconds, RELAP5 57 seconds), the rapid depressurization stops. The RELAP5 calculation shows a second pressure increase up to the point where the primary pressure re-reaches the pressurizer safety valve opening setpoint. The primary pressure stays at this safety valve setpoint with the aid of the cyclic opening and closing of safety valve until the combination of Emergency Feedwater Flow supply and the sufficiently

low reactor power cools down the reactor system. Other differences between the RELAP5 computation and the results reported in CESSAR appear to be due to this break flow difference. For example, the RELAP5 secondary side pressure did not increase until the mass inventory became very small (see the section on steam generator nodalization) and timing differences on MSIV closure are similarly based.

SLB accident analysis study has been concerned with the safety margin available for maintaining the integrity of fuel pins under severe overcooling condition. The saturated boiling and the possible subsequent departure from nucleate boiling in connection with the rapid depressurization, and the return to the high reactor power by the reactivity feedback due to the large moderator density change are the event scenarios which have been investigated extensively. Recent attention has been given to the integrity of the vessel wall under the severe thermal stress generated by a large temperature difference across the wall surface. Figure 3b shows the calculated reactor power for the SLB case with the zero initial power. Depnding on what moderator temperature is used for the reactivity feedback calculation, the peak reactor power varies signficantly. By using the cold side core temperature, the calculated reactor peak power is 47%, whereas using the broken side cold leg temperature, the peak reactor power becomes 180%. The first power peak is due to the heat transfer degradation caused by reduced SG inventory. The cooling trend starts again when the MSIV starts to close thereby collapsing the liquid in SG. Finally, the reactor power decreases by the reactor scram. The reactor power calculated by using the cold leg temperature as the moderator density feedback temperature does not show this behavior, because the moderator feedback from the coldleg overwhelms the Doppler feedback from the core heat slab.

Figure 3c shows the temperature responses of the vessel downcomer coolant fluids for the full power SLB case with and without RCS pump running. The cold side temperature starts to increase at 120 seconds because the steam generator quality is so high that the broken side steam generator loses most of its heat sink capability. Note that the decrease rate of temperature changes at 80 seconds due to the HPSI actuation.

There exist several factors contributing to the severity of SLB accident results.

1. The break flowrate plays a very important role in determining the severity of transient response. However, since break size and shape are merely postulated, it is the break flow which is the important parameter -- not the critical flow model.

2. The accident scenario and the operating procedure are very important. For the vessel wall thermal shock problem, the calculation without RCS pumps running yields more severe results, while a higher DNBR is obtained with RCS pumps running.

3. The flow mixing in the reactor vessel is very important for both the thermal shock problems and the DNBR calculation.

CONCLUSIONS

In performing or any safety analyses, the user must be aware of the limitations and capabilities of the computer codes being used as he undertakes analysis of plant transient behavior. Calculated results vary significantly with the modeling of the plant and choice of code. Selection of the initial conditions and the accident scenario, including the availability of various reactor protection systems, should be carefully made to yield physically reasonable accident results.

Table 1.

Event	Setpoints	Result (Time/Values) CESSAR	Standard FLB Model	High FW Enthalpy Case
Break Initiation	0.2 ft^2	0.0	0.0	0.0
Loss of Heat Sink		33.8	~50.1	>50.
LWL Trip from Broken SG	Empty (24.5 ft)	34.4	16.5	24.
EFAS from Broken SG	Empty (19.75 ft)	34.4	20.75	31.5
High Pressure Reactor Trip	2475 psia	34.4	47.15	20.35
Pressurizer Safety Open	2525 psia	34.6	47.75	22.35
Loss of Power Supply		35.9	49.10	22.35
LWL Trip from Intact SG	-	36.9	18.75	25.
Maximum Values:				
RCS Pressure		38.2/2843 psia	50/2828 psia	24/2590 psia
Pressurizer pressure		2587 psia	2578 psia	2525 psia
Surge line flow		2206 lb/sec	2218 lbm/sec	653 lbm/sec
Main Steam Safety Valves Open	1282 psia	40.5	59.0	24.
EFAS from Intact SG		44.6	69.0	>100.
Maximum SG Pressure		44.8/7318 psia	59.5/1283 psia	29/1344 psia
Pressure Safety Close	2625 psia	45.4	55.	
Main Steam Safety Close	1218 psia	73.8	63.	48.
Emergency Feedwater Flow Initiated		79.4	114.5	>100.
MSIV Closure	810 psia	165.6	122.6	--
EF Flow Terminated to Broken SG	170 psia	173.6	248.0	
Main Steam Safety	1282 psia	314.2	chattering	

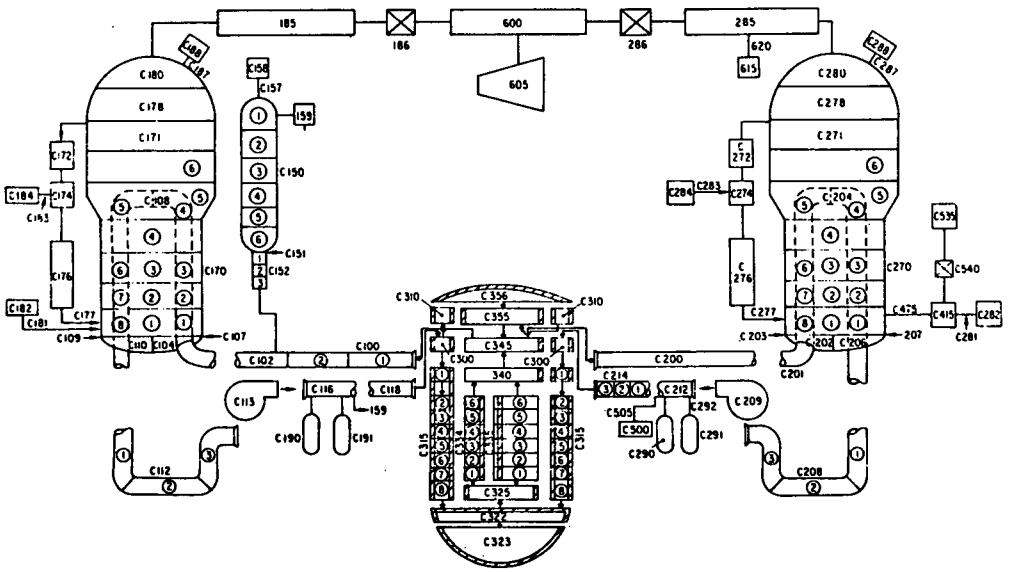


Fig. 1a. RELAP5/1 Plant Input Model.

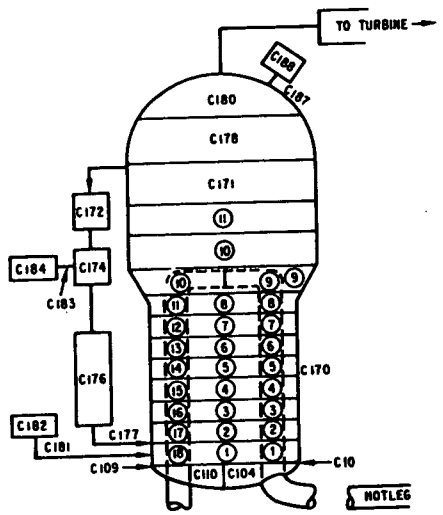


Fig. 1b. Multi-Volume SG Model.

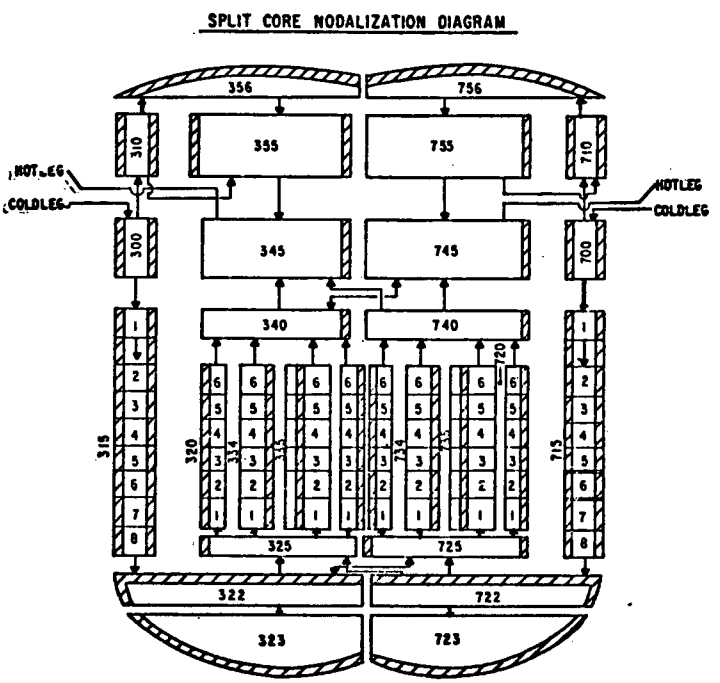


Fig. 1c. Split Core Noding Diagram.

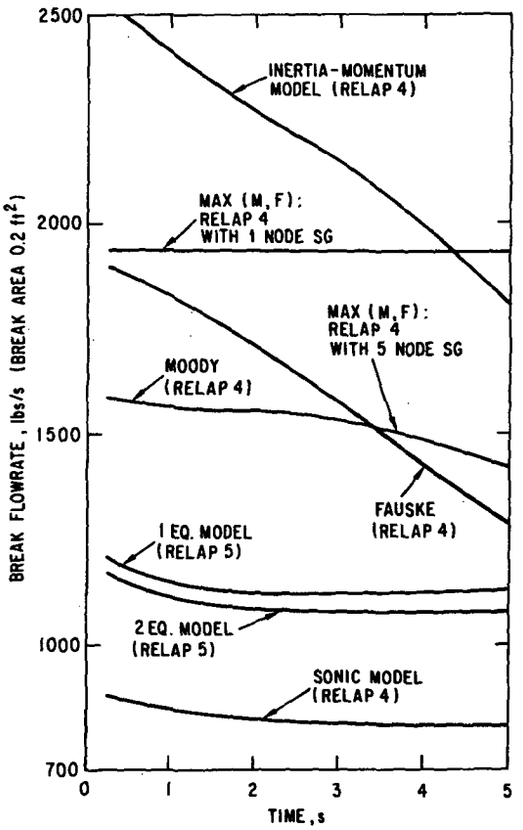


Fig. 2a. Break Flowrate Calculated by Various Critical Fow Model.

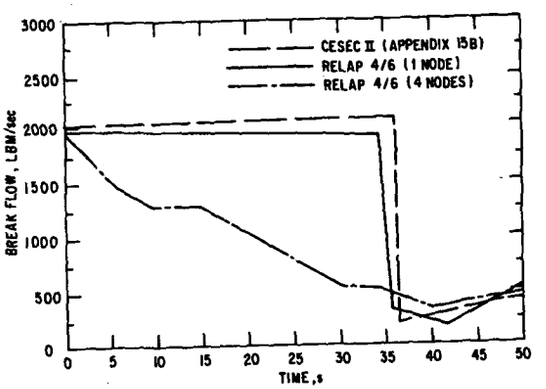


Fig. 2b. FLB Break Flowrate Behavior Calculated by RELAP4/6 and CESSAR.

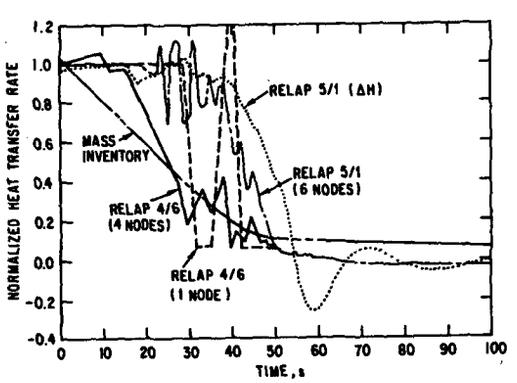


Fig. 2c. Code Calculated Total Heat Transfer Rates.

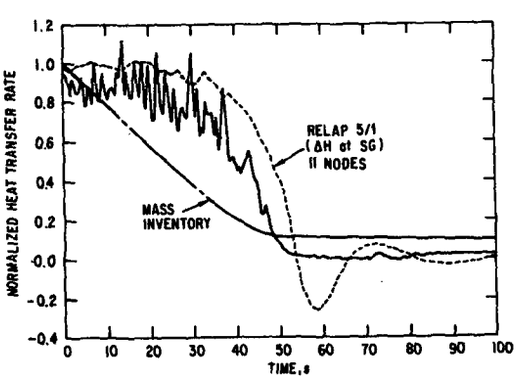
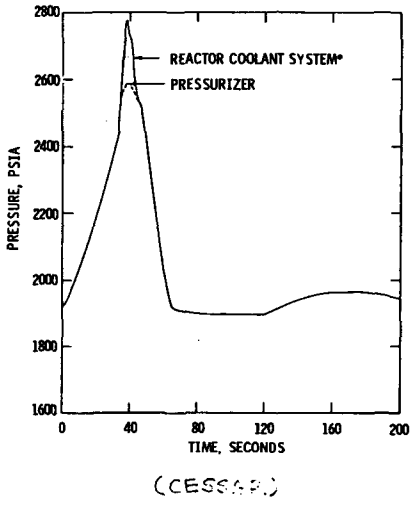


Fig. 2d. Total Heat Transfer Rates Calculated Using a Multi-Node SG Model.



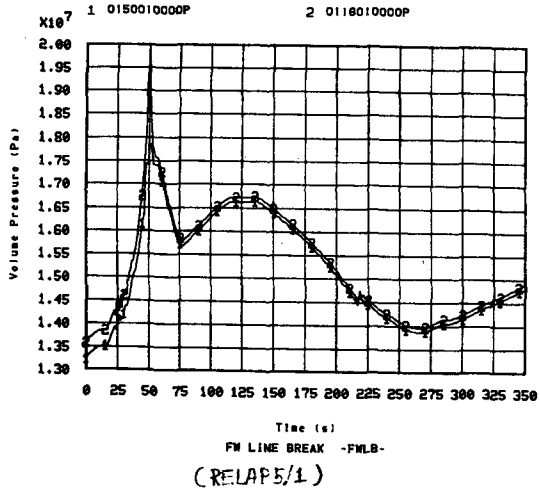


Fig. 3a. RCS and Pressurizer Pressure vs Time.

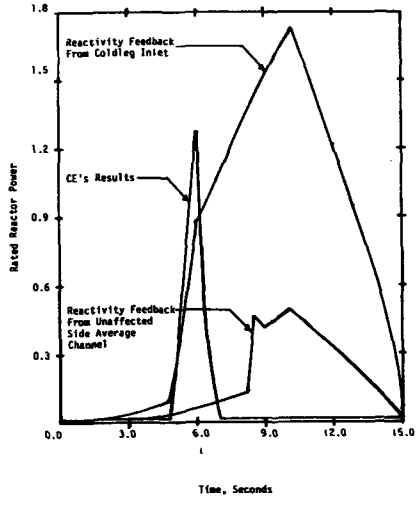


Fig. 3b. Calculated Reactor Power vs Time for SLB Zero Power Case.

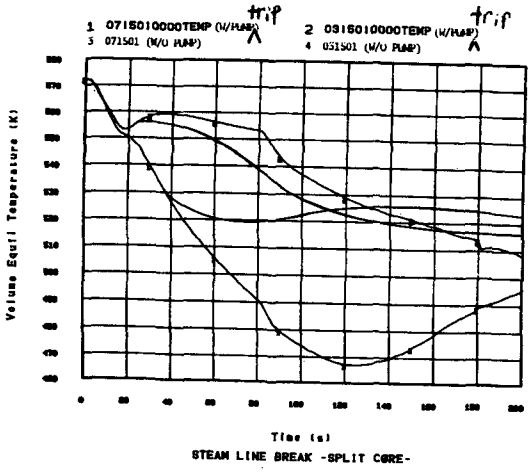


Fig. 3c. Calculated Downcomer Coolant Temperature for SLB Full Power Case.

STEAM-GENERATOR-TUBE-RUPTURE TRANSIENTS FOR PRESSURIZED WATER REACTORS*

D. Dobranich, R. J. Henninger and N. S. DeMuth

Los Alamos National Laboratory
Los Alamos, New Mexico 87545, U.S.A.

ABSTRACT

Steam generator tube ruptures with and without concurrent main-steam-line break are investigated for pressurized water reactors supplied by the major US vendors. The goal of these analyses is to provide thermodynamic and flow conditions for the determination of iodine transport to the environment and to provide an evaluation of the adequacy of the plant safety systems and operating procedures for controlling these transients. The automatic safety systems of the plant were found to be adequate for the mitigation of these transients. Emergency injection system flows equilibrated with the leakage flows and prevented core uncovery. Sufficient time was afforded by the plant safety systems for the operators to identify the problem and to take appropriate measures.

INTRODUCTION

Steam generator tube ruptures (SGTRs) with and without a concurrent main-steam-line break (MSLB) were investigated for the three generic types of US Pressurized Water Reactors [Westinghouse (W), Babcock-and-Wilcock (B&W), and Combustion Engineering (CE)]. These transients recently have received attention from the Nuclear Regulatory Commission (NRC) because of the relatively large potential for radionuclide release to the atmosphere along with the possibility of core uncovery and subsequent damage. Main-steam-line breaks are relatively low-probability events whereas, steam generator tube ruptures occur frequently, as indicated by licensee event reports for operating plants. The NRC requires utilities to analyze both single failure accidents in their safety analysis reports, but multiple failure accidents involving both a MSLB and SGTR have not been addressed.

The analyses provide best-estimate evaluations of the severity and consequences of the accidents using the Transient Reactor Analysis Code (TRAC) [1], version PD2. TRAC is a two-fluid, nonequilibrium, thermal-hydraulics code for investigating accidents in light water reactors and has been assessed against data from a diverse range of experimental facilities. The goals of the calculations are to provide thermodynamic and flow conditons for the determination of iodine transport to the

*Work performed under the auspices of the US Nuclear Regulatory Commission.

environment and to evaluate the adequacy of the plant safety systems and operating procedures for controlling the transients. The determination of the radionuclide exposures and dose rates is not a part of this study; only the thermodynamic and flow source terms necessary for this analysis are described. Analyses include calculations of 1, 5, and 10 steam generator tube ruptures with and without concurrent main-steam-line break.

MODEL DESCRIPTION AND ASSUMPTIONS

To simulate the transients for the three plants, comprehensive numerical models were developed for TRAC-PD2 including a three-dimensional vessel with related internal hardware, fuel rods with a point kinetics formulation of reactivity feedback, hot- and cold-leg piping, main coolant pumps (MCP), pressurizer (with heaters), once-through or U-tube steam generators (SG), upper-plenum vent valves (where applicable), accumulators, high and low pressure injection systems (HPI and LPI), primary-volume makeup system, main and auxiliary feedwater (MFW and AFW) with secondary-side water level control, steam lines with atmospheric relief valves (ARV), and turbine stop valves.

Approximately 150 finite-difference mesh cells were used for each of the plant models. The tube ruptures were modeled as double-ended breaks by connecting the primary side of the steam generator to the secondary side. The length and hydraulic diameter of the connecting pipe equaled the length and hydraulic diameter of a single tube and the flow area was adjusted according to the number of tube ruptures assumed. Additional loss coefficients were added to account for the discharge losses of the ruptures. A brief summary of the three generic PWRs modeled for these analyses is shown in Table I.

Automatic and operator-controlled actions were modeled to provide a best-estimate approximation of the system response as designed. The SGTRs occur at time zero ($t = 0.0$) and were modeled as double-ended breaks at the top of the SGs. The MSLBs also occured at time zero. The steam line was assumed to break (complete guillotine rupture) outside the containment and upstream of the isolation valves. Table II lists the automatic actions during these transients for each of the three plants.

In addition to these actions, the HPI flow was throttled if the pressurizer level recovered to the normal range (assumed operator response) and AFW was controlled to maintain a specified secondary-side water level. The major operating difference of the three plants is the primary temperature control of the ARVs for the CE plant. Both W and B&W plants control ARV opening on secondary pressure. Because

TABLE I

SUMMARY OF PWRs

Plant	Vendor	Number of SGs	SG Type	Number of tubes per SG	Single tube flow area (m^2)
TMI-1	B&W	2	Once-through	7765	1.571×10^{-4}
Zion-1	W	4	U-tube	3388	3.043×10^{-4}
Calvert Cliffs-1	CE	2	U-tube	8519	2.167×10^{-4}

TABLE II

AUTOMATIC PLANT RESPONSE

Action	Plant		
	TMI-1	Zion-1	CC-1
Reactor scram	P_p < 13.1 MPa or 12% overpower	P_p < 13.1 MPa or 16% overpower	P_p < 11.9 MPa or 6.5% overpower
Close turbine stop values	Concurrent with reactor trip	Concurrent with reactor trip	Concurrent with reactor trip
ARVs open	P_s > 7.2 MPa	P_s > 7.1 MPa	T_p > 550 K
MFW trip	P_s < 4.1 MPa or concurrent with reactor trip	60% excess steam-flow or concurrent with reactor trip	P_s < 3.5 MPa or concurrent with reactor trip
Initiate AFW	After MFW has ended	After MFW has ended	After MFW has ended
Initiate HPI	P_p < 11.1 MPa (30 s delay)	P_p < 11.7 MPa (30 s delay)	P_p < 10.9 MPa (30 s delay)
MCP trip	30 s after HPI initiation	30 s after HPI initiation	30 s after HPI initiation
Accumulator valves open (initially)	P_p < 4.14 MPa	P_p < 4.14 MPa	P_p < 1.48 MPa

P_p [=] primary pressure
P_s [=] secondary pressure
T_p [=] primary temperature

each plant has a different turbine bypass capacity to the condensers, it was assumed that steam relief would be through the atmospheric relief valves only.

STEAM GENERATOR TUBE RUPTURES

Three Mile Island, Unit-1

Except for the timing of the trips and the emergency core cooling (ECC) flows, the results for 1, 5, and 10 SGTRs generally were very similar. The sequence of events for these transients are summarized in Table III.

Initially, the pressurizer heaters and primary-system makeup flow were actuated in response to the decreasing primary pressure and pressurizer water level. This was insufficient, however, to prevent primary depressurization and a reactor trip signal was generated because of low system pressure.

When the system pressure decreased to 11.1 MPa, the HPI flow was actuated and began injecting subcooled liquid into the cold legs. The HPI flow was sufficient to make up for the primary liquid being lost through the ruptured tubes and the primary pressure stopped decreasing and leveled. For the 5- and 10-SGTR cases, the pressurizer level did not recover. Therefore, the HPI flow remained at its maximum value, which was sufficient to remove all the core decay energy. For the 1-SGTR

TABLE III

TMI SGTR SEQUENCE OF EVENTS[a]

Event	Time (s) 1-SGTR	5-SGTR	10-SGTR
SGTR	0.0	0.0	0.0
Reactor scram, (Close turbine stop valves)	492.8	72.1	34.7
MFW coastdown	517.3	91.7	54.2
Initiate HPI	523.4	94.6	54.0
Initiate AFW (SG level control)	522.3	96.7	59.2
Trip main pumps	583.3	154.5	113.8

[a]The event sequences are similar for Zion and Calvert Cliffs.

case, the pressurizer level did recover and the HPI flow was throttled. The throttled HPI flow was capable of removing only part of the core decay energy and the SGs were required to remove the remainder by way of natural circulation. This required increased opening of the ARVs and for this reason, the amount of primary liquid lost out the ARVs was considerably more than would be expected compared to the 5- and 10-SGTR cases.

The damaged steam generator secondary filled with liquid because of primary leakage. The assumption was made that the operators had identified the damaged SG by this time and initiated actions to prevent the steam line from filling. In an actual plant, the problem may have been identified sooner; however, waiting until the SG is full represents a maximum time allowed to initiate action without introducing the possibility of damaging the steam line. The assumed operator action was the opening of the ARV on the intact loops. This allowed depressurization of that SG, which greatly enhanced primary-to-secondary heat transfer and in turn decreased the primary pressure. The opening of the ARV was controlled so that the AFW could maintain the SG water at the prescribed operating level. Once the primary pressure decreased to the damaged secondary-side pressure, the tube rupture flow ended, and the transients were terminated. If no operator action were taken, the steam line on the damaged loop would fill with liquid. The ARVs would then begin relieving liquid directly from the primary. The primary pressure and leakage flow for the 5-SGTR case are shown in Figure 1.

Zion, Unit-1

The response of the system for Zion was basically the same as the response for TMI. Again, the primary pressure dropped, tripping the power and initiating HPI flow. The pressurizer refilled for the 1-SGTR case, requiring opening of the damaged loop ARV to accomodate decay energy removal. Because three intact SGs were available for primary depressurization (only one for TMI), termination of primary leakage required less time to accomplish after operator action was initiated. It was also necessary for the operators to throttle the HPI flow in conjunction with secondary-side blowdown to terminate leakage. This was necessary because HPI for Zion consists of charging flow and safety injection flow that continues to increase

as primary pressure drops. The increasing safety injection flow greatly reduced the primary depressurization rate. The primary pressure and leakage flow are shown in Figure 2 for the 5-SGTR case.

Calvert Cliffs, Unit-1

Although system response was very similar to TMI and Zion, some small differences in the operating procedures and the ECC system led to somewhat different results.

As the power decayed and the HPI flow began, the secondary-side pressure stabilized at 6.1 MPa where it remained until the operator intervened. The HPI flow was sufficient in all cases to make up for the primary liquid lost through the ruptured tubes. The pressurizer partially refilled only in the 1-SGTR case. In the 5- and 10-SGTR cases, the pressurizer remained empty until the operator intervened. The combination of once-through cooling (the HPI liquid went through the vessel and out the tube rupture) and boiling of secondary-side water maintained a primary temperature of 550 K. For the 1-SGTR case, the amount of once-through cooling provided by the HPI flow was lower because of the reduced leakage rate and hence higher primary pressure. This required a higher secondary boiling rate to maintain the primary temperature at 550 K. Therefore, increased opening of the ARVs to remove the excess decay energy was necessary. Figure 3 shows the primary pressure and leakage flow for the 5-SGTR case.

SUMMARY OF STEAM GENERATOR TUBE RUPTURES

For the SGTR transients, the HPI was sufficient to equilibrate with the leakage flow and prevent accumulator injection. Water levels remained well above the top of the core for all cases. For the cases involving one ruptured tube in W and B&W plants, the pressurizer refilled, requiring throttling of the HPI. This throttling had a significant effect on the amount of primary liquid lost to the environment because of the decreased once-through core cooling. When the HPI was throttled, the HPI flow was no longer sufficient to remove all the decay energy. The excess decay energy induced natural circulation flow through the steam generators, which in turn required increased opening of the atmospheric relief valves and increased loss of primary fluid to the environment. Although the pressurizer never refilled for Calvert Cliffs, the low HPI flow at high system pressure was insufficient to remove all the decay energy and the secondary liquid continued to boil. The principal factor that influenced the primary leakage was the operator response time. As soon as primary and secondary pressures equilibrated, leakage was terminated. There was never any danger to the core in these transients; the automatic safety systems functioned to prevent core uncovery until operator action was initiated. Tables IV and V list the total amount of leakage out the ARV and primary, respectively. Because the operating systems and geometries for the three plants vary considerably, it is difficult to draw conclusions as to which plant performs best. The tables are compiled for two different assumptions:

(1) Operator action to depressurize the primary when the damaged SG secondary is filled with liquid, and

(2) Operator action to depressurize the primary 10 minutes after reactor trip.

Some extrapolation was necessary to compile these numbers. In general, all plants behave similarly and result in approximately the same amount of leakage. However, Zion has an advantage with respect to limiting leakage because three-out-of-four intact steam generators are available to remove decay heat and depressurize the primary compared to only one-out-of-two for TMI and Calvert Cliffs.

TABLE IV

SUMMARY OF TOTAL FLOWS LEAKED TO ATMOSPHERE
FOR SGTR TRANSIENTS

	Total ARV Leakage (10^4 kg)		
Case	TMI-1	Zion-1	CC-1
1-SGTR[a]	4.7	1.4	5.4
5-SGTR[a]	2.1	0.52	2.7
10-SGTR[a]	1.8	0.51	2.4
1-SGTR[b]	3.1	0.43	1.9
5-SGTR[b]	1.9	0.48	1.7
10-SGTR[b]	1.8	0.51	1.7

[a]Operator action to depressurize the primary when the damaged SG secondary is filled with liquid.
[b]Operator action to depressurize the primary 10 minutes after reactor trip.

TABLE V

SUMMARY OF PRIMARY LEAKAGE FLOW FOR SGTR TRANSIENTS

	Total Primary Leakage (10^4 kg)		
Case	TMI-1	Zion-1	CC-1
1-SGTR[a]	15.0	11.0	7.7
5-SGTR[a]	15.0	9.0	11.0
10-SGTR[a]	11.0	6.0	12.0
1-SGTR[b]	2.8	1.9	2.7
5-SGTR[b]	10.0	4.1	4.7
10-SGTR[b]	11.0	4.2	5.4

[a]Operator action to depressurize the primary when the damaged SG secondary is filled with liquid.
[b]Operator action to depressurize the primary 10 minutes after reactor trip.

STEAM GENERATOR TUBE RUPTURES WITH MAIN-STEAM-LINE BREAK

Three Mile Island, Unit-1

In analyses of SGTR with concurrent main-steam-line break, a double-ended break of the steam line outside the containment and upstream of the main-steam-line isolation valve was assumed. Because the steam lines from the SGs connect into a common header, all SGs initially blow down to the atmosphere until the turbine stop valves or main steam isolation valves are closed. The initial response of the system for all cases were similar because the secondary blowdown was the dominant effect. Reactor trip and turbine stop valve closure were initiated by an overpower signal. The power increase was caused by a positive reactivity insertion due to overcooling of the primary during secondary-side blowdown. Main feedwater also was terminated near this time. HPI was initiated on a low primary pressure signal. The sequence of events for these transients are shown in Table VI.

For the 5- and 10-SGTR cases, voiding of the upper elevations of the system occurred because of the system liquid contraction (from rapid cooling) and the high leak rates associated with the large number of tubes ruptured. Steam flow out the rupture lowered the primary pressure to the accumulator set point. The accumulators slowly discharged and helped to maintain the primary pressure and liquid level at constant values. For rupture of less than five tubes, the HPI equilibrated with the leakage flow and maintained the primary pressure above the accumulator set point. Figure 4 shows the primary pressure and leakage flow for the 5-SGTR case.

Zion, Unit-1 [2]

The response for Zion was very similar to the TMI transients. HPI flow was sufficient to keep the system full and re-establish subcooling for ruptures of less than five tubes. For the rupture of more than five tubes, the core remained covered but the upper parts of the system were voided. In particular, the tops of the intact SG U-tubes contained steam, blocking natural circulation cooling to those SGs. Leakage would continue until the primary pressure is reduced to atmospheric. Figure 5 shows the primary pressure and leakage flow for the 5-SGTR case.

TABLE VI

TMI SEQUENCE OF EVENTS FOR SGTRs WITH MSLB

Event	TIME (s) 1-SGTR	5-SGTR	10-SGTR
MSLB, SGTR	0.0	0.0	0.0
Reactor scram, close loop-A turbine stop valve	5.82	5.81	5.80
Initiate HPI	16.5	14.6	14.2
Main feedwater coastdown	21.5	21.5	21.5
Initiate AFW	26.5	26.5	26.5
Trip main pumps	76.5	74.4	74.1

Calvert Cliffs, Unit-1

Again, the results for Calvert Cliffs closely resemble those for TMI and Zion. HPI flow in the 1- and 5-SGTR cases was sufficient to refill and subcool the primary system. The core was cooled by a combination of once-through HPI flow and heat transfer to the intact steam generator secondary. HPI flow in the 10-SGTR case refilled the vessel to the top of the upper plenum; the intact steam generator, upper vessel head, and pressurizer contained vapor. In the 10-SGTR case, the core was cooled by once-through HPI flow. Figure 6 shows the primary pressure and leakage flow for the 5-SGTR case.

SUMMARY OF STEAM GENERATOR TUBE RUPTURES WITH MAIN-STEAM-LINE BREAK

Accumulator injection initiated for the cases involving MSLB with five or more ruptured tubes for B&W and W plants. The accumulator flow helped to refill the primary and stabilize the pressure. Accumulator flow did not begin in the CE plant because of the much lower accumulator setpoint and the slightly higher HPI capacity available at low pressures. The leakage rate stayed constant after it equilibrated with the combined HPI and accumulator inflow and the core remained covered with water throughout the transients. For the cases with more than five ruptured tubes, voiding of the upper elevations of the hot legs occurred when the primary fluid temperature dropped below the intact-loop secondary-side liquid temperature. This loss of driving potential for natural circulation led to phase separation with the vapor rising to the top of the loop. In the absence of natural circulation, lowering the primary pressure by blowing down the intact SG would be difficult without additional operator action such as "bumping" the primary pumps to remove the voids and temporarily restore primary cooling. The operators may be required to use an alternate strategy to depressurize the primary, such as opening a primary pressure relief valve. When the primary pressure reaches atmospheric, the operator will then have to initiate decay heat removal systems to ensure core cooling and to allow throttling of ECC flow. ECC flow must continue until the power decreases sufficiently to allow this. Primary leakage will continue until this is accomplished and the primary pressure is reduced to atmospheric. The total amount of primary leakage and the equilibrium leakage rate at 2500 s are given in Table VII.

TABLE VII

SUMMARY OF PRIMARY LEAKAGE FOR SGTRs WITH MSLB

	Total Leakage (10^4 kg)/Primary Leakage Rate (kg/s) at 2500 s		
Case	TMI-1	Zion-1	CC-1
1-SGTR	6.5/25	6.0/21	3.7/12
5-SGTR	20.0/60	24.0/59	12.0/50
10-SGTR	22.0/60	NC	19.0/75

NC-not calculated

CONCLUSIONS

Steam generator tube ruptures with and without a main-steam-line break for the three generic plants are relatively severe accidents with respect to the potential for radionuclide release to the environment. However, they do not represent accidents that existing safety systems cannot mitigate. Operator action will be required to depressurize the plant and terminate the transient; but, automatic actions are sufficient to maintain the plant in a safe condition until such action is taken. The ECC system will provide sufficient time for operators to evaluate the situation and to take appropriate steps.

The HPI capacity, in many instances, is greater than the flow required to mitigate the accident. In general, as long as the HPI flow is sufficient to equilibrate with the leakage flow, partial unavailability of the HPI will not impede recovery of the plant. Sufficient cooling capacity is available from the remaining intact steam generator(s), if the HPI flow is throttled.

With respect to the amount of primary leakage, the results though reasonable, are not what one might expect. The amount of primary fluid leaked to the environment depends more upon cooling requirements than the number of tubes ruptured. The principal factors that influence the leakage are the throttling of the HPI flow and the operator response time. Lower HPI flow results in lower once-through cooling, requiring more secondary-side boiling. This, in turn, requires more steam flow from the ARVs and hence a higher primary leakage rate to the environment. The operator response time determines the termination of leakage and, therefore, the total amount of primary liquid lost.

REFERENCES

1. Safety Code Development Group, "TRAC-PD2, An Advanced Best-Estimate Computer program for Pressurized Water Reactor Loss-of-Coolant Accident Analysis," Los Alamos National Laboratory report LA-8709-MS (May 1981).

2. Dean Dobranich, "Analysis of Steam-Line-Break-Induced Steam Generator Tube Rupture," American Nuclear Society Transactions, Vol. 38, pp. 438-439 (June 1981).

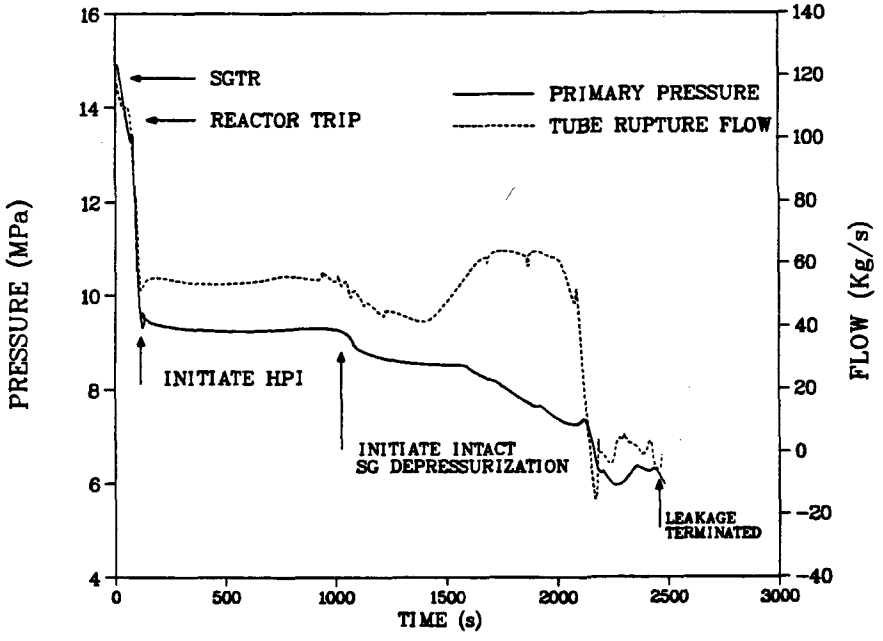


Fig. 1. System response for 5-SGTR, B&W case.

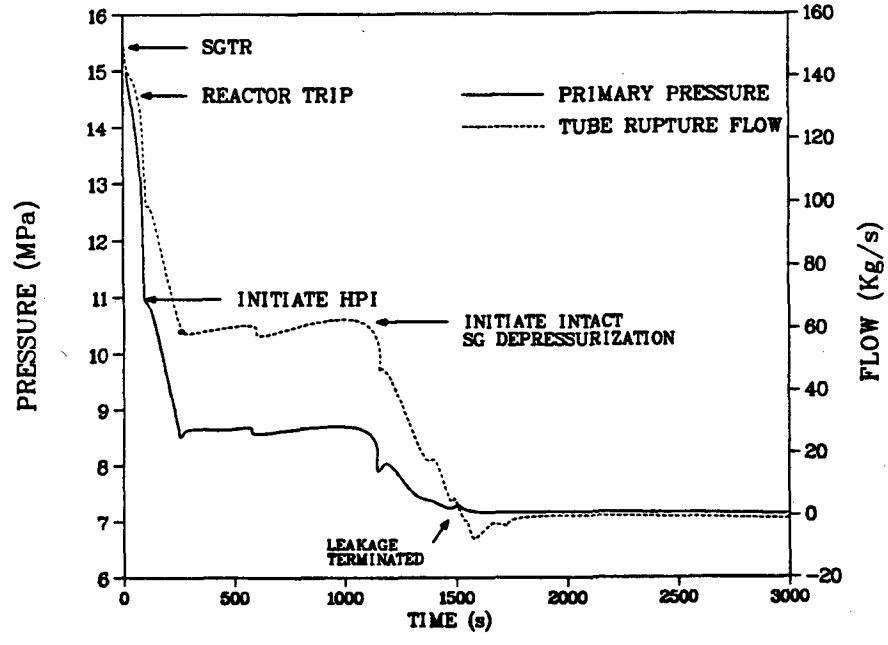


Fig. 2. System response for 5-SGTR, W Case.

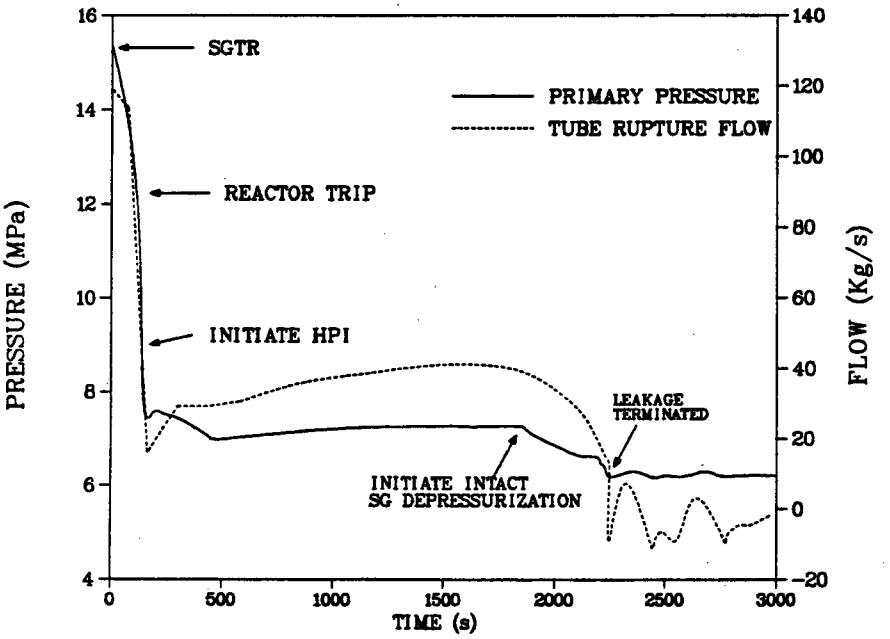


Fig. 3. System response for 5-SGTR, CC case.

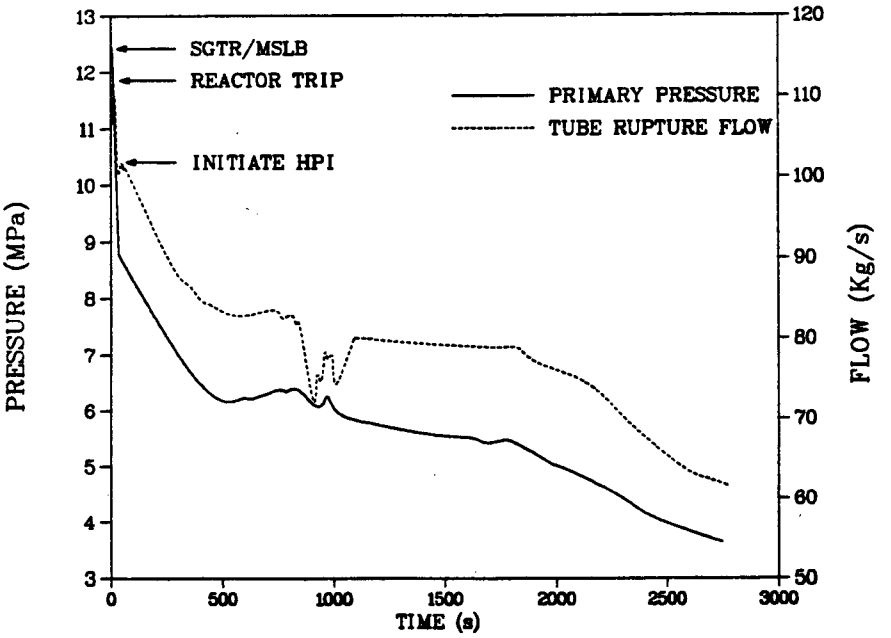


Fig. 4. System response for 5-SGTR/MSLB, B&W case.

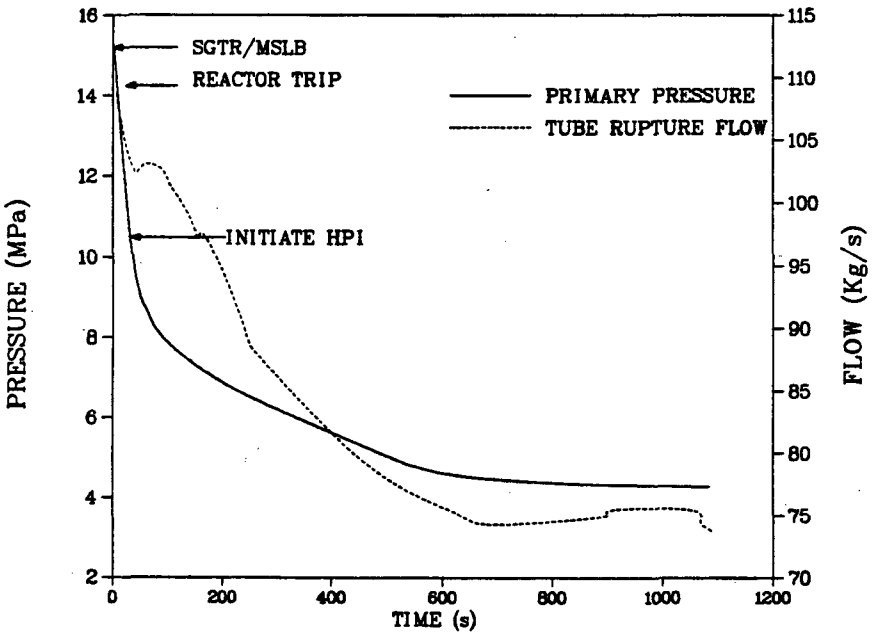


Fig. 5. System response for 5-SGTR/MSLB, W case.

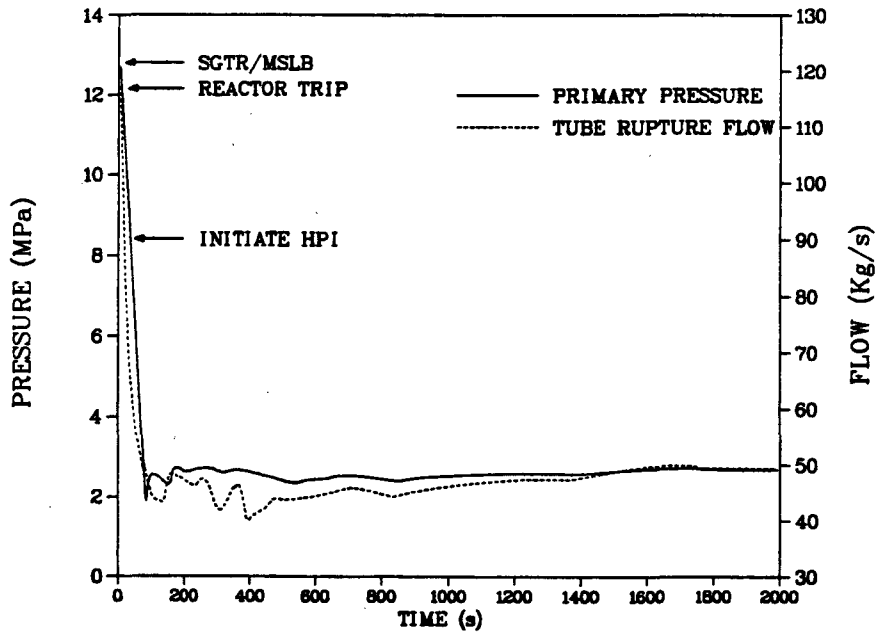


Fig. 6. System response for 5-SGTR/MSLB, CC case.

PREDICTIONS ON ANGRA 1 BEHAVIOUR DURING STARTUP TESTS USING THE ALMOD CODE

CLAUDIO T. M. CAMARGO

Departamento de Reatores
COMISSÃO NACIONAL DE ENERGIA NUCLEAR
Rio de Janeiro - Brasil

ABSTRACT

The Angra Nuclear Power Plant Unit 1, a Westinghouse 2-loop PWR, was schedule to achieve full power in 1982. To predict plant behaviour during some of the startup tests, a modified version of the ALMOD3 code, which can simulate the control systems of Westinghouse NPP's was developed. Transients such as 10% load swing, large load reduction and natural circulation were calculated and are presented in this paper. The natural circulation prediction is compared with experimental test results. The model verification of the new version, called ALMOD 3W, will be carried out through comparisons between calculated transients and those recorded at the plant during the test phase.

INTRODUCTION

The first Brazilian Nuclear Power Plant, Angra 1, is a Westinghouse 2-loop PWR which was scheduled to achieve full power in 1982.

In coming years, the Brazilian Nuclear Program is committed to build 4-loop PWR plants of KWU design.

In 1980, a copy of the ALMOD[1] code, version 3, was delivered to CNEN. This code, while very useful in simulating transients, was too specific to KWU plants and that motivated developing a work to make it able to simulate Westinghouse NPP's also.

The main differencesbetween KWU standard plants and Angra 1, as related to the ALMOD models, are located in the pressurizer surge line, in the steam generators' secondary side and in the control systems.

The first two differences were handled by the use of sensitivity studies in some input variables. Calculations could then be performed[2] as part of the licensing process for accident analysis review, where control systems are assumed not to function. However, the control system models were too restrictive and Angra 1's characteristics could not be introduced by input data manipulations only.

For competence in making independent calculations and to qualify the model proposed by the utility, a new version called ALMOD 3W was developed which had the ability to simulate the controls of primary temperature, pressurizer pressure, steam generator level and steam dump, for Westinghouse plants.

Several transients were calculated using this code[3] to predict plant behaviour during the startup test phase. The specific results presented are a 10% load swing at

30% power, a 50% load reduction from 100% power and a natural circulation test at 3% power.

The natural circulation test prediction is confronted with some experimental results, although this comparison has been limited by inadequate scaling of experimental data.

CONTROL SYSTEMS MODELLING

The rod control system of Angra 1 maintains the reactor coolant average temperature as a linear function of the turbine load. The rods will move according to a combination of two temperature error signals. One is between programmed and actual temperature and the other signal is a temperature error equivalent to the rate of change of power mismatch (Figure 1).

The final control reactivity is dependent on rod velocity demand and on the differential rod worth as a function of bank position. Starting from an estimated rod position as a function of nuclear power, the ALMOD 3W monitors the rod movement, calculating reactivity increments.

The reactor coolant system's pressure is kept near a reference value using pressurizer heaters and spray actuation. The control system, a proportional-integral-differential controller, takes into account the real pressure error, the steady state error and the rate of change of pressure deviation.

Two banks of heaters are used to compensate a pressure decrease. One is proportionally actuated and the other is an ON-OFF type.

In the case of a pressure increase, the ALMOD 3W uses a variable area spray valve with the modulating factor proportional to the compensated pressure error.

Two power operated relief valves are also part of the pressure control system. One is actuated by an electric signal coming from the measured pressure. The other is actuated by the compensated pressure signal. As this second mode of actuation will be eliminated, to avoid spurious valve opening, the ALMOD 3W model takes only the first way into account.

A three element controller is used to maintain a programmed steam generator water level as a function of nuclear power by changing the feedwater valve opening. The total error signal is dependent on an error in level and on a mismatch error between steam and feedwater flow. A valve characteristic curve is used in ALMOD 3W to give the feedwater flow correspondent to the valve opening demand (Figure 2).

A three operating mode steam dump system was simulated, introducing one additional steam generator relief valve with a modulated area. In the load rejection mode, the modulating factor is the difference between programmed and actual reactor coolant average temperature. In the plant trip mode, the modulating factor is the difference between average temperature and no-load reference temperature. An additional mode can be selected, setting a desired steam pressure which is used to generate the deviation signal.

Starting from the block transfer functions in the "S" domain and using Laplace inverse transforms, finite difference equations in time domain were written for process variables in the above four control systems.

The original ALMOD routines used to simulate the KWU rod control system and steam generator level control were replaced and pressurizer control was slightly modified. The new version, ALMOD 3W, made almost no change in the original running time nor in

the required computer memory.

CALCULATIONAL RESULTS FOR ANGRA 1

During the startup test phase, several parameters responsible for the dynamic behaviour of the plant are tested and checked out against their previously designed values. With a detailed monitoring of plant variables, transient conditions are initiated and adjustments are made in time constants, gains and setpoints to assure an optimized and safe performance of the control systems.

These test results are valuable in verifying models of computer programs used in safety analysis, as well as verifying some of the conservative assumptions generally made in this area.

Owing to a delay in the power ascention schedule of Angra 1, up to this time it has been impossible to confront the ALMOD 3W predictions with plant test results at power levels greater than 3%.

Several cases were run[3] for tests at different power levels and the specific results presented were chosen to shown the main features of the simulated control systems. Post-experience calculations will be performed for adequate code tuning.

Ten Percent Load Swing at Thirty Percent Power

With the plant initialy at 30% power and all control systems in automatic mode, the load in electric generator is manually reduced to 20%. When the system achieve a new equilibrium condition, the turbine load is increased to 30% again. In this test, the rod control system is responsible for the load following performance of the plant. Relief and safety valves must stay closed and nuclear power is not expected to undershoot or overshoot too much. Figure 3 shows the time behaviour of some parameters as calculated by ALMOD 3W. The perturbation was introduced as a 10% step variation in the steam flow coming from the steam generator. Various calculations have shown that the peak pressure, either on the primary or on the secondary side, are strongly dependent on the initial recirculation ratio in the steam generator. The recirculation ratio at low power levels is not known in advance and it is one of the most important parameters for transient analysis modelling. The comparisons between calculated and experimental results will be useful to tune the code. The recirculation ratio used for this specific calculation was 5.34. The rod control system is designed in such a way that pratically no undershoot or overshoot was observed. For load reductions greater than 10%, the steam dump would be necessary.

Fifty Percent Load Rejection From Full Power

From a full power equilibrium condition and with the control system in automatic mode, the turbine load is manually reduced to a 50% condition. The steam dump system is responsible for removing the energy stored in the primary system until a new equilibrium condition is established. The system is designed to assure that neither safety injection nor relief or safety valve actuation will occur.

In figure 4, the steam pressure has an initial fast increase due to the sudden restriction in steam flow. After that, when the steam dump starts to modulate, as seen in the steam flow curve, the slope of the steam pressure curve decreases. In around two minutes, all the parameters have achieved the new equilibrium point, except the pressurizer pressure that is in its minimum and starting to increase by the action of the pressurizer heaters.

For a nominal condition, most of the parameters are known and the recirculation ratio in steam generators is approximately 3. The comparisons between experimental and

calculated results for this transient will be useful in checking the overall performance of the code.

Natural Circulation

The plant design's ability to establish a natural circulation flow is verified in the startup test phase, maintaining constant nuclear power at a 3% level and tripping the reactor coolant pumps. The rod control system, on manual, is used to keep the power constant. The steam generator level control is also on manual with the operator maintaining the initial water level. The steam dump is operating in pressure mode, removing the heat of the reactor coolant system. The input variables for control systems in ALMOD 3W were modified to approximate the operator action. In this way, the temperature channel in the rod control system was eliminated and the gain in the power mismatch channel was increased.

The energy removed in the steam generator is extremely sensitive to variations in feedwater flow and temperature, specially at low power when control has to be made manually. The feedwater flow history is not known beforehand and, for ALMOD 3W analysis, an adjusted function had to be searched for, in order to satisfy the condition of constant steam generator level.

A comparison between the ALMOD 3W calculations and the first natural circulation test performed at the plant is presented in figure 5. Due to plant computer loss during the last part of the test, just 800 seconds of printout was available and an inadequate scaling in plant recorders did not permit additional comparisons.

During the test, the pressurizer PORV was actuated twice by the compensated pressure signal, as a result of the time integral of pressure error. After that, the auxiliary spray was mannualy actuated. In the ALMOD 3W model there is no PORV actuated by compensated pressure and the valve opening occured later when the real pressure setpoint was reached. With no auxiliary spray simulated the pressure history could no longer be compared.

In addition to that, the uncertainty of the operator action in keeping the power constant with control rods also caused different nuclear power histories.

Indication of a stable natural circulation flow is the constant ΔT over the core and an indirect measure gave a flow of around 4.5% while the ALMOD 3W calculations gave 2.5%. The reason for this discrepancy was expected since the way of calculating the friction losses is inadequate for low flow conditions. The ALMOD model determines constant friction coeficients from the initial pressure distribution when the pumps are running.

CONCLUSION

The ALMOD 3W has widened the applicability of the original code to predict transients in PWR primary systems. The analysis showed a safe performance for Angra 1 during the startup test phase and demonstrate its ability to establish natural circulation flow as a way to cool the reactor in case of shutdown coincident with loss of offsite power.

Comparisons between calculated and experimental results, or a post-experience calculation, will be useful to calibrate the code for future analysis.

REFERENCES

1. W. FRISCH, et al, ALMOD 3 - Nichtlineares Anlagenmodell zur Simulation von Störfällen in Druckwasserreaktoren Programmbeschreibung. GRS-A-477 (1980).

2. C. T. M. CAMARGO, Primeira Simulação de Acidentes em Angra 1 Usando o Código ALMOD - Relatório CNEN/DR-Nº 95/81, February 1981.

3. C. T. M. CAMARGO, Introdução de Modelos de Sistemas de Controle no Programa ALMOD 3 para a simulação de Testes de Partida da Central de Angra 1 - Relatório CNEN/DR-Nº 102/81, September 1981.

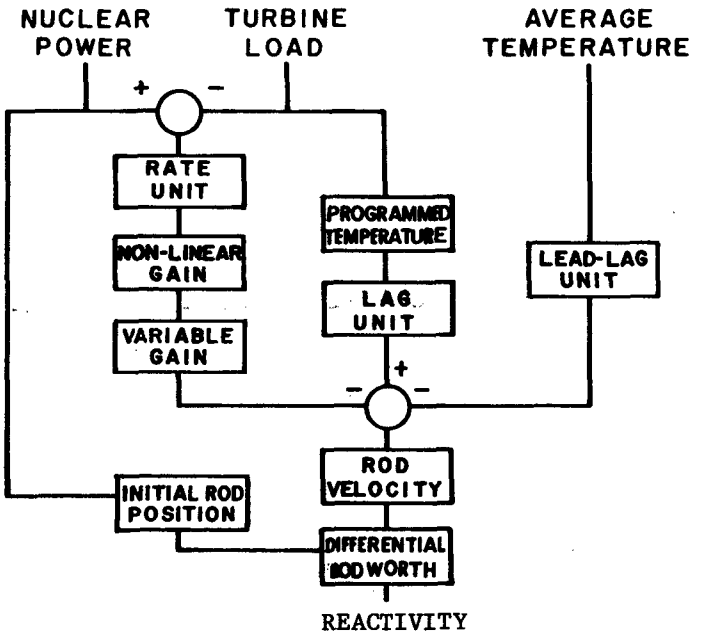


Fig. 1. Rod Control System of ANGRA 1 as Built in ALMOD 3W.

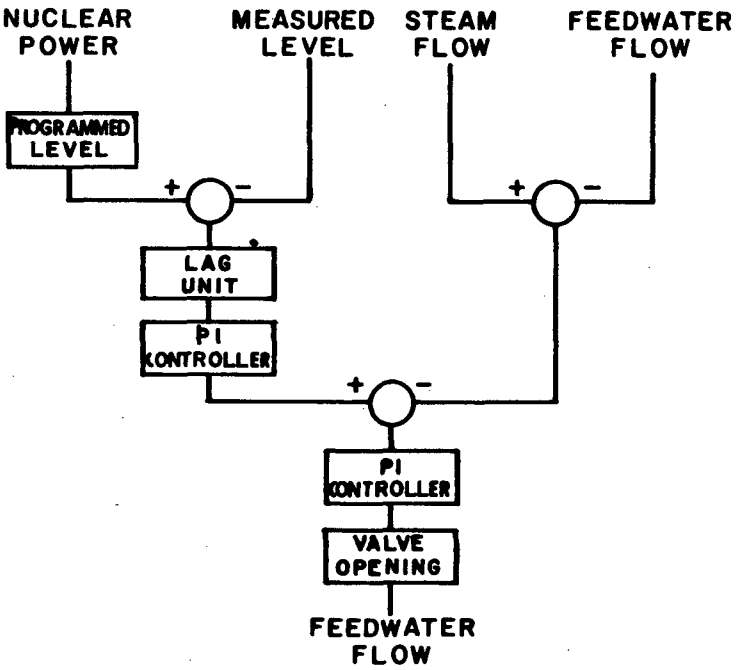


Fig. 2. Steam Generator Water Level Control System of ANGRA 1 as Built in ALMOD 3W.

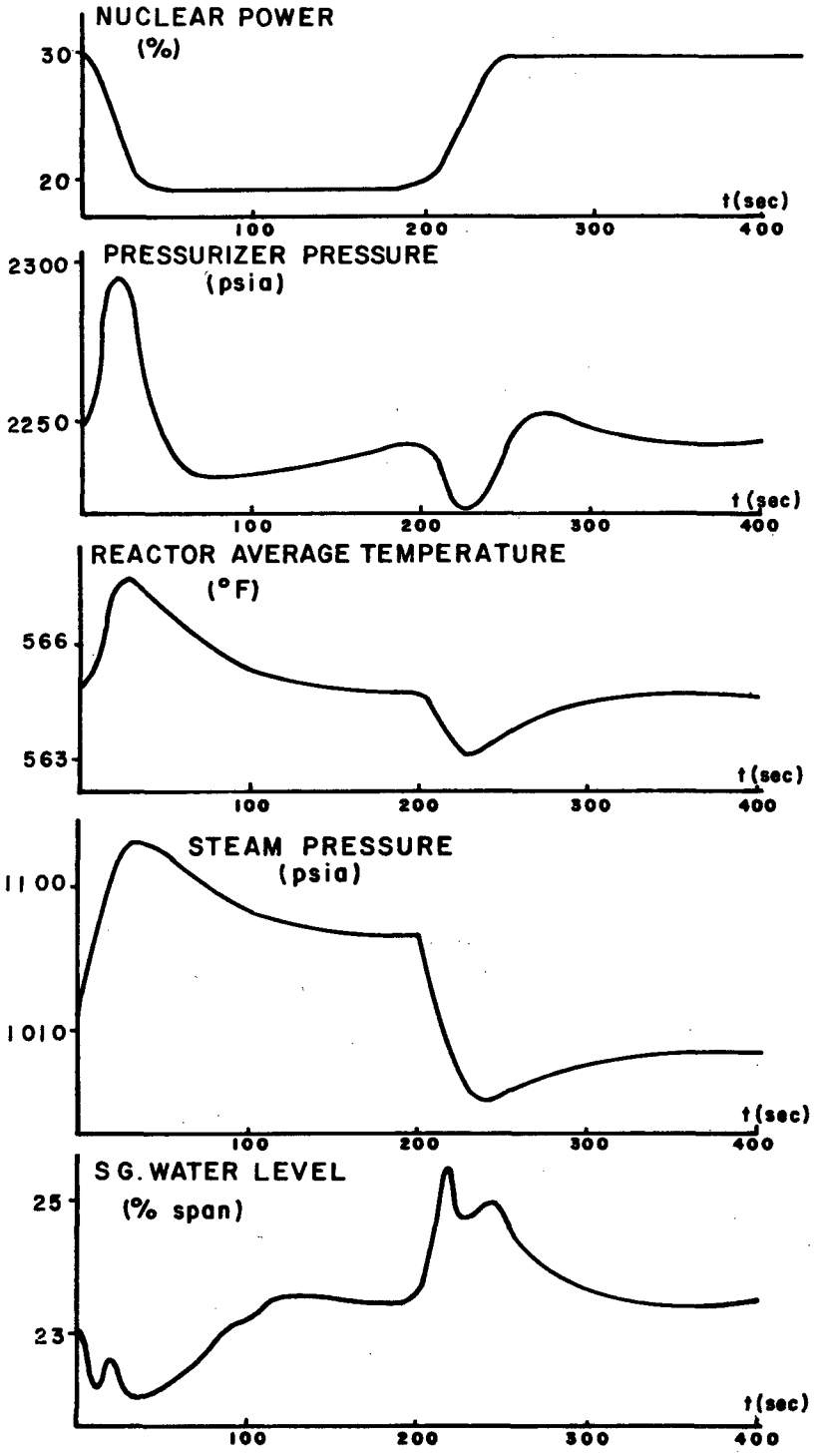


Fig. 3. Ten Percent Load Swing at Thirty Percent Power in ANGRA 1 as Calculated by ALMOD 3W.

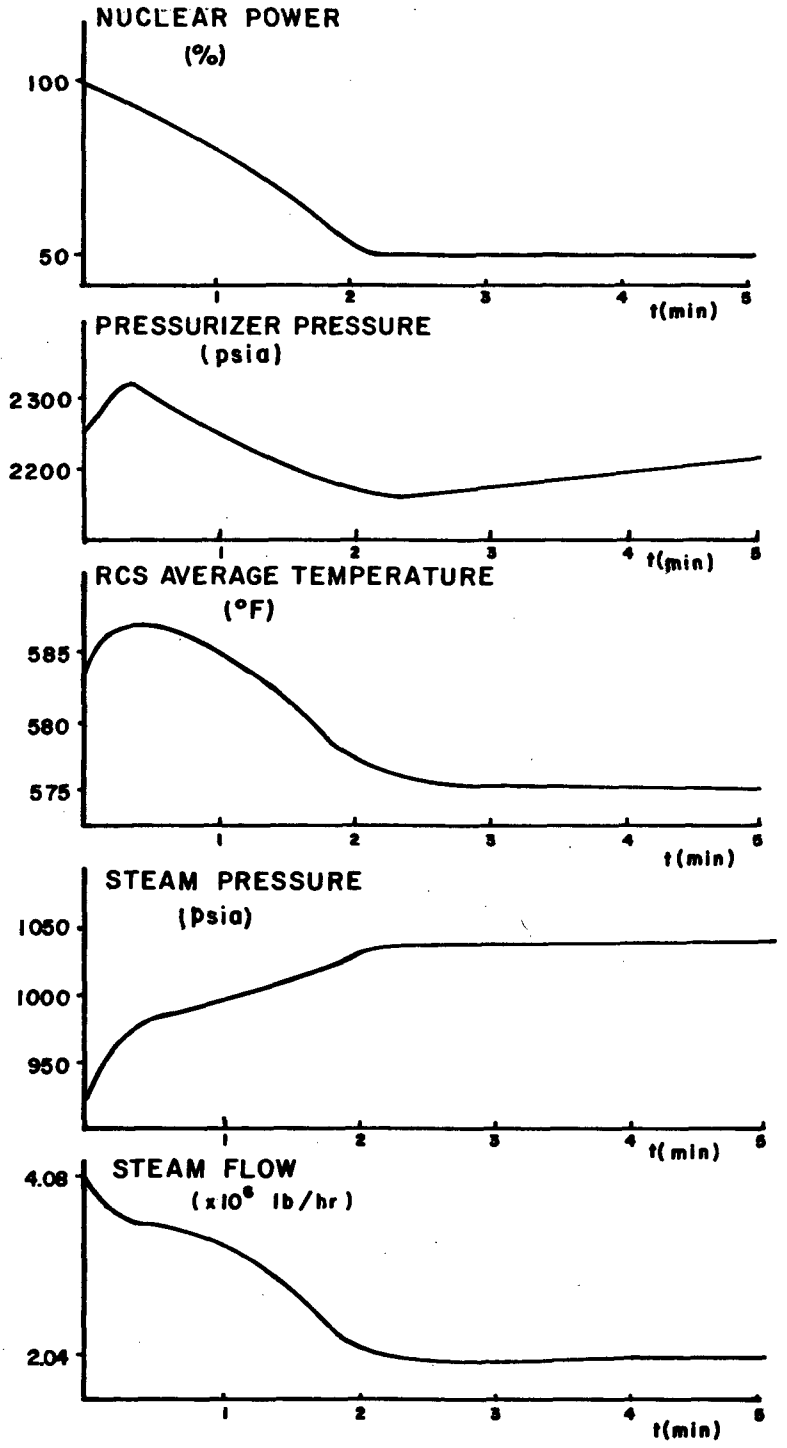


Fig. 4. Fifty Percent Load Reduction from Full Power in ANGRA 1 as Calculated by ALMOD 3W.

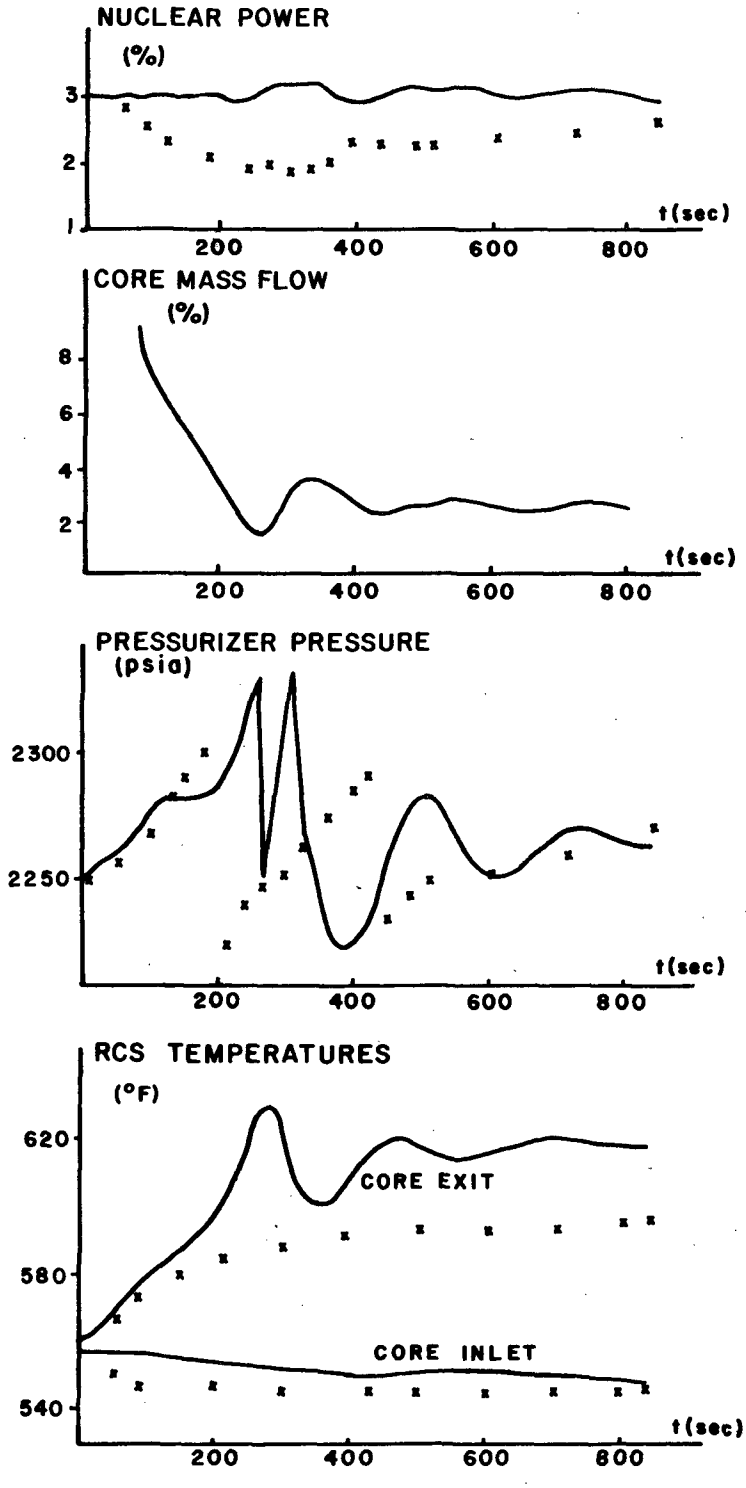


Fig. 5. Comparison between Experimental Results and ALMOD 3W Calculation Test at 3% Power in ANGRA 1.

RETRAN OPERATIONAL TRANSIENT ANALYSIS OF THE BIG ROCK POINT PLANT BOILING WATER REACTOR

George R. Sawtelle, John D. Atchison, and Richard F. Farman, Energy Incorporated, P.O. Box 736, Idaho Falls, Idaho 83402;

David J. VandeWalle and Henry G. Bazydlo, Consumers Power Company, 212 West Michigan Avenue, Jackson, MI 49201.

ABSTRACT

Energy Incorporated used the RETRAN* computer code to model and calculate nine Consumers Power Company Big Rock Point Nuclear Power Plant transients. RETRAN, a best-estimate, one-dimensional, homogeneous-flow thermal-equilibrium code, is applicable to FSAR Chapter 15 transients for Conditions I through IV. The BWR analyses were performed in accordance with USNRC Standard Review Plan criteria and in response to the USNRC Systematic Evaluation Program. The RETRAN Big Rock Point model was verified by comparison to plant startup test data. This paper discusses the unique modeling techniques used in RETRAN to model this steam-drum-type BWR. Transient analyses results are also presented.

INTRODUCTION

Energy Incorporated (EI) used RETRAN -- a computer code developed for the Electric Power Research Institute for calculation of nuclear power plant transient thermal-hydraulic behavior -- to model and analyze Big Rock Point (BRP) nuclear power plant transients. The BRP plant, a boiling water reactor designed by the General Electric Company, is operated by Consumers Power Company. The plant-specific analysis was performed in accordance with U.S. Nuclear Regulatory Commission (USNRC) Standard Review Plan criteria in response to USNRC Systematic Evaluation Program inquiry.

EI performed the analysis with RETRAN using a single, basic input model for nine transients, changing only the boundary conditions to effect each particular transient. This paper discusses the unique techniques used to model the BRP plant and identifies RETRAN's major features which accurately characterize particular designs and make the best use of computer and analyst time.

MODELING

The BRP plant RETRAN model described the thermal-hydraulic system, from the feedwater flow into the steam drum, through the reactor and steam drum, and to the turbine stop valves at the turbine inlet. A geometric nodalization diagram is shown in Fig. 1.

---

* Developed for the Electric Power Research Institute for calculation of power plant thermal-hydraulic behavior. The RETRAN code has undergone extensive validation and is used worldwide.

Unlike modern BWRs, the BRP plant is a steam drum type BWR which consists of a reactor vessel with a two-phase steam interface in the upper plenum and in the steam drum above the reactor vessel. This steam drum BWR design required modeling techniques different from those for more recent BWR designs. The flexibility of the RETRAN code permitted an accurate characterization of this design.

The detailed RETRAN Model (38 volumes, 51 junctions) developed for BRP consists of separate recirculation loops with sufficient nodalization detail to provide a representative response for a broad range of transients, including coastdown to natural circulation. Several of the pertinent model features are discussed below.

The BRP design contains a two-phase to steam interface in the upper plenum and in the steam drum requiring a RETRAN Bubble Rise Separation Model in each region. A "dummy" junction was used in the upper plenum to allow for a steam region above the two-phase mixture region, both within the upper plenum volume. The Temperature Transport Delay (TTD) Model was used in all subcooled regions, including the recirculation loop, lower steam drum volume, and core support tubes in the lower plenum. The TTD model maintains the inventory and transport time of an enthalpy front moving through a volume due to a change in upstream flow rate or fluid enthalpy and mitigates the corresponding effects of numerical mixing. A three-volume average core and a seven-volume hot bundle were included to provide detailed information on the thermal-hydraulic transient response. The hot bundle model was also used for input to the RETRAN auxiliary DNB model which provided the time-dependent DNB ratio. The Steady-State Initialization (SSI) feature was used to provide a consistent set of thermal-hydraulic initial conditions with appropriate fractions of system energy removal by the cleanup and the feedwater-steam line systems.

Steam bypass was proportionally controlled by steam line pressure and featured a quick opening response to a loss of load. Feedwater flow was controlled on feed flow - steam flow mismatch and steam drum liquid level. A block diagram of these control systems is shown in Figs. 2 and 3.

RETRAN trip logic provided reactor scram on any one of several reactor protection system (RPS) signals. The RPS was modeled with a combination of direct, indirect (OR), and coincident (AND) trips. The RETRAN code generalized trip logic allowed for activation of a reactor scram on any of several sensed variables, including high pressure, low level, and high flux. A schematic of the trip logic is shown in Fig. 4.

FEEDWATER TRAIN MODEL

Some transients that involve perturbations in the steam generator feedwater conditions are change in flow or feedwater heater failure. An independent RETRAN model of the feedwater train was constructed to calculate the feedwater enthalpy response to these perturbations. See Fig. 5.

Heat transfer to the heat exchangers was characterized by nonconducting heat transfer surfaces, with the heat transfer rate defined explicitly as a function of time. In the feedwater increase transient, the heat transfer rate was assumed constant in all three exchangers. In the loss-of-feedwater heater transient, the heat transfer to one feedwater heater was conservatively assumed to drop to zero in 0.1 second. The resulting time-dependent feedwater enthalpy for these transients is shown in Figs. 6 and 7.

The utility of using this separate feedwater train model rested in the relative simplicity of the physical description and rapid execution time. The initial checkout analysis was also economical because the problem execution did not carry the overhead costs of the entire reactor coolant system. The total computer time for the 100-second loss of IP heater transient including steady-state initialization was 228 CPU seconds on a CDC 6600.

RETRAN CAPABILITIES

RETRAN* was designed as a best-estimate one-dimensional, homogeneous-flow thermal-equilibrium code with a fairly extensive set of heat transfer correlations and generalized control system models. The code is applicable to a broad range of PWR and BWR transients, including FSAR Chapter 15 transients for Conditions I through IV.

RETRAN's unique steady-state initialization feature allows for a minimum set of flow, enthalpy, and pressure inputs and provides a consistent mass, energy, and momentum distribution within the model. This time-saving feature allows mild operational transients to be analyzed, and permits, if needed, timely analyses of accident situations at different initial conditions. An iterative time-step size option allows the user to specify the numerical accuracy of the transient solution rather than requiring a separate more costly time-step convergency analysis. Additional user-oriented features include convenient and flexible editing including printer plots, re-edit and restart from magnetic tape, and a Calcomp routine for report-quality parameter plots.

RETRAN LIMITATIONS

The major theoretical limitations of RETRAN relative to performing reactor transient analyses are: (1) the requirement (excluding the auxiliary neutron void model) that the phase temperatures are equal for two-phase conditions; (2) the limited nature of the vector momentum model relative to multi-dimensional flow problems; (3) the effects of noncondensible gases on the fluid behavior; and (4) the fact that the quenching process cannot be accounted.

BIG ROCK POINT PLANT MODEL VALIDATION

The RETRAN steady-state initialization (SSI) option was used to produce internally consistent initial conditions throughout the system model at 102% of full power. A minimum set of known parameters was input, from which the SSI option calculated flow rates, enthalpies, and pressure distributions. The code-calculated values were cross-checked against actual plant steady-state conditions. Once the thermal-hydraulic steady-state values were satisfactory, the control systems were initialized to corresponding values. Sensitivity studies provided a reliable SSI convergence criteria with a minimum of iterations, computer time for steady-state initialization was thereby minimized.

A null transient was run for two complete loop transport times to verify that a consistent thermal-hydraulic and control system steady-state initialization was obtained. This simple check can easily reveal inconsistent input.

A validation test was performed for evaluation of the capability of the BRP plant RETRAN model to accurately represent the transient behavior of the primary system. A two-pump trip and coastdown transient was initiated from an intermediate power level at steady-state conditions. The RETRAN-calculated results were compared to recorded data from BRP plant startup tests as shown in Fig. 8. This investigation disclosed several model changes required for a more realistic representation of the BRP plant. After revisions, the results matched the experimental flow coastdown data for the first five seconds of the transient. Because the available plant data did not define the operator actions, the predicted results after five seconds yielded a higher flow value than the test data.

---

* Extensive validation of the RETRAN code is documented in EPRI NP-2175, RETRAN-01 --A Program for One-Dimensional Transient Thermal-Hydraulic Analysis of Complex Fluid Flow Systems, Volume 4, Applications (December 1981).

As a further check on the model, the two-pump trip simulation was then run using an improved version of the code, RETRAN-02 with dynamic slip option. The RETRAN-02 calculation indicated a different initial quality and mass distribution in the two-phase regions as expected. The transient results agreed with the homogeneous flow case of RETRAN-01, and also with the data. The RETRAN-02 calculations required considerably less computer time, both for steady-state initialization and for the transient calculation. The 50% reduction in total computer time for steady-state initialization and the transient run was attributed to improved numerics in RETRAN-02.

Later a steam line nodalization and time step convergence study was performed on the turbine trip without bypass (TTWOB) transient. This demonstration of convergence contributed to the confidence in the validity of the model.

TRANSIENT ANALYSIS

The transient results for the BRP plant were submitted and accepted by NRC. The results were reasonable and well behaved for the duration of the transient which included the system response for 20 seconds following SCRAM; well beyond the time of MCPR. The extended calculation was performed to show the plant tends toward a safe shutdown condition.

For the several transients performed, the transient time, computer time (CDC 6600 CPU time per second), and ratio of computer to transient times are shown in Table I. All the transients were run using a common base model by changing only the boundary conditions. Because of the completeness of the model and the ease of modifying the RETRAN input, only three man-months was required to run and document 12 transient cases - 9 submittal cases and validation transients. Note that the run times are based on a CDC 6600 computer and hence would require six to ten times less CPU time for a CDC 7600 or equivalent IBM system. The computer time to transient time ratio varies significantly, depending on the severity of the particular transient. A mild transient such as the IPR failure and steam line flow increase run quite rapidly. A startup of an inactive loop and a turbine trip without bypass (very rapid enthalpy and pressure change transients) are more severe and hence require smaller time steps and more computation time.

The computer times shown in Table I include time for steady-state initialization (SSI), a one-second null, the transient run, and 46 printer plots. The steady-state initialization feature required 46.5 CPU seconds and provides a consistent set of initial conditions. The one-second null was a user choice to carefully identify initial values on plots generated from the run. The 46 printer plots generated at the end of each run required 23 CPU seconds computer time. The printer plots allow the analyst to quickly evaluate the results of the transient and are generated at a very reasonable cost.

The RETRAN auxiliary Departure from Nucleate Boiling Ratio (DNBR) model is a side calculation user option. The auxiliary DNBR model was used to qualitatively evaluate the Minimum Critical Power Ratio (MCPR). Table II compares the RETRAN MDNBR and COBRA-IV MCPR predictions. Because the RETRAN DNBR was based on a Janssen-Levy correlation and the COBRA-IV MCPR was based on the XN-2 correlation, the relative MDNBR and MCPR values do not correlate. However, the time of occurrence of the minimum values agree very well. A known major difference in the correlations is that Janssen-Levy predicts a higher sensitivity to flow. Since no effort was made to qualify or optimize the DNB model, the differences in results are not surprising. For long-term use, a generalized model with an optimized DNB model could provide relative core performance information for different transients without the necessity for the COBRA analysis for each case.

The above analysis effort required thirteen man-months of labor and ten hours of CDC 6600 CPU time over five calendar months. This effort included the detailed

planning for each transient, converting from a LOCA to a detailed operational transient model, validating the model by comparison to data, running and documenting 12 transients, including a letter report with CALCOMP plots and a microfiche of each computer output.

CONCLUSION

A model of the Big Rock Point system was prepared and several transients performed. RETRAN provided sufficient flexibility to model the steam drum type BWR system and a relatively simple feedwater train. The steady-state initialization and printer plots are two RETRAN features which make for efficient use of analysts' time and allowed the total effort to be completed in five calendar months using only thirteen man-months of labor and ten hours of CDC 6600 CPU time.

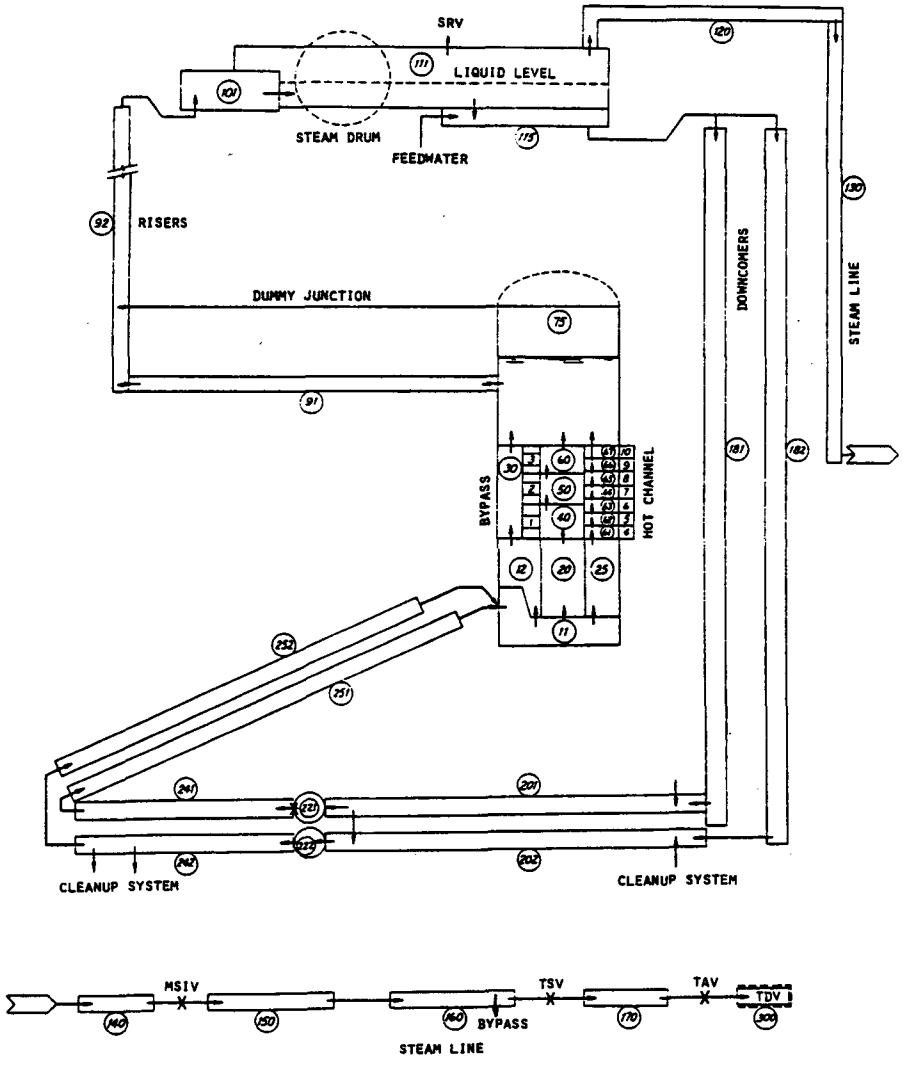


Fig. 1. Nodalization Diagram for Big Rock Point Nuclear Power Plant RETRAN Model

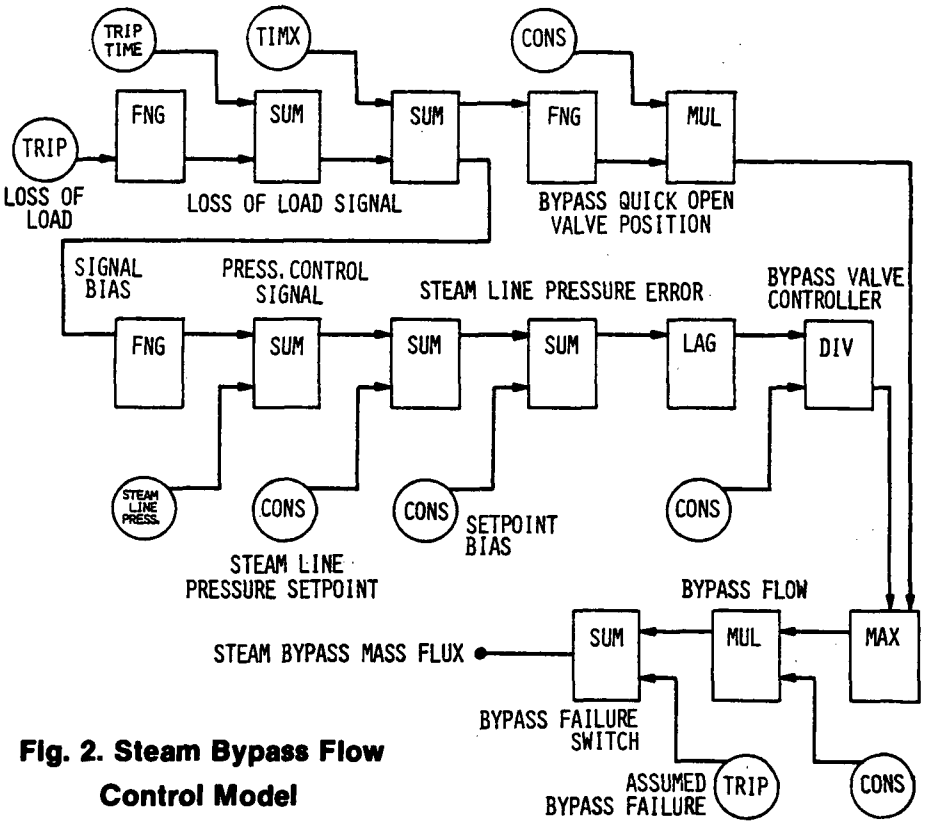


Fig. 2. Steam Bypass Flow Control Model

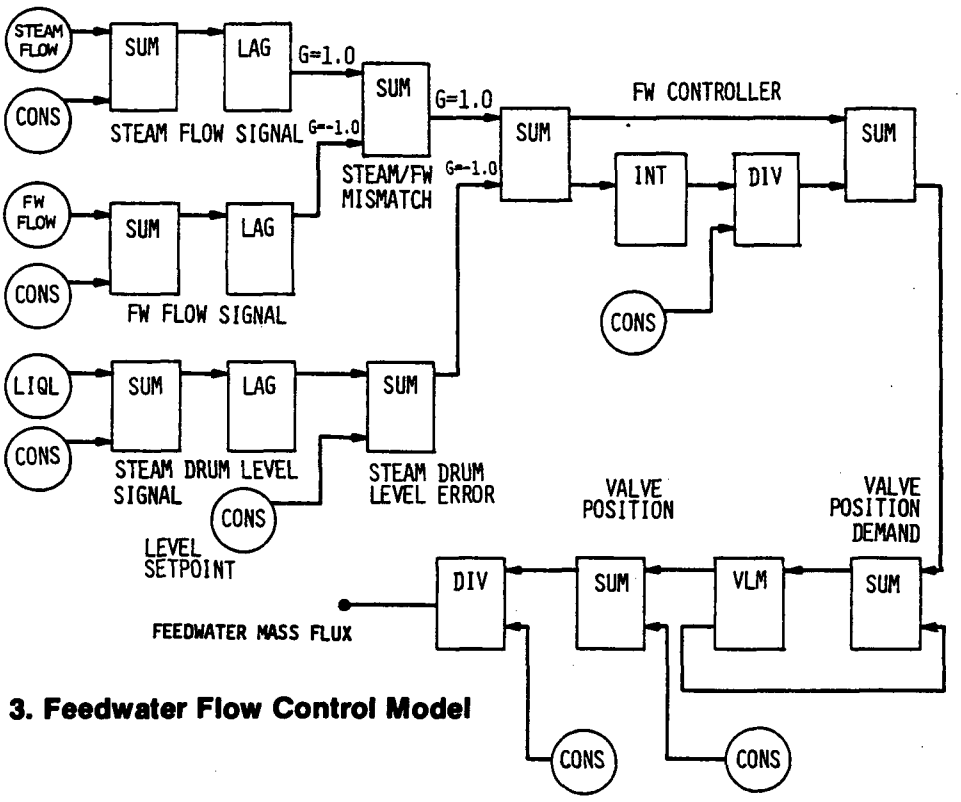


Fig. 3. Feedwater Flow Control Model

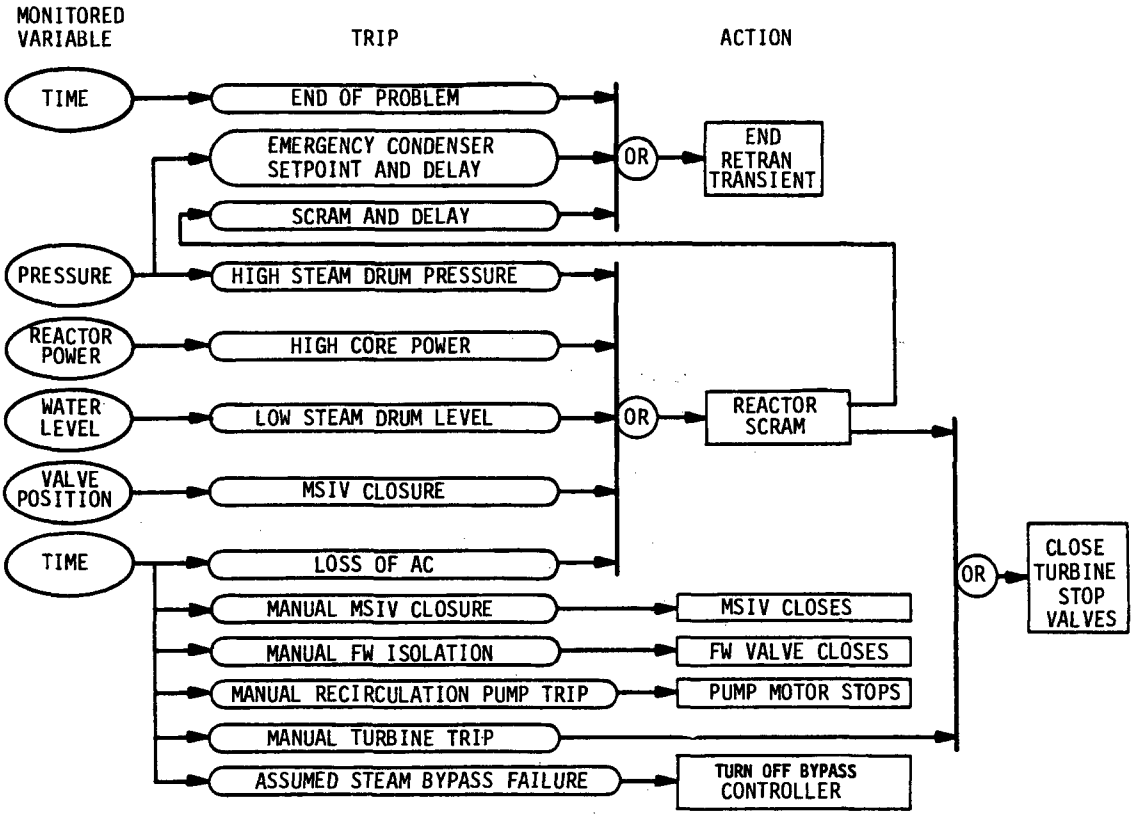


Fig. 4. Big Rock Point Trip Logic Diagram

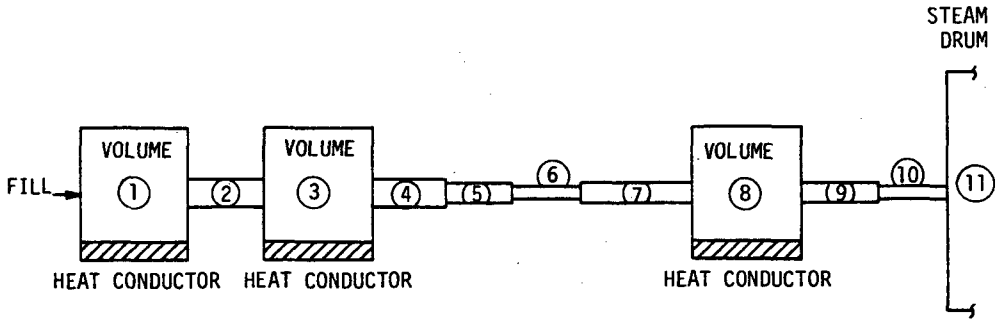


Fig. 5. Big Rock Point Feedwater Train Model

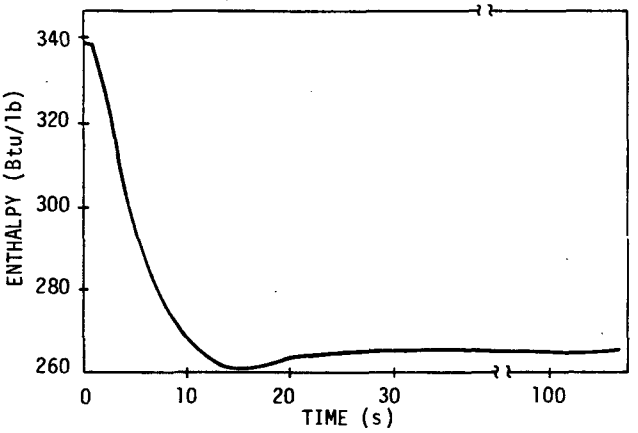


Fig. 6. Feedwater Enthalpy Response to Loss Of IP Heater

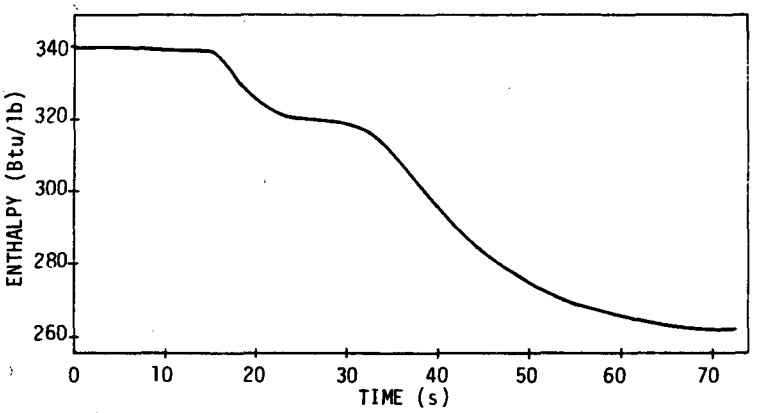


Fig. 7. Feedwater Enthalpy Response To Feedwater Flow Increase

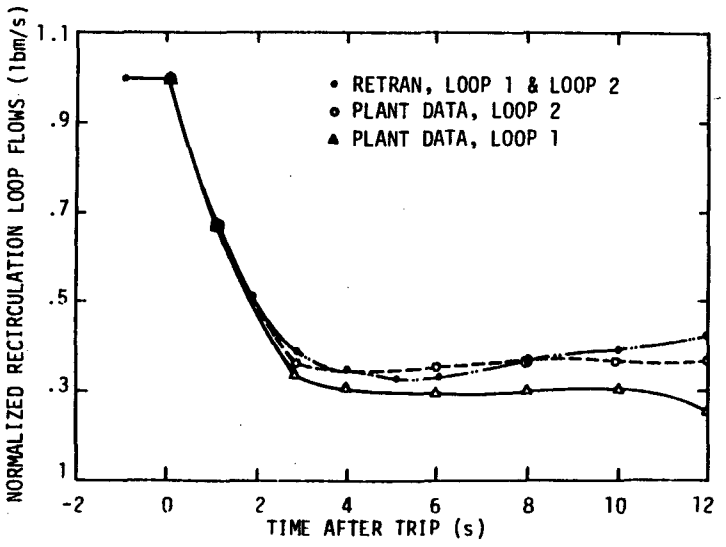


Fig. 8. Two Pump Trip

TABLE I

TRANSIENT TIME VERSUS COMPUTER TIME

TRANSIENT	TRANSIENT TIME (s)	COMPUTER TIME (CDC6600 CPU s)	COMPUTER TIME / TRANSIENT TIME
Loss-of-Feedwater Flow	50	1574	31.5
IPR Failure	60	642	10.7
TTWOB	24	1538	64.1
Steam Line Flow Increase	60	652	10.9
Loss of IP Heater	52	1461	28.1
Feedwater Flow Increase	35	1201	34.3
Loss of HP Heater	60	735	12.2
Two Pump Trip	62	1031	16.6
Loss of Offsite Power	28	1458	52.1
Startup of Inactive Loop	14	2597	185.5
Locked Rotor	30	474	15.8
Null Transient	60	668	11.1

* The computer time includes 46.5 CPU seconds for steady-state initialization, 17.2 s for a 1-s null and 23 CPU s for 46 printer plots.

TABLE II

RETRAN-01 DNBR VERSUS COBRA-IV MCPR

	RETRAN		COBRA-IV	
TRANSIENT	MDNBR(1)	Time (s)	MCPR(2)	Time (s)
Loss of IP Heater	1.20	32.0	1.43	33.0
Increase in Feedwater Flow	1.71	14.55	1.57	15.5
Increase in Steam Flow	2.01	1.75	1.67	1.75
Turbine Trip w/o Bypass	1.15	2.47	1.40	2.4
Loss of Offsite Power	1.53	1.65	1.65	1.4
Loss of Normal Feedwater	1.85	12.75	1.65	12.75
Locked Rotor	0.906	1.0	1.60	1.6
Startup of an Inactive Loop	1.293	9.30	1.77	9.5

(1) RETRAN MDNBR based on Janssen-Levy correlation.
(2) COBRA-IV MCPR based on XN-2 correlation.

TRAC-BD1/MOD1, AN IMPROVED ANALYSIS CODE FOR BOILING WATER REACTOR TRANSIENTS

W. L. Weaver, M. M. Giles
J. D. Milton, C . C. Tsai

Idaho National Engineering Laboratory
Idaho Falls, Idaho 83415, U.S.A.

ABSTRACT

The mission of the TRAC-BD1/MOD1 code has been expanded to provide an analysis capability for not only a large and small break Loss-of-Coolant Accident (LOCA), but also operational transients and anticipated transients without scram in Boiling Water Reactor (BWR) systems and related experimental facilities for which point reactor kinetics are adequate. New models developed to support this expanded mission include a reactivity feedback model, improved void distribution models, and a control systems model. These models are described and results of a generator load rejection transient and a main steamline isolation valve closure transient using these new models are presented.

INTRODUCTION

The TRAC-BWR Code Development Program at the Idaho National Engineering Laboratory (INEL) is developing versions of TRAC to provide the Nuclear Regulatory Commission, and the public, a best estimate capability for the analysis of postulated accidents and transients in BWR systems and related experimental facilities. These codes are based on a developmental version of TRAC supplied to INEL by the Los Alamos National Laboratory containing a two-fluid hydrodynamic model in both one- and three-dimensional flow components. New models required for BWR analysis have been developed by the INEL Code Development group in cooperation with the Code Development group at the General Electric Company.

The development of the TRAC-BWR code has been planned to take place in three major steps. The first step led to the release of TRAC-BD1 [1,2] which provides a basic best estimate capability for large and small break LOCAs. BWR-specific hardware components developed for TRAC-BD1 include: fuel canister, jet pump, separator-dryer, automatic depressurization valve, downcomer water-level trip, and control rod guide tubes. The fuel assembly module provides for the detailed simulation of heat transfer and hydraulic phenomena within a fuel bundle including radiation, quenching and leakage of flow paths. The code also provides the capability to simulate thermal hydraulic phenomena of particular importance in BWR transients: countercurrent flow limiting breakdown, critical flow, upper plenum, emergency core coolant, mass and enthalpy distribution, and boiling transition with flow history.

The second step undertaken in FY-1982 will result in TRAC-BD1/MOD1, which will provide a capability for modeling BWR operational transients including anticipated transient without scram, and other multiple failure events. Although TRAC-BD1/MOD1 will provide a multidimensional capability for modeling thermal hydraulic phenomena in the reactor vessel, point kinetics will be used to determine power response.

TRAC-BD1/MOD1 will possess a controls package and simple balance-of-plant and containment models. Also, improvements identified by the independent assessment of TRAC-BD1 will be made as quickly as schedule and funding permit.

The third and final step is the development of TRAC-BD2. TRAC-BD2 will provide spatial neutron kinetics. Also, any remaining improvements identified by the independent assessment of TRAC-BD1 and TRAC-BD1/MOD1 will be made. TRAC-BD2 then will provide the final, best estimate capability for the analysis of a wide spectrum of transients in BWR systems.

MODEL DEVELOPMENT FOR TRAC-BD1/MOD1

The TRAC-BD1/MOD1 models to be described in this paper include: a reactivity model for the point kinetics neutronic model already contained in TRAC, and a control systems model. In conjunction with the reactivity feedback model, improvements have been made in the prediction of the void distributions so that a more accurate prediction of the void reactivity feedback can be made. These three areas will be discussed separately.

Improved Void Predictions

In a two-fluid hydrodynamic model, the computed void fraction distribution is determined by the wall and interfacial heat transfer and the wall and interfacial friction. Recent modifications in these models include implementation of the Andersen-Ishii interfacial shear model, implementation of a subcooled boiling model, and a direct moderator heating model. The Andersen-Ishii interfacial shear model is based on the drift-flux correlations of Ishii [3]. The equivalent interfacial shear relations were derived by Andersen [4] and are obtained from a static momentum balance. The accuracy of the predicted void distribution using this interfacial shear model is shown in Figure 1, which shows the measured and predicted void distribution in an adiabatic pipe experiment [5] performed at the Centre Information Studi Esperienze Laboratory in Italy. Flows of known quality were generated by a preheater and injected into an adiabatic test section. Quick acting values then isolated the test section, and the void fraction in the test section was obtained by weighing the liquid captured in the test section. Repeated tests were performed at a fixed pressure and mass velocity with varying inlet qualities to generate the void distribution shown. The test results shown in Figure 1 are for a pressure of 50 bars and a mass flux of 388 $kg/m^2/sec$. As can be seen in Figure 1, good agreement between the test data and the predictions using the new interfacial shear model are obtained. Comparisons with the test data at other mass fluxes and pressures are equally good.

The subcooled boiling model implemented into TRAC-BWR is based on Lahey's mechanistic subcooled boiling model [6]. The net void production in subcooled boiling is a result of the competition between void formation at the wall and void collapse due to condensation in the subcooled liquid core. A modification of Lahey's mechanistic subcooled boiling model was used to divide the wall heat flux into a portion which goes into producing vapor directly and the remainder which goes into increasing the sensible heat of the subcooled liquid. The interfacial heat transfer was also modified to compute the rate at which the void created at the wall is condensed by the subcooled liquid. Figure 2 shows the results of the computation of a test in the FRIGG [7] test facility in Sweden using both the subcooled boiling model and the Andersen-Ishii interfacial shear model. The FRIGG test facility is a natural circulation test loop containing a test section with either a 6 or 36 electrically heated rod bundle. The TRAC simulation modeled only the test section and imposed the measured flow rate as a boundary condition. The agreement between the test data and the TRAC prediction is excellent. Comparisons of computed void distributions have also been made with the data of Christensen [8] and Marchaturre [9], and the results are equally good for these tests [10].

Finally, a direct moderator heating model was developed to model the direct nuclear heating of the fluid. The model adds a void-weighted user input fraction of the neutron and decay power directly into the liquid phase while the remainder is deposited in the fuel rods. This model is needed since the power deposited directly into the moderator creates voids sooner (more promptly) than the power deposited into the fuel rods, which must be conducted from the interior of the fuel rod to the cladding surface before voids may be created. This affects the timing of void creation and the resulting void reactivity feedback.

Reactivity Feedback

A neutronic model is used to compute the reactor power history during an operational transient or an ATWS. TRAC-BD1 contains a point-kinetic neutronic model in which the total reactivity is input in a tabular form. An auxiliary reactivity calculation is needed to generate the reactivity table before TRAC can be used for these types of transients. Great care has to be taken to ensure that the input reactivity table is consistent with the power history and computed hydraulic conditions which resulted from the use of the table. This method is adequate when the major portion of the reactivity comes from control rods which were inserted early in the transient which is typical of the LOCA transients for which TRAC-BD1 was originally designed. In order to more accurately and easily model operational and ATWS transients, a reactivity feedback model [11] was developed to compute the portion of the total reactivity due to changes in the thermal and hydraulic conditions during the transient. The control rod reactivity is still input as a user input table of values.

The model accounts for the reactivity due to changes in fuel temperature (Doppler effect), moderator temperature, void distribution, and soluble boron. The model assumes that the reactor is just critical at the beginning of the transient and computes changes in reactivity using the initial state of the system as the reference state. Each core average property; i.e., fuel temperature, moderator temperature, and void fraction and boron concentration, is computed using either power squared weighting or simple volume averaging. These core average properties are then used to compute the reactivity components using quadratic reactivity coefficient functions. User input or default reactivity coefficient functions may be used. The fuel Doppler reactivity coefficient is a quadratic function of core average void which attempts to compensate for the interference between the Doppler and void reactivity effects. The moderator temperature and void reactivity coefficients are functions of core average moderator temperature and core average void fraction, respectively, while the boron reactivity coefficient is a function of core average moderator density. The total reactivity is the sum of these four reactivity components and the control reactivity computed from the user input table.

This reactivity feedback model was tested by the simulation of the initial phases of an ATWS transient initiated by the inadvertent closure of the main steam isolation valve. The thermal hydraulic model used in the simulation is a simple model of a BWR/6 reactor plant using nominal plant data and is shown in Figure 3. Default reactivity coefficients are used and the simulation was used to demonstrate the validity of the computational method rather than predict the actual transient behavior of a particular reactor plant. The computed relative power history during the transient is shown in Figure 4. The power begins to rise shortly after the main steam isolation valve begins to close at 0.7 sec. The power continues to rise after the valve is fully closed at 1.7 sec and peaks at a relative overpower of approximately 500%. The reactivity history for this transient is shown in Figure 5. The closure of the main steam isolation valve causes an increase in the system pressure. The increased pressure in the system collapses the voids in the reactor core causing a positive reactivity insertion which initiates the transient. As the power increases, the fuel and moderator temperature increase adding negative reactivity to compensate for some of the reactivity due to the void collapse. The increased fuel temperature also begins to create new voids (after a time delay related to the thermal diffusion time constant in the fuel), which

reinserts negative reactivity into the system and terminates the transient. The scenario shown in Figures 4 and 5 is consistent with the accepted scenario for this transient and demonstrates the adequacy of the reactivity feedback model for transients of this type.

Control Systems Model

In the simulation of longer operational transients and for some ATWS transients, the automatic control systems present in a reactor plant may affect the results of transients and must be included in the simulation if accurate results are to be obtained. The control systems model developed for TRAC-BWR is based on a simple functional control block formulation [12]. A control block accepts up to three inputs, either algebraic or logical, performs an algebraic or logical operation on these inputs, and generates a single output. Sixty three (63) types of control blocks are available, such as add, multiply, logical AND, etc., which gives the user great flexibility in modeling any type of control function desired. Simple default controllers are built into the code to assist the user in generating the desired steady state or initial condition for a transient. These default controllers consist of a pressure controller to obtain the desired steam dome pressure, a recirculation pump controller to obtain the desired core flow rate, and a feedwater flow controller to obtain the desired downcomer water level. The default controllers were used to obtain a steady state in the simple system model shown in Figure 3.

A detailed control system representing the Browns Ferry Plant, consisting of 209 control blocks, was used to simulate the generator load rejection transient test performed on the plant. The transient was initiated by a loss of generator load which caused the turbine to speed up. TRAC does not contain a turbine model as yet so the turbine dynamics were modeled using the control system to compute the turbine speed. A failure of the power/load relay in the test disabled the fast closure of the turbine stop valve (TSV), but it did begin to close slowly, and the bypass valve (BPV) began to open rapidly. When the turbine speed reached 110%, the fast closure of the TSV was initiated causing a reactor scram. The pressure increased, causing the safety relief valve (SRV) to open. The water level decreased due to the high steam flow rate, causing the main steam isolation valve (MSIV) to close and the control system increased the feedwater flow to raise the level back up to the set point. Figures 6 through 10 show comparisons between the measured data and the TRAC simulation. Agreement is excellent between the data and the computations, except for the feedwater flow and downcomer level.

Figure 6 shows the very good agreement obtained between the code prediction and reactor power test data. The initial dip in the reactor power is a result of a reactor core pressure decrease which causes an increase in steam voids and a corresponding decrease in reactivity. Increasing core flow causes the void fraction to decrease, thus increasing the power level. The turbine overspeed set point (110%) is reached at 1.54 sec and the control rods are scrammed, thereby making the reactor subcritical with an accompanying rapid drop-off of power.

In Figure 7, the agreement is again seen to be quite good between the predicted and measured steam dome pressures. The TSV fast closure causes a rapid pressure rise such that a SRV opens at 2.86 sec. Also aiding in the pressure reduction is the fact that both the BPV is fully open and the reactor is shutdown; consequently, less steam is being generated. By 7.06 sec, the pressure has decreased sufficiently that the SRV closes. Between 6.38 and 10.0 sec, the MSIV is closing as a result of a low water level trip. As the MSIV closes, the pressure again increases.

Figure 8 indicates that the steam flow out of the reactor vessel is accurately predicted. There is a rapid drop in steam flow when the TSV is closed and the reactor is shutdown (so that less steam is being produced). Between 2.86 and 7.06 sec, the SRV is open and the predicted steamline flow shows a marked increase. A corresponding

increase is not observed in the test data, possibly indicating an overprediction of the SRV flow. The experimental data is somewhat suspect, however, since the steamline flow rate should have gone to zero after ten sec when both SRV and MSIV were closed. To model what appears to be a sensor failure, the simulated flow sensor measurement was constrained by a lower limit of 12.75% to be in better agreement with the Browns Ferry Plant reported data. The simulated actual steam flow rate (now shown here) was unaffected by limiting the sensor value so the thermal hydraulic solution was not affected in any way.

The feedwater system in a BWR plant consists of feedwater heaters, a turbine driven feed pump and associated piping and control valves. The turbine and feedwater heater models being developed for balance-of-plant modeling were not completed at the time that this simulation was performed so that a second order differential equation model was used to represent the dynamics of the feedwater system. The differential equation was solved by the control system model and the resulting feedwater flow rate supplied to the simulation as a boundary condition. As can be seen in Figure 9, the control system simulated response differs from the measured data. No effort was made to "tune" the control system model since mechanistic models are being developed for the simulation of the feedwater system and will be available shortly.

The measured downcomer water level shown in Figure 10 exhibits a periodic oscillatory behavior that is not predicted by the TRAC-BD1/MOD1 thermal hydraulic model. Three explanations have been advanced to account for this "ringing" phenomenon: (1) there is side-to-side sloshing or wave rippling in the annular downcomer, (2) there is manometer-like coupling between the downcomer water level and the reactor core steam voids, and (3) there are sensor line dynamic effects in the differential pressure measurements to calculate the downcomer water level height. An attempt was made to understand the discrepancy between the measured and computed downcomer water level by disabling the feedwater controller and using the measured feedwater flow rate as a boundary condition. The computed downcomer water level did improve slightly, but the periodic oscillatory behavior was not predicted. Further investigation is needed to resolve this discrepancy. The overall agreement between the prediction and the test data is excellent which is very encouraging since no "tuning" of the hydraulic models or controllers was needed to obtain the results shown.

SUMMARY AND CONCLUSIONS

The new models which have been developed for TRAC-BD1/MOD1 allow the application of the code not only to design basic LOCA transients, but also operational and ATWS transients, in which point kinetics are applicable. Comparison of the results of separate effects and systems tests with available data demonstrates the accuracy and validity of these new models. These new models enable the TRAC-BWR code to perform the analysis of the initial phases of operational and ATWS transients. Other models currently under development will allow the long-time behavior of BWRs for operational and ATWS transients to be simulated. These models include a containment model for simulation of the thermal response of a BWR containment, balance-of-plant models for feedwater heaters and turbines, and a one-dimensional neutron kinetics model to improve the prediction of reactor power and account for the strong changes in axial power shape caused by changes in the core void distribution.

REFERENCES

1. J. W. SPORE et al, "TRAC-BD1: An Advanced Best Estimate Computer Program for Boiling Water Reactor Loss-of-Coolant Accident Analysis," Report EGG-2109, NUREG/CR-2178, Idaho National Engineering Laboratory (October 1981).

2. J. W. SPORE et al, "TRAC-BD1 - Transient Reactor Analysis Code for Boiling Water Systems," *Proc. of the Third CSNI Specialists Meeting on Transient Two-Phase Flows*, Pasadena, California (March 23-25, 1981).

3. M. ISHII, "One-Dimensional Drift-Flux Model and Constitutive Equations for Relative Motion Between Phases in Various Two-Phase Flow Regimes," Report ANL-77-74, Argonne National Laboratory (October 1977).

4. J. G. M. ANDERSEN, "Interfacial Shear for Two-Fluid Models," *Trans. Am. Nucl. Soc.* 41, 669-69 (June 1982).

5. G. AGOSTINI, A. ERA, and A. PRENOLI, "Density Measurements of Steam/Water Mixtures Flowing in a Tubular Channel Under Adiabatic and Heated Conditions," Report CISE-4-291 (December 1969).

6. R. T. LAHEY, "A Mechanistic Subcooled Boiling Model," *Proc. of the Sixth Int. Heat Transfer Conference, Vol. 1*, Toronto, Canada (1978).

7. O. NYLUND et al, "FRIGG Loop Project," FRIGG-3, Report ASFA-ATOM, Vasteas, Sweden (1970).

8. H. CHRISTENSEN, "Power-to-Void Functions," Report ANL-6385, Argonne National Laboratory (July 1961).

9. J. F. MARCHATURRE et al, "Natural and Forced-Circulation Boiling Studies," Report ANL-5735, Argonne National Laboratory (May 1960).

10. R. E. PHILLIPS and R. W. SHUMWAY, "TRAC-BWR Heat Transfer: Model Description and Steady State Experimental Assessment," Report WR-CD-82-064, Idaho National Engineering Laboratory (May 1982).

11. C. C. TSAI, "TRAC-BWR Completion Report, Implementation of Reactivity Feedback Model," Report WR-CD-81-049, Idaho National Engineering Laboratory (June 1981).

12. M. M. GILES and J. D. MILTON, "TRAC-BWR Completion Report, TRAC-BD1 Control Systems Model," Report WR-CD-82-056, Idaho National Engineering Laboratory (February 1982).

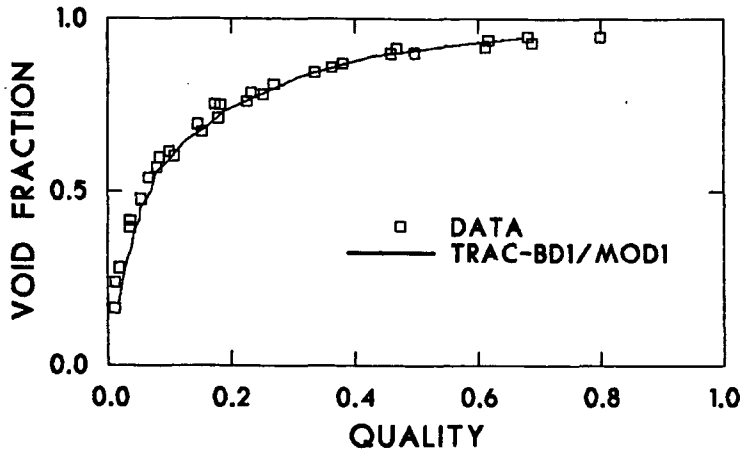


Fig. 1. CISE Adiabatic Void Fraction Test.

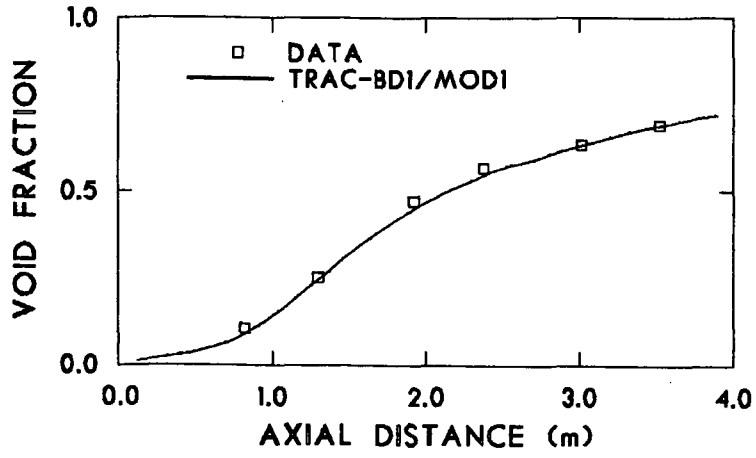


Fig. 2. FRIGG Void Fraction Test.

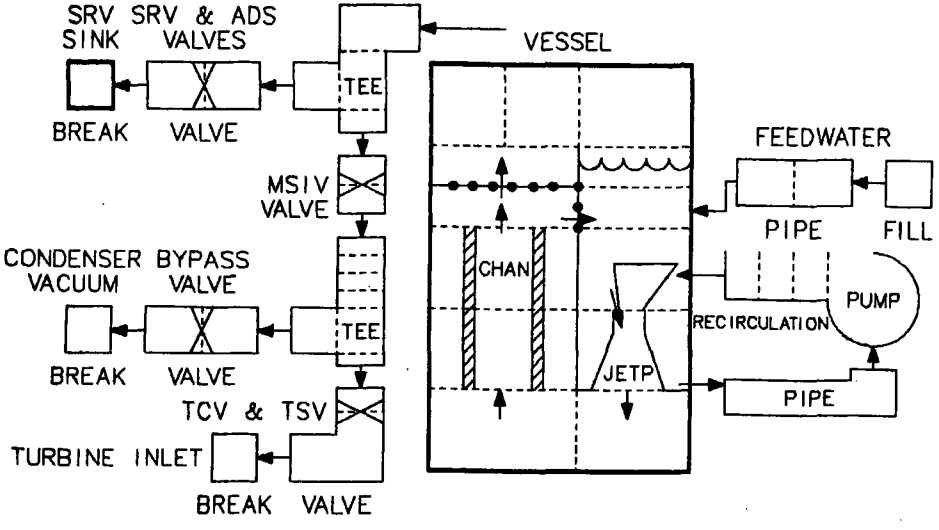


Fig. 3. Thermal Hydraulic Model.

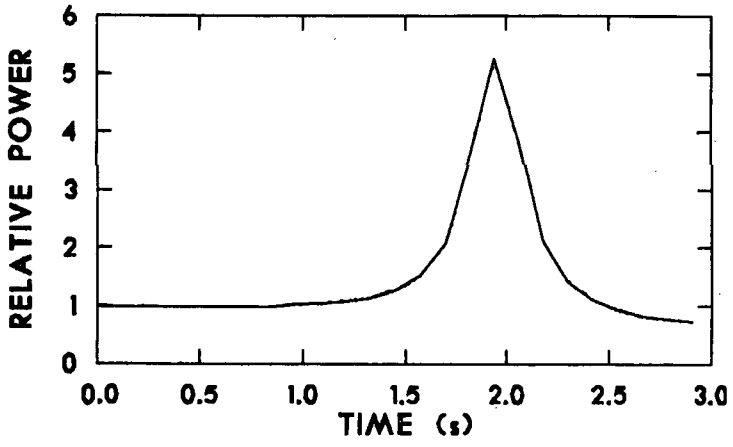


Fig. 4. Relative Reactor Power.

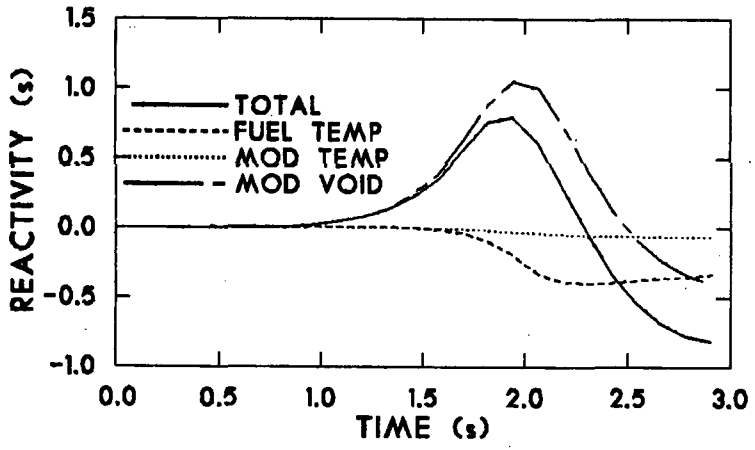


Fig. 5. Reactivity History.

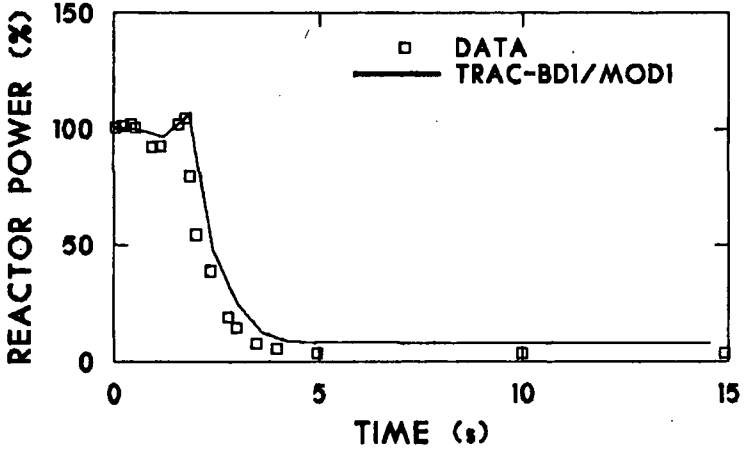


Fig. 6. Reactor Power.

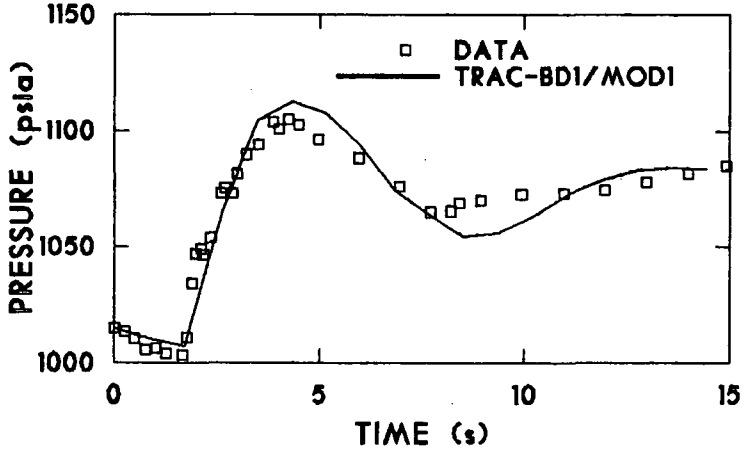


Fig. 7. Steam Dome Pressure.

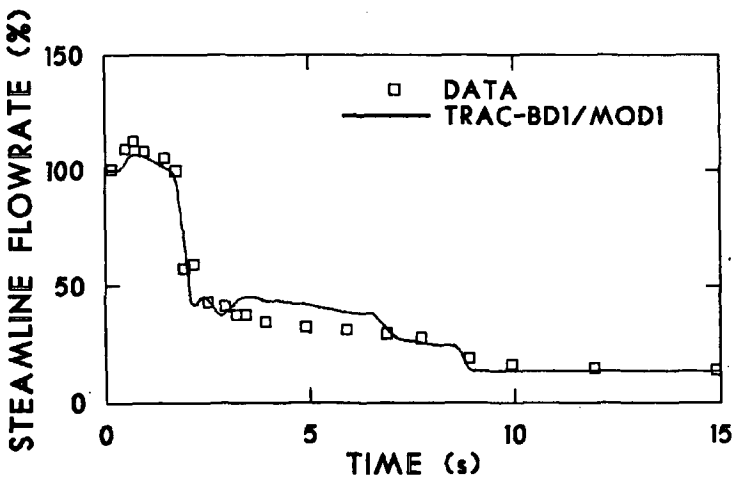


Fig. 8. Steamline Flow Rate.

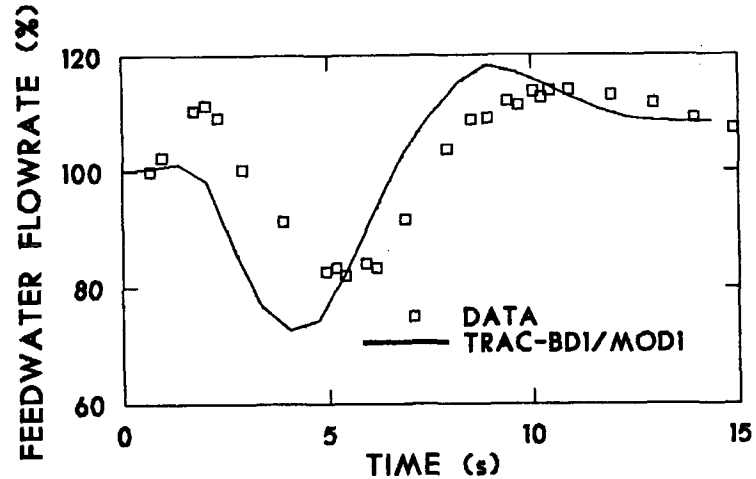


Fig. 9. Feedwater Flow Rate.

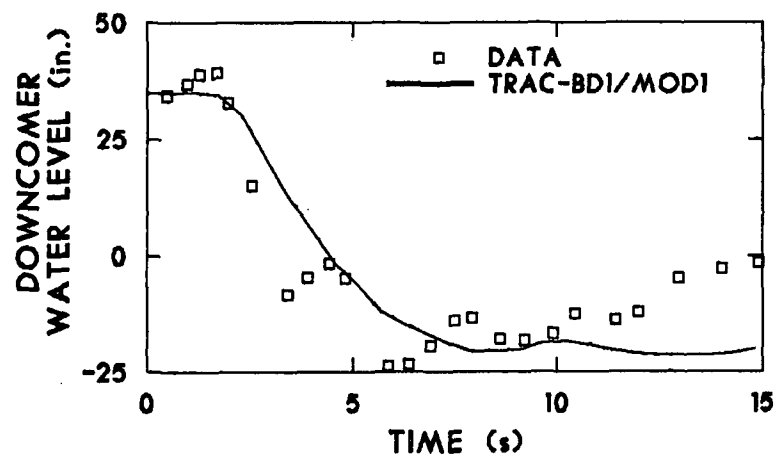


Fig. 10. Downcomer Water Level.

A SYSTEMATIC EVALUATION OF TRANSIENTS IN SWEDISH BWR POWER PLANTS

Kari J. Laakso

AB ASEA-ATOM
S-721 04 Västerås, Sweden

ABSTRACT

In this paper we present a summary of the results and the methods from the first phase of the project "An analysis of steps to be taken in order to reduce the reactor scram frequency" in Swedish BWRs of the ASEA-ATOM design. The present study has been done in close cooperation with the Swedish Nuclear Power Inspectorate and the utilities. The second phase of the study will be completed during 1982. Both phases include a total of five operating nuclear power units with several years of operating experience.

In the results from phase 1 we point out failure/problem areas. Detailed studies of these areas will be carried out as a part of phase 2 with the purpose of reducing the annual reactor scram and turbine trip frequency. During phase 2 of this study we will work out proposals for steps required, e.g. design improvements, and predict their probable effects on transient frequency and on the probability of severe core damage.

The goal of this project is to improve nuclear safety against the background of transients having a dominating effect on the probability of severe reactor core damage [1]. The used and developed methods for analysis and feed back of operating experience and the first results obtained during phase 2 of this study will also be briefly presented in this paper.

RESULTS FROM THIS STUDY

We have to date analysed a total of about 600 transients, of which about 450 are reactor scrams and about 230 turbine trips, some of which also gave rise to reactor scram. The annual distribution of the number of reactor scrams in three of these units is presented in Fig. 1.

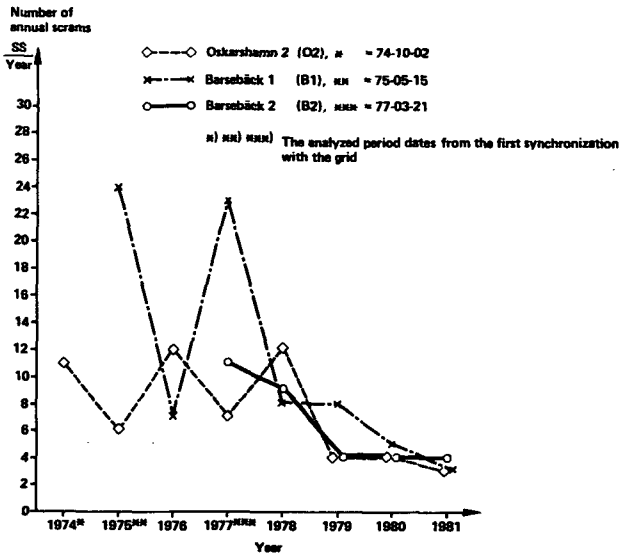


Fig. 1 Comparison of the annual scram frequencies

The mean figure for e.g. the 2nd unit in Oskarshamn is 7,5 scrams per year. The trend for the scram frequency has, however, been decreasing since year 1978 and is 3,7 scrams per year during the later period 1979-1981 for this unit.

A total of about 1100 failure events have been identified as contributing causes to the analyzed transients in the five units.

The failure events, which have contributed to the reactor scrams in the first unit of Oskarshamn, have been broken down into plant parts as shown in Fig. 2.

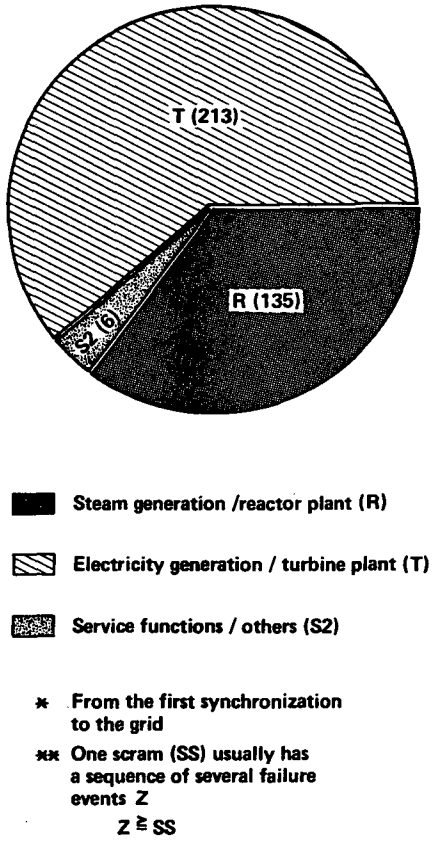


Fig. 2 Oskarshamn 1. Scram analysis*. Breakdown of failure events** into plant parts

As seen in Fig. 2 a large number of failure events, which have contributed to reactor scrams, is to be founded in the turbine plant systems and components [2]. The turbine plants in more recently - started units have also had a significant, though somewhat lower effect on the reactor scram frequency. The turbine plants in ASEA-ATOM BWRs are designed with 100 percent dumping capacity in order to be able to cope with turbine trips and full load rejections without reactor scram. The analysis as shown in Fig. 3 shows that about 50 percent of all turbine trips and generator load rejections have been accomodated without tripping the reactor. Opportunities for improving this percentage in individual units have been identified during the study. Similar design modifications to those, realized in the latest nuclear power units now in commercial operation i.e. TVO I and II (ASEA-ATOM turnkey deliveries in Finland) and Forsmark 1 and 2 in Sweden, can therefore be applied in the earlier units.

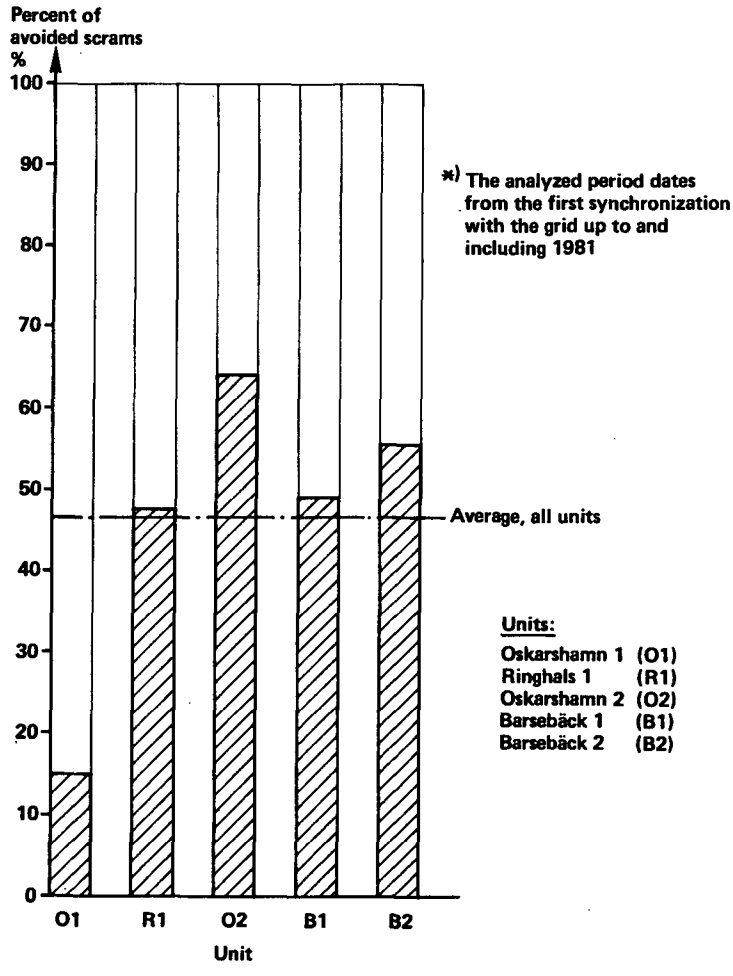


Fig. 3 The proportion of turbine trips and load rejections*, which did not lead to reactor scram

In most of the remaining turbine trips and load rejections scrams have occurred because of system malfunctions and inadvertant protection functions in reactor and turbine plants together with complicated co-operating failure mechanisms.

The results for the second unit in Oskarshamn show that the following problem areas are suitable for study in order to further reduce the scram frequency.

- System malfunction and/or human error in reactor presure control influenced by the turbine control and bypass control valves

- System malfunction, component failure and testing of turbine speed and power control system

- Inadvertant protection function tripped by isolation channels and monitoring sensors

- System malfunction in turbine bypass steam inlets

- Failure events in turbine condenser and vacuum system

- Human error in switching IRM-channels

As pointed out in the study inadvertant reactor core protection functions have considerably affected the frequency of reactor scrams. As shown in Fig. 4 corrective action in this problem area has given a very promising effect. Operating experience and a minor change in the "oversensitive" reactor core protection system have resulted in a total absence of scrams from this particular problem area, compared to an annual average of 3 scrams previously.

As pinpointed in the study the behaviour of the components and process variables [3] in turbine systems have a significant effect on the transient frequency. For example turbine vibrations in the second unit at Oskarshamn have increased the average annual turbine trip frequency by about one turbine trip as seen in the Fig. 5. The shaft geometry of the LP-turbine has therefore been modified in order to reduce the imbalance sensitivity.Since then no transients caused by turbine vibrations have occurred.

Several opportunities for reducing transient frequency in individual units have up to now been identified during the study. Thus different steps for design improvements are recommended for detailed surveys in individual units. Similar design modifications resulted in an improved system performance since being realized and tested in the latest generation of BWRs.

BACKGROUND

The present study is based on follow-up and analysis of Swedish BWR operation experience. The units are of earlier ASEA-ATOM design and they are owned by Swedish utilities. Four of the five turbine plants analyzed are designed by and manufactured by STAL-LAVAL TURBIN AB, three of them in license co-operation with Brown, Boveri & Cie. The first unit, Oskarshamn 1, was synchronized to the power grid in 1971. In this way the study represents an analysis and feedback of a total of 39 years operating experience.

The background to this study is that the probability of severe reactor core damage being caused by transients is much higher than that caused by a postulated LOCA (Loss-of coolant accident). Sufficient reason exists therefore to aim at decreasing the transient frequency even further. Such a reduction of transient frequency would also lead to an increased electricity production and to a reduction of thermally and dynamically induced stresses that may contribute to damage and leakage in components and piping. Some transient events, for instance turbine trips, which do not lead to reactor scrams may, nevertheless, have an effect on nuclear safety. A reduction of such events also contributes to a lower probability of severe core damage.

In the case of the latest BWRs now in commercial operation a systematic approach was taken to reduce the transient frequency. Feedback of operating experience from the earlier units was implemented in the functional analysis and commissioning of the newer units and their systems. Suitable design modifications were introduced as a result of the analysis of commissioning tests and experienced operational disturbances. The resulting design improvements implemented by the vendors (ASEA-ATOM and STAL-LAVAL) have contributed to the fact that the newer units have exhibited a fairly low transient frequency from the start of operation. It is therefore evident that this design and operating know-how can be used to support utilities in reducing the transient frequency in BWRs.

METHODS USED IN THE ANALYSIS

The methodology of the analysis of the occurred transients will be briefly presented in this chapter.

The sequence of the transient events and the failure functions for reactor scrams and turbine trips have been analyzed with the help of event, operating and maintenance reports from the power plants together with analyzed results from both planned and unplanned similar transients reported during commissioning of the most recent BWRs.

To be able to divide the contributing causes into failure types we have defined five failure types, which are shown in Table I.

TABLE I

Failure types

1.	System malfunction - Unsuitable design due to insufficient knowledge of behaviour of process variables - Insufficient capacity - Poor redundancy
2.	Component failure - Component unsuited to the environment - Unreliable component which can be a result of poor preventive maintenance
3.	Inadvertant protection function - Protection function was tripped even though the event had not caused any damage
4.	Testing - Intentional trip due to planned test - Unplanned trip initiated during testing
5.	Human error - Incorrect or unclear operating instructions - Deviations from operating instructions

These failure types are specified so that each one is matched with one type of corrective action required.

The nuclear power unit is very complex and involves several hundred technical subsystems. The original method of system classification is derived from traditional plant design aspects and the present system lists could not be used for this analysis or for transfer of operating experience between different units without further consideration. The units were therefore divided into more suitable functional groups [4] for this study. These groups (Table II) are organized according to their function.

TABLE II
Breakdown of unit into functional groups, an example

T1	Generation of mechanical work/Turbine
T1:01	Steam lines 311 Main steam lines 414 Steam inlet valves (HP-control and stop valves) 432 Turbine bypass
T1:02	HP-turbine 413 HP-turbine
T1:03	Moisture separator/reheater 412 Moisture separator/reheater 414 LP-valves
T1:04	LP-turbine 413 LP-turbine
= =	= =
T1:10	Reactor pressure control 417 Control oil system 461 Turbine power control system
T1:11	Turbine speed and power control 416 Trip oil system 417 Control oil system 418 Power oil system

An example of an (transient) event analysis is shown in Fig. 6. It should be noticed that one transient is usually caused by several co-operating failure events in different functional groups. This means that a sole cause of the actual disturbance sequence cannot usually be identified.

A computer program has been used to store and handle the transient data accumulated during the study. This has facilitated the statistical treatment of the many failure events and identification of their long - term trends and recurring failure events.

We are aware that similar projects concerning analysis and evaluation of operating experience are being performed in USA by e.g. Institute of Nuclear Power Operations, Electric Power Research Institute, the Nuclear Regulatory Commission [5] and by plant vendors and in other parts of the world, too. The Nuclear Safety Board of the Swedish Utilities has started a Swedish ERF-System for Feedback of Operating Experience, where ASEA-ATOM is also contributing.

For the Ringhals 1 unit a probabilistic risk assessment study [6] is available. This study will be applied in calculating how the corrective actions, which will give a reduction of transient frequency, contribute to a reduction of the probability of severe core damage.

Steps in analysis project being developed during phase 1 and still being developed during phase 2 of this study are summarized in Fig. 7.

CONCLUSIONS

One important result is that a systematic analysis of operating experience can be performed and used as a powerful tool for safety improvement work. During the work some new tools for empirical safety and availability analyses have been developed and some improvements have been made to existing methods. These spin-offs can also be applied in other similar studies and in the feedback of operating experience of other production and distribution plants.

The goals for the second phase of this study are to develope new techniques for the analysis and feedback of operating experience and to qualify them by suggesting corrective actions and giving an estimation of the expected reduction of transient frequency and probability of severe reactor core damage.

A strong indication exists, arising from the study, that further reductions in scram frequency can be achieved by relatively modest efforts within the systematically selected problem areas in individual units, e.g. design modifications in reactor and turbine systems.

ACKNOWLEDGEMENT

This study is performed under the auspices of the Swedish Nuclear Power Inspectorate.

REFERENCES

1. Reactor Safety Study, An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants. USNRC Report WASH-1400 (Nureg-75/014).

2. K. J. Laakso, Oskarshamn 1/2 - An analysis of steps to be taken in order to reduce the reactor scram frequency (in Swedish), AB ASEA-ATOM, PM KSD 80-141 (1981).

3. W. Traupel - Thermische Turbomaschinen, 2. Aufl. Springer-Verlag, Berlin/Heidelberg/New York, 1968.

4. Y.G. Rosen, L.N. Nyh - Availability Study of Forsmark 3 Nuclear Power Plant, 1980 Annual Reliability and Maintainability Symposium, San Francisco, Jan 22-24, 1980.

5. Carlyle Michelson - Operational Transient Experience - NRC Perspective, presented at Nuclear Power Reactor Safety Course, Massachusetts Institute of Technology, July 7, 1981.

6. G.A. Ericsson et al - Ringhals 1 Safety Study (in Swedish), AB ASEA-ATOM/Swedish State Power Board, Sweden, 1981.

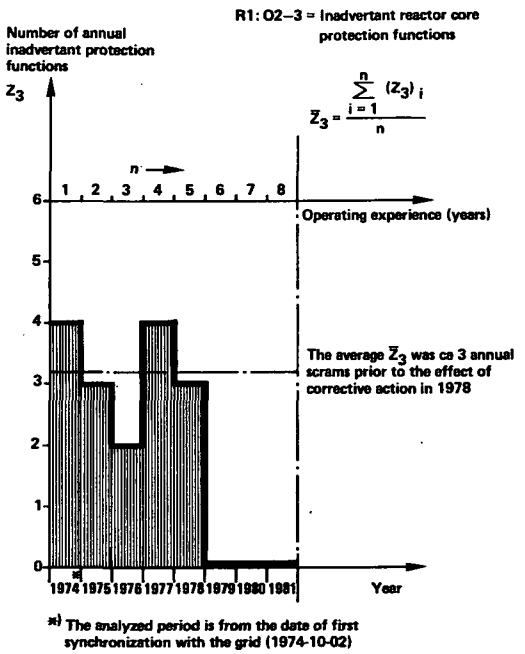


Fig. 4 Unit Oskarshamn 2. The annual frequency of inadvertant reactor core protection functions

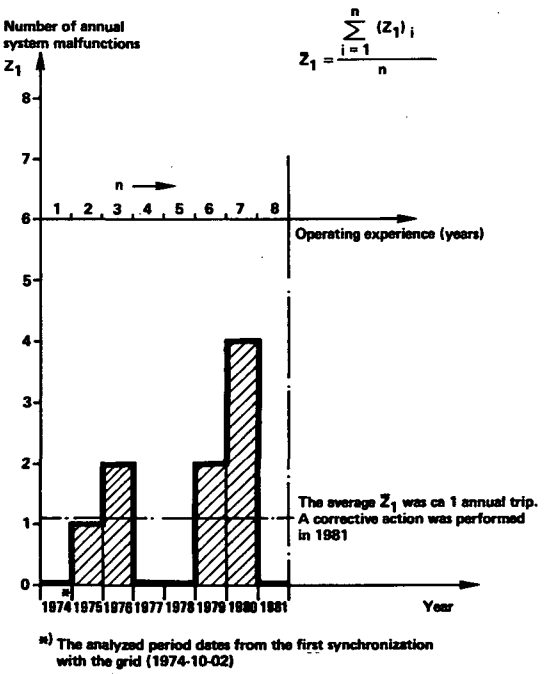


Fig. 5 Unit Oskarshamn 2. The annual frequency of LP-turbine system malfunctions

EVENT ANALYSIS

Date 76-07-14 Time 11.10 SKI No. 2-4/76

Tripping condition TSS, SS10 (Extra high neutronflux relative to core coolant flow)

	Operational data before disturbance	Operational data after disturbance
Operational state	B	
Reactor power (MW_t)	~ 1200	
MC–flow (kg/s)	3100	
Control rod configuration	9160	
Generator power (MW_e)	365	0

Failure events	Functional group	Failure type
1. Inbalance problems occured in the turbine	T1:04	1
2. An attempt was made to counter the vibrations, by increasing the bearing oil temperature, without any success. On reducing the temperature to normal operating level, vibrations increased further leading to turbine trip.	T1:04	4
3. The mismatch of turbine inlet valves and bypass valves caused a pressure transient in reactor tank.	T1:10	1
4. A "very short lived" increase of the neutron flux resulted in tripping of reactor scram (SS10).	R1:02	3

Functional groups: (Function/equipment)

- R1 Steam generation/Reactor
- R2 Containment of radioactivity/PS
- R3 Reactor maintenance/Handling – and storage equipment
- R4 Emergency core cooling/ Safety systems
- R5 Service functions/Others
- T1 Generation of mechanical work/Turbine
- T2 Generation of electricity. 21 kV/ Generator
- T3 Feed water generation 70 bar, 160°C/ Condensate, feed water and pre-heaters
- T4 Gen. at 400 kV, 6 kV/ and auxiliary power
- T5 Service functions/Others
- S1, S2 Service functions/Others

Failure types

1. System malfunction
2. Component failure
3. Inadvertant protection function
4. Testing
5. Human error

Fig. 6 Event analysis. An example

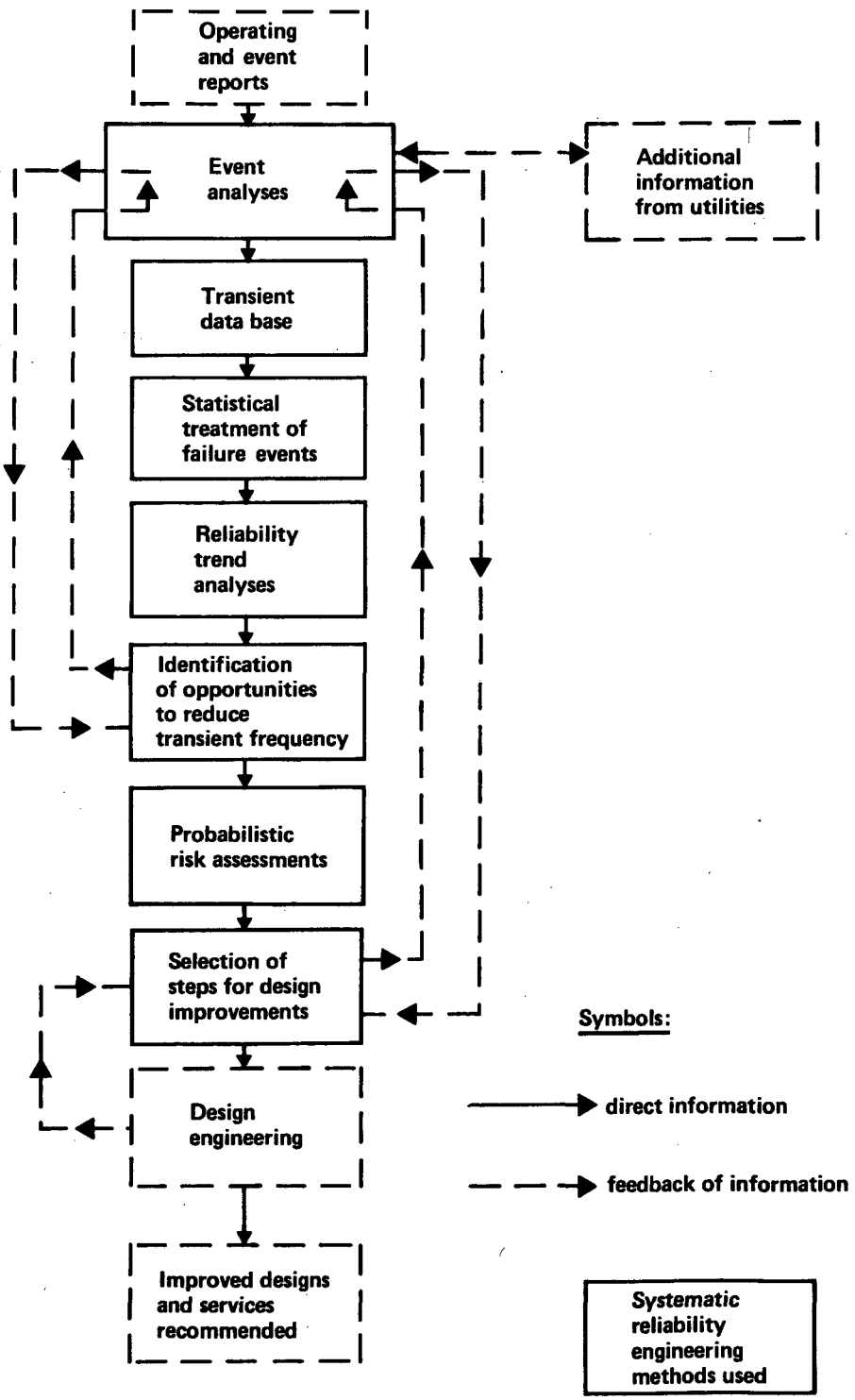


Fig. 7 Steps in the analysis and feedback system of operating experience at plant level

SAFETY-RELATED DYNAMIC RESPONSE MEASUREMENTS ON CEGB REACTORS AT POWER

M. J. Bridge

Central Electricity Generating Board
Berkeley Nuclear Laboratories, Berkeley, Gloucestershire, U.K.

ABSTRACT

An important component of nuclear plant safety cases is a detailed set of fault transient calculations which show that the reactors remain within prescribed limits for all credible faults. This paper reviews measurements of reactor transient response made on the CEGB's reactors during power operation in support of these calculations. The work covered includes both the estimation of reactor parameters, such as reactivity feedback coefficients and trip thermocouple response, and the validation of fault study codes. The significant benefits which have accrued to the CEGB from this work are an improvement in the accuracy of some important data items in the safety calculations and an increased confidence in the theoretical methods which underlie safety cases.

1. INTRODUCTION

The CEGB power reactors are gas cooled, graphite moderated plants either of Magnox type using uranium metal fuel bars clad in magnox alloy cans or AGR (Advanced Gas-Cooled Reactor) in which the UO_2 fuel,clad in stainless steel, is mounted in elements of 36 pins, 8 elements per channel.

During the commissioning of any nuclear plant a major programme of testing is done to ensure that the performance and safety design requirements are met. In addition to these scheduled commissioning tests, various analyses and reactor experiments have been conducted on the CEGB's reactors with the aim of providing particular items of data or verifying certain aspects of reactor response related to safety. It is the latter category of tests on reactors operating at power which is reviewed in this paper.

2. FUEL TEMPERATURE REACTIVITY FEEDBACK IN AGR

The fuel temperature coefficient of reactivity (α_u) in an advanced gas-cooled (AGR) plays an important part in limiting the temperature transient caused by postulated reactivity faults. The temperature coefficient is negative by virtue of the ^{238}U Doppler effect but reduces in magnitude with the build-up of ^{239}Pu during burn-up. Uncertainties in the prediction of these counteracting effects are undesirably large and so a technique was devised for determining experimentally the reactor fuel temperature coefficient on the commercial AGR's. Since the effect of fuel temperature feedback is masked by other reactivity components in steady state situations, dynamic techniques are employed in which control rod bank movements are used to generate power transients and the effect of temperature feedback is deduced from analysis of the measured neutron flux changes. In fact two different types of reactivity perturbation have been used, firstly a simple 'boxcar' reactivity perturbation

by rod bank movement, and secondly a sequence of small amplitude rod bank oscillations.

The boxcar was typically 20 mN reactivity (0.02% in k_{eff}) and of 30 secs duration. The neutron flux was measured by a standard installed fission chamber in a thermal column outside the reactor, the signal being recorded on a purpose-built high speed logger of high resolution. Interpretation of the flux transient to extract the fuel temperature coefficient was achieved by inverse kinetics analysis of the flux to deduce reactivity as a function of time and a calculation of mean fuel temperature using a detailed single channel thermal hydraulics model with input power change equal to the measured flux transient. From a plot of the deduced reactivity against deduced fuel temperature (Fig.1) it can be seen that when the rods are stationary, reactivity varies linearly with temperature over the range of perturbation and the fuel temperature coefficient of reactivity can be deduced from the slope of the line without requiring any knowledge of the reactivity worth of the control rod movement.

The alternative rod oscillation tests took the form of a multifrequency binary sequence of small rod movements imposed manually. Control rod position and neutron flux were measured and the frequency response of flux to control rod movement was found by Fourier analysis. The frequency response depends primarily on reactivity worth of the rod movement and fuel temperature feedback. Since the feedback only affects the low frequency spectrum the reactivity worth of rod movement may be determined by normalising the model to the measured amplitude at high frequency. The reactivity feedback is then obtained by a least squares fit to the measured gain and phase. Results are shown on Fig.2 for two rod oscillation tests at core burn-up of 3100 MWD/Te.

Values of fuel temperature coefficient of reactivity (α_u) obtained by the ramp and oscillation methods are compared with theoretical predictions as a function of core burn-up on Fig.3. The two measurement techniques give consistent results and confirm the predicted magnitude and variation of α_u with burn-up within the one standard deviation uncertainty of about $\pm$0.1 mN/^{o}C. This is to be compared with the previously estimated uncertainty on theory of $\pm$0.3 mN/^{o}C.

These measurements have supported the safety case for start-up reactivity faults in AGR's and avoided the possible need for restrictive protection systems being imposed to accommodate the previously perceived large uncertainties in reactivity feedback.

3. TIME RESPONSE OF OUTLET GAS THERMOCOUPLES IN AGR

Channel gas outlet thermocouples are installed at the outlet of each fuel channel of the AGR's for control and safety purposes. The c.g.o. thermocouples are situated about 5m above the fuel, downstream of the neutron scatter plug, a fairly massive steel structure of irregular shape. The response of c.g.o.'s to channel gas temperature changes is strongly affected by the neutron scatter plug and is difficult to calculate from first principles. The response is therefore determined by rig measurements and has been checked by analysis of temperature transients in instrumented fuel stringers which contain thermocouples near the top of the fuel. Two different types of temperature transient have been used for this analysis; firstly, reactor trip transients in which control rods drop, rapidly reducing reactor power, but gas circulators also trip automatically within a few seconds; and secondly the temperature perturbations caused by the fuel temperature coefficient tests described above.

Analysis of a reactor trip transient is shown on Fig.4 where it can be seen that prediction of c.g.o.temperature, based on the simple empirical model to which rig data was fitted, is poor around the 100 to 200 sec.period, when circulators have run down and are about to restart (at about 200 sec). The reasons for this discrepancy at the very low flow existing ($\sim$3% full flow) are conduction and radiation from

relatively hot and massive steel components to the thermocouple together with inaccuracies in measurement of flow at these low, natural circulation, levels. Additional terms in the model to represent these effects improved the agreement markedly. These terms are not in fact necessary for the high flow conditions under which the thermocouples are used for safety trips.

A typical set of c.g.o. and fuel outlet gas temperature transients arising during the fuel temperature coefficient tests is shown on Fig.5. A three-term empirical model of the following form was fitted to the measured data:

$$H(j\omega) = \frac{1+j\omega n\tau_p}{(1+j\omega\tau_p)(1+j\omega\tau_t)}$$

Fitted values of the parameters τ_t, τ_p and n are shown on Fig.6 for a range of channel flow rate. The error bars were deduced from the fitting procedure. The solid curve represents a least squares fit through the points as a function of flow. Equivalent parameters deduced from rig data and from reactor trip analysis are also shown as a function of flow by dashed and dotted lines respectively.

The different methods of measuring the parameters appear to give significantly different results in terms of model parameters. However, differences in predicted response to a ramp change in temperature characteristic of fault conditions of interest are small after the initial 20 seconds in which the model predictions are just significantly different compared with the fitting errors. Correlation between the fitted parameters is largely responsible for this insensitivity to changes in parameter.

At the conclusion of this study of c.g.o. thermocouple response for AGR's it was possible to be confident that experimental data from several sources were in satisfactory agreement for application to fault studies. The work also demonstrated the importance of a proper account being taken for correlations and showed that a significant reduction in the margin for pessimism could be obtained in some cases if this is done.

4. TIME RESPONSE OF COOLANT THERMOCOUPLES IN MAGNOX REACTORS

Reactor protection against several fault types is provided in the Berkeley Power Station reactors by thermocouples on fuel element cans. The linkages of these thermocouples are prone to failure and, since replacement would be very costly, it was decided to use channel gas outlet thermocouples (c.g.o.'s) for some lines of safety tripping, provided that their time response was adequate. Some early tests indicated that the gas flowing past the outlet thermocouples was not representative of the bulk outlet gas from the channel but was affected, in a rather variable manner, by the surroundings of the pockets in the channel wall in which the thermocouples are situated. Modifications were made, in the form of gas deflector plates, to increase the gas flow past the thermocouples and a means of testing was needed to determine the thermocouple response to channel outlet gas temperature changes and to show their adequacy for safety purposes.

Various methods have been used for measurement of c.g.o. thermocouple frequency response. In early tests control rods were oscillated at different frequencies and the frequency response of the channel outlet gas thermocouples was determined from the amplitude and lags of the gas thermocouples relative to the measured fuel element temperatures. A lengthy experiment was required for these tests and the results showed large variability from channel to channel. A similar but quicker measurement technique achieved by moving a fuel element grab in and out of the reactor near to the channel of interest and Fourier analysing the resulting temperature transients relative to fuel element temperatures also gave results which varied very considerably.

The most consistent results have been obtained from analysis of gas temperature transients following a reactor trip at a scheduled maintenance shutdown. In this test several channels can be tested simultaneously. The c.g.o.thermocouple response has been obtained relative to the calculated gas temperature change at the top of the active core. Measurements of fuel element temperatures have been made during the same tests in order to confirm the theoretical model used to predict gas temperature.

Typical temperature transients following reactor trip are shown on Fig.7 normalised to initial temperature above inlet temperature. Measurements were made on channels with and without deflector plates,the cross-hatched areas indicating the spread of results (one standard deviation). The measured and calculated temperatures were used to derive response parameters in a three-term empirical model (similar to that applied to AGR c.g.o.'s) by means of a least squares fitting procedure. It was found that the individual fitted parameters were sensitive to the way the fitting was done and differed considerably from those deduced by other measurements. This is largely due to the limitations of the empirical model and correlation between the different parameters but does not represent significant differences in c.g.o.response for practical situations. To demonstrate this point the c.g.o.response to a linear ramp in core outlet gas temperature was used as being representative of a typical postulated fault temperature transient. It was possible to show that the empirical model could give essentially identical 'c.g.o.ramp responses' for typical sets of parameters from the different experiments over the complete range of possible fault timescales (>160 seconds) with significant differences only occurring for times <30 seconds.

The derivation of thermocouple responses from the analysis of reactor trip transients has significantly reduced the uncertainty in the thermocouple response parameters at Berkeley Power Station and has enabled these thermocouples to be used in protection circuits without needing to apply large pessimistic allowances for uncertainty which would have led to operationally restrictive trip margins.

5. REACTOR NOISE MEASUREMENTS FOR PARAMETER ESTIMATION

The relationships between fluctuations in temperature, flow and power which naturally occur in a reactor potentially contain useful information on the time response behaviour of the reactor. Some attempts have been made to analyse some inherent reactor noise measurements on the Berkeley Power Station reactors to see if important parameters such as fuel heat transfer and reactivity feedback can be determined by this means.

Measurements of gas and fuel clad temperatures were Fourier analysed to derive a clad to coolant temperature transfer function. A theoretical model was then set up with equations representing neutron flux, fuel,clad and gas temperatures in an average reactor fuel channel. It was realised that the observed transfer function would depend on the position at which the noise enters the system. If there is only one noise source then the observed transfer function can be shown to be independent of its amplitude, but for multiple noise sources their relative amplitudes would need to be known. The effective transfer function was therefore calculated from the model using noise source input to one variable of the model at a time. Theoretical transfer functions corresponding to noise inputs in (1) local coolant temperature, (2) heat transfer coefficient and (3) flow, are compared with the measurements on Fig.8. It can be seen that none of the model predictions agrees well with the measurements and that the type of noise source is important.

To attempt to clarify the type of noise existing in the reactor a comparison has been made of measured and predicted spectra of clad and gas temperature noise. Noise sources were assumed white and were input to inlet gas temperature, heat transfer coefficient, gas flow, and neutron flux. The measured spectra are shown on

Fig.9 with predictions for noise sources in heat transfer and neutron flux. This comparison suggests that noise in heat transfer (or gas flow which gives similar results) could explain the observed high frequency spectrum shape and noise in neutron flux could be responsible for the low frequency noise. Inlet temperature noise is unlikely to be a source since it would give larger temperature noise in coolant than clad, contrary to observation.

It is clear then that the effective transfer function derived from analysis of inherent noise measurements is very dependent on where the noise source occurs. Examination of the gas and clad temperature spectra has not enabled the noise source to be identified positively. Without a better understanding of noise sources it is therefore not possible to use inherent noise to quantify parameters in the theoretical model.

6. DEMONSTRATION OF IMPROVED THERMOCOUPLE RESPONSE

A rather different application of noise analysis of thermocouple signals has been used for determining what improvement in thermocouple frequency response occurs when gas deflectors are installed near the thermocouple pockets in a Magnox reactor. In this case it has been found that the spectrum of inherent noise changes in a systematic manner when the deflector is installed. A measurement of these spectrum changes may therefore be used as a check that the deflectors have achieved the desired improvement in thermocouple response. This is a simple measurement to make, requiring only the c.g.o.thermocouples themselves to be recorded before and after fitting deflectors.

To investigate what changes in inherent noise spectrum occur and how these relate to improvements in frequency response an experiment was made in which inherent noise was measured and also the thermocouple frequency response was determined by the refuelling frequency analysis method (section 4. above). Both measurements were made before and after fitting gas deflectors.

Fig.10 shows a sample extract of inherent noise of four c.g.o.thermocouples and a fuel element thermocouple recorded simultaneously. By inspection there is a clearly larger noise content in the CGO 1 and CGO 2 signals than in CGO 3 and 4. This apparent difference was found to disappear when deflector plates were fitted and thermocouple response was improved as shown earlier. A more quantitative indication of the effect of deflectors is obtained from a comparison of the noise power spectra as shown on Fig.11 for CGO 1. The observed increase in slope of the spectrum when deflectors were fitted was characteristic of all channels tested. The 'good' response achieved with deflector plates resulted in noise power being inversely proportional to the square of the frequency.

The analysis of inherent noise spectrum has thus provided a simple but effective test of thermocouple frequency response improvement.

7. TRANSPORT DELAY MEASUREMENT BY NOISE ANALYSIS

Transport delays between different regions of a reactor can often be identified by cross-correlating noise signals from the different regions. One example of the use of this technique was in determining the relationship between coolant temperature as measured in the outlet gas duct of a Magnox reactor and in-core fuel element temperature measured in the reactor. The transit time of gas from channel exit to duct is only about 2 seconds but the measured lag was found to be very much longer. Heat transfer to the reactor structure is believed to be the cause of the observed long lag. The plausibility of this explanation was confirmed by comparing a model prediction of cross-correlation function with the observations.

The observed cross-correlation between fuel and duct temperatures and autocorrelation of fuel temperature are shown on Fig.12 (solid lines). The theoretical model used was appropriate to flow in a uniform pipe and was characterised by three time constants; reactor structure (τ_s), gas (τ_g) and transit time (τ_t). The theoretical cross-correlation of fuel element and gas duct temperatures was found from numerical integration of

$$\phi_{xy}(t) = \int_0^t h(\tau)\phi_{xx}(t-\tau)d\tau$$

where $h(\tau)$ is the impulse response function and was found analytically from the model. A triangular autocorrelation for fuel temperature was used which approximates to the observed autocorrelation.

The resulting theoretical cross-correlation is shown by dashed lines on Fig.12. This very reasonable fit to the observed cross-correlation function was achieved with plausible time constants in the model, viz: τ_s= 10 sec, τ_g = 0.67 sec, τ_t= 3 sec.

This experiment showed that inherent reactor noise could be used to measure the delay between fuel and duct gas temperature, and in this case it has led to an improved understanding of heat transport in the path from fuel to gas duct.

8. VALIDATION OF COMPUTER CODES

Confidence in the computer codes used for safety calculations is obtained by a variety of checks and tests including rig measurements and code to code comparisons, but reactor transient tests provide further confirmation of the code's ability to correctly model the real plant. The possible range of tests on commercial power plant is limited by economic considerations to normal operational manoeuvres and modest perturbations apart from neutronic tests at essentially zero power. A programme of more severe reactor transient tests has in fact been carried out on the prototype AGR at Windscale at the end of its operating life when the same limitations did not apply but here we describe some analyses of operational transients and tests on the CEGB's commercial AGR and Magnox plant which have assisted in validating three fault study models.

Single Channel Reactor Model for AGR (KINAGRAX)

This code models the neutronic and thermal hydraulic behaviour of a single representative channel in an AGR reactor (containing 8 elements of 36 fuel pins each) and is used for symmetric reactor fault studies.

Two types of large operational transient have been simulated on KINAGRAX and the predicted temperatures and neutron flux compared with measurements. During the commissioning of Hinkley Point 'B' reactor 4 the reactor power transient which accompanied boiler feeding during start-up took place under manual reactor operation and consisted of a fairly rapid increase in power from about 5% to 15% full power over a period of a few minutes. The power rise was initiated by withdrawal of a bank of control rods for about 10 seconds and was terminated by fuel temperature reactivity feedback. Fig.13 shows the measured and predicted power transient. The peak power depends primarily on reactivity insertion and fuel temperature feedback. The theoretical model, normalised by adjusting the reactivity addition to produce the observed power rise, agrees well with the measurement, and the fitted value of control rod reactivity addition agrees with zero power doubling and halving time measurements to within 5%, well within the experimental uncertainty.

Reactor trips cause the largest rapid change in reactor power achievable during normal operation. An analysis of the temperature transient in an instrumented channel resulting from a reactor trip at Hinkley Point AGR is illustrated on Fig.14. The control rods all tripped in, circulators tripped at 10 seconds and ran down to stall at about 100 secs,followed by a period of natural circulation and then restart of some circulators. During the first 40 seconds or so, when the coolant flow is well known from venturi meter measurements, the KINAGRAX prediction agrees closely with measurement. A sensitivity study indicated that this level of agreement implies that errors in the model are less than the equivalent of about 5% in can heat transfer. In the longer term, when gas flow is determined by natural circulation, T_2 is very dependent of the level of flow assumed and the comparison with measurement is dominated by uncertainties in the predicted natural circulation flow. In fact these trip transients analyses can be helpful in checking the flow under these conditions.

Single Channel Reactor Model for Magnox Reactors (KINAX)

Core power oscillations have been observed at certain insertions of auto control rods on one of the Wylfa Magnox reactors. This had been predicted to arise as a result of the non-linear effect of the control system deadband when moderator temperature coefficients became large and positive due to increased fuel irradiation.

To investigate this behaviour an experiment was performed in which oscillations were deliberately induced by switching the auto control system gain to a low setting. Steady oscillations of about 20 minutes period were established within an hour (see Fig.15). Measured temperatures and reactor power etc.(47 parameters in total) were recorded every 20 seconds and were pre-analysed by fitting to a form $ae^{bt}\sin(ct+d)+e+f$.

A theoretical model of the reactor was developed on the basis of the KINAX neutronic and thermal hydraulic model but incorporating a simple 3-term empirical boiler representation and replacing the finite difference axial solution by a modal expansion. In this model the equations were linearised and the whole calculation was set within a minimisation routine so that a selected set of physics parameters could be varied so as to get a best fit model to the observed frequency and relative phases and amplitudes of observed variables.

The resulting fitted parameters, relative to input values, are given in the Table below with the standard deviation uncertainty derived from the fitting process.

TABLE

Parameter	Estimate (relative to input)	σ
Moderator temperature coefficient	1.1	.1
Rod reactivity	1.2	.2
Control gain	1.0	.1
Control dead band	1.0	.1
Graphite conductivity	1.0	.2
Can heat transfer coefficient	0.9	.1
Moderator heat transfer coefficient	1.4	.3

It is seen that this oscillation analysis gave good estimates of seven reactor parameters including a value for the moderator feedback coefficient which, unlike values previously derived from measurement, was independent of assumed values of xenon or rod worth.

Three Dimensional Reactor Models (SKIP and SKAR)

Asymmetric reactivity fault studies require three dimensional modelling of the reactor and its rod control system. The codes used by the CEGB for these studies in Magnox and AGR reactors are SKIP and SKAR. These have both been tested by comparison with control rod runout tests under auto control at power. In Magnox reactors control operates in typically nine independent sectors whereas in the Hinkley B AGR there are 37 independent auto-control rods.

The Magnox reactor tests included a slow withdrawal of rods in one sector leading to about 12% power rise in the sector after 2½ hours. The observed temperature rises and autocontrol rod movements were predicted well by SKIP, generally within about 10% of the change near to the rod. Larger differences were found on the opposite side of the core but these were attributed to fluctuations in inlet temperature which were not modelled in SKIP, and they are of no safety significance. Two faster rod bank faults have been simulated, one involving 24 rods with autocontrol immobilised and the other 4 sector rods. Again the SKIP predictions were found to be an adequate simulation of the reactor behaviour.

On the commercial AGR at Hinkley Point a series of tests on single rod withdrawal were made with full autocontrol on remaining rods and also with adjacent rods immobilised. Two tests have been analysed using the SKAR code and comparisons made with measured gas temperatures and control rod positions. Agreement with measurement was generally good, as shown for example in Fig.16 where the change in gas temperature is shown for two channels adjacent to the moving rod, with all other rods on auto.

The successful interpretation of these rod runout experiments in AGR and Magnox reactors improved confidence in the application of the three dimensional reactor codes to the asymmetric reactivity fault situations which are very similar to the experimental tests performed.

9. CONCLUSIONS

Significant benefit has been derived from dynamic response measurements on the CEGB's reactors during power operation. Of the analyses reviewed here

(a) Fuel temperature coefficient of reactivity measurements on AGR have avoided the need for over-restrictive protection system against reactivity faults.

(b) Coolant thermocouple response measurements have confirmed rig results on AGR in situ increasing the confidence in their application and have enabled coolant thermocouples to be used in place of fuel element thermocouples in protection circuits on a Magnox plant.

(c) Inherent noise in reactor signals has been found to be useful in some determinations of temperature time lags and in verifying improved coolant thermocouple response but it has not been possible to use stable inherent reactor noise signals to deduce parameters in the reactor neutronic and thermal hydraulic model.

(d) Confidence in the validity of fault study codes and data has been enhanced by successful predictions of reactor transients such as start-up, trip, rod runout for Magnox and AGR reactors.

10. ACKNOWLEDGEMENT

The work reviewed here has been performed by a number of different authors. Their assistance and the co-operation of the power station staff is gratefully acknowledged. This paper is published with the permission of the Central Electricity Generating Board.

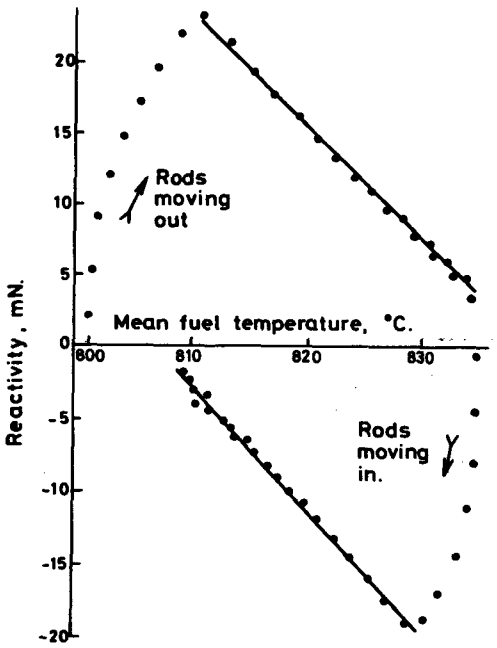


Fig.1 Reactivity Versus Fuel Temperature in AGR Temperature Coefficient Measurement.

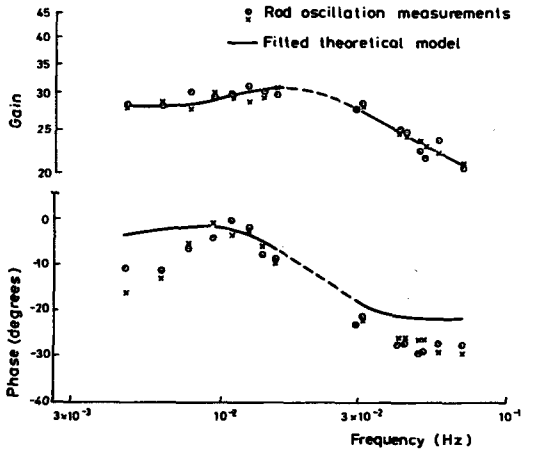


Fig.2 AGR Reactivity to Power Frequency Response Function (∿3100 MWD/Te).

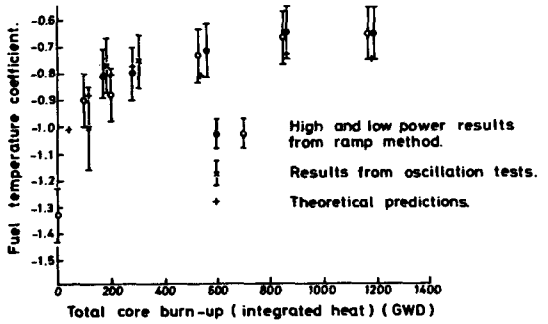


Fig.3 AGR Fuel Temperature Coefficients.

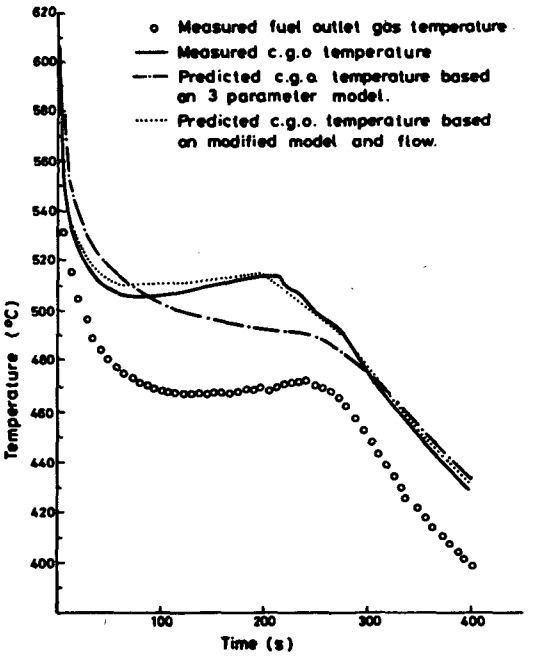


Fig.4 Gas Temperature Transients in AGR Trip from 80% Power.

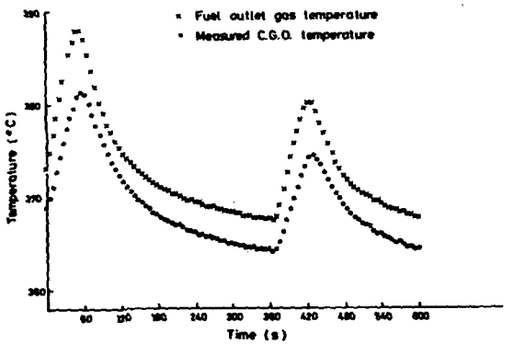


Fig.5 Typical Gas Temperature Transient During Temperature Coefficient Test.

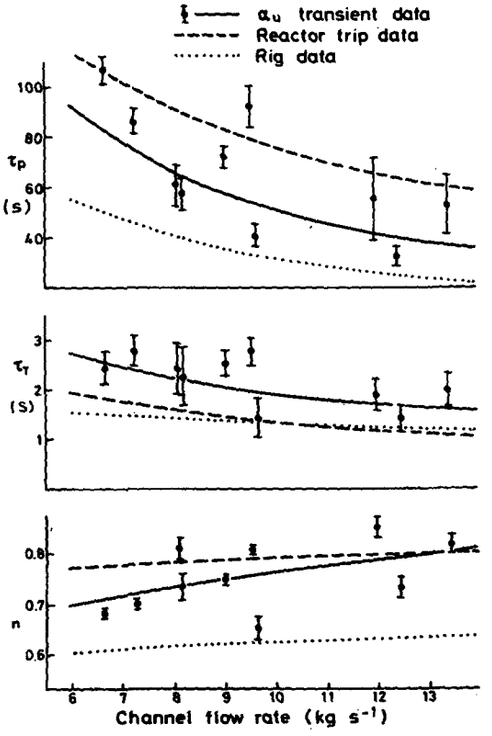


Fig.6 C.G.O. Response Parameters for Hinkley Point 'B" AGR.

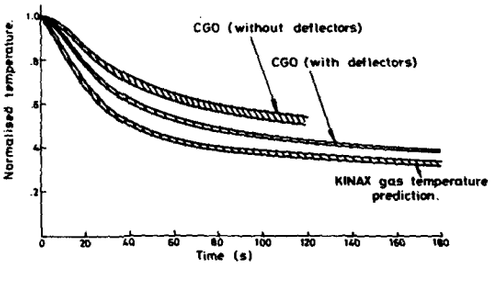


Fig.7 Magnox Reactor CGO Trip Transients.

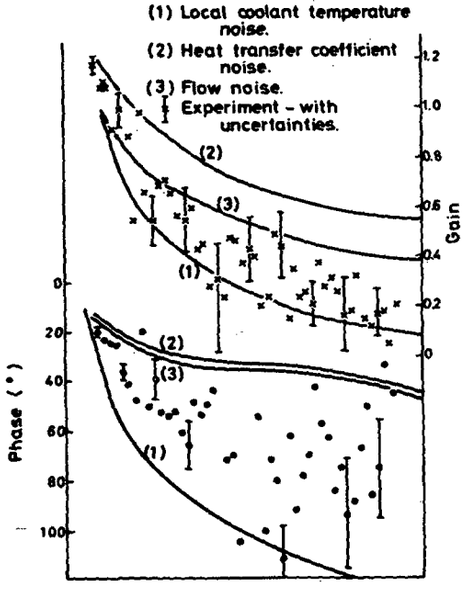


Fig.8 Can to Coolant Transfer Function in a Magnox Reactor.

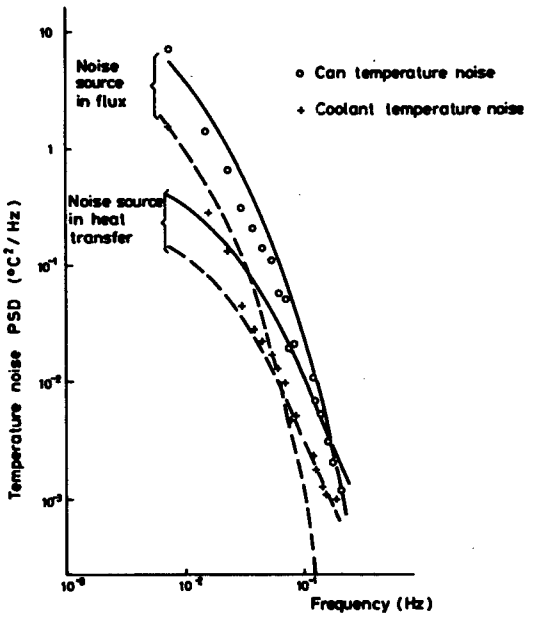


Fig.9 Can and Coolant Temperature Noise Spectra in Magnox Reactor.

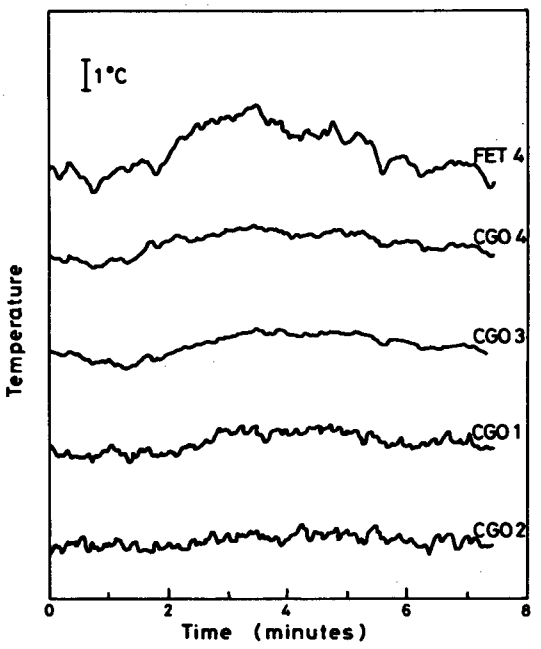


Fig.10 Extract from Inherent Temperature Noise Signals in Magnox Reactor.

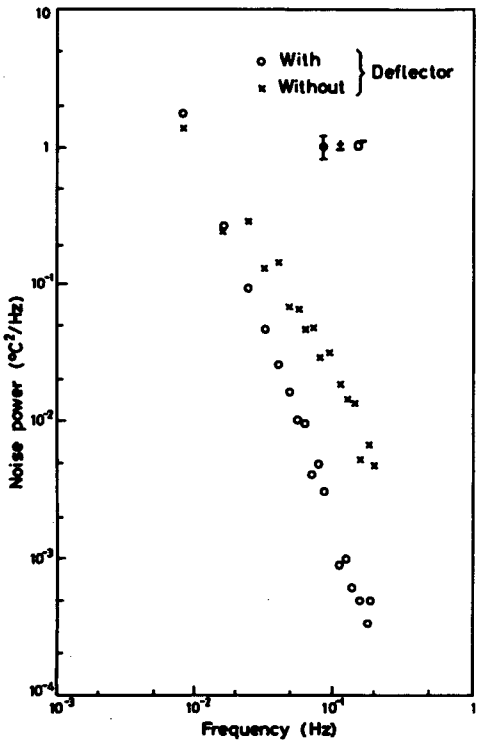


Fig.11 Inherent CGO Noise in Magnox Reactor.

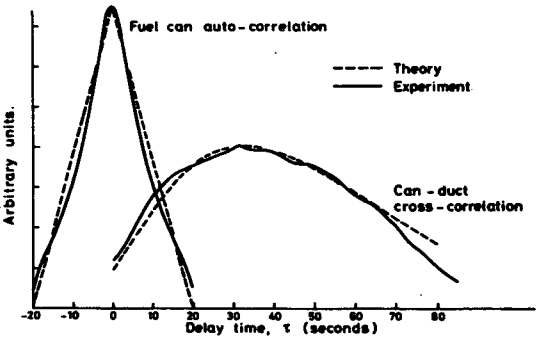


Fig.12 Correlation Functions for Can and Gas Duct Temperatures in a Magnox Reactor.

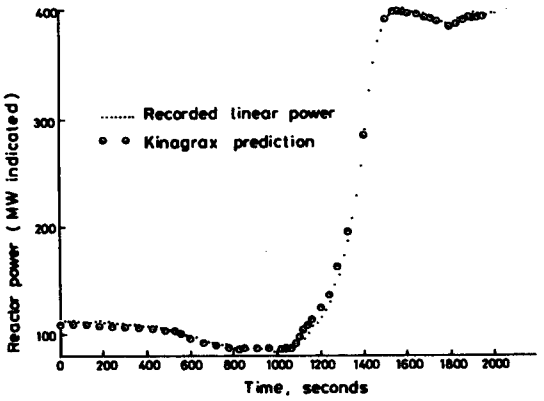


Fig.13 AGR Reactor Start-Up Transient.

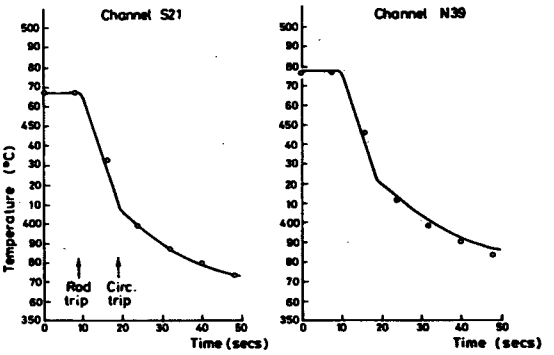
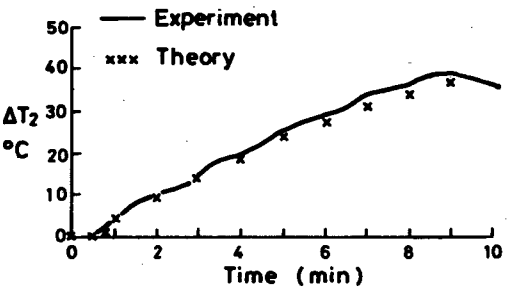
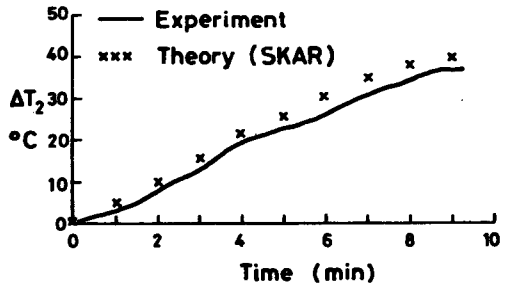


Fig.14 Mean Coolant Outlet Transients in AGR (Short Term).



Channel H 31



Channel H 33

Fig.15 AGR Rod Run-Out Transient Coolant Temperature in Channels Adjacent to Rod.

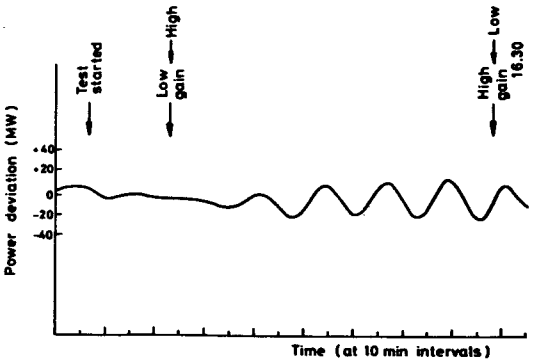


Fig.16 Power Deviation in a Magnox Reactor with Low Auto Control Gain.

RETRAN-02-MOD001 MODELING OF KUOSHENG UNIT 1 TRANSIENT ANALYSES

E. Lin, P. C. Chen, J. K. Hsiue, R. Y. Yuann

Taiwan Power Company
242 Roosevelt Road, Sec. 3, Taipei, Taiwan, R. O. C.

ABSTRACT

Both full power LOAD REJECTION and MSIV(Main Steam Isolation Valves) FULL REACTOR ISOLATION transient tests performed in KUOSHENG UNIT 1 Power Test Scheme were simulated by KUOSHENG RETRAN-02-MOD001 Model. The major transient parameters, such as system pressure, reactor power, reactor water level, feedwater flow and steam flow, were compared with the power test measured data. These measured data were retrieved from plant transient recorder (STARTREC). The results demonstrated that the RETRAN-02 predictions were satisfactory and the modeling can be successfully used as a basis for predicting some further operating transients.

INTRODUCTION

KUOSHENG UNIT 1 is a boiling water reactor (BWR/6), MARK III CONTAINMENT, plant with rated core power of 2894 MW (thermal) and rated core flow of 38.4×10^3 T/hr (2.347×10^4 lb/sec). It has been in commercial operation since December 1981. The KUOSHENG RETRAN-02-MOD001 model was set up to simulate the two planned transient tests (i) Load Rejection (ii) MSIV(Main Steam Isolation Valves) Full Isolation. These two transient tests were performed during the KUOSHENG Power Test Condition 6.

The L/R (Load Rejection) test was initiated by tripping the generator output breaker OCB-3580. The reactor scramed as a result of a sudden load unbalance which caused a fast closure of turbine control valves. Both recirculation pumps tripped to low speed. The reactor pressure rose to peak value of 75.5 kg/cm^2 (1074 psia)which was far below the lowest relief valve setpoint 78.6 kg/cm^2 (1117.7 psia). Reactor water level dipped to a low level but remained above LEVEL 3. Feedwater control system responded properly to secure the low water level.

For MSIVFI (MSIV Full Isolation) test, the isolation was initiated by pulling fuses F6A and F6B in the control room panel. As a result of the isolation, a reactor scram occurred from the RPS limit switches on the MSIV. In addition, the MSIV position switches initiated the main turbine bottle-up system which tripped the main turbine. The recirculation system pump motor power supply was tripped from high frequency (60 HZ) to the low frequency (15 HZ). The water level dipped to LEVEL 2[33.5 cm (1.1 ft) below separator bottom] which initiated RCIC system. The HPCS system was initiated when the water level dipped to 49.1 cm

(1.61 ft) below separator bottom. Two lowest setting 78.6 kg/cm^2 (1117.7 psia) relief valves lifted automatically to control the reactor pressure transients.

Both the two overpressurization transient tests described above were simulated by KUOSHENG RETRAN-02-MOD001 model and results showed almost all the key parameters agreed well with the data retrieved from plant transient recorder (STARTREC). Some discrepancies were found in steam flow transient for L/R simulation and pressure transient for MSIVFI simulation. These two discrepancies were discussed in results section.

MODEL DESCRIPTION

The KUOSHENG RETRAN-02-MOD001 model, as shown in Figure 1, contained 26 control volumes, 31 normal junctions, 4 conductors, 1 pump and 3 positive fills. Almost all geometry data were calculated from plant as-built drawing. Plant system parameters e.g., power, pressure, feedwater flow, main steam flow, recirculation system characteristics, valve curves and scram reactivity curve were collected from FSAR, GE design specifications and power test reports. Table I described the control volumes. The core and bypass flow region were modeled with three vertically stacked control volumes and 1 control volume respectively. The four main steam lines were lumped into one loop. Two recirculation system were also lumped into one loop. Both steam separator interior and exterior were modeled as bubble rise models. Safety relief valves, bypass valves, turbine control valves and MSIV's were modeled as normal junction. The feedwater flow, HPCS and RCIC were modeled as positive fills. The feedwater flow was controlled by a three-element control system as shown in Fig. 2.

RESULTS

1. Load Rejection Case

The key event sequence calculated by RETRAN-02-MOD001 during the first 20 sec were shown in Table II. Also shown for comparison were power test data. The calculated peak pressure 75.5 kg/cm^2 (1074 psia) and time duration (16 sec) for bypass flow reclosing agreed well with the power test data as shown in Table II and Figure 3. The other key parameters' transient, reactor power, water level, feedwater flow and steam flow, were shown on Fig. 4 through 7. The results also agreed well with the data except some discrepancies were found in main steam flow transient. The calculated steam flow was on the average 6% greater than that from measured data. This is due to defect of steam bypass flow modeling.

2. MSIV Full Isolation Case

Table III listed the key event sequence comparison between RETRAN-02-MOD001 results and data during the first 20 sec transient. There existed some difference in the time for water level to reach LEVEL 2 and thus had different RCIC and HPCS initiation time. But the time for dome pressure to reach relief valve lowest setpoint 78.6 kg/cm^2 (1117.7 psia) and the peak pressure were almost the same as shown in Table III and Figure 8. This overpressurization was the major concern in MSIV full isolation transient. Figures 8 through 12 showed the key parameters transients (steam dome pressure, reactor power, water level,

feedwater flow and steam flow) during the first 20 sec. There were some discrepancies for water level and dome pressure transient. However, the other parameters' were very satisfactorily simulated.

The dome pressure transient discripancies resulted from the calculated reverse flow which was caused by sudden closure of MSIV. The dome pressure started to increase continuously when the MSIVFI was initiated. Between t = 5.8 sec and t = 11 sec, the pressure was ceased to rise and oscillate at some low value due to the effect of reverse flow. After t = 11 sec, the reverse flow disappeared and the pressure rise again to the peak value 78.6 kg/cm^2 (1117.7 psia) which caused the two relief valves of lowest setpoint 78.6 kg/cm^2 (1117.7 psia) to lift automatically.

The water level transient in the first 7 sec was somewhat different from data. But the later transients was agreed with data.

CONCLUSION

In general, the results calculated by KUOSHENG RETRAN-02-MOD001 model for both Load Rejection and MSIV Full Isolation transients were agreed with power test data. Based on this, it revealed that RETRAN CODE and KUOSHENG RETRAN-02-MOD001 model provide reasonable simulation of overpressurization transients. This is the beginning of a series analyses planned for KUOSHENG plant. Application to safety analysis and operations support is the goal.

TABLE I

DESCRIPTION OF CONTROL VOLUME

Volume Number	Volume Description
1	Lower plenum
2	Core bottom
3	Core middle
4	Core top
5	Core bypass
6	Upper plenum
7	Stand pipe
8	Steam separator interior
9	Steam separator exterior
10	Dryer
11	Steam dome
12	Lower downcomer
13	Jet pump
14	Recir pump suction
15	Recir pump discharge
16	Main steam line
17	Main steam line
18	Main steam line
19	Main steam line
20	Main steam line header
21	Turbine
22	Bypass header
23	Bypass line
24	Condenser
25	Suppression pool
26	Upper downcomer

TABLE II

COMPARISON OF RESULTS BETWEEN RETRAN-02-MOD001 AND POWER TEST
(LOAD REJECTION TRANSIENT)

POWER TEST	TIME (S)		RETRAN-02-MOD001
Start	0	0	Start
Reactor scram	0.036		
Bypass valve start to open	0.055	0.055	Bypass valve start to open
Turbine control valve start to shut	0.065	0.065	Turbine control valve start to shut
		0.1036	Scram table initiated
		1.4	Normalized reactor power 10%
APRM reads 10%	3.3		
Reactor dome pressure at peak (75.5 kg/cm^2)	3.77	3.8	Reactor dome pressure at peak (75.5 kg/cm^2)
Water level lowest at (36.6 cm) above separator bottom	7 7	9.0	Water level lowest at 42.1 cm above separator bottom
Reactor dome pressure at 66.1 kg/cm^2 BPV start to close	16.2	16.0	Reactor dome pressure at 66.1 kg/cm^2 BPV start to close
		20	END of calculation

TABLE III

COMPARISON OF RESULTS BETWEEN RETRAN-02-MOD001 AND POWER TEST (MSIV FULL ISOLATION TRANSIENTS)

POWER TEST	TIME(S)	RETRAN-02-MOD001
Start	0	0 Start
Reactor scram	0.47	
		0.57 Scram table initiated
Water level reach LEVEL 2 (RCIC initiated)	4.0	
MSIV full isolation	4.53	4.53 MSIV full isolation
HPCS initiated	5.51	
Water level reach lowest level (57.9 cm below separator bottom)	5.75	
		7.5 Water level reach LEVEL 2 (RCIC initiated)
		7.8 HPCS initiated
		8.0 Water level reach lowest level (51.8 cm below separator bottom)
Two lowest setting (78.6 kg/cm^2) relief valve(F051C, F051D) open	17.87	
		18.8 Two lowest setting (78.6 kg/cm^2) relief valves (F051C, F051D) open
		20 END of calculation

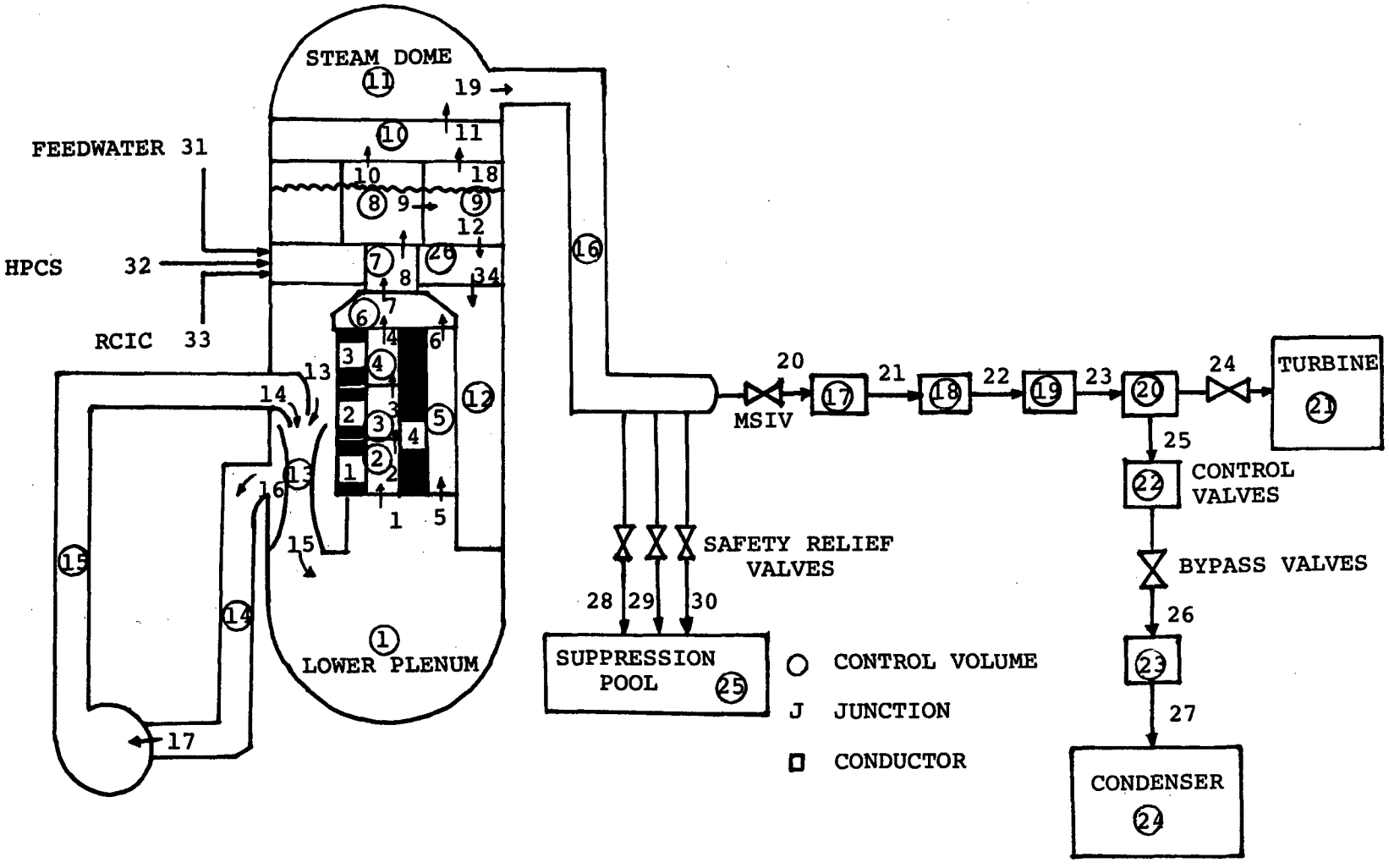


Fig. 1 KUOSHENG RETRAN MODEL

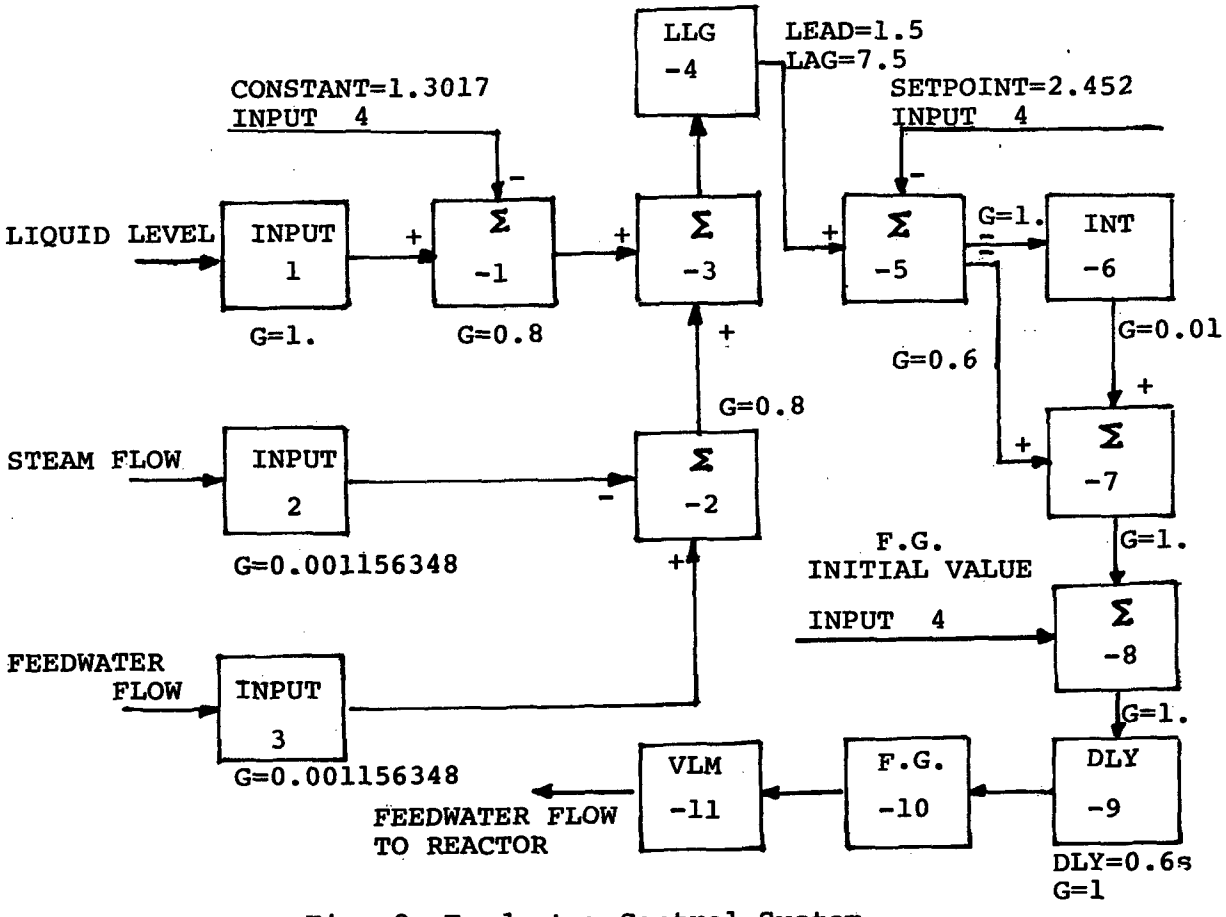


Fig. 2 Feedwater Control System

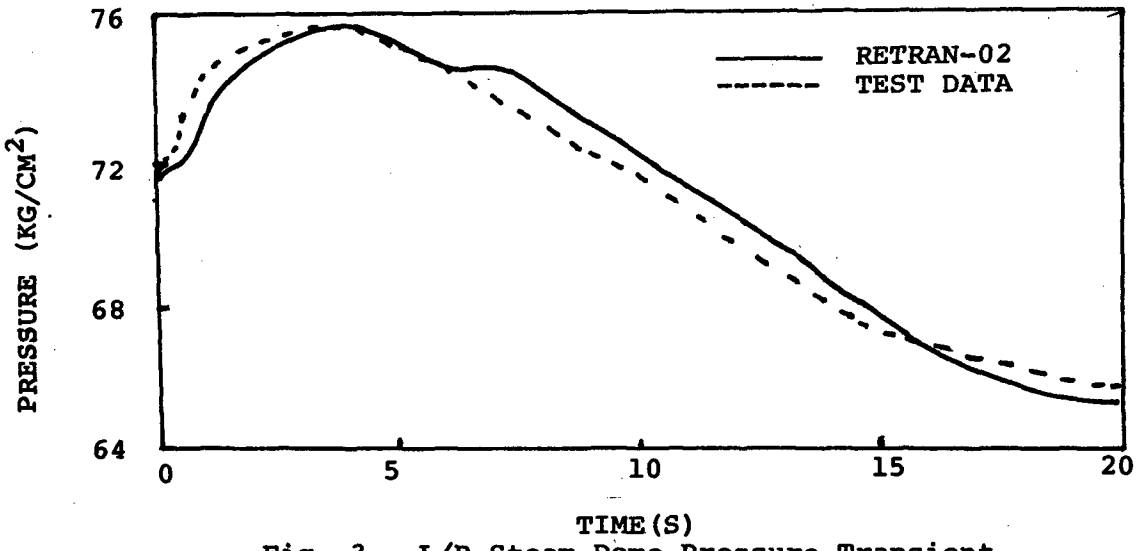


Fig. 3. L/R Steam Dome Pressure Transient

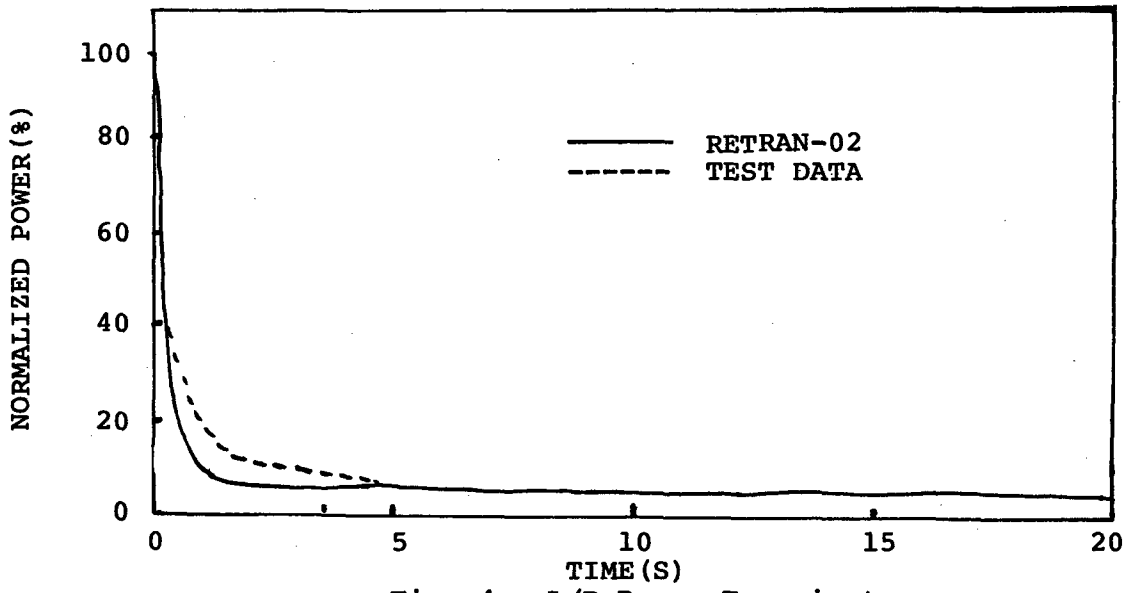


Fig. 4. L/R Power Transient

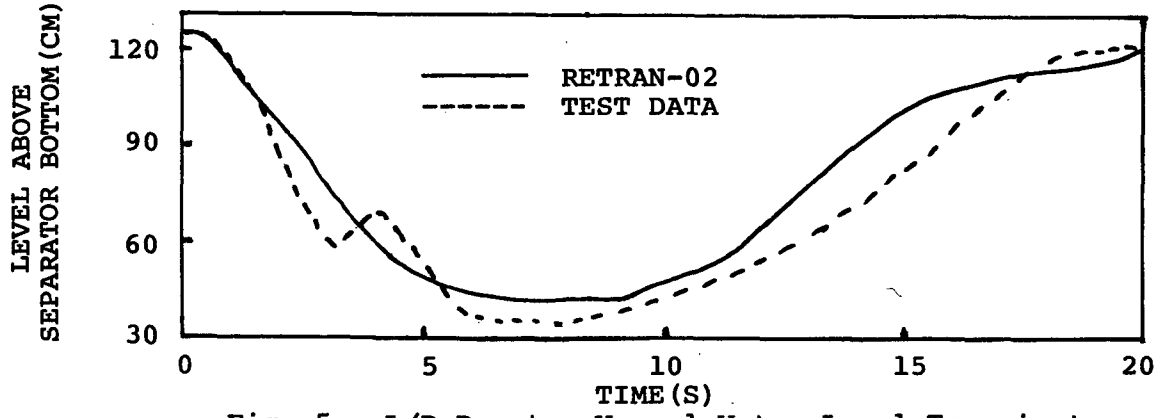


Fig. 5. L/R Reactor Vessel Water Level Transient

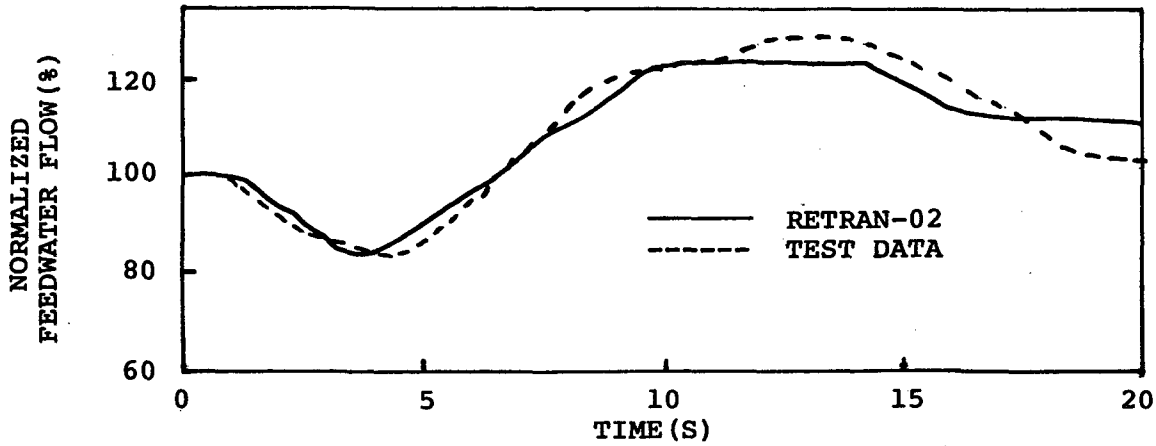


Fig. 6. L/R Feedwater Flow Transient

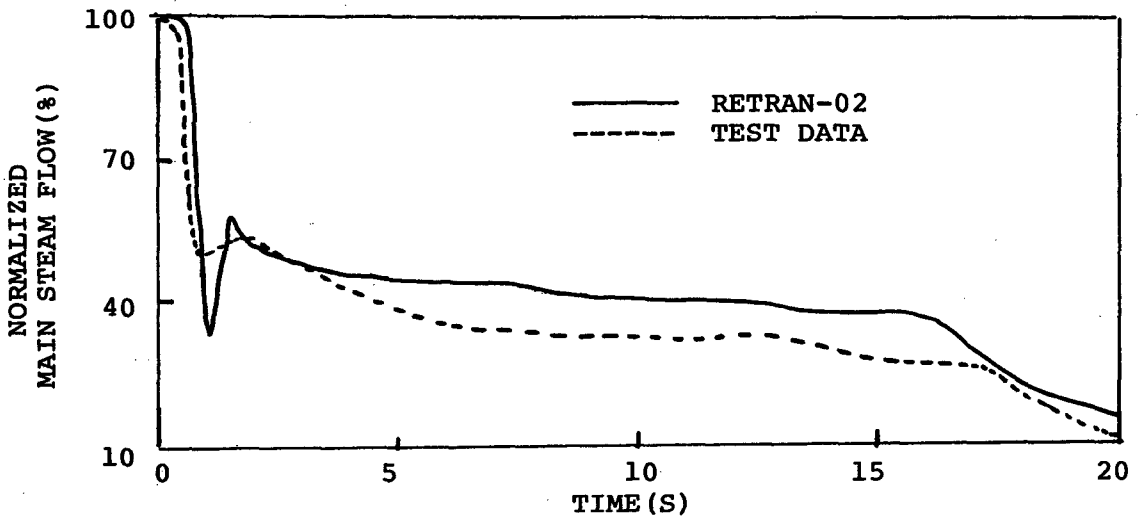


Fig. 7. L/R Main Steam Flow Transient

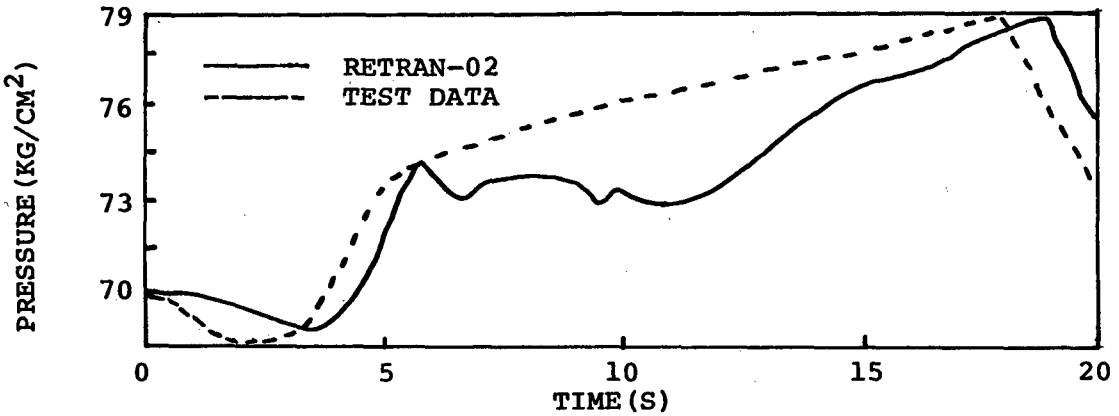


Fig. 8. MSIVFI Steam Dome Pressure Transient

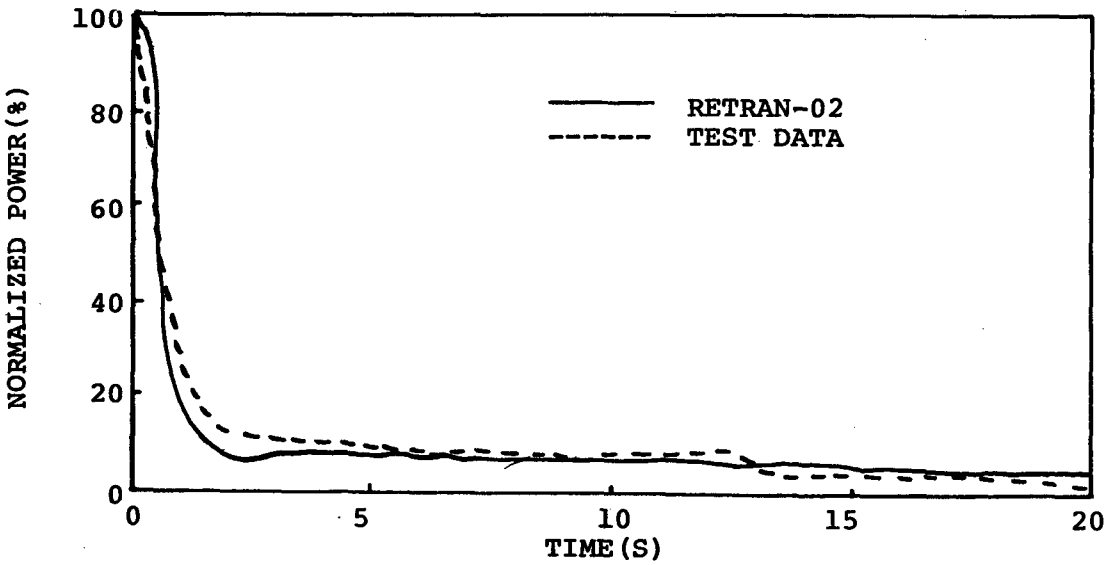


Fig. 9. MSIVFI Power Transient

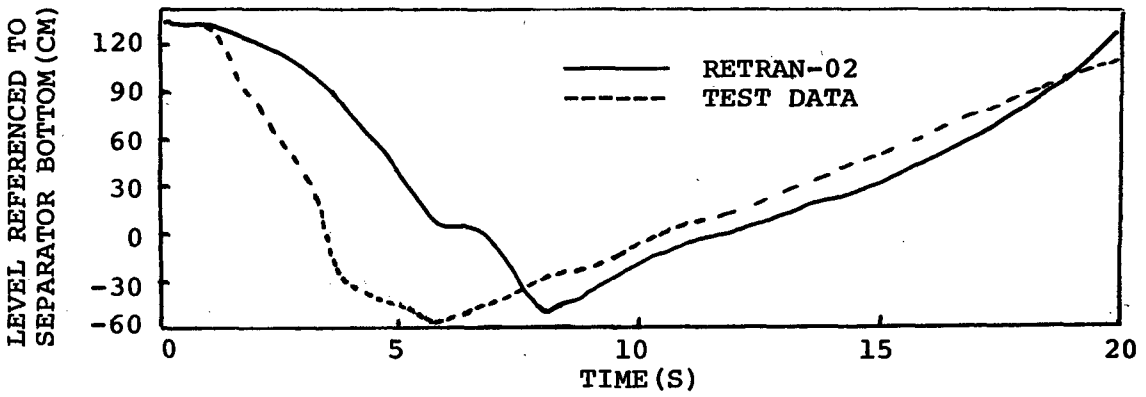


Fig. 10. MSIVFI Reactor Vessel Water Level Transient

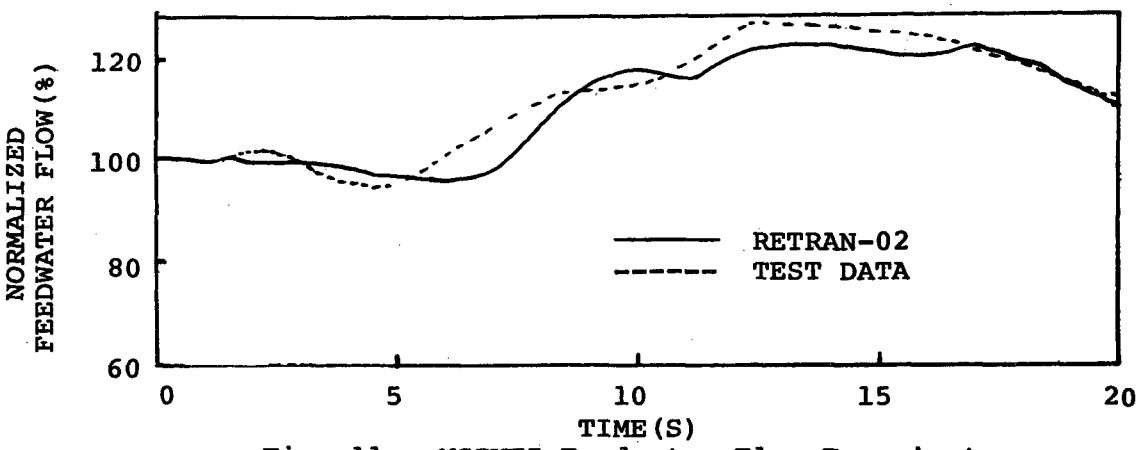


Fig. 11. MSIVFI Feedwater Flow Transient

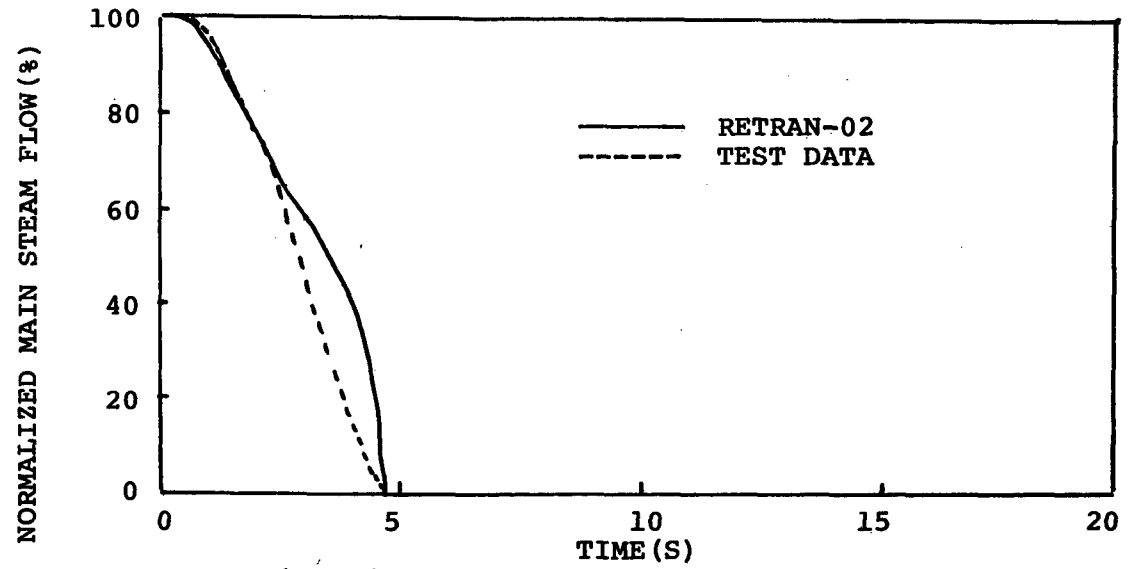


Fig. 12. MSIVFI MAIN STEAM FLOW TRANSIENT

DESIGN AND INSTRUMENTATION OF LOBI[1] U-TUBE STEAM GENERATORS FOR SMALL BREAK AND SPECIAL TRANSIENTS TESTS

W. L. Riebold, T. R. Fortescue, K. H. Günther

Commission of the European Communities
EURATOM, Joint Research Centre - Ispra Establishment
LOBI Project, Heat Transfer Division
I-21020 ISPRA/Varese (I)

ABSTRACT

In view of the forthcoming LOBI small break LOCA and Special Transients experiments, the two existing inverted U-tube steam generators will be replaced by new ones having much more detailed volume and height scaling and very extensive instrumentation on both primary and secondary side. The design rationals for volume and height result from the particular simulation requirements imposed by the objectives of the LOBI Project. The measurement instrumentation is concentrated in those regions where significant changes in the heat transfer regime are expected to occur during the transients under consideration. The results to be obtained are intended to be used for the validation of the analytical models for the heat exchanger characteristics of steam generators.

INTRODUCTION

The LOBI test facility, at present the only high-pressure integral system test facility in Europe for the investigation of PWR LOCAs, contains two inverted U-tube steam generators designed originally for large break LOCA investigations, having only a global volume and height scaling / 1 /.

LOBI is a two active loop system, operating at normal (KWU) PWR conditions of 290°/320°C and 155 bar on the primary side, and 210°C feed water temperature and 54 bar on the secondary side. Turbines are simulated by a condenser, followed by a cooler which reduces the condensate temperature to 210°C at the inlet to the feedwater pump.

For the primary circuit, very detailed attention was paid to scaling: all coolant volumes, not only of the individual components (Pressurizer, Accus, SGs etc.) but also of the pipework between them, have been scaled by a factor of 712 with respect to the reference reactor. Heating power is also scaled by 712 leading to a power of 5.3 MW

[1] Loop Blowdown Investigations

for the LOBI 8 x 8 rod bundle. Heat transfer surfaces, i.e. heater rods, and SG U-tubes are full length. All component heights, and elevations have also been preserved 1 : 1 in order to retain the correct gravitational heads.

The TMI-2 accident led to a review of the LOBI experimental programme, and in particular, to a review of the adequacy of scaling, and flexibility of operation of the LOBI secondary loop, for the purposes of small break and Special Transients tests. Following this review, it was considered essential to replace the existing SGs by ones having much more detailed volume and height scaling, and very extensive instrumentation, on both primary and secondary side.

Further additions considered necessary were, on the primary side, the High Pressure Injection System, and on the secondary side, the Auxiliary Feedwater System, Steam Generator isolation and pressure relief valves, and feed and steam line mass flow measurements. These additions are being installed in the second half of 1982, / 2 /, and a series of 16 small break tests is planned for the period April 1983 to December 1984.

The present paper describes the design rationals for the volume, volume ratio and height scaling as well as the measurement instrumentation system of the new LOBI SGs.

DESIGN RATIONALS

The design criteria for the new LOBI inverted U-tube steam generators result, as do those for the whole LOBI integral system test facility, from the particular simulation requirements imposed by the objectives of the LOBI Project. Two steam generators were required, one for the "broken", one for the "intact" loop, having a capacity ratio between the two of 1 : 3 with respect to coolant volume and mass flow, to heat transfer surface and, hence, to heat exchanger power.

For the "broken" loop steam generator, the scaling down factor of 712 was applied to the appropriate quantities of the reference plant steam generator, which led to a heat exchange power of 1.32 MW, and to 8 U-tubes (+ 1 installed spare). To simulate, as closely as technically possible, the thermohydraulic behaviour of the reference plant steam generator, in particular under small break LOCA and Special Transients conditions, the following design and scaling criteria were applied:

- Volume scaling had highest priority, in order to obtain the same SG time behaviour as in the reference plant. A total of 3 primary and 5 secondary volumes within each SG were defined, and have been individually scaled, Fig. 1, Table I.
- The height of the lowest U-tube bend above the main coolant pipe centre line has been preserved, because of its strong influence on change-over from "natural circulation" to "reflux condenser" operation mode in the case of small break LOCA conditions.
- For small break experiments, it was not thought essential to maintain the heights in regions above the lowest U-tube bend, as long as the volumes were correctly scaled.

TABLE I: Design Data for Steam Generators

	Size in Reference SG	LOBI-SG (broken loop)						LOBI-SG (intact loop)					
		for scaling 1 : 712			for scaling with respect to primary volume			for scaling 1 : 712			for scaling with respect to primary volume		
		Nominal	Actual	Deviation %	Nominal	Actual	Deviation %	Nominal	Actual	Deviation %	Nominal	Actual	Deviation %
Heat transfer surface	5400 m²	7,58 m²	7,75 m²	2,2				22,75 m²	23,36 m²	2,7			
VP2 (Primary water volume)	23,43 m³	32,9 l	33,8 l	2,8				98,7 l	102 l	3,3			
VP1+VP3 (Primary volume in in-and outlet plena)	13,39 m³	18,8 l	19,0 l	0,8	19,3 l	19,0 l	1,9	56,4 l	57,1 l	1,2	58,3 l	57,3 l	2
VS1 (Downcomer volume below feed ring)	20,40 m³	28,7 l	29,2 l	1,9	29,4 l	29,2 l	0,7	86,0 l	89,3 l	4	88,7 l	89,3 l	0,7
VS2 (Riser volume up to top highest U-tube)	50,64 m³	71,1 l	73,9 l	3,9	73,5 l	73,9 l	0,6	213 l	221 l	3,5	222 l	221 l	0,4
VS3 (Riser volume between highest U-tube and H_N)	12,99 m³	18,2 l	18,7 l	2,4	18,8 l	18,7 l	0,6	54,7 l	55,6 l	1,6	56,7l	55,6l	1,9
VS4 (Downcomer volume between H_N and feed ring)	20,0 m³	28,1 l	29,8 l	6	28,9 l	29,8 l	2,9	84,3 l	88,9 l	5,5	87,2 l	88,9 l	2,0
VS5 (Steam dome volume above H_N)	74,72 m³	105 l	109 l	3,7	109 l	109 l	0	315 l	317 l	0,8	329 l	317 l	3,5

- For Special Transients experiments, system behaviour for mixture levels between nominal, and lowest U-tube levels could be important: in particular, transient behaviour of recirculation rate should be preserved, as far as possible. However, the actual distance between highest and lowest U-tube bend was not considered to be critical, particularly as mixture level transitions between them are expected to be comparatively rapid.
- An adjustable throttle device is being installed at the lower end of the downcomer, to allow the recirculation rates in the two LOBI SGs to be set up, and matched to each other on the basis of flow and temperature difference measurements.
- Each LOBI SG contains coarse and fine separators, having the same design as those of the reference plant. The coarse separator was reduced in height and diameter with respect to the real one to maintain reactor typical inlet velocities of 7 - 8 m/s.
- Design calculations for the individual flow pressure losses along the secondary coolant flow path between feedwater ring and highest U-tube bend have shown reasonably good agreement between the LOBI SG and the reactor SG.

The pressure losses in the cross flow regions, at the inlet to the riser, and at the U-bends, are expected to be lower for the LOBI design than for the reactor steam generators. However this should be at least partially compensated for, at the riser entrance, by the flow throttle devices used to set up the recirculation rates in the SGs, and above the U-bends, by the increased pressure drop expected in the coarse separators.

The permissible operating pressure on the secondary side of the new steam generators has been raised to 100 bar to permit representative feed-and-bleed operation on the secondary side.

Tappings have been included to allow connection between the secondary side at the tube plate, and either the inlet or outlet plenum on the primary side, in order to simulate U-tube ruptures: an orifice in the connection line defines break area, i.e. number of U-tubes ruptured.

The general form of the design adopted can be seen in Figure 1. It consists of a single cylindrical pressure vessel with an annular downcomer separated from the riser region by a skirt tube. This tube is supported above the tube plate, and carries the coarse separator. The U-tubes are arranged in a circle within the riser region, around an axially mounted filler tube, with the U-bends crossing over one another above it. This design permits cross flow between co-current and counter current legs of the U-tubes over their entire length, heat transfer between riser and downcomer, and extremely precise volume scaling (see Table I); at the same time extraneous thermal capacity in the filler elements is minimized.

Principal problems are the instrument penetrations for temperature and pressure measurements on the primary side within the U-tubes, and holding the design tolerances during manufacturing. In particular the broken loop steam generator calls for a 6 mm downcomer gap width over a length of 7.5 metres: in view of this, original plans to use a welded construction for the pressure vessels were dropped by the manufacturer, who is now boring them from solid bars, using gun boring techniques.

MEASUREMENT INSTRUMENTATION SYSTEM

The new SGs are instrumented in such a way as to provide a maximum of information on both the magnitude, and location of the heat transfer processes taking place between primary and secondary circuits. In particular, instrumentation is more concentrated in the region of the lowest U-bend, and immediately above the tube plate in order to detect changes in the heat transfer regime.

Instrumentation includes "3-hole" tubes mounted at three positions at the same level, around the circumference of the SG: these should permit direct measurement (and therefore adjustment) of the recirculation rate during steady state, and during transients, measurement of not only the vertical, but also the circumferential component of the flow.

Differential pressure measurements should provide both collapsed level, and relatively local void fraction information on the primary side, and in both downcomer and riser regions of the secondary side. Fluid temperature information in the same regions will be provided by 0.8 mm diameter inconel sheathed thermocouples. It is hoped to obtain direct measurement of the mixture (not collapsed) level in the riser region using an experimental Time Domain Reflectometer probe.

One of the major problems encountered during the design was the need to allow for the differential expansion (up to 30 mm) between U-tubes, and SG pressure vessel, if the secondary side is allowed to dry out, and then refilled using the auxiliary feedwater.

The approximate locations of the various instruments are indicated in Fig. 2.

In addition to this instrumentation, measurement inserts are being installed in the secondary side feed and steam lines: these should provide inlet and outlet mass flow information under both steady state, and transient conditions, including during feed-and-bleed operation. Turbine meters are used in the feed lines: in the steam lines, turbine meters, drag bodies, and vortex meters are being installed.

CONCLUSION

It has been suggested that detailed investigation of SG behaviour is best performed using separate effects tests. However, there are very few separate effects facilities which can also be used to investigate SG performance during transients at high pressure. The new LOBI SGs are intended to provide information under just these conditions, results which it is hoped will be complementary to those obtained from other facilites, and will allow the validation of the analytical models for the heat exchanger characteristics of SGs.

ACKNOWLEDGEMENT

The LOBI Project is being executed in the framework of an R&D contract between the Bundesminister für Forschung und Technologie (BMF), Bonn, and the Commission of the European Communities.

REFERENCES

1. W. L. RIEBOLD, H. STÄDTKE, "LOBI - Influence of PWR Primary Loops on Blowdown. First Results", invited paper presented at the ANS 27th Annual Meeting, June 7 - 11, 1981, Bal Harbour, Florida/USA and USNRC 9th Water Reactor Safety Research Information Meeting, October 26 - 30, 1981, Gaithersburg, Maryland/USA

2. W. L. RIEBOLD, L. PIPLIES, "The LOBI-Project Small Break Experimental Programme", paper presented at the ANS-EPRI Specialists Conference on Small Breaks in LWRs, August 25 - 27, 1981, Monterey, California/USA.

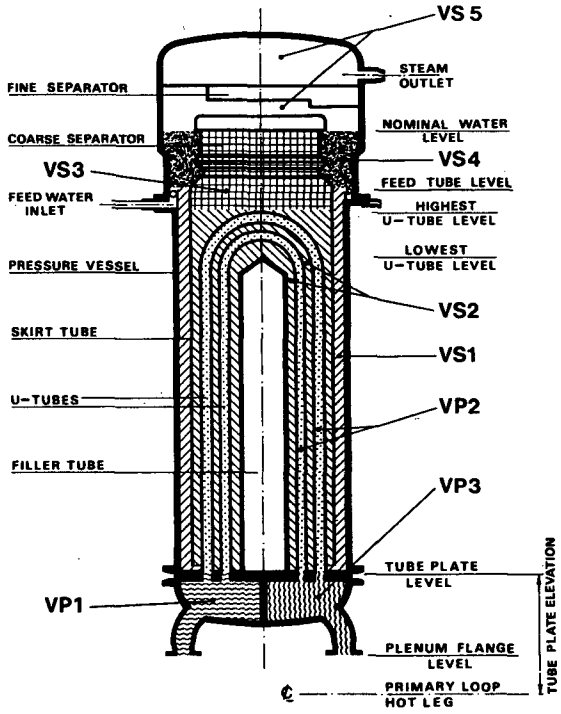


Fig. 1. LOBI Mod 2 Steam Generators Scaling.

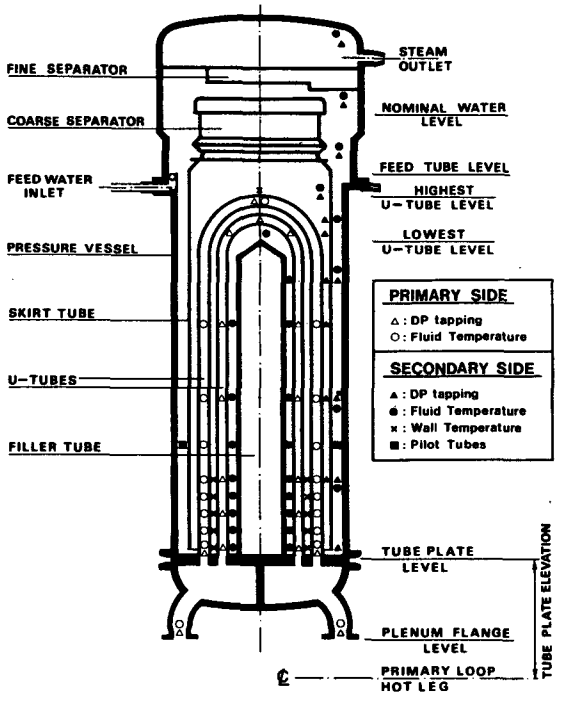


Fig. 2. LOBI Mod 2 Steam Generators Instrumentation.

CALCULATION OF A BWR "PARTIAL ATWS" USING RAMONA-3B

D. I. Garber, D. J. Diamond and H. S. Cheng

Brookhaven National Laboratory
Upton, New York 11973

ABSTRACT

The RAMONA-3B code has been used to simulate a boiling water reactor (BWR) transient initiated by the closure of the main steam line isolation valves in which all the control rods in one-half the core fail to scram after reactor trip. The modeling of the nuclear steam supply system included three-dimensional neutron kinetics and parallel hydraulic channels (including a bypass channel). The transient is characterized by an initial pressure spike and then by oscillations in the pressure due to the opening and closing of relief valves. These oscillations in turn affect all thermohydraulic properties in the vessel. The simulation was continued for 7 minutes of reactor time at which point boron began to accumulate in the core. The calculation demonstrates the importance of using three-dimensional neutron kinetics in conjunction with the modeling of the nuclear steam supply system for this type of transient. RAMONA-3B is unique in its ability to do this type of calculation.

INTRODUCTION

Anticipated BWR transients in which there is no reactor trip (i.e., no scram) continue to be an unresolved licensing issue. Since the reactor does not shut down immediately, it is particularly important to adequately analyze the core neutronics and thermohydraulics during the transient. For those transients in which only part of the reactor is scrammed, as occurred in Browns Ferry Unit No. 3 (on June 28, 1980), a multidimensional treatment of the spatial effects occurring in the core is essential. RAMONA-3B [1] offers the unique capability to dynamically represent the spatial neutronics coupled explicitly with the thermohydraulics of the entire system. For this reason, a transient accompanied by partial scram failure was simulated to provide a test of the overall code capability to perform such analyses.

The accident analyzed with RAMONA-3B is initiated by the (inadvertent) closure of the main steam line isolation valves (MSIVs) from (approximately) rated core power and flow conditions. It is assumed that all control rods in one-half the core fail to scram after the reactor trip signal is received. Other safety systems are assumed operable; the recirculation pumps trip, pressure relief valves operate, and the high pressure coolant injection system, the reactor core isolation cooling system and the standby liquid control system all actuate when required.

The MSIV closure event is one of the most limiting for peak vessel pressure and suppression pool temperature considerations. Although RAMONA-3B does not calculate the pool temperature, it does provide the steam flow through the safety and relief valves which is required for the pool temperature calculation.

Analyses of this accident have been performed at General Electric [2] and at BNL [3]. Both of these analyses used auxiliary steady-state core calculations to help determine the core power and used assumptions slightly different than those used with RAMONA-3B. Nevertheless, the results reported herein are consistent with the previous work.

MODELING OF ACCIDENT CONDITIONS

The reactor modeled for this calculation was a BWR/4 at end-of-cycle conditions similar to those used previously [3]. The initial reactor state corresponded to operation at 104.5% of rated power (3440 MW) and 100% rated flow (12800 kg s^{-1}). All control rods were initially withdrawn.

A coarse mesh was used in both the steam line (8 nodes) and the core (12 axial nodes). This mesh was found to be acceptable based on comparisons with calculations using a finer mesh [1]. The core model used had 32 nodes in the x-y plane for the neutron kinetics calculation, but took advantage of half-core symmetry. Figure 1 shows the half-core configuration and the numbering for the neutron kinetics nodes and thermohydraulic channels. When the rods in half the core are inserted, it is the left side (i.e., nodes 1-3, 7-9, 13 and 14) that becomes rodded.

The cross sections used were originally derived for use with a two dimensional (R,Z) coupled neutron kinetics and core thermohydraulics code. The method used to obtain the data [4] did not include core burnup calculations. Beginning-of-life data were systematically varied until the core-average axial power distribution gave agreement with the expected end-of-life (Haling) power distribution. This procedure resulted in eleven cross-section sets which are distributed to 16 material (or exposure) zones based on eight axial and two radial divisions.

In transforming the actual core geometry into the configuration shown in Fig. 1, no attempt was made to homogenize fuel bundles with reflector water for the nodes at the core periphery. The good agreement in radial power distribution with a more detailed calculation [1] justifies this approach.

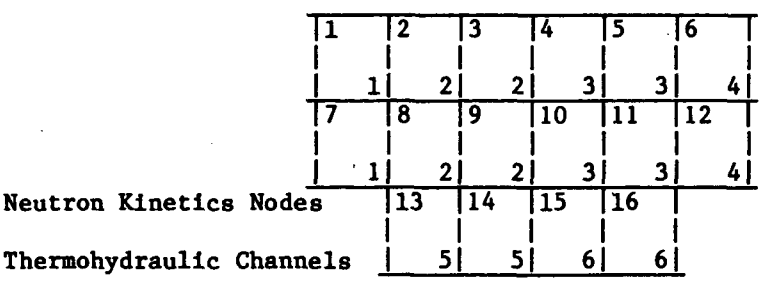


Figure 1 Core Configuration for Partial Scram Calculation

Reactor trip would normally occur due to the signal for MSIV closure, however, that signal is ignored and the assumption is that the trip signal will be due to high power. The control rods in half the core move at a speed of 0.91 m s^{-1}. The low level signal for both the high pressure coolant injection (HPCI) and the reactor core isolation cooling (RCIC) systems is -1.77 m relative to the initial water level outside the steam separator skirts. The HPCI and RCIC systems are assumed to take 3 s to reach their full flow rate after a delay time of 27 s.

The 13 safety and relief valves are grouped into four banks. The opening and closing flow rates are assumed to be exponential with a time constant of 0.1 s. The feedwater control system is represented by an input boundary condition. The flow rate was obtained from GE [2] where it was calculated for a similar accident situation. Figure 2 is a plot of the flow rate from the feedwater sparger. The early flow (< 200 s) is due to the feedwater system (water at 196°C) and the latter flow (> 300 s) is due to the HPCI and RCIC systems (water at 48.9°C). The standby liquid control system was initiated on a time signal to represent operator action at 255 s coupled with a delay time of 45 s. The rate of boron addition to the vessel at the location of the jet pump instrumentation lines corresponds to an injectant flow rate of 2.7 kg s^{-1} (43 gpm) with a boron concentration of 23,000 ppm.

RESULTS

The transient calculated with RAMONA-3B was initiated by an MSIV closure and then calculated for 400 s. During this period, control rods were inserted, the recirculation pumps tripped, pressure relief valves opened and closed, the amount of feedwater changed and the HPCI/RCIC and SLCS systems were actuated. The effect of these actions and the interaction of the different feedback mechanisms makes the local and global system behavior very complex. The major events and trends during the transient as calculated by RAMONA-3B are given in Table I. The following discussion is separated into five parts in order to explain certain features of the calculation.

Initial Overpressurization Transient

The MSIV closure causes an increase in pressure in the vessel (cf. Fig. 3). This pressure pulse is less severe than that caused by a turbine stop valve closure due to the relatively long time (4 s) it takes for the MSIV to close. The increase in pressure collapses steam voids which has the effect of increasing core power (cf. Figs. 4 and 5). This tends to be self-limiting because an increase in power increases the void fraction. However, the insertion of control rods due to an overpower (120% of rated power) signal, the decrease in flow due to the RPT and the decrease in pressure due to the opening of relief valves combine to terminate the early phase of the transient.

Figure 5 shows the fission rate during this early phase for (neutron kinetics) channel 5 (cf. Fig. 1) in which all control rods are inserted and channel 2 in which no control rods move. Reactor trip occurs at 2.5 s and by 10 s only the decay heat level is significant in channel 5. Note that the ability to monitor behavior such as in Fig. 5 requires a code with spatial neutron kinetics. The changes in fission rate that are most pronounced on Fig. 5 (and not seen on Fig. 4 because of the different scale) occur after 2.8 s with a frequency of 3 Hz. These are due to the insertion of control rods and the coarseness of the axial mesh. This can be eliminated with a finer noding or with an appropriate control density function for a node. This effect should not change the behavior of the fission rate averaged over several periods ($\sim$1 s). Figures 6 and 7 which show the radially averaged axial power at different times during the transient also demonstrate the importance of spatial neutron kinetics. The figures show that the spatial and temporal behavior is non-separable.

Effect of Recirculation Pump Trip (RPT)

The RPT occurs due to the pressure exceeding 8.03 MPa at 5 s. The resulting flow rates for (thermohydraulic) channels 2 and 3 (cf. Fig. 1) are shown in Fig. 8. (The drive loop flow rate and the pump speed after a RPT with only a feedwater trip and no control rod insertion have been compared with GE results for up to 10 s [5] and found to be within 3%. Channel 3 contains control rods after the reactor trip and channel 2 is unrodded. Because the power is higher in channel 2 than in channel 3, the flow

TABLE I

TRANSIENT CHRONOLOGY

Time (s)	Event/Comment
0	MSIV begins to close initiating the transient. It closes completely in 4 seconds. System pressure rises, voids collapse, and reactor power rises.
2	Feedwater trip. Feedwater reduced to zero in 18 s (see Fig. 2).
2.2	Power reaches 120% of rated power. After 0.3 s delay half of the control rods are inserted in 4 s.
3.8-4.0	System pressure reaches the setpoints of relief valve banks 1-3. All valves stay open until approximately 15 seconds.
4.1	Overall reactor power peaks at 2.9 times the steady-state power. Unscrammed side of reactor peaks at 3.5 times the steady-state power.
4.5	System pressure reaches 8.03 MPa. After 0.53 s delay recirculation pump trips.
5-6	Power in scrammed half of reactor at decay heat levels and remains so for duration of transient.
6-7	Average fuel temperature for hottest node peaks at 1300°C.
8	System pressure peaks at approximately 8.3 MPa.
15	Liquid velocity in downcomer drops below bubble rise velocity setting up situation for countercurrent flow.
20	Feedwater shut off completely.
30-400	Relief valve bank 1 opening and closing drives the system pressure in an oscillatory manner. Other system variables including reactivity follow.
35	Downcomer water level at temporary low. Feedwater turned on to simulate control system response.
35-120	Water level rises above steam separator skirt.
60	Recirculation pump coastdown completed.
155	Feedwater flow rate reduced to zero.
140-350	Water level decreases.
180-220	Liquid in vessel approaches saturation temperature following removal of subcooled feedwater. Average void fraction in core increases from 0.23 to 0.30. In response to system pressure oscillations, liquid in vessel goes from being superheated to subcooled and vapor generation rate changes accordingly.
300	Boron injection is initiated.
320	Boron enters core.
350	HPCI flow initiated.
360	Water level stabilized. HPCI flow approximates the steamline flow.
375	Subcooled water from HPCI injection reaches core entrance.
400	End of demonstration run.

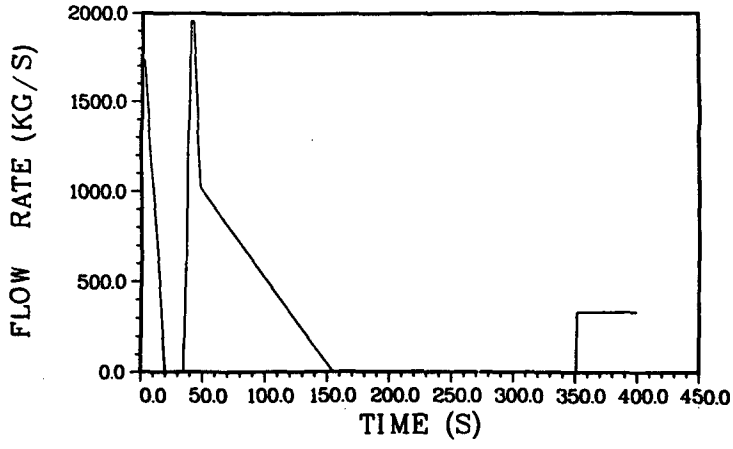


Figure 2 Flow Rate at Feedwater Sparger

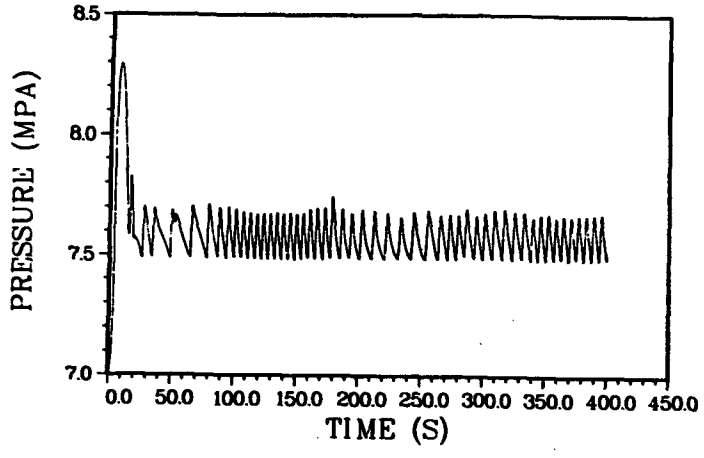


Figure 3 System Pressure

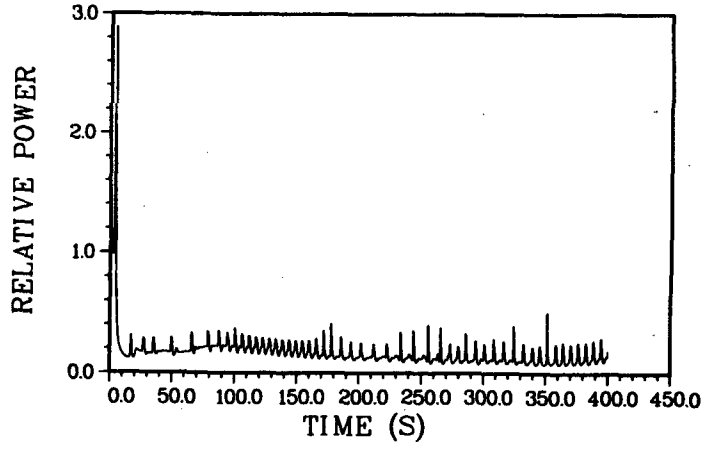


Figure 4 Relative Core Power

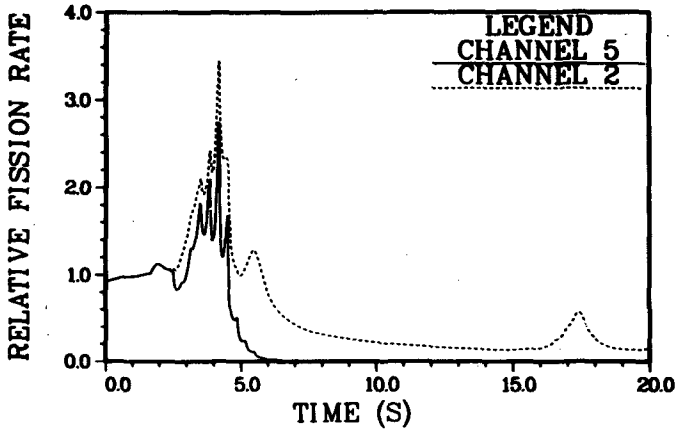


Figure 5 Fission Rate in Neutron Kinetics Channels

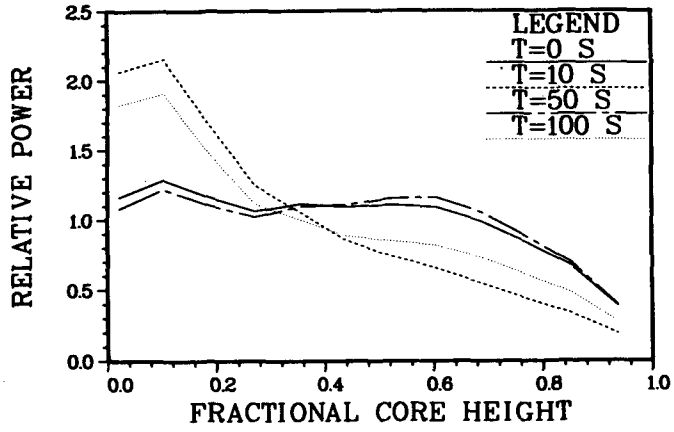


Figure 6 Axial Power Distribution at Different Times

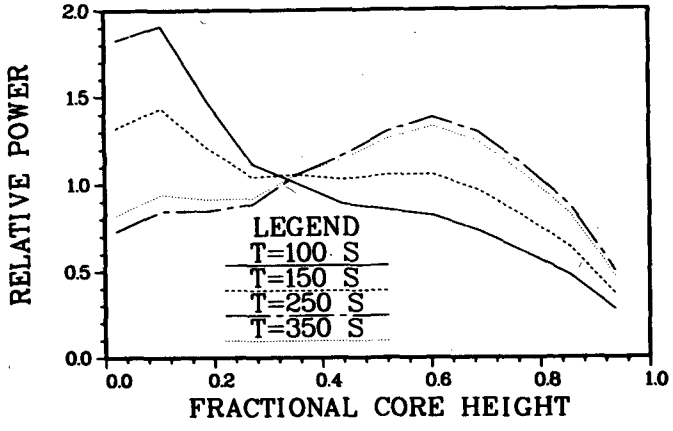


Figure 7 Axial Power Distribution at Different Times

rate is also higher. Figure 8 shows that the natural circulation flow rate in this transient is 25-30% of the steady-state flow rate.

By reducing the flow rate to natural circulation, the void fraction is maintained reasonably high. Because of void feedback the reactor power is kept lower than might have been attained otherwise. (Note that the pressure is approximately 7.6 MPa during the transient which is higher than the initial value of 7.0 MPa, and this by itself would decrease the void fraction.) This is an important strategy for dealing with this type of accident. Figure 4 shows that the time-average relative power is $\sim$20% up to 150 s and $\sim$15% during the latter part of the transient.

Effect of Relief Valve Cycling

The initial overpressurization (cf. Fig. 3) is sufficient to open all three banks of relief valves. However, after a 10 s period of venting and a reduction in core power, the pressure is only sufficient to actuate one bank of valves. Since the MSIVs have closed, the vapor generated in the core exhausts through this bank. The opening of valves reduces pressure, and hence, the valves open and close in a fairly regular cycle. The flow rate through all the valves is given in Fig. 9. The period of the valve cycling ranges from 5-15 s. Hand calculations at two different time intervals ($\sim$70 s and $\sim$130 s) confirmed the periods calculated by the code. The variation of this time period is expected since the rate of pressure drop when the valve is open is primarily governed by the difference between the steam flow rate out of the vessel and the total vapor generation rate in the vessel, i.e., a small difference between two large numbers.

The cycling of the relief valves affects the system pressure (cf. Fig. 3) and this in turn cause the oscillation in power during the transient (cf. Fig. 4). These oscillations can also be seen in the flow rates shown in Fig. 8 and in the core-average void fraction.

The flow rates at the core exit for a channel in which the power is relatively high and for a channel with only decay heat are not in phase. During the latter half of the transient they are close to 180° out-of-phase with the flow rate increasing in one channel when it is decreasing in the other and vice-versa.

Water Level in the Vessel

Figure 10 shows the water level in the downcomer region. The water inventory in the vessel and the level in the downcomer are closely related to the feedwater flow, as can be seen by comparing Fig. 2 with Fig. 10. The water level calculation in RAMONA-3B takes into account that steam voids are present in the downcomer; the measurement in a BWR uses an instrumentation line in which the void condition may be different. Hence, care must be exercised in interpreting the calculated water level.

Core Inlet Subcooling

The core inlet subcooling is a strong function of the feedwater flow rate. The inlet subcooling (along with the flow rate and power) helps determine the void fraction in the core. When the inlet subcooling is close to zero at times greater than 200 s, the void fraction significantly increases. This reduction in inlet subcooling corresponds to a reduction in subcooling throughout the vessel. When this occurs, the pressure oscillations cause the vessel liquid state to oscillate between subcooled and superheated and flashing and condensation can take place.

The Effect of Boron

Boron enters the vessel at the location of the jet pump at 300 s. It starts to enter the core approximately 20 s later and increases to a concentration of $\sim$20 ppm by the time the calculation is terminated at 400 s. This is insufficient to shut

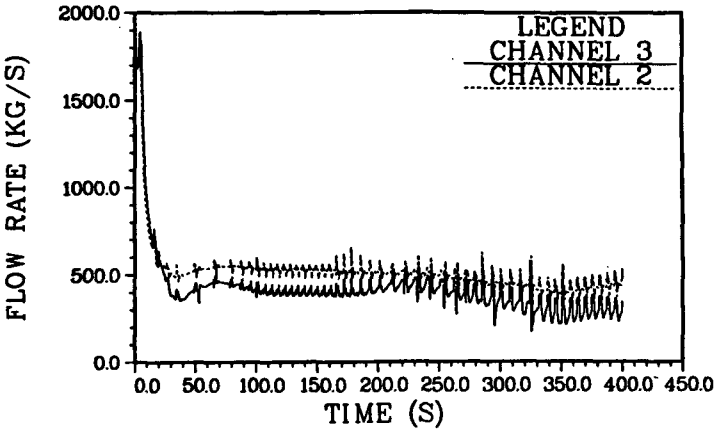


Figure 8 Inlet Flow Rate in Different Thermohydraulic Channels

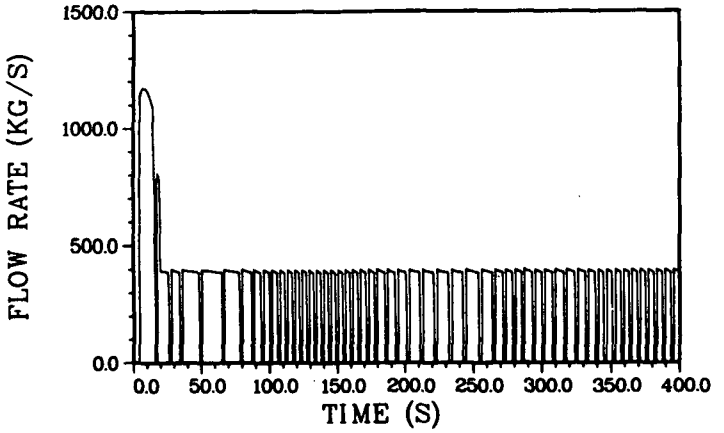


Figure 9 Steam Flow Through Relief Valves

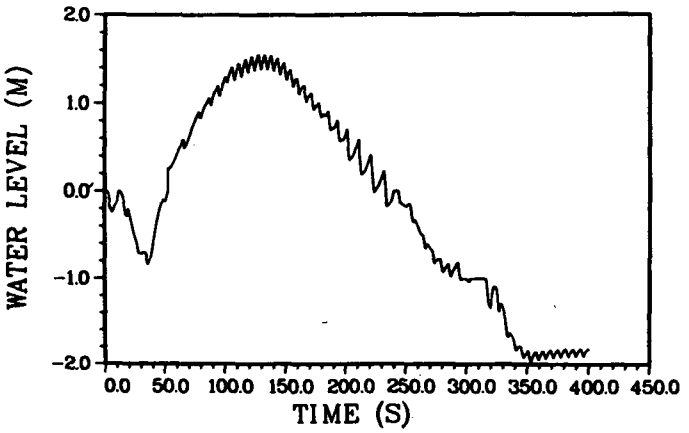


Figure 10 Mixture Water Level in Downcomer

down the reactor. It is expected to take 400 ppm of boron before the fission rate is reduced to a negligible level and this will take approximately 2000 s.

CONCLUSIONS

RAMONA-3B has been successfully applied to a transient initiated by MSIV closure in which only the control rods in half of the core are inserted after reactor trip. This accident is an excellent example of a situation in which it is important to model the steam supply system with a core component that includes three-dimensional neutron kinetics. RAMONA-3B is unique in its ability to satisfy this requirement. This calculation has involved not only the basic vessel and steam line thermohydraulic models and the neutron kinetics model, but also the activation of different parts of the control and protection system model.

The code calculated over a range of conditions encountered in 400 s of reactor time with a (reasonable) computing time on BNL's CDC-7600 equipment that averaged 15 times reactor time. The results are in qualitative agreement with those reported elsewhere [2], i.e., there is an initial overpressurization phase followed by a long period of operation with natural circulation characterized by oscillations with a frequency of 0.1 Hz. This oscillatory behavior is reflected in power, pressure, flow and other system variables. Quantitative comparisons with other calculations [2,3] are not possible because of differences in the assumptions used in each calculation.

ACKNOWLEDGEMENT

The authors appreciate the efforts of A. L. Aronson, H. R. Connell, S. V. Lekach, C. J. Ruger, and W. Wulff in the development of the present version of RAMONA-3B and for assisting in the calculation of the partial ATWS. The work was performed under the auspices of the U. S. Nuclear Regulatory Commission.

REFERENCES

1. D. J. DIAMOND, et al., "Water Reactor Safety Research Division, Quarterly Progress Reports," Jan. 1979 - Dec. 1981, NUREG/CR-0821, 1035, 1248, 1403, 1506, 1618, 1800, 1960, 2160, 2381, Brookhaven National Laboratory.

2. R. H. BUCKHOLZ, Letter to P. Check, USNRC, Aug. 29, 1980, General Electric Co.

3. M. S. LU, et al., "Analysis of a Partial Scram Event in a Typical BWR/4," BNL-NUREG-31417, Brookhaven National Laboratory (1982).

4. M. S. LU, et al., "Analysis of Licensing Basis Transients for a BWR/4," BNL-NUREG-26684, Brookhaven National Laboratory (1979).

5. "Final Safety Analysis Report - Peach Bottom Atomic Power Station Units No. 2 and 3," Philadelphia Electric Co. (1972).

SESSION 6

SAFETY GOALS

Chair: W. Y. Kato *(BNL)*
Y. Togo *(UT)*

Panel Discussion on

SAFETY GOALS

Chair: W. Y. Kato *(BNL)*

Panelists

F. Remick *(NRC)*
R. Anthony *(NII)*
A. Birkhofer *(GRS)*
Z. Domaratzki *(AECB)*
P. Tanguy *(CEA)*

DEVELOPMENT OF RISK-BASED SAFETY-RELATED CRITERIA FOR LICENSING CANDU NUCLEAR POWER REACTORS

W. Paskievici*, A. Pearson**, and J.T. Rogers***

*Ecole Polytechnique, Montreal H3C 3A7, Canada
**P.O. Box 422, Deep River, Ont. K0J 1P0, Canada
***Carleton University, Ottawa K1S 5B6, Canada

ABSTRACT

The first safety criteria used in Canada for licensing power reactors contained both a safety goal and general requirements to ensure that the safety goal was achievable. Present criteria set reference dose limits for individuals and total population for normal operation, for process system failures and for coincidental failures of both process and safety systems; they also set maximum frequency limits for the last two conditions. Recently, new criteria have been proposed which explicitly state safety objectives in terms of risk and set maximum dose exposures for individuals according to the frequency of postulated accidents. Problems in defining these risk-based criteria are discussed with special emphasis on ECCS performance specifications.

HISTORICAL BACKGROUND

Safety criteria for licensing nuclear power plants were first enunciated in Canada during the late 50's and the early 60's [1,2,3]. These criteria contained both a safety goal and general requirements to ensure that the safety goal was achievable. As the main concern was then - as today - to minimize the probability of accidents of large consequences, Laurence [3] proposed that the probability of a "disastrous" accident should be less than 10^{-5} per year. He further proposed that this probability could be achieved by providing "protective devices" and "containment provisions" which were completely separate from the "process systems" and from each other. If this separation was sufficiently complete that the probability of cross-linked failure was very small, then the probability of a "disastrous accident" could be determined by the product of the frequency of a serious failure in the process systems and the probabilities that the protective devices and containment provisions do not perform as intended.

This approach was incorporated in the first Siting Guide [4] developed by the Atomic Energy Control Board in 1964, in conjunction with the acceptance of the proposed Pickering site. The Siting Guide set "reference dose limits" for individuals and total population for three conditions: (a) normal operations; (b) process failures; (c) process and protective failures. The Siting Guide also set maximum frequency limits for conditions (b) and (c). By setting both dose and frequency limits for two broad accident conditions (called hereafter "single" and "dual" accidents), AECB implicitly set risk criteria for normal and accident conditions of acceptable consequences (≤25 rem to the most exposed individual from the population) but ignored "triple" accidents, i.e. simultaneous failure of a process system and of two of the independent protective or containment systems, on the basis of their very low probability of occurrence (less than 3×10^{-6}/year). This approach permitted

reasonable limits to be chosen: frequency of occurrence of significant faults in the process system were to be less than 1 per three years and the unavailability of the protective devices and of containment provisions (later, both called special safety systems) were to be each less than $10^{-2.5}$. The individual and collective dose limits (0.5 rem/yr for normal operation and single failures, 25 rem for dual failures; 10^4 man-rem and 10^6 man-rem for single and dual failures respectively) were chosen on the basis of comparative risk: the risk of leukemia, considered as the most significant radiological hazard, should be small with respect to its natural rate of occurrence. These requirements are summarized in Table I.

TABLE I

AECB Siting Guide Reference Dose Limits
Normal Operation and Accident Conditions [5]

Situation	Maximum Frequency	Maximum Individual Dose Limits	Maximum Total Population Dose Limits
Normal Operation	--	0.005 Sv/yr whole body 0.03 Sv/yr to thyroid	100 man-Sv/yr whole body 100 thyroid - Sv/yr
Single Failure (Process System)	1 per 3 years	As for normal operation	As for normal operation
Dual Failure (Process System and Safety System)	1 per 3×10^3 years	0.25 Sv whole body 2.5 Sv to thyroid	10^4 man - Sv whole body 10^4 thyroid - Sv

These basic criteria still hold today with only two minor modifications [5]:

a) the protective devices and the containment provisions are called "special safety systems". They now include two independent shut down systems, an emergency core cooling system (ECCS) and the containment;

b) the maximum permissible unavailability of a special safety system has been reduced to 10^{-3} (this decreases the probability of a triple failure to 3×10^{-7}/yr).

In intervening years, designers and regulators have specified secondary criteria to ensure that the basic criteria can be met. Some of these criteria are now common practice: diversity to ensure that there is more than one way to perform a function, redundancy to ensure that a single malfunction cannot disable a system, testability to ensure that the special safety systems meet the required availability standards, the use of reliable safety support systems, etc. Some other criteria are now under review, e.g. the required effectiveness of the ECCS and the required effectiveness of the containment. Finally, new criteria are now under discussion, such as a testable definition of safety system reliability.

It is emphasized that the general Canadian approach to reactor licensing is that the regulatory authority, the Atomic Energy Control Board (AECB), established overall safety objectives and criteria rather than specifying detailed design requirements. Thus, the AECB imposes a minimum of such safety requirements leaving the responsibility for a safe design with the designers themselves as well as the burden of proof

that the design meets the overall safety objectives and criteria. Recently, statements of the AECB requirements for safety analysis for CANDU nuclear power plants [6] and for special safety systems [7-9] have been issued for public comment.

Safety analyses have been carried out, in Canada, on the following basis: any failure of a process system alone must meet the Siting Guide limits for a "single" failure, and any combination of a process system failure and failure of one of the safety systems must meet the limits for a "dual" failure. The "single/dual" failure approach provides a good basis for a systematic review of the safety aspects of a nuclear power plant. However, the simple form in which the guidelines exist have caused during recent years some difficulties in application.

These difficulties have become increasingly important with the growth in system size, power rating and complexity, and an accompanying growth in techniques for in-depth analysis. An Inter-Organisational Working Group (IOWG) set up by AECB in 1977 to review the existing safety requirements for licensing CANDU nuclear power plants recognized the roots of these difficulties as being related to the fact that the original approach: a) does not distinguish amongst single (or dual) failures with differing rates of occurrence and consequences (i.e. a single reference dose limit is applied to all situations without regard to their rates of occurrence); b) does not fully recognize that some systems have within them many subsystems, the failure of which should be separately considered; c) does not give explicit guidance with respect to a frequency of an event below which its consequences need not be considered (a "cut-off" frequency); and d) does not explicitly treat external events.

The IOWG therefore proposed a set of safety requirements [10] which incorporated existing practices as well as new features. The most significant was the definition of risk criteria for six accident categories, with probability of occurrence ranging from 10^{-1} to 10^{-6} per year and reference dose limits ranging from 5×10^{-4} to one Sievert respectively (See Table II). Also a cut-off frequency of 10^{-7} per year was proposed.

The IOWG proposals were not adopted as such, due to two main objections; the increase in the maximum dose reference from 0.25 Sv to 1.0 Sv (25 rem to 100 rem) was considered unacceptable, although the new limit would apply for events of extremely low probability; also, not enough confidence existed in the analytical tools (fault-tree and event-tree analysis) and insufficient statistical data on systems reliability were available to ensure that probability calculations were accurate within an order of magnitude.

In its Licensing Requirements No 39 [6], AECB has retained the concept of several categories of accidents (5 instead of 6) for which maximum dose limits were proposed (ranging from 5×10^{-4} to 0.25 Sv); these categories were defined in a deterministic way by grouping together, from a predetermined list, postulated accidents of probabilities within the same estimated (but not explicitly stated) ranges (See Table III).

More recently, the AECB Advisory Committee on Nuclear Safety (ACNS), has undertaken a general review of safety objectives and requirements for all nuclear activities in Canada. In its Report ACNS-2 [11], which has been accepted by the AECB, the ACNS explicitly states the general safety objectives in terms of risk:

1. *Nuclear activities should not lead to unacceptable risks to the workers involved or the general public.*
2. *For hazards due to ionizing radiation: a) all early detrimental effects to individuals should be avoided and the risks of deferred effects ... should be minimized in accordance with the ALARA principle; b) the probability of possible malfunctions that could lead to the escape of radioactive material or the exposure of people to ionizing radiation, should be limited to small values,*

decreasing as the severity of the potential consequences increases so that the likelihood of catastrophic accidents is virtually zero.

3. *The risk to any future generation associated with each nuclear activity should be taken into account and given a priority for prevention not less than that given to risks presented to the current generation.*

The ACNS is presently in a final stage of drafting a statement on general safety requirements for nuclear power plants which specifies target as well as maximum risks for normal and accident conditions and sets a number of general requirements concerning siting, design, safety analysis, construction, commissioning, operation, effluent and waste management, and decommissioning which must be followed "to provide insurance that the safety objectives will be achieved" [12].

Some of these proposed general requirements are described in the following section. It should be emphasized that the final version of the ACNS recommendations may differ somewhat from those in the present draft.

TABLE II

IOWG Proposed Reference Values [10]

Reference Dose Interval, Sv		Reference Value for the Sum of the Predicted Rates of Occurrence of Failures within the Corresponding Reference Dose Interval
Whole Body	Thyroid	(Per Reactor Unit Per Annum)
$0\text{-}5 \times 10^{-4}$	$0\text{-}5 \times 10^{-3}$	10^{-1}
$5\times10^{-4} - 5\times10^{-3}$	$5\times10^{-3} - 5\times10^{-2}$	10^{-2}
$5\times10^{-3} - 5\times10^{-2}$	$5\times10^{-2} - 0.5$	10^{-3}
$5\times10^{-2} - 0.1$	0.5 - 1.0	10^{-4}
0.1 - 0.3	1.0 - 3.0	10^{-5}
0.3 - 1.0	3.0 - 10.0	10^{-6}

TABLE III

AECB Proposed Reference Values [6]

Class of Postulated Event	Reference Dose Limits, Sv	
	Whole Body	Thyroid
1	0.0005	0.005
2	0.005	0.05
3	0.03	0.3
4	0.1	1.0
5	0.25	2.5

PROPOSED GENERAL SAFETY REQUIREMENTS

On radiological dose limits for normal operations, the ACNS documents states:

The siting, design, construction, commissioning, operation and decommissioning, of a nuclear power plant shall, as far as practical, ensure that the effective dose equivalent and committed effective dose equivalent to any member of the public due to normal operation of any nuclear power plant should not exceed a small fraction (about one per cent) of the regulatory limit (0.005 Sv/year); for multi-unit sites, the maximum dose to any individual should be below the product of one per cent of the regulatory limit times the number of units or five per cent, whichever is less.

This statement is a judgement, based on experience of the extent to which doses can be limited through the application of the ALARA principle to CANDU nuclear power plants. The statement of these levels does not imply that further methods of reducing exposure should not be taken, where such methods are readily available and not unduly costly. Conversely, if a thorough and conscientious application of the ALARA principle has been made in the design and operation of a plant, levels above those stated above may be acceptable.

On safety analysis, the ACNS draft document states:

For accident conditions, the estimated radiological risk to the public shall not exceed significantly the acceptable risk for normal operations. To ensure that the design provides adequate safety, an analytical evaluation of the consequences of potential failures is necessary. To the extent practical, all potential fault sequences should be analyzed in a realistic manner. Where this is not feasible, sets of sequences having similar characteristics should be identified and a bounding case analyzed.

It also states:

1. *All models and data used in safety analyses must be based on sound, relevant theoretical, experimental and/or operational knowledge.*
2. *The identification and analysis of potential fault sequences, for the demonstration of conformity with requirement 3 below, shall employ fault-tree, event-tree, or equivalent analytical techniques acceptable to the AECB.*
3. *The risk estimated from analysis of various fault sequences shall be judged, in general, with reference to Figure 1. Fault sequences having approximately the same consequences shall be grouped. The rate of occurrence of events within a group shall be summed.* (The procedures for grouping accident sequences and the number of groups to be employed are now under consideration by the ACNS. These recommendations will be included in the final version of the report.)
   (a) *If the sum lies above the higher line of Fig. 1, the estimated risk is not acceptable.*
   (b) *If the sum lies below the lower line, the estimated risk is acceptable.*
   (c) *If the sum of the rate of occurrence lies in a region of conditional acceptability, the sequences shall be subject to special examination. The AECB may accept such situations, taking into account uncertainties, conservatism and any other mitigating factors, provided it is convinced that the risk is as low as reasonably achievable.*
4. *The consequences of any single event or of a sequence of events having a predicted rate of occurrence less than 10^{-7} per reactor unit per annum need not be included in this analysis, provided that the sum of the rates of occurrence of all such single events and sequences of events is less than 10^{-6} per unit per annum.*

.....

6. *In calculating doses for the purposes of requirement 3 above, realistic meteorological or dispersion conditions and internationally accepted relationships between exposure or intake and effective dose shall be used.*

The rationale for the risk diagram of Fig. 1 is discussed below (See also Fig. 2).

The top points of the lower and the upper curves represent the target (ALARA) and the regulatory limit individual dose equivalents for normal operation, 5 x 10^{-2} mSv and 5 mSv respectively. Since the top point of the target curve represents the ALARA goal for normal operation and since economic and social factors are among the factors to be considered in judging the acceptability of grouped fault sequences, the lower (target) curve may be interpreted as representing an extension of the ALARA principle to reactor accident conditions.

The lower curve is based on the recommendations of the IOWG. The higher-frequency portion of this curve represents a constant risk for these more-frequent fault sequences which is the same as the target risk for normal operation. For higher-consequence summed event sequences with frequencies of 10^{-3} and less, the lower curve has a steeper slope, thus providing a risk aversion effect for these more serious faults. The curve reaches a cut-off limit at a frequency of 10^{-7} events per reactor year with a corresponding dose-equivalent of 1 Sievert. The upper curve, lies near points representing the present single-failure and dual-failure frequencies and dose-equivalents. The higher frequency portion of this curve has a slope of about -1.75 while the lower-frequency portion of the curve, below 10^{-3} per reactor year, has a slope of about -6.6. This slope was chosen to provide the same cut-off point for the upper curve as that for the lower curve.

A justification for the cut-off is that the most comprehensive generalized studies of reactor risks, the Reactor Safety Study (Rasmussen Study) in the USA [13] and the German Risk Study [14] show that particular and overall risk curves for reactor power plants become very steep as the probability of an accident sequence decreases below about 10^{-6} per year. This behavior indicates relatively insignificant

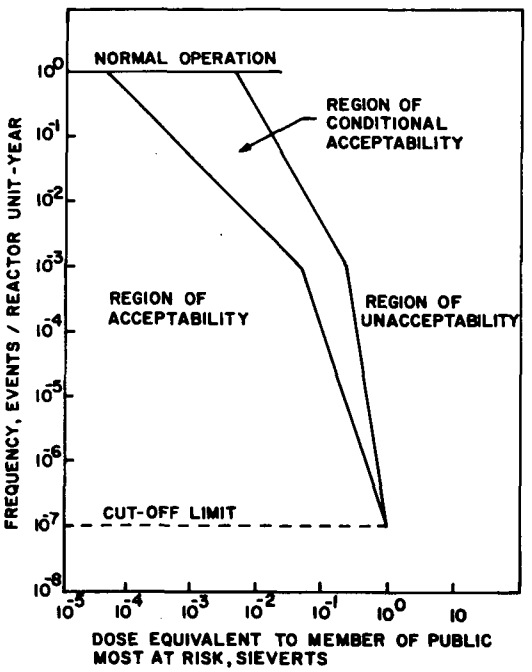


FIGURE 1. Risk Diagram for Safety Analysis

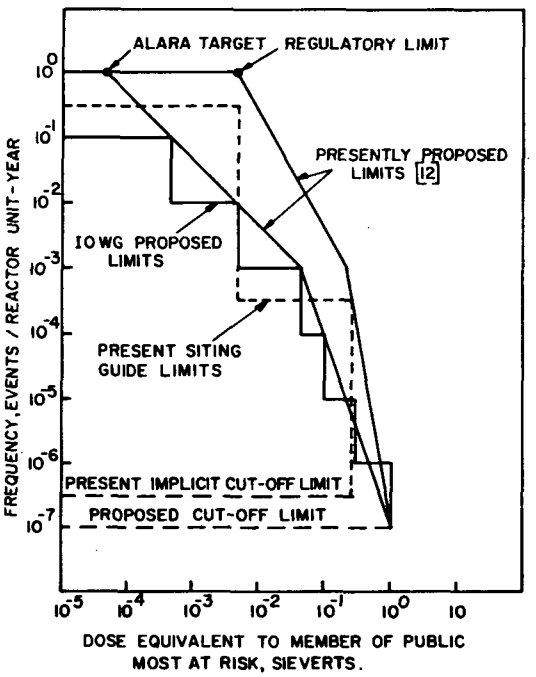


FIGURE 2. Comparison Between Risk Diagrams

contributions to overall risk from potential accident sequences of probabilities less than about 10^{-6} per year. (Note that these probabilities are associated with 100 reactors in the US study and 25 reactors in the German study.) This behavior also implies an upper limit to the magnitude of the consequences of any reactor accident which is not much greater than that associated with an event with a probability of 10^{-6} per year.

While no such comprehensive study of CANDU reactor risks has been undertaken, various studies of severe accident conditions in CANDU reactors indicate that there will be no fuel melting in a LOCA even with ineffective emergency coolant injection (e.g., [15]), which is not the case for a light water reactor. Thus, we would expect that the expected total probability of core melts would be less for a CANDU than for an LWR. Since the Reactor Safety Study and the German Risk Study show that there is no significant risk to the public unless core melting occurs, it is concluded that the overall risk associated with accident conditions in a CANDU will not be greater than that associated with accident conditions in an LWR. Therefore, the use of information from the American and German risk studies to establish safety criteria for CANDU reactors is justified.

A practical consideration in the stipulation of a cut-off limit is that the analysis of accident sequences of very low probability becomes extremely difficult and the results will be very speculative. Thus, it is doubtful that the analysis of such events would be meaningful; requiring such analysis could divert attention from more probable events which are the major contributors to the overall risk.

A social justification for the choice of a frequency of 10^{-7} per reactor year is that various investigations (e.g., [16,17]) have found that the public in general tends to be unconcerned with risks to the individual of the order to 10^{-6} to 10^{-7} per year.

The overall expected risk of reactor accidents will depend on the final definition of the accident sequence categories. However, it is expected that the target risk, conservatively calculated, will be of the order of 1 to 2 x 10^{-4} Sieverts per reactor year and that the maximum acceptable risk will be of the order of 2 to 3 x 10^{-3} Sieverts per reactor year. These figures must be compared to expected risks of normal operations which are 5 x 10^{-5} Sieverts per reactor year for the ALARA target and 5 x 10^{-3} Sieverts per reactor year at the regulatory limit (See Table IV).

TABLE IV

Expected Values of Risk

A) Normal Operation

Criterion	Risk, Sieverts/Reactor-year
ALARA Target	5.0×10^{-5}
Regulatory Limit	5.0×10^{-3}

B) Accident Sequences

Criterion	Risk, Sieverts/Reactor-year
AECB Siting Guide	1.75×10^{-3}
IOWG Recommendation	1.64×10^{-4}
ACNS-4, Lower Curve[a]	1.60×10^{-4}
ACNS-4, Upper Curve[a]	2.70×10^{-3}

[a]The risk lines in ACNS-4 are considered as complementary cumulative distribution functions; the integration is carried out according to specifications given in [18].

On population dose limits, the ACNS has not taken a definitive stand. It has recognized that the difficulty of calculating total population doses in a reliable manner precludes meaningful specification of population doses. It has felt, however, that population doses should be evaluated as one of the factors in the site selection process.

ECCS PERFORMANCE SPECIFICATIONS

In this section, the application of the approach recommended by the ACNS to the establishment of ECCS performance requirements is discussed.

Until recently, no detailed requirements were set by the AECB for the emergency core cooling system but in the Siting Guide [5], it was stated that "the emergency core cooling system must be capable of limiting the fuel and sheath temperature so that no more than a very small fraction of fuel is likely to fail in the event of the failure of any pipe or vessel in the primary system". In other words, the ECCS should ensure that there are no significant fuel failures from a LOCA.

The "dual" failure limit requires that in the event of a major rupture of the primary coolant circuit, the ECCS shall limit the amount of fission products released from the core to the extent that even with an impairment in the containment (i.e., a dual failure), the quantity of fission products released into the environment would not result in radiation doses to individuals and to the public greater than those stated in the Siting Guide.

It has been found, however, that for certain low probability events, the criterion of no significant fuel failures cannot be demonstrated with any reasonable degree of certainty given existing knowledge, current analysis techniques, and present emergency core cooling system designs. This fact was originally recognized during the Bruce "A" G.S. safety analysis, although the predicted releases of radioactivity were still small enough to result in an acceptably low public risk.

Therefore, it became necessary to develop more suitable criteria for emergency core cooling in CANDU nuclear plants. These criteria were to be consistent with the established Canadian approach to reactor licensing described earlier in this paper. This approach is contrary to the use of the type of criteria used in the USA and elsewhere of specifying conservative limits on fuel sheath temperatures and oxidation limits under loss-of-coolant conditions as predicted by certain defined analytical codes.

In July 1981, the AECB issued, for public comment, a document containing the requirements for ECCS for CANDU nuclear power plants [9]. Also in 1981, the ACNS was requested by the AECB to examine questions concerning emergency core cooling functions on CANDU reactors. The Committee published its findings in December 1981 [19]. Its recommendations have been accepted by the AECB and are now under consideration by AECB staff for implementation.

The ACNS recommendations are based on the general safety objectives states in ACNS-2 [11], as cited earlier in this paper. Specifically, the ACNS recommended that the primary requirement for the performance specification for the emergency core cooling system, as for any special safety systems, should be that the basic risk criterion for nuclear power plants, such as given in ACNS-4 [12], will be met.

In more detail, the ACNS recommended that:

1. *There should continue to be a requirement for a system whose sole function is to cool the nuclear fuel by injecting, circulating and removing the heat from an emergency coolant, in the event that the normal coolant is escaping through a*

breach in the primary heat transport system. This requirement should apply regardless of the availability and effectiveness or other heat removal paths.

Essentially, this statement means that an emergency coolant injection system is mandatory, even if analysis could show that none was required to meet the risk objectives. On the other hand, it should be noted that it is not necessary that the required system accomplish the emergency core cooling function entirely by itself.

2. *In order to verify compliance with the primary requirement of the ECCS, the estimation of risk due to failure of the ECCS should be done as realistically as possible taking into account any means by which heat might be removed from the fuel and the primary circuit while giving due consideration to the availability and effectiveness, at the time of the incident, of each heat removal path.*
3. *There should be secondary performance specifications (which include effectiveness standards) associated with the emergency core coolant injection and circulation system acting in conjunction with other means by which heat might be removed from the fuel and the primary circuit which, if achieved, would enhance the assurance that the primary risk-based requirement will be met. These secondary specifications need not be the same for all classes of events leading to loss of normal coolant.*
4. *The secondary specifications should be: a) for small breaks in the primary circuit having a relatively high probability of occurrence, fuel integrity should be maintained (i.e. there should be no fuel sheath failures that are a direct consequence of a LOCA); b) for large breaks in the primary circuit having a low probability of occurrence, fuel channel integrity should be maintained. More specifically, for feeder sized breaks, fuel sheath integrity should be maintained and that for all breaks, pressure tube integrity should be maintained.*

These recommendations are consistent with the established Canadian approach to reactor licensing. It should be noted that they put considerable emphasis on the exercise of judgement by the AECB staff in assessing the safety analyses, but that they permit the designers to utilize realistic analysis of accident sequences as well as conservative bounding analyses.

CONCLUSIONS

In this paper, we have briefly reviewed the historical development of reactor safety and licensing criteria in Canada. We have pointed out that, although there have always been certain deterministic requirements, the basic approach has been to recognize that a rational reactor safety analysis must be risk-based. The development of the risk-based aspect of Canadian reactor safety criteria has been traced, and the current work of the Advisory Committee on Nuclear Safety of the AECB, in consultation with AECB staff, the designers and the utilities, in the further rationalization of the Canadian approach to reactor safety has been described.

It is anticipated that consistent and concise recommendations on general safety requirements for Canadian power reactors will be issued in the near future.

ACKNOWLEDGEMENTS

The authors are members of the Advisory Committee on Nuclear Safety to the Atomic Energy Control Board. They acknowledge the contribution of other members of the Committee, but the responsibility of opinions expressed in this paper is entirely theirs and do not necessarily represent the Committee's views on the subject. The Committee's views are expressed through published documents such as [11] and [18].

REFERENCES

1. E. SIDDAL and W.B. LEWIS, "Reactor Safety Standards and their Attainment", AECL-498, Atomic Energy of Canada Ltd. (1957).
2. E. SIDDAL, "Statistical Analysis of Reactor Safety Standards", *Nucleonics* 17, 2, p. 64 (1959).
3. G.C. LAURENCE, "Reactor Siting in Canada", AECL-1375, Atomic Energy of Canada Ltd. (1961).
4. ATOMIC ENERGY CONTROL BOARD, "Reactor Siting and Design Guide" (1964).
5. D.G. HURST and F.C. BOYD, "Reactor Licensing and Safety Requirements", AECB-1059, Atomic Energy Control Board (1972).
6. ATOMIC ENERGY CONTROL BOARD, "Licensing Guide No 39. Requirements for the Safety Analysis for CANDU Nuclear Power Plants", AECB Consultative Document C-6 (1980).
7. ATOMIC ENERGY CONTROL BOARD, "Licensing Guide No 40. Requirements for Containment Systems for CANDU Nuclear Power Plants", AECB Consultative Document C-7/Rev. 1 (1982).
8. ATOMIC ENERGY CONTROL BOARD, "Licensing Guide No 41. Requirements for Shut Down Systems for CANDU Nuclear Power Plants", AECB Consultative Document C-8/Rev. 1 (1982).
9. ATOMIC ENERGY CONTROL BOARD, "Licensing Guide No 42. Requirements for Emergency Core Cooling Systems for CANDU Nuclear Power Plants", AECB Consultative Document C-9 (1981), C-9/Rev. 1 (1982).
10. "Proposed Safety Requirements for Licensing of CANDU Nuclear Power Plants", The report of the Inter-Organizational Working Group, AECB-1149, Atomic Energy Control Board (1978).
11. ADVISORY COMMITTEE ON NUCLEAR SAFETY, "Report ACNS-2. A Proposed Statement on Safety Objectives for Nuclear Activities in Canada", AECB INFO-0055, Atomic Energy Control Board (1981).
12. ADVISORY COMMITTEE ON NUCLEAR SAFETY, "Recommended Safety Requirements for Nuclear Power Plants" (Draft #6) (1982).
13. "Reactor Safety Study. An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants", WASH-1400 (1975).
14. "The German Risk Study. Summary", Federal Minister of Research & Technology (1979).
15. D.A. MENELEY and W.F. HANCOX, "LOCA Consequence Predictions in a CANDU-PHWR", in *Proc. IAEA International Conference on Nuclear Power Experience*, Paper No 145, International Atomic Energy Agency, Vienna (1982).
16. C. STARR, "General Philosophy of Risk-Benefit Analysis", Chapter 3 in *Energy and the Environment: A Risk-Benefit Approach*, Pergamon Press (1976).
17. L. CAVE, R.E. HOLMES and P.J. HOLMES, "Public Attitudes in Relation to the Risks Presented by New Technologies", in *Proc. Topical Meeting on Probabilistic Analysis of Nuclear Reactor Safety*, American Nuclear Society, Vol. 1 (1978).
18. D.C. COX and P. BAYBUTT, "Limit Lines for Risk", *Nucl. Techn.* 57, 120 (1982).
19. ADVISORY COMMITTEE ON NUCLEAR SAFETY, "Report ACNS-5. Emergency Core Cooling Systems in CANDU Nuclear Power Plants", AECB INFO-0068, Atomic Energy Control Board (1981).

SAFETY POLICY IN THE PRODUCTION OF ELECTRICITY

E. Siddall
AECL Engineering Company
Mississauga, Ontario
Canada L5K 1B2

ABSTRACT

When safety is properly understood, defined and quantified, it can be seen that the development of our present industrial civilization has resulted in a progressive and great improvement in human safety which is still continuing. Increased safety has come with increased wealth in such close association that a high degree of cause-and-effect relationship must be considered. The quantitative relationship between wealth production and safety improvement is derived from different sources of evidence. When this is applied to the wealth production from electricity generation in a standard module of population in an advanced society, a safety benefit is indicated which exceeds the assessed direct risk associated with the electricity generation by orders of magnitude. It appears that a goal or policy intended to confer the greatest safety benefit to the population would result in attitudes and actions diametrically opposite to those which are conventional at the moment.

Introduction

The generation and use of electricity on a large scale is a major feature of present day industrial civilization which has conferred the highest quality of life that man has ever known on those societies which have developed it. An important question of today has three related parts:-

What degree of safety is associated with the present electricity generating industry; what should the degree of safety be; and what policy should be followed to achieve it?

Perfect safety is not attainable in any human situation; a complete absence of safety is of no interest. A meaningful answer to the first two clauses of the question must therefore be quantitative, which in turn means that safety must be defined quantitatively and measured. As will be seen, properly defining the word "safety" appears to provide a logical basis for answering the three clauses of the question.

The definition and measurement of safety

Safety amounts to freedom from the risk of injury, illness and premature death. It is enough for most purposes to consider premature death alone, since it is so much more a serious matter, although the same kind of reasoning is equally applicable to injury and illness. Risk in the past is indicated by mortality, about which extensive, reliable and detailed information is available.

Management (reduction) of risk and mortality is a human activity of a special kind, in that it is concerned with a multitude of possible things which it is desired should not happen, and which very seldom do happen. This is in direct contrast to creative and productive human activities which are concerned with a narrow range of things which it is desired should happen, and which happen most of the time.

It is a fact of life, applicable to man just as it is to other forms of life, that the species survives but the individual does not. Mortality from every cause in man varies in various ways with age. Beyond middle life, say at age 40, a recognizable general aging sets in, consistent with a progressive reduction of robustness which in turn results in overall mortality roughly doubling every eight years. Fig. 1 shows the actual mortality rates (Canada 1979) as a histogram with dots to indicate an eight year doubling rate; it will be seen that the fit is good. For this reason total (crude) mortality in a group is of little use as a measure of safety; it tends simply to reflect the proportion of old people in the group. In epidemiology, this difficulty is partly circumvented by "age standardization", meaning correcting the mortality to an arbitrary age distribution in the population. More fundamentally, some kind of "weighting" of death according to age is necessary to distinguish between premature (and therefore potentially avoidable) death and death from age. Fig. 2 shows some possible weightings. Curve A amounts to assessing the number of years of life lost. Curve B roughly represents the material investment of the society in the person concerned and curve C is a smooth composite with constant weight up to age 40 and an "S" curve to zero at 80. For the purposes of this study of safety, the simplified form D has been used, where death is considered to be premature before age 65 and due to age beyond that. A few trial cases using line A have shown that the conclusions are broadly similar.

A single meaningful premature mortality figure for the study of safety is obtained if age standarization is based on a notional population in equilibrium with its age-specific death rates. Fig 3 shows the implications of this step. The two curves apply to population elements of 1 million people in equilibrium with British death rates for 1861 and 1964. It will be seen that the birth rate necessary to maintain the population fell from 23,400 to 14,100 py and the number surviving to age 65 rose from 7,700 to 10,600 py. This is the difference between a less safe and a more safe society.

The development of safety

Table I traces the change in mortality and therefore safety from primitive to developed societies. The last column is the percentage of new-born members who survive to age 65, which is a convenient and direct index of safety. The "premature deaths" column indicates the scale of effort needed if safety is to be appreciably affected (improved).

The first four lines are primitive societies separated from our present civilization by time and space. They were entirely without industry in the usual modern sense of the word. The fifth line is the arithmetical average and serves as a meaningful base level. Almost nobody survives to age 65 in such societies.

The succeeding lines show the unmistakeable progressive improvement as our industrial civilization progressed, using Britain, for which the earliest reliable data are available, and Canada as examples. The close similarity between these cases is often obscured because the average age of the population of Britain is considerably older than that of Canada. It will be seen that almost 80% of Canada's new-born now survive to age 65, but that there are still 2,685 premature deaths per year per million equilibrium population.

A few other cases are shown for interest. Portugal is typical of several countries which have improved very rapidly in the last few decades. Greece was safer than the USA in 1964 because the lower mortalities from road accidents and heart disease were dominant factors.

Fig. 3 is a plot of data from a number of "western" countries. In Fig 4, the smoothed curve is shown as applied to an average population of 400 million in about 1925 and 800 million in 1988. The enormous number of lives saved (premature deaths averted) in the past, and the expected future are shown, i.e. 280 million from 1875 to 1975 and 8 million from 1975 to the end of the century. (The immense influenza epidemic of 1919 and the London smog episode of 1952 disproportionately affected people of age greater than 65. The two major wars occurred mostly between points on Fig 3 and are in effect excluded).

It is a commonly held belief that industry has been harmful to people. In the century from 1875 to 1975, all the elements of industry which it is fashionable to regard as iniquitous in respect to safety were in full effect. Decision making was widely decentralized amongst individuals and small groups motivated by profit. Intense competition generally prevailed so that dollar efficiency was the foremost requirement, and most jobs went to the lowest bidder. Every kind of conspicuous technological disaster, such as the Tay bridge collapse, the sinking of the Titanic and the Vaiont dam disaster, a steady stream of lesser accidents to ships, trains and aircraft and millions of road deaths are all contained in the data. Despite all such adverse factors, it is clear that the overall consequences of a century of rapid industrial development have been overwhelmingly beneficial to human safety (see also Table II).

Fig 6 indicates the pattern of causes of premature death at the beginning and end of the century considered. From Fig 6 in particular it will be clear that systematic attempts to improve safety (reduce risk) must take the form of the management of a large number of separate efforts each directed at a relatively small risk. Ref. 1 discusses this problem and shows how it should be dealt with, the basic guide being that roughly 300,000 $ should be spent to save an extra statistical life. Table III, condensed from ref 2, shows the irrelevancy and futility of the exaggerated concern for some particular fashionable risks. It is surprising that the immense improvements in safety in our societies shown in Table 1 were achieved despite the almost total lack of understanding of the problems revealed in Table III.

Amongst the very large number of risks indicated in Fig 6, there were some which increased in the century 1875-1975. The "balance sheet" is roughly as shown in Table II. The net saving of life is the starting point, so that if any additional adverse component came to light, it would need to be compensated for by increasing the saving from "all other causes". Table II lacks precision for several reasons, including the fact that available data often does not enable premature and total deaths to be separated.

Safety, good living and wealth production

Just as the total risk to life has always resulted from the summation of a large number of small risks, so the saving of life which has accompanied the development of our industrial civilization has mostly arisen from the unobtrusive reduction or elimination of many different risks by a great variety of actions. Smallpox was dealt with by vaccination long before anything was known about viruses. Typhoid fever was slowly cut down by better sanitation. Polio yielded to sophisticated scientific method. The total accident toll has fallen, despite the increase in road deaths, because of changed attitudes.

However, these are only particular examples. Above all, safety has increased with "better living", and both have clearly followed the growth of available wealth. Wealth is the product of industry, which itself requires a large input of wealth. Industry amplifies or converts wealth; it seldom creates it from nothing. Fig 7 therefore best illustrates what happens. Of the wealth available in a particular time interval, a high fraction must be fed back into industry as capital or operating cost, but if this "loop" is kept viable, a substantial amount can be diverted to the end use of better living, of which safety forms a part. Improved safety results from direct efforts such as doctors, hospitals, medical research, fire brigades etc., but perhaps equally so from cleanliness, warmth and good nutrition amongst hundreds of other indirect factors. It is a semantic problem whether these activities and factors need wealth or constitute wealth, but in the hard realities of present day life, they always involve the availability of real money, that is, money backed up by the availability of all the things which people want to buy with the money.

The quantitative relationship between wealth and safety

When proper allowances are made for the variation of the real value of money with time, the production of wealth in a society is indicated by its GNP (gross national product), which is usually expressed in money. Another index is personal monetary income. Both of these indices are best considered per head of population.

Fig. 8 shows how the measure of safety derived above has varied with these measures of wealth in three cases.

In the Appendix, these cases and two others are analyzed to arrive at a correlation between wealth and life saving. It will be seen that a "middle" figure of one extra life saved per extra 3.3 Million $ (Cdn, 82) of GNP is derived. The extent to which there is a cause-and-effect relationship in this ratio requires much more investigation than has been possible so far. It is however proposed as a working hypothesis that, in the correlation between GNP and life saving, the cause-and-effect relationship amounts to 50%. This would mean, for instance, that if the real GNP in a society ceased to increase, the improvement of safety would continue but at a rate only one half of what has prevailed in recent years. On this assumption, a life is saved for $3.3 \div 5 = 6.6$ million $ (Cdn.82) of GNP in a given population.

Wealth production by the electricity industry

The reliable generation and distribution of electricity at low cost is a small but important factor in the modern industrial way of life. Canada's province of Ontario and the TVA area in the USA, for example, have obviously benefitted more than other similar areas which have lacked this energy source. To explore the quantitative effect on safety, a net contribution of 4.5 cents (Cdn.82) per KW hr produced and sold is used. This is proposed as appropriate if the electrical energy is provided as part of a society-wide industrial activity intended to create wealth and to result in better living, as has been the case in the western world over most of the last century.

The safety impact of electricity production on society

The preceding evidence and hypotheses can now be integrated. The whole population of an advanced society such as Canada or the USA can be considered to be made up of the necessary number of modules of 1 million each. The safety figures above are applicable if the population in each model is notionally assumed to be in equilibrium with its age-specific death rates, in this case those of Canada in 1982. Such a module would use, as an integral part of its industrial way of life, an electricity generating station of 2 GW capacity. At 70% capacity factor and using the figures proposed, this would contribute 552.2 million $ per year to the GNP of the module, which would then confer an indicated safety benefit from wealth production of

$$\frac{552.2 \text{ M\$}}{6.6 \text{ M\$}} = 79$$

lives saved per year (actually premature deaths averted which would otherwise have occurred).

The whole safety situation in this module of 1 million people is shown in Table IV. The reference risk levels are from Table I. The rich and poor risk levels are from ref 2 and fig. 8. In the case of coal, the direct risk from operating the station is arbitrarily shown as 20, this being towards the low end of a number of published estimates such as ref. 9. The "total nuclear" figure is taken from UNSCEAR 77 (ref 14). It mostly arises from mining and refining of uranium, and the number used is intended to reflect present and future rather than past practices. The nuclear accident risk is that proposed as a working hypothesis by the author in ref 8 , being in effect, the Rasmussen Study as modified in the light of the German Risk Study (Birkhofer), the whole being normalized to the actual record. The "actual record" figure shown is the TMI 2 case (33 person-Sv exposure) in 1900 reactor-years, at 50 Sv per total fatality (including all delayed), and assuming 2 reactors.

Discussion

Table IV hardly needs comment. The safety credit which is indicated seems high at first sight, but the numbers in the sections above surely lend credence to it; if the difference between urban rich and urban poor in an advanced country in one year can be as great as 2,077 per million equilibrium population-year, and the average mortality has fallen by over 14,000 per mep-year in a century, it is surely not excessive to credit the whole electricity source with 79 per mep-year. On the debit side, the nuclear accident figure as assessed is three orders of magnitude less than the indicated benefit and 4 1/2 orders of magnitude less than the average premature mortality which is what must be appreciably altered if safety is to be appreciably affected. The actual nuclear accident record is two orders of magnitude less still than the assessed figure.

Conclusion

If the preceding analysis is even roughly right, present attitudes and practices relating to the safety of electricity production, particularly nuclear, are diametrically wrong. It can be seen that, unless the total accident risk is orders of magnitude greater than the global average indicated, forcing a nuclear station to shut down or operate at reduced power, or delaying its start up, or reducing its net wealth production by forcing up capital or operating costs is likely to have an effect on society-wide safety which is exactly the reverse of what is intended, and much greater.

The safety goal (policy) at the present general state of technology should be to strive for maximum and most economical output even at a considerable increase in direct risk.

REFERENCES (Abbreviated List)

1. SIDDALL, E., "Risk, Fear and Public Safety, Report AECL 7404 (1981) AECL Engineering Co., Mississauga, Ontario Canada L5K 1B2

2. WIGLE, D.T., & Mao. Y, "Mortality by income level in urban Canada" Health and Welfare Canada, Ottawa, Ontario Canada K1A 0L2 (1980)

3. PRESTON S.H., KEYFITZ N., SCHOEN R., "Causes of death" - Seminar" Press. New York & London (1972)

4. Causes of death. Cat. 84-203 Annual. Statistics Canada, Ottawa. Ontario Canada K1A OT6 (years concerned)

5. Occupational Mortality 1970-1972 England and Wales. H.M. Stationery Office, London, England.

6. DOLL, R. & PETO, R. "The Causes of Cancer". J. Nat. Cancer. Inst. Vol. 66 No. 6 (June 1981).

7. World Almanac 1981 Newspaper Enterprise Association Inc., New York 1981.

8. SIDDALL, E., Safety, reliabiity & efficiency in the nuclear industry. Proc. Can. Nuclear Society Annual Conference, Toronto, June 9, 1982 Also AECL # 7535.

9. PORTER, A. (Chairman) Report of the Royal Commission on Electric Power Planning, Vol. 6., Queen's Printer of Ontario (1980).

10. LOVEJOY, C.O. & Al. Palaedemography of the Libben Site, Ottawa County, Ohio. Science, Vol. 198, pp 291-293 (1977).

11. CHAGNON, N.A. The Structure of human populations. Clarendon Press. Oxford, England (1972).

12. CHARBONNEAU' H., "Vie et mort de nos ancetres - etude demographique". Les presses de l'Universite de Montreal (1975)

13. U.S. Dept. of Commerce, Statistical Abstract of the United States 100th Edition (1979).

14. UNSCEAR 77, Sources and effects of ionizing radiation. United Nations, New York, 1977.

APPENDIX (Abbreviated)

Relationship between income or GNP & life saving (M $ equals million 1982 Canadian $) GNP per head taken as 1.47 times income per head (Canada 1982)

1. Primitive society versus Canada, 1982 (1 life saved per .4 m$)
   - linear relationship. This would be an appropriate figure for a country in an early stage of development.

2. Primitive society versus Canada 1982
   - assuming exponential relationship (simple diminishing returns, see fig. 4) 1 life saved per 2.1 M $

3. Canada 1977 versus 1979 Ref. 4 1 life saved per 7.0 M $
   (see GNP curve in fig 8).

4. Canada, mortality versus income group, ref. 2
   (see curve in fig. 8) 1 life saved per 3.4 M $

5. Britain, mortality versus social - economic (income)
   group ref. 5 (see curve in fig 8) 1 life saved per 1.1 M $

6. Assuming 10.6% of GNP spent on life-saving activities and 1 statistical life saved per 340,000 $ (CDN, 82) (see app 4 of ref. 2) 1 life saved per 3.2 M $

"Middle" figure from this list 3.3 M $

TABLE I
SAFETY - HISTORICAL

Society	Date AD	Ref	Per Year in 1 Million Pop in Eq. Birth	Premature Deaths	"Age" Deaths	% Survival To Age 65
Indians, Ohio	950	10	50,333	50,333	0	0
Aleuts, Fox Is.	1830	11	28,347	23,749	4,598	16.2
Eskimo, Labrador	1830	11	32,427	29,272	3,155	9.7
Indians, Amazon	c1965	11	64,516	64,516	0	0
Average Primitive			44,000	42,000	2,000	4.5
Quebec, White	c1690	12	27,832	21,904	5,928	21.3
Britain	1861	3	23,767	15,952	7,815	32.9
Britain	1901	3	21,519	13,377	8,142	37.8
Britain	1931	3	16,583	6,932	9,651	58.2
Canada	1931	3	16,601	6,724	9,877	59.5
Britain	1951	3	14,646	4,324	10,322	70.5
Canada	1951	3	14,647	4,277	10,370	70.8
Britain	1964	3	14,045	3,440	10,605	75.5
Canada	1965	4	14,043	3,483	10,560	75.2
Canada	1979	4	13,585	2,875	10,710	78.8
Canada (extrap.)	1982	-	13,487	2,685	10,742	79.6
Portugal	1920	3	16,998	18,852	8,146	30.2
Portugal	1964	3	15,424	4,915	10,509	68.1
Greece	1964	3	13,999	3,077	10,922	78.0
USA	1964	3	14,321	4,082	10,239	71.5

TABLE II
LIFE SAVING BALANCE SHEET 1875 - 1975
"WESTERN" (OECD) WORLD POPULATION (1925), c.400 Million

Net saving of life - fig. 5			280.0 M	
Debits	Increased cancer incidence except smoking & occupational (ref. 6)	13.9 M		
	Cancer resulting from smoking (ref. 6)	10.7 M		
	Road accidents (ref. 3)	4.5 M		
	Occupational cancer (refs 3 & 6)	1.6 M		
	Air pollution from coal	.9 M		
	Miners "black lung" & similar	.4 M		
	All man made "disasters" (ref. 7)	.1 M		
	Total debits	32.1 M		
Benefit	Reduction of mortality from all other causes	312.1 M		
	Net Benefit	280.0 M	280.0 M	

The net benefit is firm. All other figures are rough estimates.

TABLE III
SELECTED RISKS - CANADA 1979

ICDA Category		Rank	Deaths per year		
			Pre-mature Age<65	Other Age≥65	Total
410	Heart Attack	1	9,172	21,238	30,410
162	Lung Cancer	2	3,492	4,624	8,116
412	Chronic Heart Disease	3	2,797	16,108	18,905
174	Breast Cancer	4	1,559	1,522	3,308
E812	Motor Vehicle Collision	5	1,274	202	1,761
153	Intestinal Cancer	6	725	2,897	4,171
157	Cancer of Pancreas	7	709	1,330	2,055
250	Diabetes	8	681	2,206	2,915
E814	Pedestrian struck by vehicle	9	669	221	902
431	Cerebral Hemmorrhage	10	653	1,380	2,033
	Subtotal - 10 Major Categories		21,731	52,845	74,576
E891	Fire in Public Building	248			39
E840.2, E841.2	Major Aircraft Accidents (including DC 10's) (Long Average Estimate)	265			30
E921	Pressure Vessel Explosions (Average)	407			6
-	Nuclear Power (Long Average)	437			3.1
-	Asbestos in Buildings	612			≤ 0
-	Chemical Wastes (like Love Canal)	612			≤ 0
-	PCB's	612			≤ 0
-	Dioxins	612			≤ 0
-	Nuclear Spent Fuel (30 year Period)	612			≤ 0
-	Nuclear Waste (30 year period)	612			≤ 0
-	Plutonium	612			≤ 0
	Sub Total - 12 very minor cats.				78
	Total - All Categories				168,183

This Table is condensed from Ref. I.

TABLE IV

SAFETY IMPACT OF ELECTRICITY PRODUCTION

CATEGORY	ITEM		PREM. DEATHS PER MILLION EQ.POP.P.Y. INCURRED OR AVERTED	
Reference Points	Primitive Society		42,000	Est. Table I
	Britain 1875		17,000	Firm Ref. 3
The Real Safety Problem	Society-Wide Risks Levels Canada	Poor, Urban, 1971	4,018	Firm Ref. 2
		Average 1982	2,685	Firm Ref. 4
		Rich, Urban, 1971	1,941	Firm Ref. 2
Safety Credit	Indicated from Wealth Creation - 2 GWE Station		79	WH Text
Safety Debits	2 GWE Station Total Mortality - Coal		20	WH Note 1
		- Nuclear	1.3	Est.
	Nuclear Accident Risk - Assessed		.08	WH Ref. 8
		- Actual Record	.0007	Firm Text

WH - Working hypothesis proposed by author to fit evidence
Est-Estimate mainly by others.

Note 1 Ref. 9 gives "selected range" of 6.2 to 214 (for 2 GW)

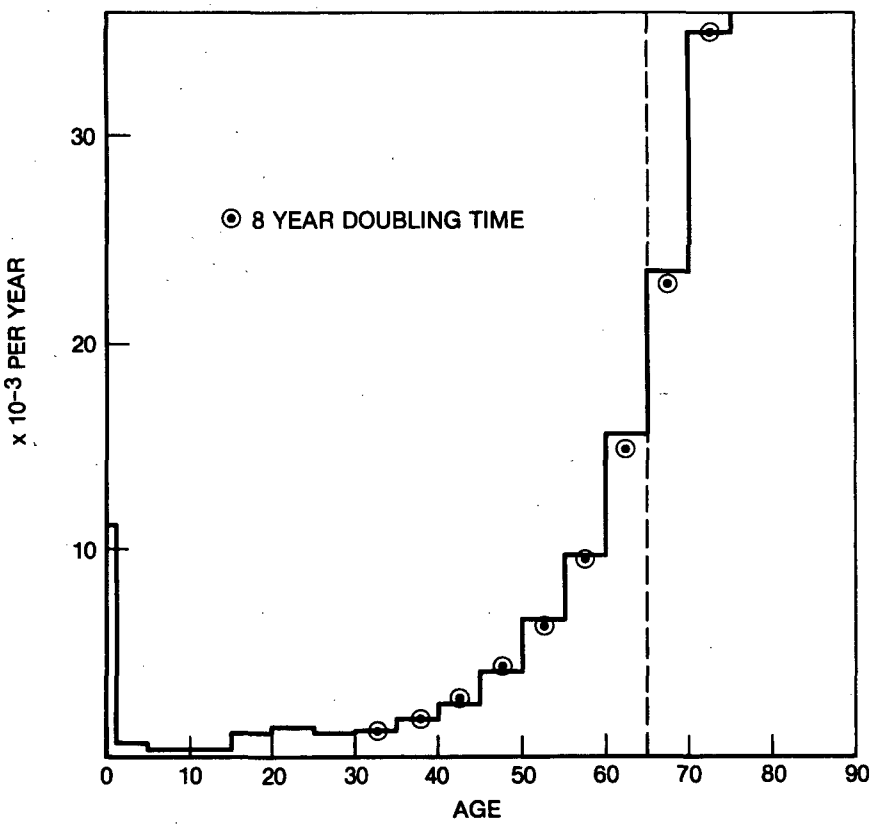


FIGURE 1 DEATH RATE VS AGE CANADA 1979

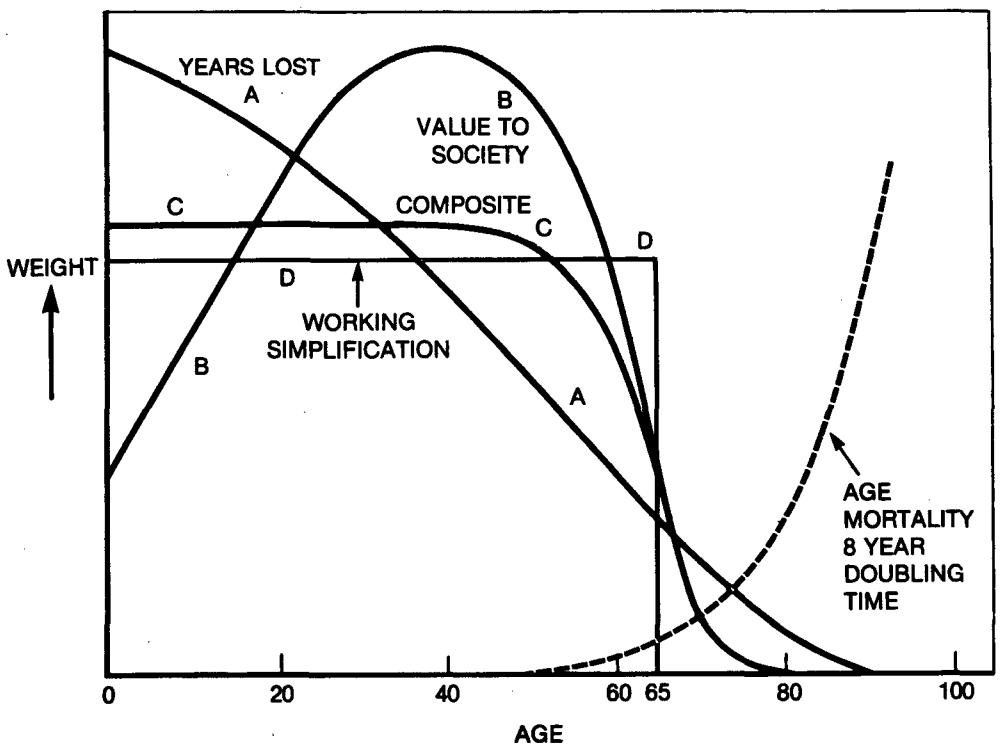


FIGURE 2 RELATIVE VALUE OF A LIFE SAVED

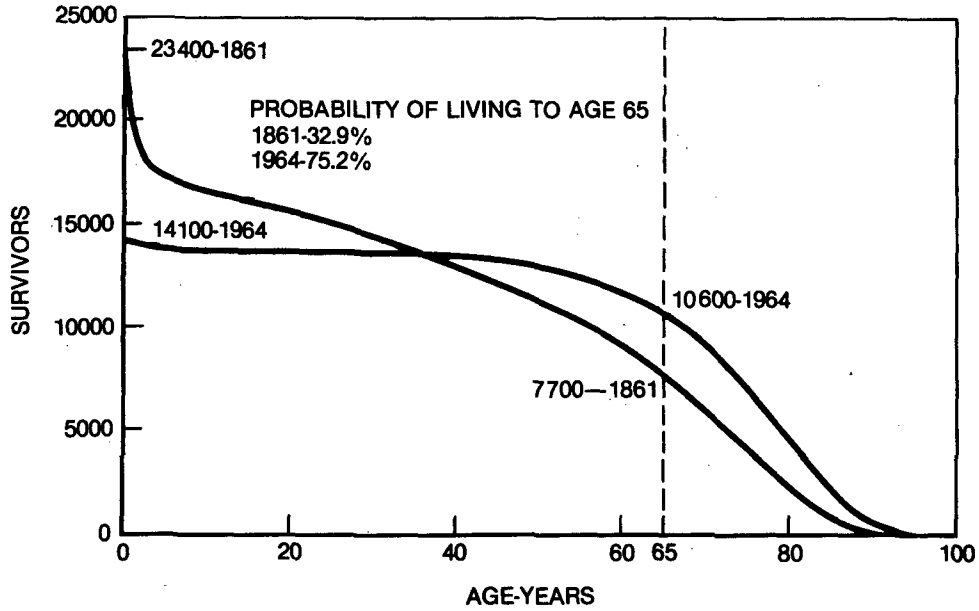


FIGURE 3 ONE MILLION POPULATION IN EQUILIBRIUM

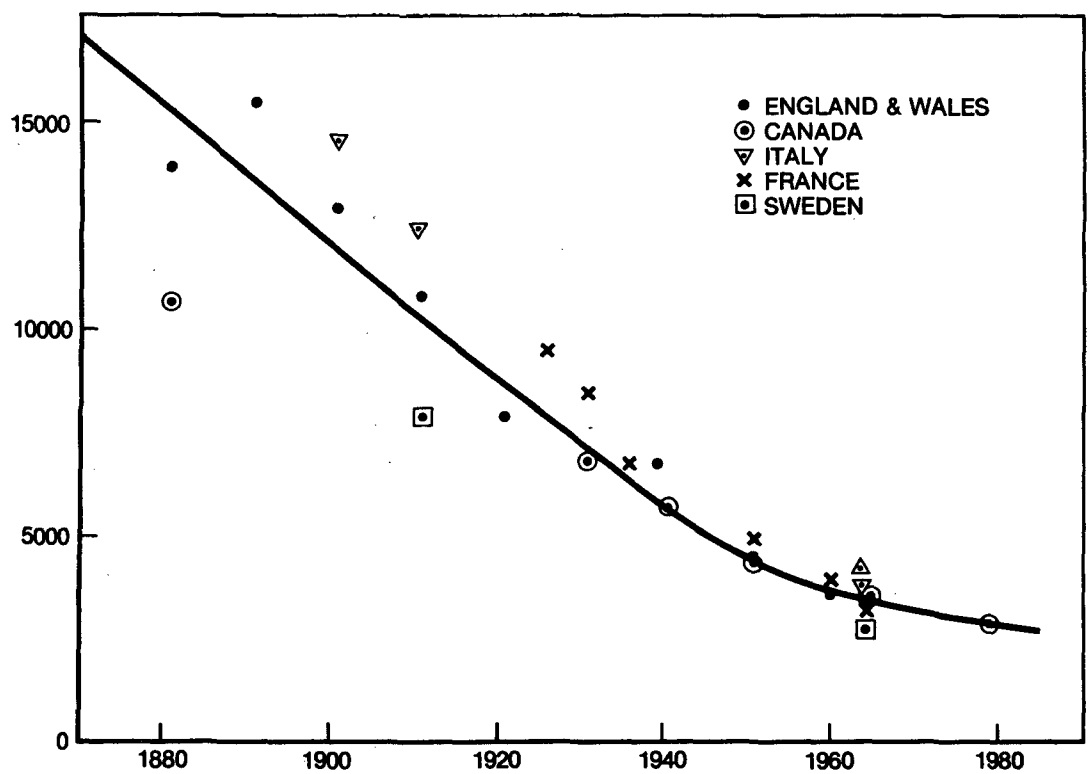


FIGURE 4 "WESTERN" WORLD — PREMATURE DEATHS PER YEAR PER MILLION EQ. POP.

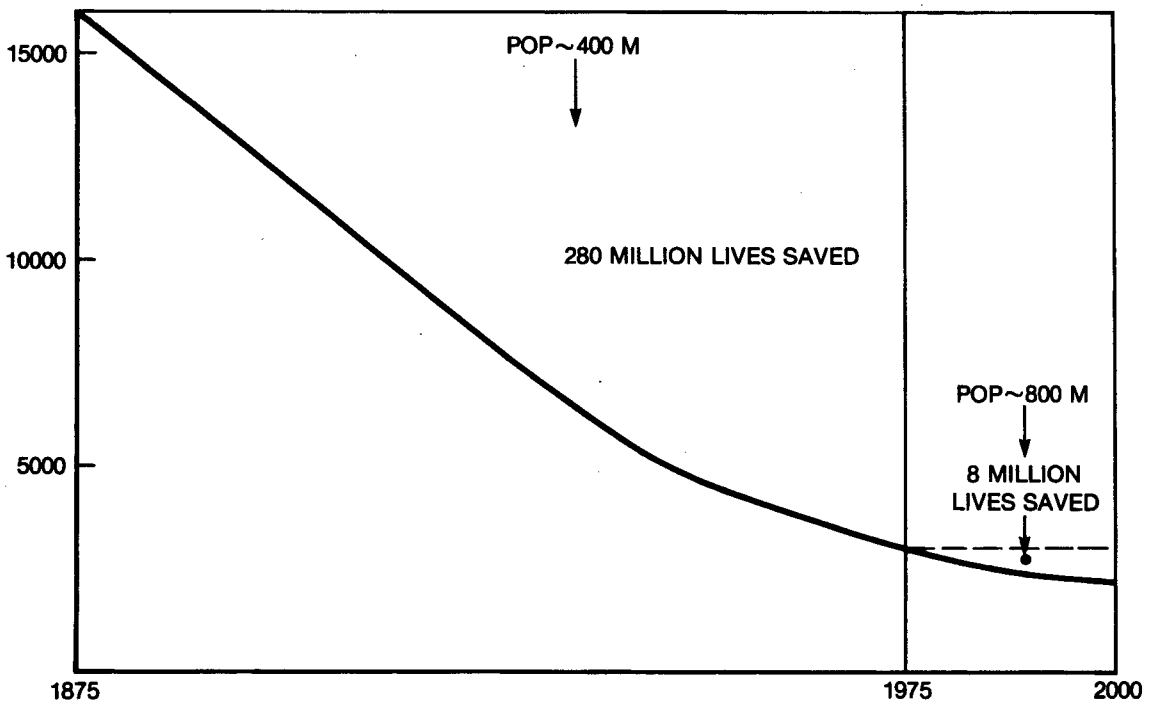


FIGURE 5 "WESTERN" WORLD — A CENTURY OF RISK REDUCTION

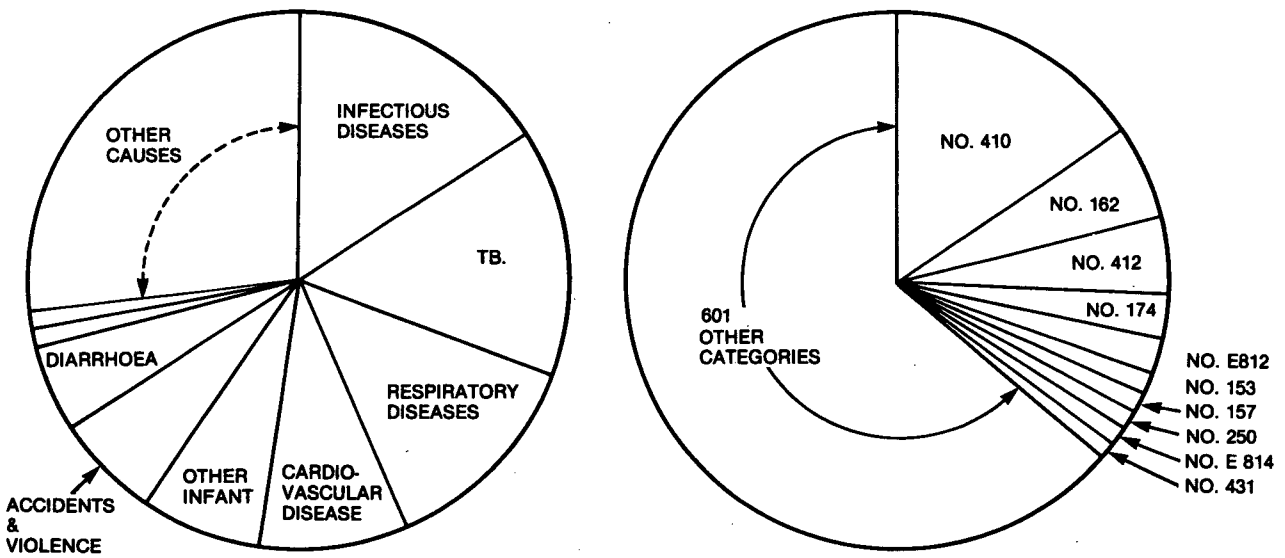


FIGURE 6 CAUSES OF PREMATURE DEATH

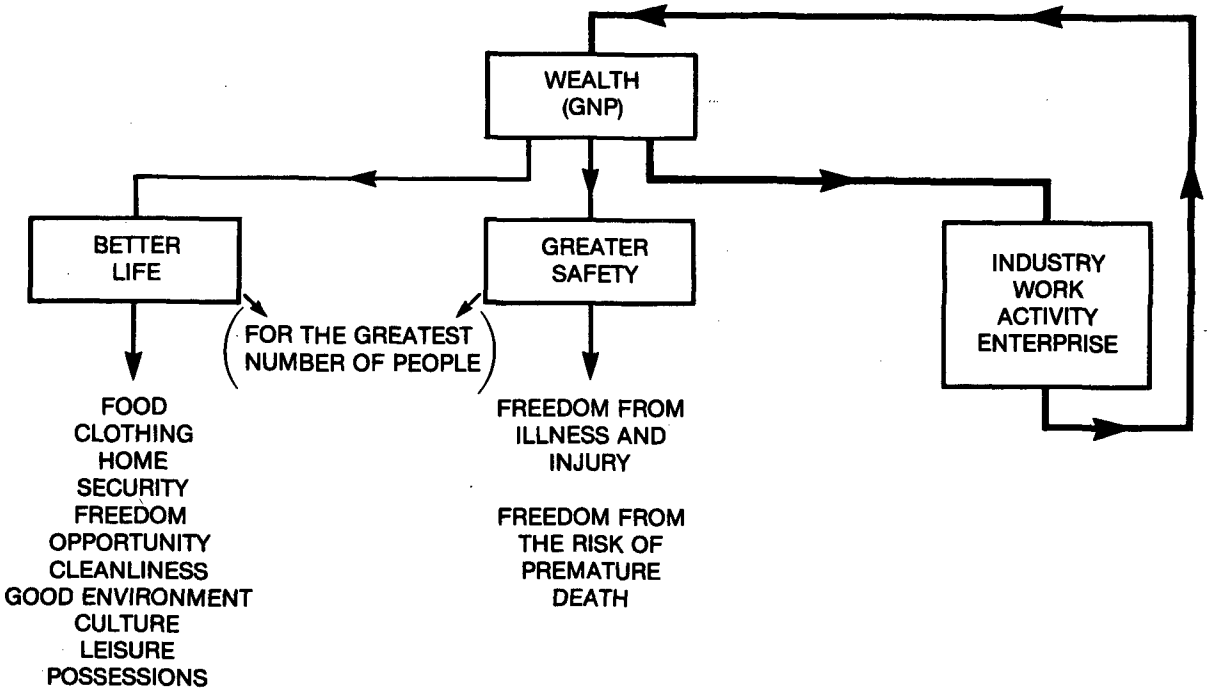


FIGURE 7 INDUSTRIAL CIVILIZATION 1675-1875-1975-ON.

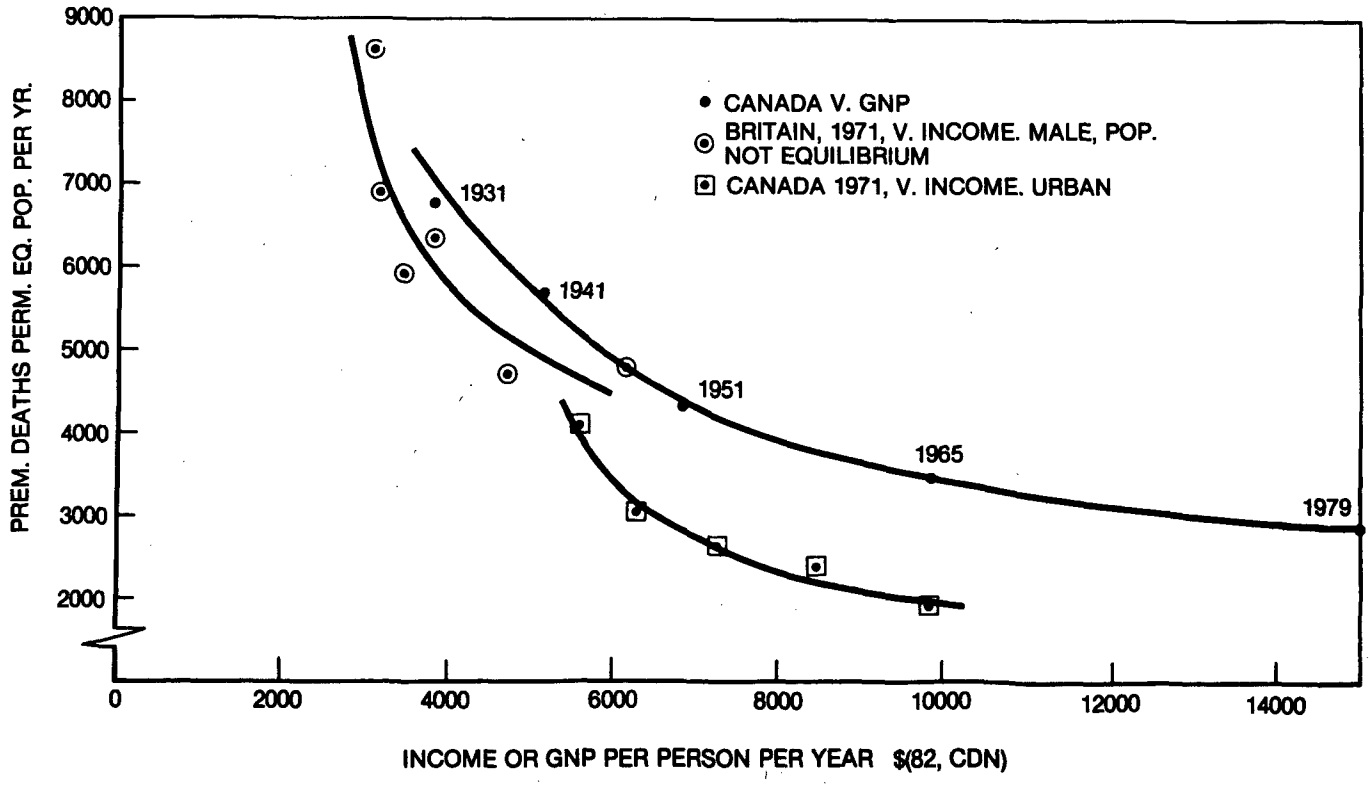


FIGURE 8 MORTALITY V. WEALTH

DEALING WITH UNCERTAINTIES IN EXAMINING SAFETY GOALS FOR NUCLEAR POWER PLANTS

W. R. Rish and J. J. Mauro

Ebasco Services Incorporated
Lyndhurst, New Jersey 07071, U.S.A.

ABSTRACT

Qualitative safety goals and provisional numerical guidelines for nuclear power plants have been proposed by the NRC for individual and societal mortality risks, large-scale core melt probability, and benefit-cost criteria for use in decisions on plant safety improvements.

A major problem encountered when attempting to demonstrate compliance with these goals is the numerous and significant uncertainties inherent in such analyses. A methodology is presented and demonstrated which gives explicit consideration to uncertainties when assessing compliance with quantitative safety goals for risks from airborne radioactive emissions from the routine operation of a typical PWR located at a representative U.S. site. A probabilistic method is used to examine the implications of uncertainties inherent to, (1) determining the radiation exposure limit required to meet a given mortality risk goal, and (2) estimating the individual and population doses and mortality risks from routine PWR emissions.

INTRODUCTION

The Nuclear Regulatory Commission (NRC) and the nuclear industry, represented by the Atomic Industrial Forum (AIF), have been working toward the establishment of quantitative safety goals for use in regulating nuclear power development. In February 1982 the NRC published for comment NUREG-0880, "Safety Goals for Nuclear Power Plants: A Discussion Paper" which contains proposed qualitative safety goals and associated numerical guidelines for nuclear power plant accident risks. Table I is a comparison of the numerical safety goal proposals.

The establishment of levels for these goals is only the first step toward implementing a regulatory program based on quantitative safety goals. It still remains to develop methods for demonstrating compliance with these goals. A major problem encountered when attempting to demonstrate compliance is the numerous and significant uncertainties inherent in such analysis.

This paper presents an example of the application of a methodology for giving explicit consideration to uncertainties when assessing compliance with the proposed quantitative safety goals for a typical nuclear power plant. The methodology used has been adapted from one developed and demonstrated by F. Owen Hoffman for nuclear power plant assessment[1] and by Granger Morgan and his colleagues for coal-fired power plant assessment.[2,3] The specific example chosen for examination is assessing compliance with individual and population risk goals for mortality risks from airborne radioactive emissions due to the routine operation of a typical PWR with minimal effluent controls located at a representative inland U.S. site.

TABLE I

COMPARISON OF QUANTITATIVE SAFETY GOAL PROPOSALS

SAFETY GOAL ELEMENTS	NRC-OPE	AIF
Prompt Fatality Risk	0.1% of U.S. Avg. Accident Risk	1% of U.S. Avg. Accident Risk
Latent Fatality Risk	0.1% of Background Cancer Risk	0.1% of Background Cancer Risk
Cost-Benefit Criterion	$1000/Man-Rem	$100/Man-Rem
Large Scale Core Melt Risk (Prob. Per Reactor/Yr)	1×10^{-4}	1×10^{-4}

The analysis is limited to five radionuclides which were judged to be the most critical with respect to mortality risks from routine emissions. These are: XE-133, I-131, SR-90, CS-137 and H-3.

The analysis is also limited to risks from routine operation of the plant. The proposed safety goals will most likely relate to risks from routine operation and accidents; however, the modelling techniques for estimating doses from routine emissions are well accepted and standardized, and the uncertainties involved are reasonably quantifiable, both of which facilitate the application of our methodology. Future work will be directed at applying the methods to estimating mortality risks from accidents, to be combined with the results presented in this study.

METHODOLOGY

In this study, a standard analysis of offsite doses and mortality risks due to routine airborne emissions from a PWR was performed; however, key uncertain model parameters were represented by probability distributions and a Monte Carlo simulation approach was used to propogate these uncertainties through the analysis. Each of the parameters required to perform a calculation of individual and population doses are described in Regulatory Guide 1.109.[4] The parameters considered to have relatively significant uncertainty are:

1) the average annual radionuclide release rates (Ci/yr),
2) the atmospheric dilution (CHI/Q) and deposition (D/Q) factors,
3) the transfer rates of radionuclides from soil to vegetation to milk, and
4) the inhalation and ingestion whole body equivalent dose conversion factors (rems/micro Ci).

Judgmental probability distributions representing uncertainties about each of these parameters were developed as inputs to the simulation in order to obtain probability distributions representing uncertainty about estimated doses. Figure 1 shows the cumulative probability distribution representing uncertainty about the annual average source term for SR-90 which was used as input to the calculation. Similar distributions were developed for each of the other four radionuclides examined. The median value of 10^{-3} Ci/yr was obtained using the GALE (Gaseous and Liquid Effluent) computer code for the base case plant being analyzed. The standard PWR assumptions, delineated in NUREG-0017[5], were used, and it was assumed that the plant has no effluent controls except for a 30 day hold-up capacity for gaseous wastes stripped

FIGURE 1

JUDGMENTAL PROBABILITY DISTRIBUTION REPRESENTING UNCERTAINTY ABOUT THE ANNUAL AVERAGE SOURCE TERM FOR SR-90

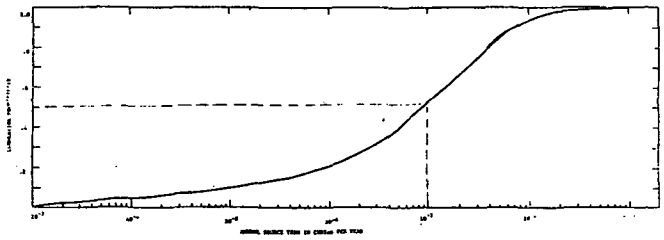


FIGURE 2

JUDGEMENTAL PROBABILITY DISTRIBUTIONS REPRESENTING UNCERTAINTY IN DISPERSION MODEL ESTIMATES OF ANNUAL DILUTION FACTORS

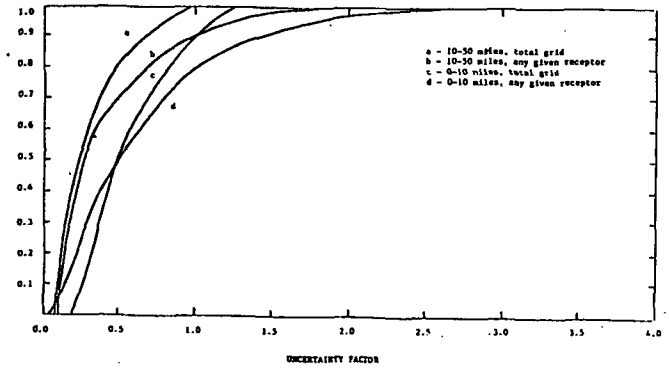


FIGURE 3

CUMULATIVE PROBABILITY DISTRIBUTION REPRESENTING UNCERTAINTY ABOUT MILK & VEGETATION TRANSFER COEFFICIENTS FOR SR-90

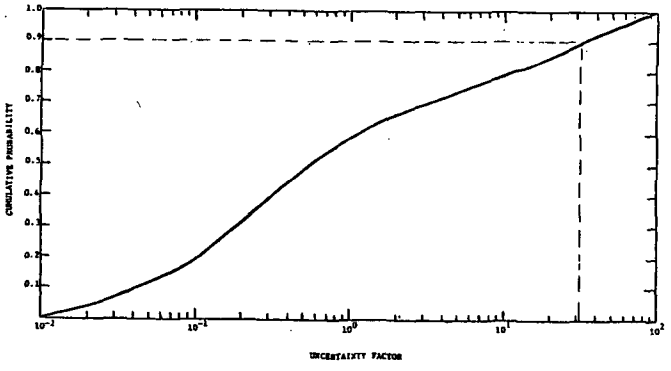
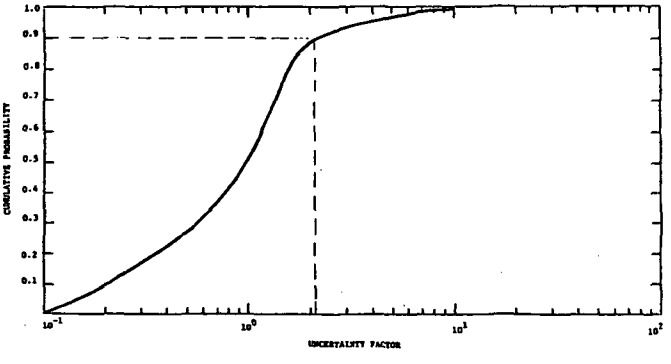


FIGURE 4

CUMULATIVE PROBABILITY DISTRIBUTION REPRESENTING UNCERTAINTY ABOUT DOSE CONVERSION FACTORS FOR ALL FIVE RADIONUCLIDES



from the chemical and volume control system. Median values for the release rate for each of the five radionuclides considered in this study were obtained in this fashion. The uncertainties in these values were obtained considering uncertainty in the various parameters of the GALE code and a review of operating data for 30 PWRs.

Figure 2 presents the distributions of dimensionless adjustment factors for uncertainties in predicted annual average atmospheric dilution factors used in calculating air and ground activities resulting from the emissions. These distributions were elicited from meteorological experts for the site analyzed using a formal elicitation technique. Curves a and c represent uncertainty about average annual dilution factors for the overall regions between 10 - 50 and 0 - 10 miles from the plant. These uncertainties relate to the calculation of population exposures. Curves b and d represent uncertainty about dilution factors for specific locations within 10 - 50 and 0 - 10 miles, respectively. These uncertainties relate to the calculation of the maximum individual exposure. Uncertainty about deposition factors (D/Q's) was assumed to be represented to first order by the distributions for dilution factor uncertainty in Figure 2. The strength of this assumption is subject to question; however, uncertainty about these meteorological parameters were found to be insignificant contributors to overall uncertainties about estimated annual average doses.

Figure 3 presents the cumulative probability distribution representing uncertainty about SR-90 transfer coefficients for transfer from soil to vegetation and from soil to pasture to milk. This and similar distributions for the other four radionuclides were developed from a study performed by F. Owen Hoffman.[1]

Figure 4 shows the probability distribution representing uncertainty about the dose conversion factors (inhaled and ingested) for the radionuclides considered. Note that these are equivalent whole body dose factors, which precludes the need to perform dose calculations for individual organs. The distribution represents uncertainty about the "best estimate" conversion factors provided in Appendix B of NUREG/CR-0150.[6] It was obtained by a review of existing data, largely that provided in ICRP-30.[7] The spread of the uncertainty is based primarily on uncertainty in absorption of inhaled and ingested material and uncertainty in biological half life.

Figure 5 presents the cumulative probability distribution representing uncertainty about the radiation exposure risk coefficient (fatalities per person-rem) for routine operation dose levels. The median or best estimate value selected is 10^{-4} and is based on BEIR-3[8] and ICRP-26.[9] The distribution of uncertainty provides for dissenting opinions, such as those described in BEIR-3, which claim that the risk could be as much as 10 times higher than current estimates. In addition, the distribution provides for the possibility that the mortality risk per rem at low dose rates, such as those associated with routine power plant operation, is zero. Though negative fatalities cannot be ruled out at these levels, it was not explicitly considered in this analysis.

Figure 6 represents another way to present the information provided in Figure 5. The information is presented in this form to facilitate comparison of current offsite dose criteria (such as 5 mrem/yr) with the proposed safety goals. For example, given an annual exposure of 5 mrem/yr, Figure 6 indicates that one may be 50% confident, given uncertainties in the risk coefficient, that the fatality risk is less than or equal to 5×10^{-7} per year. It also indicates that at 1 mrem/yr, one may be over 90% confident that the individual risk is less than 5×10^{-7} per year. It is important to recognize that there may be considerable disagreement among radiobiologists regarding the shape of Figure 5, and it would be instructive to develop a set of such curves in order to provide a more complete picture of the relationship between current offsite dose criteria and the proposed safety goals.

FIGURE 5

JUDGMENTAL PROBABILITY DISTRIBUTION

REPRESENTING UNCERTAINTY ABOUT

FATALITIES PER DOSE

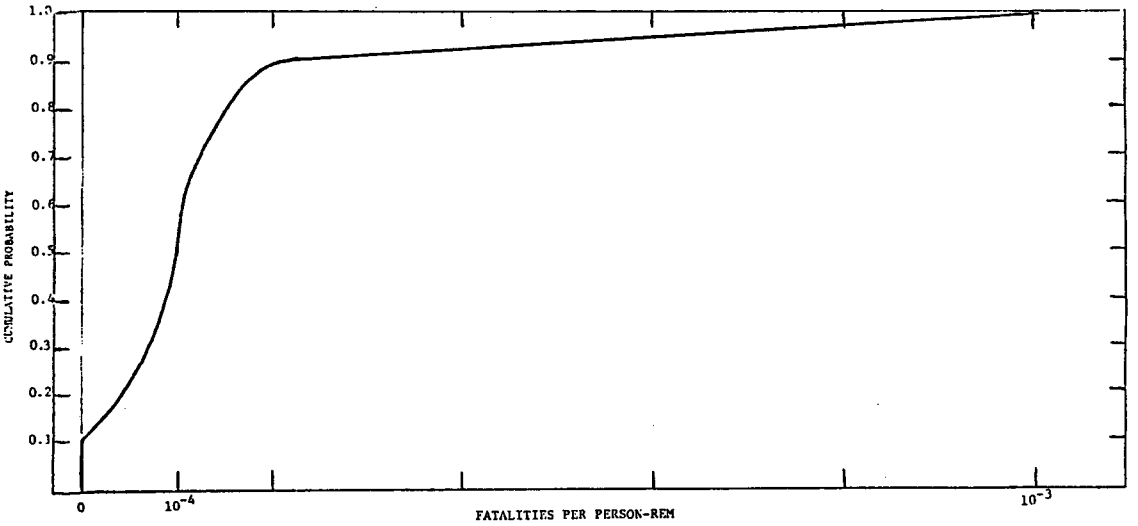
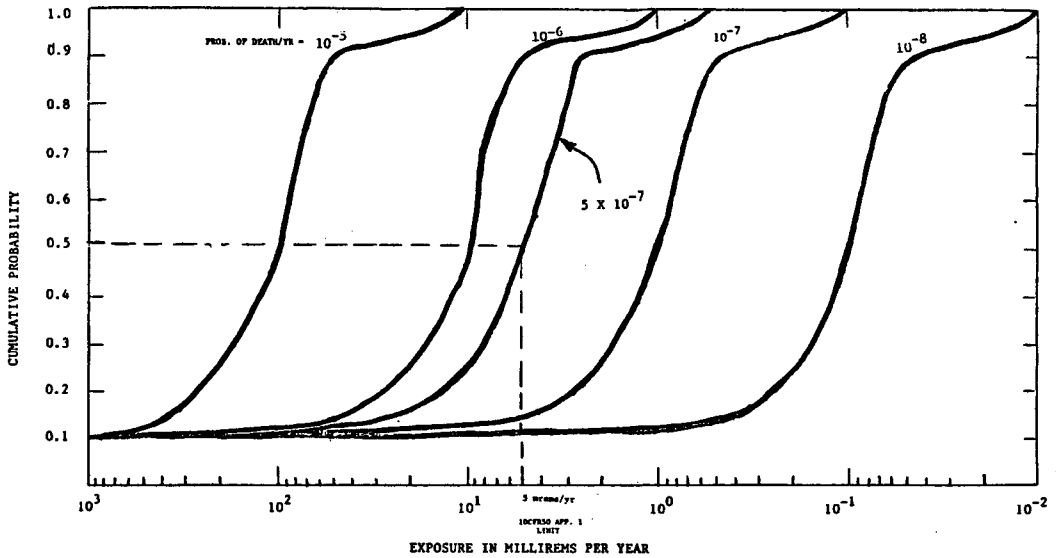


FIGURE 6

UNCERTAINTY IN MORTALITY RISK

FROM A GIVEN EXPOSURE LEVEL



RESULTS

Using the probability distributions presented above as inputs, a stochastic simulation of the dose calculation was performed to produce histograms of individual and population dose estimates. Values for each uncertain parameter were drawn using a selection procedure that yields the desired probability distribution for each parameter. The dose calculations were then done using these drawn parameter values. This process was repeated many times to yield a histogram of the dose estimations, approximating a probability distribution representing uncertainty about dose estimates from routine plant operation.

Figure 7 displays the resulting cumulative probability distribution representing uncertainty about the estimated highest annual equivalent whole body dose from the five radionuclides considered to an individual located at the site boundary. Note that Figure 7 shows that, for this base case plant with minimal effluent controls, one can be 90% confident, given the uncertainties modelled, that the individual dose is less than or equal to 400 millirems per year. Even without effluent controls one can be 25% confident that this plant meets the current offsite dose criteria of 5 millirems per year.

Figure 8 shows the uncertainty distribution for the estimated annual equivalent whole body dose from the five radionuclides to the population within 50 miles of the plant.

The distributions for the dose estimate uncertainties in Figure 7 and 8 were multiplied by the distribution for the mortality risk coefficient in Figure 5 to produce probability distributions representing uncertainty about individual and population annual mortality risks for routine airborne emissions from the base case PWR. These results are presented in Figures 9 and 10 for individual and population mortality risk, respectively. Note in Figure 9 that one can be 90% confident, given the uncertainties modelled, that the individual annual mortality risk due to routine emissions from the base case PWR is less than or equal to 5×10^{-5} per year, while the "best estimate", or median value, for individual risk is 2×10^{-6} per year. Figure 10 indicates that one can be 90% confident of less than or equal to about 3×10^{-3} population fatalities per reactor-year, with a median value of 1.6×10^{-4} population fatalities per reactor-year, from routine airborne emissions from the base case plant with minimal effluent controls.

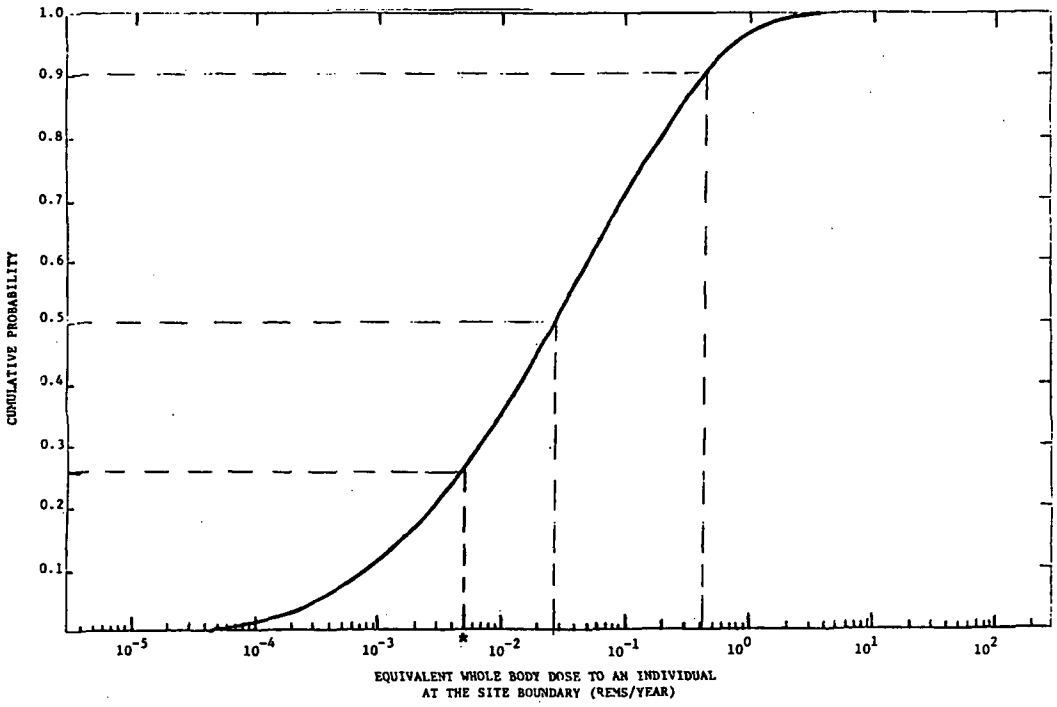
SUMMARY

Table 2 shows a summary of the results for annual individual and population dose and mortality risk uncertainties for routine emissions of five key radionuclides from a PWR with minimal effluent controls. The 90% confidence interval for individual dose estimate uncertainty spans about three orders of magnitude, from 1/100 to 20 times the median value. The 90% confidence interval for population dose estimate spans about two orders of magnitude, from 1/20 to 15 times the median value. Individual mortality risk estimate uncertainty ranges from 0 to 2×10^{-4} per year, while population mortality risk estimate uncertainty ranges from 0 to 3×10^{-3} fatality per year.

It is interesting to compare these results to similar probabilistic results for mortality risk uncertainty obtained for several equivalent capacity coal-fired power plants by Morgan, et al.[2] The coal-fired plant results were for 1000 MWe plants without scrubbers, and were for sulfur air pollution risks only. The reported uncertainty distributions for population mortality risk displayed median values of 4 to 32 fatalities per year and a range of uncertainty from 0 to 150 fatalities per year. These results for equivalent capacity coal-fired plant population risk are in excess of four orders of magnitude higher than those reported in Table 2. A direct comparison is not possible since risks from accidents are not included in Table 2 and risks from other air pollutants were not included in the coal-fired plant study. Nevertheless, the

FIGURE 7

CUMULATIVE PROBABILITY DISTRIBUTION REPRESENTING UNCERTAINTY
ABOUT THE ESTIMATED ANNUAL EQUIVALENT WHOLE BODY DOSE
TO AN INDIVIDUAL AT THE SITE BOUNDARY



*5 millirems/yr

FIGURE 8

CUMULATIVE PROBABILITY DISTRIBUTION REPRESENTING UNCERTAINTY
IN THE ESTIMATED ANNUAL EQUIVALENT WHOLE BODY DOSE
TO THE POPULATION WITHIN 50 MILES

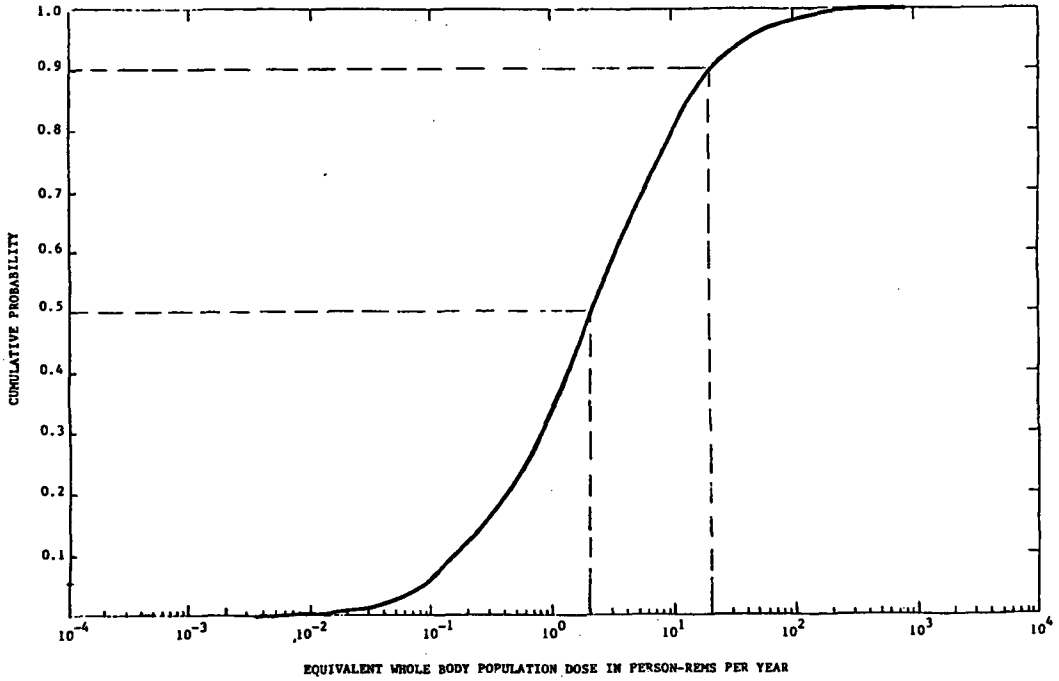


FIGURE 9

UNCERTAINTY IN INDIVIDUAL ANNUAL MORTALITY RISK
FOR ROUTINE AIRBORNE EMISSIONS FROM BASE CASE PWR

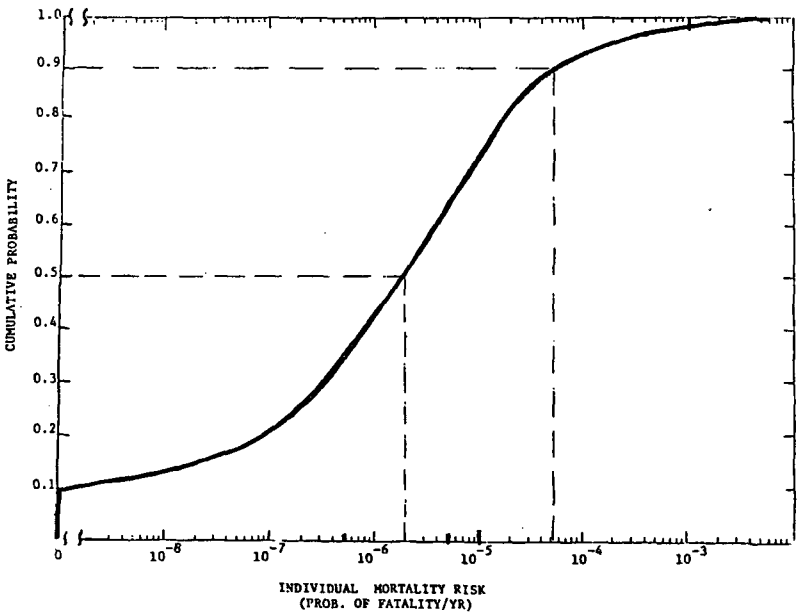
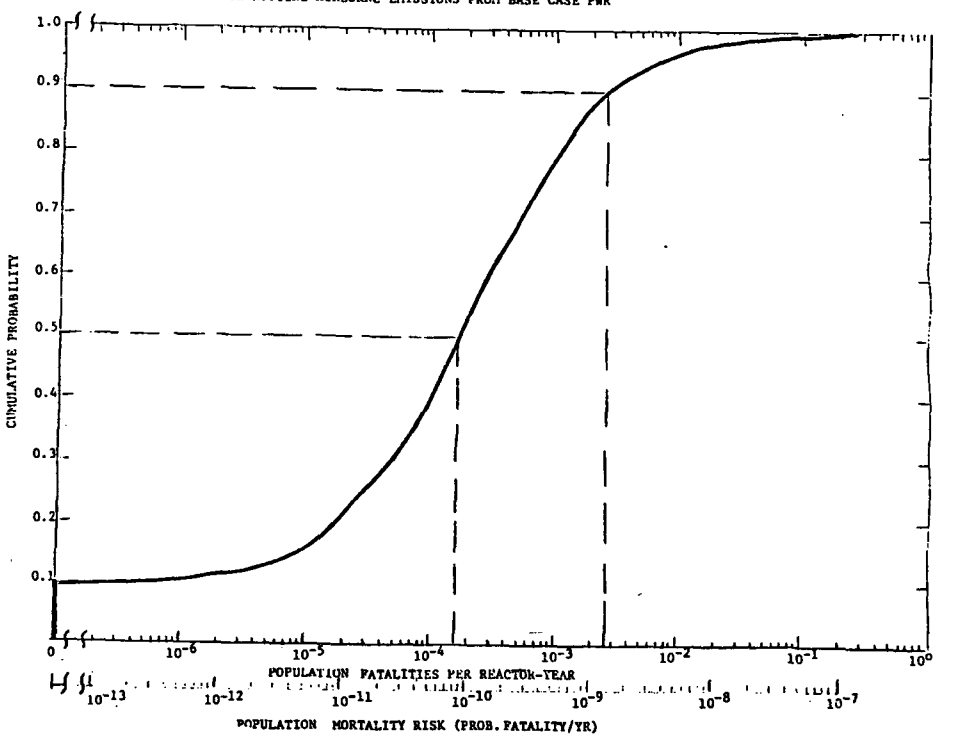


FIGURE 10

UNCERTAINTY IN POPULATION ANNUAL MORTALITY RISK
FOR ROUTINE AIRBORNE EMISSIONS FROM BASE CASE PWR



comparison indicates the possibility that more restrictive regulatory policies which might be adopted for routine nuclear plant operation, while in the interest of protecting public health and safety, might by virtue of excessive costs create an incentive to build fossil technologies which, even accounting for uncertainties, could result in much higher risks and thus be counterproductive to the intent of the policies.

TABLE II

SUMMARY OF DOSE UNCERTAINTY

		90% CONFIDENCE INTERVAL	
	50%	ABSOLUTE	FACTOR OF MEDIAN
INDIVIDUAL	30 mrems/yr	0.3 - 700 mrems/yr	$\frac{1}{100}$ - 20 (3 decades)
POPULATION	2 p-rem/yr	0.1 - 30 p-rem/yr	$\frac{1}{20}$ - 15 (2 decades)

SUMMARY OF MORTALITY RISK UNCERTAINTY

		90% CONFIDENCE INTERVAL	
	50%	ABSOLUTE	FACTOR OF MEDIAN
INDIVIDUAL	2×10^{-6} per yr	0 - 2×10^{-4} per yr	----
POPULATION	2×10^{-4} fatality/yr	0 - 3×10^{-3} fatality/yr	----

CONCLUSIONS

1. The methodology demonstrated in this study allows for the identification of sources of key uncertainties in calculating dose and risk estimates and provides a quantitative indication of the relative contribution of each uncertain parameter to the overall uncertainty in risk estimates.

2. The analysis shows in an explicit, quantitative manner that in order to answer the question "What is the risk?" one must first answer "How sure do you want to be?"

3. A quantitative safety goal assessment is not complete until a level of confidence in compliance is specified. This is <u>not</u> a recommendation that a level of confidence be specified in the proposed goals (such as "best estimate" or "90% confidence level"). The decision on level of confidence should depend on the possible costs and consequences of being wrong about risk estimates due to uncertainties, on a comparison of the costs associated with different levels of confidence (i.e., the cost of being more certain) and on cost-benefit analyses such as that presented in Reference 3. The analysis presented in this study can be done with a reasonable level of effort, and provides information on uncertainties which is in a form that can be quite useful for providing insights to regulatory decisions being made in the face of significant uncertainties.

4. A natural extension of the work presented in this study is to use these probabilistic mortality estimate results along with probabilistic estimates of control technology costs and efficiencies to derive probability distributions representing uncertainty in the optimum level of control, where optimum level of control is determined by minimizing the sum of control technology costs and human mortality costs at several assumed investment levels to avert a fatality. This analysis is now in progress, as well as a probabilistic estimation of PWR accident risk uncertainties done in the manner of the work presented here.

REFERENCES

1. F. Owen Hoffman, private communication (1982).

2. M. Granger Morgan et al, "A Probabilistic Methodology for Estimating Air Pollution Health Effects from Coal-Fired Power Plants", Energy Systems and Policy, 2, No. 3, p. 287 (1978).

3. M. Granger Morgan, William R. Rish, et al, "Sulfur Control in Coal Fired Power Plants: A Probabilistic Approach to Policy Analysis", APCA Journal, 28, No. 10, p. 993 (1978).

4. Regulatory Guide 1.109, Rev.1, "Calculation of Annual Doses to Man from Routine Releases of Reactor Effluents for the Purpose of Evaluation of Compliance with 10CFR50, Appendix I", USNRC (Oct. 1977).

5. NUREG-0017, "Calculation of Releases of Radioactive Materials in Gaseous and Liquid Effluents from Pressurized Water Reactors", USNRC (April 1976).

6. NUREG/CR-0150, Volume 3, Appendix B, "Estimates of Internal Dose Equivalent to 22 Target Organs for Radionuclides Occurring in Routine Releases from Nuclear Fuel Cycle", ORNL (1981).

7. ICRP-30, "Limits for Intakes of Radionuclides by Workers", Annals of the ICRP, Permagon Press (1979).

8. BEIR-3, The Effects on Populations of Exposures to Low Levels of Ionizing Radiation, Committee on Biological Effects of Ionizing Radiation, Division of Medical Sciences, Assembly of Life Sciences, National Research Council, National Academy of Science (1980).

9. ICRP-26, "Recommendations of the International Commission on Radiological Protection", Annals of the ICRP, 1, Part 3 (1977).

PROPOSED SAFETY GOALS FOR NUCLEAR POWER PLANTS

Forrest J. Remick, Director
Dennis K. Rathbun, Deputy Director
Jerry N. Wilson, Senior Policy Analyst
Office of Policy Evaluation
U. S. Nuclear Regulatory Commission

ABSTRACT

This paper presents the substance of a proposed policy statement for nuclear power plants issued by the United States Nuclear Regulatory Commission for public comment. The focus is on reactor accidents which may release radioactive materials from the reactor to the environment. Proposed qualitative goals and associated numerical guidelines for nuclear power plant accident risks are presented. The qualitative goals state that the risk of a nuclear power plant accident not be a significant contributor to a person's risk of accidental death or injury and that a limit be placed on the societal risks posed by reactor accidents. The significance of the goals and guidelines, their bases and rationale, and their proposed mode of implementation are indicated.

INTRODUCTION

In its response to the recommendations of the President's Commission on the Accident at Three Mile Island, the United States Nuclear Regulatory Commission (Commission or NRC) stated that it was "prepared to move forward with an explicit policy statement on safety philosophy and the role of safety-cost tradeoffs in the NRC safety decisions." In February of this year the Commission issued for public comment a proposed safety-goal policy statement [1] as a step in that direction.

The proposed policy statement focuses on nuclear power plant accidents which may release radioactive materials from the reactor to the environment. The safety goal does not include risks from routine emissions, from the nuclear fuel cycle, from sabotage or from diversion of nuclear material. The objective of the proposed policy statement is to develop goals for limiting to an acceptable level the additional, potential radiological risk which might be imposed on the public as a result of accidents at nuclear power plants.

In developing the draft policy statement, the Commission conducted two workshop discussions involving persons representing a broad range of perspectives and disciplines drawn from industry, public interest groups, universities, and elsewhere. The Commission also held one-day public meetings in Atlanta, Boston, Los Angeles, and Chicago to receive comments on its proposed policy statement. The Commission received 124 comments at the public meetings and 159 written comments were submitted. These comments and the proposed implementation plan submitted by the staff will be used by the Commission in their consideration of possible revisions in the Safety Goal policy statement. The policy statement and the implementation plan will then be combined into an integrated document which will contain the revised policy statement and implementation plan. The integrated document will also be sent out for public comment prior to final issuance of a Safety Goal Policy Statement for Nuclear Power Plants.

QUALITATIVE SAFETY GOALS

The Commission proposed adoption of qualitative safety goals supported by provisional numerical guidelines. The intent is to require a level of safety such that individuals living or working near nuclear power plants should be able to go about their daily lives without special concern by virtue of their proximity to such plants. Thus, the first proposed safety goal is:

- Individual members of the public should be provided a level of protection from the consequences of nuclear power plant accidents such that no individual bears a significant additional risk to life and health.

The Commission also proposed that a limit be placed on the societal risks posed by reactor accidents. This proposed goal has two elements. First, the risk of accidents should be such that, when added to the risk of normal operation, the total risk to the public from an operating nuclear power plant would be comparable to or less than the risk from other viable means of generating the same quantity of electrical energy. Second, the risks of accidents should be reduced to the extent that is reasonable achievable through the application of available technology. Thus, the Commission's second proposed safety goal is:

- Societal risks to life and health from nuclear power plant accidents should be as low as reasonably achievable and should be comparable to or less than the risks of generating electricity by viable competing technologies.

The comparative part of this goal is to be interpreted as requiring that the risks from accidents should be low enough that the total risks of nuclear power plants resulting from normal operation and accidents are comparable to or less than the total risks of the operation of competing electricity generating plants.

PROVISIONAL NUMERICAL GUIDELINES

General Considerations

Since the completion of the Reactor Safety Study, further progress in developing probabilistic risk assessment and in accumulating relevant data has led to recognition that it is feasible to begin to use quantitative reactor safety guidelines for limited purposes. However, because of the sizable uncertainties still present in the methods and the gaps in the data base, the quantitative guidelines are not substitutes for existing regulations.

Individual and Societal Mortality Risks

Two provisional numerical guidelines are proposed:

- The risk to an individual or to the population in the vicinity of a nuclear power plant site of prompt fatalities that might result from reactor accidents should not exceed one-tenth of one percent (0.1%) of the sum of prompt fatality risks resulting from other accidents to which members of the U. S. population are generally exposed.

- The risk to an individual or to the population in the area near a nuclear power plant site of cancer fatalities that might result from reactor accidents should not exceed one-tenth of one percent (0.1%) of the sum of cancer fatality risks resulting from all other causes.

The Commission proposed this 0.1% ratio of the risks of nuclear power-plant accidents to the risks of accidents of non-nuclear-plant origin to reflect the first qualitative goal, which would provide that no individual bear a significant additional risk. In addition, the 0.1% figure is consistent with the provision of the second qualitative safety goal, since calculations suggest that the risk of accidents at a nuclear power plant that is consistent with the proposed numerical guidelines would compare favorably with risks of viable competing technologies. The 0.1% percent ratio to other accident risks is low enough to support an expectation that people living or working near nuclear power plants would have no special concern due to the plant's proximity.

The individual risk is taken as the estimated probability of prompt or delayed fatality from a nuclear power-plant accident for an individual in the vicinity of the plant. The individual risk limit is applied to the biologically average individual (in terms of age and other risk factors) who resides at a location within one mile from the plant site boundary.

The individual mortality risk of prompt death in the United States is about 5E-04 per year for all accidental causes of death. Thus, on the average 5 persons out of 10,000 die annually as a result of accidents in the United States. The prompt mortality risk guideline, which would be set at 0.1% of this risk (i.e., 1/1000 x 5E-04 = 5E-07 PF/yr-site), would limit the increase in an individual's annual risk of accidental death by an increment of no more than 5 in 10,000,000 per year per site.

The individual mortality risk of death from all forms of cancer in the United States is about 1.9E-03 per year. Thus, on the average about 19 persons per 10,000 population die annually in the United States as a result of cancer. The delayed mortality risk guidelines, which would be set at 0.1% of this risk (1/1000 x 1.9E-03 2E-06 DF/yr-site), would limit the increase in an individual's annual risk of a cancer death by an increment of no more than 19 in 10,000,000 per year per site.

The area within one mile of the nuclear power-plant site boundary is proposed, since calculations of the consequences of major reactor accidents suggest that individuals in the population within a mile of the plant site boundary would be subject to the greatest risk of prompt death attributable to radiological causes. Beyond this distance, atmospheric dispersion and radioactive decay of the airborne radioactive materials sharply reduce the radiation exposure levels and the corresponding risk of prompt fatality.

In applying the numerical guideline for cancer fatalities as a population guideline, the statement proposes that the population considered subject to significant risk be taken as the population within 50 miles of the plant site. A substantial fraction of exposures of the population to radiation would be concentrated within this distance. This guideline would ensure that the potential increase in delayed cancer fatalities from all reactor accidents at a typical site would be no more than a small fraction of the year-to-year normal variation in the expected cancer deaths from non-nuclear causes. Moreover, the limit protecting individuals provides greater protection to the population as a whole. That is, if the guideline is met for individuals in the immediate vicinity of the plant site, the risk to persons much farther away would generally be much lower than the limit set by the guideline. Thus, compliance with the guideline applied to individuals close to the plant would generally mean that the aggregated societal risk within a 50-mile-radius would be a number of times lower than it would be if compliance with just the guideline applied to the population as a whole were involved.

Benefit-Cost Guideline

The following benefit-cost guideline is proposed for use in decisions on safety improvements which would reduce individual and societal risks below the levels specified in the first and second numerical guidelines in accordance with the "as low as reasonable achievable" (ALARA) principle:

- The benefit of an incremental reduction of risk below the numerical guidelines for societal mortality risks should be compared with the associated costs on the basis of $1,000 per man-rem averted.

This guideline is intended to encourage the efficient allocation of resources in safety-related activities by providing that the expected reduction in public risk that would be achieved should be commensurate with the costs of the proposed safety improvements. The benefit of an incremental reduction of risk below the numerical guidelines for societal mortality risks should be compared with the associated costs, including all reasonably quantifiable costs (e.g., design and construction of plant modifications, incremental cost of replacement power during mandated or extended outages, changes in operating procedures and manpower requirements.

Justification of proposed plant design changes or corrective actions would be related to the reduction in risk to society measured as a decrease in expected population exposure (expressed in man-rem) under accident conditions. To take into account the fact that a safety improvement would reduce the public risk during the entire remaining lifetime of a nuclear power plant, both the estimated cost of the improvement and the benefit (risk reduction) should be adjusted to reflect only the remaining years during which the plant is expected to operate (i.e., annualized).

Plant Performance Guideline

An important objective of efforts to reduce the public risk associated with nuclear power plant operation is to minimize the chance of serious reactor core damage since a major release of radioactivity may result from accidents involving core damage. Because of the substantial uncertainties inherent in probabilistic risk assessments of potential reactor accidents, especially in evaluation of accident consequences, the Commission proposes a limitation on the probability of a core melt as a provisional guideline for NRC staff use in the course of reviewing and evaluating probabilistic risk assessments of nuclear power plants. The proposed guideline is as follows:

- The likelihood of a nuclear reactor accident that results in a large-scale core melt should normally be less than one in 10,000 per year of reactor operation.

The Commission also recognizes the importance of mitigating the consequences of a core-melt accident, and continues to emphasize containment, remote siting, and emergency planning as integral parts of the defense-in-depth concept.

IMPLEMENTATION

The Commission's intention is that the goals and guidelines would be used by the NRC staff in conjunction with probabilistic risk assessments and would not substitute for NRC's reactor regulations. Rather, individual licensing decisions would continue at present to be based principally on compliance with the Commission's regulations.

The NRC staff has submitted a proposed action plan for implementing the goals and guidelines to the Commission for their review. This action plan would implement the plant performance guideline and the benefit-cost guideline as shown in Table I. The action plan considers the numerical guidelines as design objectives and proposes that the design objectives must be achieved in the design of new plants. The benefit-cost guideline would be used as one consideration in deciding whether corrective measures or safety improvements should be made in plants previously approved for construction or operation. Benefits would be measured in terms of estimated annual reduction in radiological risk due to reactor accidents. Costs of safety improvements would be annualized over the remaining plant life.

TABLE I

Implementation Proposal

Core Melt Frequency (per Reactor-Year) (Median Estimate from PRA based on internal events)		Action Required
		° New construction permit applicants must fix to meet Design Objective without regard to the benefit-cost guideline. ° Operating license applicants and operating reactors must fix to meet Operating Limit without regard to the benefit-cost guideline
0.001	(Operating Limit)	
		° New construction permit applicants must fix to meet Design Objective without regard to the benefit-cost guideline. ° Operating license applicants and operating reactors should fix to meet Design Objective subject to benefit-cost guideline.
0.0001	(Design Objective)	
		° New construction permit applicants should reduce core melt frequency subject to the benefit-cost guideline. ° Operating license applicants and operating reactors are OK unless individual sequences are greater than 0.00001. These individual sequences should be fixed subject to the benefit-cost guideline.
0.00001	(Reasonable Confidence)	
		° New construction permit applicants should reduce core melt frequency subject to the benefit-cost guideline. ° Operating license applicants and operating reactors are OK unless upper bounds (90%) of individual sequences are greater than 0.0001. These individual sequences may be fixed subject to benefit-cost guideline.

Because of the large uncertainties in probabilistic risk assessments, the staff has proposed that action levels be established at a factor of 10 above and below the design objective, as shown in Table I. Under the NRC staff's proposal, operation for an extended period of time would not be permitted if the operating limit is exceeded for core melt frequency. The NRC staff's implementation plan also proposes to use probabilistic risk assessments and safety goal guidance to; (1) identify generic safety issues that require prompt attention; (2) establish research and inspection priorities; and (3) develop and assess rules, standards, and guides.

In all applications of the goals and guidelines, the probabilistic risk assessments, if performed, should be documented, along with the associated assumptions and uncertainties, and considered as one factor among others in the regulatory decision-making process. The nature and extent of the consideration given to the numerical guidelines in individual regulatory decisions would depend on the issue itself, the quality of the data base, and the reach and limits of analyses involved in the pertinent probabilistic calculations. The proposed numerical guidelines should aid professional judgment, not replace judgment with mathematical formulas.

REFERENCE

1. Safety Goals for Nuclear Power Plants: A Discussion Paper. NUREG-0880. U.S. Nuclear Regulatory Commission (1982).

SAFETY GOALS FOR NUCLEAR POWER PLANTS: THE POSITION IN THE UNITED KINGDOM

R.D. Anthony
HM Nuclear Installations Inspectorate
Health and Safety Executive
London, England

ABSTRACT

This paper describes the approach to safety and licensing of nuclear power stations in the United Kingdom adopted by HM Nuclear Installations Inspectorate. The main objectives of the Inspectorate's Safety Assessment Principles for Nuclear Power Stations are outlined and their basis described in both qualitative and quantitative terms. Future trends are discussed and comparisons made with NRC's proposals for safety goals as set out in NUREG-0880.

SUMMARY

A number of detailed reviews of the approach adopted by HM Nuclear Installations Inspectorate (NII) to the safety and licensing of nuclear power stations in the United Kingdom have been presented on previous occasions, refs [1-4]. In this paper are summarised briefly the safety goals, both explicit and implicit, which are embodied in the NII's Safety Assessment Principles for Nuclear Power Reactors, ref [5]. Some suggestions are made about possible next steps in the development of workable safety goals. The approach adopted in the UK is then compared with that proposed in NUREG-0880, ref [6], and a number of observations are made on the NRC's proposed goals and guidelines.

INTRODUCTION

In the UK, if a generating board wishes to install and operate a nuclear power station it must obtain a licence from the Health and Safety Executive (HSE) under the Health and Safety at Work etc. Act 1974 and the associated relevant statutory provisions of the Nuclear Installations Act, 1965. HM Nuclear Installations Inspectorate (NII) is that part of the HSE which carries out this licensing and regulatory function under the relevant Acts. Hence, whilst the law makes it clear that the operator is responsible for the safety of the station, the Inspectorate is responsible for ensuring that an acceptable standard of safety is met, and an intending operator must satisfy the Inspectorate that it will meet the required standards in the design and operation of the station. This is done by putting forward a safety case for the plant. In turn the Inspectorate uses a set of safety assessment principles against which the plant is judged. These principles provide a framework and basis for our assessment work and, in addition, give guidance to designers and operators about our requirements.

The Inspectorate's approach to setting safety goals is, basically, rather different from that proposed in NUREG-0880 although the levels of safety actually achieved may turn out to be quite similar in both cases. Our principles require that any reactor system put forward for licensing should meet certain basic safety standards or limits and that all that is reasonably practicable should then be done to improve safety still further. These requirements are supplemented by a considerable number of detailed engineering principles, based largely on experience, which, amongst other things, aim to ensure that there is a high standard of integrity and reliability of key components, together with the necessary redundancy, diversity and attention to layout and segregation. The proper implementation of the engineering principles should ensure that the level of safety on the plant is as high as reasonably practicable and should give the Inspectorate confidence that the plant meets our basic principles and the five fundamental principles which are intended as an expression of the safety requirements and policy of the Inspectorate.

This policy may be summarised as follows. The first aspect is that, in normal operation, it should be shown in the safety case that the recommendations of the International Commission on Radiological Protection (ICRP), ref [7], and the requirements of the Euratom directive on radiological protection standards ref [8] are followed with regard to radiation exposures to persons on site and to members of the general public. The second aspect of the policy concerns the limitation of the likelihood and consequences of accidents. It should be shown that all reasonable steps have been taken to prevent plant failure or plant damage and thus to reduce the chance of accidents occuring and to reduce the consequences of any foreseeable accident should it occur.

Design, construction and operation are the key features in the safety of a plant. Thus the emphasis in the Principles is on ensuring a sufficient standard of engineering in the plant against fault conditions so that the chances of more severe accidents than the limiting design basis accidents are sufficiently remote that they do not need to be further considered in the actual design of the plant, although consideration may be given to additional design features, such as core catchers, secondary containment etc., to mitigate the effects of very severe accidents. It is considered that this is particularly important in that it should be possible to understand and describe the sequence of events in relation to design basis accidents, whereas there is a good deal of uncertainty about possible sequences beyond the design basis.

NUREG-0880 essentially starts at the opposite end from the NII principles by proposing safety goals and numerical guidelines for fault conditions that contain implicit judgements on what is an acceptable level of safety for nuclear plants compared with the normal risks of life and with the risks from competing electricity generating plants. The concept is then that the techniques of Probabilistic Risk Assessment (PRA) will be used to demonstrate the extent to which any particular plant meets the numerical guidelines. They will also presumably be used to identify areas in the engineering of the plant that require improvement. It is important to recognise that NRC intends the safety goals and numerical guidelines to supplement the existing regulations in 10 CFR Chapter 1 and not replace them.

In this paper detailed comment on the proposals in NUREG-0880 follow an explanation of the main aspects of the NII Safety Assessment Principles.

THE NII SAFETY ASSESSMENT PRINCIPLES

The NII Safety Assessment Principles, the third edition of which was published in April 1979, are based largely on the experience accumulated by NII staff over some 18 years of licensing commercial nuclear power stations in the UK. The principles fall into three broad categories. The first category comprises a set of fundamental principles upon which the second and third sets are based.

The second contains basic principles and a variety of overall objectives concerning the limitation of the radiological consequences of the operation of a nuclear reactor installation in normal and fault conditions. The third category is mainly concerned with those engineering features upon which the implementation of the basic principles depends. It should be noted that these principles are for guidance of staff in their assessment work and are not mandatory.

Fundamental Principles

The five fundamental principles are as follows:

1. No person shall receive doses in excess of the appropriate dose equivalent limit as a result of normal operation.

2. The exposure of persons shall be kept as low as is reasonably practicable.

3. Having regard to principle 2, the collective dose equivalent to operators and to the general public as a result of operation of the nuclear installation shall be kept as low as reasonably practicable.

4. All reasonably practicable steps shall be taken to prevent accidents.

5. All reasonably practicable steps shall be taken to minimise the consequences of any accident.

Clearly these principles are mainly concerned with radiological health detriment and do not directly address such effects as loss of land through contamination, hazards and costs of disruption as the result of accidents, etc. It is recognised that such effects may be important but they are difficult to factor into the engineering safety assessment of the plant.

Basic Principles

There are 19 basic principles which are to be used by the assessor in judging the extent to which the fundamental principles have been satisfied in any particular installation. These principles are based on experience and represent a level of protection against the radiological consequences of normal operation and fault conditions that should in most circumstances prove to be reasonably practicable. It is not a requirement that all the basic principles must be rigidly adhered to although it would be expected that any licence applicant would show good cause for any adverse departure from them. In several of the basic principles and in the subsequent detailed engineering principles there is a general requirement that the risks of exposure should be reduced as far as is reasonably practicable. The nature of this requirement necessitates case-by-case analysis and whilst a number of the principles are expressed in numerical terms no generally applicable numerical interpretation is appropriate. However, there comes a point at which further consideration of the case would itself be more costly in resources than any likely benefit. Assessors are therefore given guidance on the levels at which they can confine their studies to the validity of the estimates submitted to them and need not embark on detailed working aimed at establishing whether further improvements would be legitimately described as reasonably practicable. These assessment levels are not to be taken as targets for designers and operators, whose duties remain those of reducing risks as far as is reasonably practicable, and in any case of meeting any defined limits or requirements.

There are a number of assessment levels concerned with the radiological impact of the plant on operators and the general public during normal operation.

The three main principles are:-

1. The dose equivalent or dose equivalent commitment from routine or planned operations received by any occupationally exposed person on site whould be no more than one third of any of the appropriate annual dose equivalent limits.

2. The average dose equivalent or dose equivalent commitment from routine or planned operations received by all the occupationally exposed workers on site should be no more than one tenth of any of the appropriate annual dose equivalent limits when taken over a calender year.

3. The dose equivalent received by any person outside the site boundary from all sources originating on the site, including direct radiation and any discharged waste, should in any year be no more than 1/30 of the appropriate dose equivalent limits for the general public.

These principles are of importance since it can readily be shown that a significant part of the radiological risk from a nuclear power plant comes from its normal operation.

For fault conditions the assessment levels are summarised as in Table 1.

Table 1: Assessment levels for discrete fault sequences

Assessment Level	Frequency of occurrence, yr^{-1}
Up to 1/30 of the dose equivalent limit for any individual member of the public (eg. 0.17 m Sv (17m rem) whole body)	$> 3 \times 10^{-2}$
Up to the dose equivalent limit for any individual member of the public (eg. 5 m Sv (500m rem) whole body)	$3 \times 10^{-2} - 3 \times 10^{-4}$
Up to the Emergency Reference Level (ERL) (eg. 100 m SV (10 rem) whole body)	$< 3 \times 10^{-4}$
Exposures above ERL	As remote as reasonably practicable

In these assessment levels the ERL is used as the upper assessment level for accidents to give expression to our implicit safety goal that nuclear power stations should be so engineered that they need not be considered by the public as being different from non-nuclear stations. (The ERL is the level of dose at which countermeasures would need to be considered to ameliorate the exposure of members of the public). According to our principles, accident sequences giving exposures above the ERL should have a frequency of occurrence of less than once in 3000 years (corresponding to the conceptual UK "reactor programme" of 100 reactors, each having an operational life of 30 years) and the application of "as remote as reasonably practicable" means that the likelihood of such releases is much less than this in practice.

The main aim of our review of discrete fault sequences is to identify effective barriers to control the release of radioactive material to the environment. An effective barrier is essentially a set of engineered provisions which will prevent a release of activity for a given fault sequence or reduce the release to an acceptable level. The barrier defined in this way bears no simple relationship to physical barriers to the release of radioactivity, such as the fuel cladding or the coolant circuit boundary. For example, the elements of an effective barrier against an intermediate LOCA on a PWR include: reactor shutdown, containment isolation, containment fan coolers, containment spray, auxiliary feed to 2 out of 4 steam generators, steam relief, high head safety injection system and reactor heat removal by recirculation.

As an example of the application of the effective barrier approach, any discrete fault sequence for which the estimated release is greater than that which would lead to the ERL and for which the expected frequency of occurrence is less than about once in 10^3 - 10^4 years (but is not so small that it can be ignored) should be shown to be controlled by the presence in the plant of at least one effective barrier. A well-proven barrier is expected to have a reliability of about one failure in 10^4 demands and so it is clear that for a sequence leading to a release greater than the ERL our assessors would be looking for a frequency of occurrence of about 10^{-7} or lower. In addition to assessing the frequency and consequences of individual fault sequences the assessor is required to investigate the distribution of all foreseeable discrete fault sequences to ensure that all reasonable steps have been taken in the design of the plant to avoid a distribution of faults having frequencies or consequences such that their cumulative effect on the overall risk would be significant.

Engineering Principles

Finally there are nearly 280 principles which are concerned with various safety related aspects of plant engineering. These principles are expected, if met by the design, to lead to a plant which would be consistent with the Fundamental and Basic principles. Examples of these principles are the single failure criterion (SFC) applied to passive as well as active components (to ensure sufficient redundancy), the common mode failure (CMF) cut-off at one in 10^5 demands (to ensure sufficient diversity), the need for automatic protection in the first 30 minutes following a fault (to avoid operator error at this crucial time) and the need for attention to layout and segregation and protection against external hazards. Other principles refer to the need to use well established techniques and codes in the design of pressure circuit and structural components, the need to maintain coolable geometry of the fuel, and so on.

Discussion

It will be seen from the above discussion of accident criteria that our objective is to make the potential for the more severe accidents (i.e. releases significantly above the ERL) sufficiently remote that they may be discounted. This approach is consistent with the philosophy that (a) resources should be put into making the plant safe by good engineering so that people have confidence in it, (b) it should be possible at all times to demonstrate that the plant meets the safety standards and this becomes much more difficult if a degraded core situation is allowed to develop, and (c) there is a need to take account of the apparent situation that a single major nuclear accident causing a number of casualties is viewed as worse than a number of small accidents giving the same total number of casualties (risk aversion).

If the design has been well conceived and executed at the engineering level, and the principles of redundancy, diversity, layout and segregation applied, then this should achieve the safety objective, and be a sound basis for acceptance and it would not always be reasonably practicable to go further than this because of the increased complexity that is introduced which brings its own problems in terms of adverse systems interactions and difficulty in describing and understanding what would happen in fault conditions. Hence meeting the engineering principles produces a standard that, so far as it can be quantified in terms of risk, is at least comparable with attempts based on the risk approach alone, and gives greater confidence.

However, we do recognise the need to go further than the design basis accidents to explore what happens next, in case a sudden change in consequences, at high level of risk, occurs which could or should be further protected against. After that, estimation of the probabilities and consequences of severe accidents has in our view only limited use in terms of plant safety.

Looking to the future, a number of objectives might be put forward which would help to both define and achieve safety goals.

It is clearly necessary to refine the methodology so as to include systems interactions and human error for example, and to improve the data base so that there can be confidence in the way the plant is described and in the numbers which result from the calculations. This applies to the radioactivity release and dispersal calculations and the dose/risk relationships for those exposed as well as to the plant itself.

We should aim for a high standard of design and engineering and an improved understanding of plant performance in normal and fault conditions so that there is confidence that the safety principles and criteria are met. This should produce a design which will be well proven, which can be repeated as a standard design and in which the likelihood of a severe accident will have been made sufficiently remote as to be virtually discounted.

We should then be in a better position to estimate the risk from the plant, on any given site, so that this may be compared with agreed criteria on risk to the population, though what these should be is of course the subject of this debate. Comparisons can be attempted in cost-benefit terms or in terms of what are apparently acceptable risks from other industries, though in the UK we do not at present have any formal guidance on these aspects.

In the NII, we have gone no further than our accident criteria, as has been described above, though we have in the past considered the use of a guideline known as "$\sum$ p Ci" (the sum of the product of frequency per reactor or station operating year of the fault sequences and the releases which result, eg. measured in curies of iodine 131), where this should not exceed some number chosen as a measure of overall risk. Back in the 1960's this figure was $\sum$p Ci = 12, but more recently it has been suggested that it should be closer to 1. At this level the risk from accidents is not very different from the risk from releases arising from normal operation of the plant, and this in itself is a worthwhile goal to aim for.

NUREG - 0880 : SAFETY GOALS FOR NUCLEAR POWER PLANTS

Introductory remarks

The formulation of safety goals for nuclear power plants as formulated in NUREG 0880 is a significant step.

In both the qualitative safety goals and the numerical guidelines NRC have attempted to express what they believe to be the level of risk from nuclear plants that should be acceptable to the US population at large. This will have implications not only for the US but also for all other countries with commercial nuclear power plants. Further, the implicit judgements on an acceptable level of safety inherent in such goals will have ramifications in other, non-nuclear industries. NRC have clearly stated that they intend to adopt a cautious stance towards the use of these proposed goals in the regulatory process and we believe that this caution is important because, once the goals and guidelines have been endorsed, they are likely to be endowed with the mantle of the regulatory requirements.

General Comments

The construction of the discussion paper lays undue emphasis on accidents as the major component of the risk to members of the public from a nuclear power plant and it does not include the contribution from routine radioactive releases during normal operation. In our opinion any valid estimation of the risk from a nuclear power plant should include the risk from normal operational releases as well as the risk from accidents.

The way the safety goals and numerical guidelines are developed in the discussion paper puts considerable emphasis on low-probability, high release events (this is particularly evident in the Plant Performance guideline), with less attention being given to accidents within the design basis. As explained earlier, we consider this emphasis to be misplaced. The public should be reminded that the aim of reactor design is to prevent any accidents beyond the design basis occurring. Having made that point the paper should then go on to point out that accident sequences beyond the design basis need to be analysed to ensure that there is no sharp escalation in the predicted consequences of such remote fault sequences which would make an unacceptable contribution to the overall risk.

Further, it needs to be stressed that the proposed goals and guidelines are to some extent arbitrary and may need to be revised, in either direction, as understanding of the social acceptability of risks improves and the quantification of these and of other, non-nuclear risks increases. We feel there is a danger that the public might be misled into believing that the nuclear industry has a tool, in PRA, which will allow it to demonstrate unambiguously that the goals and guidelines have been satisfied for any particular plant. There should be a clear recognition of the many uncertainties involved in showing that any particular plant satisfies the quantitative guidelines. Thus with the state of the art as it is at present the demonstration of the extent to which the safety goals and guidelines are met would be expected to be relatively inaccurate.

Our final general comment is that the proposed safety goals and guidelines are too restricted in the detriments they consider. If they are to deal with the totality of the risk from a nuclear plant they should also include:

(1) non-fatal health effects

(2) contamination of land by activity released in an accident

(3) loss of livelihood of people evacuated or relocated

(4) the costs resulting from the loss of the plant which can be much greater than the simple cost of the lost electrical capacity, as TMI-2 showed, and can have wide-ranging effects on the progress of the whole nuclear power programme.

Specific comments

(1) Safety goal 1: we see no particular problems with this goal, apart from the difficulty of demonstrating whether or not this goal, or goal 2, has been met for any particular site.

(2) Safety goal 2: we would have no difficulty in principle in accepting the first part of this goal but we consider that the second part needs careful consideration and possibly some rewording. It should be made clear whether the whole nuclear cycle (of which the nuclear power plant is only one component) is being compared against the entire chain of facilities required to generate electricity by "a viable competing technology", or whether it is intended that the nuclear power plant should be compared against the non-nuclear power plant. If the latter is what is meant, it may be difficult to show that societal risks from nuclear power plant accidents are comparable to or less than those from non-nuclear power plant accidents, see for example ref [9]. We should like to see evidence provided to demonstrate that such risks are, in fact, comparable.

(3) Numerical guidelines 1 and 2: we note that the risks from reactor accidents are being compared with the risks to which the public is exposed from all other sources, both "voluntary" and "non-voluntary". It is frequently suggested that a distinction should be made between "voluntary" and "non-voluntary" risks, and that nuclear risks should perhaps be compared with the sum of other non-voluntary risks. However, it is often difficult to draw an unambiguous distinction between "voluntary" and "non-voluntary" risks.

The maximum levels of risk to the public, quoted in numerical guidelines 1 and 2, are considered to be reasonably consistent with those that might result from a nuclear power plant in the UK. However, we see the need for NRC to have sufficient evidence available to demonstrate that these guidelines implement that part of Goal 2 which requires that the risks from a nuclear power plant be as low or lower than those of a conventional plant. We note that the limits protecting individuals provide even greater protection to the public as a whole; this is worth emphasising since adverse comments may be received about the application of a 1 mile cut-off for delayed fatalies. Another consequence of this is that the numerical guidelines do not, in fact, specify a societal mortality risk even though they claim to do so.

Finally, it is noted that "the individual and societal mortality risk guidelines should be applied on a per-site basis". This will lead to tighter requirements being imposed on plants at multi-unit sites than at single-unit sites and could lead to problems where there is an existing, operating reactor on a site proposed for a new plant.

(4) Benefit-cost guideline: we agree with the general approach that decisions about reducing societal risks below the levels specified in the numerical guidelines should be quantified, as far as possible, in accordance with the ALARA principle. However, we consider that the most careful consideration should be given to the consequences of adopting the monetary value proposed. This would appear to imply a cost per life saved more than an order of magnitude greater than the average value associated with other activities in the US and give unnecessary support to the view that a radiation-included mortality is in some sense worse than any other mortality. Furthermore it suggests that a man-rem is always of the same value, irrespective of circumstances, and we have doubts about this.

It is accepted that in the current climate of public apprehension about nuclear reactor safety, and also considering the many uncertainties that exist about plant performance, accident consequences etc, it may be necessary to adopt a value of around $1,000 per man-rem averted but it would be wrong to imply that the same (high) value would necessarily be appropriate in the future. Our concern is that the adoption of a value of the man-rem at this point in time which is not well founded may prejudice future decisions about nuclear plant, even though many of the current uncertainties about safety may have been resolved satisfactorily by then.

(5) Plant Performance Guideline: the guideline concerning the likelihood of a large-scale core-melt appears to be out of place in this discussion. We are not convinced that there are any good reasons for singling out this plant-orientated guideline while ignoring others (why not specify a guideline for the likelihood of containment failure?). It is not thought that the guideline will have much merit in allaying public apprehension about the likelihood of very large accidents. (A guideline of 10^{-4} per year will be interpreted as implying a significant risk over the lifetime of any individual in the US, where something like 100 reactors are in operation). Also it is not clear how the guideline will be used by NRC staff (what precisely is meant by "large-scale"?).

In view of the large amount of research work being carried out at present in an attempt to improve our understanding of the physical processes leading to degraded core situations we consider that it may be premature to include this guideline at this time.

CONCLUSIONS

In summary, we congratulate the NRC on their initiative in taking this step towards formulating high-level safety goals for nuclear power plants. However, we are not totally convinced that it is particularly opportune to publish them at this time. The proposal to publish rests on the assumption that the risks can be validly estimated, and that sufficient and reliable data are available, and we have doubts that this is the case. However, if it is decided to proceed with them then the most careful consideration needs to be given to their wording to ensure that they are logical and self-consistent. Also there is a need to be sure that there will be a net benefit in terms of reactor safety, public acceptability, licensing procedures, etc., before a final commitment is made to these safety goals. Their use will involve a commitment of resources to PRA and to the consideration of severe accidents which may not necessarily result in a commensurate increase in reactor safety.

In the UK the Nuclear Inspectorate is in the process of finalising a set of Safety Assessment Principles for nuclear chemical plants which will parallel the reactor document. We shall continue to refine and improve the techniques of fault and event tree analysis, and the associated data bases, with the aim, mainly, of identifying weak areas in the plant's safety engineering. We are less convinced that the further step of estimating the component of individual or societal risk from severe accidents (ie. beyond the design basis) is sufficiently well understood at present to make a very significant impact on the acceptability of any plant for licensing.

REFERENCES

1. GAUSDEN, R and FRYER, D.R.H, Criteria for Guidance in the Safety Assessment of Nuclear Installations in the United Kingdom. International Conference on Nuclear Power and its Fuel Cycle, IAEA, Salzburg, Austria, 2-13 May 1977.

2. GRONOW, W.S. and LEWIS, G, Regulatory Control of Nuclear Power Stations in the United Kingdom. International Conference on Radiation Protection in Nuclear Power Plants and the Fuel Cycle, BNES, Bristol, England, 1979.

3. GAUSDEN, R and WOODS, P.B. Organisation and Experience of the Regulatory Review in the United Kingdom. Specialist Meeting on Regulatory Review in the Licensing Process, Nuclear Energy Agency, Madrid, Spain, 7-9 November 1979.

4. GAUSDEN, R. Two decades of Nuclear Power Plant Operation. International Conference on Current Nuclear Power Plant Safety Issues, IAEA, Stockholm, Sweden, 20-24 October 1980.

5. Safety Assessment Principles for Nuclear Power Reactors. HM Nuclear Installations Inspectorate, HSE, April 1979.

6. Safety Goals for Nuclear Power Plants: A Discussion Paper. US Nuclear Regulatory Commission, NUREG-0880, February 1982.

7. Recommendations of the International Commission on Radiological Protection, Oxford, Pergamon Press, ICRP Publication 26, Ann. ICRPÍ, No. 23 (1977).

8. EEC Directive of 15 July 1980, laying down the revised basic safety standards for the health protection of the general public and workers against the dangers of ionising radiation.

9. COHEN, A.V. and PRITCHARD, D.K. Comparative Risks of Electricity Production Systems: A critical survey of the literature. HSE Research Paper 11, HMSO, 1980.

CONSIDERATIONS ON A PROPOSED RATIONALE FOR QUANTIFICATION OF SAFETY GOALS

A. Birkhofer, A. Jahns

Gesellschaft für Reaktorsicherheit (GRS) mbH
Köln, FRG

ABSTRACT

The present concept proposes qualitative and quantitative criteria to give guidance for further development of detailed safety requirements. The criteria are based on probabilistic considerations. Essential element of the proposal is the concept of the individual risk limitation. The whole spectrum of events (normal operation, design basis accidents and severe accidents) will be considered. Concerning numerical guidelines for the assessment of quantitative safety goals, admissible and inadmissible risk values are directly related to the respective doses as prescribed in the Radiological Protection Ordinance. Risk curves will be suggested. These curves define different regions of risk in a dose-frequency diagram. By means of these curves, calibration points for the frequency respectively the dose of certain events are derived and a graduation of a differentiated safety concept is suggested. The proposed concept is not intended to replace the present methods of safety assessment. Rather, it might be a useful supporting tool.

INTRODUCTION

The discussion on quantitative safety goals for the safety assessment of nuclear power plants, going on in many countries, especially in the USA, naturally has had an impact to the discussions in the FRG. In spite of the performed risk studies and risk-oriented studies there does not yet exist an unanimously accepted opinion among technical experts whether the present state of knowledge allows to define very detailed criteria for quantitative safety goals. It is therefore the aim of the following to present our thoughts on probabilistic safety criteria or "safety goals".

The proposals are aimed at

- giving guidance for further development and improvement of detailed safety requirements

- using present regulations like the Radiological Protection Ordinance as a frame for the assessment of quantitative safety goals.

The proposals are preliminary, they present the opinion of the authors. At the present time they neither represent the position of the Federal Minister of the Interior (BMI) nor that of his advisory bodies.

It should be pointed out that the proposed concept is not intended to develop new safety requirements. The approved methods, principles and criteria for safety assessment will be maintained. Rather, the criteria proposed in the concept shall contribute to a rationale for the decisionmaking in borderline cases. They could be used as a useful supporting tool for the harmonisation of safety requirements in the special view of a balanced safety concept.

BASIS FOR A CONCEPT TO QUANTIFY SAFETY GOALS

General Remarks

Concerning quantitative safety goals with regard to public health and safety, our feeling is that limitation of mortality risk receives the highest priority. It therefore will be a particular objective of the proposal to limit the cumulative mortality risk for an individual resulting from design basis and more severe accidents.

An essential element of a concept to quantify safety goals with regard to harmonisation in the view of a balanced safety concept continues to be the requirement for limitation of the total risk and for limitation of the risks from individual events. For that purpose, individual events should be combined and then be classified according to different release-categories.

When determining safety goals on a probabilistic basis, one should not only define limits but in addition determine with which certainty these goals may not be exceeded. This requirement is based on the fact that probabilistic statements are always statements on distributions.

In this context, one has to differentiate between risk, extent of damage and probability. As a reference figure for the component "extent of damage" the individual dose should be chosen. This is an indispensable prerequisite in particular when evaluating the maximum dose as limiting element because of regulations in the Radiological Protection Ordinance. It is agreed generally that the frequency of an event (per reactor year and site) can be chosen as reference figure for the component "probability". For quantitative considerations it seems to be reasonable to express the "risk" by the product of the event frequency and a related representative individual dose. Are to be considered several kinds of unwanted events, the measure for the total risk results from a linear superposition of the risks resulting from the individual events.

Risk Curves

For the reasons mentioned above, in particular to account for regulations in the Radiological Protection Ordinance, we suggest in the first step risk curves as follows:

As quantitative normative settings, the legislator has established dose limits for radioactive releases during normal operation and design goals for radiological consequences of certain postulated accidents (30 mrem/year and 5 rem-concept of the Radiological Protection Ordinance).

Applying the usual dose-risk relations for somatic early or latent radiation health effects and genetic radiation effects in subsequent generations, these normative settings may directly be interpreted as permissible risk values. The risk quantification should therefore start from these values. All other numerical guidelines should be derived from the permissible risk values, or it should be demonstrated that they are compatible with the permissible risk values.

Considering permissible dose values and usual dose-risk relations borderline curves in a dose-frequency diagram should be worked out. Following this idea, different risk curves may be derived forming a basis for the definition of the different risk classes.

Curves constructed in this way represent the constant mortality risk supplemented by risks for genetic effects for subsequent generations. All events falling on a given curve can be considered as equal under the aspect of risk of lethal or genetic radiation effects. Examples of such a type of curves are shown in Fig. 1.

Assuming a linear superposition of the mortality risks for acute and delayed radiation health effects, the particular shape of the risk curves in Fig. 1 (slope and curvature) follows directly from the respective risk coefficients and dose-risk relations of ICRP-26 and the German Risk Study. The normalization has been chosen in compliance with the Radiation Protection Ordinance.

The curves first show a constant negative gradient as a function of the radiation exposure according to the risk of delayed fatalities and genetic effects. In order to account for acute injuries, a threshold of approximately 50 rem has been assumed. Due to the exponentially increasing contribution of mortality from acute injury, the dose limit curves show a steeper negative gradient above the threshold. Preliminary calculations performed up to now have shown that for the analysed release categories 90 % of the doses are in the range of 5 to approximately 50 rem. Higher doses are extremely rare so far. In these calculations, reasonable emergency procedures have been taken into account.

It will be investigated at the present time, if and to what extent collective risks and risks for serious acute health effects must be introduced as independent criteria. It can be expected that limiting the individual risk, the collective risk will be limited also to a sufficient degree.

Risk Classes

Having established curves of constant mortality risk in a frequency-dose diagramm, in the next step we will define different risk classes. In particular, it is useful to define a high and a low risk threshold. In this way, three risk classes evolve.

Qualitative definition of risk classes:

Class I	The risk class I contains events in the inadmissible region.
Class II	The risk class II contains events in the admissible region. The design of safety related systems and components has to be performed in such a way that this class will be attained.
Class III	The risk class III contains events which are significantly below the admissible risk.

In this context "events" are considered to be release categories which are formed by grouping together event sequences which lead to similar releases.

For classification, one has to consider the estimated frequency of the initiating events and the sequence of the event. The risk class of a certain event sequence results from its frequency and from the estimated individual dose of the related release category. The estimated individual dose of the release category is considered to be a representative value for the given release such that this value will presumably not be exceeded in the vicinity of the plant. As a reference figure we suggest the 90 %-fractile of the respective distributions of the individual doses where all representative weather situations are accounted for according to their probabilities.

Event Frequency Classes

A classification of events solely under the aspect "risk" would exclude a differentiated judgement of the components "damage" and "probability". With respect to the general principle - the avoidance of damages by putting emphasis on preventive means - and in order to achieve an adequate high effectiveness, functionability and reliability of systems to control plant transients or incidents there is therefore a need for additional criteria, i. e. criteria for the assessment of the component "probability".

In order to perform such an additional judgement, to get a relation to the present design practice (list of design basis accidents) and for reasons of practicability, a classification of event frequency classes will be proposed in addition to the risk classes. The distinguishing qualitative criterion is "to be expected/not to be expected". Reference scale is a representative time scale. It is based on the following rationale: There are events which occur in each plant during its life time. These events have to be evaluated different from those expected to occur only once in the lifetime of all present and future plants, or those which may be excluded as far as one judges or because of scientific-technical reasons.

Definition of event classes (Fig. 2):

Class I	The event frequency class I contains event sequences which are expected to occur during the design lifetime of a plant.
Class II	The event frequency class II contains event sequences which are not expected to occur during the design lifetime of a plant, but which cannot be excluded for one of the plants during the cumulative design lifetime of a representative group of plants.
Class III	The event frequency class III contains event sequences which neither are expected during the design lifetime of one nor during the cumulative design life time of a group of several plants for one of the plants. They however cannot be excluded with sufficient confidence.
Class IV and Class V	The event frequency classes IV and V contain event sequences which practically can be excluded during the cumulative design life time of a representative group of several plants judging on a historical time scale and from a rational point of view.

Radiological Hazard Classes

As a next step one has to introduce criteria for the assessment of the component "damage".

In order to perform such an additional evaluation and to get a relation to the present design practice (dose values of the Radiological Protection Ordinance) respectively to dose values for the initiation of emergency procedures (Basic Recommendation for Emergency Procedures), a classification according to the radiation exposure will be proposed.

A rough classification is given by the threshold for acute health effects, a more detailed classification in the range of low doses according to the dose values

of the Radiological Protection Ordinance (30 mrem/5 rem). In the range of high doses it is usual to specify reference values for the average lethal dose (LD-50).

For this reason it seems to be appropriate to distinguish between 4 classes, denominated with the preliminary title "radiological hazard class".

By means of these classes, the considered spectrum of dose values may be differentiated according to kind and extent of possible radiation health effects.

Proposed is the qualitative criterion "acute health effects/latent health effects to be expected/not to be expected".

Radiological hazard classes (Fig. 3):

Class I — The radiological hazard class I contains event sequences which do not lead to radiation exposures higher than the limits set for normal operation in the Radiological Protection Ordinance ($\leq$ 30 mrem annual whole body individual dose). These values are in the variation range of the annual natural background radiation.

Class II — The radiological hazard class II contains event sequences which do not lead to radiation exposures higher than the limit set by the Radiological Protection Ordinance for occupationally exposed personnel ($\leq$ 5 rem annual whole body individual dose). This value also corresponds to the exposure limit for design basis accidents.

Class III — The radiological hazard class III contains event sequences, with radiation exposures expected to be in the range of 5 to 50 rem effective whole body individual dose. In this range, malignant injuries for an individual are very seldom, lethal early injuries for an individual are excluded.

Class IV — The radiological hazard class IV contains event sequences with radiation exposures in the range of 50 to 400 rem effective whole body individual dose. In this range, malignant latent injuries for an individual are dominating, somatic early injuries for an individual can occur in up to 50 % of the cases.

For the calculation of doses, the following aspects are relevant:

- the assignment of event sequences to relevant release categories
- the estimated extent of the released radiologically representative nuclides as determined by the respective release categories
- the estimated frequency of representative weather situations.

Similar to the dose concept, reference values are the basis for the calculation of release and transport of fission products.

Results of a preliminary investigation have shown that such a concept is feasible for the assessment of releases during normal operation, design basis accidents and more severe accidents. Therewith a common basis is given for the comparison of radiation exposures which result from events occurring during the three above cited plant conditions.

CONCLUSION

Preliminary calculations have shown that the total risk for the individual from all events in the region of normal operation/design basis accidents/severe accidents is limited and is below risk class I described in Fig. 1, that means that existing health and accident risks are not increased significantly by a nuclear power plant.

The concept presently will be discussed in the technical and scientific field. A major point of the discussion is to review whether the proposed methodology is appropriate for the derivation of quantitative safety goals. In particular, investigations are performed in order to find a rationale - without relying on the planning values for radiological relevant accidents according to the Radiological Protection Ordinance - for particular case requirements to cope with severe accidents.

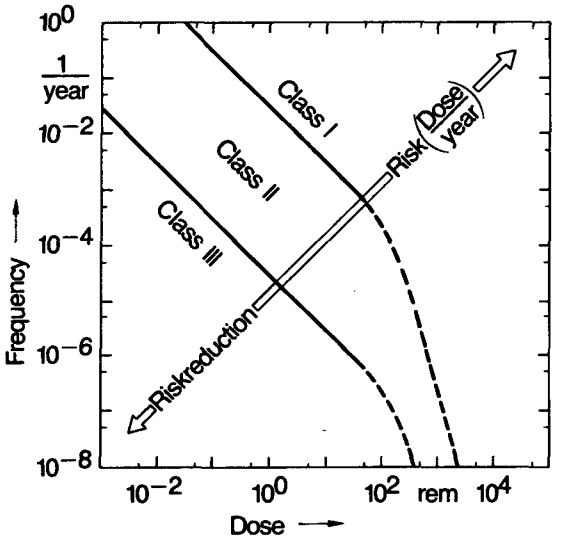


Fig.(1): Risk Curves and Risk Classes

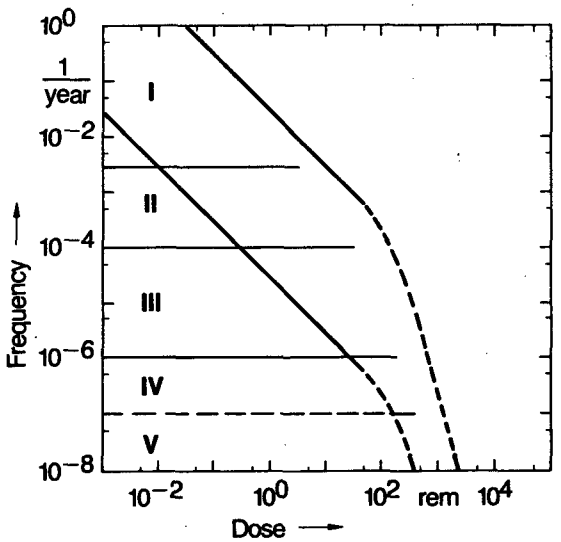


Fig.(2): **"Frequency of Event" Classes**

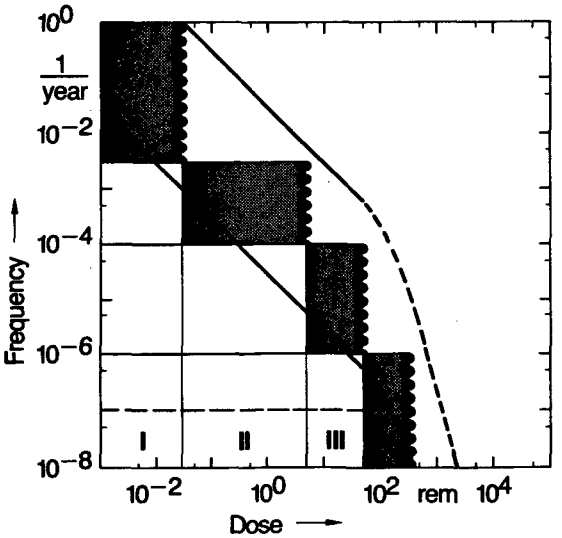


Fig.(3): **Relation of "Frequency of Event" and "Radiological Hazard" Classes**

RISK CLASSES IN A FREQUENCY-DOSE DIAGRAM

SAFETY GOALS AS APPLIED IN CANADA

Z. Domaratzki

Atomic Energy Control Board
Ottawa, Canada

ABSTRACT

Early in the 1960's the Atomic Energy Control Board published a list of fundamental safety requirements which, with some modification, continue to be the basis for reactor licensing in Canada. Included in these fundamental goals were quantitative statements which defined the risk to individuals and to the population around a nuclear power plant arising from normal operation and a wide spectrum of accidents. During operation of a reactor it is possible to verify in a relatively short period of time (several years) whether a plant is meeting the established goals.

The Canadian approach, while shown by experience to be sound, is not without its weaknesses. These are discussed along with the approaches adopted to compensate for what is rather a simplistic approach.

The USNRC Proposed Policy Statement on Safety Goals is examined and the ojbectives compared with the Canadian practices. Potential difficulties in the interpretation and the application of the safety goals are discussed in light of Canadian experience.

INTRODUCTION

From the beginning of the nuclear power program in Canada the Atomic Energy Control Board (AECB) adopted the philosophy that the primary responsibility for nuclear power plant safety rested with a licensee. The role of the regulatory agency was to ensure that a licensee fulfills this responsibility. In keeping with this philosophy the AECB consciously avoided establishing detailed regulations or requirements relating to siting, design, construction or operation of nuclear power plants. Instead the AECB chose to establish some broad safety goals and a set of fundamental principles and criteria. Licensees had considerable flexibility in their choice of design concepts and details providing they could show that they met the broad goals.

CANADIAN SAFETY GOALS

When the first two prototype CANDU power reactors were being designed in the late fifties and early sixties the designers proposed a safety goal - the risk from each plant would be less than 10^{-2} deaths per year. This goal was tacitly accepted by the AECB, an organization which at the time had a complement of five technical

staff in addition to the President. During the first half of the 1960's there was considerable discussion of safety goals which led in 1964 to a publication on the subject by the President of the AECB. The quantitative safety goals which he outlined more than 17 years ago still form the fundamental framework for licensing nuclear power plants in Canada. These goals, in their most simplistic form can be reduced to one table. Table I as it exists today is only a somewhat modified version of the safety goals published in 1965.

Some of the principles and criteria which follow naturally from Table I are:

i) the quality and nature of the process systems essential to the reactor must be such that the total of all serious process failures should not exceed one per three reactor years. (A serious process failure is any failure of equipment or procedure that in the absence of safety system action could lead to a significant release of radioactive material from the station);

ii) each special safety system must be tested at a frequency to demonstrate that its availability is less than 10^{-3};

iii) special safety systems must be physically and functionally separate from the process systems and from each other.

The objectives of the quantitative safety goals are at least threefold:

i) to identify, for design and operating purposes, a limit on individual and societal risk resulting from normal operation and a wide spectrum of accidents;

ii) to ensure an acceptable level of defense-in-depth by requiring that the consequences of accidents fall within defined limits even in the event of failure of a special safety system;

iii) to be able to verify in a relatively short period of operation whether a plant is meeting the established goals.

In the case of the third objective it is clearly not possible to verify that safety systems will limit the consequences of severe accidents to the calculated values. It is however practical to verify that the frequency of serious process failures is not significantly greater than predicted and that the availability of special safety systems is as calculated.

EXPERIENCE WITH CANADIAN SAFETY GOALS

The quantitative safety goals have served Canadians reasonably well over the years. A clearly identified target for the reliability of special safety systems gave designers and operators considerable flexibility in the design and in-service testing of systems. For instance, safety system logic circuits in Canada usually include three independent channels with actuation of two resulting in system operation. However, two-out-of-three logic is not a requirement; rather, it is only the quantitative target which has been specified by the AECB. Thus, when in one case experience showed a significant incidence of spurious actuations of a safety system during routine in-service testing the designers/operators were able to change to a three-out-of-four logic network because they could show that this would have minimal effect on their ability to meet the prescribed quantitative target. Also, this numerical target gave designers a basis for deciding on trade-offs between redundancy in systems and required in-service test frequencies.

The reference dose limits specified for serious process failures and serious process failures combined with failure of any special safety system give designers a

benchmark against which they must measure the effectiveness of the special safety systems for a wide range of accident conditions and allows them to determine when improvements in effectiveness are necessary. Without prescribing, for instance, how ventilation systems should be designed it allows designers to establish the requirements for the logic which isolates that system under accident conditions.

From the outset however it was recognized that the application of the safety goals to the safety evaluation of CANDU plants was somewhat simplistic. For instance, a wide range of single serious process failures were examined but combinations of process failures which might have similar consequences were not. The combinations of process failures so ignored could have probabilities of occurrence higher than the serious process failures considered.

A further weakness was that the approach tended to emphasize ensuring the effectiveness of safety systems in coping with rather stylized accidents such as a LOCA or a uncontrolled power increase and less emphasis was placed on the effectiveness of the human operator and his role in events which would unfold more slowly, e.g., interruption of service water flow.

It was stated in the safety goals that special safety systems should be completely independent of the normal process systems. Such independence has been essentially achieved in the separation between control systems and reactor shutdown systems. It is not really practical however to achieve the same high degree of separation between the reactor cooling system and the emergency core cooling system. Nevertheless the goal of separation tends to push, perhaps to an extreme, the attempts to reduce the interdependence.

A further shortcoming of these safety goals is that they are difficult to apply without clarification. In the absence of pertinent operating data, experience has shown, for instance, the need for two independent and fully effective shutdown systems, two different parameters where practical to sense any serious process failure and the need for seismic qualification of equipment. Because they are written in general terms these goals can be misleading for the inexperienced and can result in widely differing interpretations by the experienced.

To assist in the application of the safety goals, two evolutionary changes have been made and are still ongoing. One change has been to distill many of the engineering judgements made over the years with respect to special safety systems and document them in the form of regulatory guides. This publication of safety requirements in much more detail is a deviation from the earlier practice of the AECB. However this action was taken not only because the AECB considered that further clarification was necessary but also in response to the perceived wish of the general public and the open and frequent requests of the nuclear industry.

The second change has been to require a more thorough review of a plant design in order to identify combinations of faults which could result in an accident. A rigourous application of sound reliability practices using fault trees and event trees started in 1974 and has expanded to the present day. This type of safety evaluation has been shown to be particularly useful and necessary in evaluating the potential for accidents arising from failures in the common service systems (service water, instrument air and electrical power), but is also essential for identifying interdependencies among systems.

USNRC SAFETY GOALS

Both the Canadian and the USNRC safety goals have the same objective - to define the individual and societal risk to the populace in the vicinity of a nuclear power plant. In both cases, being goals, they are given in broad terms and or their own

are not adequate to communicate regulatory requirements to system designers. Of course, the USNRC safety goals (like the Canadian goals) are not purported to be such a communication device. On the contrary, NUREG-0880 makes it clear that "the licensing of individual plants would continue to be based principally on NRC regulations rather than conducted with direct reference to the safety goals and associated numerical guidelines". The situation is analogous to that in Canada where the safety goals have been clarified with detailed regulatory requirements. In Canada it is common for reactor licensees to argue that if they can show compliance with the safety goals, then compliance with the detail requirements should be optional. One would expect a similar debate in the USA; given that a licensee demonstrates compliance with NRC regulations, then the need to show compliance with the safety goals and numerical guidelines could be argued to be optional. Such discussions could be minimized if the safety goals and numerical guidelines of NUREG-0880 can be shown to be consistent with the NRC regulations, i.e., either path results in approximately the same individual and societal risk.

A first order comparison between the NRC regulations and the proposed safety goal could be done by a comparison of WASH-1400 and the safety goal. In WASH-1400 the consequences in terms of early fatalities and latent cancer fatalities were presented for reactor accidents ranging in frequency from one in 20,000 per reactor year to one in 10^9 per reactor year. The proposed safety goal could be translated into early fatalities and latent cancer fatalities for accidents having a similar range of frequencies. A comparison of the two sets of values would indicate whether the safety goals are consistent or not with the current regulations.

Both the US and Canadian goals have been the subject of the same criticism - namely that they are too remote from the nitty-gritty decisions which system designers and regulatory staff must make every day. On both sides of the border the solution proposed is often the same one and entails adherence to design practices which have been followed over the years. This valid criticism of the goals is not, however, a reason for abandoning them. Each decision on a safety question cannot be directly linked to the general safety goal. Nevertheless, the impact of the sum-total of the decisions should be reviewed at intervals and compared against the safety goals using the best risk assessment tools available.

Neither the proposed NRC safety goal nor the Canadian goals discourage siting in heavily populated areas. In both cases compliance with the guidelines applied to individuals close to a plant is more demanding than compliance with the guideline applied to the population as a whole. Consequently, the regulatory requirements tend to be the same for a sparsely populated area as for a heavily populated area.

CONCLUSION

The proposed NRC safety goals like the Canadian safety goals are written to express regulatory requirements in the broadest sense. In themselves they are not an adequate communication to system designers and need to be clarified by detailed requirements based on past practise and experience. This recognized weakness notwithstanding a statement of general safety goals is especially important in an era when more emphasis is being put on a probabilistic approach to reactor safety evaluation.

TABLE 1

Operating Dose Limits and Reference Dose Limits for Accident Conditions

Situation	Assumed Maximum Frequency	Maximum Individual Dose Limits	Maximum Total Population Dose Limits
Normal Operation[a]		0.5 rem/yr whole body 3 rem/yr to thyroid	10^4 man-rem/yr 10^4 thyroid rem/yr
Serious Process Failure (single failure)	1 per 3 years	0.5 rem whole body 3 rem to thyroid	10^4 man-rem 10^4 thyroid-rem
Process Failure plus Failure of any Safety System (dual failure)	1 per 3×10^3 years	25 rem whole body 250 rem to thyroid	10^6 man-rem 10^6 thyroid-rem

[a] The operating target for all nuclear power plants in Canada is 1% of these limits.

A FRENCH VIEW ON THE PROPOSED NRC POLICY ON SAFETY GOALS

P. Y. Tanguy

Institut de Protection et de Sûreté Nucléaire - CEA
92260 Fontenay-aux-Roses, France

ABSTRACT

French regulatory authorities have favored for several years the progressive introduction of probabilistic safety criteria in the licensing process. Since the implementation of Probabilistic Risk Assessment implies the definition of accepted safety goals, we recognize the importance of the NRC proposed policy statement, NUREG-0880. My comments will deal with three main topics :

- The purpose of safety goals : in my view, the primary objective should not be to convince the public that nuclear power is safe enough, but to explicit in terms of risk the past and present decisions taken by safety experts and enlarge the field of experts ;
- The formulation : we should not overlook the uncertainties associated with extreme accidental sequences, and we should not forget that plant safety rests essentially on good design, correct construction, and appropriate operating rules ;
- The application in the regulatory process : I think that P.R.A. implies the use of best-estimate evaluations, and most important, has to be validated, as far as possible, with experience feedback.

INTRODUCTION

The status in France regarding the use of safety goals and probabilistic risk assessment (PRA) in the regulatory process was presented in previous meetings [1], [2] . I will just mention here that important regulatory decisions, based on a probabilistic approach to safety, have been made for french nuclear power plants, relative to accident prevention as well as consequence mitigation. For instance, additional safety features were required to cope with the total loss of redundant systems, such as electrical supplies, and ultimate technical specifications were developed making it possible for the operator to minimize the consequences of degraded reactor conditions.

But, even if in fine I shall refer to french practice, this paper will be mainly devoted to a few comments on "the NRC policy statement on safety goals" submitted for comments in the NUREG-0880 report [3] . The ideas expressed in this paper are my own and obviously should not commit french safety authorities.

I shall begin with some general remarks. I have often noticed in the past that on nuclear safety quantification, two types of attitudes are encountered : first, even when there is an agreement on the basis of such quantification, the objections made to all proposals lead to reject finally any concrete project ; second, when a proposal is deemed to be acceptable, practical applications to the regulatory process are opposed to, by fear of unforeseen consequences. In practice, both attitudes result in the blockage of any real advance.

To day, we have in front of us a consistent project, which was the subject of many previous discussions with a number of experts. I am of the opinion that it represents a significant advance, and that consequently, whatever the critical comments which could be made on such or such items, it constitutes already a first step on the right track. However, I feel that up to now the Nuclear Regulatory Commission has not clearly stated how these proposals are going to be implemented. In fact, the authors of NUREG-0880 seem to be still in doubt about that implementation, as shown by the questions raised at the end of the report.

My remarks will then be oriented in the following direction : the most important problem we have to face to day is not so much to amend the NRC proposal on a few specific points, but rather to propose a practical method for its implementation, at least as a test.

SCOPE OF THE SAFETY GOALS

I find myself in full agreement with most of the arguments developed in the first chapter of the NRC Report, and in particular with the need for making explicit the safety philosophy upon which the regulatory decisions are based, in order to improve the consistency and the predictability of safety procedures.

I shall expand a little on a single point. I do not think that safety goals by themselves can convince the public that nuclear plants are safe enough, or even gain public's confidence. But I believe that the public would be reassured if it could be sure that safety decisions are taken only after a sufficient mumber of competent and independent experts have agreed upon those decisions. An important objective of safety goals and of PRA's is therefore to enlarge the field of competent experts, through a better explicitation of the safety regulations, and to clarify the discussions by insuring a better consistency between various specialists. -We all know that any specialist is apt to consider that his field only is of importance-.

This public confidence could be an indirect consequence of safety goals implementation. But we should be also very careful of the direct impact if the safety goals' formulation is not correctly perceived by the public. We all realize that the adoption of quantitative safety goals means that the nuclear community recognizes that absolute safety does not exist, and that nuclear plants are a source of hazards to the population. This may seem trivial, but it may not be so ; I have been amazed by some of the words used by one of the NRC's Commissioners, Commissioner Gilinsky, in his separate views in NUREG-0880. I quote :

"The electric utilities should, with sufficient care, be able to avoid large accidents altogether, and that should be the safety goal for each facility. Nuclear power plant staffs should be instructed to prevent severe reactor core damage and to prevent significant uncontrolled releases of radioactivity from containment <u>under all circumstances</u>".

In my paper, I have underlined "under all circumstances". Such a phrase is probably quite adequate for reassuring the public, but I wonder whether this is not a way to go back to the good old D.B.A. (Design Basis Accident). It reminds me of the argument which is often raised in public hearings : why don't you put around your reactors containments strong enough to withstand all accidents ? We are back to the myth of absolute safety, of zero risk.

We must not neglect that aspect. I consider it very useful if politicians, at the proper level, could take a clear position on the risk issue. But such a statement should me made with great care, in order to avoid any erroneous or biased interpretation, based for instance on mumbers of fatalities which have no real significance. Moreover, the public and the political circles should understand why such a political statement is now deemed necessary.

I suggest that such a statement be associated with an analysis of operating experience. There are presently in the world several hundreds of reactors in operation. If those responsible for the safety of the public think timely to state publicly which risk for the neighbouring populations is associated with these plants, they have to explicit what means for each individual that accepted risk, and how it relates to the operating experience of the plants. For each of us, expert or member of the public, the operating experience is made essentially by the incidents, all those abnormal occurrences that keep the public all the more worry as they seem to be contradictory to the high safety level claimed by the nuclear community.

The analysis of abnormal events, or LER's, as it is performed by safety bodies, and in particular in the recently published report from the Oakridge National Laboratory for NRC, seems to me extremely important from that standpoint. This type of analysis should be multiplied, in order to show that the experience is consistent with the previsional safety evaluations, -or in order to correct consequently these evaluations-. Perhaps more important, these analysis should be use to trace the trend of operating experience with time : check that some initiating events have been efficiently corrected, and that, thanks to lessons learned, the safety is eventually improved through a decrease of significant events' frequency.

QUALITATIVE SAFETY GOALS

I shall now turn to the second chapter of the NRC Report, which deals with qualitative goals.

Once again, I do agree with most of the NRC statement, and I shall limit myself to two remarks :

- The first goal -no significant additional risk to life and health-, seems an effective answer to public concern, and for me it comes under the political statement I just mentioned earlier. On the other hand, it is not obvious that at such a global level the goal could be easily used in a decision-making process, and it seems to me that it should rather be considered more as an overall evaluation result than as an operational objective ;

- The second qualitative goal, -societal risks as low as reasonably achievable, and comparable to the risks from competing technologies-, seems to me more easily applicable, for plant design as well as for authorization by regulatory authorities, as soon as the implementation methodology has been agreed upon ; that is the point we are going to review now.

NUMERICAL GUIDELINES AND IMPLEMENTATION

I shall discuss simultaneously the proposed numerical guidelines and their implementation ; the two aspects are as a matter of fact in close conjunction, as indicated by the authors of NUREG-0880.

As concerns the individual risk, the proposed values seem reasonable. In order of magnitude, they correspond to an absolute risk around 10^{-6} per reactor and per year ; this is sufficiently less than the basic individual risk to avoid endless discussions with little meaning ; (such would not be the case if they were raised by a factor 10). When used as aiming points, they are consistent with the present evaluations for plants under construction, using best estimate values.

But on an other hand I am not sure that the maximum individual risk is the best criterion from which the decisions are to be made. Since another criterion, the societal risk, is also proposed, which overlaps the first one, and which seems to me more easily usable, I should deem preferable to retain the individual risk only as the final

result of the assessment, and as a basis for the political statement I proposed earlier.

Regarding the societal risk, which, associated with an optimization requirement applying a cost-benefit method, would constitute the decision-making criterion, I shall propose first that its value correspond effectively to the objective aimed at : this is not presently the case, since the authors of NUREG-0880 admit that compliance with the individual guideline largely covers the societal guideline. An EPRI study estimates the margin to more than a factor 100. I do not understand the purpose of such a margin, as soon as an attempt is made to obtain a realistic risk assessment, and it seems unjustified, if only because of the use which could be made of these figures by nuclear opposents.

I come now to the point which is essential to me : the delayed risk to the population within 50 miles of the plant site. Personnally, I would have perferred a radius of about 30 kilometers, but this is not a fundamental issue. This overall societal risk agglomerates the results of studies which are of completely different technical natures. To be schematic, I would identify three steps :

- Plant performance, with its safety and safeguards systems ;

- Containment behaviour in extreme conditions, and operator ability to implement ultimate procedures ;

- Site, emergency planning, and medical consequences evaluation.

Here, I join Commissioner Gilinsky's views, in pointing out that, in my opinion, a complete trade-off beteween the three aspects cannot be accepted, which would be the case if only the overall result was a subject of concern. The NUREG-0880 introduces an intermediate limitation an plant performance, with a maximum core-melt probability, which corresponds to the first of the three aspects I have mentioned. I think it would be desirable to define also reference values for the other two aspects, for instance :

- conditional probability for total loss of containment,

- and criteria for population around the site and emergency planning efficiency.

To summarize, I suggest :

1) To use the delayed risk for population around the plant as the decision-making criterion in the regulatory procedure ;

2) To complement this overall criterion by three intermediate reference figures, which could be :

   - the maximum probability of a large core-melt,

   - the conditional probability for loss of containment,

   - a site criterion.

3) For each guideline, in order to take into account the uncertainties associated with best estimate evaluations, to retain the principle of maximum and minimum levels : below the minimum, the criterion is considered as fulfilled, and nothing more is required ; beyond the maximum, the design is deemed to be inacceptable ; between the two, the optimisation is applied, with a cost-benefit criterion. For that last one, I believe that for the sake of consistency, the value proposed by the ICRP should be used.

4) On the accepted design, to evaluate the maximum individual risk, which will generally be acceptable if the preceding goals have been correctly chosen.

COMPARISON WITH FRENCH REGULATION

I shall open here a parenthesis to indicate briefly that above suggestions should comply with the present practice in France. I must however acknowledge that I have not performed a detailed comparison which would allow me to be quite definite on the subject.

We use in France, in terms of goals :

- A combined probability for core-melt and loss of containment of 10^{-6} per reactor and per year ;
- An additional conditional probability for brutal atmosphéric rupture of containment between 10^{-1} and 10^{-2} ;.
- Features designed to limit the radioactivity release to the environment in the event of a slow rupture of the containment ;.
- Site criteria related to the efficiency of an emergency plan for the maximum considered release to the environment.

FINAL REMARKS

I will end by making two specific remarks :

- It seems to me too early for applying the guidelines to earthquakes. Probabilistic studies must be developed in that field before they can be used in such procedures ;
- One must not forget to include in the cost-benefit optimization the assessment of the risks related to any new provision, that is the possible cost in man x rem, as well as the accidental risk. I remind that the Enrico Fermi accident originated in a metallic shed added for safety reasons.

REFERENCES

[1] P. TANGUY et F. COGNE, "Utilisation des methodes probabilistes dans l'évaluation de sûreté des installations nucléaires", NUCLEX, BALE (1978).

[2] P. TANGUY, "French Practice of Limited application of quantitative safety goals", International ANS/ENS Topical Meeting on Probabilistic Risk Assessment, Port-Chester, USA (1981).

[3] Safety Goals for Nuclear Power Plants : A Discussion Paper. NUREG-0880 For Comment, U.S.N.R.C. February 1982.

SESSION 7

PRESSURIZED THERMAL SHOCK - 1

Chair: R. Noel *(EdF)*
M. Vagins *(NRC)*

THE INTEGRITY OF PWR PRESSURE VESSELS DURING OVERCOOLING ACCIDENTS*

R. D. Cheverton S. K. Iskander G. D. Whitman

Oak Ridge National Laboratory
Oak Ridge, Tennessee 37830, U.S.A.

ABSTRACT

The reactor pressure vessel in a pressurized water reactor is normally subjected to temperatures and pressures that preclude propagation of sharp, crack-like defects that might exist in the wall of the vessel. However, there is a class of postulated accidents, referred to as overcooling accidents, that can subject the pressure vessel to severe thermal shock while the pressure is substantial. As a result of such accidents vessels containing high concentrations of copper and nickel, which enhance radiation embrittlement, may possess a potential for extensive propagation of preexistent inner surface flaws prior to the vessel's normal end of life.

For the purpose of evaluating this problem a state-of-the-art fracture-mechanics model was developed and has been used for conducting parametric analyses and for calculating several recorded PWR transients. Results of the latter analysis indicate that there may be some vessels that have a potential for failure in a few years if subjected to a Rancho Seco-type transient. However, the calculational model may be excessively conservative, and this possibility is under investigation.

INTRODUCTION

The reactor pressure vessel in a pressurized water reactor (PWR) is normally subjected to temperatures and pressures that preclude propagation of sharp, crack-like defects (flaws) that might exist in the wall of the vessel. However, there is a class of postulated accidents, referred to as overcooling accidents (OCA's), that allow cool water to come in contact with the inner surface of the vessel wall, resulting in high thermal stresses and a reduction in fracture toughness near the inner surface. This introduces the possibility of propagation of preexistent inner-surface flaws, and this possibility increases with reactor operating time because of the additional reduction in fracture toughness that results from exposure of the vessel material to fast neutrons.

Thermal loading (thermal shock) by itself presumably cannot drive a flaw all the way through the wall; however, if the primary-system pressure is substantial, a

*Research sponsored by the Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission under Interagency Agreements 40-551-75 and 40-552-75 with the U.S. Department of Energy under contract W-7405-eng-26 with the Union Carbide Corporation.

potential for vessel failure could exist; that is, a preexistent flaw, under proper circumstances, could penetrate the vessel wall and provide a large enough opening to prevent flooding of the reactor core. The nuclear industry has been aware of this problem for quite some time, [1,2,3] but the probability of the existence of the requisite conditions for significant flaw propagation seemed very remote. In recent years however, several PWR OCA initiating events have occurred,[4,5,6] and there has also been a growing awareness that copper and nickel significantly enhance radiation damage in the vessel.[7,8] As a result a reevaluation of the integrity of PWR pressure vessels during OCA's has been undertaken.

A complete evaluation of the OCA problem in terms of its threat to pressure vessel integrity requires consideration of a number of factors, including postulated accident initiating events, reactor system and operator response to these events, specific design features of the reactor vessel and core that affect fluence-rate and coolant-temperature distributions adjacent to the inner sufrace of the vessel wall, sensitivity of the vessel material to radiation damage, size and orientation of preexistent flaws, and remedial measures. This paper examines primarily the fracture-mechanics-related conditions that could lead to a potential for vessel failure.

THE TENDENCY FOR INNER-SURFACE FLAWS TO PROPAGATE DURING THERMAL-SHOCK LOADING ONLY

The tendency for inner-surface flaws to propagate as a result of thermal-shock loading is illustrated in Fig. 1, which shows the temperature, resultant thermal stress, and fracture toughness distributions through the wall of the vessel (exclusive of cladding) at a particular time during a postulated large-break loss-of-coolant accident (LBLOCA). Also included in the figure for the same time in the transient are the stress intensity factors (K_I) for long axial flaws of different depths and the radial distribution of the fast neutron fluence. As indicated, the positive gradient in temperature and the steep attenuation of the fluence result in positive gradients in the crack initiation toughness (K_{Ic}) and the crack arrest toughness (K_{Ia}), and these positive gradients tend to limit crack propagation. However, K_I for the assumed long axial flaw also increases with flaw depth, except near the back surface, and for the particular case and time analyzed it is evident that both shallow and deep flaws can initiate; that is, $K_I \geq K_{Ic}$ for a broad range of crack depths. As the crack tip moves through the wall it encounters higher toughness material and for this particular case eventually arrests.

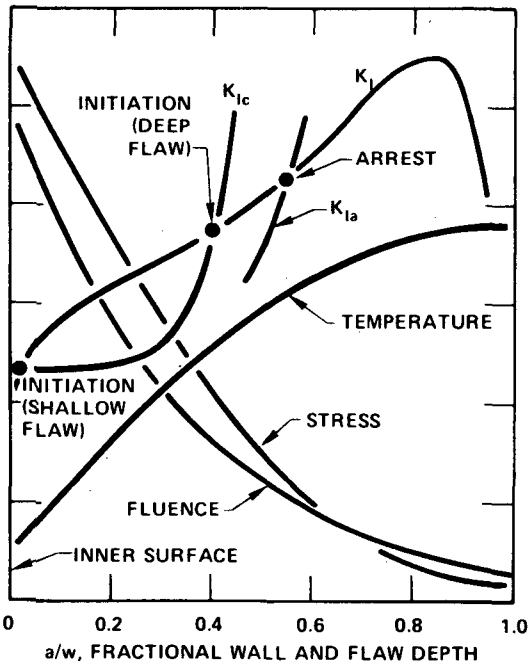


Fig. 1. Radial distributions in a vessel wall of several fracture-mechanics-related parameters at a specific time during a PWR LOCA.

If the crack depths corresponding to the initiation and arrest events are plotted as a function of the times in the transient at which the events take place, a set of curves referred to as the critical-crack-depth curves is obtained that indicates the behavior of the flaw during the entire transient. A typical set of critical-crack-depth curves for a LBLOCA is shown in Fig. 2. As indicated by the dashed lines the long axial flaw would propagate in a series of initiation-arrest events and, if a phenomenon referred to as warm prestressing (WPS) were not effective, would penetrate deep into the wall.

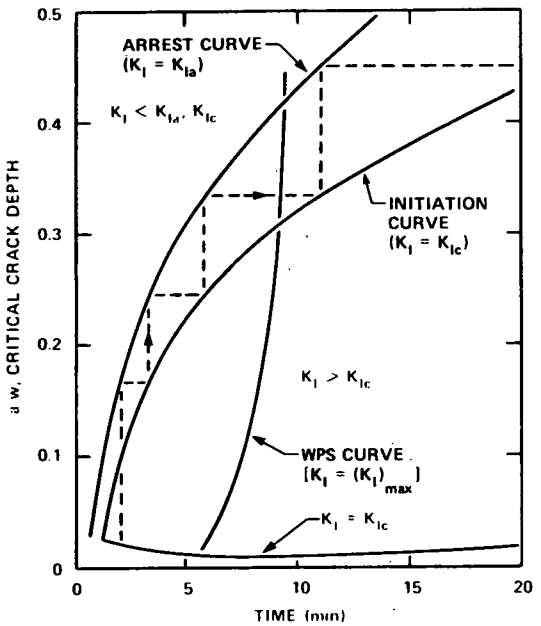


Fig. 2. Critical-crack-depth curves for a PWR LOCA assuming a long axial flaw, high concentrations of copper and nickel, and normal end-of-life fluence.

Warm prestressing, as referred to above, is a term used to describe a situation where K_I is decreasing with time (t) when K_I becomes equal to K_{Ic} by virtue of a decrease in temperature. It has been postulated[9] and demonstrated experimentally[9,10] that under these conditions a flaw will not propagate; that is, a flaw will not initiate while K_I is decreasing. In Fig. 2 the WPS curve is the locus of points for $K_I = (K_I)_{max}$ ($dK_I/dt = 0$). To the left of the WPS curve $dK_I/dt > 0$ and thus crack initiation can take place, but to the right of the WPS curve $dK_I/dt < 0$, and crack initiation will not take place. For the particular case illustrated in Fig. 2, WPS limits crack propagation to ∿40% of the wall thickness.

Even if WPS were not effective, the flaw could not completely penetrate the wall under thermal-shock loading conditions only. This is a result of the substantial decrease in K_I as the crack tip approaches the outer surface (see Fig. 1) and has been demonstrated recently in a thermal-shock experiment.[11] However, when pressure is applied in addition to the thermal loading, the possibility of vessel failure (complete penetration of the wall) exists for some assumed conditions.

FRACTURE MECHANICS CALCULATIONAL MODEL

Linear elastic fracture mechanics (LEFM)[12] has been used thus far to analyze the behavior of a flaw during the postulated overcooling accidents. The initial flaw was assumed to be quite long on the vessel surface, to be oriented either in an axial or circumferential direction and to extend radially through the cladding into the base material. The thin layer of stainless steel cladding on the inner surface was included as a discrete region, in which case its effect on temperature and stress and thus K_{Ic}, K_{Ia}, and K_I were accounted for.

Fracture toughness data (K_{Ic} and K_{Ia} vs T − RTNDT, where T is the temperature and RTNDT is the reference nil ductility temperature) were taken from ASME Section XI,[13] and the reduction in toughness due to radiation damage was estimated using Eq. 1, which was recently proposed (tentatively) by Randall[8] as a revision to Reg. Guide 1.99, Rev. 1.[14]

$$\Delta RTNDT = f\,(Cu, Ni, F) \propto (F)^{0.27}\,, \qquad (1)$$

where

$2 \times 10^{17} \leq F \leq 6 \times 10^{19}$ neutrons/cm^2 ,

ΔRTNDT = change in RTNDT at tip of flaw due to fast neutron exposure,

Cu, Ni = copper and nickel concentrations, wt %

F = fast neutron fluence ($E \geq 1$ MeV) at tip of flaw

A typical attenuation of the fluence through the wall of the vessel that includes a correction for the effect of displaced atoms (DPA) on radiation damage was also recently proposed by Randall[8] and is being used in the ORNL studies. The relation is

$$F = F_o e^{-0.0094a\ mm^{-1}}, \quad (2)$$

where

F = fast neutron fluence at tip of flaw

F_o = fast neutron fluence at inner surface of vessel

a = depth of flaw

It is of interest to note that the use of Eq. 1 as opposed to Reg. Guide 1.99, Rev. 1, and the inclusion of the effects of DPA in the fluence attenuation equation result in relatively greater estimated values of radiation damage (ΔRTNDT) deep in the wall of the vessel.

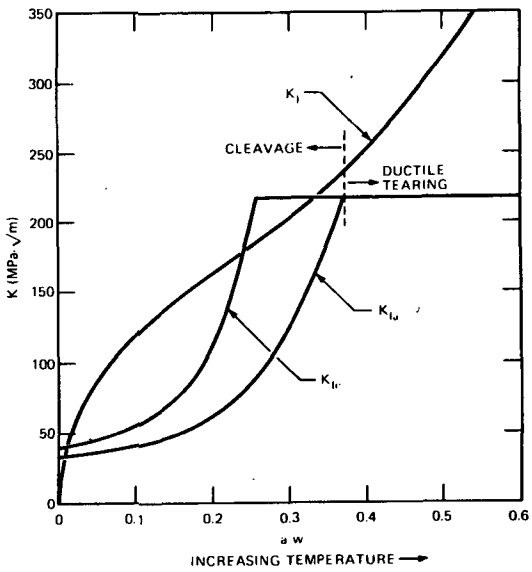


Fig. 3. Plots of K_I, K_{Ic} and K_{Ia} vs fractional crack depth at a specific time in an OCA transient, indicating initiation but no arrest unless on the upper shelf.

For some postulated OCA's, following crack initiation the tip of the fast-running crack will encounter upper-shelf-toughness temperatures prior to crack arrest, as illustrated in Fig. 3. Since techniques are not yet well established for evaluating flaw behavior under these conditions, it was assumed that crack arrest would not occur if K_I was above an arbitary upper-shelf toughness value of 220 MPa $\sqrt{m}$ prior to a calculated arrest event.

The procedure used for evaluating the integrity of a pressure vessel was to calculate, using the above model, the threshold or critical values of RTNDT corresponding to incipient initiation (II) of a flaw and incipient failure (IF) of the vessel (extension of the flaw through the wall) and then compare these critical values with the estimated actual values for a particular PWR pressure vessel. To obtain the critical values of RTNDT it is necessary to specify a transient, the fracture-mechanics model, a failure criterion and an initial (zero fluence) value of RTNDT ($RTNDT_o$), although the results are not very sensitive to the latter parameter. To obtain the actual value of RTNDT for a specific plant it is necessary to have a consistent set of values for the fluence, Cu, Ni and $RTNDT_o$ that corresponds to an area of the vessel wall that is most likely to experience propagation of a flaw; that is, the area in which the worst combination of the four parameters exists.

For convenience the particular values of RTNDT that are compared with each other are the values corresponding to the inner surface of the vessel wall, using material properties for the base material rather than for the cladding. These values of RTNDT are referred to herein as $(RTNDT_s)_C$, the critical value, and $(RTNDT_s)_A$, the actual value.

The critical value of RTNDT is the minimum value, with respect to both time in the transient and crack depth, that results in $K_I = K_{Ic}$ and/or crack penetration of the wall (no arrest). Since $K_{Ic} = f\ (T, RTNDT_o, \Delta RTNDT)$ only,[13] where T is the temperature at the crack tip, it is only necessary to determine these three parameters

and K_I to perform the analysis. Values of ΔRTNDT are calculated from Eq. 3, which was obtained by combining Eqs. 1 and 2.

$$\Delta RTNDT = \Delta RTNDT_s \; e^{-2.54 \times 10^{-3} a \; mm^{-1}} \tag{3}$$

The complete analysis for obtaining $(RTNDT_s)_c$ was performed with the computer code OCA-II,[15] which accepts as input the downcomer-coolant-temperature and primary-system-pressure transients and automatically searches for $(\Delta RTNDT_s)_c$. For some OCA's $(\Delta RTNDT_s)_c$ corresponds to incipient initiation followed by crack arrest and no reinitiation, as shown in Fig. 4 assuming WPS to be ineffective. However, increasing $\Delta RTNDT_s$ will eventually result in failure (no arrest), and the corresponding minimum value is $(\Delta RTNDT_s)_c$ for incipient failure. For other OCA's, $(\Delta RTNDT_s)_c$ corresponds to both incipient initiation and incipient failure because, as shown in Fig. 5, there is no arrest following initiation of a shallow flaw. This latter situation tends to be typical of high-pressure transients and the former of low-pressure transients.

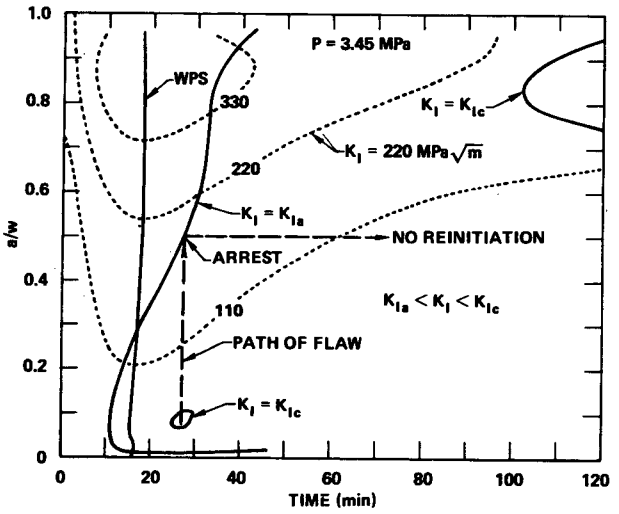


Fig. 4. Critical-crack-depth curves for an OCA illustrating incipient initiation followed by arrest and no reinitiation.

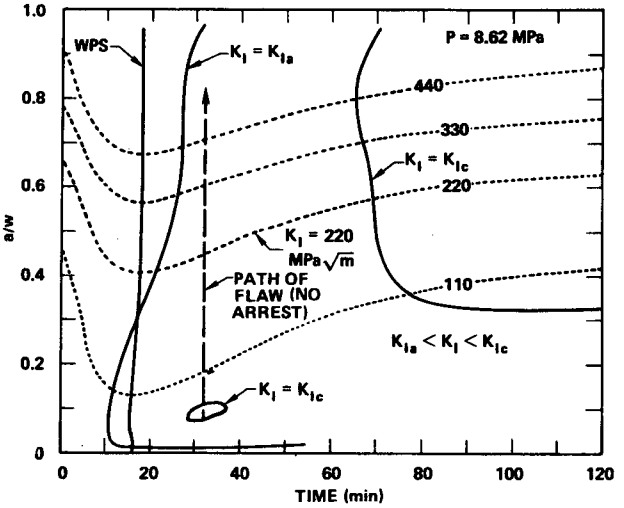


Fig. 5. Critical-crack-depth curves for an OCA illustrating incipient initiation and failure (no arrest unless on the upper shelf).

The sets of critical-crack-depth curves in Figs. 4 and 5 include the locus of points for constant values of K_I. This allows one to determine if arrest takes place in accordance with a maximum specified value for K_{Ia} (220 MPa $\sqrt{m}$ for these studies). In Fig. 4 it does and in Fig. 5 it does not. [The initiation and arrest curves in Figs. 4 and 5 were extended beyond points corresponding to existing maximum values for K_{Ic} and K_{Ia} (∿200 MPa $\sqrt{m}$) using the K_{Ic} and K_{Ia} equations in Ref. 13 for extrapolation purposes; thus, the extensions of the initiation and arrest curves beyond these points are fictitious to some extent but nevertheless allow one to apply different upper-shelf toughness values when using the critical-crack-depth curves to evaluate flaw behavior.]

The existence of two initiation loops (locus of points for $K_I = K_{Ic}$) in Figs. 4 and 5 suggests additional criteria for calculating $(\Delta RTNDT_s)_c$. One is a reasonable range of depths for initial flaws, and the other is the duration of the transient (t_{max}). For the cases depicted by Figs. 4 and 5, specification of a maximum initial fractional flaw size of 0.15 made a difference, because for lower values of $\Delta RTNDT_s$ the small initiation loop (actually just a point for incipient initiation) would disappear, and $(\Delta RTNDT_s)_c$ would be determined by the other initiation loop in accordance with some other criteria such as a greater critical flaw depth.

EVALUATION OF THE FM MODEL

The validity of LEFM for application to thermal-shock problems has been verified in a series of thermal-shock experiments with thick-walled steel cylinders.[10,11,16] These experiments were designed to exhibit flaw behavior trends calculated to exist during OCA's and thus included initiation and arrest of long axial shallow and deep flaws, a stepwise progression of the flaw deep into the wall, arrest in a rising K_I field ($dK_I/da>0$) and WPS with $dK_I/dt<0$. There are still some areas of uncertainty, but in each of these areas the FM model described above is believed to be conservative. The degree of conservatism is not known at this time, but programs are underway to obtain such information. The presumed conservative features in the model include (1) consideration of long flaws that extend through the cladding, (2) no arrest on the upper shelf, and (3) to some extent a disregard for the beneficial effects of warm prestressing. Long surface flaws have a greater potential than others for penetrating deep into the wall, but the probability of a long flaw existing as an initial flaw and of any length flaw extending through the cladding presumably is very small. One justification for assuming long flaws was that under thermal-shock loading conditions and in the absence of cladding short flaws tend to extend on the surface to become long flaws.[17] However, it may be that the cladding will prevent short flaws from extending on the surface and if so would limit radial growth of the flaw.[18]

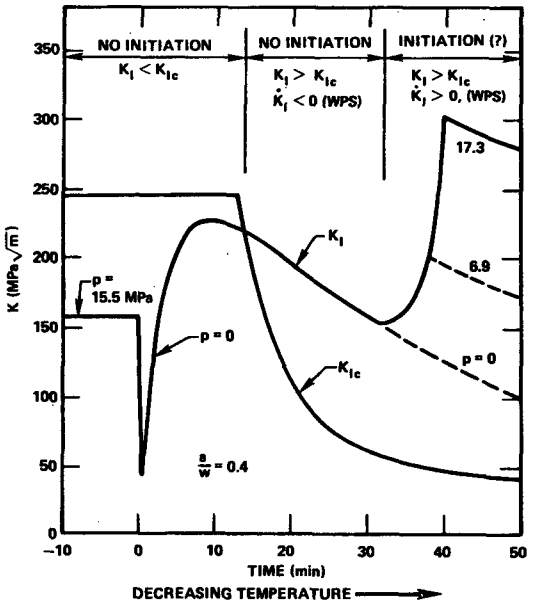


Fig. 6. Illustration of an OCA transient involving repressurization and two types of WPS.

If long flaws through the cladding must be considered, there is still the possibility that the tearing resistance of the material will be sufficient to permit arrest on the upper shelf, and it is also possible that WPS effects in addition to the one mentioned earlier will help to limit flaw propagation. For instance, Fig. 6, which compares K_I and K_{Ic} for a particular crack depth during a postulated transient involving loss of pressure and then repressurization, indicates two types of WPS. During normal operation of the reactor ($t<o$), the material toughness corresponds to upper shelf conditions and K_I is relatively low, as indicated. The transient starts at time zero, and as it progresses K_I becomes equal to K_{Ic}, but only after K_I has begun to decrease with time. Thus, crack initiation would not take place even though K_I becomes substantially greater than K_{Ic}. When repressurization finally takes place, K_I increases with time again, but WPS experiments conducted by Loss, Gray and Hawthorne[9] indicate that because of the particular thermal and loading history that the stationary flaw was exposed to the effective value of K_{Ic} would be elevated, perhaps to a value equal to the previous maximum value of K_I. Thus, presumably some repressurization would be possible, but this particular beneficial effect of WPS was not included in the FM model. (There is some hesitancy at this time to take advantage of WPS even with $dK_I/dt<0$ because there is no assurance that dK_I/dt will remain negative.)

OCA PARAMETRIC ANALYSIS

To obtain a better understanding of the sensitivity of $(RTNDT_s)_c$ to the many parameters involved in an OCA FM analysis, a parametric study was conducted, assuming a constant pressure and an exponential decay of the downcomer coolant temperature.

The temperature transient is expressed as

$$T_c = T_f + (T_i - T_f)e^{-nt} \quad , \tag{4}$$

where

T_c = downcomer coolant temperature,
T_i = initial temperature of vessel wall and coolant,
T_f = final (asymptotic) temperature of coolant,
n = decay constant,
t = time in transient.

The fluid-film heat transfer coefficient (h_f) which is a necessary input to OCA-II, was assumed to be independent of time and for most cases was assigned a value that is achieved with the main circulating pumps running (5680 $W \cdot m^{-2} \cdot °C^{-1}$). In order to determine the sensitivity of $(RTNDT_s)_c$ to h_f a relatively low value corresponding to natural convection cooling (1700) was also used for a few calculations.

A list of pertinent input data for the parametric analysis is included in Table 1, and a summary of results of the analysis is presented in Fig. 7, which shows the relation between $(RTNDT_s)_c$ and pressure (p) for $RTNDT_o = -7°C$ and for several values of T_f and n, ignoring the beneficial effects of WPS. The dashed lines in Fig. 7 correspond to both incipient initiation (II) and incipient failure (IF), the latter corresponding to no crack arrest following crack initiation. The solid line corresponds to II only; however, as indicated, only a small increase in $RTNDT_s$ is required for failure, except as the pressure approaches zero. As already mentioned, thermal shock alone will not drive the flaw completely through the wall.

Table I. Input data for parametric analysis

Vessel dimensions, mm	
Outside diameter	4800
Inside diameter	4370
Cladding thickness	5.4
Flaw type	Long, axial, through clad
T_i, °C	288
T_f, °C	66, 93, 121, 149
n, min^{-1}	0.015 — ∞
t_{max}, h	2, 1[a]
h_f, $W \cdot m^{-2} \cdot °C^{-1}$	5680, 1700[a]
p, MPa	0—17.2 in 1.72 increments
$RTNDT_o$, °C	−29, −7, 4

[a]Used in a few cases for comparison purposes.

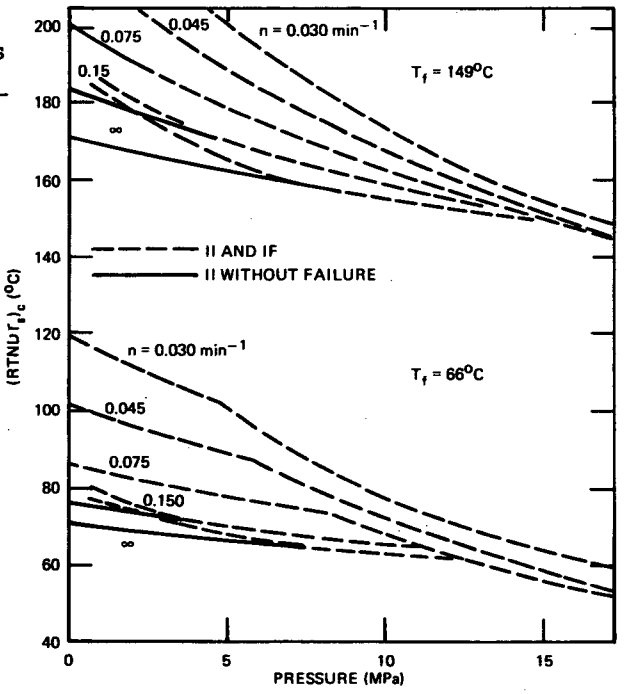


Fig. 7. Summary of results for OCA parametric analysis showing $(RTNDT_s)_c$ vs p for two values of T_f and three values of n and ignoring the beneficial effects of WPS.

The results in Fig. 7 show that at high pressure and for $n>0.030$ min^{-1}, $(RTNDT_s)_c$ is insensitive to the rate at which the coolant temperature decreases; and for the highest pressure considered (17.2 MPa, which is approximately the safety-valve setting) it was found that over the range of T_f values considered (66-149°C)

$$(RTNDT_s)_c \simeq 1.10\ T_f - 22°C \quad . \tag{5}$$

Equation 5 might be used for obtaining a conservative maximum permissible value of $RTNDT_s$ by specifying a reasonable minimum value of T_f. Suppose such a value of T_f is 120°C. Then the maximum permissible value of $RTNDT_s$ would be ∿110°C.

The sensitivity of $(RTNDT_s)_c$ to $RTNDT_o$ was found to be rather small (∿3°C) over the range of $RTNDT_o$ values considered. Furthermore, the sensitivity to t_{max} over the range of 1 to 2 h and to h_f over the range of 1700 to 5680 W·m^{-2}·°C^{-1} was found to be small except for a few cases involving a sensitivity to t_{max} as shown in Table II. For very slow transients ($n = 0.015$ min^{-1}), $(RTNDT_s)_c$ decreased significantly with the decrease in t_{max}. Of course for cases where II takes place prior to 1 h (see Figs. 4 and 5), changing t_{max} from 2 to 1 h would make no difference. This tends to be the case for the more rapid transients.

Table II. Effect of h_f and t_{max} on critical values of $\Delta RTNDT_s$ corresponding to II without WPS

Case			$(\Delta RTNDT_s)_c$, °C			
T_f	n	p	h_f, W·m^{-2}·°C^{-1} /t_{max}, hr			
°C	min^{-1}	MPa	5680/2	1700/2	5680/1	1700/1
66	0.015	3.4	152	157	196	208
66	0.015	17.2	101	107	163	173
66	0.15	3.4	79	95	79	95
66	0.15	17.2	58	61	61	71
149	0.015	3.4	>220	>220	>220	>220
149	0.015	17.2	177	181	216	>220
149	0.15	3.4	180	194	180	194
149	0.15	17.2	151	153	151	157

Another sensitivity investigated was that of $(RTNDT_s)_c$ to the imposed limit on the maximum critical crack depth. Decreasing this limit tends to increase $(RTNDT_s)_c$, and the increase is larger for high-pressure cases since the critical crack depths are greater for higher-pressure transients. Calculations were made for two limiting fractional crack depths of 0.15 and 0.076 and for $n = 0.015$ and 0.15 min^{-1}, $T_f = 66$ and 149°C, and for $p = 17.2$ MPa. The differences in $(RTNDT_s)_c$ associated with the two limits on critical crack depth were small, the maximum values being 8°C.

ANALYSIS OF SEVERAL RECORDED PWR OCA's

Several PWR OCA's have occurred in recent years, and recordings of the pressure and temperature transients have been used as input to fracture-mechanics analyses, using the FM model described herein. The temperature transients were measured upstream of the injection point for the emergency core coolant and thus do not necessarily reflect the temperature of the coolant in the downcomer. However, in the

absence of more accurate data the recorded transients were used so as to obtain some indication of the severity of actual OCA's in terms of pressure vessel integrity.

Table III. Values of $(RTNDT_s)_c$ for several recorded PWR OCA's

Plant (date)	$(RTNDT_s)_c$ w/o WPS, °C	
	Flaw Orientation	
	Long.	Cir.
Robinson (1970)	161 (F)[a]	177 (A)
Robinson (1972)	193 (F)	>249
Robinson (1975)	179 (F)	189 (A)
Rancho Seco (1978)	146	165 (A)
TMI-2 (1979)	98 (F)	124 (F)
R. E. Ginna (1982)	—	192 (F)

[a] A and F in parentheses indicate arrest (with no reinitiation) and failure.

The accidents analyzed and the results obtained are shown in Table III. The values of $(RTNDT_s)_c$ correspond to either incipient initiation followed by crack arrest and no reinitiation or to incipient initiation and failure, as indicated; WPS was ignored, and the imposed limits on critical fractional crack depth were 0.025 and 0.15, the lower limit disallowing crack initiation in the cladding. Because copper and nickel concentrations can be very much different in the circumferential and axial welds, $(RTNDT_s)_c$ was calculated for both crack orientations for the plate-type vessels.

Estimates[14] of $(RTNDT_s)_A$ for all PWR pressure vessels in service today indicate that at this time (September 1982) a few vessels have values approaching 120°C for axial welds and 140°C for circumferential welds. Thus, assuming appropriate flaws to exist in the welds, the analysis indicates that these few unidentified vessels would have a potential for failure today, if the reactor facilities were subjected to a TMI-2-type OCA; however, the Rancho Seco-type transient would not be a threat for several more years.

SUMMARY

A state-of-the-art fracture-mechanics model has been developed that is based on LEFM, includes recent modifications to the radiation-damage trend curves and to the fluence attenuation curve, and is believed to be conservative. The results of an OCA parametric analysis indicate that crack propagation will not take place under the most severe accident conditions if $RTNDT_s < 1.10\ T_f - 22°C$, and it was determined that this relation was not sensitive to $RTNDT_o$, h_f or the assumed duration of the transient over a reasonable range of values.

A fracture-mechanics analysis was also performed for several PWR recorded OCA's, and it was determined, based on preliminary estimates of actual values of $RTNDT_s$ for existing PWR vessels, that a few vessels may have a potential for failure in a few years if subjected to the 1978 Rancho Seco-type transient.

Presumed conservatisms in the fracture-mechanics model are associated with arrest on the upper shelf, the effects of cladding on surface extension of short flaws and warm prestressing. These areas are being investigated to determine the degree of conservatism and to see if the model can be modified to remove excessive conservatism, should it exist.

ACKNOWLEDGMENTS

These studies were sponsored by the Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission (NRC). The authors wish to acknowledge the direction and encouragement provided by Milton Vagins, NRC Project Manager.

REFERENCES

1. W. H. Tuppeny, Jr., W. F. Siddall, Jr., and L. C. Hsu, *Thermal Shock Analysis of Reactor Vessels Due to Emergency Core Cooling System Operation*, Combustion Engineering, Inc., Report A-68-9-1, March 15, 1968.
2. R. C. Hutto, C. D. Morgan, and W. A. Van Der Sluys, *Analysis of the Structural Integrity of a Reactor Vessel Subjected to Thermal Shock*, Babcock & Wilcox Power Generation Division, Topical Report BAW10018, May 1969.
3. D. J. Ayres, W. F. Siddall, Jr., *Finite-Element Analysis of Structural Integrity of a Reactor Pressure Vessel During Emergency Core Cooling*, Combustion Engineering Report A-70-19-2, January 1970.
4. (March 20, 1978, Rancho Seco) Nuclear Safety Information Center Accession #0020-138830).
5. (February 26, 1980 Crystal River 3) Nuclear Safety Information Center Accession #0020-160846.
6. (April 23, 1979 Three Mile Island 2) Nuclear Safety Information Center Accession #0020-137918, 137919, 139931.
7. L. E. Steele, *Neutron Irradiation Embrittlement of Reactor Pressure Vessel Steels*, Technical Report Series No. 163, International Atomic Energy Agency, Vienna, 1975.
8. Personal communication with P. N. Randall, U.S. Nuclear Regulatory Commission, 1982.
9. F. J. Loss, A. A. Gray, Jr. and J. R. Hawthorne, *Significance of Warm Prestress to Crack Initiation During Thermal Shock*, Naval Research Laboratory, Washington, DC, NRL/NUREG 8165, September 1977.
10. R. D. Cheverton, et al., "Thermal Shock Investigations," *Heavy-Section Steel Technology Program Quart. Prog. Rep. for October–December 1980*, NUREG/CR-1951 (ORNL/NUREG/TM-437), March 1981, pp. 37–54.
11. R. D. Cheverton et al., "Thermal Shock Investigations," *Heavy-Section Steel Technology Program Quart. Prog. Rep. for October–December 1981*, NUREG/CR-2141, Vol. 4 (ORNL/TM-8252), April 1982, pp. 52–80.
12. S. T. Rolfe and J. M. Barsom, *Fracture and Fatigue Control in Structures, Applications of Fracture Mechanics*, Prentice-Hall, Inc., 1977.
13. T. U. Marston (editor), *Flaw Evaluation Procedures: ASME Section XI*, EPRI NP-719-SR, August 1978.
14. USNRC, "Effects of Residual Elements on Predicted Radiation Damage to Reactor Pressure Vessel Materials," *Reg. Guide 1.99*, Rev. 1 (Sept. 16, 1976).
15. S. K. Iskander, R. D. Cheverton, D. G. Ball, *OCA-I, A Code for Calculating the Behavior of Flaws on the Inner Surface of a Pressure Vessel Subjected to Temperature and Pressure Transients*, ORNL/NUREG-84, August 1981. OCA-II is a modification of OCA-I. A report is in preparation.
16. R. D. Cheverton, et al., "Thermal Shock Investigations," *Heavy-Section Steel Technology Program Quart. Prog. Rep. for July–September 1981*, NUREG/CR-1197 (ORNL/NUREG/TM-370), April 1980, pp. 52–80.
17. R. D. Cheverton, et al., "Thermal Shock Investigations," *Heavy-Section Steel Technology Program Quart. Prog. Rep. for October–December 1979*, NUREG/CR-1305 (ORNL/NUREG/TM-380), May 1980, pp. 67–70.
18. G. C. Robinson and J. G. Merkle, "Stainless Steel Cladding Investigations," *Heavy-Section Steel Technology Program Quart. Prog. Rep. for October–December 1981*, NUREG/CR-2141, Vol. 4 (ORNL/TM-8252), April 1982, pp. 118–123.

THERMAL-HYDRAULIC CONSIDERATIONS FOR PRESSURIZED THERMAL SHOCK IN PWR's

R. A. Hedrick and R. D. Dabbs

Science Applications, Incorporated
Jackson Plaza Tower, Suite 1000
800 Oak Ridge Turnpike
Oak Ridge, Tennessee 37830

ABSTRACT

The physical mechanisms which produce pressurized thermal shock are discussed considering the nuclear power station systems involved. Particular events presented are large break LOCA, small break LOCA, main steam line break, and steam generator overfeed. The simulations used and the assumptions made to provide the thermal-hydraulic boundary conditions for the fracture mechanics calculations are discussed. The simulations are from government sponsored research, nuclear utilities, and nuclear vendors. The limitations and conservatism of the simulations are also presented.

INTRODUCTION

Pressurized Water Reactors (PWRs) are susceptible to pressure vessel wall crack propagation if flaws are preexistent, the material fracture and arrest toughness have been sufficiently decreased by neutron fluence, and certain thermal-hydraulic events occur. The thermal-hydraulic events which create the environment for vessel wall crack propagation combine rapid cooling of the vessel wall while either maintaining or recovering the primary system operating pressure. These events produce "pressurized thermal shock." The following sections discuss the physical mechanisms and nuclear power station systems involved in pressurized thermal shock events, the phenomena and hardware which require simulation to predict the vessel wall environment, and the results of past and current simulations.

PRESSURIZED THERMAL SHOCK EVENTS

A pressurized thermal shock event must include both rapid cooling of the vessel wall and maintenance or recovery of the primary system operating pressure. Figure 1 shows the three heat transport mechanisms from the high irradiation section of the reactor vessel: conduction to low temperature areas, external heat transport, and heat transport to fluids in the downcomer. The plant systems involved in these three heat transport mechanisms are shown in Figure 2.

Conduction to low temperature areas is a mechanism which occurs normally at operating conditions and is not a significant phenomenon in pressurized thermal shock because of the low spatial temperature gradients and subsequent long transport times.

External heat transport is a mechanism which can involve containment air as the receiving medium or water if the reactor cavity has been flooded. The reactor cavity can be flooded by rupture of any of several water systems which penetrate containment or by actuation of containment sprays. Heat transport from the reactor vessel is limited by the reactor vessel insulation. Even with this insulation removed, free convection to air will not contribute to a pressurized thermal shock event. Operation of the power station with portions of the insulation removed is not considered a likely event; therefore, operation without vessel insulation and flooding the reactor cavity has even a lower probability. Although the degradation of the insulation because of water absorption due to cavity flooding has not been analyzed, it is not judged to be sufficient to produce a pressurized thermal shock event. The conclusion is that external heat transport is not a significant phenomenon in pressurized thermal shock.

Heat transport to fluid in the downcomer requires lowering of the fluid temperature. This can be accomplished in any of three ways: depressurization of the reactor coolant system, injection of colder fluid, and enhanced heat removal from the recirculated reactor coolant. Depressurization of the reactor coolant system will result from any breach of the primary system with the magnitude of the depressurization and subsequent recovery being determined by the hole size and the safety injection systems capacity. The actuation of the safety injection systems result in injection of colder water into the primary system. The temperature of the fluid next to the vessel wall will depend on the quantity and point of injection as well as the degree of mixing with the primary fluid. Heat can be removed from the recirculated reactor coolant by any of three systems: chemical and volume control, residual (decay) heat removal, and the steam generators. The chemical and volume control and the residual heat removal systems do not have the capacity to produce a pressurized thermal shock event. The steam generators, however, have ample capacity to overcool the primary fluid. The conclusion is that reactor coolant system depressurization, safety system injection, and excessive heat removal by the steam generators are all capable of producing pressurized thermal shock events.

From the above discussion, pressurized thermal shock events are limited to three classes: loss of primary coolant, main steam line break, and steam generator overfeeds. Loss of primary coolant events are normally subdivided into large break and small break. The large break event does not result in primary system repressurization and, therefore, does not produce pressurized thermal shock but only thermal shock. Therefore, our interest is limited to the small break event (e.g., open pressurizer relief valves). These events result in primary coolant temperature reduction due to depressurization and the mixing of the safety injection fluid with the primary coolant. The main steam line break class includes rupture of the steam line, open bypass valve, and open relief/safety valve events. These events often result in safety injection system actuation from the contraction of the primary coolant volume resulting from the excess heat removal through the steam generator. The same phenomenon often accompanys the steam generator overfeed class events which range from feedwater flow-power mismatches to full runaway feedwater events where the steam generators are rapidly flooded.

PRESSURIZED THERMAL SHOCK EVENT SIMULATION

Thermal-hydraulic simulation is required to provide temperature and pressure boundary conditions at the reactor vessel wall for any of the previously discussed classes of pressurized thermal shock events. These boundary conditions are sub-

sequently used in the fracture mechanics analysis of the vessel. This section discusses the major models required for these simulations. Figure 3 is a diagrammatic layout of a typical Babcock and Wilcox system. Other vendor plants have components which perform the same functions, therefore this figure is useful in understanding the system component models required to perform an acceptable simulation. This is particularly true for the steam generator feedwater train.

One model required for Babcock and Wilcox plants is unique, the vent valves and associated downcomer mixing. For events in which the reactor coolant pumps are tripped, the vent valves (Figure 1) can open and allow mixing of the warmer upper plenum fluid with the low pressure safety injection system and core flood tank fluid in the downcomer and the high pressure safety injection fluid and primary coolant mixture entering through the cold legs. For some events this mixing can be significant. Figure 4 shows the Babcock and Wilcox calculation [1] of the vessel azimuthal fluid temperature profile for a small break loss of coolant event. Their analysis shows the region of thermal shock to be reduced when mixing with the vent valve flow is considered. The region is a fan shape of approximately three (3) feet in width 65 inches below the center line of the cold leg nozzle and twice that width 135 inches below the center line of the cold leg nozzle one hour into the transient. Similar mixing models are required for all plant types in the cold legs. The degree of mixing of the safety injection fluid in the cold legs will determine the temperature of the fluid next to the vessel wall. In addition to analytical work, the Electric Power Research Institute has a large experimental program in this area.

As previously discussed, most pressurized thermal shock events have a period of reactor coolant system depressurization either from loss of coolant or energy removal. The actuation of the safety injection system results in tripping of the reactor coolant pumps. Therefore, any simulator used must be capable of handling the forced flow to natural circulation transition. Further, in many events sufficient volume reduction occurs in the primary system to void the pressurizer, upper head, and the "candy cane" in once through steam generator systems or top of the U-tubes in U-tube steam generator systems. This results in loss of natural circulation. With the recovery of the primary system by safety system injection, the simulator must model the void collapse and the pressurizer refill. The timing of the pressurizer refill and primary system repressurization can be very important if warm prestressing is taken as a credit. This results from the limited feedwater supply for the steam generators causing, in certain events, the primary fluid temperature to increase before the system is fully repressurized.

Table I presents main steam line break case information for two simulations, IRT [2] and TRAC [3], for a Babcock and Wilcox plant. These simulations have different assumptions concerning the behavior of the pressurizer during refill. The IRT has a "non-interacting" steam-water model. It assumes the incoming water compresses the steam without condensing any of it. As can be seen in Figure 5, the IRT model predicts system repressurization to begin at approximately 10 minutes into the transient; while the TRAC simulation, which allows full mixing in the steam-water interface node, does not predict any repressurization in the first 19 minutes. These two simulations are bounding analyses for system pressurization for this event.

Because of the importance of the steam generators in pressurized thermal shock events, more detailed modeling of the secondary or power conversion loop is required in the simulations. The two simulations of Table I do not have detailed secondary models but use assumed steam generator secondary-side boundary conditions. The assumptions are quite different in that IRT maintains full feedflow to the ruptured steam generator for 20 minutes while TRAC isolates the generator in 2 minutes. The results of these differing assumptions on the downcomer fluid temperature can be seen in Figure 6. The comparison is dramatic. The IRT event produces pressurized thermal shock while the TRAC event does not. This illustrates the importance of modeling the secondary loop performance in order to provide realistic steam generator secondary-side conditions.

TABLE I

Main Steam Line Break Case Information
(Babcock and Wilcox Plant)

	IRT (Ref. 2)	TRAC (Ref. 3)
Break	Full Shear Main Steam Line	Full Shear Main Steam Line
Intact Steam Generator Feedflow	100% For 40 sec. Linearly Ramped to 0% in 2 min.	100% for 40 sec. Linearly Ramped to 0% in 2 min. Emergency Initiated @ 30 sec.
Temperature	460°F for 40 sec. Linearly Ramped to 90°F in 2 min.	460°F for 40 sec. Linearly Ramped to 95°F in 2 min.
Ruptured Steam Generator Feedflow	100% for 20 min.	100% for 40 sec. Linearly ramped to 0% in 2 min.
Temperature	Same as Intact Steam Generator	Same as Intact Steam Generator
Pressurizer	"Non-Interacting" Two-Phase on Refill	"Full Interacting" Two-Phase on Refill
HPI	Not Throttled	Not Throttled

The Oak Ridge National Laboratory is performing a pressurized thermal shock study on Duke Power Company's Oconee I plant. Part of this study is the development of a feedwater train model. The predictions of this model [4] for feedflow to the ruptured steam generator during a main steam line break are compared to the assumed boundary conditions of IRT and TRAC in Figure 7. It can be readily seen that without operator intervention the assumption of full feedflow is justifiable except that its duration for the Oconee I plant is 15 minutes instead of 20 minutes. It should be noted that this time lies in the middle of the boundary analyses repressurization times and could, therefore, make warm prestressing an important consideration at Oconee I. Figure 8 compares the feedwater temperature predictions of the ORNL study with the assumed boundary conditions of IRT and TRAC. The ORNL model indicates a much higher feedwater temperature than was previously assumed for most of the transient. This should translate into higher primary coolant temperatures and pressures and a less severe pressurized thermal shock event, although the analysis is not yet complete.

SUMMARY

In summary, there are three major thermal-hydraulic areas requiring modeling attention: mixing, repressurization, and secondary loop. Mixing includes the cold leg injection, the downcomer injection, and Babcock and Wilcox vent valves. Repressurization includes loss of forced circulation; establishment, loss, and recovery of natural circulation; and system repressurization time. The secondary loop includes feedwater train, steam line, and bypass lines. In conclusion, the ORNL study has emphasized the need for plant specific analyses for certain scenarios.

REFERENCES

1. "Reactor Vessel Pressurized Thermal Shock Evaluation," DPC-R5-1001, Duke Power Company, January 1982.

2. R. CERBONE (BNL) to R. KRYTER (ORNL), "Analysis of a Steam Line Break with Primary System Overcooling for a Typical B&W Reactor," August 14, 1981.

3. S. FABIC (NRC) to C. SERPAN (NRC), "Completion of Scheduled Analysis on Pressurized Thermal Shock Scenarios," June 22, 1981.

4. R. KRYTER et al, Oak Ridge National Laboratory Preliminary Results, Unpublished.

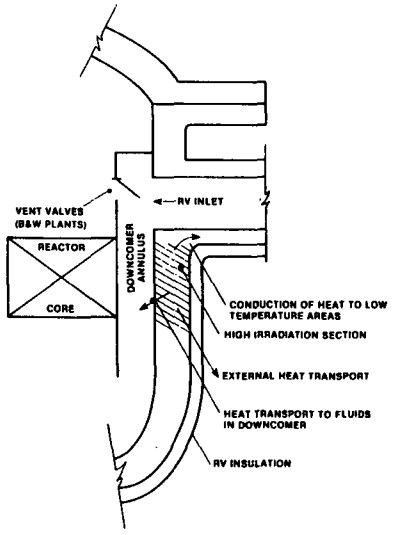


FIGURE 1. HEAT TRANSPORT MECHANISMS FROM HIGH IRRADIATION SECTION OF THE REACTOR VESSEL

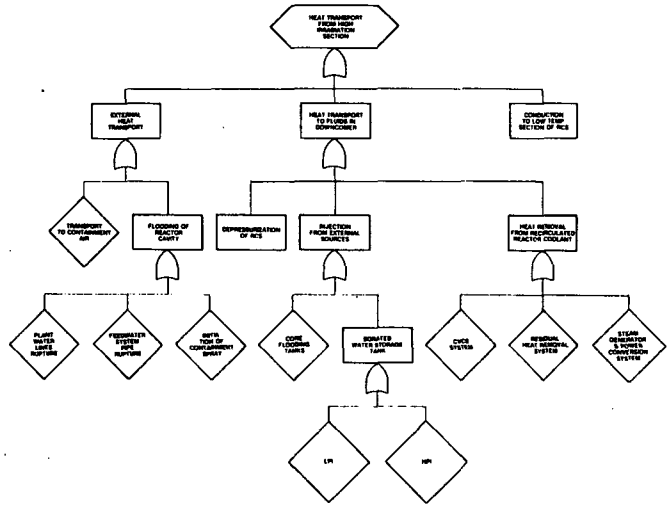


FIGURE 2. SYSTEMS INVOLVED IN HEAT TRANSPORT FROM HIGH IRRADIATION SECTION OF REACTOR VESSEL

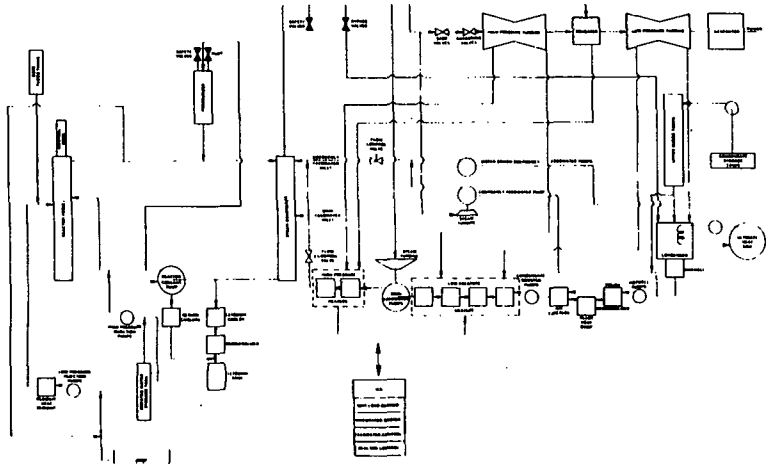


FIGURE 3. B&W DIAGRAMMATIC LAYOUT

FIGURE 4. B&W CALCULATION OF VESSEL AZIMUTHAL FLUID TEMPERATURE PROFILE FOR SBLOCA (REF. 1)

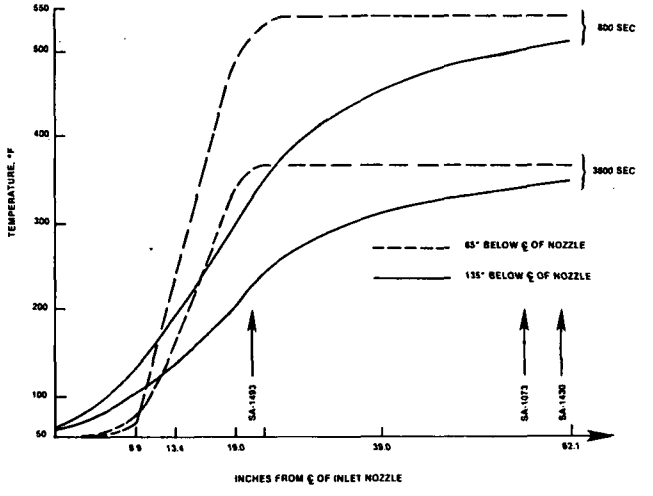


FIGURE 5. PRIMARY PRESSURE PREDICTIONS FOR MAIN STEAM LINE BREAK

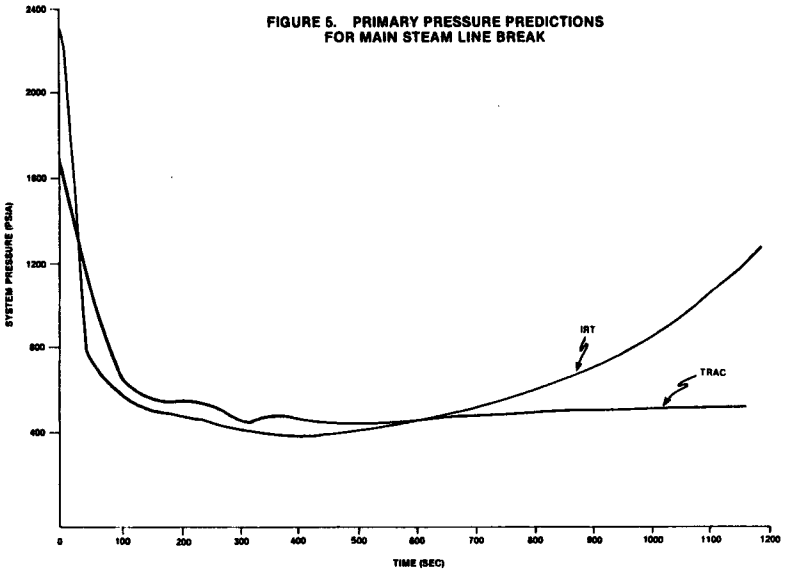


FIGURE 6. DOWNCOMER TEMPERATURE PREDICTIONS FOR MAIN STEAM LINE BREAK

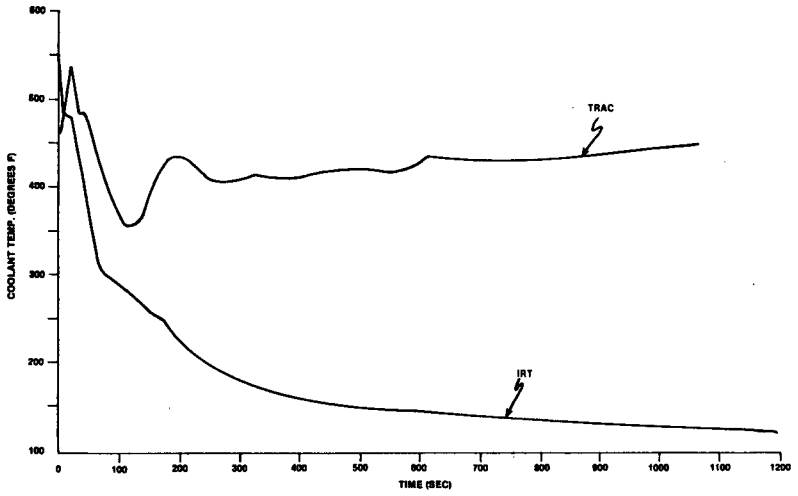


FIGURE 7. COMPARISON OF RUPTURED STEAM GENERATOR MAIN FEEDFLOW BOUNDARY CONDITIONS

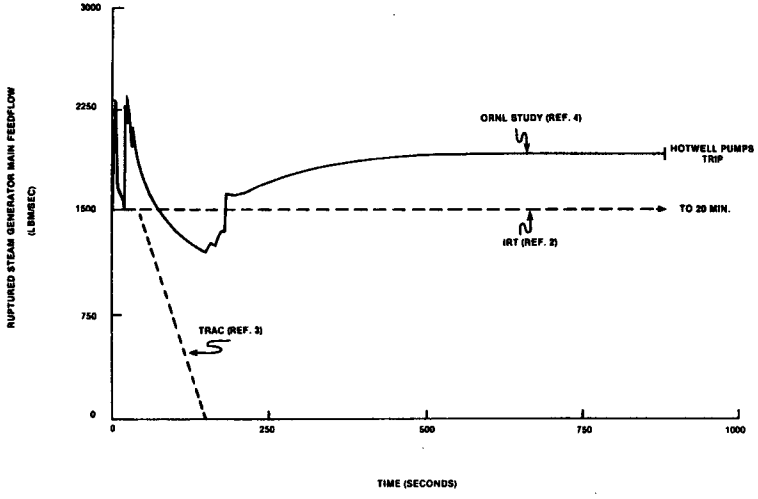
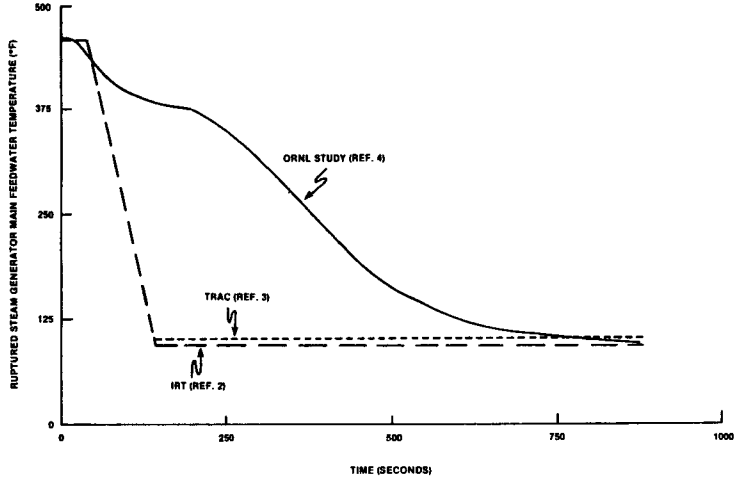


FIGURE 8. COMPARISON OF RUPTURED STEAM GENERATOR MAIN FEEDWATER TEMPERATURE BOUNDARY CONDITIONS



NONLINEAR FRACTURE MECHANICS ANALYSIS AND EXPERIMENT ON THERMAL SHOCK BEHAVIOR OF RPV PLATES

G. Yagawa, K. Ishihara and Y. Ando

Department of Nuclear Engineering
University of Tokyo
Hongo, Bunkyo-ku, Tokyo 113, Japan

ABSTRACT

In this paper, we study two basic thermal shock behaviors of reactor vessel plates with initial cracks: one of which is related to a large break loss of coolant accident(LBLOCA) and the other to a small break loss of coolant accident(SBLOCA). In order to make clear the behaviors of cracks in the reactor pressure vessel steels under these conditions, two kinds of experiments are performed.

First, we show briefly a thermal shock fracture experiment concerning the LBLOCA using a 250 mm thick A533B class-1 steel plate. Next, we explain another experiment simulating the pressurized thermal shock anticipated in the SBLOCA using a 15 mm thick A508 class-3 steel plate. With regard to the latter experiment, a numerical analysis is performed on the three-dimensional as well as nonlinear fracture mechanics parameters J and $\hat{J}$.

The comparison between the experiment and the numerical analysis is found favorable.

INTRODUCTION

In these years, the role of nuclear power plants becomes large with the increasing demand for economical and reliable energy sources. Particularly, it is believed that the LWRs(light water reactors) which are operated in many places would play the most significant role for the rest of this century. To evaluate the safety and reliability of this class of reactors has a very important meaning in this context.

From the structural integrity point of view, it is essential to design and construct reactors so reliably that no fatal accidents occur under severe conditions caused by some incident, and make clear whether any possibility of these accidents does exist.

In this regard, there are some discussions that the PWRs(pressurized water reactors) can endure a class of incidents termed pressurized thermal shock(PTS), which is characterized by the rapid cooling of the primary coolant by injection of water using the high pressure injection system, while

at the same time the primary pressure is maintained during the course of the transient with subsequent repressurization[1]. The causes of such events include accidents such as small line break and steam line break.

If the appropriate conditions are met at the time of the above mentioned transient, there might occur the crack propagation from the small flaw located in the inner surface of the pressure vessel, and in the worst case a serious vessel failure results. The conditions of such a phenomenon are the presence of initial flaw, highly embrittled material and applied stresses sufficient for crack initiation and propagation.

In this respect, some studies have been performed particularly in U.S.A. from the view point of experimental and theoretical fracture mechanics[2]~[5]. Almost all of these studies, however, are based on the linear elastic fracture mechanics, though the reactor vessel material is too ductile and tough to apply the linear elastic fracture mechanics in the relevant temperature range of the transient. It is also noted that the three-dimensional approach is inevitable to study the crack initiation and propagation behavior under the thermal transient, because the initial flaw is usually of three-dimensional shape such as semi-circular or semi-elliptical one, the temperature distribution in the direction of the vessel thickness is an important factor for the fracture mechanics analysis and the material toughness differs from one point of the thickness to the other due to the one-sided distribution of the neutron dose.

In this paper, we show first a thermal shock test concerning 250 mm thick A533B class-1 steel plate with an initial surface flaw. The test is performed by injecting the cold water to the plate surface which is held at high temperature initially.

Another thermal shock test is then made with A508 class-3 material manufactured for the use of the nozzle part of the pressure vessel. In this test, we employ the plate with a circular hole simulating the nozzle of the pressure vessel and the initial fatigue cracks are prepared at the edges of the hole before the test. The thermal shock test is performed in the same manner as the first test except that in this case the tension force is applied during the thermal transient to study the effect of pressure holding.

Finally, the test result for the last experiment is discussed using the three-dimensional fracture parameter $\hat{J}$ which is a modification from the conventional J to take account of the thermal stress effect.

THERMAL SHOCK EXPERIMENTS

Experiment Simulating LBLOCA

The actual thick A533B class-1 steel plate is employed for the thermal shock experiment concerning the LBLOCA. The configuration of the specimen is given in Fig. 1. The initial crack is of a semi-elliptical shape with 400 mm length on the cooled surface and 40 mm depth at the center, the front of which is machined with 0.2 mm thick cutter. The initial temperature of the specimen is held at 495°C and no mechanical loading is applied. Then, the water of room temperature is injected at the rate of 0.03 m^3/min to the cooled area(see Fig. 1).

The temperature distributions in the thickness direction measured with thermo-couples located in the hole at the center of the specimen are illustrated in Fig. 2. Figure 3 shows the crack extension after the test on the cooled surface(X-Y plane). On the other hand, Fig. 4 shows the crack extension observed on the crack surface teared after the test. It is observed from these photographs that the crack extension amount due to the thermal shock is about two milimeters at maximum and the crack extension is limited along the crack front line near the cooled surface to about 30 mm depth from the surface.

Experiment Simulating PTS

The specimen employed in this experiment is made of A508 class-3 steel which is usually used in the nozzle portion of the nuclear reactor pressure vessel. The specimen here has two initial through wall cracks which are oriented perpendicularly to the pre-loading direction, and emanating from a circular hole which is machined to simulate the structural discontinuity of the nozzel of the pressure vessel(see Fig. 5). The crack tips are made acute by fatigue testing machine after saw cutting.

The specimen is heated gradually with the induction heating coil up to the temperature of 400°C which is the initial temperature for the present thermal shock test. After holding at the temperature for a while, the specimen loaded mechanically to the tension pre-load of 981 kN with the testing machine. Then, we give the thermal shock to the specimen by spraying the water of room temperature at the rate of 0.094 m^3/min to the both sides of the specimen. The ends of the specimen are fixed at the constant displacement during the thermal transient.

The measured load between two pins versus the load point displacement during the test is illustrated in Fig. 6. As the edges of the specimen are fixed at the constant displacement while it is cooled, the additional load of 343 kN at most occurs in the specimen due to the induced thermal stress.

Figure 7 shows the transient distributions of the temperature in the thickness direction measured with thermo-couples located at plugged holes in the specimen. It can be seen from the figure that the temperature of the specimen decreases fairly fast and the temperature at the mid-thickness becomes nearly as low as that of the cooling water in about 20 seconds. Therefore, it is supposed that the attained maximum load as mentioned above is already reached nearly at this time.

Figures 8(a) and (b) are the photographs of the latticed marks which are punched on one surface of the specimen before the test at intervals of about 1 mm to get the information about the deformation of the vicinity around the crack tip on the cooled surface. The accurate values of the displacements of the marks are used to obtain the strain distribution through a picture processing technique with the aid of the finite element method[6]. Figure 8(a) shows the blunted crack tip at 400°C in the stage of the pre-loading. The measured crack opening displacement as estimated from this photograph is about 0.2 mm. On the other hand, Fig. 8(b) shows the photograph of the crack growth in the direction slanted to the initial crack which is taken after the thermal shock test at room temperature. The lengths of the extended cracks are measured to be about 1.0 mm and the COD about 1.0 mm.

Figure 9 shows the crack surface released by force to permit the examination of the fracture surface. As shown in the figure, the crack extension of 1.3 mm length at maximum is observed at the center portion of the thickness.

THEORETICAL STUDY

Non-linear Fracture Parameters

Here, we show two parameters of the non-linear fracture mechanics defined in the three-dimensional field[7].

First, we introduce a surface integral J_m which is defined as a component of the generalized force vector for the crack extension to the direction in the X_m axis, i.e.

$$J_m=\frac{1}{B}\left[\int_{S+S_c}(W\delta_{jm}-\sigma_{ij}u_{i,m})n_j ds\right] \tag{1}$$

where $S+S_c$ is an arbitrarily chosen closed surface including the specified crack front length B with S_c being the crack surface and S the rest(see Fig. 10). B, W, δ_{jm} and n_j are the specified length along the crack front, the strain energy density, the Kronecker's delta and the outward unit normal vector on $S+S_c$, respectively.

Evaluation of the J-integral based on Eq. (1) has such a merit that the integral surface $S+S_c$ can be arbitrarily chosen in the body with the condition that it includes the specified length B of the crack front. In the finite element method, this feature of the present method is beneficial, especially in applying it to surface crack whose geometry is usually complex[7].

It is, however, necessary to note that the calculated value based on the above equation is the average in the finite length B along the crack front.

Since the J-integral given in the above is not applicable to the thermal stress problem which is our concern here, we next introduce the $\hat{J}$-integral, which is defined as the rate of the energy flowing into the crack tip in the three-dimensional solid[7][8], i.e.

$$\hat{J}_m=\frac{1}{B}\left[\int_{S+S_c}(W_e\delta_{jm}-\sigma_{ij}u_{i,m})n_j ds+\int_V \sigma_{ij}(\varepsilon^p_{ij}+\varepsilon^t_{ij})_{,m}dv\right] \tag{2}$$

where W_e, ε^p_{ij}, ε^t_{ij} and V are the elastic strain energy density, the component of plastic strain, the thermal strain and the region surrounded by $S+S_c$, respectively.

Numerical Analysis

A numerical analysis is carried out for the experiment simulating PTS using the finite element method with the model depicted in Fig. 11, which represents only 1/8 part of the specimen because of the geometrical symmetry. The twenty nodes isoparametric element is used and the total number of degrees of freedom is 2463. Three layers of the elements from A to C are arranged in the thickness direction. The material properties, viz. Young's modulus, Poisson's ratio, yield stress, work hardening modulus and thermal expansion rate used here are E=205.8 GPa, ν=0.3, σ_y=441 MPa, H'=1960 MPa and $\alpha=1.0\times10^{-5}{}^{\circ}C^{-1}$, respectively. The flow theory is adopted as the plasticity

theory. The J and $\hat{J}$-integrals are calculated based on Eq. (1) and Eq. (2), respectively, using the three different integral surfaces No.1, 2 and 3 for each layer A through C as illustrated in Fig. 11.

Following the calculation for the pre-loading stage, the numerical analysis for the thermal shock stage is carried out with the boundary condition that the displacement at the top and bottom edges of the plate are zero. The temperature distributions in the thickness direction as shown in Fig. 7 are used to calculate the time dependent thermal stress which occurs in the plate.

Figures 12(a) and (b) show the elasto-plastic boundaries at several time steps. Based on these results, it is estimated that the plate ligament becomes fully plastic in 3 seconds.

Figure 13 shows the comparison between the distribution of the $\hat{J}$-integral in the thickness direction and that of J_{IC} at each time step. Because of the dependency of J_{IC} on temperature, the transient distribution of J_{IC} has the tendency to increase first at the surface of the plate and later gradually at the center, while the $\hat{J}$-integral is always larger at the center than at the surface. According to these trends, it is supposed that the initiation of the crack extension takes place at the center of the thickness at about 2 seconds after the injection of water. It is also noted that, as soon as the crack extends at the mid-thickness, the condition for the crack initiation, i.e. $\hat{J} > J_{IC}$ is satisfied at the surface. Moreover, the large increase of the $\hat{J}$-integral over the critical level for the initiation J_{IC} at the mid-thickness may imply that the length of the crack extension is bigger at the mid-thickness than that at the surface. This qualitative view coincides well with the experimental result as shown in Fig. 9.

DISCUSSION

Here, we discuss the condition of the latter experiment simulating the PTS comparing, say with the normal operating condition of the actual plant. In this experiment, 400°C is selected as the initial temperature of the specimen, which is higher by 75°C than the normal operating temperature 325°C of the pressurized water reactor. As for the hoop stress, that of the actual reactor vessel is as large as 130 MPa caused by the internal pressure, while that of the present test specimen is about 160 Mpa due to the pre-loading of 981 kN. Thus, neglecting the biaxial effect, the stress due to the pre-loading in this experiment is larger by 30 MPa than the membrane hoop stress of the actual vessel. From the above rough consideration, the experimental result in this study may give a certain degree of the conservatism in assessing the pressurized thermal shock in the actual vessel.

Speaking of thickness of the plate, that of the present experiment is definitely thin compared with that of the actual vessel due to the limitation of the capacity of the employed testing machine. This may introduce the plane stress condition to the crack tip, which perhaps involves a kind of resistance against the crack propagation different from the plane strain

condition which is the case in such a thick plate as the actual reactor pressure vessel. In addition, the compliance of the vessel itself is not taken into account in this experiment, although the effect of the compliance on the stability of the crack extension is considered to be significant[9]. These effects on the integrity of the reactor vessel under the PTS should be clarified in the forthcoming studies.

CONCLUSION

The stable cracks of a few milimeters extended from the initial surface crack in the 250 mm thick plate of A533B class-1 steel subjected to the thermal shock relating to the LBLOCA.

In the another thermal shock test simulating the PTS for the A508 class-3 thin plate with the cracks emanating from a circular hole, we observed the stable crack extensions of about 1 mm. The numerical result for the last experiment coincided well at least in quality with the experimental result.

In order to study the stability of a pre-existing crack in the actual reactor vessel under the pressurized thermal shock, it may be necessary to make clear such effects as the thickness of the specimen and the compliance of the vessel itself.

ACKNOWLEDGEMENT

The authors are pleased to acknowledge the discussions by the members of HST and TS Committees organized in the Japan Welding Engineering Society. This work was financially supported by the Japan Atomic Energy Research Institute.

REFERENCES

[1] R. C. Kryter, et al, "Evaluation of Pressurized Thermal Shock," Report NUREG/CR-2083 ORNL/TM-8072, Oak Ridge National Laboratory, (1981).

[2] R. D. Cheverton, et al, "Experimental Verification of the Behavior of Surface Flaws in Thick-steel Cylinders during Severe Thermal Shock," Trans. 6th Structural Mechanics in Reactor Technology, G9/1, (1981).

[3] C. B. Buchalet and W. H. Bamford, "Method for Fracture Mechanics Analysis of Nuclear Reactor Vessel under Severe Thermal Transients," 75-WA/PVP-3, American Society of Mechanical Engineers, Winter Annual Meeting, (1975).

[4] G. Yagawa, M. Ichimiya and Y. Ando, "Theoretical and Experimental Analysis of Semi-elliptical Surface Cracks Subject to Thermal Shock," American Society for Testing and Materials, Special Technical Publication 677, (1979), p.381.

[5] G. Yagawa, M. Ichimiya and Y. Ando, "Thermal Shock Fracture of Initially Cracked Hollow Cylinder," in Proc. 4th International Conference on Pressure Vessel Technology, C23/80, (1980), p.125.

[6] G. Yagawa, S. Matsuura and Y. Ando, "Strain Measurement Using Point Recognition Picture Processing," Trans. Japan Society of Mechanical Engineers, (to be published).

[7] Y. Ando, G. Yagawa and K. Ishihara, "Three-dimensional Non-linear Fracture Analysis Related to Thermal Shock," in Proc. Japan Society of Mechanical Engineers, No.820-2, (1982), p.253.

[8] K. Kishimoto, S. Aoki and M. Sakata, "On the Path-independent Integral-$\hat{J}$," Engng. Fracture Mech. 13(4), (1980), p.841.

[9] P. C. Paris, et al, "The Theory of Instability of the Tearing Mode of Elastic-plastic Crack Growth," American Society for Testing and Materials, Special Technical Publication 668, (1979), p.5.

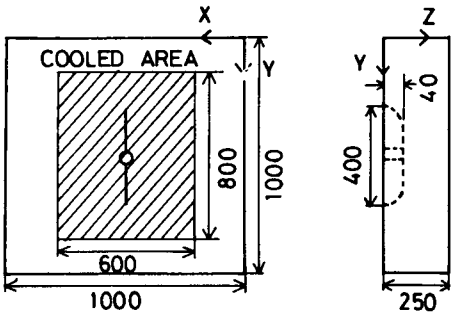


Fig. 1 Specimen for Experiment Simulating LBLOCA.

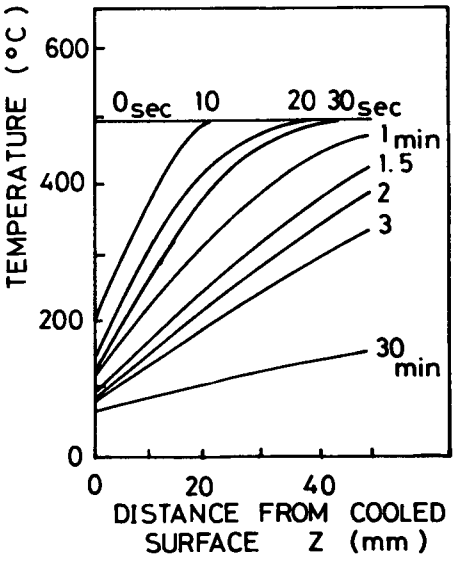


Fig. 2 Temperature Distributions in Thickness Direction.

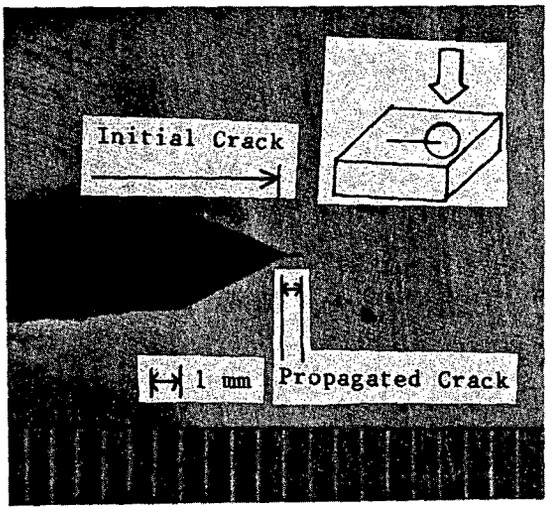


Fig. 3 Crack Growth on Cooled Surface after Test.

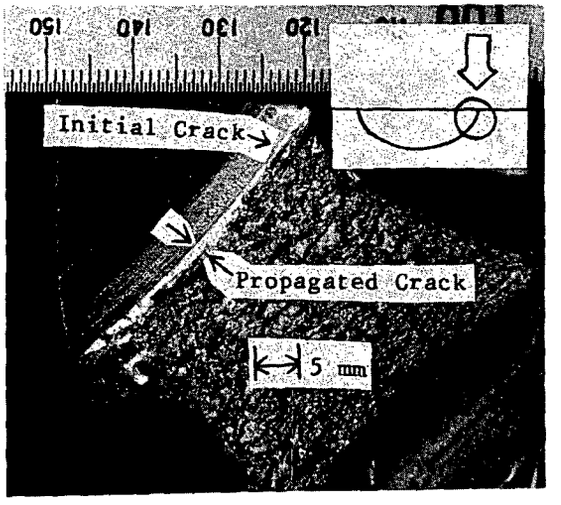


Fig. 4 Crack growth on Crack Surface after Test.

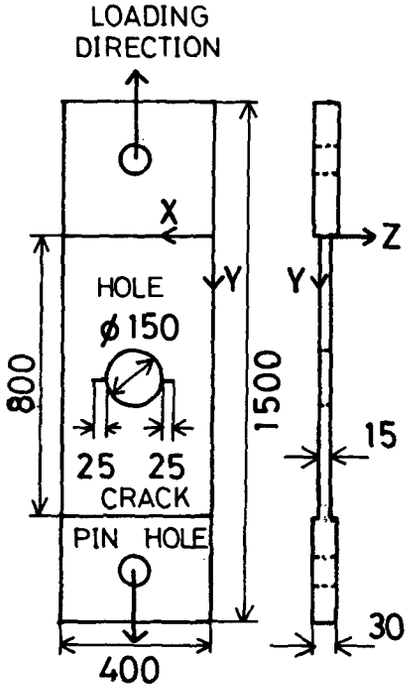


Fig. 5 Specimen for Experiment Simulating Pressurized Thermal Shock.

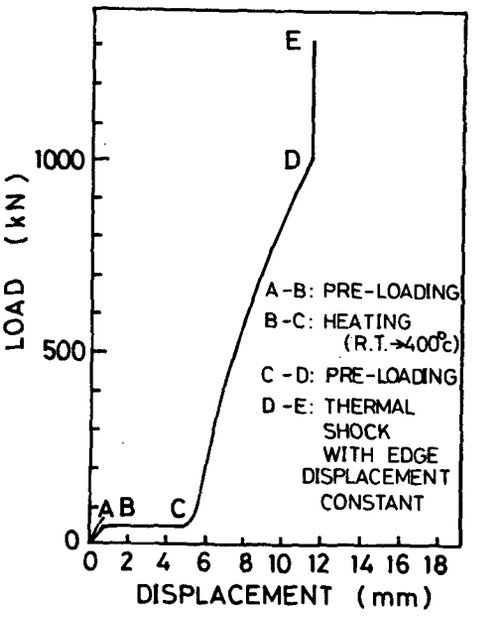


Fig. 6 Load versus Load Point Displacement during Test.

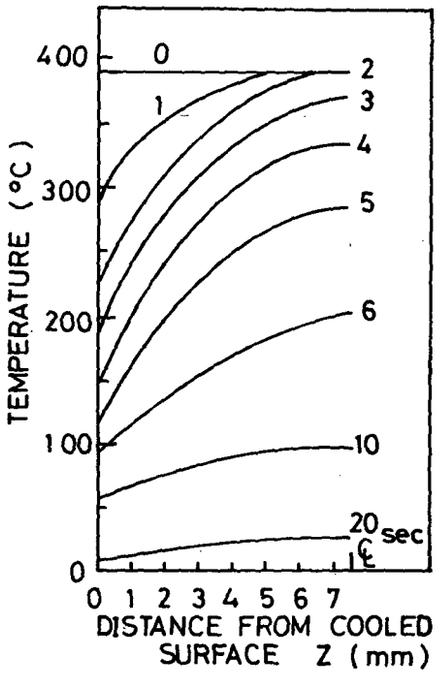


Fig. 7 Temperature Distributions in Thickness Direction.

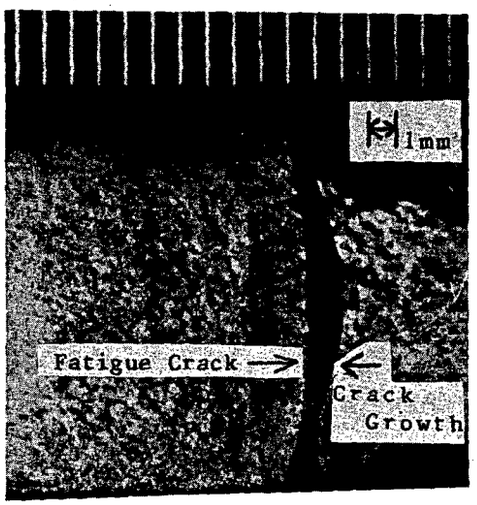
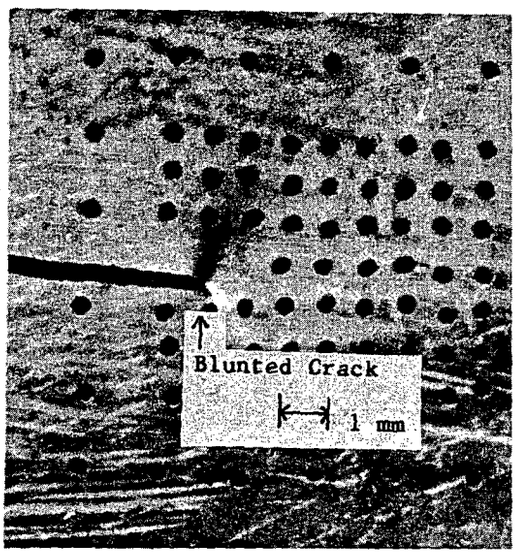


Fig. 9 Crack Growth on Crack Surface.



(a) At Pre-loading Stage (400 C) (b) After Thermal Shock Test (Room Temp.)

Fig. 8 View of Crack on Cooled Surface before and after Thermal Shock.

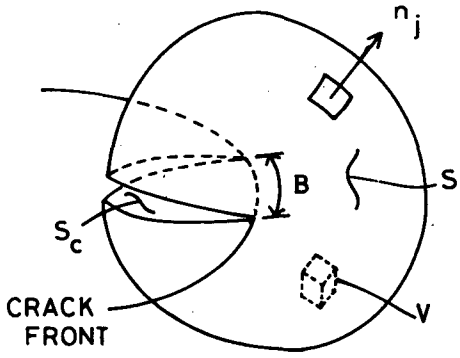


Fig. 10 Integral Closed Surface $S+S_c$ with Specified Crack Front Length B.

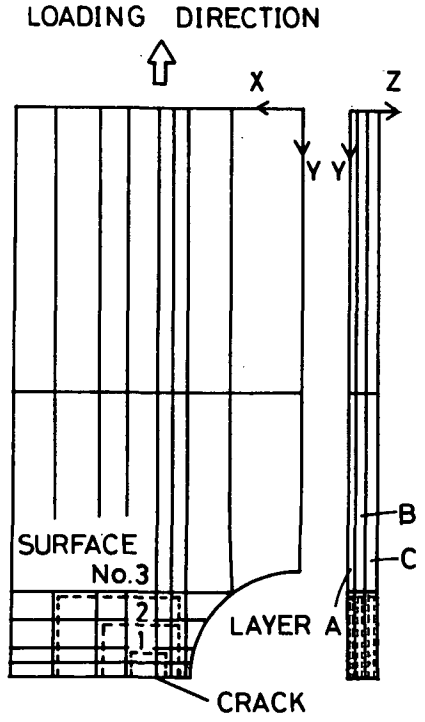
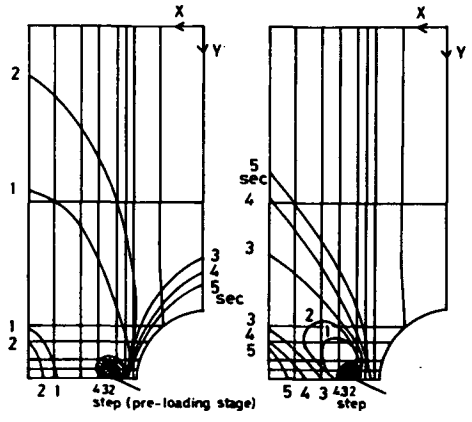


Fig. 11 Model for Finite Element Method Analysis.



(a) Near Surface (2z/t=0.15, t: Thickness)

(b) Near Mid-thickness (2z/t=0.7)

Fig. 12 Elastic-plastic Boundaries during Thermal Shock Test.

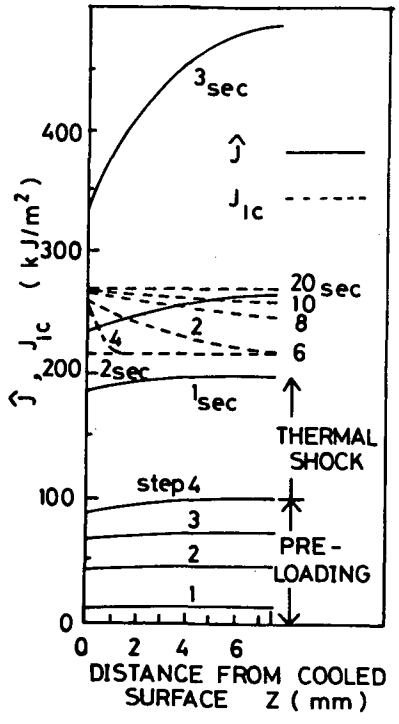


Fig. 13 Comparisons of J and J_{IC} in Thickness Direction.

AN EXPERIMENTAL AND THEORETICAL STUDY FOR THE EVALUATION OF THE RESIDUAL LIFE OF THE PRIMARY CIRCUIT OF LWR'S

A.C. Lucia
Commission of the European Communities
Joint Research Centre - Ispra Establishment
21020 Ispra (Va) - Italy

ABSTRACT

A research activity, aimed at the evaluation of the degree of deterioration of the integrity and at the estimation of the residual life of a nuclear structure is going on at the CEC-JRC of Ispra. Two lines of research have been followed in the last five years:

i) set up of a methodology and implementation of a numerical code for the estimation of the probability of failure of pressure vessels;
ii) on-line monitoring of fatigue crack formation and propagation on scale 1 : 15 models of vessels.

The paper summarizes the main results of these activities and outlines the follow-up: a set of experiments on scale 1 : 5 cladded models of PWR vessels in SA 508 and SA 533 steels.

INTRODUCTION

An investigation programme called Primary Circuit Components Life Prediction, has been started at CEC-JRC of Ispra some five years ago with the aim of developing and validating procedures and methodologies for residual life estimation. This programme is based on the following three activities:

1) Evaluation of the failure probability of reactor pressure vessels in operation, starting from pre-service NDI data and assuming crack propagation laws based on LEFM.
2) Tests on scale 1 : 15 models of BWR vessels for real time monitoring of fatigue-crack formation and propagation.
3) Tests on scale 1 : 5 models of PWR vessels.

The first two activities are approaching their end, while the third one has been just started. The aim of these activities is to develop progressively a systemic approach to the assessment of the safety of reactor primary circuit, i.e. an approach in which material and load histories are jointly considered taking into account uncertainties and evolution in time of the degree of information of the operator.
In this approach inspection techniques associated with accurate estimation of the loading history have a privileged role. Many studies and intercomparison exercises like PISC have put in evidence the limitations still existing in standard procedures based on a single inspection technique. So a reliable approach should rely on a combined use of different inspection techniques.

Figure 1, comparing the values adopted in our study for the probability of non detecting a flaw by US inspection with the values resulting from PISC 1 (alternative

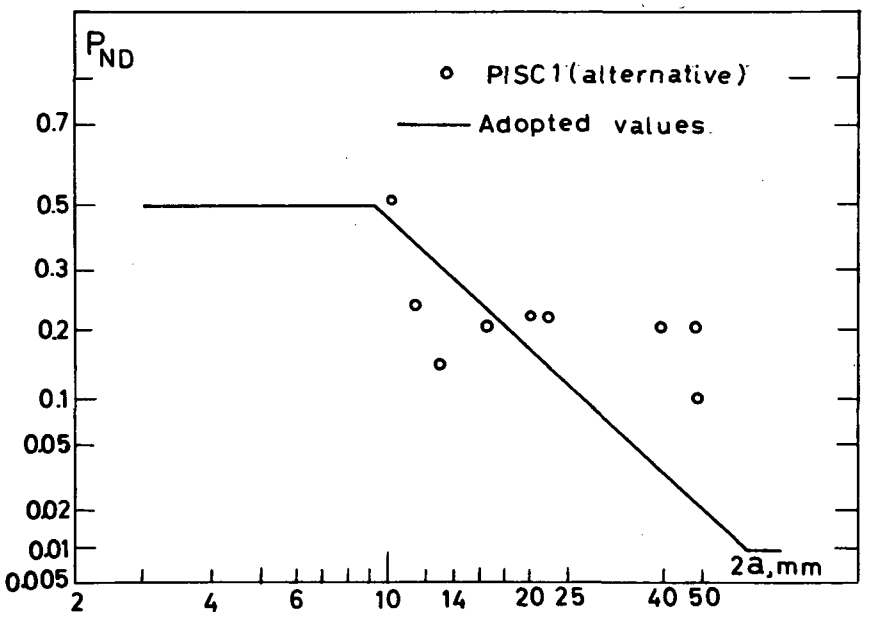


Fig. 1 - Probability of non detecting a flaw by US inspection.

technique), clearly shows how critical is the actual reliability level of US techniques.

ESTIMATION OF THE FAILURE PROBABILITY OF RPV'S

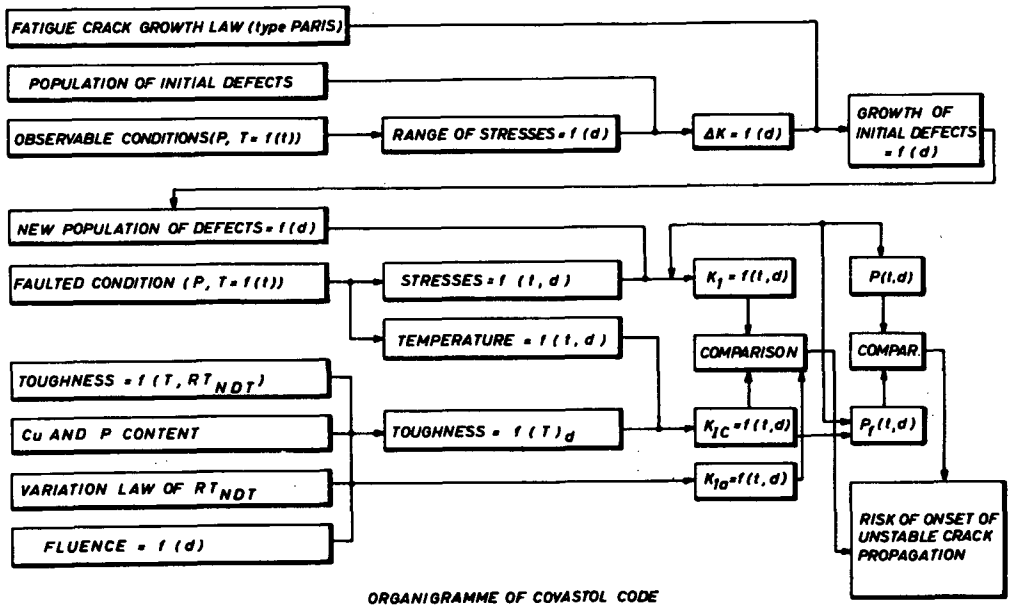
In 1976 the Commission of the European Communities (Ispra Joint Research Centre), the French Commissariat à l'Energie Atomique and Framatome set up a joint committee to direct a research program with the task of developing a method of assessing pressure vessel fast fracture probability and implementing the required digital codes. A computer code (COVASTOL) has been consequently developed. Based on LEFM, it has been designed for application to nuclear reactor pressure vessels [1]. The areas of the vessels susceptible to failure which have been considered were: all the welds of the PV, including nozzle attachment welds, and the inner side of the nozzle including the inner corner.

The basic principle of the computer code (a simplified block diagram of the organisation of its calculation procedure, is shown in Fig. 2), is to introduce the main parameters of fracture mechanics with a statistical distribution.

Actually, we did not use distributions, but histograms built for each parameter on the basis of all the data we collected on it.

The COVASTOL computer code takes into account all the possible combinations of the histogram class intervals at each stage of the computation, but maintaining, when necessary, a certain degree of correlation, in order to keep closer to the physics of phenomena. More details about the code COVASTOL and the related studies have already been published [1, 2, 3].

A sensitivity study has been performed varying the main parameters used in the code, in order to evaluate their importance. Some relevant results of the study on reliability assessment and of the use of COVASTOL for large, intermediate and small LOCA's and steam break accident are here reported. Data obtained from three manufacturers concerning the distribution of defects in LWR pressure vessel welds as



ORGANIGRAMME OF COVASTOL CODE

Fig. 2 - Organigramme of COVASTOL code.

detected during preservice inspection show the great importance of the calibration procedure of the ultrasonic (US) method. For the most sensitive method (CPFC) the overall density of defects is 1.2 defects per meter of weld.

This density shows relevant variations from weld to weld (from 0.2 defects/m up to about 5 defects/m). The length of the defects observed before repair ranges between 3 mm and 1400 mm. These defects are mainly located at the boundary between weld and base metal. A very poor agreement has been found between US data and XR data.

The parameters, having the highest influence on failure probability, are the static fracture toughness (K_{1c}), the width of the defects, their position through wall thickness, and the radiation embrittlement. For the belt line, the conditional probability of rupture decreases by a factor of ten, when the defect goes from the inner surface to a depth of 6 mm. Thermal shocks are the most critical loading, and the temperature of the Emergency Core Cooling Water strongly affects the value of the failure probability, which increases by a factor ten when this temperature is lowered from 20 to 10°C.

Table I summarizes some of the results of the sensitivity analysis. The reported probabilities of onset of unstable crack propagation include the probability of crack existence but are conditional with respect to the accidents. The population of defects and its probability distribution is defined in ref. 2 and 3. The crack dimensions are: width (2a): from 3 to 12 mm; length (2b): from 8 to 64 mm.

From a more general point of view, the following considerations can be singled out from the results of the study:

i) it is very important to correctly size the defects located in the first 2 - 3 cm of the wall inner side;

ii) a sensitivity analysis carried out on the PV as a whole can be misleading: the weight of each parameter on the failure probability depends on the zone of the vessel which is under examination;

iii) pressurized thermal shock loading and surface or under cladding defects constitute dangerous situations requiring further investigations and experiments.

TABLE I

Sensitivity Analysis - Belt Line Weld. ECC Water Temperature = 20°C.			
Input Data	Failure Probability		
	Small LOCA	Inter. LOCA	Large LOCA
Ref. values	8×10^{-9}	2.5×10^{-6}	3.3×10^{-6}
σ x 0.9	10×10^{-9}	4.2×10^{-6}	4.6×10^{-6}
ΔRTNDT x 1.1	10×10^{-8}	1.4×10^{-5}	1.3×10^{-5}
$\Delta\sigma$ x 1.1 (fatigue)	8.8×10^{-9}	2.5×10^{-6}	3.4×10^{-6}
2a x 1.5	3.6×10^{-7}	1.3×10^{-5}	9.7×10^{-6}
2b x 1.5	6.9×10^{-8}	6.3×10^{-6}	6.3×10^{-6}

Inlfuence of ECC Water Temperature - Belt Line Weld. Input Data = Reference Values.			
ECC Water Temperature	Failure Probability		
	Small LOCA	Inter. LOCA	Large LOCA
20°	8×10^{-9}	2.5×10^{-6}	3.3×10^{-6}
10°	2.1×10^{-7}	2.5×10^{-5}	1.5×10^{-5}
3°	3.1×10^{-7}	not calculated	not calculated

TESTS ON SCALE 1 : 15 MODELS OF VESSELS

A research activity, aimed at the development of a method for a reliable monitoring of fatigue deterioration processes in reactor vessels, is going on in collaboration with the University of Milan [4]. This activity is based on a series of experiments carried out on 2 models (scale 1 : 15) of BWR vessels. A three-nozzle uncladded model was used, cyclically pressurized between 0.8 and 14.0 MPa, at a frequency ranging from 10 to 20 cpm. The AE signals, analysed in real time, supplied an immediate information on the continuous degradation of the structure. The same signals, stored on magnetic tapes, were later on subjected to more accurate analyses enabling a verification of the correlation existing between acoustic emission and fracture mechanics parameters. Pre-service and periodic inspections of the vessel were also made by ultrasonics, X-rays and laser interferometry. Comparisons have been made between three-dimensional, finite element calculations (Bersafe code, elastic and elasto-plastic field) and experimental values measured by strain-gages placed on the inner surface of the nozzle regions.

Main results

The results and indications obtained during the tests on scale 1 : 15 models of vessel can be briefly summarized by the following statements:

1) The AE measurement carried out during the hydrostatic test allowed the defective (or high risk) zones of the structure to be identified;
2) The AE measurements carried out during the fatigue cycles allowed the monitoring, in real time, of both the propagation of defects already existing in the weld and the formation of fatigue cracks in the zones of highest stress of the nozzle. The indications in the case of cracks in the weld were, however, more evident than for cracks in the inner corner of nozzles;

3) The interferograms, made with the laser interferometry technique at regular intervals of the fatigue cycling, have provided indications which perfectly agree with those of AE;
4) It was, in one case, quite difficult to detect by US inspection a fatigue through-crack in the inner corner of the nozzle;
5) A combined, complementary use of many different NDI techniques and computer based, correlated analyses of their outcomes seem to be the best way for improving NDI reliability;
6) The strain gage data and the finite element calculations show good agreement in the elastic field. In the elasto-plastic field (the theoretical and experimental values of circumferential deformations as well as the value of the pressure corresponding to the passage from linear-elastic to plastic behaviour have been compared) , some of the experimental data on deformation show a rather relevant discrepancy from calculated values [5].

TESTS ON SCALE 1:5 MODELS OF PRESSURE VESSELS

Starting from the results of the two lines of research presented in the first two chapters, we have started an activity on scale 1:5 cladded models of pressure vessels[6, 7]. The project is aimed at the evaluation of the degree of deterioration of the structural integrity and at the estimation of the residual life of the structure by use of NDI data and analytical models. It is based on a series of tests to be carried out on three identical models (scale 1 : 5, cladded) of PWR vessels. The estimation of the residual life will be made utilizing, as a starting point, the code COVASTOL which will be modified in order to allow the utilization of all data coming from NDI during service (acoustic emission, ultrasonics, radiography, laser interferometry, eddy currents, electric potential method, strain gages, pressure and temperature transducers).

Experimental set-up

The scale 1 : 5 of the vessel models has been chosen in order to have a structural complexity and a size allowing the extrapolation of most of the results obtained. The presence of the stainless steel cladding allows to investigate several problems like cladding effect during thermal shock, undercladding flaws behaviour, effect on US inspection and on acoustic emission measurements, etc. In order to facilitate US inspection from inside (immersion technique) and to be able to apply different methodologies for US inspection, a polishing of the cladding surface has been made with the following prescriptions: roughness $\leqslant 20$ μm, discontinuity between adjacent strips $\leqslant 0.3$ mm. Fabrication defects have been introduced in two of the three identical models of vessel. Lack of fusion, lack of penetration, solidification crack (undercladding) flaws have been realized in two circumferential welds, in the longitudinal one and in the attachment of one nozzle. The dimensions of the defects are approximately: width = 3 mm, length = 30 mm. The pressurization medium is water of controlled and periodically retreated chemical composition. Table II summarizes the main characteristics of the experimental installation.

Phases of the experimental programme

The experimental activity is based on four phases:

a) Phase 0: it includes all NDI pre-service tests for vessels acceptance and qualification, before the first pressurization. A parallel activity on specimens is also included in this phase. The aim of this activity is to supply data on the properties of the ingot from which our vessel models are made, at the same loading conditions at which the vessels will be subjected. This will enable a more appropriate formulation of the distributions of the input data (as far as material properties are concerned) to our codes. Furthermore: the results from tests on specimens

TABLE II

Hardware

Equipment	Main Characteristics
Vessel Models	3 models scale 1 : 5, made from the same ingot; fabricated according with ASME codes; dimensions: h = 217 6 mm; ϕ_{ext} = 892 mm; thickness = 46 mm; number of nozzles: 2; cladding thickness: 3 mm; material: nozzles = SA508 cl.2 steel; vessels = SA533B steel; cladding = AISI 347, strip, one layer.
Spare parts and materials for specimens	SA533: 1 plate, equivalent to one vessel; SA508: 6 cladded nozzles, for replacing on the vessels the failed nozzles; 4 nozzles for specimens; 5 forged rings (same dimensions of nozzles) for specimens.
Pressurization system	P_{max} = 300 bars; flow rate: 180 lt/min; pressurization medium: water; controlled by DAS.
Data Acquisition System (SAS)	Based on multi-task computer (128 Kbytes), connected with a Central Computing System (CCS). Data collected from: strain gages, pressure and temperature transducers, US inspection channels, analog channels, BCD channels. Communication with and control of: pressurization system, US automatic scanner, transient recorders.
Laser interferometry experiment	Based on a 5W Argon laser.
US inspection automatic scanner	For inside inspection. Controlled by DAS. Two arms with removable transducer-slides.
Acoustic emission equipment	Computer based, 16 channels, with transient recorder.
US instrumentation	Multichannel, with transient recorder.
Central Computing System (CCS)	Multi-task computer, with disc, disc-pack and tape mass storage Graphic facilities. Used for data storage and off-line analyses. Connected with JRC main computer (Amdahl).
FEM 181	Tektronix 4081, FEM 181 for automatic meshing of structures for finite elements stress calculations.
X-ray	400 kV equipment.

will be analysed and extrapolated to predict the behaviour of the 1 : 5 scale models under identical loading conditions. The results of the extrapolation will be compared with those obtained on the vessel models themselves. This procedure will assure a check of the extrapolation method.

b) Phase 1: hydrotest. Acoustic emission monitoring during pressurization. The vessel will be completely re-inspected after the hydrotest. The initial population of defects will be identified, also on the basis of results of Phase 0 inspections.

c) Phase 2: hydraulic fatigue at 20°C, $f \leqslant 10$ cpm.

d) Phase 3: high temperature loadings, including thermal shocks.

The results of PISC 1 (alternative procedures) and PISC 2 will be considered for defining inspection procedures and techniques and for comparison with inspection results on loaded structures (service induced defects). During the tests, all the data coming from NDI (pre-service inspection, continuous monitoring and periodic inspection) and from sensors (strain gages, pressure and temperature transducers, etc.) will be collected and stored by a computer. The complete story of each vessel will therefore be stored and will be available at any time for elaboration. Intercomparison of independent analyses performed by different groups will be then possible.

Preliminary theoretical investigations

Preliminary stress analysis of the unflawed vessel model under different loads and at different temperatures have evidenced the relevance of the effect of the cladding. The stress analysis of the flawed model is underway. The theoretical study of thermal shock has been started with the calculation of quench front velocity in the rewetting of the hot dry surface and of temperature distribution through the wall. All the results of these preliminary analyses will be used for the final definition of the experimental conditions.

REFERENCES

1. A.C. LUCIA, J. ELBAZ, R. BRUNNHUBER, "COVASTOL: A Computer Code for the Estimation of Pressure Vessel Failure Probability", in Proc. 5th SMIRT Berlin, 13-17 August, 1979.
2. J. DUFRESNE, A.C. LUCIA, "A Probabilistic Approach to the Evaluation of Pressure Vessels Safety Margins", in Proc. 6th SMIRT Post Conference Seminar N.8., Paris, 17-21 August, 1981.
3. CEC-CEA-Framatome Collab. Contract on PV Failure Probability. Final Report. In press.
4. A.C. LUCIA, C. MAROZZI, A. TERRANOVA, "Detection of Fatigue Crack Formation in Nozzle Welds of Pressure Vessels", ASME Paper 79-PVP-101, June 1979.
5. P. GAVARDI, A.C. LUCIA, A. TERRANOVA, "Analisi Teorica e Sperimentale dello Stato di Sollecitazione di Recipienti in Pressione con Bocchello in Campo Elastico ed Elasto-Plastico", to be published.
6. A.C. LUCIA, J. ELBAZ, "Outline of the Experimental and Theoretical Programme on 1:5 Scale Models of LWR Pressure Vessels", Technical Note N.1-06-01.81-154, Feb. 1981.
7. A.C. LUCIA, "Programme on 1:5 Scale Models of LWR Pressure Vessels", Status Report N.1, Technical Note N.1.05-01.82-95, July 1982.
8. J. AIROLA, M. BIGGIO, U. LOMBARDINI, "Three-Dimensional Elastic Stress Analysis of a 1:5 Scale Model of PWR Pressure Vessel", Technical Note N.1.06.01.82-45, May 1982.
9. J. AIROLA, M. BIGGIO, U. LOMBARDINI, "Three-Dimensional Elasto-Plastic Stress Analysis of a 1:5 Scale Model of a PWR Pressure Vessel", Technical Note N.1.06.01.82-75, June 1982.
10. J. ELBAZ, "Transformazione della Geometria di un Fascio Ultrasonoro mediante Uso di un Diaframma: Applicazione al Metodo per Trasmissione", in Proc. Convegno Naz. Prove non distruttive nella Sorveglianza degli Impianti, Siracusa (Italy), May 1982.

Acknowledgements

The work reported is the result of the collaboration of the CEC-Joint Research Centre with several external organizations, principally CEA (France), Framatome (France) and Politecnico of Milan (Italy).

The author is deeply indebted with Mr. G. Volta, Head of Engineering Division, for his effective and continuous contribution of suggestions, discussions and ideas.

The author wishes also to acknowledge Messrs M. Biggio, R. Brunnhuber, S. Crutzen, J. Elbaz, M. Franchi, M. Galli, P. Jehenson, U. Lombardini, G. Mancini, R. Metivier, G. Piatti for their contributions to the various items of the reported work.

SESSION 8

PRA-2; SYSTEMS APPLICATIONS OF RELIABILITY AND RISK METHODS

Chair: L. Lederman *(CNEN)*
I. Wall *(EPRI)*

AUXILIARY FEEDWATER SYSTEM RELIABILITY

T. J. Raney

Ebasco Services Incorporated
Lyndhurst, New Jersey 07071, U.S.A.

ABSTRACT

The NRC now requires quantitative reliability studies of the Auxiliary Feedwater System as part of the Operating License application for Pressurized Water Reactor plants. These analyses, patterned after those presented in NUREGs 0611 and 0635[2,3], are useful both as absolute indicators of system failure probability and for judging the value of potential design and operating improvements with certain limitations.

The results show that a well designed (i.e., proper mechanical and electrical independence), automatically actuated AFS with three full capacity pumps and no unusual test or maintenance actions affecting it has a reliability which exceeds the NRC acceptance criteria (unreliability between 10^{-4} and 10^{-5} per demand) for the study. The results of full scope nuclear plant probabilistic risk assessments suggest that these partial scope AFS studies become invalid beyond this threshhold because common cause/external events outside their scope have probabilities in this range.

INTRODUCTION

In March 1980 the NRC began requiring all pending Operating License applications for plants utilizing Westinghouse (W) and Combustion Engineering (CE) Nuclear Steam Supply Systems (NSSSs) to perform an availability analysis of the plant Auxiliary Feedwater System (AFS). This was the first broad scale NRC requirement for any quantitative reliability type study as a licensing requirement, and is widely viewed as the beginning of an NRC movement to gradually introduce Probabilistic Risk Assessment (PRA) as an integral part of the licensing process.

AFS DESCRIPTION

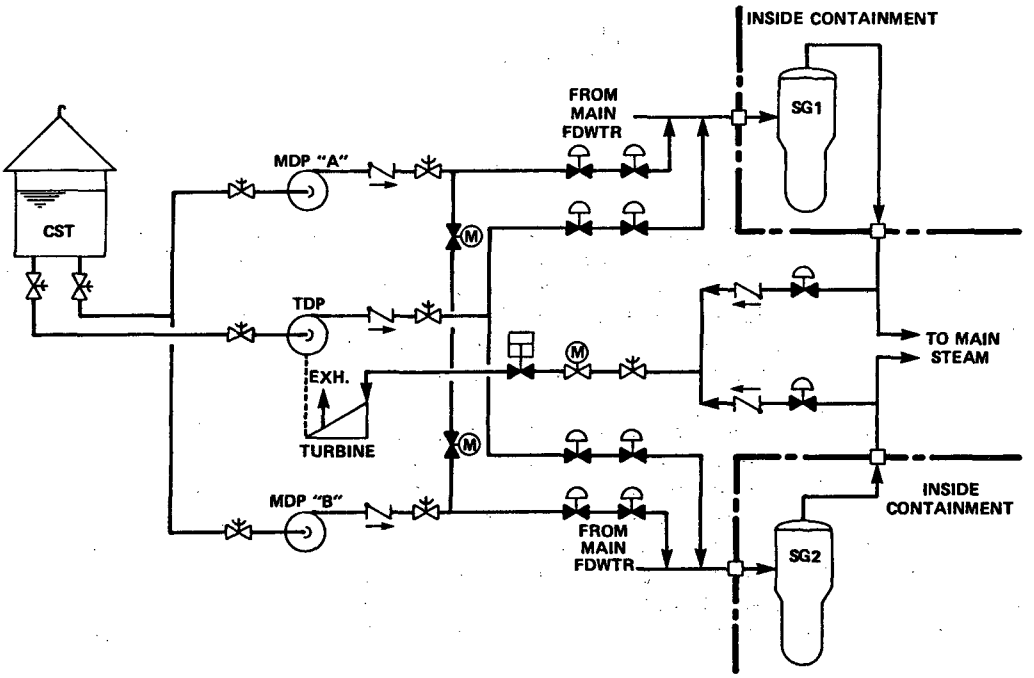
The AFS is a Pressurized Water Reactor Residual Heat Removal System (RHRS) which is used when the Main Feedwater System is not available to hold the Reactor Coolant System (RCS) at hot standby and/or reduce RCS temperature/pressure to the point (approximately 350°F/400 psig) where the closed loop RHRS can be used. The AFS performs this function by providing water from the Condensate Storage Tank (CST) to the secondary (feedwater) side of the Steam Generators (SGs), where RCS heat is removed by a controlled steaming release of SG inventory. The AFS is designated as an Emergency Feedwater System if it is used only for off-normal and accident conditions.

AFS designs vary extensively, but the most widely used design is a "3-pump" system as shown on Figure 1, which employs one 100% capacity steam turbine driven pump (TDP) and two 50% capacity electric motor driven pumps (MDPs). The SGs are the steam source for the TDP and the emergency diesel generators are the power sources

for the MDPs and some power operated valves in the system. DC power from the station emergency batteries is usually required for the control of all pumps and of some power operated valves in the system.

FIGURE 1

FLOW DIAGRAM - TYPICAL AFS



The NRC now requires that the AFS be automatically actuated. Most plants base this actuation on low SG level and some plants additionally utilize a selective logic based on differential pressure between the SGs to avoid releasing additional mass and energy into containment through a faulted steam generator. In the latter case, there is no single "safe" position for the AFS SG admission valves. Most AFS do not automatically modulate flow, but rather run "full throttle" until the operator manually regulates flow using a flow control valve.

The AFS design flow rate is specified by the NSSS vendor based on conservative licensing design basis transient and accident analyses. However, the AFS flow requirements for the plant conditions considered in the availability analysis are typically 60% of the conservative licensing design basis flow requirement. For CE plants and smaller W plants, which usually employ only two SGs, the system function can be fulfilled by either dividing the required flow between the SGs or directing all the flow to one SG. For larger W plants, which employ three or four SGs, the flow must be divided among at least two SGs. (Actually, the AFS flow requirement when one SG is not fed is slightly less than for when all SGs are fed because of the RCS energy dissipated as the unfed SG boils away its inventory).

DETAILS OF STUDY REQUIREMENTS

The AFS availability study was originally mandated by a 3/10/80 NRC letter which specified several new AFS requirements stemming from Item II.E.1.1 of the TMI Action Plan. For the availability study the letter simply referenced similar studies done by the NRC for operating W and CE plants which were presented in NUREGs 0611 and

0635[2,3].

The important features of the required analyses are listed below. It should be noted that some were stated explicitly, some implicitly through the analyses presented and some developed through meetings with the NRC in the course of their review of actual plant analyses.

- The analysis was to calculate AFS availability to function demand; reliability through the system mission was not included.

- Three separate plant conditions were to be considered:

  - CASE 1: Loss of Main Feedwater (LMFW) only,
  - CASE 2: LMFW with a Loss of Offsite Power (LOOP),
  - CASE 3: LMFW with a Station Blackout (SB).

- Standard fault tree analysis techniques were to be used.

- Point estimate results only were required.

- Support systems, such as AC and DC power and actuating logic were to be considered.

- The component and human failure probabilities given in NUREG 0611/0635 were to be used as strictly as possible.

- External events, explicit passive failures and spatially coupled system interactions were not to be considered.

No acceptance criteria were given for the results initially, but the NRC later revealed their judgement criteria for the plants analyzed in NUREG 0611/0635 as shown on Table I. The adjectives under judgement criteria refer to availability while the numbers are unavailability.

TABLE I

NRC JUDGEMENT CRITERIA FOR
AFS AVAILABILITY STUDY

PLANT CONDITION	JUDGEMENT CRITERIA		
	LOW	MEDIUM	HIGH
CASE 1	$10^{-2} - 10^{-3}$	$10^{-3} - 10^{-4}$	$10^{-4} - 10^{-5}$
CASE 2	$10^{-2} - 10^{-3}$	$10^{-3} - 10^{-4}$	$10^{-4} - 10^{-5}$
CASE 3	$1 - 10^{-1}$	$10^{-1} - 10^{-2}$	$10^{-2} - 10^{-3}$

Finally, in the 6/81 Edition of the Standard Review Plan (NUREG 800), the NRC included an Acceptance Criteria in Section 10.4.9 that "an acceptable AFWS should have an unreliability in the range of 10^{-4} to 10^{-5} per demand using.... NUREG 0611 and NUREG 0635."

ANALYSIS RESULTS

The quantitative results of four such analyses performed by Ebasco Services, Incorpor-

porated for a variety of AFS designs are shown on Table II. Table III shows the qualitative system failure mode for the dominant minimal cut sets.

TABLE II

AFS AVAILABILITY STUDIES
QUANTITATIVE RESULTS

AFS SYSTEM TYPE	UNAVAILABILITY		
	LMFW	LMFW/LOOP	LMFW/SB
Plant 1A 2-50% MDPs & 1-100% TDP Automatic	3.4×10^{-4}	4.8×10^{-4}	2.6×10^{-2}
Plant 1B 2-100% MDPs & 1-200% TDP Automatic	1.3×10^{-5}	3.9×10^{-5}	2.6×10^{-2}
Plant 2A 2-100% MDPs & 1-200% TDP Manual	5.1×10^{-4}	5.3×10^{-4}	2.8×10^{-2}
Plant 2B 2-100% MDPs & 1-200% TDP Automatic	$< 10^{-5}$	1.9×10^{-5}	1.4×10^{-2}
Plant 3 2-50% MDPs & 2-50% TDPs Automatic	5.6×10^{-5}	2.0×10^{-4}	4.6×10^{-2}
Plant 4 1-100% MDP & 1-100% TDP Automatic	2.0×10^{-4}	1.1×10^{-3}	2.5×10^{-2}

TABLE III

AFS AVAILABILITY STUDIES
DOMINANT FAILURE TYPES

SYSTEM TYPE	DOMINANT FAILURE TYPE		
	LMFW	LMFW/LOOP	LMFW/SB
Plant 1A	TDP[1] and One MDP[2]	TDP and One MDP	TDP
Plant 1B	• System Valve Alignment Error • One Pump and It's Discharge Check Valve	• TDP and Both MDPs • One Pump and It's Discharge Check Valve	TDP
Plant 2A	Operator Failure to Actuate System	Operator Failure to Actuate System	TDP
Plant 2B	• MDPs Suction Line Valve and TDP • TDP and SG Adm. Valve for Each MDP	• MDPs Suction Line Valve and TDP • TDP and SG Adm. Valve for Each MDP	TDP
Plant 3			TDP
Plant 4	MDP and TDP	DG and TDP	TDP

NOTES: 1. TDP Includes Pump, Turbine and Steam Regulating Valve and Speed Controller.
2. MDP Includes Pump, Motor and, for Case 2, the Associated Emergency Diesel-Generator (DG).

Comparing the quantitative results on Table II to the NRC judgement criteria on Table I, it is seen that Plant 2B fell offscale on high side for Case 1 and was in the high range for Case 2. Plant 4 was in the medium range for Case 1, but fell into the low range for Case 2. All plants appeared in the medium range for Case 3, with Plant 2B having the highest availability.

Useful insight into the relative value of certain design features can be gained by comparing the availability results of systems whose principal difference is the design feature of interest. The results of such comparisons are shown below. It should be noted that such comparisons do not yield absolute indicators of the availability improvements from the design feature of interest, as this is dependent on the order in which the features are applied to the system.

- Automatic AFS Actuation: The unavailability difference between Plants 2A and 2B for Cases 1 and 2 is due almost entirely to the automatic actuation of Plant 2B versus the manual actuation of Plant 2A.

- System Flow Requirement Changes (Realistic vs. Licensing Design Basis): Plants 1A and 1B are actually the same plant with no hardware differences, except that Plant 1A reflects the licensing design basis flow requirement for the system success criteria, where Plant 1B uses the more realistic flow requirement for the conditions analyzed. This effectively upgraded the MDP capacity from 50% to Plant 1A to 100% for Plant 1B. The Case 3 results were unchanged because upgrading the TDP (the only active pump in Case 3) capacity from 100% to 200% does not decrease the pump failure probability and does not affect the fault tree logic model, as the pump can fulfill the system minimum success criteria either way.

- Common Cause Failure From Maintenance Error: Plants 1B and 2B are very similar except that Plant 2B had a connection to an unrelated system which required an incapacitating realignment of some manual valves in the AFS to perform a maintenance operation during plant shutdown. This is similar to the valve misalignment which incapacitated the AFS for several minutes at TMI. The potential for failure to restore the AFS alignment after the maintenance operation was the dominant contributor to unavailability for Plant 1B, and was the major cause of the difference in availability between Plant 1B and 2B for Cases 1 and 2.

- Equipment Protective Trips: The improvement from Plant 2A to 2B for Case 3 is from the removal of the electronic pump overspeed trips for Plant 2B. These trips were redundant to the mechanical overspeed trip, and although they were desirable from an equipment protection standpoint, they were undesirable from an availability standpoint in that they could cause spurious pump trips.

USEFULNESS OF RESULTS

The availability results determined using the NUREG 0611/0635 methodology are good absolute indicators of the reliability of the AFS to perform its mission for the plant conditions analyzed, and can therefore be used as a basis for judging design or operating improvements as long as the following are true:

1. There are no single passive failure vulnerabilities in the system: Passive failures were excluded because of their low probability of occurrence as compared to active failures. However, single passive failures do have probabilities of occurrence in the same range as the simultaneous occurrence of two or three independent active failures. Therefore, the exclusion of passive failures is not justified and will skew the results if single passive vulnerabilities exist in the system.

2. Calculated system unavailability is less than 10^{-5}: The results of full scope PRA studies have shown that external events which can incapacitate an entire system begin to become visible contributors to system failure in this region. For example, the Zion Probabilistic Safety Study found that a severe seismic event which would incapacitate multiple safety systems (including the AFS) has a mean annual frequency of 5.6×10^{-6}. Such numbers are site and plant specific, but 10^{-5} is considered to be a reasonable failure probability threshhold to stop using the results of NUREG 0611/0635 type studies, which do not consider external events, as an absolute indicator of AFS failure probability on demand.

The other simplifying features of the NUREG 0611/0635 analyses did not affect the usefulness of the study results, as discussed below.

1. Availability to Start on Demand vs. Reliability: Neglecting system failure to continue to function through the AFS mission is valid because failure to begin to function on demand dominates over failure to continue to function for the short (4-24 hours) AFS mission for typical AFS components.

2. Failure Data: A verification of the NUREG 0611/0635 failure data base was performed as part of the availability for one plant by reviewing the available AFS operating history ($\sim$5 years) at a similar plant. The results are shown on Table IV. As seen on the figure, there was insufficient data to verify all failure categories, but no major discrepancies were found. Thus, the failure data from NUREG 0611/0635 appeared to be valid.

TABLE IV

DATA BASE VERIFICATION -
NUREG 0611/0635 VS. ONE OPERATING PLANT EXPERIENCE

BASIC EVENT	PROBABILITY (POINT ESTIMATE)		AGREEMENT
	NUREG 0611/0635	OPERATING PLANT	
COMPONENT FAILURES ON DEMAND			
Pump* w/Monthly Test	5×10^{-3} - 1 in 200	0 in 195	Good
Mov* w/Monthly Test	3.1×10^{-3} - 1 in 323	1 in 358	Good
Check Valve	1×10^{-4} - 1 in 10,000	0 in 207	Inconcl.
Manual Valve	1×10^{-4} - 1 in 10,000	0 in 464	Inconcl.
Auto Actuation Logic	7×10^{-3} - 1 in 143	---	---
HUMAN ERRORS			
Failure to Actuate Manual System in 15 Min.	5×10^{-4} - 1 in 2,000	0 in 240	Inconcl.
Misaligned Valve (Local Double Check, No CR ZIL)	5×10^{-3} - 1 in 200	0 in 81	Inconcl.
MAINTENANCE CONTRIBUTION			
Pump	2.1×10^{-3} - 18.5 Hrs/Yr	17.5 Hrs/Yr**	Good

*Includes Control Circuit.
**Plant Policy Allows Preventive Maintenance During Power Operation.

CONCLUSIONS

The NUREG 0611/0635-type AFS availability analyses have been useful for judging design and operating improvements for most AFS systems in use today. Such studies show that a well designed (i.e., proper mechanical and electrical independence) automatic 3 pump system with no unusual test and maintenance actions has a very high availability. However, such studies should not be used for analyzing further availability improvements for such a system, as events outside the scope of this study probably begin to become visible failure contributors in this low ($< 10^{-5}$) failure probability range. In addition, the wide variety of results presented demonstrates that there is no across-the-board dominant failure cause for the AFS. This is highly dependent on the specific design of each system.

REFERENCES

1. Letter from D. F. Ross Jr. (NRC-NRR-DPM) to All Pending Operating License Applicants of Nuclear Steam Supply Systems Designed By Westinghouse and Combustion Engineering, 03/10/80.

2. United States Nuclear Regulatory Commission "Generic Evaluation of Feedwater Transients and Small Break Loss-of-Coolant Accidents in Westinghouse Designed Operating Plants", (NUREG 0611), January, 1980.

3. United States Nuclear Regulatory Commission "Generic Evaluation of Feedwater Transients and Small Break Loss-of-Coolant Accidents in Combustion Engineering Designed Operating Plants", (NUREG 0635), January, 1980.

RELIABILITY ANALYSIS OF A BWR DECAY HEAT REMOVAL SYSTEM

Authors : R.N. Dumolo, Electrowatt Engineering Services (London) Ltd.
Grandford House, 16 Carfax, Horsham, Sussex, RH12 1UP. U.K.

Dr. A Tiberini, Kernkraftwerk Leibstadt AG.
CH-4353, Leibstadt, Switzerland.

ABSTRACT

The reliability of an additional low pressure heat removal system, installed in Leibstadt Nuclear Power Station, has been analysed using probabilistic risk analysis techniques.

Leibstadt is a General Electric boiling water reactor of the BWR/6 product line with a Mark-III containment. The need for the additional system is discussed in terms of the Licensing Criteria applicable to nuclear power plants in Switzerland. As a result of the concern in the U.S. over the reliability of decay heat removal capability of LWR's, further analyses have been undertaken to determine the effect of this additional system on the reliability of the decay heat removal function of Leibstadt.

INTRODUCTION

The Leibstadt Nuclear Power Plant in Switzerland is based upon a General Electric BWR/6 reactor with a Mark III containment. In 1980, Electrowatt Engineering Services Ltd. was awarded a contract by Kernkraftwerk Leibstadt AG (the utility) to perform reliability analyses on the emergency core cooling systems.

An interesting feature of the Leibstadt plant is an additional low pressure ECCS and decay heat removal system which was provided in order to satisfy Swiss licensing criteria. This system, called the "Special Emergency and Heat Removal" (SEHR) system, is similar to some of the "alternate decay heat removal" system variants being discussed in the U.S. Such systems are being considered in order to improve the overall reliability of the decay heat removal (DHR) function, especially following design basis transients and accidents. Of particular interest, therefore, in the work performed by Electrowatt is the improvement in this regard derived from the SEHR system.

This paper describes some of the reliability analysis performed with specific reference to the contribution of the SEHR system towards decay heat removal (i.e. suppression pool cooling). Aspects of decay heat removal from the core are not covered in this analysis since this function does not lead to any dominant accident sequences. Since the work is still under way, and certain aspects of the design (test intervals, logic details, etc) are still unfrozen, the results presented here are preliminary.

LICENSING APPROACH FOR LEIBSTADT

Many aspects of the Swiss licensing basis correspond to U.S. criteria and the Leibstadt plant is, therefore, largely designed in accordance with U.S. practice. Certain licensing rules defined by the Swiss authorities have also influenced the design. In particular, requirements concerning redundancy of safety systems and rules pertaining to decay heat removal under special emergency conditions have affected not only the systems design but also the resulting accident analysis. "Special Emergencies" in this context refer to events such as sabotage, airplane crash, explosion, major fires etc..

General Project Planning Rule 2 (GPPR2) requires that safety systems must be able to fulfil their functions in the event of a single failure. In addition, if the components used in the safety systems require maintenance the safety function must still be fulfilled in the case when one of these components is unavailable due to maintenance or repairs and another component fails on system demand. These requirements result in the so-called "(n-2) criterion".

Compliance with GPPR2 and also the general rules on the removal of decay heat under special emergency conditions has lead to the introduction of an extra system to the Leibstadt Nuclear Power Plant. This system has the dual function of removing decay heat from the core and/or the suppression pool.

The deterministic accident analysis for Leibstadt has been carried out with the assumption that the main heat sink (turbine condenser) is interrupted. Again, this assumption is one of the General Project Planning Rules. This assumption has also been included in the limited PRA being undertaken for Leibstadt by pessimistically assigning a conditional failure probability of unity to the main heat sink for all accident scenarios.

DECAY HEAT REMOVAL

Background

In the U.S., concern over the reliability of the decay heat removal function was prompted by the WASH-1400 study *[1]* which showed that it played a significant role in both PWR and, in particular, BWR transient sequences leading to core melt. As a result, a study to assess decay heat removal concepts for LWR nuclear power plants was undertaken as part of the Nuclear Regulatory Commission (NRC) light water reactor (LWR) safety programme *[2]*. This concern over the decay heat removal function was enhanced by the TMI-2 accident and the topic was subsequently designated as an Unresolved Safety Issue, Task A-45 *[3]*. A part of this Task will be to investigate the need and possible design requirements for improving the reliability of decay heat removal systems of boiling water reactors (BWR's).

The importance of the decay heat removal function for the BWR/6 with a Mark III containment is highlighted in the report of the PRA undertaken for Grand Gulf as part of the RSSMAP programme *[4]*. This report states that sequences involving failure of long term decay heat removal contribute 90% of the total predicted core melt frequency.

Standard BWR/6 systems at Leibstadt

The standard BWR/6 Residual Heat Removal (RHR) System at Leibstadt consists of three independent closed loops (RHR-A, B and C loops). Each loop is located in a separate protected area of the auxiliary building. Two loops consist of a heat exchanger, main system pump, and associated piping. The third loop has no heat exchanger but is arranged so that, at the operators discretion, it can be connected

to either heat exchanger of the other two loops for RHR duty. A system schematic is given in Figure 1.

Removal of decay heat from the containment to the environment relies on the ultimate heat sinks (UHS) available to the RHR heat exchangers. Each of the two RHR heat exchangers has two possible UHS. Under accident conditions the normal heat removal chain is by the Nuclear Island Closed Cooling Water (NICCW) system using the service water system (River Rhine) as the final link to the environment. On failure of this path the Emergency Service Water (ESW) system is valved into the secondary side of the RHR heat exchangers. The ESW system is a closed loop system rejecting heat to air by forced draught cooling towers. System make-up is provided by dedicated ground-well water pumps. The NICCW and ESW for each of the RHR heat exchangers are separated and supplied by different electrical divisions.

The SEHR System

The SEHR system is a low pressure core and/or containment cooling system which is provided to perform both a special emergency function and a post-LOCA core and containment cooling function. It is very similar to a single RHR loop with its own dedicated initiation circuitry, heat exchanger, cooling water source and power source. In order to achieve a highly reliable system all active components are redundant and separated from each other by distance and/or physical barriers.

The SEHR system draws water from the suppression pool and discharges it through a heat exchanger either to the reactor vessel or to the suppression pool. Cooling water for the heat exchangers, diesels and pump room coolers is drawn from one of two ground water wells and discharged into the River Rhine. This source of cooling water adds diversity to the overall DHR concept.

Independence from the other Emergency Core Cooling systems has been achieved except for the two following areas :-

i) The use of the ADS valves which are required to depressurise the vessel for the core injection mode of operation (SEHR is a low pressure system). ADS valves are however provided with additional solenoid valve actuation systems which are classed as part of the SEHR system.
ii) The use of the LPCI-B and C loop vessel nozzles for injection into the vessel.

Power supply to the SEHR system is provided by two dedicated diesel generators. The redundant components of the SEHR system have been divided into two divisions and each division is supplied by one of the diesel generators. No direct connection to the Offsite Power Source is provided in the short term for two specific reasons. Firstly, loss of offsite power under emergency conditions is relatively likely and secondly, the absence of a direct connection prevents the propagation of faults from the offsite power network to the SEHR system. A manual connection to the external 6.6kV power source is provided to enable long term SEHR operation without running the diesels.

The main features of the SEHR system are shown in the conceptual flow diagram given in Figure 2.

SYSTEMS RELIABILITY ANALYSIS

Analysis Techniques

Throughout this limited PRA study for Leibstadt the system reliability analysis has been undertaken using fault tree methodology. System fault trees were analysed using the computer programs FTAP *[5]*, to determine the minimal cutsets, and KITT1 *[6]*, to calculate the system reliability characteristics. Failure data used in the quantification was taken from various sources as given in the following section.

Functional level fault trees involving systems and their interactions were analysed using the in-house program MERLIN *[7]*. This program combines cutsets from the systems analysis through the necessary logic to produce the minimal cutsets for the functional level fault tree 'top event'. The use of MERLIN reduces computer time and allows system interactions to be modelled explicitly.

Sources of Component Failure Data

Quantification of the fault trees was undertaken using mean component failure data which was taken from various sources. Where possible data directly related to nuclear experience was used.

Mechanical and electrical component failure data was taken from the Reactor Safety Study *[1]* with the exception of that for pumps and valves. Data for these last two categories was from the EG & G analysis of the Licensee Event Reports *[8,9]*.

Failure data for instrumentation as given in IEEE-500 *[10]* was used in this analysis. Items of instrumentation of most concern for this PRA study were those required for ECCS initiation, in particular sensors used for pressure, level and temperature measurement.

System control in Leibstadt is achieved by solid state logic. Failure data for the logic boards was determined using manufacturers documentation in conjunction with the standard reference MIL-217C for failure data of electronic components *[11]*.

Human error rates are important during the decay heat removal phase of plant operation because this mode of systems operation can only be realised with operator interventions. The human error rates used have been determined using methodology and data from the report by Swain and Guttmann *[12]*.

RESULTS

Of the analysis carried out to date only those results applicable to decay heat removal are presented. System reliability characteristics are, therefore, given for firstly, the standard decay heat removal systems as installed at Leibstadt and secondly, the Special Emergency and Heat Removal system. A combination of these results, considering all possible system interactions, leads to the failure probability of the decay heat removal function for the Leibstadt plant with the pessimistic assumption of total unavailability of the power conversion system for all accident scenarios.

Standard RHR systems analysis

Analysis of the functional fault tree was carried out not only for the case with all equipment available but also for periods during which major items of equipment are undergoing maintenance and are, therefore, unavailable on a system demand. Components which were considered to be under maintenance were diesel generators, main pumps and motor operated valves.

The mean probability of RHR system failure on demand with no equipment under maintenance was determined to be $3,6.10^{-4}$. This mean probability increased to $1,1.10^{-3}$/demand when maintenance of components during normal operation was considered.

Maintenance on the motor operated valves of the discharge lines cause the largest increase in DHR failure probability. During these maintenance acts there is only one discharge line available to the suppression pool or reactor vessel (maintenance restricted to one discharge line at any one time) and the failure probability of the remaining equipment to provide a DHR function is $1,6.10^{-2}$/demand. Assuming that the 3 principle valves in a discharge leg are maintained sequentially the resulting DHR mean failure probability is $2,9.10^{-4}$/demand corresponding to this maintenance act. The mean probability of the valves being in a failed state due to maintenance was determined using the methodology of WASH-1400 with similar values for the mean duration and frequency of maintenance acts.

In all accident sequences decay heat must be removed from the containment for a considerable period after the event. In this operating regime the reliability characteristic of interest is the "probability of the system being in a failed state at a time t hours after the event". Various values for this probability can be determined depending on the assumptions made for the analyses. Two bounds can be determined relatively easily for this phase, these depending on whether or not repair of failed components is possible. If no repair is possible the probability of system failure increases continuously with time as shown in Figure 3. If repair is possible a lower bound is determined. For components which only have to operate once, i.e. power relays, it is assumed that repair is possible with a recovery factor of $\exp(-t/\tau)$ where t is the time after the event and τ is the mean time to repair. If the components are operating continuously and are monitored then their probability of being a failed state at t approaches an asymptotic value of $\lambda\tau/(1+\lambda\tau)$ where λ is the component failure rate and τ is the mean time to repair. In the long term the probability of the DHR function being failed at time, t, is comprised of the failure probabilities of both repairable and non-repairable components and results in the characteristic shown in Figure 3. The initial large decrease in the probability of being in a failed state is due to the restoration of the offsite power supply for which an initial failure probability of 0.1 at the initiating event was assumed together with a mean restoration time of 2 hours.

Special Emergency and Heat Removal System Analysis

The SEHR system analysis was carried out in a similar manner to that for the standard DHR systems. The calculated mean probability of failure of the SEHR system on demand with all equipment available was $1,8.10^{-3}$/demand. This mean failure probability increases to $3,2.10^{-3}$/demand if maintenance is considered to be undertaken on the system during plant operation. Maintenance was considered for the major items of equipment i.e., diesel generators, pumps, motor operated valves. The time dependent failure characteristics of the SEHR system with and without repair are given in Figure 4. The rapid increase in failure probability for the case with no repair is due to the the failure of the diesel generators, which are the sole source of electrical supplies for this system, and which have a relatively high failure rate.

Reliability of the DHR Function for Leibstadt

The decay heat removal function for Leibstadt is provided by the standard DHR systems and the SEHR system. Decay heat removal by the power conversion system has been pessimistically omitted in this analysis due to the imposition of licensing criterion as discussed earlier. The steam condensing mode of operation of the RHR system was not considered in this analysis because the scope of work undertaken to date has dealt only with LOCA scenarios. This mode of RHR operation is unavailable for LOCA scenarios in the short term due to valving logic and in the long term due

to low steam pressures.

The systems considered for DHR have some common equipment as indicated in the SEHR system description given earlier. Failure of these common components does not result in failure of the DHR function since there are other routes available to discharge the flow to the Suppression Pool. Because there are no common failure modes the systems can be treated as independent. This leads to an overall DHR mean failure probability on demand of $3,4.10^{-6}$, which is the product of the individual system failure probabilities. The inclusion of simultaneous maintenance acts in this product is acceptable and in accordance with the Station Technical Specification.

In the long term the probability of the DHR function failing and not being restored in sufficient time to prevent containment failure and hence core melt is dependent on many factors which affect the chances of repair. Some of the factors are location of failed components, availability of spares and maintenance personnel, time of 'system failure' after the initiating event, etc.. The worst case of failure probability is again determined if no repair is assumed and this results in a probability of $3,2.10^{-5}$ at a time of 24 hours after the initiating event. If it is assumed that components outside the fluid boundary can be repaired then the failure probability at 24 hours after the event is $1,8.10^{-6}$.

DISCUSSION

Analysis to date shows clearly that the SEHR system makes a significant contribution to the reliability of the decay heat removal function of the Leibstadt plant for LOCA scenarios. The large impact on reliability has resulted from the licensing criteria which required the SEHR system to be independent from the other emergency core cooling systems. Independence was achieved by the use of dedicated power supplies and a diverse heat sink.

The influence of the SEHR system on transient initiated scenarios has not yet been analysed. Post-transient decay heat removal could make use of the steam condensing mode of the RHR operation as well as the power conversion system, hence the reliability of the standard DHR systems would be better than the figures indicated for post-LOCA situations. The impact of the SEHR system on overall DHR reliability would therefore be lower.

Failure of the decay heat removal function is the major contributor in most of the dominant accident sequences identified in the risk studies of not only Peach Bottom *[1]* but also Grand Gulf 1 *[4]* boiling water reactors. Such sequences account for 44% and 90% of core melt frequency respectively. All such dominant sequences involving failure of decay heat removal are transient initiated except for one LOCA initiated sequence identified in the Grand Gulf study. A short discussion of these sequences when considered in the context of the Leibstadt systems configuration follows.

For the single dominant LOCA initiated sequence identified for Grand Gulf, the SI sequence (small LOCA followed by failure of decay heat removal by the two RHR systems), the SEHR system would have a very benefical effect. For Grand Gulf this sequence is assigned a probability of $4,6.10^{-6}$/year which represents about 12% of core melt frequency. It is estimated that inclusion of the SEHR system would decrease this by at least 2 orders of magnitude since it provides another independent path for the removal of decay heat.

For the transient scenarios it is more difficult to provide a direct comparison of the expected results for Leibstadt because not all the possible decay heat removal paths have been analysed. The dominant transient initiated sequence identified for Peach Bottom and Grand Gulf was in both cases the TW sequence (transient followed by

failure to remove decay heat). Both of these studies included the power conversion system and, for Grand Gulf, other modes of RHR operation, in the analysis of the decay heat removal function. Assuming that similar sequences would apply for Leibstadt, simple addition of the SEHR system would reduce their probability by at least two orders of magnitude. Without proper analyses of system interaction and event dependency effects, such a value must be considered as an upper bound estimate of what reduction might be achievable. Nevertheless, in view of the high degree of independence of the SEHR system , it is to be expected that actual gains would be substantial.

It is worth considering the overall effect on core melt frequency which would result from such an improvement in decay heat removal system reliability. This may be estimated using a simplistic scaling factor on the probabilities assigned to dominant sequences involving total failure of decay heat removal. Applying the Grand Gulf figures to Leibstadt, an improvement in the overall DHR systems reliability by a factor of 10 or 100 would then reduce predicted core melt frequency by about 77% or 85% respectively. Clearly, other sequences (e.g. ATWS) become dominant in this situation, but these figures show that even a 10 - fold improvement in DHR systems reliability has a substantial impact on core melt frequency. It is emphasised that rigorous analysis would be required to justify such estimates.

REFERENCES

1. Reactor Safety Study, an Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH-1400 (NUREG-74/014), US NRC, October 1975.

2. D.L. Berry and P.R. Bennett, Study of Alternative Decay Heat Removal Concepts for LWR's - Current Systems and Proposed Options, SAND80-0929 (NUREG/CR-1556).

3. Unresolved Safety Issues, NUREG-0606, US NRC.

4. Reactor Safety Study, Methodology Applications Program : Grand Gulf 1 BWR Power Plant, NUREG/CR-1659, Vol. 4, US NRC, October 1981.

5. R.R. Willie, Computer Aided Fault Tree Analysis Program, FTAP., Operations Research Center, University of California, Berkeley; ORC 78-14, August 1978.

6. W.E. Vesely and R.E. Narum, PREP and KITT; Computer Codes for the Automatic Evaluation of a Fault Tree, Idaho Nuclear Report IN-1349, August 1980.

7. MERLIN Users Guide, Electrowatt Engineering Services (London) Ltd.

8. W.E. Hubble and C. Miller, Data Summaries of Licensee Event Reports of Valves at U.S. Commercial Nuclear Power Plants, EGG-EA-5125 (NUREG/CR-1363), June 1980.

9. W. Sullivan and J. Poloski, Data Summaries of Licensee Event Reports of Pumps at U.S. Commercial Nuclear Power Plants, EGG-EA-5044, (NUREG/CR-1205), January 1980.

10. IEEE Nuclear Reliability Data Manual, IEEE Standard - 500, 1977.

11. Reliability Prediction of Electronic Equipment, MIL-HDBK-217C, April 1979.

12. A. Swain and H. Guttmann, Handbook of Human Reliability Analysis with emphasis on Nuclear Power Plant Applications, NUREG/CR-1278, US NRC, October 1979.

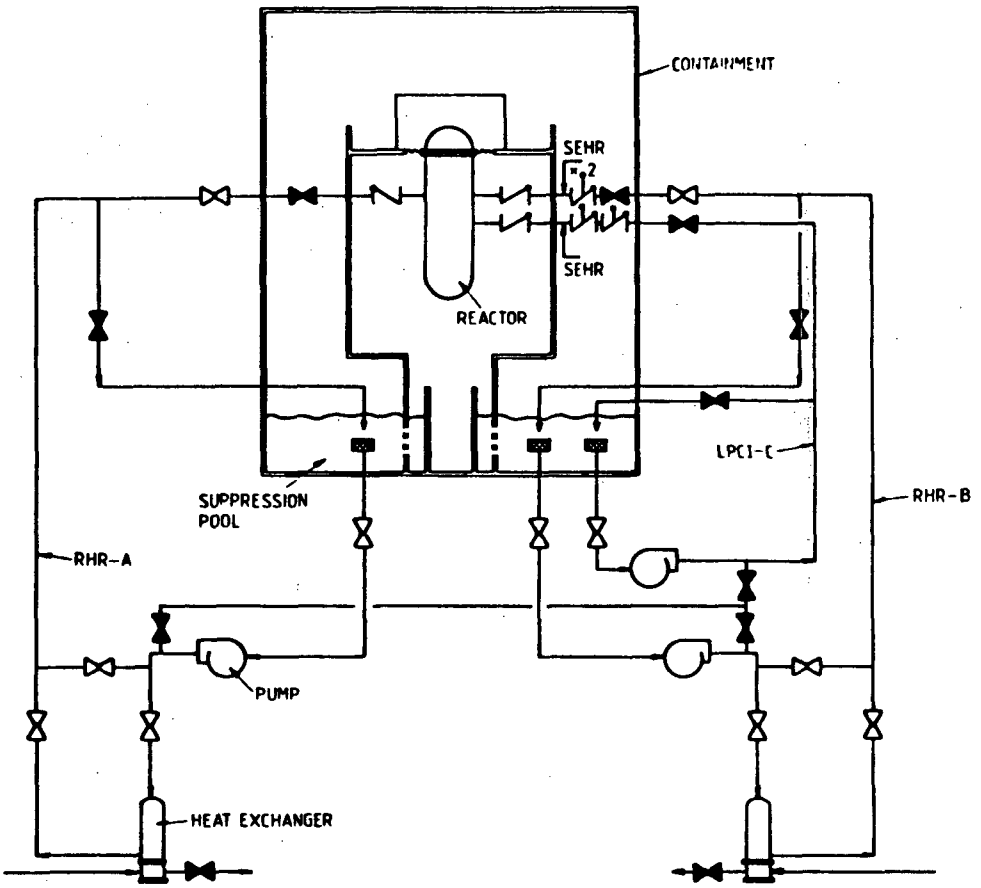


FIGURE 1. SCHEMATIC OF STANDARD RHR SYSTEM

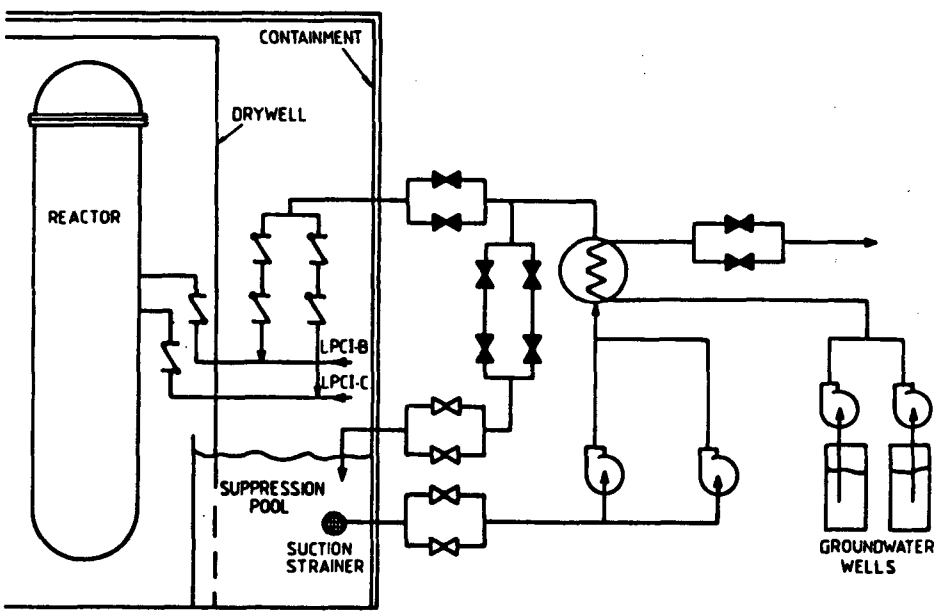


FIGURE 2 SCHEMATIC OF SEHR SYSTEM

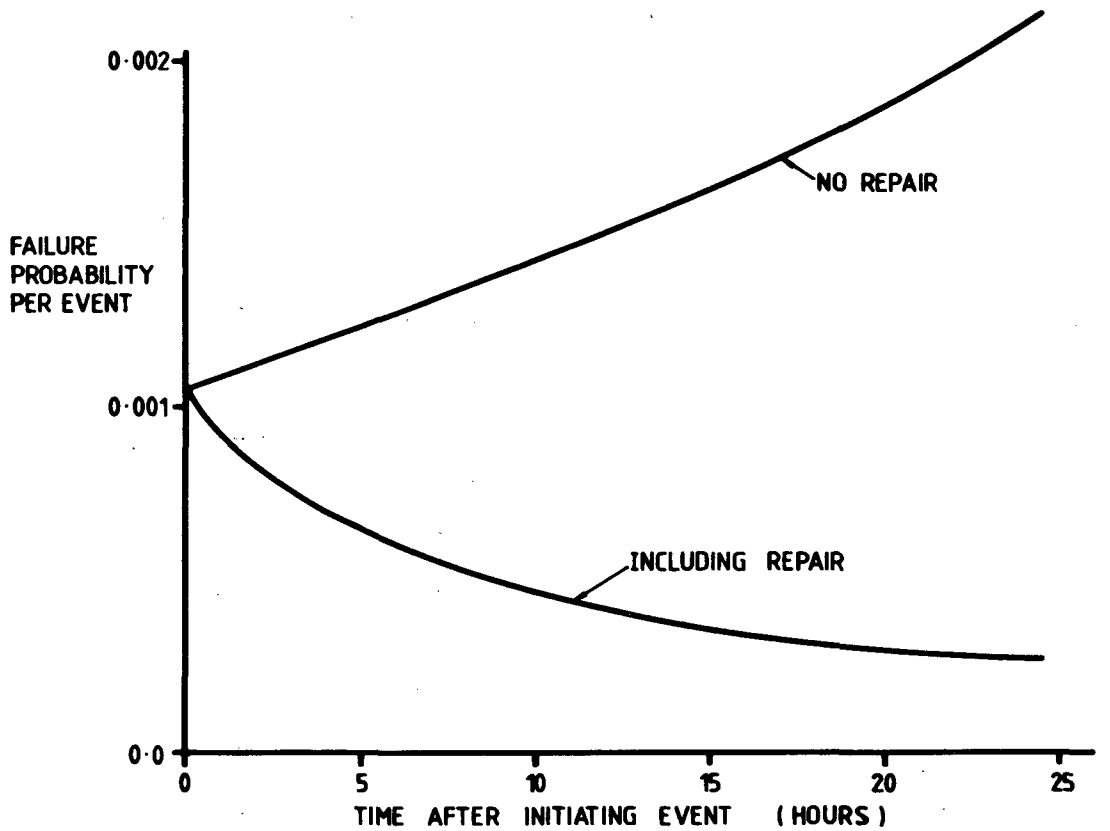


FIGURE 3. FAILURE CHARACTERISTICS OF STANDARD DHR SYSTEMS

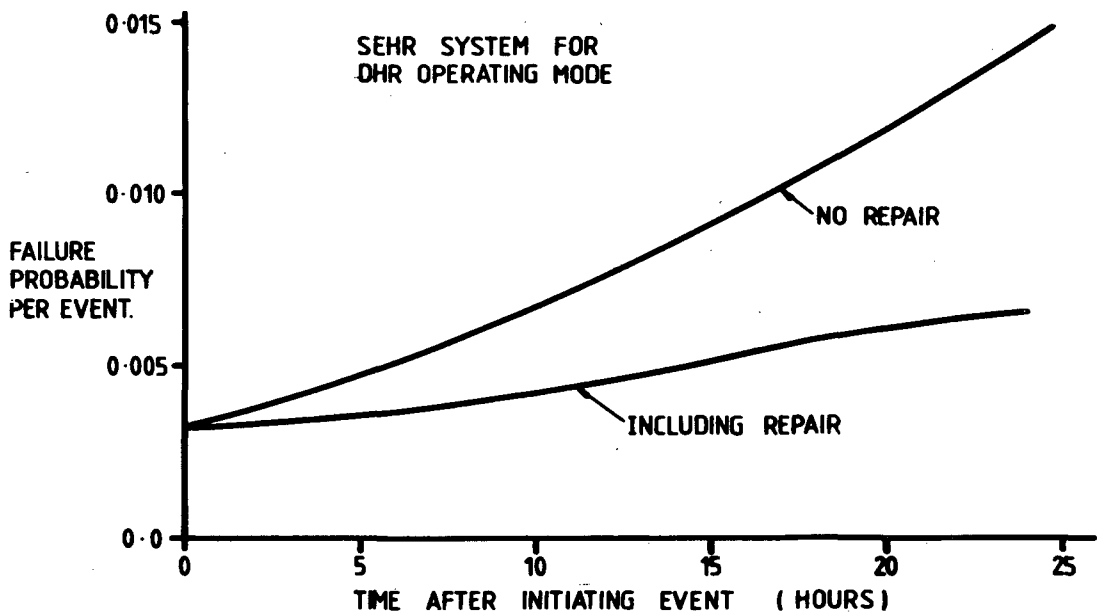


FIGURE 4. FAILURE CHARACTERISTICS OF SEHR SYSTEM.

ESTIMATING FAILURE-TO-CLOSE PROBABILITIES FOR PRESSURIZER VALVES

W. W. Weaver
Babcock & Wilcox, Nuclear Power Generation Division
Lynchburg, Virginia 24505, U.S.A.

ABSTRACT

A necessary ingredient for quantifying small break loss-of-coolant accident probabilities is estimating the probabilities for pressurizer valve failure in the open position. Such factors as application, coolant state, and valve manufacturer affect these failure probabilities. Operational data on all three pressurizer valve types (electric motor-operated block valve, pilot-operated relief valve, pressurizer safety valve) reveal important differences from previously reported generic valve data. Rare event methods are employed in failure probability estimation when operational data are lacking. Factors that influence the selection of appropriate rare event methods are presented.

INTRODUCTION

Because of the prominent role played by the pressurizer pilot-operated relief valve in the Three Mile Island Unit 2 (TMI-2) accident, the Nuclear Regulatory Commission (NRC) has renewed its interest in quantifying the probabilities of small break loss-of-coolant accidents (SBLOCAs) through pressurizer valves. Unfortunately, most of the studies conducted to date have relied on either WASH-1400 data or the meager but readily available operational experience for pressurizer valve failure data. This paper estimates the failure probabilities for a variety of pressurizer valves to reclose per demand. The valves considered include the electric motor-operated block valve (EMOV), the pilot-operated relief valve (PORV), and the pressurizer safety valve (PSV). Unlike the PORV and EMOV, the PSV does not receive a command signal to close, but rather closes when the differential pressure between the inlet and outlet of the valve drops to a preset value. PSV failure to reclose is defined here in terms of reseat pressure. If the reseat pressure is below 70% of opening pressure, it is considered a failure. Closures below the design setpoint but above 70% blowdown are not considered failures for the purpose of this report. As is the case with the other valves, weeping and leaks are not considered failures. The raw data used are discussed, along with the logic and techniques employed to assess the failure probabilities.

The estimation of these valve failure probabilities was a major input to the analysis conducted to support the redesign of the flow path associated with the PORV for Babcock & Wilcox (B&W) 205-fuel assembly (FA) reactors. Another important input was transient frequency estimation. Space limitations preclude discussion of either the frequency estimation study or the specifics of the design.

The mechanics used in constructing the valve failure probabilities are described in depth. This discussion may be useful to analysts who are attempting to quantify probabilities based on limited data. All probability values expressed in this paper are the mean of the given distribution unless otherwise noted.

PORV FLOW PATH DESIGN

B&W's operating philosophy has been to use the PORV to control expected operational pressure changes and especially to permit reactor runback without reactor trip for larger disturbances, such as turbine trip. For example, prior to the TMI-2 accident the setpoint for PORV actuation was 2255 psi, while the high reactor coolant system (RCS) pressure setpoint was 2355 psi. This not only allowed the system to ride out upsets while remaining at power, but also enhanced runback. For example, the plant is capable of performing a runback to 60% power on loss of a feed pump or to 15% power on turbine trip or loss of load without causing reactor trip. The B&W 205-FA units employ the same philosophy as the TMI-vintage plants with the PORV set at 2295 psi and the RCS high-pressure trip at 2355.

An open PORV flow path is said to occur when the PORV is open and the RCS pressure drops low enough to initiate emergency safety features actuation. This requires that both the block valve and the PORV be open. The probability of having an open PORV flow path is the product of the demand frequency and the probability of failure to reclose. Demand to open can result from either a transient condition or a spurious opening command. Due to the design and reliability of the control circuits, the latter contribution is calculated to be relatively minor. The block valve design also incorporates an automatic closure signal, which is generated when low RCS pressure exists coincidental with an open PORV indication.

With 1E sources of power to the EMOV and PORV, this contribution to failure is also minor, which leaves valve hardware itself as the major contributor to the undesired event of an open PORV flow path. This situation is similar to the safety valve flow path, in which valve hardware is the only contribution to failure. If further improvements are to be made, they must come from valve reliability enhancements.

The frequency of pressure transients that involve the PSVs is partly a function of the PORV status. If the PORV is failed closed (or if the EMOV is closed or closes too quickly), some pressure excursions that the PORV would normally limit could reach the PSV setpoint, thereby increasing the PSV demand frequency and therefore the probability of a stuck-open PSV. This precludes a design whose only objective is to minimize PORV demands — an example of which is to leave the block valve closed at all times. In responding to questions from the NRC on NUREG 0737 (at II.K.3.2), GPU Nuclear points out that there is an increase of about 25% in PSV demand when operating with a blocked PORV.[1] The desired criterion for PORV design is to minimize SBLOCA probabilities from the pressurizer on the whole.

ESTIMATION OF VALVE FAILURE PROBABILITIES

Three distinct categories of valves were considered in this study for failure to close: (1) EMOV, 2 to 4 inches in diameter; (2) PORV; and (3) PSV. For each category a Bayesian approach is employed to estimate failure-to-close probabilities incorporating previously unreported data sources. The resultant values differ from some well known sources of data, such as WASH-1400[2] and NPRDS[3].

Electric Motor-Operated Block Valve

The EMOV data are based on NUREG/CR-1363[4] and RADCAS[5]. A value of 8.1×10^{-4} for failure to close per demand was calculated from the tables in reference 4. This value was used to construct a lognormal distribution [mean = 8.1×10^{-4}, range factor (RF) = 3], which was then used as the prior in the Bayesian analysis. This resulted in a lognormal with a median value of 6.5×10^{-4} with 5th and 95th percentiles at 2.16×10^{-4} and 1.94×10^{-3}. From the RADCAS data[5], 34 failures in 1433 demands were used to update the prior distribution. The resultant posterior distribution mean is 1.85×10^{-2} with the 5th and 95th percentiles at 1.33×10^{-2} and 2.46×10^{-2}. While the fact that the posterior distribution differs substantially from both the prior and the

evidence is not cause within itself to be concerned, it was felt that a RF of 3 for these valve data was inappropriate because of the questionable quality of the LER data in addition to the potential plant-to-plant variation. Another run was made with a larger assumed uncertainty (RF = 10). This resulted in a posterior mean of 2.22×10^{-2} with 5th and 95th percentile values of 1.63×10^{-2} and 2.98×10^{-2}. The change in the relative importance of the evidence on the posterior increases as the uncertainty in the prior is made larger. Table I summarizes the values on the EMOV.

Table I. Failure to Reclose — EMOV

Prior			Posterior		
Mean	Range factor	Evidence	5th	Mean	95th
8.1×10^{-4}	3	34/1433	1.33×10^{-2}	1.85×10^{-2}	2.46×10^{-2}
8.1×10^{-4}	10	34/1433	1.63×10^{-2}	2.22×10^{-2}	2.98×10^{-2}

Pilot-Operated Relief Valve

All B&W plants but one have the same type of PORV. In addition, the same valve is used on six Combustion Engineering (C-E) operating units. Those operating units have reported zero failures in 38 demands.[6] The EPRI valve test data also include zero failures in 27 demands on this valve.[7] The experience of the B&W operating units reveals four mechanical failures based on 127 demands that were recorded (i.e., reactor trips; with the pre-TMI setpoint, at least one PORV demand must have occurred prior to reactor trip). There were other, unrecorded, demands on the PORV which included transients that resulted in multiple PORV openings and those plant upset conditions in which the PORV functioned as designed (i.e., the plant rode out the disturbance without reactor trip). Including these demands produces a distribution (the number of demands above is not known with certainty) with a mean value of approximately 9.8×10^{-3} for this type of PORV. This pooled method (total number of failures/total number of demands) of failure probability determination is preferable to an estimation based on average failure probabilities. For example, in this case the value obtained from the mean of the averages (7.8×10^{-3}/demand) underestimates the failure probability. As can be seen from equation 1, the results may be biased when any k_i equals zero:

$$\frac{1}{N} \sum_{i=1}^{N} \frac{k_i}{n_i} \qquad \text{where } k = \text{number of failures, and } n = \text{number of demands.} \qquad (1)$$

The value of k is zero in two of the three terms that appear in equation 1. The direction of the bias depends on the number of demands; that is, equation 1 treats zero failures in one demand and zero failures in a thousand demands as equivalent.

The 205-FA plant owners are considering using a different type of PORV than the one used on the 177-FA plants. This new valve has accumulated approximately 25,000 cycles without failure in a pressurizer spray valve application, but in a different environment than the PORV. This application is actually more stressful to the valve internals than the PORV application; however, the intermittent operation of a PORV would appear to induce a higher chance of failure than would the regular demand of the spray valve application (e.g., typically eight per day). One could employ either a chi-square estimate or a binomial method[8] using zero failures in 25,000 demands to arrive at a point estimate for a prediction of the failure probability for this valve in the PORV application of 2.4×10^{-4} (at 50% confidence). Both methods produce the same result, as would be expected since the beta (binomial method) is related to the chi-square. While this value is a good predictor for the spray valve application, it should not within itself be used for the PORV application because of the differences in frequency of demand.

A Bayesian approach was taken to arrive at the failure distribution of the new PORV. It has been argued that a uniform distribution is appropriate for the prior distribution if not much information is available.[9] However, this is not accurate in the event the evidence is zero failures since the placement (in terms of probability) of the prior will affect the posterior distribution; the smaller the probability values of the prior, the more the posterior — which never peaks — is shifted toward zero. In this study, the PORV experience in 177-FA plants was used as the prior and updated with zero failures in 25,000 cycles, producing a distribution with a mean of approximately 4×10^{-4} per demand. Another estimate of the mean was calculated based on the procedure for the ratio of two Poisson means, as described in reference 10. This estimate is 3×10^{-4} per demand, which is essentially the same as the Bayesian result. The Bayesian procedure employed in this study utilized the gamma (two-parameter) distribution, which is not only very flexible but also computationally easy to use. A gamma prior with Poisson likelihood produces a gamma posterior but with shifted parameters. The more exact method for calculation of failures on demand is the beta prior, binomial likelihood, and beta posterior; however, the gamma is a good approximation if either the number of failures is much smaller than the number of demands (which is the usual case in nuclear power plant components) or there are zero failures.

Pressurizer Safety Valve

The probability of failure for a safety valve to reclose depends on whether the valve is passing steam, water, or a mixture. This is in contrast to the PORVs discussed above, whose failure probability is not a function of the type of fluid passed. Very little data have been obtained to date on PSV failures. There have been only two events when PSVs have operated in the B&W operating plants' experience — one at Rancho Seco on March 20, 1978 (steam relief) and the other at Crystal River 3 on February 26, 1980 (two-phase and water relief). In both cases the safety valves reseated. There are considerable data on the main steam safety valves (MSSVs) for steam relief. Failure probabilities for PSV steam relief can be deduced by examining the operating history of MSSVs because the design principles on which they operate are the same; i.e., they both work against the closing force of a spring, and they both depend on the addition of a sudden opening force when they reach the setpoint. Some differences include the following:

1. The fluid passing through a PSV should be of a higher quality (fewer suspended solids) than the fluid passing through a MSSV.

2. The PSV is all stainless steel, whereas the MSSV, which is mainly carbon steel and subject to rusting, might introduce additional foreign material.

3. The PSV has a variable backpressure and requires a more sophisticated design that in turn has more chance of failures than the MSSV, which has essentially constant stack pressures.

4. The PSV is an ASME Class I component versus ASME Class II for the MSSV.

The third point indicates that the MSSV should have a lower failure probability, while the other points indicate that the PSV should possess the lower failure probability. The overall failure probabilities should be comparable. There have been approximately 2850 main steam safety demands in the cumulative operating experience of the B&W plants. There have been no failures to reclose as defined in the introduction. There have been instances (most notably TMI-2, April 23, 1978) in which safety valves did not reseat at proper blowdown, but in none of these occurrences did blowdown exceed 70%. This results in a mean value of 2.4×10^{-4} per demand. This distribution was constructed based on 50% confidence with zero failures and a range of values for the number of demands. While this value is an estimate of failure to close given steam relief, it is far too optimistic to use it for water relief also. The failure rate of the PSVs to reclose given water relief was estimated to be 10 to 1000 (5 to 95% cumulative probability value) times larger than the value obtained for steam relief. This was then

used as a gamma prior for the Crystal River event with zero failures in one demand as the evidence. This produces a distribution with a mean value of 6.9×10^{-2} per demand, where the prior mean was 7.5×10^{-2} per demand. Incorporation of the EPRI valve test program data for both the 500,000 lb/h (zero failures in five demands) and 300,000 lb/h (zero failures in four demands) valves produces a distribution with a mean value of 4.0×10^{-2} per demand for a PSV failure to close on water relief. Table II summarizes the failure data in this section.

Table II. Failure to Reclose on Water Relief — PSV

		Posterior		
Prior mean	Evidence	5th	Mean	95th
7.53×10^{-2}	0/1	2.20×10^{-3}	6.91×10^{-2}	2.20×10^{-1}
7.53×10^{-2}	0/10	1.27×10^{-3}	3.97×10^{-2}	1.27×10^{-1}

The procedure used to estimate this failure probability is analogous to the two-step Bayesian update procedure, in which the first evidence (Crystal River data) is used to update the prior and the resultant posterior then becomes the prior for the second evidence (EPRI data) update. For computational ease, all evidence was lumped together so only one update was required. This approach produces the same value as if the two-step procedure had been implemented.

All the probability values associated with open flow paths assumed a constant hazard function for the valves. This is accurate or even conservative for steam relief. In the case of infrequent occurrences with multiple demands, if the valve works on the first lift, there is a higher probability that it will reclose on subsequent lifts, although not necessarily at the same pressure. Alternatively, if there is a failure, it will most likely occur on the first lift. This observation would not be true if there were a strong correlation between failure probability and the relief process, which is suspected for water or alternate water/steam relief on the PSVs. For this situation a sharply increasing hazard function may apply. Since operational data for water and alternate water/steam relief on the PSV will always be scarce, obtaining these data should become an objective of the next major valve test program. The current EPRI valve test program was more a functional test than a generator of statistical data.

CONCLUSIONS

Although operational data on pressurizer valves have not been available in the comprehensive form hoped for in statistical analyses, relevant data exist that should be employed in constructing valve failure probabilities. The results of this study suggest that the PORV flow path valve failure probabilities (number of transients times valve failure-to-close probabilities) are low enough that the overall SBLOCA probability is not impacted significantly by an open PORV. Similarly, steam relief on the PSVs is not a major concern; however, more information is needed on water relief through the PSVs or any other safety valves. While it is believed that the current frequency of water demand on the PSVs is sufficiently small, efforts toward better operator recognition and training should continue to be directed toward minimizing this occurrence.

REFERENCES

[1] "Response to SER Questions on TMI-1 PORV," Doc. No. 32-1127869, Babcock & Wilcox, Lynchburg, Virginia, October 1981.

[2] "Reactor Safety Study," Report WASH-1400 (NUREG 75/014), U.S. Nuclear Regulatory Commission, Washington, D. C. (1975).

[3] "Nuclear Plant Reliability Data System — 1980 Annual Report," Report NUREG/CR-2232, Southwest Research Institute, San Antonio, Texas, September 1981.

[4] "LER Summary Report on Valves," NUREG/CR-1363, Vol. 1, Report EGG-EA-5125, June 1980.

[5] "Reliability/Availability Data Collection and Analysis System," Report NPGD-TM-378, Babcock & Wilcox, Lynchburg, Virginia (1981).

[6] "PORV Failure Reduction Methods," Combustion Engineering, Nuclear Power Systems Division, Windsor, Connecticut, December 1980.

[7] T. AUBLE and J. HOSLER, "EPRI PWR Safety and Relief Valve Test Program — Safety and Relief Valve Test Report," Research Project V102, Electric Power Research Institute, Palo Alto, California, April 1982.

[8] J. HUEBEL and G. MYERS, "Tables of Confidence Bounds for Failure Probabilities," Report UCRL-51990, Lawrence Livermore Laboratories, Livermore, California, January 1976.

[9] KAPLAN, GARRICK, and BIENIARZ, "On the Use of Bayes' Theorem in Assessing the Frequency of Anticipated Transients," *Nuclear Engineering & Design*, 65, 23 (1981).

[10] NELSON, "Confidence Intervals for the Ratio of Two Poisson Means and Poisson Predictor Intervals," *IEEE Transactions on Reliability, Vol. R-19 2*, May 1970.

RELIABILITY OF THE EMERGENCY AC POWER SYSTEM AT NUCLEAR POWER PLANTS

R. E. Battle

Oak Ridge National Laboratory
Oak Ridge, Tennessee 37830, USA

D. J. Campbell

JBF Associates, Inc.
Knoxville, Tennessee 37919, USA

P. W. Baranowsky

Nuclear Regulatory Commission
Washington, D.C. 20555, USA

ABSTRACT

The reliability of the emergency ac power systems typical of most nuclear power plants was estimated, and the cost and increase in reliability for several improvements were estimated. Fault trees were constructed based on a detailed design review of the emergency ac power systems of 18 nuclear plants. The failure probabilities used in the fault trees were calculated from extensive historical data collected from Licensee Event Reports (LERs) and from operating experience information obtained from nuclear plant licensees. No one or two improvements can be made at all plants to significantly increase the industry-average emergency ac power system reliability; rather the most beneficial improvements are varied and plant specific. Improvements in reliability and the associated costs are estimated using plant specific designs and failure probabilities.

INTRODUCTION

The NRC has identified station blackout, the loss of all ac power at a nuclear plant, as a generic safety issue because of the frequency of ac power system failures and because of the reactor core damage and radioactivity release that could result. The purpose of this study is to estimate the reliabilities of representative onsite ac power systems and to estimate the costs of reliability improvements for these systems.

The issue of station blackout involves the likelihood and duration of the loss of offsite power, the reliability of onsite ac power systems, and the potential severe accident sequences after a loss of all ac power. This paper summarizes the results of the onsite ac power system reliability analysis.

SCOPE

The scope of the onsite ac power system analysis was to (1) select a number of plants that are representative of ac power system designs used in the nuclear industry, (2) gather detailed historical data, and (3) perform a reliability analysis.

Eighteen representative plants were selected for detailed design review. These 18 plants were selected to be representative not only of diesel generator configuration, but also diesel age, vendor, and size, and other plant specific design features.

The diesel historical data were collected for 1976 through 1980 from licensee event reports (LERs) and responses to questionnaires sent to nuclear plant licensees. Each event was categorized by failure type. Detailed historical data were used to calculate probabilities of failure-to-start, failure-to-run, common-cause failure (CCF), scheduled maintenance unavailability, and system repair. A review of diesel generator subsystem failures was performed to determine failure modes and the percentage of failures caused by each subsystem.

The onsite ac power systems of the 18 plants were modeled by fault trees. A simplified schematic for a reactor with two diesels is shown in Fig. 1, and a fault tree of the same system is shown in Fig. 2. The onsite system undependability, the probability that it will fail to start or continue to run for the duration of an offsite power outage, was calculated for ac power outages up to 30 h after a loss of onsite power. Results of a sensitivity study were used to identify potentially important contributors to ac power unreliability, and costs of improvements were estimated.

TECHNICAL APPROACH

Design Review

The configurations of diesel generators at all of the operating plants were reviewed and tabulated. From this tabulation, 18 plant specific success-logic configurations representative of typical onsite power system designs were selected. There were five generic success-logic configurations in these 18 plants as follows: 1-of-2, 1-of-3, 2-of-3, 2-of-4, and 2-of-5. The success-logic represents the number of diesel generators required for successful cooling of the reactor out of the total number of diesels at the plant. These five configurations are representative of most plants in the nuclear industry.

During the design review, the onsite ac power subsystems were examined for common-cause failure (CCF) potential of both a hardware and a procedural nature. Several possible CCF candidates were identified for later evaluation during an operating experience review.

Interactions between the onsite ac power system and other plant systems were also reviewed. The only significant interactions identified were with the plant service-water system, dc power system, and the offsite power system.

Many water-cooled engines are dependent on the plant service-water system, but air-cooled engines or engines with a dedicated water-cooling system are not dependent on plant service-water. If the cooling subsystem fails, the diesel can run only a few minutes at full load before it overheats. Air-cooled diesels can continue to supply ac power even though the service-water system is unavailable.

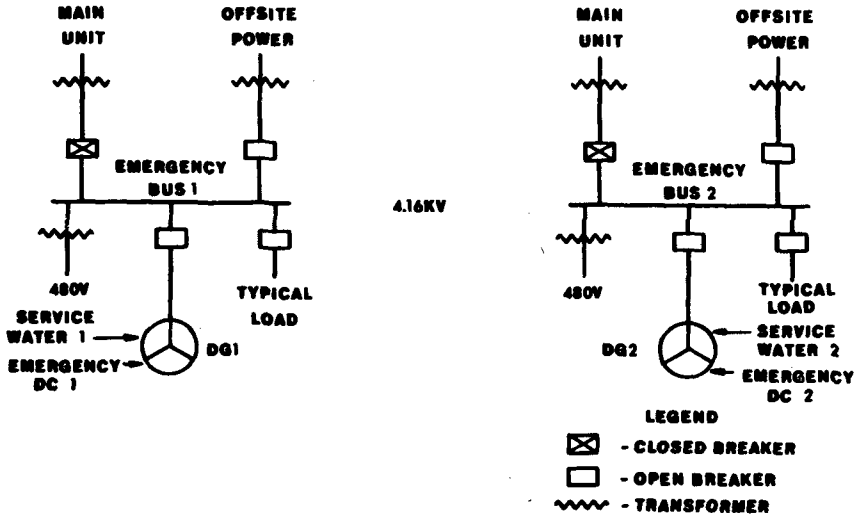


Fig. 1. Simplified 1-of-2 Onsite AC Power Distribution System.

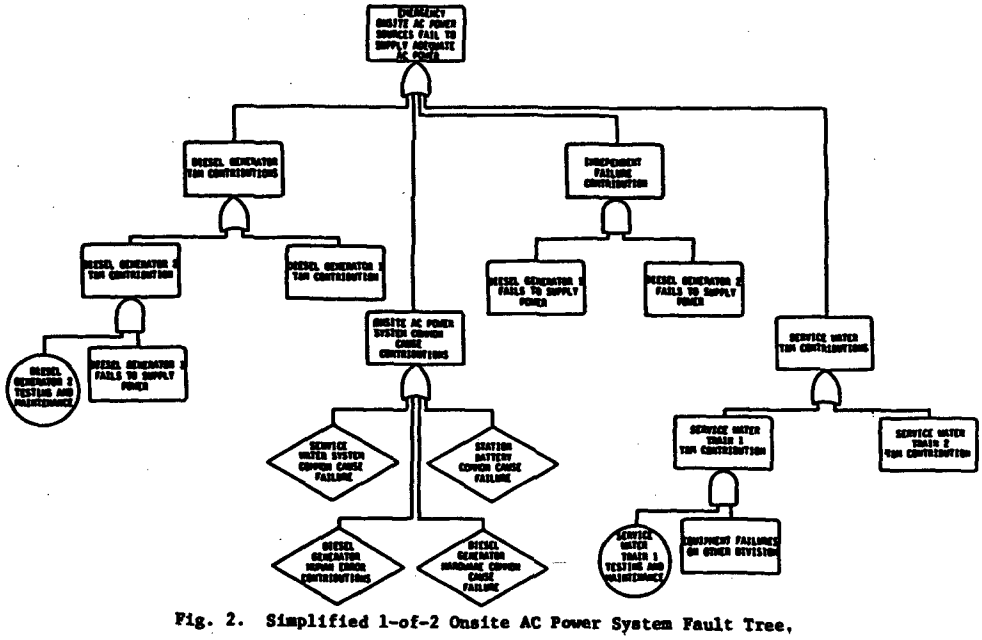


Fig. 2. Simplified 1-of-2 Onsite AC Power System Fault Tree.

For most nuclear plants, diesel generator control power is supplied by plant IE (safety system) batteries; a few diesel generators have batteries dedicated for control. However, diesels with dedicated batteries are not independent of a plant IE battery because control power to the generator output breaker is from plant batteries. Failure of a plant IE dc power source would cause failure of the associated generator output breaker to function regardless of the presence of a dedicated diesel battery.

At some plants there is a potential interaction between the onsite and offsite power systems through the dc system. Such an interaction [1] occurred at Millstone 2 when loss of the "A" battery resulted in the loss of switchyard breaker control power and loss of a diesel generator. Loss of the "A" battery resulted in loss of dc control power to one diesel generator and to breakers in the onsite and offsite power systems.

Operating Experience Review

The operating experience review contained information obtained from LERs, utility responses to TMI action plan items (NUREG-0737), and a substantial amount of operating reliability data from nuclear power plants. These operating reliability data covered 45 nuclear units having 194 reactor-years and 450 diesel-generator-years of operation in which there were 14,204 diesel starts.

There were 1522 events categorized for the years 1976-1980, of which 813 were LERs and the remainder were from other sources, mostly NUREG-0737 questionnaire responses. There were 418 primary and secondary failures, 85 autostart failures, and 1019 nonfailures. Primary failure is an intrinsic or end-of-life failure, and secondary failure is an extrinsic or externally caused failure. The definitions of failure, autostart failure, and nonfailure follow:

> *Failure: A test or emergency demand during which the diesel generator did not or would not, if offsite ac power were lost, supply sufficient ac power to the emergency bus.*
>
> *Autostart failure: An event that would be a failure except that power is restored to the emergency bus within a few minutes by operator action.*
>
> *Nonfailure: All events that were not primary, secondary, or autostart failures.*

The average probability of failure to start was calculated as a standby failure rate. An industry-average value of the probability of failure to start is 0.025. This was used in all of the generic studies, but plant specific values were used to estimate the plant specific failure probabilities.

The average probability of diesel failure on demand was also calculated from the nuclear plant data for tests, losses of offsite power, and all automatic starts not for testing. These data and results are presented in Table I. The average probability of failure on demand, 0.019, is less than the average standby failure probability, 0.025. For a diesel that has a lot of starts unevenly spaced throughout a year, which is the case for many diesels, the standby failure rate model is slightly higher than the average failure on demand. Therefore the standby failure probability was used in the reliability calculations.

There is little data for failure to run for long periods of time because most diesel generator tests are for 1 h, but there have been periodic or special tests that last longer than 1 h. The failure rate for failure to run was calculated from

TABLE I

Comparison of test and emergency start demand data

Category	Demands	No. of primary and secondary failures on demand	Probability of primary or secondary failure on demand	No. of autostart failures on demand	Probability of autostart failure on on demand	No. of DGs unavailable for T&M	T&M unavailability
Test	13,665	253	0.019	55	0.004	—	0.006
Loss of offsite power	78	2	0.026	2	0.026	3	0.038
All actual demands	539	14	0.026	5	0.009	3	0.006

tests that were scheduled to last longer than 6 h. The number of failures that occurred during these tests was divided by the cumulative run-time. There were 314 tests scheduled, 9 failures, and 3754 h of run-time. The failure rate estimate was 2.4×10^{-3}/h. This value was used in all of the reliability calculations.

The estimate of a mean-time-to-repair is the average of the repair times for primary and secondary failures. Plant specific values are used for the 18 plants studied in detail. Of the 418 primary and secondary failures, repair times were reported for 312. The mean is 36 h and the median is 8 h.

Unavailability of diesel generators because of testing and maintenance (T&M) during reactor operation contributes to onsite system unreliability. The average unavailability of a diesel is 6×10^{-3}. When this average is used, it contributes insignificantly to the onsite system unreliability. However, extensive T&M, including overhauls, performed during reactor operation at some plants contributes significantly to unreliability. There were three events in which a diesel was unavailable during a loss of offsite power, as shown in Table I, but all three incidents occurred while the reactors were shut down.

In addition to categorizing independent failures, the data were reviewed for actual and potential CCFs attributed to hardware failure or human error. There were 59 human error events that caused or had the potential to cause simultaneous unavailability of two or more diesel generators. Maintenance errors caused all but one of these events. Therefore diesel generator maintenance procedures of several plants were reviewed to determine how they might contribute to human error CCF. The procedures were graded and separated into three categories based on guidelines such as the details in checklists, test after maintenance, checks for return to normal after tests, and the clarity of the procedures. Procedures in category I were the best and those in III the worst. Procedures from 35 plants were evaluated. Nine were in category I, 16 in category II, and 10 were in category III.

The BFR computer code [2] was used to calculate human error failure rates. The group of plants in categories I and II had lower human error failure rates than those in category III. This correlation indicates that procedure quality affects the human error CCF rate. In addition to a CCF rate attributed to procedures, there is a generic human error CCF rate to which all plants are subject. The human error CCF failure rate used in this reliability study is the sum of the generic rate and the specific rate assigned for the quality of the procedures. The range of human error CCF is in Table II.

TABLE II

Probability or Frequency of Basic Events

Basic Event Description	Range of Plant Specific Initial Unavailability or Frequency		
	Low	Average	High
	Diesel Generator		
Independent failure	8.2×10^{-3}	2.5×10^{-2}	1×10^{-1}
CCF attributed to hardware	3.6×10^{-5}	4.0×10^{-4}	1.8×10^{-3}
CCF attributed to human error	7.2×10^{-5}	7.8×10^{-4}	3.7×10^{-3}
T&M	1×10^{-5}	6×10^{-3}	4.5×10^{-2}
	DC Power System		
Independent failure	1×10^{-5}	1×10^{-4}	1×10^{-3}
CCF	1×10^{-6}	1×10^{-5}	1×10^{-4}
	Service Water		
Independent failure	2×10^{-4}	2×10^{-3}	2×10^{-2}
CCF	8×10^{-6}	8×10^{-5}	8×10^{-4}
T&M	1×10^{-4}	2×10^{-3}	4×10^{-2}
	Offsite Power		
Plant centered	9.2×10^{-2}/y		2.5×10^{-1}/y
Area wide storms	1.3×10^{-2}/y		2.7×10^{-1}/y
Area wide blackouts	1.3×10^{-2}/y		2.4×10^{-1}/y

There were 12 events that caused or had significant potential to cause a CCF attributed to hardware failure. These events were classified into six failure modes of which two are inherent to all plants and four depend on plant design. The two generic failure modes to which all plants are susceptible are fuel blockage and extreme room temperature. The four plant specific failure modes are the following: (1) water in the fuel system, (2) lack of effective corrosion inhibitor in the engine jacket-water, (3) service-water system blockage, and (4) loss of air-start air pressure through interconnecting lines.

The BFR computer code was also used to calculate a failure rate for each of these six categories. A CCF rate attributed to hardware is calculated by adding the generic rate to those of each failure mode applicable to a specific plant. The range of hardware CCF probabilities is shown in Table II.

Failure probabilities for dc systems,[3] plant service water systems,[4] and offsite power systems[5] were obtained from other reports. The frequency of loss of offsite power is divided into three categories: (1) plant centered losses which can generally be repaired by maintenance facilities at the plant; (2) area wide storm losses for which recovery is affected by wide area destruction; (3) area wide blackouts which cannot be repaired at the plant. The failure probabilities or frequencies for these three systems are given in Table II.

Reliability Analysis

Fault trees developed for the 18 plants were analyzed using the MOCUS [6] and SUPERPOCUS [7] computer programs. Plant specific failure probabilities, for which the ranges are shown in Table II, were used in each fault tree. The ranges of onsite ac power system reliability for the 18 plants studied are shown in Table III.

A sensitivity analysis was performed to determine the potential for reliability improvement for several design and procedural modifications. The failure probabilities were changed to reflect achievable values based on operating experiences. The results of a sensivitity analysis are in Table IV.

Cost of Onsite System Improvements

The costs of several methods to improve the onsite ac power system are presented below. Possible improvements must be evaluated for each plant. Only the direct costs of the modifications are estimated, but indirect costs, such as the cost of additional reactor downtime, may add as much as $500,000 per day. These estimates may vary depending on plant specific characteristics.

Independent diesel failure probability cannot be significantly reduced for the nuclear industry, but plants with independent failure probabilities much higher than average may achieve a significant reduction in independent failure probability and system undependability. Several methods to reduce the independent failure probability and the associated costs are as follows: install air dryers on the air-start system, $100,000 per diesel; install gaskets on relay cabinets, $10,000 per diesel; periodic overhaul of the governors, $10,000 per diesel.

Improving maintenance procedures will reduce human error CCF probability. The cost of rewriting a maintenance procedure is approximately $5,000 per procedure.

Three hardware modifications that will reduce CCF probability are the following: install a drain on the bottom of the fuel day tank, $10,000 per diesel; remove connections between independent air-start systems, $5,000 per diesel; add an effective corrosion inhibitor to the diesel engine jacket-water, $500 per diesel per year.

TABLE III

Results of Onsite Power System Reliability Analysis

Diesel Generator Configuration	Range of System Unavailability per Demand	Dominant Failure Causes
2-of-3	$4.2 \times 10^{-3} - 4.8 \times 10^{-2}$	Independent diesel failure. Human error CCF.
1-of-2	$1.1 \times 10^{-3} - 6.8 \times 10^{-3}$	Independent diesel failure. Human error CCF. T&M outages.
2-of-4	$3.7 \times 10^{-4} - 1.7 \times 10^{-3}$	Human error and hardware CCF.
1-of-3	$1.8 \times 10^{-4} - 7.2 \times 10^{-4}$	Human error, hardware, and service water CCF. Independent diesel failure. DC power CCF.
2-of-5	$1.4 \times 10^{-4} - 2.5 \times 10^{-3}$	Human error, hardware, service water, and dc power CCF.

TABLE IV

Onsite System Sensitivity Analysis

Basic Event, Plant, and Success Logic	Basic Event Failure Probability Changed		Onsite System Unavailability Changed	
	From	To	From	To
Independent failure				
Plant A, 2-of-3	8.2×10^{-2}	4.1×10^{-2}	4.8×10^{-2}	3.1×10^{-2}
Plant B, 1-of-2	5.9×10^{-2}	3.0×10^{-2}	4.2×10^{-3}	2.1×10^{-3}
Hardware CCF				
Plant C, 2-of-5	1.8×10^{-3}	8.6×10^{-5}	2.5×10^{-3}	8.0×10^{-4}
Plant D, 1-of-3	6.0×10^{-4}	2.4×10^{-5}	7.2×10^{-4}	1.5×10^{-4}
Human error CCF				
Plant E, 1-of-2	8.8×10^{-4}	3.4×10^{-4}	1.5×10^{-3}	1.0×10^{-3}
T&M unavailability				
Plant F, 2-of-3	4.5×10^{-2}	0	4.8×10^{-2}	2.5×10^{-2}

Scheduled maintenance during reactor operation contributes to onsite system unreliability. Some plants do not schedule diesel generator downtime during reactor operation while others have scheduled maintenance unavailability equal to six times the industry-average. The cost of deferring scheduled maintenance may be the expense of hiring additional maintenance staff. Also, deferring scheduled maintenance may increase the independent failure probability. Because of these factors, scheduling of maintenance has to be evaluated on a plant specific basis.

CONCLUSIONS

The undependability of the onsite ac power system was estimated for several designs using plant specific data. The important contributors to onsite power system undependability were found to be plant specific. Independent diesel generator failure was the important contributor for most of the 18 plants modeled. Other important contributors were CCF because of hardware failure or human error, unavailability because of scheduled maintenance, and cooling subsystem undependability.

There were no dominant independent diesel generator failure modes identified in this study. Three failure modes, which caused ~17% of all diesel generator failures, are dirt and moisture on relays and switches, contaminated oil in the governor and governor setpoint error, and moisture in the air-start system. Contribution to failure by these failure modes may be reduced by improved design and maintenance. Some diesels may have a failure mode that is causing a large number of failures for that diesel. If this failure mode were reduced, the onsite system unavailability may be reduced significantly.

Common-cause failure for some plants is a significant contributor to onsite system unreliability. Diesel generator CCF potential is increased by the following design features: no drain from the bottom of the fuel day tank; inadequate corrosion inhibitor in jacket-water; and connections between independent air-start systems.

Human error contribution to CCF can also be significant. Maintenance and test procedures that are difficult to understand, do not include review of maintenance, and do not include a verification test after maintenance, contribute to the probability of CCF by human error.

Scheduled maintenance at a few plants is a significant contributor to onsite system unavailability. Rescheduling preventive maintenance should be carefully evaluated to determine if the onsite system unavailability can be reduced.

Reliability of onsite ac power systems varies from plant to plant. Several areas have been identified that can be important to onsite ac power system reliability. Any reliability improvements and the associated costs must be evaluated on a plant specific basis.

ACKNOWLEDGEMENT

Research sponsored by the Office of Regulatory Research, U.S. Nuclear Regulatory Commission, under Interagency Agreement No. 40-544-75 with the U.S. Department of Energy under contract No. W-7405-eng-26 with Union Carbide Corporation.

REFERENCES

1. Millstone 2, NRC Docket No. 50-336, LER 81-005, Event date 1/2/81.

2. C. L. Atwood and W. J. Suitt, "User's Guide to BFR, A Computer Code Based on the Binomial Failure Rate Common Cause Model," NUREG/CR-2729, Idaho National Engineering Laboratory (1982).

3. P. W. Baranowsky, A. M. Kolaczkowski, and M. A. Fedele, "A Probabilistic Analysis of DC Power Supply Requirements for Nuclear Power Plants," NUREG-0666 (1981).

4. A. M. Kolaczkowski and A. C. Payne, "Station Blackout Accident Analyses," Draft final report, Sandia National Laboratories, July 1982.

5. F. H. Clark, "Offsite Power System Reliability Analysis," letter from J. L. Anderson (ORNL) to G. R. Burdick (NRC), March 2, 1982.

6. J. B. Fussell, E. B. Henry, and N. H. Marshall, "MOCUS-A Computer Program to Obtain Minimal Sets from Fault Trees," Aeroject Nuclear Co., ANCR-1156, March 1974.

7. J. B. Fussell, D. M. Rasmuson, and D. P. Wagner, "SUPERPOCUS-A Computer Program for Calculating System Probabilistic Reliability and Safety Characteristics," NERS-77-01, Nucl. Engr. Dept., University of Tennessee, Knoxville, 1977.

THE RISKS DUE TO FIRES AT BIG ROCK POINT

Wesley A. Brinsfield

Wood-Leaver and Associates, Inc.
1340 Saratoga-Sunnyvale Road
Suite 206
San Jose, CA 95129 U.S.A.

David P. Blanchard

Consumers Power Company
Big Rock Point Plant
R. R. #3
Charlevoix, MI 49720 U.S.A

ABSTRACT

The unique and older design of the Big Rock Point nuclear plant is such that fires contribute significantly to the probability of core damage predicted in the probabilistic risk assessment performed for this plant. The methodology employed to determine this contribution reflects the unique, as constructed, plant design, while systematically and logically addressing the true effect of fires on the operation of the plant and the safety of the public. As a result of the methodology utilized in the PRA, recommendations are made which minimize the risk of core damage due to fires. Included in these recommendations is a proposal for equipment and controls to be included on the Big Rock Point alternate shutdown panel.

INTRODUCTION

As part of the probabilistic risk assessment performed for Consumers Power Company's Big Rock Point (BRP) nuclear power plant [1] a comprehensive investigation of the risk or core damage due to common mode fire related accident sequences has been carried out. The purpose of this investigation was to determine areas within the plant boundaries which are important from a fire related risk viewpoint, to quantify this risk based upon data collected on fire initiation frequencies, and to make recommendations for plant modifications which would reduce this risk. Because of the design of the plant a perhaps unique methodology for risk quantification was applied which systematically and logically reflects the configuration of the plant as actually built.

Of primary concern in the analysis was the identification of locations within the plant which contain equipment necessary for the cooldown of the plant, and the determination of the fire hazard and fire suppression capabilities in these locations. The focus of this investigation was on the identification of any single locations containing equipment (primarily electrical power and/or instrumentation and control cables) whose failure due to fire damage would be sufficient to prevent core cooling and would lead directly to core damage without any further random failures of other equipment.

It was assumed for this evaluation that the reactor was shut down, either manually or through automatic reactor protection system (RPS) operation, during the fire. Therefore, the systems of importance were those which may be called upon to handle the decay heat load of the reactor core. This assumption is important in that credit is taken for successful use of the RPS and control rod drive system to shut down the reactor.

At Big Rock Point the heat sinks available to remove decay heat after shutdown are the main condenser (MC), the emergency condenser (EC), and the shutdown cooling system (SDS). Sources of water to the core are the feedwater (FW) and control rod drive (CRD) pumps, and the core spray mode of the fire protection system (FPS). A fire in an area common to all of these systems which disabled them all is an example of common mode failures initiated by fire and leading directly to core melt due to undercooling of the core. In the analysis performed for BRP no credit was taken for the shutdown system because its operation is contingent upon low reactor vessel pressure and containment accessibility. Failure of both the main and emergency condensers would lead to either reactor depressurization system (RDS) or safety valve operation, in which case it is assumed that containment is inaccessible. Because initiation of the SDS at BRP requires manual entry into containment to close circuit breakers, the SDS could not be assumed to be available.

METHODOLOGY

Based upon a working knowledge of the plant, and upon event and fault trees constructed for the PRA, a "formula" for multiple system failures which result in core damage was determined. Using fault tree notation, with '+' representing the OR logic, and '·' representing AND, the system failures caused by the common mode of fire which would lead to core damage can be expressed as:

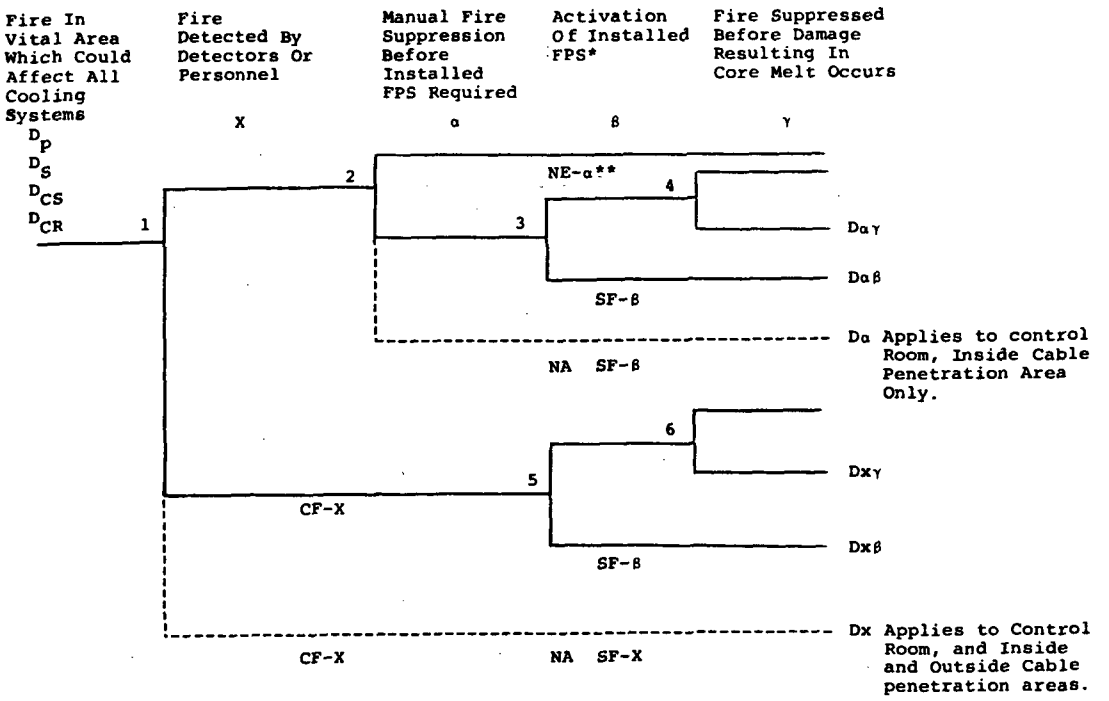
$$\text{Core Damage} = (\text{RDS} + \text{FPS}) \cdot \left[(\text{CRD} \cdot \text{FW}) + (\text{MC} \cdot \text{EC})\right] \qquad (1)$$

The objective, then, was to determine if any areas exist within the Big Rock Point plant which contain the necessary electrical or I&C cables that, if failed due to fire damage, would satisfy the conditions of Equation (1). Following a thorough physical inspection of the plant, and utilizing work previously performed for Consumers Power Company, four areas within the plant confines were identified which contained the vital components to satisfy this formula. These areas are the Station Power Room, the Inside Cable Penetration Area, the Outside Cable Penetration Area, and the Control Room. A fire in any of these spaces, if not extinguished in time, could conceivable destroy sufficient cabling to disable all cooling systems at the plant and result directly in a core melt situation. It should not be overlooked that there are other key areas within the plant in which a fire would affect just one or two systems. However, for accident sequences initiated by fire, these failures, to become important contributors to risk, must be coupled with random failures in other parts of the plant.

QUANTIFICATION

After the identification of the areas noted above, the quantification of the risk due to fires in these areas was attempted. The risk of core damage due to a fire in any of these spaces was found to be dependent upon four factors: (1) the probability of a fire starting in the space in question and being large enough to affect all of the necessary systems, (2) the probability of the fire being detected in time to initiate suppression before all systems are disabled, (3) the success of the suppression attempts, and (4) the actual amount of cable damage inflicted by the fire. To assist in this process, an event tree was constructed. This event tree is presented as Figure 1.

Figure 1 Event Tree for Fire Sequences.



* Manual activation in Outside Cable Penetration Area
Automatic activation in Station Power Room
No sprinklers in Control Room, Inside Cable Penetration Area

** NE-α = No effect due to result of event heading α
NA = Not applicable
SF = System failure
CF = Conditional failure

The initiating frequency of the fires was based upon data compiled from the nuclear industry on fires which have started within the various plant sites during operating, hot or cold shutdown, or refueling/extended outages. [2,3] This data has been broken down into pertinent areas (i.e., control room, station power room, etc.) within the plants. Twenty-five percent of these fires did or could (if not detected or extinguished) affect the engineered safety features of the plants. The compartment specific initiating frequencies were thus reduced by a factor of 75% to eliminate small, self-extinguishing fires such as those in waste baskets. In a report by Hockenbury and Yeater, [4] a factor of approximately 16% was used for the probability of safety system loss given a fire. This compares reasonably well with the 25% factor employed here. However, the remaining 25% include fires which affected any part of a safety system, but not necessarily all redundant trains of one system, or all systems in one area. Thus, for application in this analysis where total negation of systems is necessary for core melt to result, additional factors, such as cable tray loading and arrangement, were considered for each area. Cables which are tightly bunched, or in vertical tray alignment, can be expected to ignite in a fully developed fire. However, if the trays are horizontally separated, the likelihood of fire spread increases only as the size and heat of the fire increases. Therefore, a factor to account for this separation, if it exists, should be included when considering fires that lead to core melt if not extinguished. These additional factors were determined by engineering judgements on a relative scale based upon bunching of cables, cable tray separation, and proximity of cable trays. Table 1 contains the factors used to determine the initiating frequencies for the fires in the four spaces considerd. As explaination of how the factors were estimated follows.

TABLE 1

Initiating Frequencies Used For Vital Spaces

(Per Compartment Year)

Area	Frequency * If All Fires Considered	25% Frequency (Fires Which Affect Some Safety Features)	Additional Factor To Account For Affect On All Safety Features	Frequency** Used For Quantification
Control Room	4.1×10^{-3}	1.0×10^{-3}	0.1	1.0×10^{-4}
Outside Cable Penetration Area	7.2×10^{-3}	1.8×10^{-3}	0.5	9.0×10^{-4}
Inside Cable Penetration Area	7.2×10^{-3}	1.8×10^{-3}	1.0	1.8×10^{-3}
Station Power Room	1.3×10^{-2}	3.3×10^{-3}	1.0	3.3×10^{-3}

* From Reference 2, 3
** "25% Frequency" x "Additional Factor"

Virtually no separation exists in the cable penetration area inside containment, or in the Station Power Room. The cables within these spaces are tightly grouped, or in trays that are vertically arranged. Therefore, no additional decrease factor (other than the 25% factor already described) was utilized for these two areas.

The cable trays in the outside cable penetration area are separated horizontally as well as vertically. A fire in a bottom tray will involve the trays above it in almost all cases, but those to the sides will be engulfed only after all trays in the original fire zone are in flames. The predominant type of cable at Big Rock Point is polyethylene/polyvinyl chloride (PE/PVC), for which the likelihood of progation for a fully developed fire has been shown to be fairly high. [5] Therefore, although the trays are separated, it was assumed that 50% of the fires in the outside cable penetration area which could affect all safety systems, do have that effect.

A fire in the control room is important, from a cooling systems point of view, if two main panels identified in the analysis are both in flames. (Of course, any fire in the control room is important when considering control room habitability and continued monitoring of plant status). These panels are separated by distance and by other panels, making the likelihood of spread before being extinguished remote. However, the cables entering the control room all enter in one area before spreading out to the different panels. If the fire happens to start there, or spread to that point before detection or suppression, all cables will be affected. For this reason, an additional conservative factor of 10% was applied to control room fire.

Based upon this system of quantification the Station Power Room was determined to have the highest probability for a fire which could affect all necessary cooling systems if not extinguished. The total initiating frequency for fires which would involve all cooling systems and lead to core melt if not extinguished was calculated to be 6.1×10^{-3}/compartment year.

Probabilities for failure to detect the fire were based upon factors such as the presence of smoke and flame detectors and the routine plant walk-through by personnel. Insurance statistics were utilized to estimate the probability of failure of detectors and annunciators. [4, 6] A 1/3:2/3 weighting scheme for day:night walk-throughs was used to estimate the probability of human detection. [4] The total probability for failure to detect was estimated to be on the order of 3×10^{-3}/demand.

Probabilities for failure to extinguish the blaze were separated into two categories: early, or manual, suppression (i.e., using hand held hoses, extinguishers, etc.) and late, or automatic, suppression (i.e., installed fire sprinklers). These probabilities are also affected by cable and cable tray proximities, as well as accessibility for fire fighting apparatus, among other things. Several of the identified areas do not have automatically initiated sprinkler systems. Failure to detect a fire in these areas was assumed to result in extensive cable damage which would then result in damage to the fuel. The probabilities for failure to manually suppress the fire before the sprinklers (if in place) are required range from 1×10^{-3} to 1×10^{-1}/demand, depending upon the location, the availability of fire fighting equipment, the arrangement and density of cable trays, etc. The failure to extinguish the fire with the automatic sprinklers is on the order 10^{-3}/demand. These values are consistant with "non-suppression" factors reported in Reference 4. Within this report it is stated "... these probabilities are useful for preliminary ranking but should not be taken as final values", seemingly in acknowledgment of the difficulty encountered in dealing with such a subjective subject matter.

A final factor in determining the probability of core damage due to fires is the determination of the extent of cable damage. Even if the fire is successfully extinguished there is a chance that extensive damage to cables and equipment may already have occurred.

Based upon References 2 and 7, through 1978 there were a total of eight fires involving grouped electrical cables (including Browns Ferry). Because the Browns Ferry fire damaged more than 1600 cables before being extinguished, of which over 600 contained safety-related circuits, it will be considered as a data point for failure to suppress a detected fire before excessive damage occurs to the cables. This results in a failure rate of 1/8, or 0.125, per demand. If the fire is undetected, and only the automatic sprinkler system is available, this probability increases due to the longer period of time that the fire burns before suppression begins. If an additional 10% chance of failure is assumed for damage due to undetected fires, the total probability becomes 0.225/demand for spaces where automatic sprinklers are available.

A summary of the factors employed for the quantification of fire initiated sequences is presented in Table 2.

Using Figure 1 as a guide for the quantification of the fire sequences, and utilizing the applicable failure rates discussed previously and contained in Table 2, the risk of core damge due to fires at Big Rock Point was estimated to be 2.3×10^{-4} per reactor-year, nearly twenty five percent of the total core damage frequency calculated in the PRA performed for this plant. [1]

To reduce this risk, several recommendations were made, including equipment to be powered from an alternate shutdown panel at the site. The recommendations include (1) procedural modifications instructing the operator to immediately establish a secondary decay heat sink, which is known as the emergency condenser at Big Rock Point, and to supply makeup water to the secondary side of this condenser, (2) improved sprinkler coverage in the areas identified, and (3) separating power supplies and control circuitry for specific plant cooldown equipment from the four areas identified to an alternate shutdown panel. Included on this panel would be main steam isolation valve power and control circuitry, emergency condenser valve and secondary side makeup power and control, steam drum, reactor pressure, and emergency condenser

TABLE 2

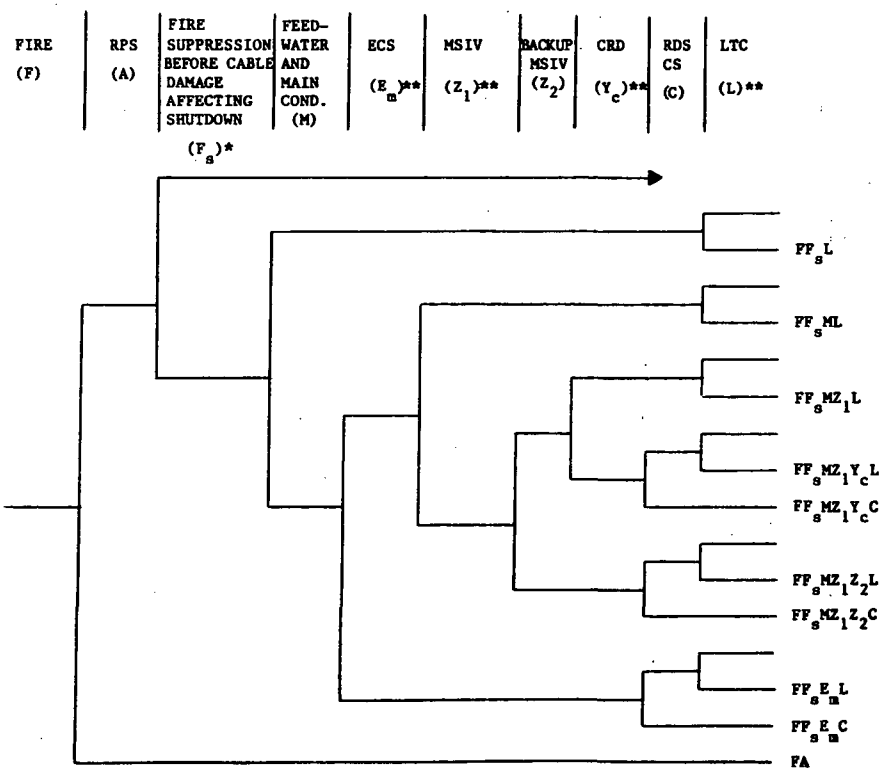
Probabilities Used in Event Tree Quantification

Area	Fire Initiating Frequency (Per Compartment Year)	Fire Not Detected (Per Demand)	Fire Not Manually Supressed Before Sprinklers Required (Per Demand)	Failure Of Sprinklers To Activate (Per Demand)	Failure To Prevent Cable Damage With Sprinklers (Per Demand)
Control Room	1×10^{-4}	1×10^{-4}	1×10^{-3}	1.0*	NA
Inside Cable Penetration Area	1.8×10^{-3}	3.1×10^{-3}	1×10^{-1}	1.0*	NA
Outside Cable Penetration Area	9×10^{-4}	3.1×10^{-3}	1×10^{-2}	3×10^{-3}	0.125** 0.225
Station Power Room	3.3×10^{-3}	3.1×10^{-3}	1×10^{-1}	2×10^{-3}	0.125** 0.225

* These areas have no sprinklers. Failure of manual action implies cable damage will result with probability unity.

** Large value used if no manual action taken before sprinklers activate, so that fire is larger when sprinklers are required. (see write-up)

Figure 2 Alternate Shutdown Area Fire Tree



* Quantified as in Figure 1

** Controls and Power supplies located on alternate shutdown panel

instrumentation, and controls and power for a control rod drive pump, which is capable of maintaining level in the reactor vessel at the decay heat level. The increased sprinkler coverage and cable separation is effective in reducing the probability of significant cable damage in systems required for shut down cooling of the reactor core. Quantification of this effectiveness is somewhat subjective, however. Quantification of the reduction in core damage frequency due to the shutdown panel is more definitive because equipment failure is dependent on random failure rates rather than the fire in this case. A large data base exists for random component failure rates. Using Figure 2 as an aid, and employing system failure rates calculated from fault trees constructed for the Big Rock Point PRA, the core damage frequency due to fires was calculated to be 3.3×10^{-6}/year with the shutdown panel in place.

CONCLUSIONS

The risk of core melt due to fire at Big Rock Point is relatively high, on the order of 2.3×10^{-4} per reactor year. This number reflects what are believed to be conservative assumptions, and is based upon limited data. Engineering judgement has been used to determine, on a relative scale, the risk due to fire in four vital areas within the plant.

The largest contributors to risk from fire are the areas of the Station Power Room and the Inside Cable Penetration Area. These areas have the least cable separation, and are less accessible for fire fighting purposes than the Outside Cable Penetration Area or the Control Room.

As indicated by the probability of core melt due to fires, the risk is great and awareness of this danger may help reduce this risk. This risk can be reduced by improved fire protection design, but will remain relatively high unless some cable separation takes place.

If cable separation and improved automatic sprinklers are considered, and the operators are instructed to establish the emergency condenser as a heat sink immediately upon fire identification in one of the four areas indicated, the probability of core damage due to fires decreases significantly. If an alternate shutdown panel is installed remote from the four areas of concern, core damage probability due to fire sequences is estimated to be reduced to 3.3×10^{-6}/year.

Big Rock Point is now involved in preparations for installation of the alternate shutdown panel. Other recommendations have been accepted by Consumers Power Company and are being incorporated into the operation of the plant.

REFERENCES

1. Consumers Power Company, Probabilistic Risk Assessment, Big Rock Point Plant, March 1981.

2. A. G. Sideris, R. W. Hockenbury, M. L. Yeater, W. E. Vesely, "Nuclear Plant Fire Incident Data File," Nuclear Safety, Vol. 20, No. 3, May-June 1979.

3. G. Apostolakis, M. Kazarians, "The Frequency of Fires in Light Water Reactor Compartments," CONF-800403/V-1, ANS Topical Meeting of Thermal Reactor Safety, Knoxville, Tenn., April 1980.

4. R. W. Hockenbury, M. L. Yeater, "Development and Testing of a Model for Fire Potential in Nuclear Power Plants," NUREG/CR-1819, November 1980.

5. L. J. Klamerus, "Fire Protection Research Program at Sandia Laboratories," paper presented at US NRC Eighth Water Reactor Safety Research Information Meeting, October 1980.

6. D. S. Moelling, A. G. Sideris, R. W. Hockenbury, "Reliability of Fire Protection Systems in Nuclear Power Plants," CONF-800403/V-1, ANS Topical Meeting on Thermal Reactor Safety, Knoxville, Tenn., April 1980.

7. J. H. Talbert, "Fire Hazards and Consequences of Fire in Nuclear Power Plants," Nuclear Safety, Vol. 21, No. 1, Jan-Feb. 1980.

THE PROGRAM TO STUDY THE RELIABILITY OF SAFETY SYSTEMS IN THE PALUEL 1300 MWe PWR POWER PLANT : ORGANIZATION, METHODOLOGY, FIRST CONCLUSIONS

M. LLORY - A. VILLEMEUR
Electricité de France - Direction des Etudes et Recherches
Service Réacteurs Nucléaires et Echangeurs
6, Quai Watier - 78400 CHATOU, FRANCE

P. BRUNET
Electricité de France - Direction de l'Equipement
Région d'Equipement de Clamart
2, Avenue du Général de Gaulle - 92141 CLAMART Cedex, FRANCE

ABSTRACT

The paper outlines the program to study the reliability of safety systems in the PALUEL power plant, the first of plant of Electricité de France's 1300 MWe series of units. Studies started in July 1981 and should be completed by the beginning of 1983.

Having reviewed the aims of this research program, the organization set up to perform fourteen system studies is depicted. These systems are : electric power supply systems, engineered safety features, safety thermohydraulic systems and the spent fuel cask handling crane.

Then, follows a description of the method employed for each type of study which comprises FMEAs, the analysis of potential common mode failures and human errors and of operating experience gained with 900 MWe power plants, and, finally, the identification of system failure configurations and their quantification. Four examples are presented to illustrate the method and the first lessons drawn from this program are set out.

INTRODUCTION

The Direction de l'Equipement of Electricité de France has decided to collect a whole set of reliability analyses pertaining to the main safety systems of the PALUEL nuclear power plant, which is the first of the new series of 1300 MWe nuclear reactors.

The general objectives of the study are :

- reliability analysis of the main systems of the PALUEL plant and comparison of the results with those obtained for the first French 900 MWe unit.

- drafting of technical operating specifications to be used when partial unavailabilities of safety systems are detected.

- determination of the optimum test frequency for standby safety systems.

A quantitative and qualitative evaluation of the reliability of safety systems is necessary to be able to work out operating requirements. Our first task was therefore to carry out these reliability analyses.

The Region d'Equipement of Clamart asked the Direction des Etudes et Recherches in june 1981 to undertake this work which embraces the study of fourteen relatively different systems :

- electric and electromechanical systems : the 6.6 kV electric power supply systems, the 125 V power supply to instrumentation and controls and the standby diesel generators.

- thermohydraulic systems : the component cooling system and the service water system, the residual heat removal system, the safety injection system, the spent fuel pool, the auxiliary feedwater system, the chemical and volume control system, the containment spray system, the depressurization system of the annular space between the containments and the steam generator isolation valves.

- mechanical systems : the spent fuel cask handling crane.

The global study undertaken by the Direction des Etudes et Recherches is similar, as far as its objectives and its scope are concerned, to the one carried out from 1976 to 1978 for the Fessenheim plant, the first of the 900 MWe series of reactors [1].

The organization of the study programme and the general procedure followed to fulfil this programme are presented.

Then the present results of these studies are set forth and specific organizational and methodological aspects of the programme are highlighted, with a special stress being laid on the impact of the results on the system design.

ORGANIZATION OF THE RESEARCH PROGRAM

To carry through this task, outside engineering and design firms were requested by the Direction des Etudes et Recherches (DER) and the Region d'Equipement of Clamart to perform seven studies, FRAMATOME undertaking two other studies, the five remaining ones being carried out by the Division Etudes Probabilistes (DER) . In the framework of this general programme, EDF is responsible for the execution of part of the studies and for the follow-up of the other ones. The Direction des Etudes et Recherches intends to harmonize the studies so that the body of

analyses is on the whole, consistent as regards the hypotheses, the modelling of the different systems, the methods used for the analysis and the reliability data.

The programme of reliability studies can be successfully carried out, although the work has to be finished within a relatively short period of time as it should be completed by march 1983, thanks to the close cooperation of the concerned services of the Region d'Equipement of Clamart and of the Direction des Etudes et Recherches, on the one hand, and to the experience of the Division Etudes Probabilistes - gathered after six years devoted to reliability analysis and probabilistic methods, on the other.

A total of about 110 to 120 engineer-months will be devoted to this work.

CONTENT OF THE STUDIES

The study of each system can be subdivided in four main steps

- a thorough study of the" Dossier de Système Elémentaire" (reports on elementary systems) and the collection of the data required for the study; for each system of a nuclear unit, especially for all the engineered safety features, a file is prepared by the concerned Region d'Equipement. This file is supplemented at regular intervals and updated as the work proceeds. These "Dossiers de Systèmes Elémentaires" (DSE) contain all the data available on a system : accurate description and operation of the system for all the unit operating conditions - in particular for abnormal or accident conditions.

- a detailed qualitative analysis using proven reliability methods such as the failure mode and effects analysis (FMEA) and fault trees, including the study of common mode failures and of potential human errors. This analysis is supplemented by the processing of event reports (at the system level) submitted by the Service de la Production Thermique and of component failure reports obtained from the Système de Recueil de Données de Fiabilté, SRDF (Reliability Data Bank), which is operational since April 1978 for the 2 units of the Fessenheim power plant and the four units of the Bugey power plant [2] . This analysis takes into account our operating experience with the 900 MWe French nuclear power plants since 1978.

Henceforth, the qualitative analysis implies that all the main system failure configurations having an impact on the safety of nuclear units are identified.
- a quantitative analysis performed to determine system failure probabilities, uncertainty margins and importance factors. This analysis is based on reliability data pertaining to the equipment and components, obtained from the SRDF ;

- a synthesis of the qualitative and quantitative analyses, in order to draw lessons from each study and, in particular, to specify potential weak points in the systems.

In these studies, a special attention is given to the breakdown level, the detail level chosen for the analysis of each system, the exhaustive preliminary analysis of the various operating configurations in which each system functions - including the possible inadvertent operations - and to the system delineation for the study purpose (precise definition of the system limits ; consideration of the auxiliary sytems and/or of interactions with other systems).

The general procedure selected depends on the system nature and on the development stage reached for each system. Two different types of studies were carried out for the Paluel power plant :

- preliminary studies conducted during initial development phases which provide elements for decision making to be used at following development stages as regards the system general structure (selection of the redundancy level; incorporation or not of certain components, in some particular points of the system for instance) ;

- comprehensive studies carried out during the final development phases to check the design, to highlight the potentiel weaknesses in each system and to introduce, when necessary, a few changes in the design on the one hand to stress the need for instance to reinforce the controls, the maintenance, the prevention of human errors during operation on the other.

To illustrate this approach, four types of studies performed are described below :

- a preliminary study on the SIS of the cost-efficiency type to determine the system redundancy level ;
- a second preliminary study on the AFWS to compare several possible patterns for the system and the comprehensive study of this system during the final development phase ;
- the comprehensive study of a mechanical system : the spent fuel cask handling crane ; this study highlights the probabilistic method developped at EDF to study handling systems.

FIRST EXAMPLE OF PRELIMINARY STUDY : DEFINITION OF THE REDUNDANCY LEVEL OF THE SIS

As this system is very important for the safety of the nuclear unit and as its own design has an impact on the layout of numerous other systems, a comparative study was carried out concerning both safety and economics, for two types of the system, one with a two-train layout,and the other with a three train one (Figure 1).

To preserve all the advantages of an increased redundancy of the safety injection system, the same redundancy level must be chosen for all the supporting systems which are important for the proper operation of the safety injection sytem, ie the electric supplies, the component cooling system, the service water system, etc ... When the design is changed from a 2 train layout to a 3 train one, the cost rises significally.

Moreover, when the train number grows, it is increasingly different to find a system layout such that the components are physically well separated and efficiently protected against common mode failures ; finally, the more safety components are provided, the more work the staff has to conduct the controls, the tests and the maintenance operations.

Therefore, a view of a drawbacks of high redundancy level, it appeared necessary to evaluate its advantages from the safety point of view before the decision was taken to give up the basic two-train design.

The probabilistic study consisted in calculating the unavailability of the safety injection system for each layout in two typical situations : a small break (equivalent diameter : 1.9 to 5 cm) and a large break (diameter greater than 15 cm). The analysis was conducted on the basis of a number of simplifying hypotheses and in particular it was assumed that the probability of a pipe rupture is identical in the 4 primary system loops as well as for a hot and a cold leg. It was also assumed for conservatism's sake that the flowrate fed by the SIS train to the ruptured pipe is completely lost, whatever he break size [3] [4]. The following results are obtained with the fault tree analysis :

TABLE I

DESIGN TYPE	TOTAL UNAVAILABILITY OF SIS UPON DEMAND	
	Large Breaks	Small Breaks
2 trains	3.3×10^{-4}	5.0×10^{-4}
3 trains	2.0×10^{-4}	2.5×10^{-4}

The gain in availability, is limited by the rupture location and the volume of water assumed lost, by the impact of maintenance and of common mode failures. A median value of 5×10^{-5} was chosen for unavailabilities attributable to this type of failures [5] : nowadays, the contribution of common mode failures to the unavailabilities of SIS type-systems is estimated to vary from 10^{-3} to 10^{-4} [6] . With a value of 10^{-3}, the gain in availability of the 3 train layout against the 2 train layout is even smaller.

Figure 2 illustrates the variations of the SIS system unavailability as a function of the corresponding rise in the plant cost for each new improvement of the SIS system. The successive gains in availability thus obtained for the 2 train pattern result from a complete revision of the overall layout (evolution from the Fessenheim type design to the Tricastin one) and, after, from the complete separation of the SIS and CVCS systems (evolution from the Tricastin design to the Paluel one). But, on the other hand, if the design hand evolved into a 3 train system, the cost would have soared due to the greater redundancy of the SIS supporting systems and to the changes in plant layout.

Therefore, the 2 line solution was selected.

SECOND EXAMPLE OF PRELIMINARY STUDY : SELECTION AMONG SEVERAL DESIGNS OF THE AFWS

Four different designs were confronted. Their general structure is shown in Figure 3. Only the main components of each system were considered in this study : pumps, main piping networks, isolating and regulating devices. For each proposed design, the unavailability of the AFWS during specific situations requiring its operation, added to its failure probability during its operation is computed. Three typical situations were selected : the loss of offsite power sources, the rupture of a steam or feedwater line, a situation corresponding to all the unit condition requiring the operation of the AFWS, but not likely to affect its operation [3] [7] . The quantitative evaluation of the system failure probability is based on the calculation of three factors, separately : the contribution of random and independant failures, the contribution of maintenance and common-mode failures. A common mode failure probability of 10^{-5} was taken both for the 4-train or 3-train designs [5] . This value can be considered a lower bound, since the study of licensee Event Reports, in USA, gives a higher value [6] .

Even with this hypothesis, the prevailing impact of these failures nevertheless stands out as it may be seen on Table II.

TABLE II - AFWS UNAVAILABILITY

TYPE OF ACCIDENT	NATURE OF FAILURES	DESIGN N° 1	2	3	4
LOSS OF OFFSITE POWER	Random independant failures	$4.0x10^{-6}$	$1.6x10^{-7}$	$1.6x10^{-8}$	$8.9x10^{-9}$
	Maintenance contribution	$8.8x10^{-6}$	$7.0x10^{-7}$	$1.2x10^{-7}$	$1.2x10^{-7}$
	Common mode failures	$1x10^{-5}$	$1x10^{-5}$	$1x10^{-5}$	$1x10^{-5}$
	TOTAL	$2x10^{-5}$	$1x10^{-5}$	$1x10^{-5}$	$1x10^{-5}$

Therefore, the decision was taken to choose the design less likely to result in errors in the operational procedure and with the best physical separation of the channels. This is n° 4 (Figure 3-4).

EXAMPLE OF A COMPREHENSIVE STUDY : AFWS AT THE FINAL DESIGN STAGE

After the preliminary study performed during the initial phase of the project, in 1975-76, a detailed study of the AFWS was undertaken and completed in 1981-1982, at the last stage of the system design. The study had two purposes :

(i) identify and differenciate abnormal operating conditions in the unit during which the AFWS system must perform a safety function ;

(ii) assess the AFWS failure probability for each of these conditions.

The AFWS is made of two independant and identical flow paths, each connected to two steam generators (Figure 3-4). Each flow path comprises two trains capable of supplying a water flowrate of 100 m^3/hr to each of two SGs, thanks to a motor-driven pump and a turbine-driven pump.

The method adopted for this study was the same as the one described above although of course this study was more detailed than the preliminary one. Among others, an FMEA 8 as well as a study of common mode failures (CMF) have been conducted. The most

important potential human errors appear as external causes of failure modes. In the CMF analysis, an attempt is made at identifying human errors during reactor operation, periodic tests or maintenance. The latter analysis was performed using a systematic procedure based on standard tables. An example of this type of table is shown below.

TABLE III - TABLE USED TO STUDY CMF_s

Common mode failure category	Type of failures in this category	Incidents recorded (in the USA, in France)	Conventional protection sytems (900 MWe plants)	New protection systems or provisions (1300 MWe plants)	Quantification of these failures

The analysis helped to draw attention to the reopening of the regulating valves downstream of the pumps after they have been quickly closed by the operators to isolate a ruptured SG (in case of rupture of a feedwater or steam piping or of a SG tube). The valve reopening due to an AFWS starting order may surprise the operator and consequently the affected SG may remain unisolated for some time.

After a thorough study of all operating conditions -including abnormal and accidental sequences - five typical situations were considered :

1) loss of main feedwater system ;
2-4) loss of offsite power, of a 48 V control channel, of a 125 V control channel ;
5) rupture of a feedwater line.

Figure 4 gives an example of a partial fault tree obtained during the study ; it concerns the loss of a turbine-driven pump. Calculations were made with the FIABC code [9] [10] . Data used were obtained from EDF operational experience [2] , and in particular cases, from the Appendix 3 of the WASH-1400 report 5.

The following type of quantitative results were obtained : if a feedwater pipe breaks the AFWS (two SGs fed with 100 m^3/hr to avoid boiling of the RCS) failure rate is 5.8×10^{-4} (error factor : 1.5). The probability that no SG can be supported with water is 4.6×10^{-7} (error factor : 1.6).

The study shows the importance of condition II occurrences such as the loss of normal feedwater and the loss of offsite power. In fact, the probability of the AFWS not being capable to perform its function is the same as for condition III or IV occurrences, whereas the probability of condition II occurrences is much higher. However, the consequences of a loss of the AFWS capability to perform its intended function will differ : on the

one hand (Condition II Occurrences) the pressurizer will be filled, on the other, the RCS water will boil.

Note that the reliability study of the AFWS of Paluel plant is the subject of a Reliability Benchmark Exercise undertaken in the framework of the European Communities [11] . Eight countries and fifteen organizations of these countries participate in this exercise which will end at the beginning of 1983.

STUDY OF THE SPENT FUEL CASK HANDLING CRANE

Several studies were performed to analyze the risk of a load being dropped while handled by a crane, in the fuel building or in the reactor building [12] , [13] .

As a result of the studies, the design of the handling crane was enterily revised, as for the Bugey plant [12] , or partially improved e.g. by adding protective systems(overspeed detection devices, for instance), changing the routing of relay systems (to ensure a better physical separation), etc ... These studies revealed a "low approach" phase (height between the soil and the lower part of the load of approximatively 10 to 100 cm) for which some protective devices are useless in case of failure of the kinematic hoisting system and of inadvertent load drop. This lead to the use of damping honeycomb concrete in certain vulnerable places of structures, in particular at the bottom of the loading pits in the spent fuel pool. These damping systems can absorb the energy corresponding to the drop of the load in the low approach phase.

The studies conducted on the handling cranes and especially on the Paluel crane are original for two reasons :

1) a detailed study is performed on the kinematic handling system, including the relay system, and using FMEA and fault tree methodology ;

2) reliability data are used which have been gathered during the operating experience of approximately 200 handling cranes of the French iron and steel industry ; the manufacturing and control conditions in this industry are fairly similar to these prevailing in the nuclear industry. These conditions help explain the important gap between the failure rates of the sheaves : 5×10^{-6}/hr according to reference [14] , 6×10^{-9} /hr for steel sheaves centrifugally casted, machined and subjected to stringent controls.

Quantitative results can be considered as satisfactory :
- the probability of a handling crane failure resulting in load drop was 8×10^{-7} for 14 hours of operation by year in the power plant ;
- the probability of an overspeed of the handling crane occurring without possibility of stopping the crane is, for 14 hours of handling, 1.6×10^{-10}/year.

CONCLUSIONS

This paper was aimed at highlighting the specific characteristics of the probabilistic approach used at EDF through the 4 selected examples :

- for safety related systems, combined studies are conducted during the preliminary phase of the design to determine the overall structure of the system and, during the final phase, to analyze the system as thoroughly as possible ;

- a particular stress is laid on very detailed studies based on the FMEA , among others, which is an essential method to acquire a deep knowledge of the systems and to establish a constructive and efficient cooperation between the teams working on the projects and the reliability specialists. The search of the potential common mode failures is based on the same method. The operating experience gathered on the French 900 MWe units is taken as much as possible into account in these analyses ;

- the study durations are thus much longer : the total time spent to study the 14 safety systems of the Paluel power plant (approximatly 110 to 120 engineers/month) should thus be compared to the time estimated to perform a global risk analysis (PRA level 1) i.e 83 to 139 engineers x month [15].

These analyses will be later supplemented by the study of accident sequences. This study will be conducted in the framework of a Research and Development program considering the difficulties and certains problems it raises - such as the analysis of diagnosis errors - which have not yet found a satisfactory solution.

REFERENCES

1. B. GACHOT - M. LLORY, Probabilistic Analysis of Systems Related to P.W.R. Safety - Synthesis of E.D.F. Studies - A.N.S. Topical Meeting - Los Angeles - Newport - Beach - May 8-10, 1978

2. P. BERGERON - J. DOREY - Recueil provisoire de données de fiabilité - EDF report HP 219/79/27 - March 1979

3. R. PORTAL - A. VILLEMEUR - A Probabilistic Approach to Safety Assessment and Design Optimization of Two P.W.R. Safety Related Systems - Same reference as 1.

4. B. GACHOT - A probabilistic Approach to Design for the E.C.C.S. of a P.W.R. - Proc. 1977 Annual Reliability and Maintainability Symposium - p. 332-342

5. Reactor Safety Study - An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants - WASH-1400-NUREG 75/014 - U.S.N.R.C. - October 1975

6. M. LLORY - A. VILLEMEUR - R. PORTAL - Les défaillances de mode commum - EDF-DER Report HT-13/28/79 - September 1979

7. R. PORTAL - Projet W 1300 : Etude comparative de sûreté des schémas proposés pour la réalisation du système ASG - EDF-DER Report HT-13/2/76 - January 1976

8. J.F. BARBET - M. LLORY - A. VILLEMEUR - Application of FMEA to the nuclear power plant systems - Second International Conf. on Reliability and Maintainability - Perros-Guirec - Trégastel - September 8-12, 1980

9. M. GONDRAN - A. PAGES - Fiabilité des systèmes - Eyrolles, PARIS - 1980

10. A. PAGES - Calcul automatique de la fiabilité et de la disponibilité des systèmes réparables : le code FIABC - EDF-DER Report HI 3117/02 - May 1979

11. A. AMENDOLA - Reliability Benchmarch Exercise - Adopted Rules- Joint Research Centre - Ispra - March 1982

12. J.F. BARBET - B. GACHOT - Probabilistic Approach to Design of the Spent Fuel Cask Handling System of a Nuclear Plant - Nat. Conf. on Reliability - Univ. of Nottingham - September 21-23, 1977

13. J.F. BARBET - Méthode d'étude probabiliste de la sûreté des ponts de manutention des centrales nucléaires - EDF-DER Report HT13/44/80 - June, 25, 1980

14. Non Electronic Reliability Handbook - N.T.I.S. - RADC - TR 7522 - January 1975

15. PRA Procedures Guide-Review Draft - NUREG / CR-2300 - Vol. 1, Rev. 1 - USNRC, April 5, 1982

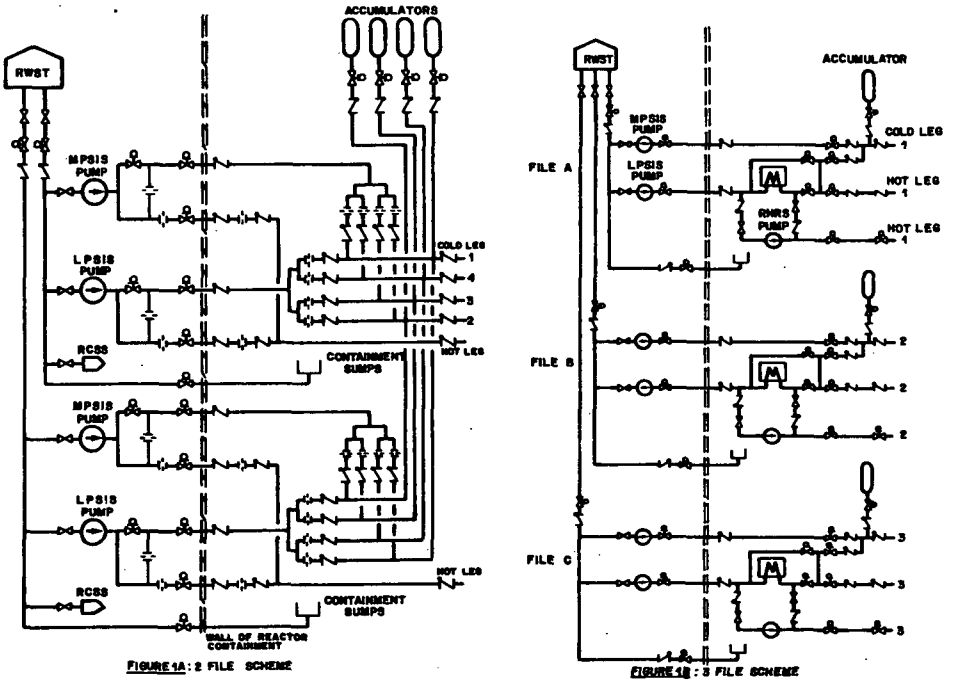


FIGURE 1A : 2 FILE SCHEME

FIGURE 1B : 3 FILE SCHEME

Fig. 1. Paluel Safety Injection System.

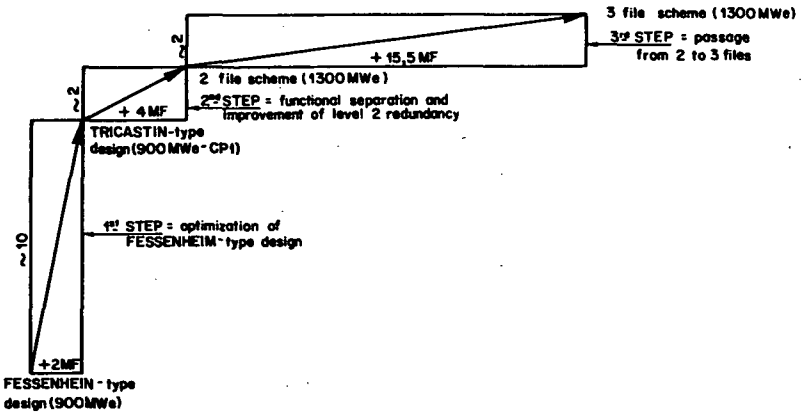


Fig. 2. Relation Between Unavailability Decrease and Cost Increase by Unit, in each Step of Improvement of SAFETY INJECTION SYSTEM.

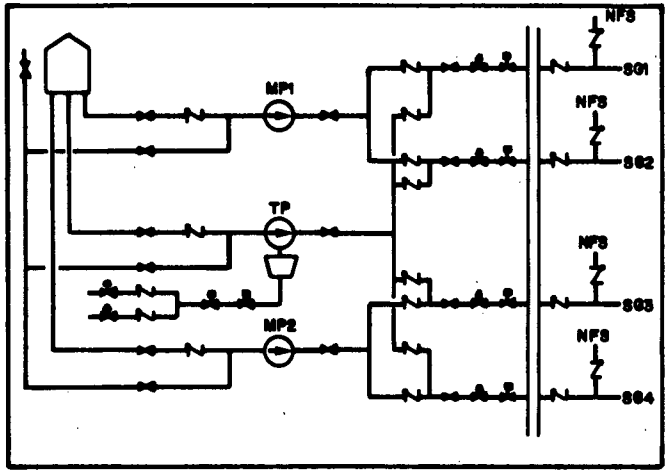


FIGURE 3-1

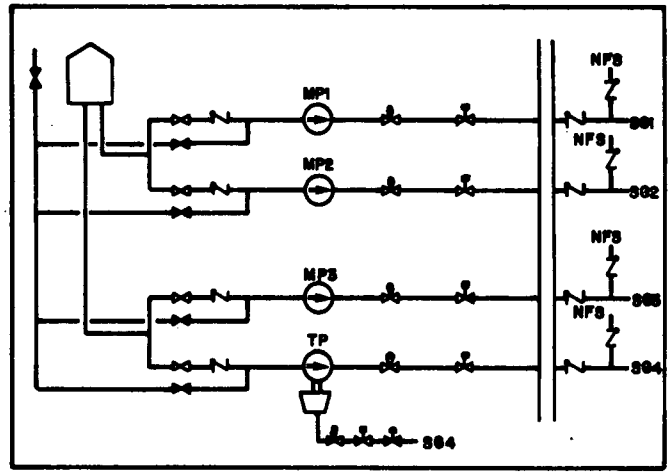


FIGURE 3-2

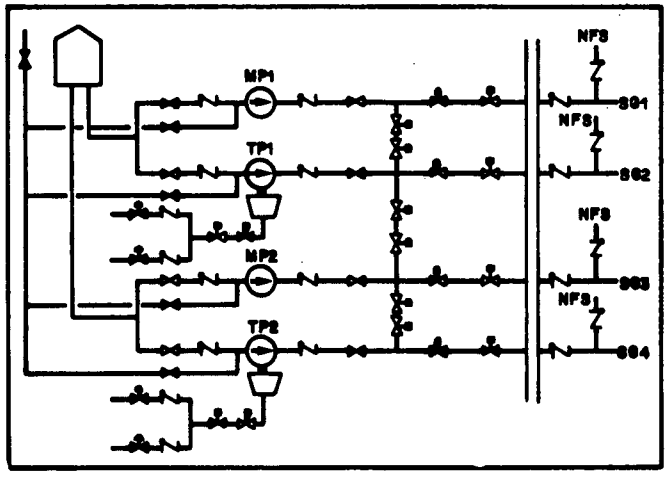


FIGURE 3-3

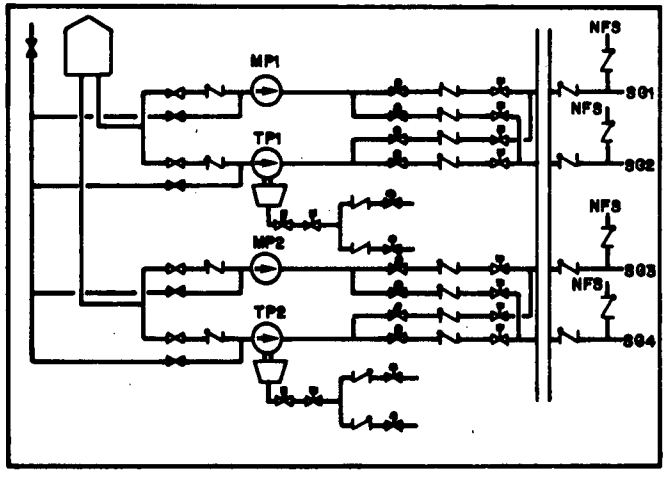


FIGURE 3-4

LEGENDE

MP: Motor-driven pump
TP: Turbine-driven pump
NFS: Normal feedwater system
SG: Steam generator

Fig. 3. The 4 Schemes Proposed for AFWS (Paluel 1300 MWe).

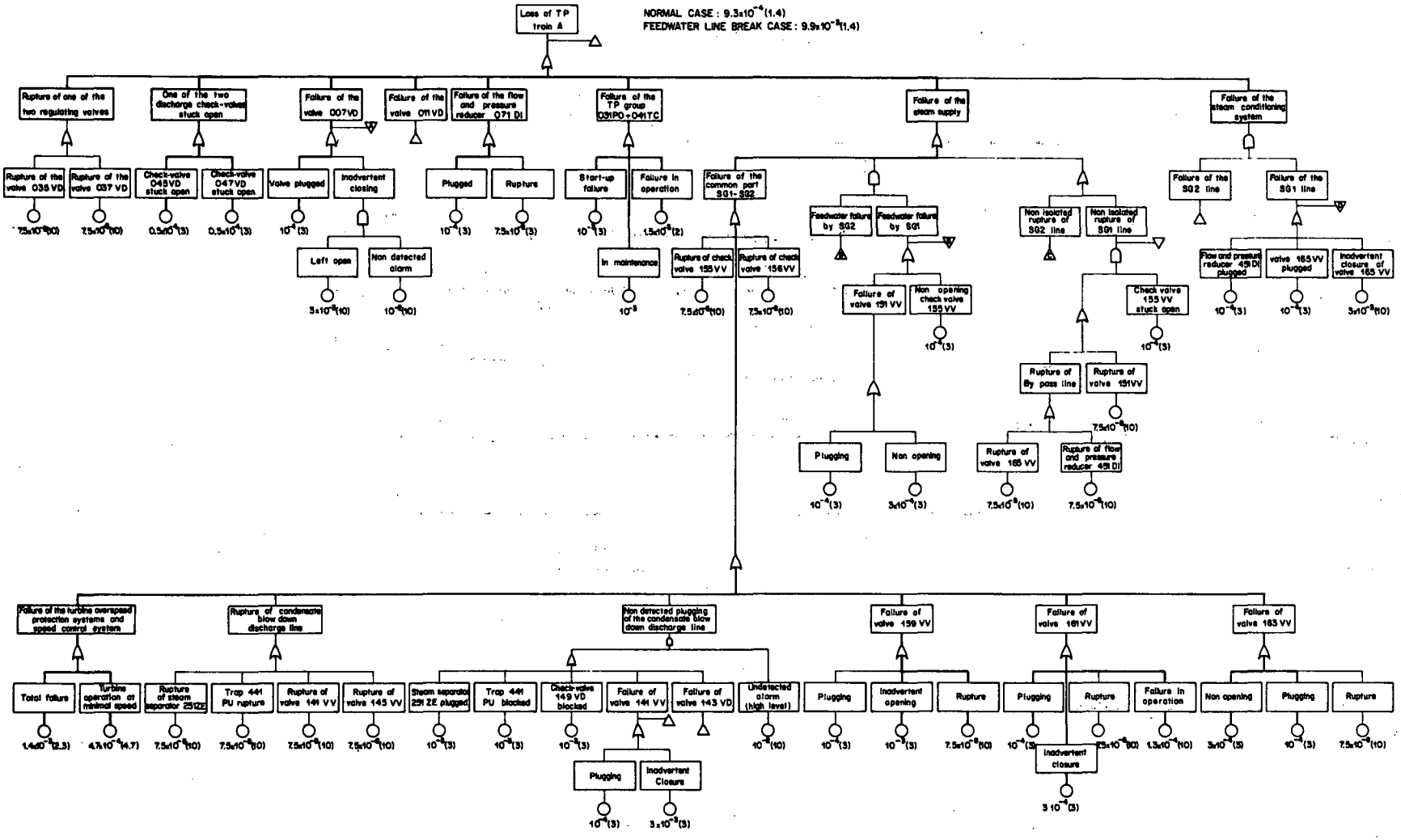


Fig. 4. Loss of Turbopump Group (Paluel AFWS-Train A).

ANALYSIS OF STATION BLACKOUT ACCIDENTS FOR LWRs

A. M. Kolaczkowski, A. C. Payne, Jr.
Sandia National Laboratories
Albuquerque, New Mexico 87185

P. W. Baranowsky
U. S. Nuclear Regulatory Commission
Washington, DC 20555

ABSTRACT

"Station Blackout," the loss of all AC power in a nuclear power plant, is a Nuclear Regulatory Commission (NRC) unresolved safety issue. This paper summarizes station blackout accident sequence analyses conducted as part of a plan to resolve this issue. The results covered include: (a) core damage probabilities for four generic classes of plants, (b) factors most affecting these probabilities, (c) containment failure insights, and (d) examples of sensitivity analyses to cover other variations of plant design.

"STATION BLACKOUT" -- AN UNRESOLVED SAFETY ISSUE

The complete loss of AC power to the essential and nonessential switchgear buses in a nuclear power plant is referred to as a "Station Blackout." Because many of the safety systems required for reactor core decay heat removal are dependent on AC power, station blackout could result in a severe core damage accident.

The issue of station blackout arose because of the historical experience regarding the reliability of AC power supplies. A number of operating plants have experienced a total loss of offsite electrical power, and more occurrences are expected in the future. Onsite emergency diesel generators have failed to start and run during tests and, in some instances, one of the redundant emergency power supplies was unavailable when a loss of offsite power occurred. This experience, coupled with results of the Reactor Safety Study [1], which showed that station blackout could result in a significant portion of the risk from all nuclear power plant accidents, raised the concern about station blackout to that of an unresolved safety issue.

PROGRAM SCOPE

This paper summarizes the results of the accident sequence analyses regarding the core damage likelihood due to station blackout for light water reactors (LWRs) as well as perspectives regarding possible containment failure. Detailed AC power reliability analyses were performed by Oak Ridge National Laboratory (ORNL) and were used as input to this work which includes an assessment of the likelihood of core damage due to a station blackout accident.

The station blackout accident sequence analyses were designed to cover a large spectrum of nuclear power plant designs and operation characteristics. These analyses included an assessment of the capability and reliability of shutdown cooling systems with a loss of AC power and an examination of the system vulnerabilities during prolonged AC loss conditions. Also included was an evaluation of the potential failure modes and time to failure for various containment types in a station blackout accident. Using this information, the relative importance of station blackout risks was determined. Station blackout induced by external events was also reviewed based on available information sources. In addition, these analyses were used to determine the sensitivity of station blackout-caused accidents to various design and procedural changes.

TECHNICAL APPROACH

The approach followed in this study involved the use of probabilistic risk analysis (PRA) techniques using event and fault tree modeling. This was initiated with an extensive review of plant design and operation characteristics. This information was obtained from past PRAs, safety analysis reports (SARs), industry responses to TMI action plan items, plant visits, plant operating procedures, and miscellaneous industry reports and letters to the NRC. Based on this review, plant designs were classified depending on decay heat removal and reactor coolant system (RCS) makeup functional capability during a loss of AC power. Pressurized water reactors (PWRs) with AC-independent decay heat removal but requiring AC power for makeup system operation were characteristic of one plant class. Boiling water reactors (BWRs) with isolation condensers were considered to be functionally different from the newer BWRs with AC-independent capability for both heat removal and reactor coolant injection. This newer BWR plant class was divided into two plant groups: those with high pressure coolant injection (HPCI) systems, and those with high pressure core spray (HPCS) systems. This was done to better analyze the effects of the HPCS train of shutdown cooling with its own dedicated division of AC, DC, and service water support systems. Thus, four plant groups were studied to obtain generic perspectives regarding station blackout accidents in LWRs.

Event trees were constructed to depict the possible station blackout accident sequences which can occur for the three plant classes. The station blackout event trees are somewhat unique in that time dependence was explicitly shown for the three characteristically different time periods of interest. These include: (1) an early time period up to about two hours in which the availability on demand of core cooling capability is important; (2) an intermediate time period of up to 12 hours in which the effects of prolonged AC power loss (e.g., depletion of DC power, room ventilation loss, ...) can affect the ability to maintain core cooling; and (3) a later time period in which there is a need to provide for long term core cooling and/or reactor coolant makeup or, in some cases, restore containment heat removal. Figure 1 displays the PWR event tree as an example to illustrate the time-dependent nature of the event tree construction. Figure 2 is the modern BWR event tree while BWRs with isolation condensers are analyzed using an event tree identical in structure to the PWR tree.

Four base case configurations corresponding to the four plant groups were defined in detail for an initial assessment of station blackout accident sequence likelihoods. In each case a two division AC/DC power configuration was included, the reliability of which was obtained from the ORNL work in this area. Reliability modeling of plant systems and features was performed using fault trees in which failure modes were grouped into power-related failures, human/operational-related failures, hardware failures, test and maintenance outages, failures caused by accident phenomena, and failures caused by dependencies on support systems. The most up-to-date design and operational information available was used to account for post-TMI changes.

The data used for quantification of the accident sequences was taken from information sources similar to that used in the review of plant design and operational characteristics as well as from NRC LER data summary reports, a review of station blackout related events reported in licensee event reports (LERs), and the results of the Accident Sequence Precursor Program [2]. These data were critically reviewed for current applicability recognizing post-TMI changes and representative values were used for the generic analyses of the four plant groups.

Containment designs were grouped into six major types based primarily on their volume and design pressure characteristics. In each case, the design's susceptibilities were investigated under station blackout conditions.

Accident sequence timing information was taken primarily from the Severe Accident Sequence Analysis (SASA) Program [3,4,5] although results were also used from PRAs, SARs, station blackout procedures, plant visits, and miscellaneous industry reports and letters to the NRC.

These models and the data were analyzed using the SETS [6] and SEP [7] computer codes to quantify the accident sequences. Uncertainty factors in the basic failure data and initiating event frequencies were propagated thru the analyses to determine the uncertainty in the accident sequence probabilities. The containment failure modes and timing were then treated separately to add a risk perspective to the overall analyses.

Lastly, external events were also reviewed using available information sources. Results of the review were used to summarize the potential core damage probabilities resulting from the loss of AC power due to external events.

RESULTS

The results of the accident sequence analyses are highlighted in Tables I and II for the four base case plant configurations and the six different containment types.

Table I summarizes the dominant accident sequence core damage probabilities and the factors which most affect these probabilities. The total core damage probability for all but one base case configuration was estimated to be in the range of 10^{-5}-10^{-4} per year. Plants with system reliability features different from the four base case designs will have different core damage probabilities.

Examples of sensitivity analyses conducted to investigate the effects of different plant design features are shown in Table III. Note that in general, no single feature by itself will significantly affect the total core damage probability.

In addition to the station blackout accident sequences initiated by system failures, current estimates [8,9,10] of the frequency of major seismic, fire, and wind events which could cause blackout related core damage are in the range of 10^{-4} to $<10^{-6}$ per year. The likelihood depends on plant features such as the plant's susceptibility to seismic activity and the effects on the switchyard and control systems, susceptibility to fire and the degree of cable separation, and susceptibility to wind or storm events and their effect on offsite power, the switchyard, and other plant equipment. In each case, though not necessarily causing a station blackout, the plant could lose the ability to supply power from the onsite electrical buses to the AC/DC loads so that plant responses occur which are similar to an actual station blackout event.

The results of the specific failure modes for each plant group are indicated in Table I. In summary, these results indicate that the important plant feature considerations include:

1. The standby reliability of decay heat removal systems following loss of AC power,

2. DC power reliability and battery capacity including the availability of instrumentation and control for decay heat removal without AC power,

3. Common service water dependencies between the emergency AC power source and the decay heat removal systems,

4. The magnitude of reactor coolant pump seal leakage and the likelihood of a stuck open relief valve during a station blackout,

5. Containment size and design pressure,

6. Operator training and available procedures,

7. External events which cause plant responses similar to an actual station blackout (but may be better analyzed independent of the station blackout issue).

CONCLUSIONS

The likelihood of core damage accidents resulting from station blackout is not only determined by the reliability of AC power supplies but also by the ability to remove decay heat and maintain reactor vessel water inventory during loss of AC power events. In particular, the reliability of support systems required for decay heat removal and the ability to maintain reactor coolant integrity significantly affect the capability and likelihood of withstanding a station blackout event.

REFERENCES

1. U. S. Nuclear Regulatory Commission, "Reactor Safety Study," WASH-1400 (October 1975).

2. J. Minarick, et al., "Precursors to Potential Severe Core Damage Accidents: 1969-1979, A Status Report," Oak Ridge National Laboratory, NUREG/CR-2497, ORNL/NSIC-182/V. 1, June 1982.

3. C. D. Fletcher, "A Revised Summary of PWR Loss of Offsite Power Calculations," EG&G Idaho, Inc., EGG-CAAD-5553, September 1981.

4. F. Haskin, et al, "Analysis of a Hypothetical Core Meltdown Accident Initiated by Loss of Offsite Power for the Zion-1 PWR," Sandia National Laboratories, NUREG/CR-1988, SAND81-0503, November 1981.

5. S. A. Hodge, et al., "Station Blackout at Browns Ferry Unit One - Accident Sequence Analysis," Oak Ridge National Laboratory, NUREG/CR-2182, ORNL/NUREG/TM-455/Vol. 1, November 1981.

6. R. B. Worrell and D. W. Stack, "A SETS User's Manual for the Fault Tree Analyst," NUREG/CR-0465, SAND77-2051, November 1978.

7. M. D. Olman, "Quantitative Fault Tree Analysis Using the SET Evaluation Program," DRAFT (to be published).

8. "Zion Probabilistic Safety Study," Commonwealth Edison Co., Fall 1981.

9. "Big Rock Point Plant PRA," Consumers Power Co., March 1981.

10. "Indian Point Probabilistic Safety Study," Power Authority of the State of New York & Consolidated Edison Co. of New York, Inc., Spring 1982.

Figure 1. GENERIC PWR EVENT TREE FOR STATION BLACKOUT

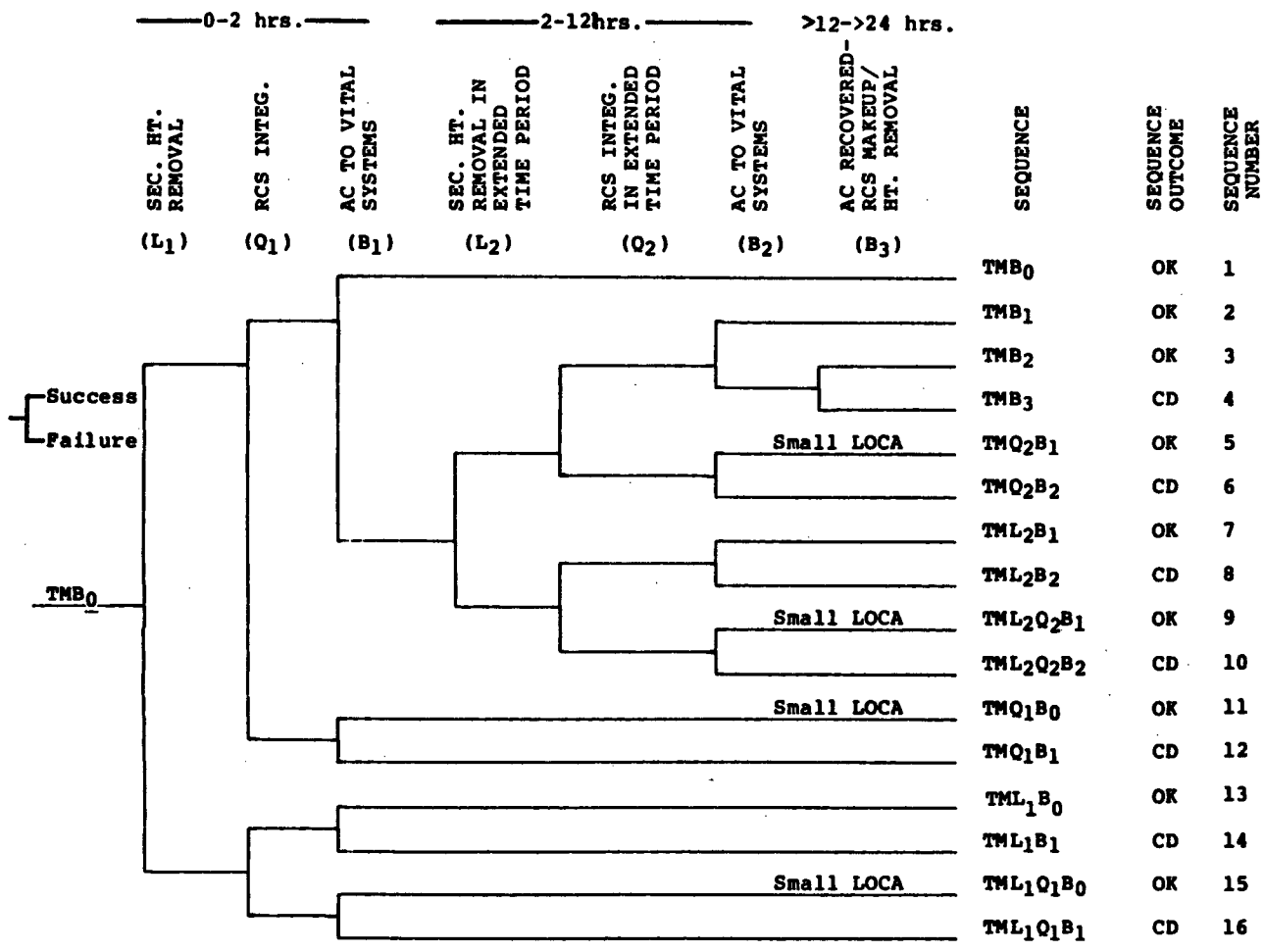


Figure 2. GENERIC BWR EVENT TREE FOR STATION BLACKOUT (BWR3 - BWR6)

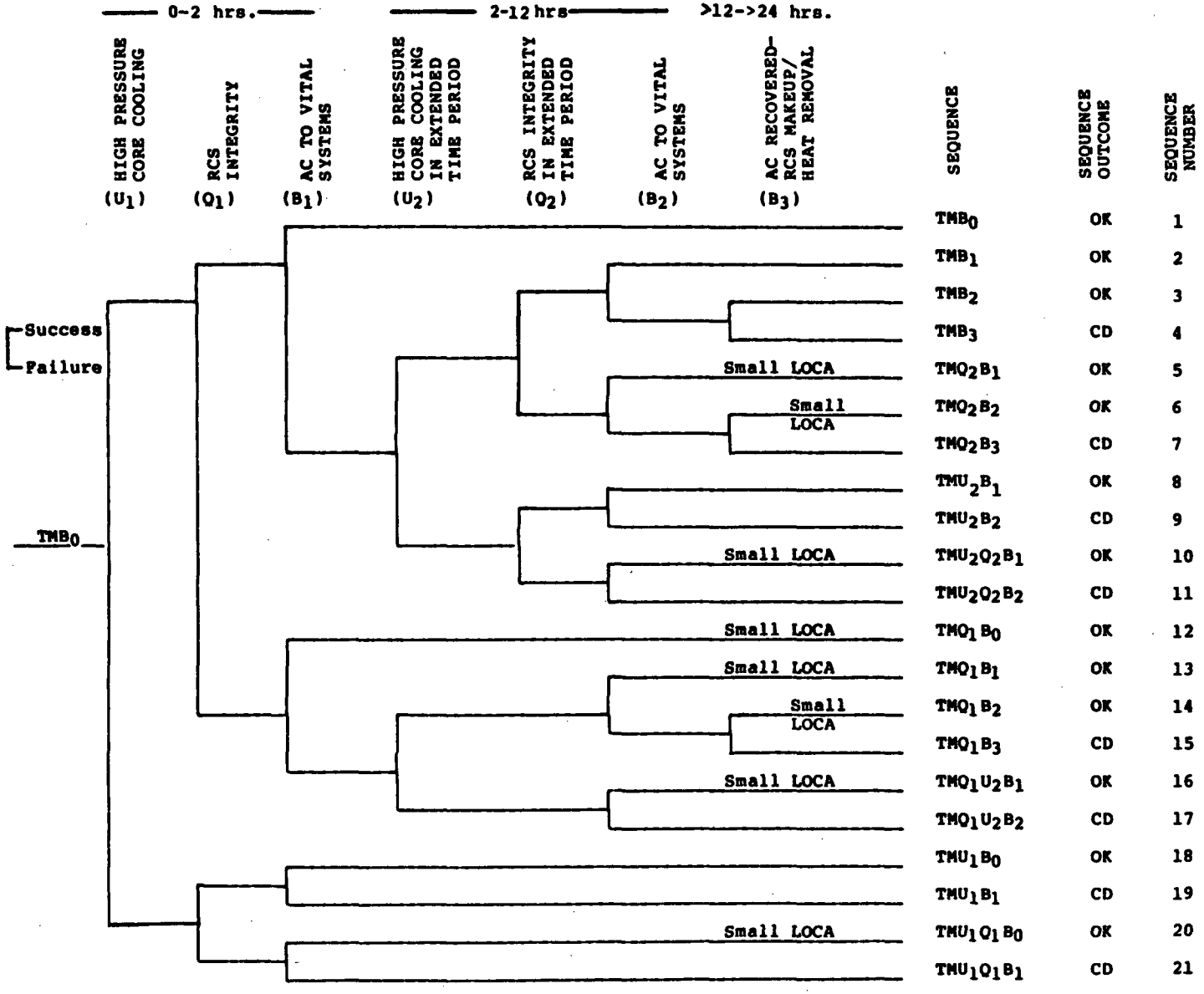


TABLE I. GENERIC PLANT CLASS DOMINANT CORE DAMAGE ACCIDENT SEQUENCES

Generic Plant Class***	Sequence	Approx. Sequence Probability*	Major Factors Affecting Sequence Probability
PWR w/1 Steam Train AFWS, 2 AC/DC Divisions	TML_1B_1, $TML_1Q_1B_1$	Low 10^{-5}	AFWS Steam Train Unavailability, AC Recovery, Possible AC Dependency for RCS Isolation
	TML_2B_2	Mid 10^{-5}	AFWS-DC Interaction, AC Recovery, AFWS Continued Water Supply Availability
	TMQ_2B_2	Low-Mid 10^{-5}	Large RCS Pump Seal Failure, AC Recovery, Common Service Water Dependencies in AC/Makeup Systems
BWR w/Isolation Condenser(s), 2 AC/DC Divisions**	TMU_1B_1	Low 10^{-5}	Isolation Condenser(s) Unavailability, AC Recovery
	TMQ_1B_1	Low 10^{-5}	Stuck-Open Relief Valve, AC Recovery
	TMQ_2B_2	Mid 10^{-5}	Large RCS Pump Seal Failure, AC Recovery, Common Service Water Dependencies in AC/Makeup Systems
BWR w/HPCI-RCIC, 2 AC/DC Divisions	TMU_1B_1	Mid 10^{-6}	HPCI/RCIC Unavailability, AC Recovery
	TMU_2B_2	Hi 10^{-5}	HPCI/RCIC-DC/Ventilation Interactions, AC Recovery, Common Service Water Dependencies in AC/Makeup/Ventilation Systems
BWR w/HPCS-RCIC, 2 AC/DC Divisions, and a Dedicated 3rd Division for HPCS	TMU_1B_1	Low-Mid 10^{-6}	HPCS/RCIC Unavailability, AC Recovery
	TMU_2B_2	Mid 10^{-6}	HPCS Unavailability, RCIC-DC/Ventilation Interactions, AC Recovery

* "Mean" value (per reactor year) for sequence.

** Sequences are denoted by replacing "L" with "U" on the PWR event tree to account for the use of the isolation condenser instead of the auxiliary feedwater system.

*** Initial station blackout probability for a typical two division system is Low-Mid 10^{-4}

TABLE II. CONTAINMENT FAILURE INSIGHTS

Containment Type	Approximate Time to Containment Failure Following Onset of Core Damage	Most Probable Containment Failure Modes
Ice Condenser	1 hr.	Hydrogen burn, steam spike, or overpressure
	At or following AC recovery	Hydrogen burn
Subatmospheric or Small Dry	2 hr.	Hydrogen burn, steam spike or overpressure
	Following AC recovery	Hydrogen burn
Large Dry	10 hr.	Overpressure
	Following AC recovery	Hydrogen burn
Mark I, Mark II	2-4 hr.	Electrical penetration failure
	4-8 hr.	Overpressure
Mark III	10-15 hr.	Overpressure
	1 hr. to following AC recovery	Hydrogen burn

Table III. Examples of Sensitivity of Core Damage Probability to Design Variation from Base Case Analyses.

Sensitivity	Dominant Sequences Affected	--------Mean Estimate Effects-------- "Base" Case Value In Study	New Value Applying Sensitivity
PWR: Base Case - 1 Steam Train AFWS	TML_1B_1	Low 10^{-5}	Low 10^{-6}
Sensitivity - 2 Steam Train AFWS	*ΣCD	Low 10^{-4}	Low 10^{-4}
BWR w/Isolation Condenser:			
Base Case - no AC-independent RCS Makeup	(All)		
Sensitivity - Additional Fire Pump (or equivalent) for RCS Makeup	ΣCD	Low 10^{-4}	Low 10^{-5}
BWR w/HPCI-RCIC:			
Base Case - 5-8 hr. Ventilation/ DC failures	TMU_2B_2	Hi 10^{-5}	Mid 10^{-5}
Sensitivity - Extend Failures Due to Ventilation/DC to 12 hrs.	ΣCD	Hi 10^{-5}	Mid 10^{-5}
All plants:			
Base Case - 2 Div. AC/DC Configuration			
Sensitivity - Possible Reductions in AC Reliability	(All) ΣCD	10^{-4} - 10^{-5}	10^{-3} - 10^{-4}
Sensitivity - Improved Reliability Due to Higher Level of Redundancy	(All) ΣCD	10^{-4} - 10^{-5}	10^{-6} - 10^{-7}

*ΣCD = Total Core Damage Probability.

USE OF RISK CONCEPT IN SAFETY EVALUATION, LICENSING AND DECISION MAKING.

PRACTICE AND TRENDS IN THE EUROPEAN COMMUNITY

W. Vinck and G. Van Reijen

Commission of the European Communities
Wetstraat 200 - 1049 BRUSSELS

ABSTRACT

Some general aspects of the use of risk concept in Safety analysis are given. It has been shown that quantification of risk is playing an increasing role. An overview of the situation in EC countries is given. In particular convergencies and divergencies are indicated.

More attention has been paid to specific aspects of the use of risk concept and probabilistic risk assessment in licensing, design and safety assement. The development and the use of specific safety objectives seems to be more advanced than that of overall safety objectives.

A number of specific topics are discussed in this paper. Overall conclusions are given.

INTRODUCTION

In the frame of the CEC harmonization efforts relating to the safety of light water reactor NPPs, which are the subject of the paper [1] of this International Meeting, in the year 1980 a survey on the use of risk concept in safety analysis has been established. At an earlier occasion Mr. VINCK presented a paper [2] which commenced with a presentation of this survey and which concluded with a number of the author's personal views and opinions on the need for and the limitations of quantified safety objectives.

This paper gives those important points of the survey mentioned above, which are relevant for a follow-up CEC action of the "problematics" of the use of safety goals/objectives, the first results of that action being the main subject of this paper. This paper expresses also personal views and opinions of the authors, which do not necessarily correspond with those of the national delegates to some of the EC Standing working groups and those of the CEC.

THE USE OF RISK CONCEPT IN SAFETY ANALYSIS

The CEC survey on the use of risk concept in safety analysis is divided in general findings and in specific topics. This distinction will be found back in the discussion of the safety goals problematics further on in this paper.

The general findings are resulting from an assessment of the safety of a given activity and can be considered supporting items for the decision about that activity

or about its implementation. Such analyses are normally defined as risk studies. Analyses can also be performed on a specific level with the purpose of an assessment of the safety in a particular case of an implementation of an activity (e.g. transportation system, industrial plant and/or its systems and components) in both the design and regulatory phases.

General findings of risk studies are usually expressed as the synthesis of two items : the negative consequences of possible events and the likelyhood of their occurence. The consequences are often given in terms of individual dose equivalent at the boundary of the site or in terms of quantities of radioactivity released. It is not easy to assign a suitable weighting factor to any consequence. Risk can also be properly represented through a graph or an equivalent form (e.g. histogram or table), where the consequences of different size and their respective probability appear. Among the purposes of such studies are the assessment of risk from nuclear power plant and its comparison with risk from natural and from other man made sources. Other results are the discovery of possible weak points in the plants and the verification of the conservatism and consistency of different deterministic criteria. Furthermore risk studies can aid in a more systematic definition of safety requirements.

In the specific level of performance of risk analysis the purpose is to assess the safety in particular cases of an implementation of an activity in both the design and the regulatory phases and also to assess specific issues of the overall safety analysis.

Examples and practices for such specific issues are :

Analysis of the initiating events to be taken into account for the design

In a few countries the probabilistic approach is used for the consideration of initiating events of both internal and external origin. More often, the probabilistic point of view is used for external events and a more deterministic point of view for internal events. As an example it can be mentioned that when the probabilistic point of view is adopted, the limit annual probability for each type family of initiating events which could result in major consequences is frequently assumed to be roughly around 10^{-6} - 10^{-7}. Initiating events with probabilities less than that value normally have no implication for the design although some consequence analysis could be requested. On the other hand this practice is not always shared, mainly because several external event types (e.g. aircraftcrash, explosions hazard) are grouped together.

Combination of events

Generally no combination of independent events occurring simultaneously is considered when the annual probability of such a combination is sufficiently low (around 10^{-7}). Within the licensing procedure of all countries only the combination of the initiating event with an additional single failure in a safety system is considered.

Reliability criteria for safety related systems

Fixed reliability values do not yet exist for licensing. Nevertheless reliability analysis are performed for these systems in all countries e.g. for comparison of the results with reliability values of existing plants or with other assessments e.g. WASH-1400.

An example of reliability criteria for reactor protection systems [3] reads as follows :

System reliabilities are conservatively determined by :

- For any single fault, the product of the initiating fault frequency and the probability of protection system failure should be less than 10^{-7} per reactor year.
- For all faults, the sum of the product of each initiating fault frequency and corresponding probability of protection system failure should be less than 10^{-6} per reactor year.

Single failure criterion

The purpose of application of single failure criterion is to ensure a minimum degree of reliability even though in qualitative terms, particularly when there is insufficient data to perform a reliability analysis.

Common cause of failure and human factors

The whole problem area of common mode failure is normally covered by means of diversity, physical and spacial separation of redundant systems and for human failure in operation also by automation of system initiation. This is usually done in a completely deterministic way. In certain cases the reliability claimed for a single system must be limited to a fixed value in view of possible hidden common mode failure.

Operational requirements

Specific safety analysis can be an aid in maintenance and test planning. Here optimization is an important item.

Data base for risk analysis

There are a number of sources of data : literature, operational experience, data banks, statistics, experimental date. A European Reliability Data System (ERDS) is now developed by the CEC Joint Research Center in Ispra [4].

Uncertainties

Generally risk assessments and probability analyses start by using the best estimate values, without considering its uncertainty. Sometimes the uncertainties of input data (physical values, calculation, etc.) which have a large effect on the result of the assessment are evaluated with a sensitivity analysis.

The considerations taken from the CEC Survey on the use of risk concept in Safety analysis and mentioned above are of importance for the follow-up action on the problematics of the use of safety goals started early 1982 as already indicated in the introduction and discussed below.

SAFETY OBJECTIVES FOR NUCLEAR POWER PLANTS

For this problem a CEC sponsored Task Force has been called together. Up to now this Task Force held two meetings during which a survey of the approaches in different EC Member States has been elaborated and discussed.

After some general observations and the presentation of the mandate ot this Task Force this survey of approaches is given and types of possible target values and safety-objectives are indicated.

1. General observations

A corollary of the discussion in the preceding section, where the possibilities for an introduction of the probabilistic/risk approach in the essentially deterministic licensing and regulatory requirements has been explained, is the question if it is possible and opportune to set quantified safety objectives. To put this question in perspective it is useful to mention two apparently opposing but in practice complementary approaches in this regard :

1° The approach to apply fully the principle saying no risk - however small - is acceptable if it can be reasonably reduced (cfr. the ALARA-concept in radiation protection). A basic question is within potential accidents having a frequency (probability of occurrence) between 10^{-5} to 10^{-7} per installation-year but with severe consequences (corresponding nevertheless to a very small individual risk of the order of 10^{-9} per installation-year) can be reasonably reduced on the basis of a cost-benefit (risk reduction) analysis.
Another unsolved question is to what extent supplementary engineered safety features to cope with such situations render the installations increasingly

complex and perhaps in the end less safe.

2° The approach to say that it is necessary to develop quantitative safety goals (how safe is safe enough) in which the nuclear activities would be put into the perspective of other public risks (e.g. other energy sources and major hazards industries) and in which the cost-benefit (risk reduction) aspects of supplementary protection and accident consequence mitigating devices would be considered.

It is likely that in conjunction with the setting of a reasonable safety goal in regard to the nuclear potential hazard (2nd approach) one will receive guidance for the answer to the basic question of tendency 1° : down to what point is it still reasonable to reduce the (residual) risk.

Important developments, as regards the second approach, are now underway in the United States. It should be mentioned that in the US NRC discussion paper on the subject distinction is made between "qualitative safety goals" and "numeric guidelines". This distinction is however artificial : an analysis of the two qualitative safety goals given in 5 reveals that in reality they are quantitative.

It may be observed that there is a tendency in the United States, but also in European countries, to combine aspects of the "safety goals" approach with the ALARA-approach. Summarized indications on the development in European countries are given below.

2. CEC Task Force on Safety Goals/Objectives

The mandate of this Task Force comprises the following issues :

- Discussion on a technical basis of the need, possibilities and limitations for/of overall and specific safety objectives, taking stock of various approaches (e.g. risk comparisons, risk-cost benefit balancing, cost-effectiveness of risk reduction, extrapolation of acceptability of radiation limits to technological/engineering aspects) in development in EC-member states and abroad.
- Examination of the merits and implications of the various (or selected) approaches and determination of the degree of coherence and the divergencies in their possible applications.

The main reason for this action is the growing need to equivalence in general safety objectives throughout the world - and within EC member countries in particular - for potentially hazardous activities of which nuclear power production is an example.

3. Survey of approaches regarding the use of safety objectives

As a starting point for further discussion a brief survey is given of the approaches in use or in development in some European countries :

- The current UK methodology embodies an evolution from the earlier "credible/incredible" approach to one combined with a comprehensive Probabilistic Risk Assessment. For the former, certain events may be accepted as being so low in risk of occurence that general further provisions or particular distortions of the design to deal with them are not justified. For the latter, numerical targets are set and reliability values are specified which relate to the performance of the kinds and numbers of components in the systems used in safety functions.
  While probabilistic risk assessment is not to be employed as the sole basis for safety assessment, it is seen to have particular value in ensuring that a systematic approach is followed and that a balanced design is achieved in terms of safety performance of the plant.
  Particular guidance in this matter is given in the NII "Safety Assessment Principles" [6]. In that document emergency reference levels ERL are defined and frequency levels for ERL's are indicated.
- In Italy generally the codes and standards of the country of origin of the plants (USA) are used. In the course of licensing of CAORSO in certain limited areas, PRA's

have been used in order to make comparison for different design solutions. For the licensing of the two new PWR plants CNEN requires a more complete PRA. Quantitive safety objectives for the maximum equivalent individual dose to the public have been formulated now. However, a standard method of implementation of these objectives is not yet defined.

- In France the use of probabilistic methods is only at the first of three stages mentioned in a paper [7] presented at the IAEA Stockholm Conference : "use as an aid to safety evaluations"; the 2nd stage "introduction of probabilistic criteria in safety rules" and the 3rd stage "realisation of a coherent system of risk acceptance criteria" have to follow.
  In France, however, two examples of very global safety objectives can be mentioned : the first one is that the overall probability of inadmissible consequences should not exceed 10^{-6} per year. This figure is an order of magnitude. The second example is that three categories of releases are defined, two of them for the so-called conceivable accidents, one for accidents at the limit of what is conceivable.
- In Germany up to now the deterministic approach is used for licensing.
  Reliability studies are used for the evaluation of the consequences of reduced redundancy of certain systems.
  The German Risk Study led to certain amelioration of systems and procedures and to some backfitting requirements for existing plants (Biblis B and plants of comparable design). Nevertheless, there seems to exist a tendency of a careful, flexible use of target figures and safety goals; a systematic examination on this is underway in Germany.
- In Belgium PRA's are not required, but nevertheless some accident probability calculations are included in safety reports, in particular for certain external impacts like aircraft crash. Actual discussions mention apart of the advantages of relatively precise risk figures, also the disadvantage of their possible misuse by anti-nuclear people. The development in the USA is followed with interest.
- In Denmark the deterministic approach is used, but comparative studies between nuclear and non-nuclear risk have been performed.
- In the Netherlands a safety objective has been developed for the choice of sites. PRA is now used in a number of nuclear and non-nuclear applications. This approach could have repercussions on the development of safety objectives in the nuclear field.
- In Sweden no legal dispositions on safety objectives exists. Several PRA's have been undertaken and are underway. They are used as an aid to diagnosis of design, construction and operation. A safety objective of 10^{-6} - 10^{-7} per year as a limit value for the probability of severe accidents is used as an a priori value for the construction of installations, but this figure is not used for licensing.

It is clear from this survey that safety objectives and their use are in the early development. There is a development in EC-countries where a certain similarity in approach seems to exist : most of these countries developed tables presenting frequency figures and corresponding dose values of limits for members of the public for various categories of levels of incident severity.

Examples of such tables developed by NII, CEGB, and ENEA corresponding with the information given in [3] and [6] are given in the table I.

TABLE I

Examples of frequency values and corresponding dose values

1. NII Safety Assessment Principles

For discrete fault sequences, Frequency per year	Assessment references levels (to Member of public)
$< 3.3 \times 10^{-2}$	16.6 m rem
$3.3 \times 10^{-2} - 3.3 \times 10^{-4}$	500 m rem
$< 3.3 \times 10^{-4}$	10 rem
"remote"	> 10 rem

2. CEGB Design Safety Criteria - Permissible Frequency of Accident Releases

Total/permissible frequency per reactor year	Accidental Releases Whole Body Dose Equivalent
10^{-2}	0.01 - 0.1 rem
10^{-3}	0.1 - 1 rem
10^{-4}	1 - 10 rem

3. ENEA, Italy
Proposed safety criteria for future nuclear power plants

Frequency per year	Equivalent Whole Body Dose limit
10^{-1} (normal operation)	< 5 mrem/year
$1 - 5.10^{-2}$	< 5 mrem/event
$5.10^{-2} - 10^{-3}$	< 500 mrem/event
10^{-3}	< 10 rem/event

It can be concluded that the figures given in such tables for different countries are similar, but it should be pointed out that the status for application of these tables differ from country to country and there may be difference in classifying events in various categories and in calculating the radiation doses.

4. Types of target values and safety-objectives

Numerous approaches to the use and further development of target values and safety objectives exist [8].
One way of categorizing them is as follows :

1° Reliability figures for safety systems in connection with frequency values of specific accident-conditions (e.g. core melt);

2° Release (or dose) limits in connection with probabilistic (frequency) values of accident conditions;

3° Individual risk values;

4° Societal risk values;

5° Comparative risk values.

Combinations of these types can be applied whilst it can be noted that the US NRC safety goals document [5] proposes a discussion of a combination of categories 3°, 4° and 5° (in conjunction with the application of ALARA), the european approaches sofar generally consider and/or discuss categories 1°, 2° and 3°.

PROVISIONAL COMMENTS MADE WITH REGARD TO NUREG-880 "SAFETY GOALS FOR NPP'S", A DISCUSSION PAPER

The following provides a synthetic survey of critical comments formulated by the CEC Task Force on "Safety Objectives".

1. General comments

a) The proposal does not clearly spell out what its scope and purpose is, e.g. guidelines for USNRC Safety-assessment purposes, proposal for public acceptability of NPP's ?

b) Especially if intended for public acceptance purpose (and also since it is publicly released anyway) the proposal should also clearly indicate the numerous preventive and mitigating measures taken to keep radioactivity releases to a minimum. At present it gives to the public the impression that basically severe accidents are to occur in NPP's and to have severe environmental consequences.

2. Specific comments

a) Goal n° 2 (Societal Risk) and associated numerical guidelines assumes applications of a 1 mile cut-off for calculation of prompt fatalities and 50 mile cut-off for delayed fatalities.
These arbitrary cut-offs may not represent the true situation for different site-conditions.

b) Basically the goals consider only the mortality risk. Especially for societal risk, other effects are to be considered such as : non-fatal health effects (i.e. morbidity), social and economic (e.g. land recovery costs) effects of contamination and emergency measures (e.g. evacuation), loss-of-plant.

The impact of psychological effects of detrimental effects plays a role in the acceptance of nuclear power, which is to be taken into consideration if the proposed goals have a wider scope than assessment purposes.
This is related to the inclusion (or not) of "risk aversion" effect for large consequence accidents, which remains a controversial issue.

c) The societal risk goal warrants special attention, especially in densily populated area's (e.g. especially european countries).

d) The risk of normal operation (which may be greater than the residual risk from low frequency high consequence accidents) should be considered in an overall approach.

5. The plant-performance guideline concerning core-melt is subject to various criticism :

   1° It is not clear what the definition of a core-melt really is in this context : gross core degradation ?, time-dependance ?

   2° PRA-methods, which are meant to demonstrate that such a guideline be met, are still subject and will remain subject to significant uncertainties (several of which are acknowledged within NUREG-0880 itself, i.e. accident initiations which are difficult to quantify such as seismic events, sabotage, multiple human error, design error).

   3° Core-degradation physical phenomena are still subject to extensive R & D; meanwhile this is also subject to uncertainties.

   4° It should not be regarded as a self-standing goal but seen in combination with the others, since one should take into consideration the engineered safeguards to protect against and mitigate severe accident conditions and emergency measures that take account of the evolution of the accident (e.g. confinement and/or evacuation measures).

6. It is not quite clear whether the first numerical guideline (prompt fatality risk) includes emergency measures such as confinement of evacuation of the public or is just based on a consequence model analysis not including those effects (N.B. in WASH-1400 and the German risk study such effects are included).

7. The choice of the 0,1 % (individual risk) value is arbitrary and may unduly penalize nuclear power versus other risks; again if considered as a self-standing goal.

   It should also not be considered as an absolute figure but as an order of magnitude (e.g. because of the uncertainties in the methodology to demonstrate it).

8. Individual and societal mortality-risk guidelines are applied (in the USNRC-proposal) on a per-site basis. This will mean more stringent requirements for multi-unit sites where, in the existance of an older plant a new plant is to be installed (or else the older plant to be backfitted or decommissioned).

9. Goal n° 2 (societal risk) alludes to comparison with generating energy from other sources. If this is done it should include the whole cycle (with all the complexities of making valid comparisons of this kind) and not just the electricity producing plants. This does not appear clearly in the proposal.

10. The inclusion of cost-benefit considerations is basically appropriate (N.B. Although legally for instance in F.R. Germany this is not possible; in actual practice it is however); however the $ 1000 per man-rem averted (reflecting what has been applied in the past) is not well founded and may be too penalizing in the future (N.B. it is one order of magnitude greater than the average value associated with other activities in the USA).

DIFFICULTIES AND LIMITATIONS, PERSONAL OBSERVATIONS

1. Verification problem

In principle it is possible to develop, establish and prescribe safety goals, however, verification is subject to considerable uncertainty : for instance, verification of an accident frequency limit of 10^{-4}/year, becomes almost meaningless if that frequency can be calculated only with an uncertainty of a factor 10 in both directions resulting in a range between 10^{-3} - 10^{-5}. Moreover, also the consequences of the incident can be evaluated only with an uncertainty of a factor 10 in both directions. The same difficulty arises for a benefit-cost guideline for risk reduction.
Here a basis of $ 1000 per man rem is mentioned, but it is hardly possible to verify such a value. The main problems of verification find their origin in the difficulty to quantify human behaviour and to identify common mode failures.

2. Human performance data in nuclear power plant operation, test, maintenance and calibration tasks

Generally there is a strong imbalance between the recognized importance of human failure and of human behaviour and the efforts to take these in consideration. The main reason seems to be that such efforts are not likely to score a success in a reasonably short delay, for quantitative evaluation of human failure probability is difficult. Just the unique capabilities contributed by human operators, such as a large adaptation of his actions to plant dynamics, disturbance characteristics, system failures, etc. are the cause of this difficulty. On the other hand in test, maintenance and calibration routines human flexibility is important, but equally leads to inaccuracy of error estimates.
Where hardware components generally have a limited set of states, human behaviour is complex and in particular the interaction between consequent tasks performed or not performed by one or more operators make it difficult to elaborate reliable model.
Nevertheless, together with methods for improving human performance also quantitative assessment in this field has to continue.

3. Common mode failure

As is stated in the RSS (Reactor Safety Study WASH-1400) the heart of successful risk assessment and a principal factor in the adequacy of the event tree/fault tree methodology is the proper identification of potential common mode failures.
Nevertheless there is no totally acceptable method for dealing with common mode failures caused for example by cascading effects or outside influences, of by component weaknesses.
The question is, that these failures are due to the fact that some possible events or combinations of circumstances have been overlooked in design, operation, inspection, etc. If they are overlooked in the mentioned activities, the chance that they all will be detected by reliability experts, less informed on the particular situation of a plant, is not large. The activity of tracing common mode failure is very useful for industrial safety. The resulting figures should be taken with scepticism.

4. Implementation of safety goals

It is certainly too early to consider the introduction of such safety goals into legislation. Apart from the difficulty of verification (see section 1), in a number of countries such an introduction cannot be seriously considered for this would require also detailed establishment of calculation methods within a legally framed network and it is feared that legally established safety goals could be detrimental for improval endeavour.
Also a more global introduction of quantitative safety goals is difficult. The problem rising in the fixing of such goals is that it is difficult to agree on the basis for such goals e.g. should they be based on :

- comparison with other risks (traffic, other industries);
- cost vs effectiveness of risk reduction;
- cost-benefit considerations;
- safety as a fundamental right for all citizens ?

But meanwhile there is certainly merit - if not a need - in looking at them as an aid for coherent guidelines in decision making.

CONCLUSIONS

Considerable efforts are underway in view of developing valid quantified safety objectives.

This task is very difficult for various reasons amongst which this : the "measuring stick", i.e. quantified risk analysis (PRA), is still subject to large uncertainties.

On the other hand there is the problem : ho to convince decision makers, that this approach and in particular the quantitative outcome of risk assessments is trustworthy.

However - and here lies its importance and at the same time its main difficulty - this approach opens an innovative way in relationships in a technologically developing society and the risks which can be considered acceptable for the individuals composing this society.

It would be unreasonable that an activity of this nature would develop in the various nations incoherently, although - because of the inherent difficulties of this task - it is not expected that on a short-term basis regulatory requirements will be significantly influenced by a concerted approach in this matter.

A global common approach towards health and safety problems, by correllating in a systematic and formal way

- safety objectives : e.g. agree on a coherent set of release (or dose) limits in connection with frequency values of accident severity-categories;
- rated (categorized) site conditions;
- ranked site related (protection) design bases;

would serve the purpose of acceptance of nuclear power.

A difficult variable remains however the influence of the human factor in plant management and operation and this subject merits therefore much care and attention in systematic approaches of this kind.

REFERENCES

1. W. ESSLER, W. VINCK - "Efforts of harmonization by the CEC relating to the safety of light water reactor NPP's" - International meeting on Thermal Nuclear Reactor Safety, Chicago, August 29/September 2, 1982.

2. W. VINCK - "Quantified reliability and risk assessment methodology in safety evaluation and licensing : survey of practice and trends in EC countries; partial contribution in decision making, perspective of safety goals". - International ANS/ENS Topical Meeting on Probabilistic Risk Assessment, Port-Chester NY, September 20/24, 1982.

3. Design Safety Criteria for CEGB Nuclear Power Stations, Central Electricity Generating Board, Health and Safety Department, March 1982.

4. G. MANCINI et al - The European Reliability Data System - ERDS : A state of the art and future developments. International ANS/ENS Topical Meeting on Probabilistic Risk Assessment, Port-Chester NY, September 20/24, 1981.

5. Safety goals for nuclear power plants : a discussion paper, NUREG-0880, USNRC Office of Policy Evaluation.

6. Safety Assessment Principles for Nuclear Power Reactors, UK Health and Safety Executive, Nuclear Installations Inspectorate, September 1978.

7. M.C. DUPUIS, VILLEROUX, LEBOULEUX, OURI - "Introduction progressive du concept de risque dans la règlementation technique et la normalisation française en matière de sûreté nucléaire - IAEA Conference on current NPP safety issues, Stockholm, October, 20/24, 1980.

8. W. VINCK - "The definition of risk and its correllations with other value for consistant decision making" - Conference "Risk in human activities", Florence, January 14/15, 1981.

SESSION 9

MAN/MACHINE INTERFACE - 1; HUMAN FACTORS

Chair: Z. Sabri *(LPL)*
A. Vuorinen *(IAEA)*

HUMAN RELIABILITY AND THE MAN/MACHINE INTERFACE: WHAT DO WE DO AFTER THE CONTROL ROOM REVIEW?

J. D. Folley, Jr., and D. L. Schurman

Applied Science Associates, Inc.
Valencia, Pennsylvania 16059, U.S.A.

ABSTRACT

The nuclear industry has focused on only one aspect of the man/machine interface--human factors engineering of control rooms--to enhance nuclear power plant (NPP) safety. There are other factors that profoundly affect the reliability of the operators and maintenance personnel of NPP which, thus, affect NPP safety and availability. This paper discusses the factors of training, selection, job engineering, and work satisfaction, describing the potential effects on reactor safety of these factors at the man/machine interface. The impact of these factors on safety and plant availability is illustrated with examples of results obtained in other fields.

INTRODUCTION

In the aftermath and fall-out of the Three Mile Island incident, an increased emphasis on human factors in the nuclear power plants (NPPs) has been observed. This emphasis is primarily observable in the promulgation of guidelines, regulations, and prescriptions regarding the design of the man/machine interface in control room (Control Room Design Reviews; NUREG-0700 and related documents), training, training simulators and organizational structures. Unfortunately, the plans for control room design reviews seem to be the only requirements and prescriptions that are firmly based on research. Prescriptions regarding training, training simulators, and organizational structure seem to have less foundation in job analysis or requirements analyses. Thus, these areas require more human factors engineering input than do control room design reviews, at this point.

Even if these various areas of emphasis were based on research, they address only part of the problem of reducing the probability of nuclear accidents by reducing the probability of human error. The problem of reducing the probability of human error is simply a part of the larger problem--improving human performance.

The primary man/machine interface, as discussed in the nuclear industry, is considered to be the interface of "The man at the controls." This view places us into the realm of panel layout, labeling, and design of controls and displays.

For example, the purpose of the control room design review is to identify specific instances in which the controls, displays, and layouts of the control room violate human-factors design principles. The intent is to modify the control room to reduce the probability of operator error (in those instances where it is believed that the benefits outweigh the costs of modification). Preliminary studies indicate that the design of layouts of control rooms indeed could have benefited from human factors engineering.[1,2,3] NPP control rooms will probably benefit from modifications based on these reviews. However, human factors engineering of control rooms--

even very good human factors engineering--deals with only part of the problem. The problem of performance improvement in the control room, and in the balance of the plant, requires consideration of more factors than just panel layout, labeling and "knobs and dials."

HUMAN RELIABILITY, HUMAN FACTORS, MAN/MACHINE INTERFACE: WHAT DOES IT ALL MEAN?

Reliability in human performance is the result of a number of factors (which have come to be called human factors). One, but only one, aspect of human factors is the so-called human engineering. The term "man/machine interface" is often considered to refer to how well controls, displays, and panels are designed for use by human operators. The "quality" of control and display design is usually evaluated by how well these controls and displays conform to recommended characteristics that were found through research to be more effective for use by human operators. The "goodness" of panels (chiefly layout) is evaluated through the application of general analytic techniques that indicate possible speed of use and, to some extent, likelihood that errors will occur in use. There are factors--"human factors"--other than the design of control room displays and panels, that can have significant effects on human reliability. The man/machine interface implies consideration of these additional factors in order to achieve a smoothly matching interface between man and machine.

What are the "Factors" in Human Factors?

The general technology that has come to be called human factors, or ergonomics, generally deals with the design of systems to match the attributes of people and equipment in order to achieve some specified level of performance. In order to achieve optimal performance in a system that has both human components and equipment components, consideration of four sets of human factors is required. The design of the equipment is only one of these factors. At Applied Science Associates, Inc. (ASA), we conceptualize four sets of human factors that form the four corners of the base of a pyramid--the apex of which is performance. We refer to this as the "Performance Pyramid."

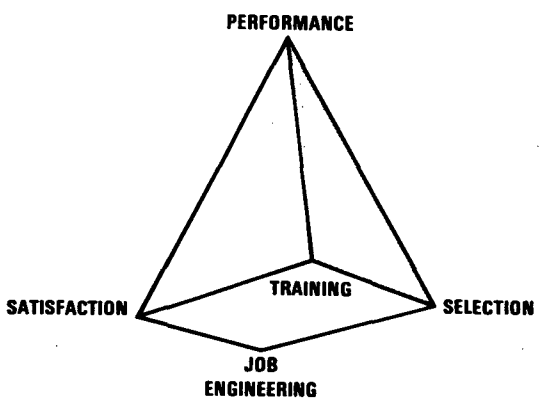


Figure 1. Performance Pyramid

What we are saying with the performance pyramid is: To perform a job well, the job incumbent, or performer, must be: (1) capable of learning adequate performance, as well as have the personal and physical attributes that are necessary (selection); (2) he/she must know what to do and how to do it; that is, be adequately trained and qualified to perform the job (training); (3) he/she must have the tools, environment, and the information required to perform the job (job engineering); and (4) there must

be some positive reason to perform effectively; there must be "something in it" for them.

As we discuss these bases of performance, we will see that all of them revolve around job- and task-analysis. The job- and task-analyses called for in NUREG-0700 and NUREG-0801 can be used for many purposes, if they are planned to be multi-use at the time they are performed. The key questions that must be answered in the industry, which will then allow us to answer the basic questions involved in the above four sets of factors, is "What do we want the person to do--What is the job--What is acceptable performance?"

FOUR FACTORS THAT INFLUENCE QUALITY OF PERFORMANCE

The four factors that we have conceptualized as the corners of the base of the "Performance Pyramid" are described below. Along with the descriptions of what the four factors are, we have included descriptions of some representative studies that support these concepts as important to quality of performance.

Job Engineering

The design of the workplace, the availability of tools, the availability of information that allow the job incumbent to perform as desired, have been well documented in many places. Much of this documentation is basic to the field of human engineering (for example, Van Cott and Kincaid[4]). A rather extensive reference list of human engineering/job engineering is presented in NUREG-0700.

Part of the "job engineering" factor is handled by detailed control room design reviews (NUREG-0700). The basic underlying question for NUREG-0700 "Control Room Design Reviews" is: "Is the job environment (equipment and facilities) designed so that it is possible for the job incumbent to perform as desired?" In many cases, design problems are obvious. For example, it is clear that human beings cannot operate two controls simultaneously if they are 10 feet apart. Sometimes it is less obvious that there is not sufficient time for an operator to operate two controls 40 feet apart. Nonetheless, the obviousness of these problems sometimes tend to obscure the importance of more subtle problems in this area.

One less obvious problem is the availability of information required for use on the job in a form that that is usable on the job. In one project done by ASA for a major steel company, it was found that electrical schematics for the process control equipment in the mill were incomplete, inaccurate, and did not indicate signal values to be expected at most test points. Further, they contained a lot of information that could not be used in troubleshooting and repair of the equipment, obscuring the useful information on the diagrams.

ASA technicians took voltage and waveshape readings on the equipment, re-drew the drawings to present complete information in a clear and systematic format designed specifically for use in troubleshooting.

This bit of job engineering--directly applicable to NPP troubleshooting--made it possible for the plant maintenance people to do their jobs much more effectively. As you will see later, they also needed some specific job training.

Selection

It should be obvious that job design features are not independent of the attributes of the human component in the system. However, this aspect of performance is frequently overlooked.

What we are saying here is that the cost effectiveness of selecting the human components to match with the equipment components is a neglected aspect of the man/machine interface. Some emphasis has been placed on the psychological stability required for NPP personnel, but other psychological attributes of these personnel have neither been addressed nor explored.[5] Psychological testing and selection procedures are often avoided by companies (in all industries) because of misconceptions regarding the Federal mandates for job-relevance of selection and testing procedures.[6]

In fact, job-relevant selection should be the aim of all companies, because this is a cost effective way of ensuring that the employees are: (1) trainable in the necessary tasks that are required for satisfactory performance, and (2) are capable of doing the job that is necessary.

Part of the misconceptions stem from the mistaken idea that the best employee for any job is the most highly intelligent, physically robust, and psychologically stable individual that can be found. For some jobs, the opposite may be true. For example, Tinkham[7] described the successful use of handicapped persons in various industries, and noted that slight amounts of mental retardation often will enable the worker to perform tedious tasks that would handicap a "normal" worker because of the very monotony of the task. Swain[8] points out that, in routine assembly line tasks, workers often complain that they do the same job day after day. He gives the example of an assembly line worker who attaches front bumpers to an automobile, and points out that "A man with an IQ of 70 might not aspire to work on rear bumpers." Thus, the general idea that the best "all-around person" is always better for the job, no matter what the job may be, is contradicted by these research findings. This is not to suggest that mentally handicapped people should be employed in NPPs, but to illustrate the point that selection is a relevant human factor.

The problem with using good selection techniques, of course, is that the goals of selection must be clearly defined.[9] This definition usually involves job- and task-analysis.

In the case of the NPP industry, however, these job- and task-analyses are already required for the detailed control room design reviews and really involve little additional expense.

Training

The preceding discussion should make it obvious that the design of job features is not independent of the attributes of the human component in the system. If the right people are selected, and the job is engineered so that it is possible to do it--those who are to perform the job must learn what to do, how to do it, and when to do it. When there is mismatch in the man/machine interface, the machine can often be redesigned to improve the match, but that is an expensive solution.

The question that should arise at this point is "Can the human be redesigned?" The first answer to this question is usually "Of course not!" but that is not true. Human behavior is incredibly flexible and, within the overall limitations imposed by physical and psychological attributes, that behavior can be redesigned (trained).

Training on what, when, and how to perform the tasks of the job is clearly job-related. To learn these things, trainees must practice--either a simulated version of the task or the task itself. The emphasis on training and qualification testing of operators in NPP has neglected the principle that cost effective training is job-related training. The training provided to NPP operators (and the qualification tests) have been developed along the lines of education in nuclear physics or nuclear engineering, rather than based on the known requirements of the job.

Training is not the same as education. Training should focus on how to perform the tasks required on the job, and should emphasize practice of those tasks--the discriminations required, the information-processing needed, and the decision-making required. Training is most effective when it does not emphasize learning theoretical information about the equipment or the processes. It should include the essential minimum of that information that will facilitate learning or permit performance of the job tasks. Cost-effective training is based on a knowledge of what the job incumbent is required to do in order to perform successfully.

A strictly job-derived course[10] in maintenance of electronic and electromechanical troubleshooting was developed and administered. This course was about 60 percent as long as the conventional course being used at the time. The experimental course, based on a detailed task analysis, concentrated on practice of specific job tasks, made use of many simple part-task trainers, and was mainly self-paced.

The conventional course emphasized theory of operation, used for a training device only the operational equipment (bench-mounted and stimulated by special devices), and was instructor-led.

Forty high-aptitude and forty medium-aptitude students took the experimental course.

The experimental course cost about 25 percent of the conventional course cost to develop and administer and, in addition, required only about one-third the student and instructor personhours.

At the end of the course, sixteen different measures were used to compare the groups and twelve measures in a field follow-up about six months later.

Figure 2 summarizes the results.

End-of-Course (16 measures)		Field Follow-Up (12 measures)	
Experimental Medium-Aptitude (LCI-M) vs. Conventional (C)	Experimental High-Aptitude (LCI-H) vs. Conventional (C)	Experimental Medium-Aptitude (LCI-M) vs. Conventional (C)	Experimental High-Aptitude (LCI-H) vs. Conventional (C)
LCI-M superior/ 3 measures	LCI-H superior/ 6 measures	LCI-M superior/ 0 measures	LCI-H superior/ 3 measures
C superior/ 4 measures	C superior/ 4 measures	C superior/ 2 measures	C superior/ 1 measure
No difference/ 9 measures	No difference/ 6 measures	No difference/ 10 measures	No difference/ 8 measures

Figure 2. Comparison of LCI and Conventional Course Results

The major point of this study is that directly job-relevant training produced performance of equal or higher quality than the traditional theory and general knowledge training, requiring many more weeks.

In another case,[11] a large steel-producing firm had been attempting to improve the quality of plant electronic maintenance. They had tried:

1. Several years of on-the-job training and tutorial instruction under the guidance of experienced experts.

   Result: Little change in on-job performance, but the problem gained significance.

2. One year (28 sessions) of classroom training covering mathematics, physics, chemistry (related to electricity and semiconductors), basic electrical machinery, and electricity.

   Result: No change in on-job performance.

3. Three years of community college sessions in industrial electronics training (90 classes). These classes covered basic electricity and electronics up through complex electronic devices.

   Result: Little improvement in on-job performance.

This company came to ASA, who determined the specific job skills required for these maintenance technicians, then designed an integrated system of maintenance aids and specific-skills training. The training required one week per trainee. The result was marked improvement in on-job performance, at much lower training costs. The additional maintenance aids required by this integrated system did not increase the cost of this system to anywhere near the cost of the previously-used systems.

A Digression

At this point in previous discussions of the "Performance Pyramid" with various industrial clients, we have been asked the question: "If human factors specialists know so much about the performance of job engineering, training and selection in the military, why are the military services still struggling so to improve performance?"

There are really two answers to this question. The first is, perhaps, best illustrated by the following story. A farmer sent his son to agriculture school. The son came back brim full of new ideas and techniques. He urged his father to try this innovation and that innovation and this technique and that technique to improve the yield on his farm. This went on several days until the farmer finally looked at him and drawled "Hell, son, I ain't farming half as good as I know how, now!"

In fact, all of us know a great deal more about improving human performance than we are putting into practice.

The second answer to this question is the fourth corner of the base of performance. That is: job satisfaction--"What's in it for the worker?"--"Why should he/she want to do this?" The second answer then brings us to the fourth corner of the base of performance--satisfaction.

The Fourth Factor--Satisfaction

Given that the job incumbent knows what to do, is personally capable of doing it, and has the equipment, facilities, tools, and information to do the job well, the question remains: "Is he willing to do it?" The conditions surrounding the job must be such that the persons in the job obtain some positive reward or satisfaction for performing the job effectively. These rewards must be ones that they do not get from performing less effectively.[13,14] Job motivation and satisfaction enjoyed a brief period of popularity in the early 1970s (see Swain[8] for a review). These ideas are finding a rebirth in the "Quality Circles" borrowed from the Japanese. It

is interesting to note that the Japanese took many of these ideas from the American "worker motivation by job satisfaction" from the 1970s.[15]

As a quick illustration of the application of the principles of increased motivation leading to improved performance, we will cite a study done by ASA for a major industrial client. ASA was asked to improve job performance at the "ABC Company" on tasks that were relatively simple and required no particular technical skills.[16] In fact, this job was so simple that there was no room for improvement through job engineering, training, or selection. Any gains in performance then would have to be increased motivation. ASA instituted a program to (1) make the job more interesting, (2) change supervisors' behavior to improve general satisfaction, and (3) to keep the work force informed on how well they were doing. In addition, publicly-awarded rewards were instituted for top performers. The rewards themselves were relatively inexpensive, but very well publicized, introducing an element of healthy competition. This program resulted in an improvement of 40 percent in error rate (from about .1 percent to about .06 percent error).

Similar gains are being posted by the quality-control circle concepts developed and implemented at Mercury Marine[17] and other major industrial concerns.

SUMMARY AND CONCLUSIONS

We have tried to bring to your attention factors other than control room design reviews and modification that can have significant impact on human performance. The included examples of specific applications of technology in this broader view of human factors show their potential impact in NPP operation. It seems apparent to these authors that "We ain't farming half as good as we know how, now!" Thus, one of our conclusions from this review is that less research is needed looking into basic principles of performance improvement and more research should be performed looking into how to implement these principles within the nuclear industry and NPPs.

We do not mean to imply that all of the questions about performance improvement have been answered--they have not. Nor do we intend to imply that basic research is not necessary. We do intend to imply that the technologies and techniques for solving many of these immediate problems of the nuclear industry are available, in principle and have worked in practice. We feel that a maximum effort to adapt these technologies to the particular needs of the nuclear industry (such as was done with job engineering in NUREG-0700) is a high priority. Technologies developed in the military and in other industries cannot be transferred directly to the nuclear industry without adaptation. But, it is there to be adapted, and it must not be ignored.

The answer to the question posed in the title of our paper should be self-evident at this point. The question is "What do we do after the control room reviews? and, perhaps, we should add "and we find out that the control room modifications don't solve all the problems?" The job design and job engineering embodied in the detailed control room design review attack only part of the problem of performance improvement (which is basic to safety enhancement).

The next step is to address the problems inherent in the other three corners of the base of the "Performance Pyramid"--selection, training and satisfaction. Much of the necessary front-end analysis work to attack these problems will have been performed by the job- and task-analyses done in the detailed control room design review--for the control room. The balance of the plant has not yet been addressed.

Control room enhancements will certainly help, but they will not solve the problem of increased safety and reliability in NPPs. The basic task-analyses must be used to develop job-related selection, job-related training, and criterion-referenced qualification testing, and--most of all--programs to increase worker satisfaction and

motivation to perform as well as they possibly can. Adapting and applying proven technologies in these areas to NPP operation and mangement must be given greater emphasis if we are really serious about thermal-nuclear plant safety.

REFERENCES

1. Seminara, J. L., Gonzalez, W. R. & Parsons, S. O. "Human Factors Review of Nuclear Power Plant Control Room Design." Electrical Power Research Institute Report No. NP-309, Palo Alto, CA, March 1977.

2. Rogovin, M. & Frampton, G. T., Jr. Three Mile Island: A report to the commissioners and the public. Washington, DC: Nuclear Regulatory Commission, 1979.

3. Kemeny, J. G., et al. Report of the President's commission on the accident at Three Mile Island. Washington, DC: Government Printing Office, October 1979.

4. Van Cott, H. P. & Kincade, R. G. Human engineering guide to equipment design. New York, NY: McGraw-Hill, 1972.

5. Edelhertz, H. & Walsh, M. The white-collar challenge to nuclear safeguards. Lexington, MA: Lexington Books, 1978.

6. "Uniform Guidelines on Employee Selection Procedures," (1978), 43 FR 166.

7. Tinkham, M. L. Vocational rehabilitation. Quality Progress, 4, 12-15, 1971.

8. Swain, A. D. Design of industrial jobs a worker can and will do. Human Factors, 15(2), 129-136, 1973.

9. Cronbach, L. J. & Gleser, G. C. Psychological tests and personnel decisions. Urbana, IL: University of Illinois Press, 1969.

10. Pieper, W. J., Folley, J. D., Jr., & Valverde, H. H. Learner-centered instruction (LCI): Volume VII - Evaluation of the LCI approach. Valencia, PA: Applied Science Associates, Inc., 1970. (AFHRL-TR-7 0-1).

11. "Diagnosing breakdowns in process control equipment." Applied Science Associates, Inc. (ASA) Brochure, Valencia, Pennsylvania, 1974.

12. Foley, J. P. Job performance aids in the nuclear power industry. In: Hickeyy. A. E. (Ed.). Simulation and training technology for nuclear power plant safet (Proceedings) Bedford, MA: American Institute for Research, 1981.

13. Gellerman, S. W. Motivation and productivity. New York, NY: American Manage ment Association, 1963.

13. Gellerman, S. W. Motivation and productivity. New York, NY: American Management Association, 1963.

14. Glaser, E. M. Productivity gains through worklife improvements. New York, NY: Harcourt, Brace, Jovanovich, 1976.

15. Oshima, M., Hayashi, Y. & Noro, K. Human factors which have helped Japanese industrialization. Human Factors, 22(1), 3-14, 1980.

16. Itkin, E. S. The ABC Company: Performance improvement. Valencia, PA: Applied Science Associates, Inc., 1980.

17. Ingle, S. Quality Circles Master Guide. Englewood Cliffs, NJ: Prentice-Hall, 1981.

REVIEW AND EVALUATION OF HUMAN ERROR RELIABILITY DATA BANKS

D. A. Topmiller, J. S. Eckel and E. J. Kozinsky

General Physics Corporation
Suite 240, 1010 Woodman Drive
Dayton, OH 45432

ABSTRACT

This paper describes a survey and comparative analysis of past and current attempts to quantify and predict human operator and maintainer performance as a function of design, training, procedural or situational factors. An assessment was made of these methods and techniques as to their potential applicability to Probabilistic Risk Assessment (PRA) or as a supplement to the data and procedures in NUREG/CR-1278, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications." Five human reliability data banks developed previously were reviewed along with five current systems which include estimates of human error related events. Both past data banks and current data systems were evaluated against a set of criteria intended to serve as guidelines for an idealized human reliability data reporting, storage and retrieval system. A set of recommendations, based on this evaluation, was generated. The original tabled human error data for the five data bank efforts are completely reproduced and included in an indexed appendix to NUREG/CR-2744, "Human Reliability Data Bank for Nuclear Power Plant Operations: A Review of Existing Human Reliability Data Banks", which this paper has summarized. The forms and relevant reporting codes are also reproduced and included in the appendix for the existing data reporting systems.

INTRODUCTION

This paper describes two tasks in a program sponsored by the Nuclear Regulatory Commission (NRC) and Sandia National Laboratories (SNL) to develop a human reliability data collection and retrieval system to be used in risk assessment of nuclear power plants. The tasks were to summarize and review five previous attempts to develop human error data banks for use in systems reliability analysis. These past data banks include: American Institutes for Research (AIR) Data Store; Bunker-Ramo Tables for Predicting the Operational Performance of Personnel; Aerojet General Human Reliability in the Performance of Maintenance; Techniques for Establishing Personnel Performance Standards (TEPPS); and, Operational Recording and Data System (OPREDS). In this review, an assessment was made of the utility of these data banks as supplementary material to the Human Error Probability (HEP) values currently presented in NUREG/CR-1278. Although the initial NRC/SNL requirement was to review and summarize the three systems of AIR, Bunker-Ramo and Aerojet General, it was decided also to review and evaluate two Navy Systems (TEPPS and OPREDS) because of the unique nature of their data.

In addition to the review of past data banks, two accident/incident systems currently employed in the military and civil aviation communities were reviewed. These data banks are the Air Force Inspection and Safety Center (AFISC) Life Sciences Acci-

dent and Incident Reporting System and the Aviation Safety Reporting System (ASRS). Four other data collection systems presently in use in the nuclear power industry were also reviewed. These data collection systems include: the Nuclear Plant Reliability Data System (NPRDS), the IEEE Human Factors Working Group SC 5.5 document, (which is not really a collection system itself, but a summary of systems)[1], the Safety-Related Operator Action Program (SROA), and the Sandia Simulator Research Program. Since these existing data collection systems are not dedicated exclusively to human reliability analysis, only those parts that were preceived as potentially relevant to a human reliability data bank were evaluated.

DISCUSSION

Past and current data banks were examined in terms of their relevancy to a human reliability data bank for nuclear power PRA applications. This was accomplished by evaluating them in terms of specific criteria established for that purpose. These criteria included factors related to the recording, processing and retrieval characteristics of a data bank system. The rationale underlying this approach was that the data bank could be designed by assessing different aspects of past and current efforts. Thus, inadequacies within these techniques could be assessed and then could provide better direction for the definition of a data bank needed for PRA applications.

The criteria that were developed are included in Tables I, II, and III. The definitions of these criteria are intended to be as operationally significant as possible.

Three project investigators from General Physics Corporation independently rated the past and existing data banks against the sets of criteria listed above. The averaged ratings, using a three-point scale (High-3, Medium-2, and Low-1) and defining the degree to which the data bank or system met the criteria, appear in Table IV. Note that the past data banks were not evaluated against criteria for data processing and evaluation since none of these banks was ever implemented in an operational system. It should also be recognized that this rating system was applied to all of the banks and reporting systems, independent of their applicability to a nuclear power industry data bank.

It can be seen from Table IV that the AIR Data Store and the Bunker-Ramo tables are virtually tied on the nuclear power plant (NPP) relevant criteria of meaningfulness, specificity and validity for the Criteria for Users. Although the ratings for the other two sets of criteria, i.e., Criteria for Collection of Data and Criteria for Data Processing and Evaluation are presented in the table, they appear to be most pertinent to the existing data systems and not to the previous data banks.

Since the IEEE SC 5.5 effort is a summary of data collection systems and banks in itself, no attmept was made to rate these summaries against the criteria. The Sandia Simulator Research Program had not generated sufficient data at the time of this report to be rated. The NPRDS and SROA systems scored highest on the NPP relevancy criteria of meaningfulness, specificity and validity but fell somewhat short on other significant data bank systems criteria.

The AFISC and ASRS systems are relatively highly developed aircraft accident/incident reporting systems which have been in operation for many years. Although the data entry and category information has low relevancy in general to NPP applications, the systems criteria are relevant to designing an optimum human reliability data

[1]The IEEE Human Factors Working Group SC 5.5 has become Subcommittee 7, Human Factors in Control Facilities.

TABLE I

Criteria for Users

1. Meaningfulness - The data should be based on measurable aspects of performance. These measures should be directly interpretable by the users. The two primary user populations will be probablistic risk assessment practitioners and equipment designers. Use of the data for training and selection is also possible. The data should be in a form compatible with common models used by those populations.

2. Specificity - HEP data relevant to human engineering equipment design features should be specific for NPP application. Performance Shaping Factors (PSFs) should be specific to the NPP working environment.

3. Objectivity/Reliability - The use of the data bank should yield repeatable results. Two users seeking the same information should retrieve the same numbers. This requires a more quantitative, objective treatment as opposed to subjective ratings. Inter-rater and intra-rater reliability must be high.

4. Comprehensiveness - All factors known to be important to NPP must be covered. All potentially relevant PSFs should be recorded.

5. Ease of Use - Use must be both fast and clear. The amount of time spent by the user should be minimized without loss of control. To control this time, instructions must be clean and well designed.

6. Veridicality - The data must have construct validity, correctly treating the quantitative effects of pertinent performance shaping factors. The data must retain its operational meaning from the input to output continuum.

7. Validity - The data in the bank must be amenable to scientific treatment. The numbers must be accurate. Some indication of how the data may be generalized to applications not specifically covered must be included.

8. Transparency - The data should not be accessible to a potential user between the input and the output side of the system even though they may have undergone certain transformations for purposes of system design efficiency. In other words, the information management system that stores, retrieves and manipulates (transforms, aggregates, etc.) the data is only modifiable by the system designer/manager, not the user.

9. Cost - The cost (time, money, etc.) of the use of the data bank must be as low as possible and, in particular, not perceived as excessive by the potential users.

TABLE II

Criteria for Data Processing and Evaluation

1. Robustness - The data must maintain their descriptive and predictive significance from the input to the output stages. The data processing system must not distort the meaningfulness of the data by virtue of processing mechanisms (coding, collating, aggregating, etc.).

2. Integration Compatibility - The data bank must have the ability to aggregate data from various sources: field, research, historical data.

3. Objectivity/Reliability - Sufficient guidelines for data processing must be developed to ensure high inter-processor objectivity, reliability and consistency.

4. Centrality - The data should be guarded against user access at any intermediate stage of processing. (The opposite of transparency.)

5. Data Recoverability - Raw data must not be lost. It must be retained in a retrievable fashion for possible later re-analysis.

6. Quantitative - All data in the bank should contain scaled values for HEPs and PSFs. Attempts should be made to keep scaled values at the interval scale of measurement. Attempts should be made to apply this criterion to subjective measures as well.

Table III

Criteria for Collection of Data

1. Ease of Use - The time required to make an entry must be summarized. Three factors must be considered: (a) accessibility of the entry mechanism, (b) time for the mechanics of entry, (c) "Ease of entry" - a one page form with perhaps one page of instructional material is the targeted size. A trade-off between speed of reporting and accuracy is required, or "How long since the event," must be considered in the use of the data collection system.

2. Reinforcement - Two facets of reinforcement must be taken into account: (a) There must be no negative reinforcement. This may be achieved by varying levels of anonymity. In the current regulatory structure, NRC involvement in the data collection and processing is not feasible. There must be no recriminations, investigations, or fines directed against data reporters. (b) Positive reinforcement should be an attribute of the system.

3. Meaningfulness - The vocabulary of the data bank must be compatible with plant equipment and operator actions. The questions posed must be behaviorally matched to the input population (designed in context with their work environment). Compatibility with the input population is required, or, at least, consonance with their frame of reference.

4. Specificity - As for users, explicit treatment of NPP equipment types and performance shaping factors is required. The input source must not be required to generalize about similar equipment types.

5. Fidelity - Attempt to represent the physical event as accurately as possible, while minimizing reporting work load. This may require trade-offs between open-ended descriptions of an event and "force fitting" an event to predefined descriptive categories.

6. Flexibility - Free form input beyond a fixed taxonomy must be allowed. This will provide information about possible limitations in the fixed taxonomy, including areas where those inputting data felt they could not adequately describe the situation in the previously defined format.

7. Acceptability - The form for data collection must be acceptable to potential data contributors.

8. Cost - The cost for the data collection must be low to those providing the data. Data processing costs must be reasonable, but are not as significant as the costs to data providers.

9. Comprehensiveness - The completeness with which the data reflect all potential situations in which human error can contribute to system safety as assessed and predicted through probability risk assessment techniques.

10. Relevance - Those sufficiently germane data, not directly collected from NPPs, but which are pertinent enough to possess acceptable construct validity.

Table IV

Criteria Data System Matrix

DATA BANK	CRITERIA FOR USERS									CRITERIA FOR DATA PROCESSING AND EVAL.							CRITERIA FOR COLLECTION OF DATA										T	$\bar{X}R$
PAST DATA BANKS	Meaningfulness	Specificity	Objectivity	Comprehensiveness	Ease of Use	Verdicality	Validity	Transparency	Cost	Robustness	Integration	Compatibility	Objectivity	Centrality	Data Recoverability	Quantitative	Ease of Use	Reinforcement	Meaningfulness	Specificity	Fidelity	Flexibility	Acceptability	Cost	Comprehensiveness	Relevance	Total N = 19	Mean Rating
AIR Data Store	3	2.5	3	2.5	2	2.5	2	1.5	2								2	2	3	2.5	2.5	1	2	1.5	2	2.5	42.0	2.21
Bunker-Ramo	2.5	2.5	1.5	2	2	2	2	1.5	2								2	2	2.5	2.5	2.5	2	2	1.5	2	2.0	39.0	2.05
Aerojet General	2	1	2	1.5	2	1.5	1.5	1.5	1.5								1.5	1.5	1.5	1	2	2	2	1.5	1	1.0	29.5	1.55
TEPPS	1.5	2	2	1.5	2	2	2	1	2								2	1.5	2	2.5	2	2	2	2	2	1.5	35.5	1.87
OPREDS	1	1.5	3	1	1	2.5	2.5	1	1.5								1	1	3	1	3	1.5	2	1	2	2.0	32.5	1.71
EXISTING DATA BANKS																											N=26	
AFISC	2	1	2	2	1.5	2	2	2	1	2.5	2	1.5	2.5	2	2	2.5	1	2	2	1.5	1.5	1.5	3	1	1	1	46.0	1.77
ASRS	1.5	1	1	2	1.5	1.5	1.5	1	2.5	1	2	1	1	1	2	2	2	3	2.5	2	1.5	2.5	2	2	1	1	43.0	1.65
NPRDS	2	2.5	1.5	1	1	1	2	1	1	1.5	2	2	1.5	1	2	2	2	1	1.5	2.5	2	1.5	1.5	2	2	2.0	43.0	1.65
SROA	3	3	3	2	2	1	3	1	2	2	2	3	3	1	3	3	2	1	3	3	3	2	2	2	2	2.5	59.5	2.29

High = 3

Medium = 2

Low = 1

storage and retrieval system. The AFISC system inputs result from professional and thorough accident investigative techniques, whereas the ASRS system is voluntary and has a built-in incentive system for reporting the incident as well as a high degree of anonymity.

The incentive system criteria for data collection should probably receive a factor or two heavier weighting on the "relevancy" scale of criteria for collection of data. This is particularly true for field data collection and deserves some special discussion. In most instances, it is very difficult to distinguish between equipment failures and human-initiated malfunctions. Part of the difficulty lies in the types of reporting systems (forms, procedures, etc.), and part resides in the reluctance of the initial "discoverer" to incriminate himself or his co-workers. The supervisor is also reluctant because it may make his section "look bad," and he is, in most instances, required by company policy to consider such reports when evaluating his personnel.

Some form of reinforcement mechanism needs to be incorporated within any proposed human error reporting system. Without such a mechanism, the authenticity of the reports themselves becomes questionable. Whether such a mechanism would utilize positive as well as negative reinforcement would depend in large part on the regulatory leverage imposed upon the system, as well as on internal company policies. The AFISC system is successful because of its inherent, structured, organizational framework. The ASRS system is successful because of the limited immunity and anonymity afforded its reporters. The NPRDS does not work as well for the utilities, probably because it has neither the required military discipline of the AFISC nor the personal operator immunity of the ASRS. Incorporation of these features would seem to be desirable in any proposed field collection system.

Industry nas long recognized that to increase profitability, production staffs can not inspect themselves. As a result, industry separated quality control functions from production functions. A similar approach may be necessary in the nuclear power industry to collect good human reliability data. Development of a separate quality control agent would not necessarily dictate an increase in the number of personnel, because the operators' time for completion of failure reports, etc. would then be reduced. Perhaps it would open a new career field to operators, thereby providing increased motivational incentives for its personnel.

RECOMMENDATIONS

Five existing human reliability data banks were reviewed as well as five current data collection systems that include categories for recording human errors. Very little data were found that could be used to improve the Human Error Probability (HEP) values that are currently recorded in NUREG/CR-1278. However, it is recommended that consideration be given to supplementing NUREG/CR-1278 tables dealing with displays (Tables 20-3 through 20-7) and controls (Table 20-13) with relevant AIR Data Store HEPs. It is also recommended that efforts be continued to obtain additional data useful to the support of probabilistic risk assessment.

Virtually no information was found that would support the scaling of performance shaping factors (PSF), which are extremely important in arriving at the specific HEP values that take into account significant contextual and environmental conditions. It is recommended that increased attention be devoted to this important issue. It is suggested that classical psychometric scaling techniques be examined for their applicability to the solution of this difficult problem. (One of the five existing human reliability data banks successfully employed a systematic psychometric scaling technique.)

As a corollary of the first recommendation, a method should be developed for selecting and integrating human engineering data into a NPP human reliability data

bank from the available experimental literature. This should be particularly productive as more of the advanced man-machine interfaces (i.e., communication interfaces, annunciator design, advanced CRT display design, etc.) are subjected to well-controlled experimental treatment by the human factors community either in part-task simulations or whole scenario studies.

Finally, it is recommended that a human reliability data bank specifically tailored for NPP PRA applications be established. Even though some of the data from existing data banks can be used for PRA applications, additional data are required.

Table V presents a condensed summary of the above recommendations.

Table V

Summary of Recommendations

- Continue Efforts to Obtain Additional Data in Support of Probabilistic Risk Assessment
- Implement a Program for Performance Shaping Factors (PSF) Psychometric Scaling
- Develop Methods for Continued Integration of Data Generated from Experimental Literature into a Human Reliability Data Bank
- Establish a Human Reliability Data Bank Specifically Tailored for NPP PRA Applications

ACKNOWLEDGEMENTS

This work was performed under the auspices of the NRC, through contract with Sandia National Laboratory (SNL). Dr. Dwight P. Miller of SNL was the technical contract monitor and made many helpful suggestions and recommendations to guide the direction of this review. Dr. Alan D. Swain and Mr. Henry E. Guttmann also of SNL, the authors of NUREG/CR-1278, provided helpful guidance in the development of the report. Ms. Barbara Jean Bell (SNL) provided the authors with useful insight into the human reliability analysis function of probabilistic risk assessment of nuclear power plant safety.

REFERENCES

1. BLANCHARD, R. E., "Likelihood of Accomplishment Scale for a Sample of Man-Machine Activities," Dunlap and Associates, June 1966.

2. HORNYAK, S. J., "Effectiveness of Display Subsystem Measurement and Prediction Techniques," Report TR-67-292, Rome Air Development Center, Griffiss AFB, New York, September 1967.

3. IRWIN, I. A., J. J. LEVITZ, and A. M. FREED, "Human Reliability in the Performance of Maintenance," Report BRP317-BSD-TDR-63-218, 1963.

4. IRWIN, I. A., et al, "Human Reliability in the Performance of Maintenance," Report RP.317/TDR-63-218, Aerojet General Corporation, Sacramento, California, May 1964.

5. IRWIN, I. A., J. J. LEVITZ, "Validation of a Method for Predicting Human Reliability," Report 9805-10-08-1/SSD-TR-64-290, 1964.

6. IEEE Human Factors Working Group SC 5.5 - "Report of a Survey for Models and Data Bases Relating to Human Performance in Nuclear Power Generating Stations," July 1981.

7. MEISTER, D., "Methods of Predicting Human Reliability in Man-Machine Systems," Human Factors, (Vol. & No.) (6), 621-646, 1964.

8. MEISTER, D., D. FINLEY, E. THOMPSON, and S. HORNYAK, RADC-TR-70-140 - "The Effect of Operator Performance on Airborne Electronic Equipment Reliability," July 1970.

9. MEISTER, D., and R. B. MILLS, "Development of a Human Performance Reliability Data System," AMRL-TR-71-74, Aerospace Medical Research Laboratory, Wright-Patterson AFB, Dayton, Ohio, June 1971.

10. MILLS, R. G., R. F. BACHERT, and S. A. HATFIELD, "Quantification and Prediction of Human Performance: Sequential Task Performance and Time," AMRL-TR-74-48, Aerospace Medical Research Laboratory, Wright-Patterson AFB, Dayton, Ohio, August 1975.

11. MUNGER, S. J., R. W. SMITH, and D. PAYNE, "An Index of Electronic Equipment Operability: Data Store," AIR-C43-1/62-RP(1), American Institute of Research, Pittsburgh, Pennsylvania, January 1962.

12. OSGA, G. A., "Guidelines for Development, Use and Validation of a Human Performance Data Bank for NTDS Combat Operations," March 1981.

13. RIGBY, L. V., "The Sandia Human Error Rate Bank (SHERB)," in R. E. Blanchard and D. H. Harris (Eds.), "Man-Machine Effectiveness Analysis," A Symposium of the Human Factors Society, June 1967.

14. SWAIN, A. D., "Development of a Human Error Rate Data Bank," in Proceedings of U.S. Navy Human Reliability Workshop, February 1971.

15. TOPMILLER, D. A., "Methods: Past Approaches, Current Trends and Future Requirements," in Proceedings of NATO Conference on Manned Systems Design, September 1980.

16. TOPMILLER, D. A., D. C. BURGY, D. R. ROTH, P. A. DOYLE, and J. J. ESPEY, "Survey and Analysis of Communications Problems in Nuclear Power Plants,". (EPRI RP-501-5), Palo Alto, California, Electric Power Research Institute.

17. NUREG/CR-1278, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," Sandia National Laboratories, October 1980.

18. USNRC (U.S. Nuclear Regulatory Commission), 1981, "Guidelines for Control Room Design Review." NUREG-0700.

19. USNRC (U.S. Nuclear Regulatory Commission), 1981. PRA Procedures Guide, "A Guide to the Performance of Probabilistic Risk Assessment for Nuclear Power Plants," NUREG/CR-2300, Review Draft.

20. WILLIAMS, H. L., "Human Performance Reliability in Operational and Maintenance Tasks," Martin-Marietta Corporation, Report OR-8729, February 1967.

21. WILLIGES, R. C. and D. A. TOPMILLER, "Technology Assessment of Human Factors Engineering in the Air Force" Unpublished; AFSC-TR-, (April 1980).

(This is only a partial listing of references. A complete bibliography can be found in NUREG/CR-2744.)

ADDITIONAL EMERGENCY PROCEDURE BASED ON NSSS PHYSICAL STATES APPROACH

P. Cadiet, G. Depond, H. Sureau

ELECTRICITE DE FRANCE
Service Etudes et Projets
Thermiques et Nucléaires
Tour EDF/GDF
Cédex 08

92080 PARIS LA DEFENSE

ABSTRACT

An additional emergency procedure called "U1 procedure" is conceived to assure best possible conditions for RCS cooling and core safety, during very unlikely and out of design situations for which event specific procedures are inappropriate and inefficient. U1 utilization criteria and required actions criteria within U1 are based on continuous post accidental diagnosis using NSSS physical states analysis completed by safety equipment status analysis. After initiating event, continuous post accidental supervision (PAS) is made by the shift technical advisor (STA) who assures human redundancy. If required from STA informations, U1 procedure is decided and used by operator.

INTRODUCTION - OBJECTIVES

Existing emergency procedures for french PWR plants are based on sequential analysis and initiating event diagnosis. This diagnosis is available only a few minutes after protection signal actuation.

Existing emergency procedures are event specific procedures, they assure the optimal recovery actions for events within the design basis of the plant and for a few out of design situations corresponding to redundant system failure (e.g. : AFW failure). But these procedures are not available for all possible events combinations and may be inadequate for very unlikely accidents, coresponding to multiple équipment or human failures simultaneous or not, e.g. : safety system total failure (SI, CSS) or initial diagnosis error or multiple events (LOCA + SG tube rupture or steam line break + SG tube rupture...).

The U1 emergency procedure (U as ultimate) is conceived to assure best possible conditions for RCS cooling and core safety during situations for which existing procedures become inadequate or inefficient.

The objectives for developping U1 procedure are : to avoid or to limit or to delay core degradations and radioactive releases, by using available means, during any situation.

Because of near term utilization requirements, U1 procedure has to be compatible with existing procedures structure and existing instrumentation. At last, no core melt and coolable core geometry are limitations for U1 availability.

METHOD AND PRINCIPLES

After any initiating event and initial diagnosis, operator uses event specific procedures until plant recovery is achieved. During recovery transient, the method by which event specific procedure must be left and U1 procedure must be used is shown by diagram in figure 1. A process is developped to diagnose, at any time and for any condition inexpected transient, which would be different from event trajectory initially diagnosed, or operator action inefficiency. Integration of this process within existing procedures appears very difficult for 3 reasons :

- difficulty to conceive accurate criteria within each procedure and within each recovery action step,
- difficulty for the operator to call his own previous decisions and actions in question again,
- difficulty to introduce this process within existing procedure organization that would lead to a new conception of it.

On the other hand it appears more interesting and feasible to conceive a continuous diagnose :

- using a specific logic which is independent of existing procedures and redundant,
- using NSSS physical states analysis with existing instrumentation [1], completed by safety equipment status analysis,
- supervised by the shift technical advisor (STA) who ensures human redundancy.

This logical process consists of a continuous post accidental supervising (PAS) made by STA intending to the following issues :

- to confirm main recovery actions prescribed in the procedure presently used by operator,
- to provide operator with guidance for additional safety actions if multiple failures occur while using event specific procedure (e.g. : additional steam generator isolation),
- to provide criteria, if more degraded conditions, for using U1 procedure instead of event specific procedure.

PAS logical diagrams (fig. 2 and fig. 3) monitors the following parameters :

- RCS fluid inventory and exit core temperatures,
- each steam generator physical state for RCS heat removal,
- secondary efficiency to reduce RCS temperature and pressure if necessary,
- containment pressure and temperature,
- safety systems status.

U1 procedure is directly used by operator. This procedure consists of a diagnosis/actions grid (See fig. 4). Diagnosis uses PAS logical diagram parameters and criteria combinations are conceived to cover all possibilities. Each combination defines one case in U1 grid and requires specific safety actions on actuators (safety injection, RCP, pressurizer relief, steam dump, AFW, steam or water SG isolation...) without necessity of numerous guidelines. At any time, U1 grid provides clear and limited informations which are independent of all possible events combinations and sufficient to mitigate the system evolution, to return if possible, towards less and less degraded states by using available means.

APPLICATIONS

The conception of PAS and U1 procedure can be synthetized as follow :

a - After any reactor trip or loss of subcooling margin, the shift technical advisor (STA) is called,

b - STA monitors PAS criteria at any time (each 5 mn),

c - Informations or confirmations from STA become operational either after operator initial diagnosis and immediate actions prescribed within event specific procedure are achieved or at least 20 mn after the beginning of accident,

d - PAS is stopped either when using U1 procedure is decided, or when a safe and stable NSSS physical state is established,

e - Using U1 procedure decision is only taken by operator from STA informations monitoring PAS criteria,

f - leaving U1 procedure decision can only be taken by chief engineer.

CONCLUSIONS

PAS and U1 procedure cover all NSSS configurations except when reactor vessel is open, they are available with existing procedures organization and existing instrumentation. PAS and U1 procedure provide an additionnal safety level beyond existing procedures.

Treatments and presentation on safety panel have been developped for PAS and U1 utilization.

For training, presentations and background informations documents have been provided for operators and STA of all operating EDF plants. A full guideline is now developped. In a near future, existing simulators with U1 specific treatments will permit diagnosis process validation and personnel training.

PAS and U1 procedure will be operating in EDF PWR plants as soon as possible during 1983.

REFERENCE

1. NSSS Accidental Physical States Analyses for Operator Assistance - P.P. Cadiet - G.M. Depond - H.M. Sureau.
Trans. Am Nucl. Soc. 38.1.776 (1981).

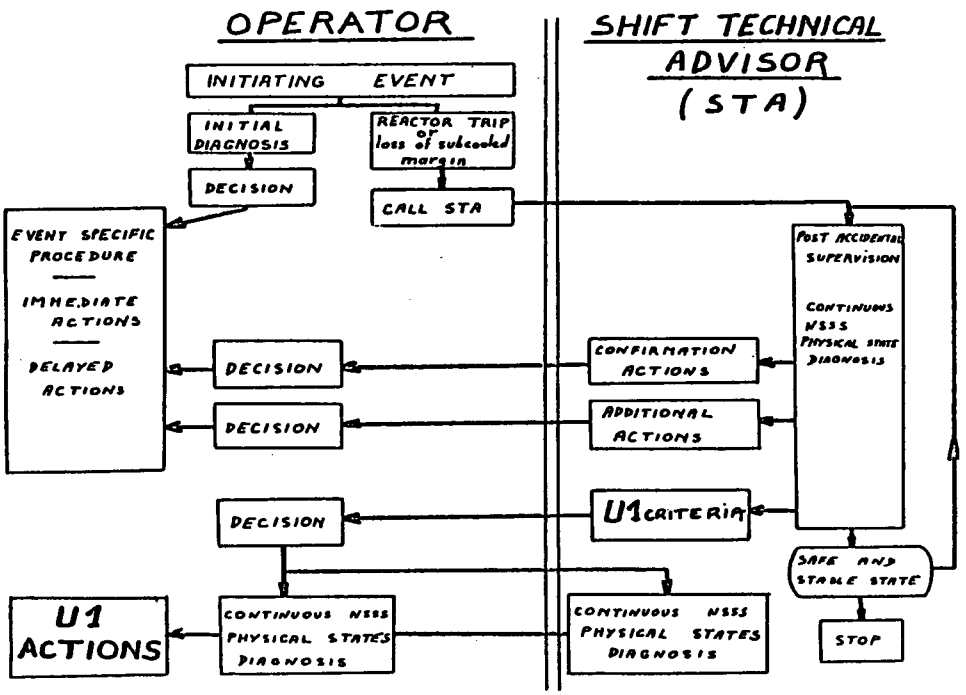


Fig. 1. Overall Structure.

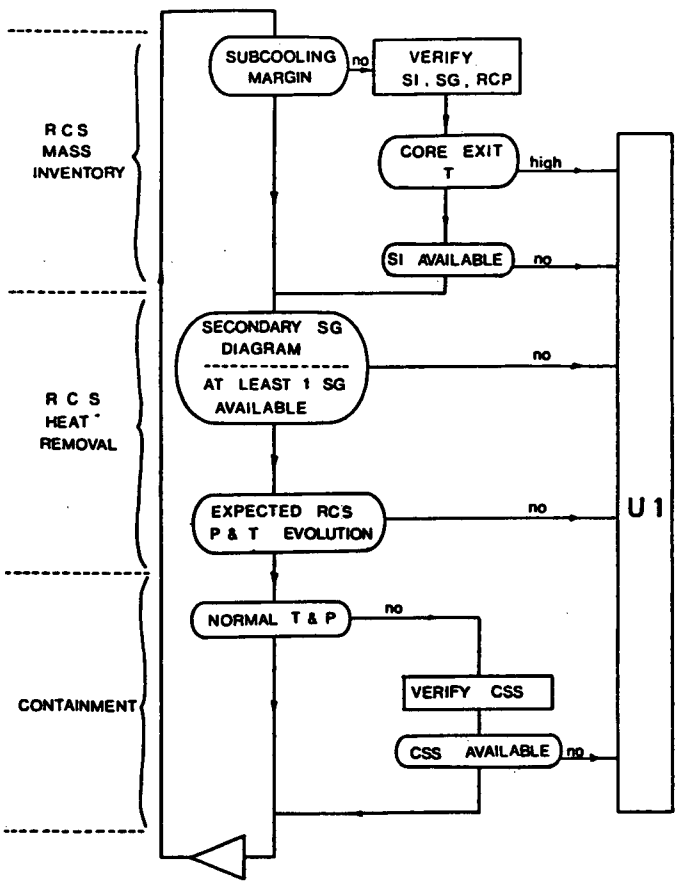


Fig. 2. PAS Diagram.

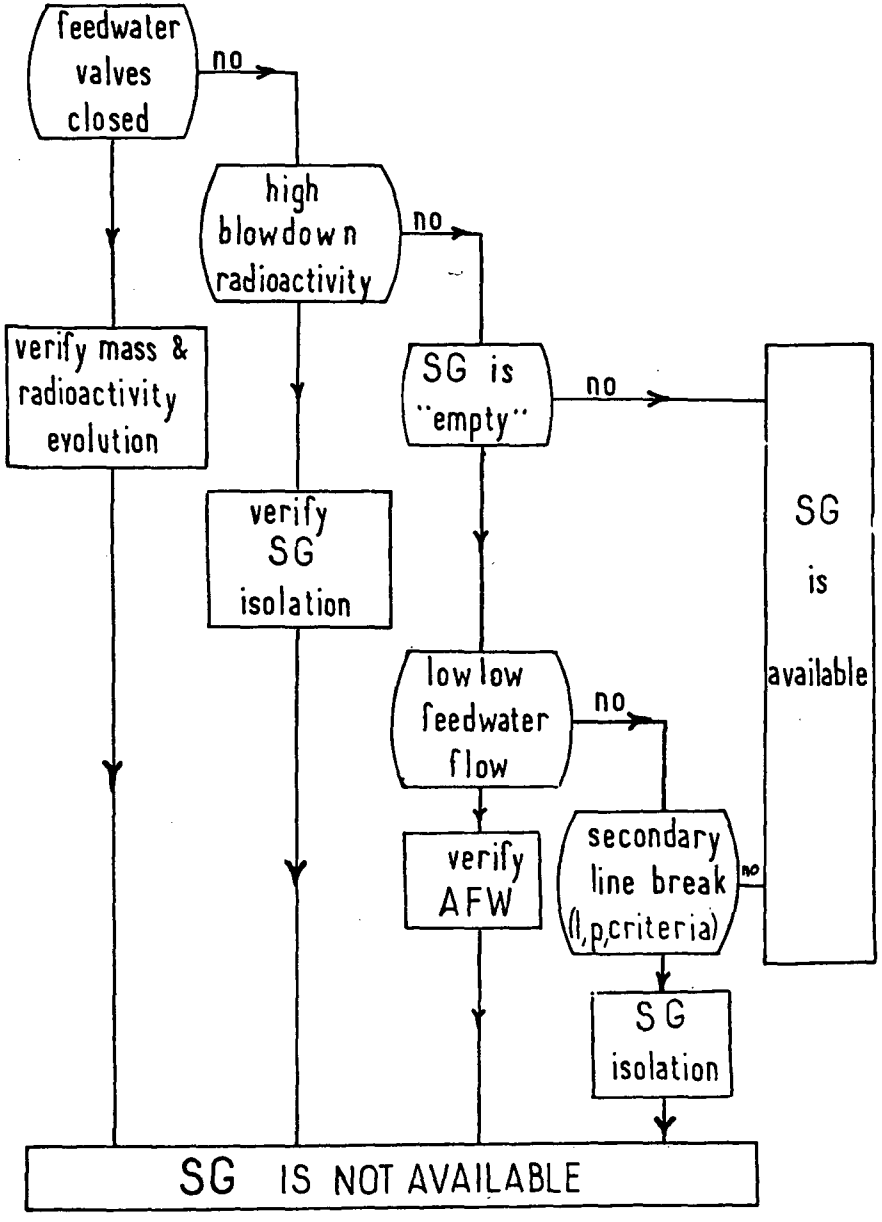
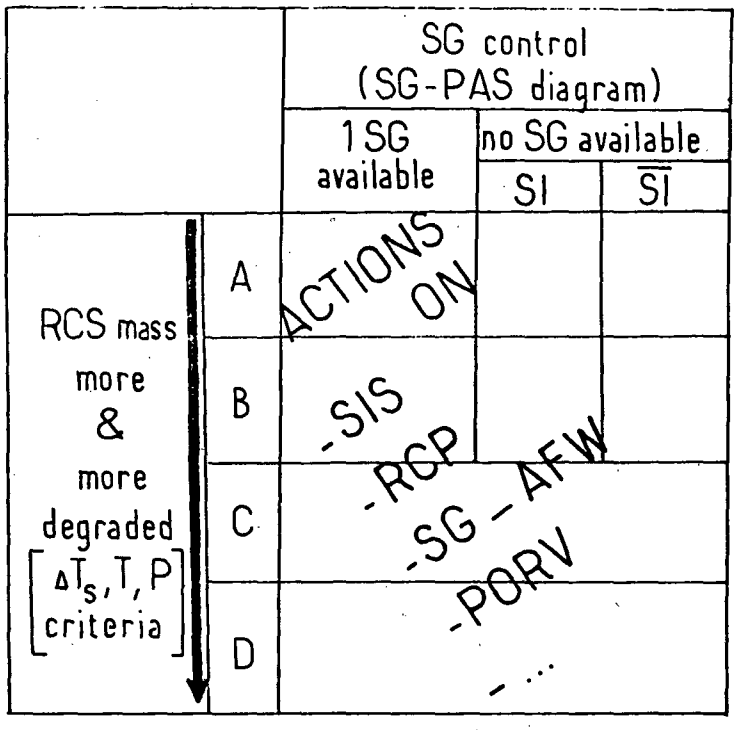


Fig. 3. PAS Secondary SG Diagram.



+ GUIDANCE TO RETRIEVE FAILED SAFEGUARD SYSTEMS

Fig. 4. Ul Grid.

DESIGN OF TEST AND EMERGENCY PROCEDURES TO IMPROVE OPERATOR BEHAVIOUR IN FRENCH NUCLEAR POWER PLANTS

Mme Griffon-Fouco

Electricité de France
3, rue de Messine
75008 PARIS

M. Gomolinski

Commissariat à l'Energie Atomique
B.P. 6
92260 FONTENAY AUX ROSES

ABSTRACT

The incident analyses performed in french nuclear power plants highlighted that deficiencies in the design of procedures are frequent causes of human errors.

The process for developing new guidelines for the writing of test and emergency procedures is presented : this process is based on operators interviews and observations at the plants or at simulators.

The main principles for the writing of procedures are developed. For example :

- the elaboration of a procedure for action and of a separate educational procedure,
- the coordination of crew responses,
- the choice of vocabulary, graphs, flow charts and so on as regards the format.

Other complementary actions, such as the training of operators in the use of procedures, are described.

WHY IMPROVE PROCEDURES ?

The first studies carried out in France in order to improve human behaviour in the operation of nuclear power plants dealt with the analysis of incidents considered as due to human errors. Those analyses allowed us to highlight different causes of human errors which are grouped in the following classes :

1 - work organization,
2 - procedure design,
3 - ergonomical design of the plant (particulary, control room design),
4 - time and duration of the work,
5 - education and training of the personnel,
6 - physical environment,
7 - social environment,
8 - history of the plant,
9 - individual performances of the personnel.

In particular, we often identified the "procedure design" as leading to performance deviations by the operators using them.

For example, we studied an incident due to a human error during the start-up phase : the operator looked at the neutronic power information transmitted by a logical indicator (this information was insufficient) but he did not look at the complementary information transmitted by a chart recorder and an analogical indicator.

This was due to different causes :

- the ergonomical design : the information transmitted by the chart recorder and the analogical indicator was unsuited to the start-up phase.

- the work organization : there was a lack of support for the control room operator because the shift supervisor dealt with other tasks.

- the procedure design : the procedures were insufficiently structured and did not indicate which kind of information it was necessary to read and who had to read this information.

As a conclusion of our incident analysis, we considered that the deficiencies of the procedure design are the main causes of the human error.

Taking into account different incidents analyses leading to the same conclusion, we decided to perform studies in order to improve the design of operating procedures. So, we elaborated guidelines for designing two kinds of procedures :

- periodical test procedures,
- emergency procedures.

Those two types of guidelines are somewhat different, since the emergency procedures call for more severe principles : they are used in non-routine tasks and sometimes in high-stress situations, so the understanding of written instructions may be degraded and the design of such procedures must compensate for losses in this ability.

METHODOLOGY FOR IMPROVING PROCEDURES

We used a similar approach for test procedures and for emergency procedures. Nevertheless, there was one main difference : for emergency procedures (steps 1, 2, 3), three independant groups of experts were consulted.

Step 1 : we observed the operators at work in order to know their difficulties in using existing procedures.

Step 2 : we chose to consult the operators in order to better analyze the user requirements. In some cases, we developed a test based on the principles underlying how the procedure should be presented.

Step 3 : we wrote different models of procedures.

Step 4 : we tested the efficiency of these models on training simulators for emergency procedures and on actual plants for test procedures.

Step 5 : we selected the "best" model or we combined the different models in a synthesis model.

Step 6 : we validated this last model.

Step 7 : we elaborated guidelines for preparing procedures.

We give some examples to illustrate the steps 2, 3 and 4.

In order to illustrate the second step, the user requirements for test procedures are given in figure 1. We see, for example, that eighty per cent asked for a breakdown between action and checking.

In order to illustrate the third step, three kinds of models for test procedures are given in figure 2. In the first model, we have done no breakdown between action and checking. In the second model, we have done a breakdown with different columns : the first one for action and the second one for checking. In the third model, we have done a breakdown with different symbols : ➡ for action and ◎ for checking. When we tested the efficiency of those models on actual plants (step 4), we found that the "best" model was the third one.

MAIN PRINCIPLES FOR DESIGNING PROCEDURES

. "Educational procedure" and "procedure for action"

If the procedures are viewed as training material, additional information, such as narrative explanations and descriptions, is needed. It provides context information for performing the actions prescribed by the procedure.

On the other hand, too much information in the procedure could encumber the use of a procedure, particulary during an emergency. As a general rule, it is better to separate training materials from procedures, since each of them has a different function and can be designed to better serve this function if separate documents are used ; so, for every test procedure and for every emergency procedure, we write two kinds of documents :

- a "procedure for action",
- an "educational procedure".

The "procedure for action" document must stay in the control room and must be used when a test is performed or during an emergency.

The "educational procedure" must stay out of the control room (i.e. in the room allocated to education) and must be used for a better understanding of the different instructional steps of the "procedure for action".

. Organization of the contents of procedures

We now give some examples of the different principles which have to be followed for organizing the contents of procedures.

- To ensure the immediate availability of information for the performance of operator actions, all critical information must be provided by a single self-contained procedure. In particular, it is necessary to avoid cross - referencing in procedures.

- The amount and kind of information provided by the procedure must be complete with respect to the needs of the user. On the other hand, too much information can create possible rejection of procedures by users. For emergency procedures, it is very important to evaluate the "level of detail" of the procedure by observing the operators training at the simulator.

- Procedures usually imply different main steps. For example, after a safety injection, an operator has to :

  1 - check the automated actions,
  2 - perform diagnosis by identifying the type of emergency,
  3 - perform immediate corrective actions,
  4 - perform delayed actions.

We then elaborate a diagnostic procedure for steps 1 and 2 and an emergency procedure for steps 3 and 4.

We give an example of the diagnostic procedure and particularly of the decision tree : cf. figure 3.

. Coordination of crew responses

The findings from several observations of operator training at the simulator underlined the need for more structured coordination of crew responses to emergencies. This would reduce the number of errors in communication and in omission of actions which currently result from relatively unstructured, uncoordinated crew responses.

When communication between personnel is needed, the procedure must specify how and to whom, and it must be clear from the way the instructions are written that one person is responsible for coordinating the activity.

For emergency procedures, we elaborated two kinds of documents :

- one document for coordinating the procedure actions,

- several documents for performing actions (one document for the actions performed on the primary circuit, one for those performed on the secondary circuit, and another one for actions performed outside the control room).

For test procedures, we elaborate two other kinds of documents :

- one document used in the control room for performing actions in the control room and for coordinating these actions with those performed outside the control room,

- several documents for performing actions outside the control room ; we design one document for each location.

An example of the document used in the control room is given in figure 4. The actions to be performed by the other users outside the control room are printed in a distinctive type face.

MAIN PRINCIPLES FOR WRITING PROCEDURES

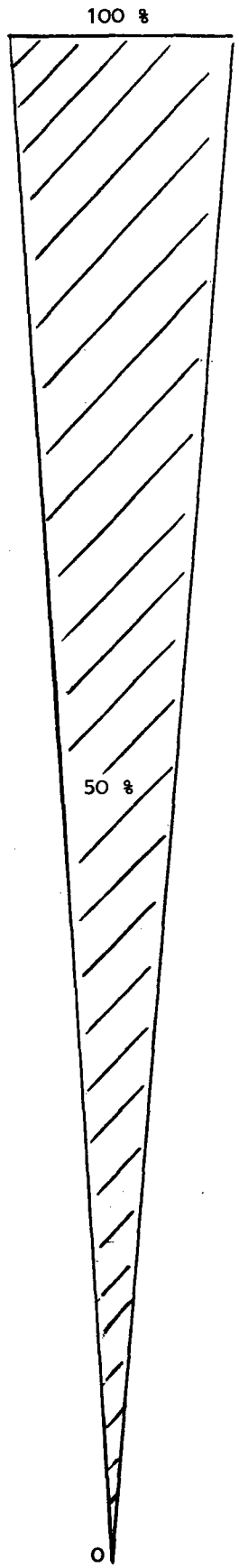
We do not develop in this paper the different principles as regards the choice of :

- vocabulary and sentence structures,
- tables for recording data,
- graphs,
- diagnostic tables,
- flow charts, etc.,

because these principles are given in many papers. Nevertheless, let us illustrate our approach by presenting in figure 5 the "best" graph of standard states which we selected by observing and interviewing operators.

CONCLUSION

To conclude this paper, let us insist on one complementary action which is necessary to improve the behaviour of the operators : the use of procedures for the training of the operators. Indeed, when the procedures are used for training as well as on-the-job application, they also contribute to the development of job skills. For emergency procedures, training must be performed on simulators. For test procedures, training must consist of on-the-job experiences, with lesser skilled personnel working with experienced personnel in progressively more responsible activities.



- One document for each operator with a complete version for the person in charge.
- Clear breakdown between action and checking.
- Use of simplified schematic diagrams.
- Directions about communication during execution and about which person is to perform each action.
- Indication of what the user should do if he obtains an abnormal system response.
- Clear identification of the location of the equipment to be worked on (when it is outside the control room).
- Distinction between educational procedure and procedure for action.
- Use of headings giving the goals of each phase.
- Identification of each step by a number.
- Clear association between actions to be performed and system response (feedback) to be checked.
- Use of a distinctive type face for the actions to be performed by the other users.
- Clear identification of stop, stand by, going on.
- Identification of equipment in the control room.

FIGURE 1 : USERS REQUIREMENTS FOR TEST PROCEDURES

FIRST MODEL

N°	OPERATIONS	LOCATION	RESULT
	Ⓒ START - UP – Start up pump unit ASG 001 PO (Train A) – Check that pump unit flows in : GV 1 GV 2 GV 3 – Return the two trains to zero simultaneously – Check that the regulating valves are closed : ASG 012 VD ASG 014 VD ASG 016 VD		

SECOND MODEL

N°	ACTION	CHECKING	LOCATION	RESULT
	Ⓑ START - UP			
	– Start up pumps unit ASG 001 PO (train A)	– Pump unit flow in : GV1 GV2 GV3		
	– Return the two trains to zero simultaneously	– Regulating valves are closed : ASG 012 VD ASG 014 VD ASG 016 VD		

THIRD MODEL

N°	OPERATIONS	LOCATION	RESULT
	Ⓑ START - UP		
S 12	Start up pump unit ASG 001 PO (Train A) ⊙ Pump unit flow in : GV1 GV2 GV3		
S 13	Return the two trains to zero simultaneously ⊙ Regulating valves closed : ASG 012 VD ASG 014 VD ASG 016 VD		

FIGURE 2 : MODELS PRESENTED TO OPERATORS

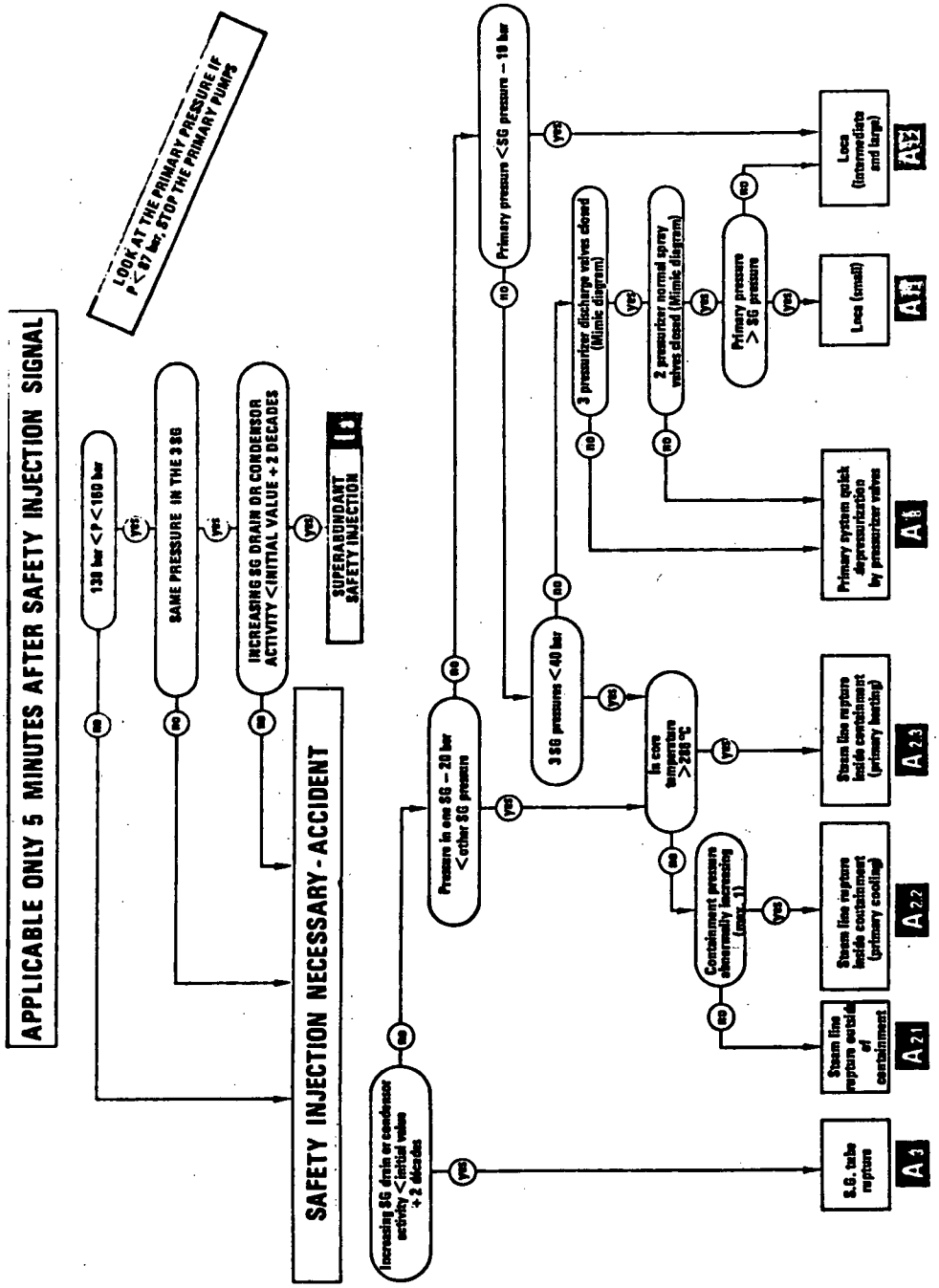


FIGURE 3 : DECISION TREE OF THE DIAGNOSTIC PROCEDURE

N°	OPERATIONS	LOCATION	RESULT
	Ⓒ MEASUREMENT OF OPERATING PARAMETERS		
	WAIT UNTIL ALL READINGS HAVE BEEN TAKEN IN THE BAN		
L. 9 L.10 L.11 L.12 L.13 L.14	• *Exterior pump vibration* • *Pump vibration on motor side* • *Motor vibration on pump side* • *Exterior motor vibration* • *Line flow at minimum flow* • *Pump suction pressure*	ASG 001 PO	
	Ⓓ STOP		
S19	Stop pump unit ASG 001 PO (Train A)	ASG 202 TL	DONE
	◎ Regulating valves completely open : ASG 012 VD	501 AA	DARK
	ASG 014 VD	503 AA	DARK
	ASG 016 VD	505 AA	DARK

FIGURE 4 : MODEL ALLOWING A COORDINATION OF CREW

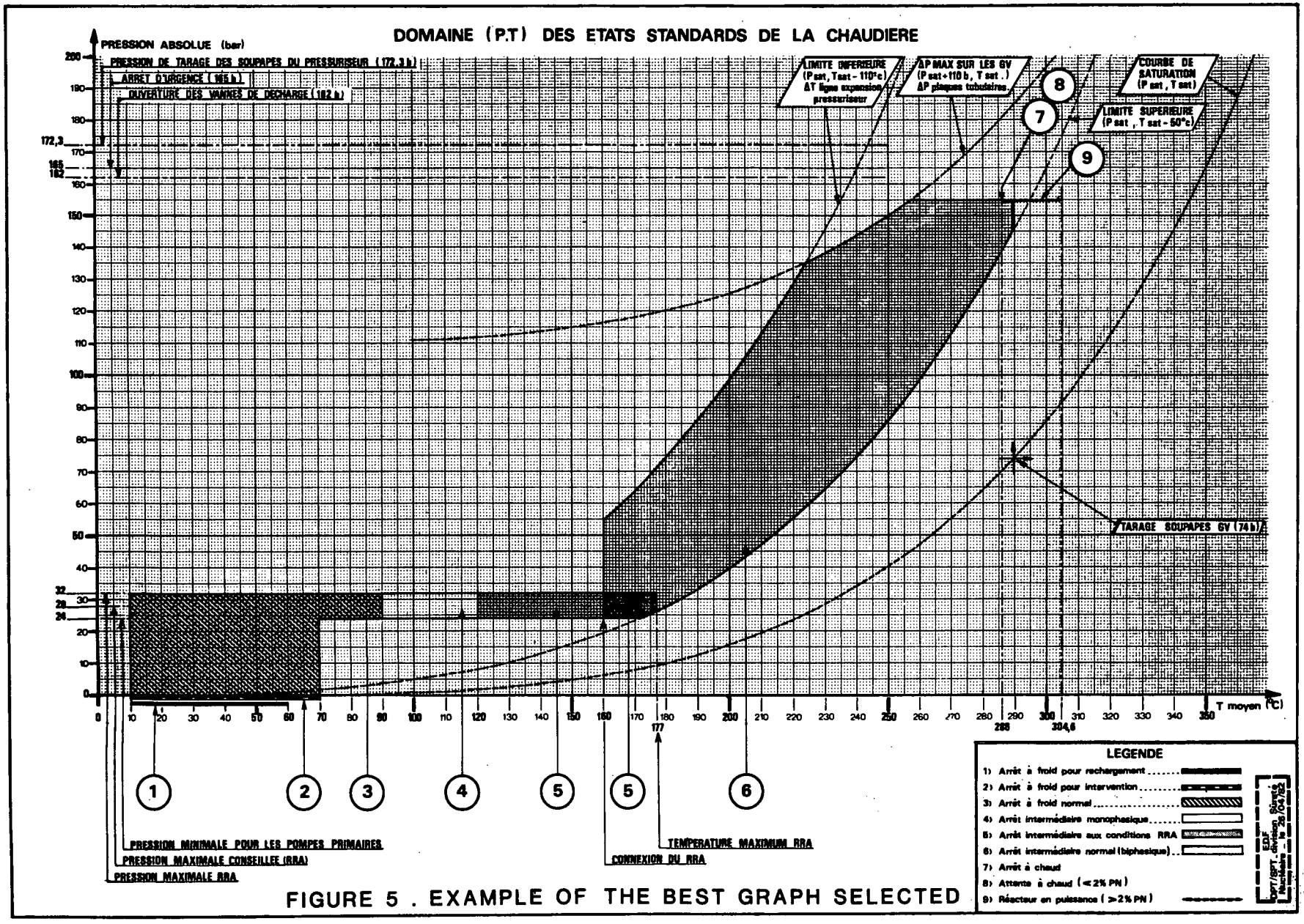


FIGURE 5 . EXAMPLE OF THE BEST GRAPH SELECTED

SURVEY OF HOW PRAs MODEL HUMAN ERROR

E. M. Dougherty, Jr.

Technology for Energy Corporation
One Energy Center, Pellissippi Parkway
Knoxville, Tennessee 37922

ABSTRACT

Human error is recognized as an important contributor to the risk of a nuclear power plant. WASH 1400 was the first probabilistic risk assessment (PRA) that had to account for human error. Subsequently, PRAs have begun to widen their view of the role of an operator in risk-relevant scenarios. Ten published PRAs and the methods of two PRAs currently in process were reviewed to identify the kinds of human errors being assessed. Most risk relevant human errors (55%) seem to require an operator's acting only partially supported by procedure. These errors—called cognitive—are often conceived to happen during an operator's attempt to recover plant systems which fail or to achieve plant functions in alternate ways. More recent PRAs exhibit techniques that are different from those of WASH 1400 to model risk-relevant human errors. The need to handle such errors is clear, but promising techniques are only now emerging and must use judgment to overcome a paucity of data.

A STATEMENT OF THE PROBLEM

WASH 1400 [1] was the first PRA of commercial nuclear power plants (NPP) and had to account for the potential of human error to add to system unavailability or to exacerbate a progressing accident. WASH 1400 used a Technique for Human Error Rate Prediction (THERP) that had been developed in the early 1960s and became the basis of the Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications [2] (1278 for short) issued in 1980.

The title of 1278 gives away the problem in assessing human error. PRA is first a machine-reliability analytical tool. It uses fault trees and other tools of the reliability trade. Humans do make errors and, on first analogy, human error may be thought of as akin to machine failure. But this analogy breaks down because human behavior is self-corrective and innovative--sometimes for benefit, sometimes not. Uncertainty in pump failure data usually accounts for limited sampling or lack of resources to characterize the data. Pumps (of a specific kind, manufacturer, etc.) are considered to behave alike. People, however, show distinct differences in

behavior across any population, and, more importantly, show considerable individual differences. Uncertainty in human error data exists because of these differences; further, some behavior may not be quantifiable.

More important than data issues, perhaps, are the differences in modeling human error versus machine failure. A fault tree of a pump is a bookkeeping device. This device begins with a statement like "the pump will not start on demand if . . .", and then disassembles the pump failure into its constituents, such as lack of lube oil, lack of AC power, a racked-out breaker, etc. THERP attempts a similar disassembly for human error.

In the military, where THERP originated, many human actions are "by the book"--fully regimented, if not explicitly proceduralized. THERP depends on this fact and models human action by its progress through a procedure. Error is defined as not doing what the procedure says to do (plus making an effect on system performance). Here the human action is disassembled using the tool of task analysis. The problem for PRA is that procedure following may not be the way plant operators really act, particularly under the stress of severe accidents postulated in PRA.

ROLE OF THE OPERATOR

It is instructive to examine PRAs and see just what sort of "error situations" are postulated under potentially risk-important conditions. PRA, in fact, prescribes a certain role for the NPP operator (where operator is used to mean a variety of people: reactor operator, maintainer, shift technical advisor, etc.). Table I lists a sampling of human errors identified in 12 PRAs published or near completion. There is a wide spectrum of plants studied--PWRs and BWRs, all four vendors, some older plants, and some recent licensees.

One distinction in the human errors listed is when the error occurs relative to the accident. Some errors happen before the initiation of an accident--during routine tasks, such as testing, maintenance, or calibration, under routine conditions. These are called latent errors because their system effect is a partial (e.g., component) unavailability or because the system is not called to service immediately after the error. Their effects lie dormant (i.e., are latent).

Other errors are more intimately connected with the accident sequence under study. Time is a crucial factor--the plant state is changing, possibly rapidly. The error under these conditions is dynamic, not necessarily because of human characteristics but because of the situation. Dynamic errors modeled in PRAs are of at least three kinds. At the onset of an accident, or off-normal plant condition, the operator needs to diagnose what's going on (procedures usually say "verify"), then do something about it (i.e., control the plant through manual actions in the control room), and, under those rare times when initial responses fail, recover. One problem with this scheme is that diagnosis may be needed at several times during the accident (in fact, diagnosis is probably a continuous, or recurrent process). Furthermore, it is not clear-cut just when manual (execution) errors become recovery errors.

The dimension that begins to distinguish recovery errors from manual errors, and maybe even diagnosis from verification, is procedural support. For example, a procedure will say "transfer to recirculation water supply upon the low level alarm in the injection supply." Under optimal conditions, there really is no need for thinking about the action. The alarm comes on; the transfer should be simple. Except the reactor vessel is losing its water, or the whole plant has lost vital AC power, or an earthquake has started the incident. These situations are the main ingredients of PRAs.

To accommodate the real (although rare) events postulated in PRA, operators must conceivably use their own wits (cognition) rather than follow "the book." Cognition is the key to managing an accident. This third dimension, procedure vs. cognition--is also displayed in Table I. It should be noted that the recently drafted NREP Procedures Guide [3] recognizes this final distinction and partitions the human error assessment tools accordingly--THERP is used with procedural errors, other recently developed techniques are used with cognitive errors.

HUMAN ERRORS IN PRA

Ten PRAs were reviewed [1, 4-10], and a sample of human errors was chosen for any of these three reasons: (1) they were part of a sequence with high risk or high frequency of core melt; (2) they were like events of the preceding kind but for plant-specific reasons their sequences were not dominant; or (3) they were interesting because of human factors.

The errors in Table I are grouped by four categories: the plant function that fails because of the error (e.g., emergency core cooling injection), the accident phase (i.e., latent vs. dynamic), the operator's role (verification, manual, recovery), and the mode of behavior (procedural or cognitive). This classification is based on judgment and the documentation for the error. The categories are not intended to be independent.

The errors show some trends (see Table II). Fifty-five percent seem to be cognitive, or at least not routine enough to depend solely on procedure. Forty-two percent of the errors were judged to be recoveries. An important observation is that 85% of the errors were dynamic. Latent errors rarely seem to be risk-important relative to dynamic errors.

Another trend concerns the probabilities of the errors (called human error probabilities [HEPs]). Most (75%) dynamic errors are assessed with HEPs greater than the greatest HEP assessed for latent errors--3×10^{-3}. Furthermore, most (76%) recovery errors have HEPs of at least 10^{-2}.

All recovery errors were considered to involve (predominantly) the cognitive mode of behavior. However, some cognitive errors (24%) were not judged to be recoveries. Table III characterizes these eight errors. Error 10 is a borderline case: the error arises when the operator tries to use the proper procedure but becomes confused. At such time, the operator is surely behaving without procedural support but not so surely by his wits. Errors 2 and 3 attempt to account for the Three Mile Island (TMI)-type event of turning off a safety system. Error 17 reverses the situation and assesses turning on the system too early. Errors 11 and 21 may be proceduralized but require the operator's cognitive wherewithal as well. In each case, some failure to understand the plant's state must be postulated to make the error plausible. TMI, in this view, was a cognitive error induced by training deficiencies--not a procedural error.

THE MODELING ISSUE

NUREG/CR-1278 is both a collection of human error data and a model (THERP). The NREP Procedures Guide suggests neither is completely sufficient; and the recent PRAs seem to come to the same conclusion. Table IV compares the different methods used in the PRA of 12 plants. The WASH 1400 and RSSMAP plants are both grouped. Both the PRA of Oconee (OPRA), sponsored by the Nuclear Safety Analysis Center, and the PRA of Susquehanna are still underway.

Table I

A Sampling of Human Errors from PRAs, Their Type and Assessed Probability

	Plant		Type			Assessed
PRA	Type	Error Description	Phase	Role	Mode	HEP
		Emergency Core Cooling-Injection (ECCI)				
1. OC	PWR	Operator fails to start ECCI during transient without scram	D	M	P	$1x10^{-1}$
2. CR	PWR	Operator prematurely stops ECCI, given large LOCA	D	V	C	$5x10^{-2}$
3. "	"	Operator prematurely stops ECCI, given small LOCA	D	V	C	$4x10^{-3}$
4. OC	PWR	Miscalibration of actuation system for ECCI (high pressure)	L	-	P	$3.2x10^{-5}$
5. OPRA	PWR	Miscalibration of actuation system for ECCI (high pressure)	L	-	P	$4x10^{-4}$
6. L	BWR	Miscalibration of four level sensors	L	-	P	$2x10^{-3}$
7. OPRA	PWR	Maintenance leaves water source valves closed	L	-	P	$2x10^{-5}$
		Recirculation of ECC or Decay Heat Removal (DHR)				
8. S	PWR	Operator fails to transfer water sources	D	M	P	$3x10^{-3}$
9. "	"	Operator fails to switch water output to hot legs	D	M	P	$3x10^{-3}$
10."	"	Operator confused by procedure for ECCR	D	V	C	$1x10^{-5}$
11. OC	PWR	Operator fails to "piggyback" high pressure ECCR to low pressure	D	M	C	$3x10^{-3}$
12.		Operator fails to open sump (water source) valves	D	M	P	$3x10^{-3}$
13. B	BWR	Operator fails to switch to recirculation	D	M	P	$1.4x10^{-2}$
14. PB	BWR	Operator fails to start heat exchanger cooling water for ECCR	D	M	P	$1x10^{-4}$
15. CR	PWR	Operator fails to initiate recirculation	D	M	P	$3x10^{-3}$
16. "	"	Operator makes an error in switching to ECCR	D	M	P	$8x10^{-2}$
17. "	"	Operator switches to empty sump (i.e., initiates ECCR too early)	D	V	C	$5x10^{-2}$
18. Z	PWR	Operator fails to achieve high pressure recirculation	D	M	P	$2.4x10^{-4}$
19. OPRA	PWR	Operator fails to attain high pressure ECCR, 2 hrs	D	M	C	$3x10^{-3}$
20. "	"	Operator fails to attain high pressure ECCR, 12 hrs	D	M	C	$3x10^{-4}$
21. "	"	Operator fails to throttle ECCR flow during large LOCA	D	M	C	$3x10^{-3}$
22. SEQ	PWR	Maintenance leaves containment compartment drain closed, isolating the water sources for ECCR	L	-	P	$3x10^{-3}$
23. OC	PWR	Maintenance leaves ECCR test valves in wrong state	L	-	P	$3x10^{-3}$

Table I (continued)

	PRA	Plant Type	Error Description	Type Phase	Role	Mode	Assessed HEP
24.	PB	BWR	Maintenance leaves ECCR support water valves unrestored	L	-	P	$2x10^{-5}$
25.	OPRA	PWR	Maintenance leaves sump valves open	L	-	P	$3x10^{-4}$
			Emergency Secondary Feedwater (EFW)				
26.	CAL	PWR	Operator fails to remotely initiate EFW	D	M	P	$1x10^{-3}$
27.	"	"	Operator fails to restore EFW in 30 min following its loss	D	R	C	$1x10^{-1}$
28.	OPRA	PWR	Operator fails to recover main or EFW, given only one option	D	R	C	$5x10^{-1}$
29.	"	"	Operator fails to recover main or EFW, given three options	D	R	C	$1x10^{-1}$
30.	OC	PWR	Operator fails to recover EFW	D	R	C	$1x10^{-1}$
			Depressurization				
31.	OC	PWR	Operator fails to start feed and bleed with ECCI and power operated relief valve (PORV)	D	R	C	$1.5x10^{-2}$
32.	"	"	Same as 31 but under failure of scram	D	R	C	$1x10^{-1}$
33.	Z	PWR	Operator fails to obtain feed and bleed, following loss of EFW	D	R	C	$1.3x10^{-4}$
34.	"	"	Same as 33 but with loss of off-site power, on-site available	D	R	C	$1.3x10^{-4}$
35.	"	"	Same as 33, following steamline break	D	R	C	$4x10^{-3}$
36.	"	"	Same as 34, but with failure to scram	D	R	C	$4x10^{-3}$
37.	CR	PWR	Operator fails feed and bleed, with loss of all EFW	D	R	C	$1.4x10^{-2}$
38.	OPRA	PWR	Operator fails to go to feed and bleed	D	R	C	$1x10^{-2}$
39.	GG	BWR	Operator fails to manually initiate automatic depressurization system (ADS)	D	R	C	$1.5x10^{-3}$
40.	PB	BWR	Operator fails to manually activate ADS	D	R	C	$1.5x10^{-3}$
			Other Recoveries				
41.	GG	BWR	Non-recovery of lost offsite power, one-half hour (partly human)	D	R	C	$2x10^{-1}$
42.	"	"	Non-recovery of lost offsite power, 28 hours, given above	D	R	C	$1x10^{-1}$
43.	CAL	PWR	Failure to restore offsite power in 8 hours	D	R	C	$1x10^{-1}$
44.	"	"	Same as 45, given successful EFW	D	R	C	$3x10^{-2}$
45.	"	"	Failure to restore diesel generator in 8 hrs	D	R	C	$7x10^{-1}$
46.	"	"	Failure to restore power for ECCI or PORV, 1 hr	D	R	C	$2x10^{-1}$

Table I (continued)

	PRA	Plant Type	Error Description	Type Phase	Role	Mode	Assessed HEP
47.	CAL	PWR	Failure to restore power for ECCI or PORV, 3 hr	D	R	C	$1x10^{-1}$
48.	"	"	Operator (or hardware) failure to close PORV, given power available	D	R	C	$1x10^{-1}$
49.	B	BWR	Operator fails to suppress fire, given it is detected	D	R	C	$1x10^{-1}$
			Generic Events				
50.	GG	BWR	Operator fails to restore maintenance faults or take other corrective action in 28 hr	D	R	C	$2.3x10^{-1}$
51.	B	BWR	Operator fails to close circuit breakers, procedure available but vague, sufficient indicators	D	M	P	$1x10^{-1}$
52.	"	"	Operator performs action for which there is no reason	D	-	-	$1x10^{-4}$
53.	"	"	Operator fails to open motor-operated valve or start pump, procedure available, location familiar, moderate stress	D	M	P	$2x10^{-3}$
54.	"	"	Operator fails to return valves or components to service	L	-	P	$1x10^{-3}$
55.	L	BWR	Operator fails to manually initiate one auto safety system following reactor trip	D	M	P	$2x10^{-3}$
56.	"	"	Operator erroneously turns off an emergency system	D	M	P	$1x10^{-3}$
57.	"	"	Operator fails to initiate normal plant function following plant trip, 20 min	D	M	P	$2.5x10^{-1}$
58.	"	"	Same as 57, 2 hr	D	M	P	$2.5x10^{-2}$
59.	"	"	Operator fails to open single manual valve in 30 min	D	R	C	$3x10^{-2}$
60.	"	"	Operator fails to ensure correct lineup of 2 manual valves	D	M	P	$1x10^{-4}$

Legend

PB - Peach Bottom, RSS
S - Surry, RSS
SEQ - Sequoyah, RSSMAP
OC - Oconee, RSSMAP
GG - Grand Gulf, RSSMAP
CR - Crystal River, RSSMAP

CAL - Calvert Cliffs
OPRA - Oconee, NSAC
Z - Zion
L - Limerick
B - Big Rock Point
L - Latent

D - Dynamic
V - Verify
M - Manual
R - Recover
P - Procedural
C - Cognitive

Table II

Percent Human Errors by Class and HEP

	No.	Percent
Total events	60	-
Events judged cognitive	33	55
Events judged recovery	25	42
HEP at least 0.1	14	56
HEP at least 0.01	19	76
HEP at least 0.001	24	96
Events judged dynamic	51	85
HEP at least 3×10^{-3} (out of 51)	38	75
Events judged latent	9	15
HEP no more than 3×10^{-3} (out of 9)	9	100

Table III

Cognitive Errors That Were Not Recoveries

Event	Characteristic
2, 3	Premature termination of a system
10	Procedural confusion
11	Deviation from design
17	Premature initiation of a system
19, 20	Failure due to confusion, distraction, or complexity
21	Nonstandard requirement

Table IV

Differences in PRA Approaches

PRA	Technique			Level		Data		Time Curves
	THERP	Modified	New	FT	ET	I278	Judgment	
WASH1400	H			H	L	H	L	L
RSSMAP		H		H	L	H	M	L
OPRA*		M	H	M	H	M	H	M
Zion		H		M	H	M	H	L
Big Rock		H	M	H	M	H	M	M
Limerick		H		H	?	H	M	M
Crystal River	M	M		H	L	H	M	L
Susquehanna*			H	?	H		H	H

Legend

H - used extensively, dominates approach
M - moderately used
L - seldom used, or not at all
? - not determinable from documentation
FT - errors in fault trees
ET - errors in event trees

*Not published as of July 1982

Four factors were identified as differentiating the PRAs: (1) the general human error modeling technique, (2) the level at which human errors are most frequently modeled in the PRA, (3) the data source used, and (4) the extent to which time curves are used to quantify human error. Each of these are briefly discussed below.

Techniques

All PRAs use insights from NUREG/CR-1278, but most modify them significantly or use different, ad hoc methods. The Crystal River PRA used the THERP event trees but included diagnostic events not handled in 1278. RSSMAP PRAs generally just borrowed from the HEPs of WASH 1400, applying them to similar events. The Grand Gulf RSSMAP PRA, however, added several recovery errors not used in WASH 1400. The Susquehanna PRA and OPRA used THERP least.

Level

WASH 1400 quantified human errors within the fault trees of various systems. Susquehanna developed event trees called operator action trees [11]. OPRA [12] and Zion developed event tree support logic that included operator actions in a fault tree format which was above the system level. The trend toward a higher level of incorporation of human events reflects the concern for the common-mode nature of human errors that influence more than one system. The higher level guarantees more visibility and forces the human error assessment to consider the full sequence circumstances.

Data

NUREG/CR-1278 is a large data bank built from non-nuclear sources and judgment. The PRAs used this data but often further used judgment (i.e., application of 1278 is not strict). OPRA and Susquehanna used 1278 data least directly, relying on systematic judgment more often.

Time Curves

There is a growing body of evidence [13] that human tasks can be put in broad categories and characterized by a response time curve (to a first approximation). Response time curves are being used more in PRAs and are recommended for cognitive error behavior by the NREP Guide. All PRAs used this concept somewhat, with Susquehanna using time curves for all dynamic errors.

CONCLUSIONS

PRAs need to assess the human element as it relates to plant risk but are constrained by limited techniques. Even so, human error has been shown to significantly contribute to risk and certainly human interaction has been a key ingredient in actual events like TMI, the Browns Ferry fire, and the Ginna tube rupture. Human errors modeled in recent PRAs are more cognitive than in WASH 1400, i.e., they at least partly assume the conditions of failure lie outside of procedures. Most human errors found significant by PRAs are dynamic, whereas latent errors are not significant unless they affect more than one system.

The techniques used to assess human error are rapidly evolving--including operator action trees, response time curves, and efforts to identify recovery potential. A key issue is whether the assessment and its techniques fairly model an operator as diagnostician, controller, and manager of the plant, particularly during the plant's greatest potential challenges. Another issue is whether human error data can be

obtained for cognitive behavior. Simulator studies suggest that response times may be useful interim sources of data [14]. But until and unless data can be obtained for operator actions in scenarios like those postulated by PRA, then the systematic application of expert judgment will still play a key role in quantifying human error [15].

REFERENCES

1. Reactor Safety Study, WASH 1400, U.S. Nuclear Regulatory Commission, Washington, D.C. (Oct. 1975).

2. A. D. SWAIN and H. E. GUTTMANN, Handbook of Human Reliability Analysis With Emphasis on Nuclear Power Plant Applications, NUREG/CR-1278, Sandia National Laboratories (Oct. 1980).

3. R. A. BARI, et al., National Reliability Evaluation Program (NREP) Procedures Guide, NUREG/CR-2815, Draft, Brookhaven National Laboratory (June 1982).

4. Reactor Safety Study Methodology Application Program: Sequoyah #1 PWR Power Plant, NUREG/CR-1659/1 of 4, Sandia National Laboratories (Feb. 1981).

5. Reactor Safety Study Methodology Applications Program: Oconee #3 PWR Power Plant, NUREG/CR-1659/2 of 4, Sandia National Laboratories (May 1981).

6. Reactor Safety Study Methodology Applications Program: Calvert Cliffs #2 PWR Power Plant, NUREG/CR-1659/3 of 4, Sandia National Laboratories (May 1982).

7. Reactor Safety Study Methodology Applications Program: Grand Gulf #1 BWR Power Plant, NUREG/CR-1659/4 of 4, Sandia National Laboratories (Oct. 1981).

8. Crystal River - 3 Safety Study, Vol. 1 - Main Report, NUREG/CR-2515, Science Applications, Inc. (Dec. 1981).

9. Consumer Power Company, Probabilistic Risk Assessment, Big Rock Point Plant, Volumes I-VII (March 1981).

10. Probabilistic Risk Assessment, Limerick Generating Station, Philadelphia Electric Company, Docket Nos. 50-352 and 50-353 (March 1981).

11. J. WREATHALL, "Operator Action Trees (OATs) Method", Conference Record of IEEE Standards Workshop on Human Factors and Nuclear Safety, Myrtle Beach, South Carolina, Aug. 30 - Sept. 4, 1981.

12. L. M. POTASH, et al., "Experience in Integrating the Operator Contributions in the PRA of Actual Operating Plants", Proc. International ANS/ENS Meeting on PRA, Port Chester, NY, Sept. 20-24, 1981

13. J. R. FRAGOLA, Systems Approach to Human Error Probability (SHEP) for Nuclear Power Generating Station Risk Assessment Applications, SAI/NY R82-7-8, Draft, Science Applications, Inc. (July 1982).

14. R. M. HAAS and T. F. BOTT, Criteria for Safety-Related Nuclear Plant Operator Actions = A Preliminary Assessment of Available Data, NUREG/CR-0901, Oak Ridge National Laboratory (July 1979).

15. D. E. EMBREY and R. E. HALL, "Quantification of Human Performance Using Performance Shaping Factors," Proc. International ANS/ENS Meeting on PRA, Port Chester, NY, Sept. 20-24, 1981.

DYNAMIC HUMAN OPERATOR MODELLING BY THE ESCS ANALYSIS TECHNIQUE

A. Amendola, CEC-JRC, Ispra, Italy
G. Reina, Studio-MESA, Milano, Italy

ABSTRACT

The actions of reactor operators are determined by complex interactions of perception and diagnosis mental processes with the time evolving aspects of physical signals. Therefore an adequate modelling of operator intervention, including recovery possibility, requires dynamic techniques, such as ESCS (Event Sequence and Consequence Spectrum). As an application example, the paper presents a study case related to an interfacing system LOCA in a PWR. Identification of critical timings for operator interventions and recovery, possibility of probabilistic quantification of incident developments and consequences, optimization of procedures and man-machine interfaces can be the major results of such kind of analyses.

1. INTRODUCTION

One of the main uncertainty sources in nuclear reactor safety assessment is the difficulty of correctly describing human interactions with the systems. Increased awareness of this problem led to various proposals of human models, and specific researches on human factors by using simulators. Nevertheless, the proposed models are still unsatisfactory since they do not properly take into account the interaction of the operator with the time evolution of the physics of the system.

Indeed, as far as the reliability models are concerned, two important different roles have been ascertained for the "operator" [1], namely execution of test and maintenance procedures, and control of reactor incidental occurrences.

In the first case, static models, such as those until now proposed [2] can well be used, especially when recovery possibilities during maintenance are properly modelled [1]. In the second case, static analysis methods can no longer be used for incident developments in which an important role is played by the man-system interaction.

Indeed, in this case not only the failures but also the timings of operator interventions and possible recovery are of the utmost importance. Recovery capability is a very dynamic process which depends upon logical and intuitive mental processes, guided mostly by written procedures and interacting with signals changing during the transient according to the physical evolution of the system. The correctness and timing of operator responses are also strongly affected by stress factors, which in turn depend on the diagnosis made, e.g. recognition of the possibility that an incident may rapidly evolve into a serious accident.

These considerations demonstrate the need for a new analysis methodology, able to process and synthesize the information on the physics of the process, on the component fault analysis, on human behaviour under normal and stress conditions, in a dynamic modelling of the man-system interaction, which may allow the analyst to:

- perform overall a priori risk analysis;
- determine critical operator response timings;
- correctly understand the mechanisms of operator intervention;
- optimize the information which must be given to the operator to allow early diagnosis and recovery;
- optimize incident procedures.

To this end we investigated by a study case the adequacy of the dynamic ESCS technique (Event Sequence and Consequence Spectrum) to deal with such problems.

2. THE ESCS TECHNIQUE

The basic outline of the methodology has been extensively described elsewhere [3, 4], and will be here only shortly summarized.

A system is described by a set of component models obtained by a quantitative failure mode and effect analysis resulting in analytical relationships characteristic of each component state. In these models step functions can be used to represent response of on-off components (switches, alarms, etc.).

In addition to these analytical relationships, the logical states of a component (nominal, failed and degraded) are suitably introduced by means of event variables. Thus, the whole system is synthetically represented in all its possible conditions by a set of parametric equations which contain both logical and physical information. The appropriate relations are selected by parametric operators, according to the event sequences generated by the analysis procedure.

The physical consequences of a generated event sequence are obtained by the numerical solution of the corresponding equation set. Only those sequences which satisfy a pre-assigned quantified TOP condition (e. g. the occurrence of a pressure above a certain value or within a certain interval, together with certain specified temperature values), are selected and logically analysed to extract the minimum ones, so that, in some way, minimum TOP sequences correspond to the cut sets of the usual fault-tree approach. As appropriate to the dynamical nature of the problem, minimum TOP sequences are determined with respect to the complete time pattern of the variables considered [5].

The corresponding DYLAM computer code [5] evaluates also the probability distribution of the TOP conditions investigated as a function of the transient time. In doing this both statistical and functional failure dependences (common mode) can be taken into account. It ought to be stressed that the functional dependency consideration is made possible just because of the step-by-step evaluation of physical variables during the transient time.

3. OPERATOR INTERVENTION STUDY CASE

The study case is derived from the analysis of a particular LOCA in a PWR, in which a check valve failure provokes a break in the low-pressure injection system, outside the primary containment [6].

In such an occurrence no water is available in the recirculation sump; the operator is asked to avoid or at least to delay as far as possible melting of the core by carrying out the following sequential emergency actions:

1) manual activation of the high pressure injection system (HPIS) at the minimum flow so that the available water in the emergency tank is injected as slowly as possible;
2) switch off the low pressure injection system (LPIS), which would be automatically called upon to operate as the pressure decreases below a certain threshold, and in this case would only waste water;
3) attempt to close the isolation valve up-stream of the LPIS.

From the previous description it can be seen how the timings of the operator

interventions can dominate the incident development.

Each error or delay, indeed, may provoke a waste of the water available in the emergency tank and recovery is possible only if allowed by residual water in this tank.

4. SYSTEM MODELLING

Since the study was essentially directed towards the development of a proper model for the human operator, the physical problem has been strongly simplified (Fig. 1). In particular, to obtain a much simpler equation set, we replaced the core by a tank, whose voiding timings are of the same order of magnitude as the real core melting. Eventually, to deal with the real case, it would be possible to apply Response Surface Methodology that permits to substitute complex computer models by simple analytical expressions.

Table I shows the model that has been adopted for the primary tank component. The event variable SBK logically simulates the break-size distribution. The choice of a specific value for break-size "A_B" is made by means of the parametric operator OSBK, that controls the physical equations for the break flow-rate "Q_{OUT}".

At the beginning of the study, also the number of signals (Fig. 1) available to the operator has been reduced to a minimum, but enough to produce coherent operational procedure assumptions; and, it was asked to the analysis to assess the quality of operator strategy assumptions and man-machine interface.

In addition to the break-size distribution, the following component failure modes have been considered:

- for the sensors: "fails high" and "stuck";
- for the automatic primary level control system: "stuck";
- for the pumps: "stuck";
- for the LPIS isolation valve: "blocked open": this condition has been considered to be in statistical common mode with the break towards LPIS, and namely the larger the break size, the larger the valve blockage probability.

5. OPERATOR INTERVENTION MODELLING

Figure 2 shows the basic logic of operator intervention general modelling. In this scheme the moment of incident initiation and the first analysis process have been represented as the trigger for successive loops: actions $\rightleftharpoons$ system evolution where operator actions are followed by a system reaction which is monitored on the man-machine interface. The model can consider both prompt and delayed diagnosis and error recovery as a result of decision control processes, check lists, delayed systems responses, etc. In each task all possible errors have been considered (i.e. omission, commission, etc., see taxonomy in ref. 7) and also discretized distributions for reaction times have been included.

In this modelling it is not needed to a priori imagine all possible dynamical sequential actions as it would be required by conventional techniques. Indeed the entire operator-system interactions are described by a set of parametric equations that by themselves contain all the required dynamic information, without pursueing by logical reasonings all the actions an operator can do during the time. In this way, the technique is able to simulate the real human interventions: the operator has access to a spectrum of simple and individual possible actions (procedure tasks) and nearly only the dynamic evolution of the accident determines how and when the operator must intervene.

These tasks have been assumed to be as follows:

a) General Procedures and Actions

- In case of a diagnosis of break towards the primary containment, the operator

is not called into operation, since he must rely on the automatic control system. But, he is asked to verify his judgement (see diagnosis and check procedures).

- In case of a diagnosis of break towards LPIS, the operator must refer to the emergency procedures, and perform the three actions described at point 3. A diagnosis check has been foreseen (see diagnosis and check procedures) between the initial action and the two last ones. The operator is asked to perform actions 1 and 2 before action 3, since there is no certainty of isolation success and in this case voiding is at least delayed.

b) Diagnosis and Check Procedures

- The operator is alerted by the signal of level in the primary tank below a first threshold l_1 which is also the trigger for HPIS automatic start-up.
- By means of level and flow-rate sensors, he is able to evaluate the break-size on the basis of a flow-rate balance.
- A first diagnosis is performed at this time by means of the reactivity sensors to locate the break.
- In all doubtful cases (failed sensors) the operator assumes the more probable event (primary break).
- Diagnosis check is performed as LPIS starts (level below a second threshold l_2)on the basis of a new flow-rate balance, as compared with the previous one.
- The correctness of manual HPIS insertion (Emergency action 1) is verified by a check on HPIS flow-rate sensor.

c) Recovery Procedures

- In case that the diagnostic check makes the initial operator judgement to change, the operator switches to the appropriate general procedures and actions (delayed recovery example).
- In case of wrong insertion discovered by the check on the flow-rate sensor, the operator can recover on the right HPIS flow-rate (prompt recovery example).

6. SIMULATION LOGIC

The resulting simulation logic is constructed as follows:

- at time t_o the alarm appears (primary level below l_1; alarms are described by step functions);
- at time $t_1 = t_o + \tau_{al}$, the alarm situation is recognized by the operator in which τ_{al} is a distributed operator perception delay. If τ_{al} is ∞, then the operator has not perceived the alarm at all;
- at time $t_1 + \tau_{syst} + \tau_d$, a first diagnosis is made by the operator. τ_{syst} is a time, characteristic of the system evolution, which can allow the diagnosis (e.g. in our case, this is the time necessary until radioactivity increase in LPIS local can be measured), τ_d is a characteristic of the operator's readiness ($\tau_d = \infty$ operator confused, not able to formulate a diagnosis);
- the diagnosis results in the decision to perform a certain number of actions (e.g. actions 1 to 3 in the procedure mentioned above). An action timing delay τ_i is associated with each of these actions. The distributions assumed for τ_i can simulate either the non-performance of some of the actions envisaged, or the inversion of the order prescribed by the procedure;
- the check points allow the operator to check his diagnosis against the development of the signals and, therefore, reverse his action (a new distributed delay is assumed for recovery).

The choice of time response distributions can be governed by stress factors that are originated by the recognition of the risk. To investigate the adequacy of the methodology to probabilistically take into account stress factors, we introduced in the model a statistical dependency between the size of the break and the distribution

of the diagnosis timing. Moreover a functional s-dependency has been introduced to consider that the time for closure of isolation valve is statistically dependent on the quantity of water flooded into the LPIS local.

7. RESULTS AND CONCLUSIONS

DYLAM results can be exploited in different ways: indeed, it evaluates:

- minimum event sequences leading to given TOP condition pattern. In our case a TOP condition could be "time course of primary vessel level";
- probability that a TOP condition is attained at certain times after incident initiation (in our case probability that vessel level goes below a certain value at time t_x);
- probability that the initial state of components affected by failure functional s-dependences change during the transient time;
- physical evolution of the simulated event sequences.

In a different ESCS application [3] we stressed the extent of DYLAM probabilistic results. In this paper we want to focus the attention on the physical aspects of the analysis that may be very relevant for system optimization, even when lack of data does not permit reliable probabilistic predictions.

Figure 3 shows the primary level behaviour in the case of a large break towards LPIS, failure of reactivity sensor in LPIS local, and nominal behaviour of all other components including operator.

The operator is aware of a LOCA occurrence by the level monitoring, but the failure of the sensor does not allow him to locate it. The more probable event is thus initially assumed, i.e. primary break. At the LPIS starting time, the diagnosis check permits recovery that is successfully accomplished.

Figure 4 shows the situation for a small break towards LPIS in nominal conditions and in the case when the operator performs a correct diagnosis but actuates 2 HPIS pumps instead of only one and recovers this failure. In the second case it can be seen how even if the operator corrects his action in a short time, the result is a very amplified delay, due to the increased time interval for reaching the LPIS start (Diagnosis Check).

It is evident that this check is of paramount importance in cases such as shown in Fig. 3, but it can be detrimental in other cases (Fig. 4). This result led to a modification (now in execution) in the study-case system modelling for which the diagnosis check on the flow-rate balance after LPIS insertion is eliminated, but further sensors are added that should permit more adequate diagnosis and recovery possibilities. The basic operator model does not, however, need to be changed. But just this result shows how the method is able to optimize procedures and design of man-machine interfaces. Moreover it would permit to quantify the risks (including operator failures in diagnosis, actions and recovery under stress factors inherent to the diagnosis performed) if reliable probabilistic data for operator behaviour were available. On the other hand, reliable data can be obtained only when models are well established.

As a last remark, basic ideas of the presented operator model could be usefully implemented into complex codes for incident analysis, to get more detailed safety assessments. Moreover they offer also a correct framework for exploiting man-machine interaction by research simulators.

REFERENCES

1. A. Amendola et al., "Dynamic and static models for nuclear reactor operators: Needs and application examples", in Proc. of IFAC/IFIP/IFORS/IEA Conf. on Analysis, Design and Evaluation of Man-Machine Systems, Baden-Baden, FRG (1982).

2. A. D. Swain and H. E. Guttman, "Handbook of human reliability analysis with emphasis on nuclear power plant applications", report NUREG/CR-1278 (1980).

3. A. Amendola and G. Reina, "Event sequences and consequence spectrum: A methodology for probabilistic transient analysis", Nucl. Sci. Eng: 77, 297-315 (1981).

4. A. Amendola and G. Reina, "ESCS, A new approach to dynamic systems safety", Proc. of ANS/ENS Int. Top Mtg. on Advances in Mathematical Methods for Nuclear Engineering Problems", München, FRG (1981).

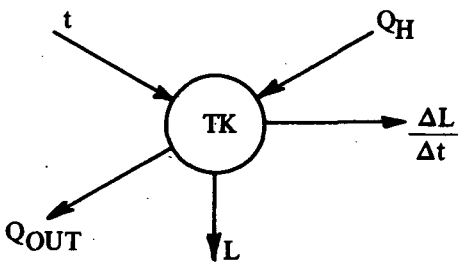
5. G. Reina and A. Amendola, "DYLAM: A computer code for event sequences and consequence spectrum analysis", Proc. of Int. ANS/ENS Top. Mtg. on Probabilistic Risk Assessment, Port Chester, N. Y., (1981).

6. J. Van Herman, R. Brown and A. Tome, "Light water reactor status monitoring during accident conditions", report NUREG/CR-1440 (1980).

7. G. Mancini et al., "Classification system for reporting events involving human malfunctions", report EUR 7444 EN, JRC-Ispra (1981).

TABLE I - PRIMARY TANK MODEL

INPUT-OUTPUT QUANTITIES



t	=	transient time
Q_{OUT}	=	break flow-rate
Q_H	=	HPIS flow-rate
L	=	tank level
$\frac{\Delta L}{\Delta t}$	=	level decrease rate

PHYSICAL BEHAVIOUR

$$Q_{OUT} = \mu A_B \sqrt{2gL}$$

$$L(t + \Delta t) = L(t) + \frac{1}{A_Z} (Q_H - Q_{OUT}) \Delta t$$

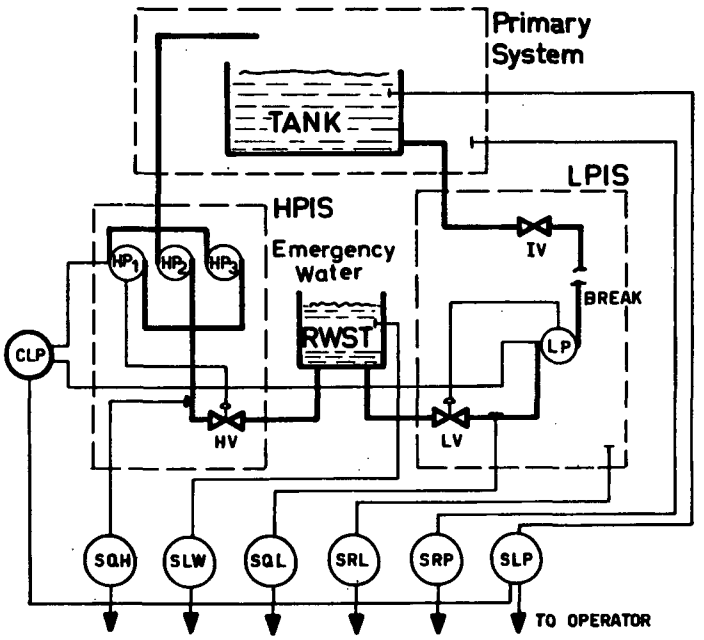
$$\frac{\Delta L}{\Delta t} = \frac{1}{A_Z} (Q_H - Q_{OUT})$$

A_B	=	break area
A_Z	=	tank cross section

FAILURE MODE AND EFFECT ANALYSIS

Different Break Sizes — SBK:
- 0 no break
- 1 small break (A_{BS})
- 2 medium break (A_{Bm})
- 3 large break (A_{BL})

$$A_B = OSBK (SBK;\ O, A_{BS}, A_{Bm}, A_{BL})$$



SLW = RWST level sensor
SQL = LPIS flow-rate sensor
SRL = LPIS radioactivity sensor
SRP = Primary radioactivity sensor
SLP = Tank level sensor
CLP = Tank level controller
SQH = HPIS flow-rate sensor

Fig. 1 - Simplified System Modelling.

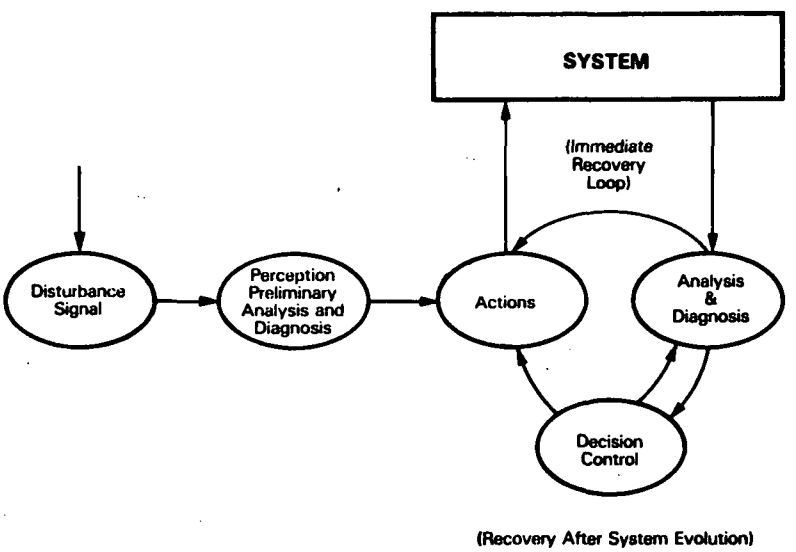
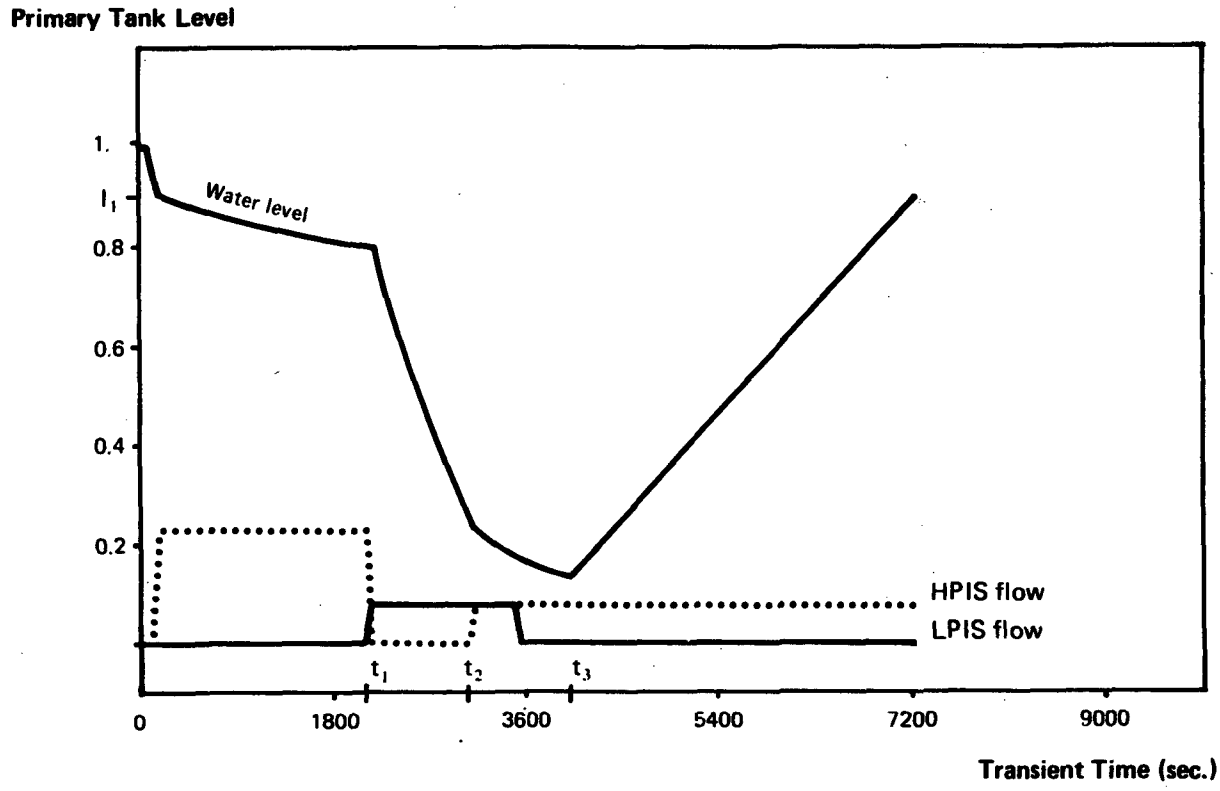
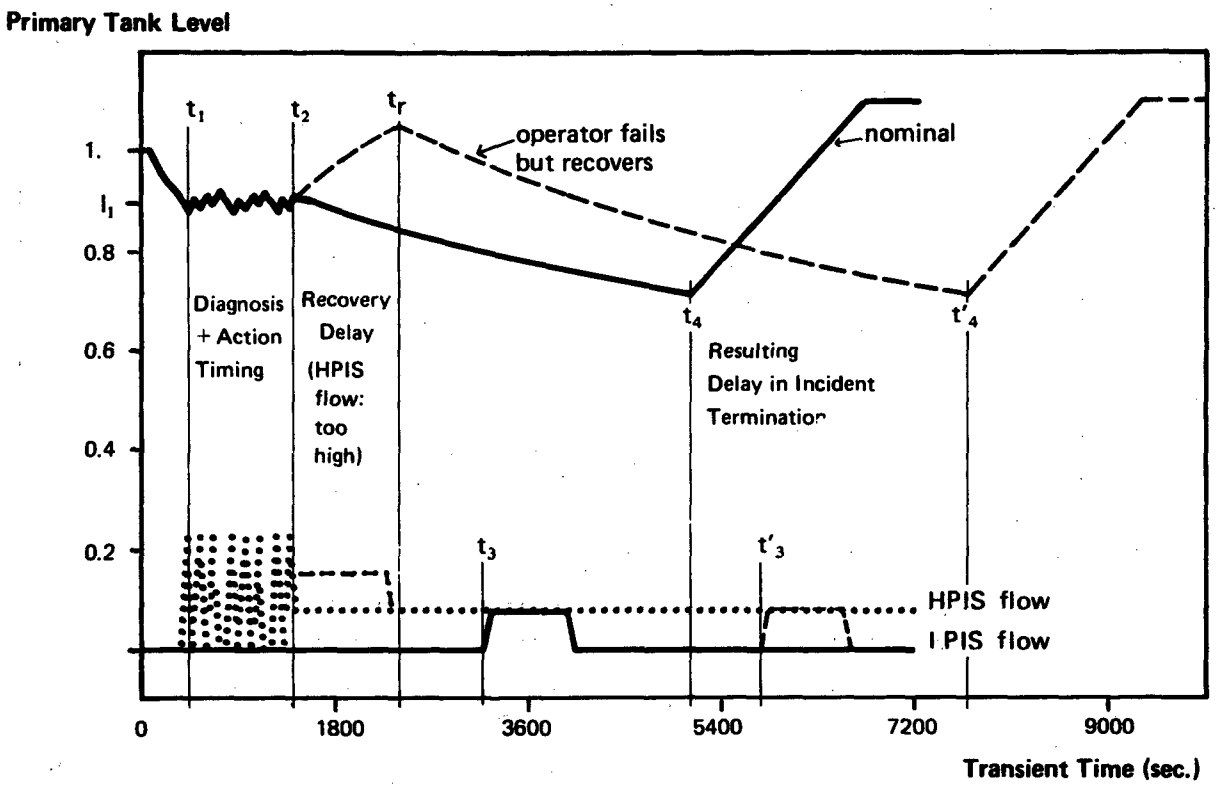


Fig. 2 - Dynamic Operator Modelling Scheme



- Until time t_1 due to SSRL1 failure, the break has been located by the operator in the primary containment.
- At time t_1 diagnosis check allows operator to recover.
- At time t_2 the right procedure is followed.
- At time t_3 isolation valve is closed.

Fig. 3 - Case of Large Break towards LPIS Local and Failure of its Reactivity Sensor. Operator Acts Correctly and successfully.



- t_1 = timing of first diagnosis
- t_2 = timing of first action
- t_3 (t'_3) = timing of diagnosis check
- t_4 (t'_4) = timing of break isolation
- t_r = timing of recovery (correct HPIS flow)

Fig. 4 - Case of Small Break Towards LPIS Local:

- nominal case
- operator fails in inserting min. HPIS flow but recovers

SESSION 10

MAN/MACHINE INTERFACE - 2; MACHINE SIDE

Chair: J. H. Hopps *(CSDL)*
E. Yaremy *(AECL)*

Panel Discussion on

MAN/MACHINE INTERFACE: HUMAN FACTORS AND MACHINE SIDE

Chair: E. Yaremy *(AECL)*

Panelists

R. Capel *(EdF)*
J. H. Hopps *(CSDL)*
R. W. Lindsay *(ANL)*
A. Long *(EPRI)*
Z. Sabri *(LPL)*

INTEGRATED OPERATOR/PLANT INTERFACE DESIGN IN CANDU NUCLEAR POWER PLANTS

T.O. McNeil and N. Yanofsky
Atomic Energy of Canada - Engineering Company
Mississauga, Ontario

A B S T R A C T

CANDU Nuclear Generating Stations exhibit the world's highest availability figures. This is credited, in part, to on-line refuelling, and a high degree of automation. In CANDU stations the refuelling sequences, and the overall plant regulation (including control of reactivity, heat transport system steam generators, and turbine) are supported by a highly reliable computer system. The computer control system permits CANDU designers to take full advantage of computer driven colour graphics for control room annunciation, logging, and information display. Computer colour graphics provide flexible, concise, comprehensive information to the operator in formats which enhance rapid interpretation. The high degree of automation performed by the computers minimizes the number of manual controls needed on the main control panels. Fewer controls, and extensive use of colour graphics reduce the clutter of instrumentation on these panels, giving more freedom to the designer to logically place the operator's control devices.

INTRODUCTION

Nuclear generating stations are complex plants of sophisticated design. Despite a high degree of automation in CANDU stations, the operator is still required to monitor the operation of the plant and take corrective actions during abnormal situations. Each generation of plant design has been characterized by increased quantities of instrumentation to provide a more detailed picture of the state of the plant such that the station can be controlled safely and reliably from the control room. This trend has presented the operator with the problem of sorting and assimilating the increasing amount of information. It has presented the designer with the problem of simplifying the operator's task.

The CANDU approach is to centralize the operation of the plant and to reduce the complexity of control panel instrumentation. This has been achieved by utilizing the station computer system, used for plant control, to perform a significant role in the control room. The use of the computer is coupled with good design practice which has catered to the needs of the operator. This has resulted in the present integrated operator/plant interface.

The evolution of the operator/plant interface began at Douglas Point, the first commercial prototype CANDU-PHW station which went into service in 1966. At Douglas Point all instrumentation is located on standup panels arranged in an arc about the the operator's desk. The panel layout is arranged with instrument devices and control devices grouped to facilitate operator control. There are no sophisticated displays installed at Douglas Point.

The Pickering A and Gentilly-1 stations started up in 1971. These were the first CANDU stations in which the control computers played an important role in the display of key plant parameters to the operator. At Gentilly-1, two computer driven CRT's are provided in the control room, an alpha numeric display for alarm messages and a vector type graphic display for process variable presentation. At Pickering A, the panel instrumentation is organized to permit the operator to readily locate and correlate information. The control panels are laid out on a system basis with meters grouped near the top of the panel to facilitate scanning and manual controls located on the desk section. Mimic diagrams incorporating these manual controls on the panels were extensively used.

The advent of relatively inexpensive raster scan displays with graphic capability allowed the next step of replacing many of the conventional panel instruments. This was implemented on the Bruce 'A' station which started up in 1976. Each Bruce 'A' unit has two monochromatic CRT monitors for annunciation and eight monochromatic CRT monitors with associated function select keyboards for information presentation.

The 600 MWe CANDU stations, the more recent design, use colour CRT monitors to take advantage of colour coding techniques and to simplify display interpretation.

This paper will describe the present approach implemented on the 600 MWe stations with particular emphasis on how changing technology and a better understanding of the operator's needs has made it possible to provide a simplified integrated operator/plant interface.

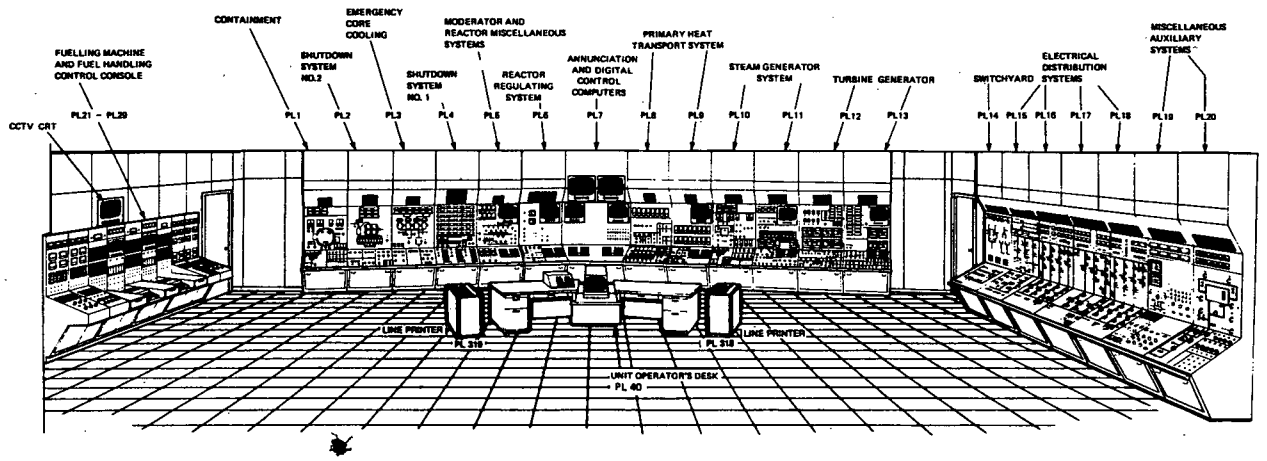
The Control Centre

In CANDU stations, the Control Centre is the focus of all operations activities. It consists of the Main Control Room, the Work Control Area, and the Control Equipment Room.

The Main Control Room centralizes the operation of both the nuclear steam supply and balance of plant. Monitoring and control of most functions is handled from this one location. The control equipment required for those systems is located in rooms adjacent to the Main Control Room. Access to this equipment is quick and under operator supervision. The daily administrative functions of operating the station are carried out in the work control area next to the Main Control Room. It is close enough to allow easy communication with the station operators, while still separating them from the distractions of normal office activities.

The Main Control Room provides a spacious, pleasant working environment. The panels are arranged to allow unrestricted movement and visibility of major displays from most places within the room. It is illuminated with diffused fluorescent lights of about 80 - 100 footcandle over the operator's desk and approximately 30 footcandles over the main control panels.

FIGURE I - CONTROL ROOM (600MW STATION)



During normal conditions, the operator is seated at a desk supporting a colour graphics information display and two high speed printers. The main control panels surround the desk in an arc, allowing the operator an unrestricted view of all panels. Panels to the right of the operator display and control the regulating systems (reactor, steam generator, turbine-generator). Panels to the left of the operator support the special safety systems (shutdown, emergency core cooling, containment).

Alarm messages, and the computer status, is presented on panels immediately in front of the operator's desk.

CONTROL PANELS

Each panel consists of three parts; a sloping desk section on which is mounted the majority of the manual controls, a vertical section for information display, and an inclined upper section dedicated to annunciation windows.

Manual Controls

CANDU control panels use a 'DARK PANEL' design concept. That is, indicating lamps are used to indicate ONLY discrepancy situations. For example, a pump switch is illuminated, only when the pump has tripped. Valve controls are lighted only when they are in motion.

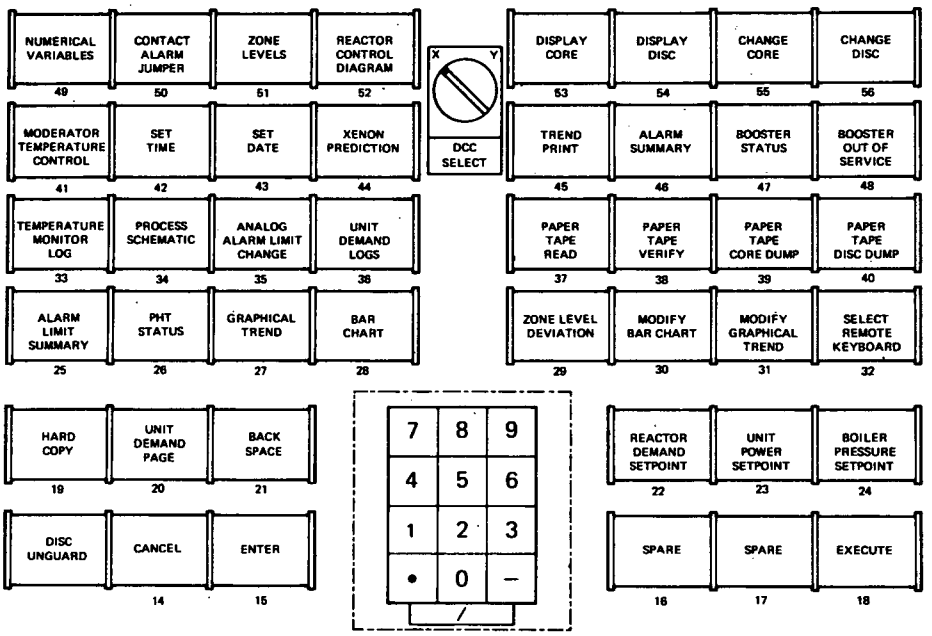
The control surfaces make extensive use of mimic diagrams in which bar type electromechanical indicators are used to display valve, damper, breaker, and reactor control rod positions.

Information Display

The vertical section of the control panels house the information displays. The majority of plant information is provided on eleven, colour graphics CRT screens.

In general, display functions can be grouped into non-interactive and interactive pages. Non-interactive pages present information one, computer to operator. Bar charts, graphic trends, status and pictorial displays are examples of this catagory. Interactive display pages allow two-way communication. These pages support operator changes via keyboard entry (eg., reactor power). As a general rule, keyboard entries are echoed to the operator and are executed by pressing an 'execute' pushbutton.

FIGURE 2 - TYPICAL KEYBOARD



The keyboard associated with each CRT has 44 unique function keys and a 13 button numeric pad. The function keys provide very rapid access to system display pages (less than 1 second). All the system's information pages are accessible on any one display. However, the associated function keyboard on each panel is configured to allow most rapid access to displays supporting that panel's functions (eg., steam generator, reactor).

Colour can be used very effectively to differentiate between classes of data (eg., points in or out of alarm). However colours must be selected carefully taking into account legibility, eye sensitivity of different colours, as well as common engineering practices. For example, green, cyan and yellow are more legible than blue, red or magenta in the NTSC (National Television Standard Committee) colour spectrum. The eye is also more sensitive to these colours.

Colour discrimination deficiencies in operators must also be considered. Approximately 8% of the male population and .4% of the female population have colour vision problems. Displays must be formulated such that colour is not the sole identifier of a state.

Alarm Annunciation

Alarm windows located above the control panels have been used for many years to identify fault conditions. They are very effective in directing attention to the

appropriate control panel but have limited information content, and provide no time sequence information.

CANDU control rooms are unique in their very limited use of overhead alarm windows. The alarm annunciation system uses the windows to provide the operator rapid, global, alarm information. More detailed information concerning the alarm is provided on two alarm message CRT's, and alarm logging printers.

Alarm messages are colour coded to identify the alarm source by system (red - safety, magenta - steam generator, turbine generator, yellow - electrical, green - auxiliary). We have found coloured rows of characters makes it easier for the eye to track across the screen in reading the message thereby reducing fatigue and irritation, and hopefully the probability of error.

Alarms are classified in three groups: (1) safety related; (2) major importance requiring immediate attention; (3) or minor importance requiring attention at the operator's discretion. These alarm priorities are identified by colour coding the alarm status symbol A (red - safety, yellow - major, cyan - minor). When the alarm returns to normal, a blinking green 'N' replaces the 'A'. All return to normal messages can be cleared from the screen by a reset pushbutton.

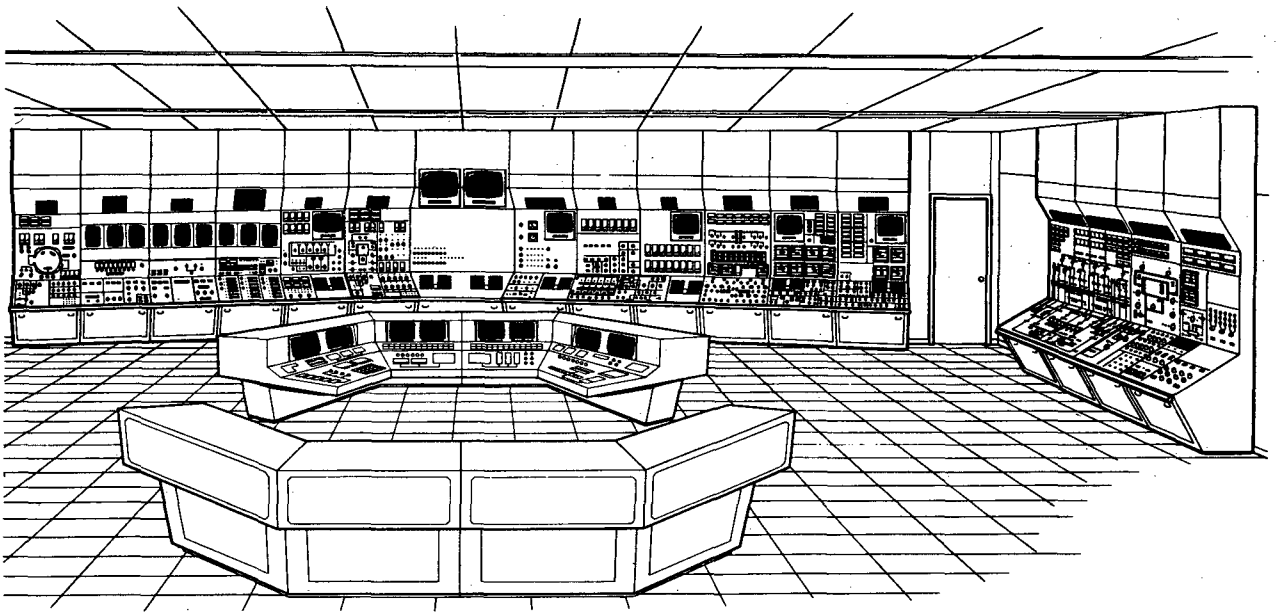
Of course, all changes of alarm state are signaled by audible horns.

During plant upsets, minor alarms are inhibited from the CRT preventing it from being flooded with messages, and hence allow the operator to act on those most important to the station. All alarms, minor and major, are printed and saved on disc for later analysis.

Alarm conditioning is also used to prevent a flood of nuisance alarms. For example, if a power supply is lost, it is alarmed. All associated equipment trip alarms, however are suppressed.

FUTURE TRENDS

FIGURE 3 - CANDU CONTROL ROOM (950MW STATION)



The current trend in control panel design in replacing conventional panel instrumentation with CRT displays, and reducing the number and size of controls is expected to continue. For example, the use of computers, and the associated colour graphics displays will be extended to the special safety systems in addition to the station regulating systems. This trend has been re-enforced by the favourable feedback we have received from operators over the past 11 years. In the future, more attention will be paid to improving data formats, and increasing the data processing role of the computer. Our goal is to further reduce the size of the control area such that the operator can execute all control functions from a compact sit down console, relegating the stand up panels to a back-up mode.

CONCEPTION OF A PWR SIMULATOR AS A TOOL FOR SAFETY ANALYSIS

J.M. LANORE - CEA/DSN - CEN FONTENAY-AUX-ROSES (FRANCE)

P. BERNARD, J. ROMEYER DHERBEY - CEA/DRE - CEN CADARACHE (FRANCE)

C. BONNET, P. QUILICHINI - CISI - CEN CADARACHE (FRANCE)

ABSTRACT

A simulator can be a very useful tool for safety analysis to study accident sequences involving malfunctions of the systems and operator interventions.

The main characteristics of the simulator SALAMANDRE (description of the systems, physical models,programming organization, control desk) have then been selected according to the objectives of safety analysis.

INTRODUCTION

An important consequence of the TMI incident was to emphasize the part of the man-machine interface during an accident sequence, and it is then the post TMI considerations which initiated in the C.E.A. Nuclear Safety Department the notion that a simulator could be a very useful tool for safety analysis.

After a more precise definition of the objectives, a simulator was then conceived in this Department, according to the needs of safety analysis. The development of this simulator (SALAMANDRE) is now in progress, and this paper will present how during the conception the main options have been selected by taking into account the specific objectives of safety analysis.

OBJECTIVES

The interest of a simulator versus a current computer code is that it enables to visualize in real time the dynamic phenomena, with the possibility of an interactive process. The main field of application is obviously the treatment of of man-machine interface problems. Now these problems present two aspects :

- The "man" side of the interface, for which the objectives may be the training of operators, or the study of operator behaviour (assessment of response time, of error probability, etc...).

- The "machine" side, that is the study of the performances requested from the operator by the machine (quantity, rapidity, complexity of actions).

Since the future users of SALAMANDRE are not plant operators but safety analysts, the objectives are necessarily of the second type. SALAMANDRE will then be used for analysing operating actions and failures sequences that can lead to damaged conditions, and best means and operator actions for reaching a safe state. More precisely the planned applications are :

- a priori analysis : analysis of operating procedures, determination of critical delays for operator actions, testing of operator assistance automatic systems.

- a posteriori analysis : analysis of real incidents, parametrical studies with additional malfunctions (what if ?).

Besides, these objectives being not long term research but present problems, the department wished to realize the simulator within the best delays available.

DESCRIPTION OF THE PLANT SYSTEMS

The plant simulated in the first version is a 3 loops Framatome 900 MW PWR (the most current type of plant in operation in France). The 1300 MW PWR version will be realized in a further step.

To study an accident sequence or a procedure, a rather detailed representation of the systems is necessary so in SALAMANDRE all the important circuits and systems, from the point of view of the dynamic behaviour of the plant, are described.

However simplification are introduced in the simulated systems when all the functional modes of the real systems remain possible. For instance :

- redundant components (pipes, valves, pumps...) that never work at the same time are represented by only one component,

- valves used for maintenance are not described.

In a general way the systems which are obviously involved in current safety problems are modelized with an accurate representation :

- Reactor Coolant System (R.C.S.) with 3 loops, Reactor Control Chemistry (R.C.C.), Residual Heat Removal (R.H.R.), Emergency Core Cooling System (E.C.C.S.), Feed Water (F.W.), Emergency Feed Water (E.F.W.), Steam Generator (S.G.), steam flow to the turbine and the feed pumps, steam by-pass to the condenser. All the automatic control system is described.

The systems wich are less directly related to safety are more simplified or treated as limit conditions :

- Recirculation Spray (R.S.), as an enthalphy condition for water in the sumps.

- Intermediary Water System (C.C.W.S.) described as a water flow, at a given temperature, at the inlet of the corresponding heat exchangers.

- Feed Water Reheater System is not described.

- The boration path is simplified the user only indicates the boron concentration and the flow of the added water.

- Conditioning circuits of tanks are not described.

PHYSICAL MODELS

The safety analysts need an efficient and reliable tool, available within a reasonable delay. So, at least in a first step, the physical models selected for SALAMANDRE are rather simple and well known models, widely tested in current physical codes :

- point neutronics,

- 1 dimensional homogeneous two phases flow in the R.C.S. (pipes and core),

- 0 dimensional volumes, one or two phases, thermal equilibrium or not (upper plenum, pressurizer...),

- global calculation of one phase flow in all circuits connected to R.C.S. (R.C.C., R.H.R., E.C.C.S.),

- 0 dimensional secundary part of the S.G., with primary-secundary heat exchange area correlated to the mass of secondary water (to describe the loss of feed water flow),

- simplified description of steam flow in the turbine.

However the programming structure of the code is sufficiently flexible to enable the introduction of more refined models when they are available.

PROGRAMMING ORGANIZATION OF THE CODE

The programming organization of SALAMANDRE is an important aspect of the development. From this organization depends the easiness and the flexibility of the simulator use, and then the wideness of its application field.

General features

SALAMANDRE is organized as a modular code in order to enable future evolutions.

The functions of the processing system are :

- initialization of the simulator in various plant conditions,

- dynamic animation of the simulation,

- files creation and management.

The dynamic part of the simulation is composed of physical independant modules and of a dynamic animation that :

- coordinates the exchanges of informations between the code and the control desk,

- organizes the numerical resolution of the system by iterating on the modules,

- introduces malfunctions in the systems.

Two aspects are particularly developed : the dynamic animation and the introduction of malfunctions.

The dynamic animation of the simulation

To enable the study of complex accident sequences, with parametric variations, the animation of the simulation will offer a wide range of possibilities. The user can :

- stop the simulation at any moment and restart at the same point,

- come back to a previous point of the sequence,

- select a simulated time different from the real time (accelerated or slackened simulation),

- ask for various editions of curves and results either during the simulation (on consols) or after (listings).

These editions can concern all the physical parameters of the simulation, or any combination of these quantities (to follow a balance, for instance).

The introduction of malfunctions in the systems

This function is performed by the A.S.L.(Anomalies Sequences Logic)subroutine. This subroutine enables the user to program several different individual or successive failures sequences that can take place either at a given time or when a logical expression composed with plant parameters is fulfilled. Such sequences can be directly introduced or suppressed on line by the user. Failures can be :

- leaks located at various points of the circuits,

- commanded systems failures (control rods, boron concentration, valves, pumps...),

- limit systems failures (C.C.W.S., tanks...),

- automatic control failures (simulation of sensors wrong signals, control failures..)

CONTROL DESK

Since the objective of the simulator is not the training of operators, a similarity of the control desk with a real control room is not necessary. So the control desk is conceived with the objective of providing all the interesting informations in a clear and simple way, manageable even by a single user.

The simulator is controlled from a control desk mainly composed of a vertical pannel and two consols (fig.1). The vertical pannel describes the system diagram of the simulated plant. Measured parameters are visualized on this diagram at the location of the measurement. Command on a given component (pump, valve...) is done by pushing on a button located on the symbol of the component in the diagram. There also exists a small horizontal pannel for automatic systems control. About :

- 200 digital measurements
- 200 digital commands
- 40 sighting slits
- 60 buttons

are present on the control desk.

The first consol is used for control of the simulation (initialization, ASL programming...). The second one is used for visualizing curves and special parameters that do not appear on the pannels.

SIMULATED SITUATIONS

The SALAMANDRE simulator will describe plant operating conditions from cold, off pressure, subcritical state, to full power conditions for a 3 loops FRAMATOME 900 MW

PWR. An important class of accidents will be accurately described by this simulator.

The limitations of SALAMANDRE are due to the validity of the physical models (one phase or homogeneous two phases flow in the R.C.S.). If the validity limit of the models is reached during a simulation the user will be informed.

SALAMANDRE is not conceived for predicting accidents final consequences (especially on the fuel elements and radioactive releases) but for analysing sequences of accidents and influence of multiple failures and operating actions. Global evolution of the accident transients must be correctly described, even the loss of coolant accidents in the case of small leaks. Detailed computations of some transients could then be performed with more refined codes.

CONCLUSION

The realization of SALAMANDRE is now in progress. A feasability study was completed in June 1981, and the simulator is planned to be operational for July 1983. The main options were selected by taking into account the objectives of safety analysis of accident sequences (especially analysis of operating procedures and of real incidents).

With these characteristics SALAMANDRE is expected to be a useful tool for the safety analysts. A wide use of this simulator will provide an improved knowledge of the accident sequences including the operator interventions, and then it will be an help for improving the safety of PWR plants.

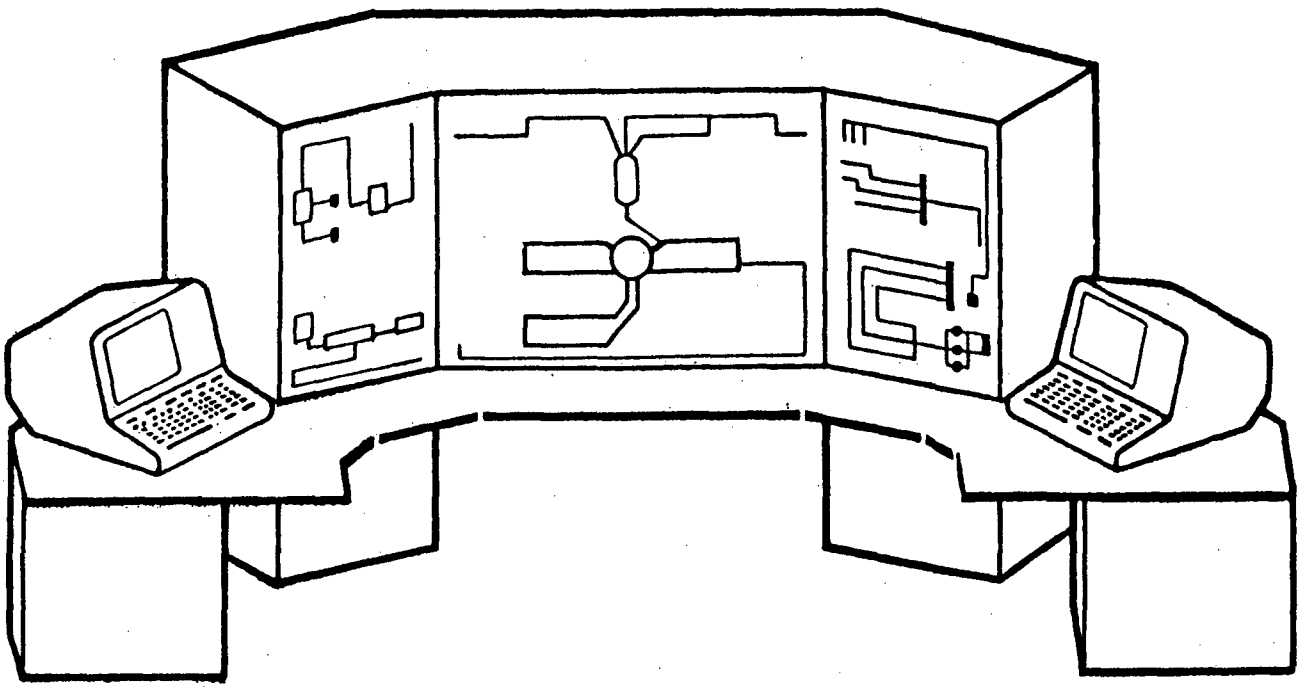


Fig. 1. Control Desk of the SALAMANDRE Simulator

MULTIVARIATE ALARM HANDLING AND DISPLAY

P.J. Visuri

OECD Halden Reactor Project
N-1750 Halden, Norway*

ABSTRACT

Two central aspects in alerting control room personnel about abnormal states in a complicated process are discussed: A method to recognize alarming process conditions and the technique to present the alarms to the operators.

It is proposed that combinations of several process signals should and can be used to form alarms that take into account the status of the whole process. This method is termed multivariate alarming. It can significantly reduce the amount of irrelevant alarms and thus enhance the operator process interface from the situation with conventional alarm systems of today. These consist mainly of establishing individual alarm limits for each process signal.

The multivariate alarming method has been combined with a novel technique for presenting the overall process operating state as well as the alarm status on a single CRT-display. The display consists of a symbolic process diagram applying low-contrast colours for operating state and high contrast colours for alarm status indication. This combination of the methodology and the display concept has been used in developing a computer based alarm handling system for a nuclear plant process.

INTRODUCTION

In order to perform all their tasks as a part of the plants overall control system, the operators of any complicated process need an efficient interface with the process. There has, however, been little systematic development work done in this field compared with the effort applied to automatic control theory. Todays control rooms are often developed by extrapolating methods and techniques that were sufficient for small and simple processes. This is especially true for process alarm systems. The method of establishing individual limits for process parameters and annunciating each limit violation separately is still prevalent in most centralized control rooms. This solution, that was adequate for simple processes, may work satisfactorily during normal operation and minor disturbances even in complicated processes. However, in major upsets the shear number of activated alarms and messages makes it impossible for the operator to perceive the essential information that he would need to supervise the process state. This problem has been especially pronounced in nuclear power plants which have a large number of automatic protection systems that are activated during disturbances. It is unfortunate that the alarm system offers least support to the operators during those situations when his role is most important in maintaining the safety of the plant.

*) Present address: TVO Power Company, Fredrikinkatu 51-53, 00100 Helsinki 10,

Some efforts have been made to relieve this well known problem of alarm avalanche. These include hardwired electronic systems to conditionally inhibit some alarms and logical cause-consequence relations programmed into a disturbance analysis computer with separate alarm messages. Even so, there has never been a theoretical framework that treats the process alarming issue as a whole and offers a basis for development and design of systems with the desired properties. This report aims to provide such a framework. The alarm system is considered as a part of the operator-process interface from both sides: Methods to recognize alarming conditions in the process and the means to transmit this information to the operators efficiently.

ALARMS REFLECTING ABNORMAL PROCESS STATUS

Describing a Process by State Vectors

The status of any process or system can generally be described by indicating the values of certain parameters. These must be selected so that they represent essential variables in the process. By increasing the number of parameters the state of any process can be described with any desired accuracy.

In control theory it is accustomary to arrange the parameters describing a process into an ordered group

$$\overline{X} = x_1, x_2, x_3 \cdots x_n$$

This ordered group of n parameters is called the state vector of the process $\overline{X}$.

By assigning a certain value for each of the parameters x_i we can define a point in the n-dimensional state space of the process. Each point in this space represents a state or a status of the process.

All the points in this general state space are not in reality possible states of the process. For example if a valve is closed, there cannot be a high flow through it. Of all *the possible* process states only a few are *acceptable* from the process operator's point of view. Thus the group of all acceptable states is a true subgroup of all the possible process states which is a true subgroup of all the points in the state space. The acceptable states are the ones that are within the control domain of the plants' control systems for normal operation. Geometrically these states can be represented by an area or possibly a few different confined areas in the state space. These areas represent the *normal operation modes* for the process. Whenever the process state is outside these areas the process is said to be in *a failure mode*. The grey area in Figure 1 represents the normal operating modes of a process.

In high risk process plants, for example in nuclear power plants, there is normally always a protection system to maintain the system under some kind of control even in failure modes. This system has limits for certain process parameters. If these limits are exceeded the system initiates control measures that promptly return the system state inside the ordinary automatic control domain. Unfortunately the state in which the process ends, when the protection system works is often a shut-down. This is acceptable although not desired. The limits and the control actions of a plant protection system are illustrated by solid lines in Figure 1.

The state vector description forms a framework to study changes in process status. The operators' role seen in this framework is twofold: he moves the plant state inside the acceptable control domain area to fulfill the orders from the utility organization. If the plant state for some reason would move outside normal operation into a failure mode, the operator's task is to counteract. Optimally the operator can turn the development of a disturbance to bring the plant back to normal operation before the plant protection system limits are reached and so maintain the plant in the desired operating mode. In the very rare occasions when the plant protection system fails to return

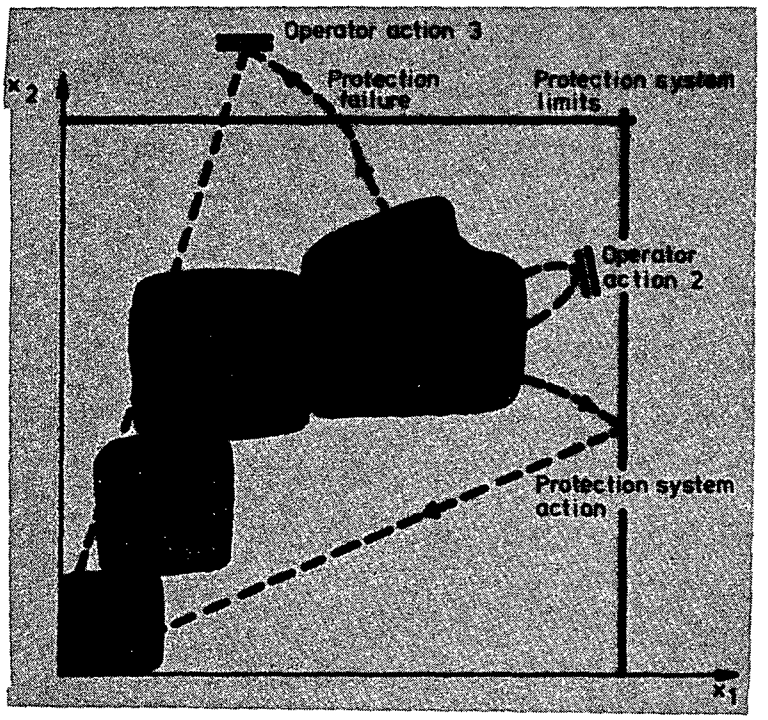


Figure 1. The normal operating modes 1 - 4 of a process represented in a two-dimensional state space $\bar{X} = (x_1, x_2)$. The protection system limits and a protection system action are illustrated. Three different types of operator actions are also shown:

- *Action 1 represents normal operation of the process within the normal operating modes.*
- *Action 2 is a counteraction when the system gets into a failure mode. Before the protection limits are reached, the operator returns the system state into the normal operating mode 4.*
- *Action 3 represents the operators measures when the protection system fails to bring the system into a state even when protection system limits have been exceeded.*

the plant into a safe state from failure mode even after the protection limits have been exceeded the operator's responsibility becomes much more important. He has to take actions to fulfill the tasks of the protection system. See Figure 1 for different types of operator actions.

To be able to take appropriate counteractions the operators should be alerted as soon as the system gets into a failure mode. This gives us a *definition* of a *process alarm*. It *is* a *signal indicating that the process is in a failure mode.*

Single and Multivariate Alarming Principle

It is possible to set individual alarm limits for each of the parameters x_i in the state vector $\bar{X}$. This way there may be two limits a_1 and a_2 for each parameter x_i:

$$a_{i1} \leq x_i \leq a_{i2}, \quad i = 1.....n$$

An alarm will be given if any of the variables x_i goes outside of the alarm limits a_{i1} and a_{i2} set for it.

Since each alarm depends on one variable only we will call this method the *single variable alarming* principle.

Geometrically this means that the alarm limits define for each variable two (n-1) -dimensional (hyper)planes in the state space. The normal operating range of the variable is between these planes. Together all the planes for different variables define an orthogonal "alarm limit box" in the state space. If the process state is outside this n-dimensional box one or more alarms are given out. Figure 2 illustrates this situation.

A simple and natural expansion of this method of setting alarms is to set several limits for each variable. Thus the first limits would correspond to a prewarning and the following limits to alarms of increasing urgency. This would correspond to defining several orthogonal alarm boxes that are inside each others. This is the most

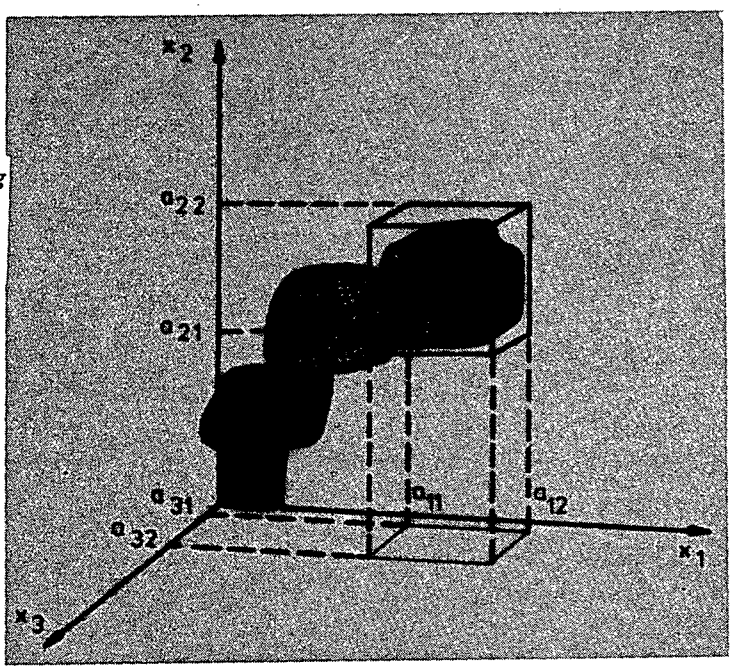


*Figure 2. An ortogonal »alarm box» defined by setting two alarm limits for each of the variables in the state vector $\bar{X} = (x_1, x_2, x_3)$ in a three-dimensional state space. The alarm limits are defined for the operating mode 4. The other three normal operating modes are also shown. The alarm area, for example for alarm 1 (x_1 low), consists of all the points in the state space for which $x_1 \leq a_{11}$. Correspondingly, each of the 6 alarms shown has a semi-infinity defined by the alarm limit as their alarm area. The only points in the state space that do not belog to any alarm area, are in the »box». So for example, for the process state indicated by *I, there would not be any alarms given out. However, for the state *II alarms for »low x_1» and »low x_2» would be given even though this state is in a normal operating mode.*

commonly used method in making alarm systems for process plants today.

In case the process described by the state vectors has several modes of operation, the corresponding areas in the state space can be very irregular. If the alarms are based on only one variable each, only a very regular area with no alarms can be defined. Usually this is chosen to include only the most common operating mode of the process. This results in a great number of standing alarms always when the process status is not in the operating mode that the alarms were defined for, see Figure 2.

There are two ways to avoid standing alarms:

The alarm limits can be set so far from the normal operating values that they certainly will not be exceeded during normal operation. This method is normally applied for setting the limits for the plant protection system (cf. Fig. 1). However, this makes the alarm system insensitive to small process abnormalities and it can not readily alert for failure modes.

The other way to avoid undesirable standing alarms is to make each alarm dependent on more than one process variable:

$a_j = a_j(x_k)$, where $k = 1...m$, $1 \leq m \leq n$, where all $x_k \in \{x_1, x_2, ...x_n\}$. Or in vector notation:

$a_j = a_j(\bar{X}')$, where $\bar{X}'$ is a subvector of $\bar{X}$ containing one or more of the variables x_i of $\bar{X}$.

The alarm limits $a_j(\bar{X}')$ now can each define a general n-dimensional surface in the state space for the process. One surface is defined for each alarm j. The surfaces have to be either closed or infinite. The corresponding alarm is given if the process state is on a predefined side of this surface, in other words if the state is in the corresponding *alarm area* A_j.

By using sets of equations of several variables as alarm limits it is possible to

define the different alarm areas so that they surround the normal operating mode areas in the state space from all sides. The alarm areas may be overlapping. So one or more alarms are always given if the system gets into a failure mode. Figure 3 illustrates the situation.

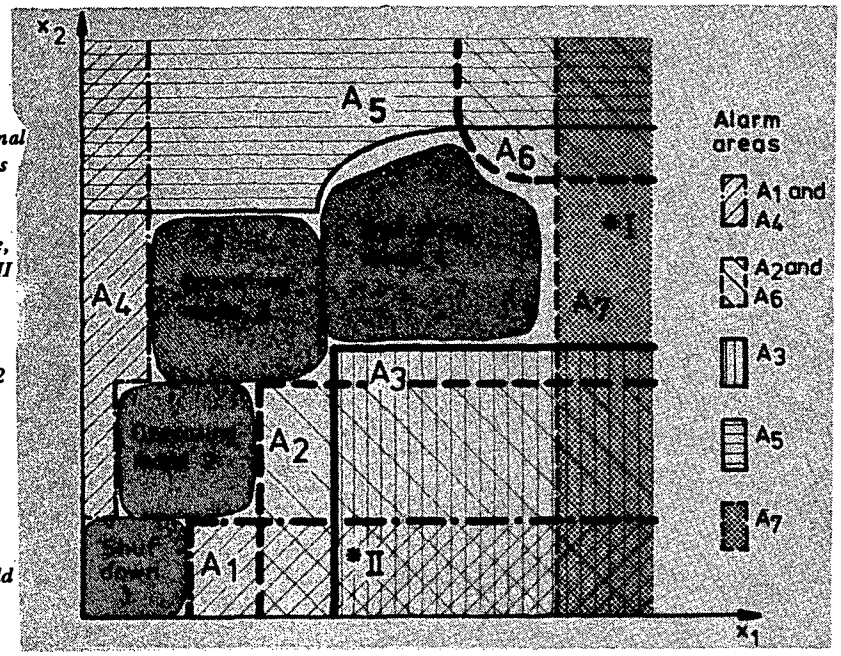


*Figure 3. By using sets of equations of the variables x_i it is possible to define the alarm limits $a_j(\bar{X})$ so that the alarm areas surround the normal operating modes from all sides. Alarm j is always given when the process operating state is in the alarm area corresponding to the limit function $a_j(\bar{X})$. For example for the state *I in the figure, only alarm 8 would be given and for the state *II the alarms 1, 2 and 3 would be given. The alarm limits can in this two-dimensional case be constructed easily by using equations of x_1 and x_2. For example some of the alarm areas in Figure 2 can be defined as follows:*

$$A_1 : x_1 \geq x_{11} \text{ and } x_2 < x_{21}$$

$$A_2 : x_1 \geq x_{12} \text{ and } x_2 < x_{22}$$

Of course any other equations of the variables can also be used. For example, a hyperbole could be used to define the alarm area A_6

Since each alarm in this method depends on several variables we will call it the *multivariate alarming principle.*

The *multivariate alarming* principle is a generalization of the *single variable alarming* method. If $\bar{X}'$ contains only one variable x_i of $\bar{X}$, the corresponding general surface in the state space is reduced to a hyperplane and the alarm area is the semi infinity on the "outside" of the plane. Even the alarm message "x_i has exceeded high/low-limit" is descriptive for the failure modes in that alarm area.

In practice the multivariate alarming means that the alarm system can take into account the general process operating state. Thus for instance a number of low temperature or low flow alarms do not need to be given if the process or parts of it are in a shut-off state. Also an alarm for missing auxiliary feed water flow can be given only in a situation when that flow is needed.

There is a need to include the possibility of having some of the alarm limits to be dependent of time as well as of the state variables in $\bar{X}$:

$$a_j = a_j(\bar{X}', t)$$

Normally the time dependence refers to the way the vector $\bar{X}'$ changes with time, for example to the rate of change of some variables or to the way the vector has changed with time. This is because some points in the state space are acceptable only if they are approached from the right direction. In other words if they have been preceded by certain other states. For example a rapid decrease in the water level in a BWR reactor tank or in a PWR steam generator is acceptable after a reactor scram from high power but can be very alarming in other circumstances. Also the alarm for a low turbine speed is not relevant if the turbine has recently been tripped.

In theory the multivariate alarming principle can be used to define an optimum alarming system for any process. However, if the process state vector $\bar{X}$ consists of

thousands of variables x_i and as there may be hundreds of alarms that are arbitrary functions of these, the amount of information processing becomes excessive with presently available processing techniques. Even if the proper alarm functions could be defined it would be impossible to continuously calculate their values to define which alarms should be given. A simple application is needed.

Simple Application of a Complicated Principle

The variables x_i in the state vector $\overline{X}$ can generally be analogue variables as well as binary signals.

If the range of an analogue variable is divided into a number of mutually exclusive zones, binary signals can be used to indicate the value of the variable.

This kind of division into zones can be done to all non-binary variables in a process state vector. By increasing the number of zones the values of the analogue variables can be given with any desired accuracy. We will use the notation $\overline{B}$ for a binary system state vector and b_i for the binary variables in the vector.

It is clear that the number of binary variables b_i required to describe a process in a reasonable accuracy is much larger than the number of corresponding general variables x_i. So at first it seems that the information processing task for an alarm system gets only worse using binary variables. However, the very nature of an alarm system makes it feasible to divide analogue variables into a low number of zones, and binary variables are especially well suited for efficient computer based information processing.

When the process description is transformed from $\overline{X}$ to $\overline{B}$ the alarm limit expressions $a_j(\overline{X},t)$ also need to be changed. It can be shown fairly easily [1] that it is possible to define any alarm area in $\overline{B}$ by using boolean algebraic expression of the variables b_i of $\overline{B}$.

All variables b_i do not need to influence all alarms j. Significant improvements over todays conventional alarm systems can be expected by using only a few variables b_i as arguments for each alarm.

In addition to being a convenient way of defining alarm areas the boolean algebra is especially well suited for computer based information processing.

As mentioned earlier, time is important for alarm functions for two reasons: For setting limits for rates of changes and for the reason that some process states are acceptable only if preceded by certain other states.

The analogue value for each rate of change needs to be produced by other systems than the alarm system and can be contained in the process vector $\overline{X}$ as any other analogue measurement.

The following method can be used for binary variables for identifying preceding events: A number of binary variables b_{ti} is allocated for each event that has influence to the need for alarms after the event. For example automatic start and trip signals or the reactor scram in a nuclear power station are such events. The values of the variables b_{ti} are all set to 1, when the corresponding event is detected. Then the values are set back to 0 one by one at predefined intervals Δ_{ti}. Now a 1 in the variable b_{ti} indicates that the event has occurred less than the time

$$t = \sum_{j=1}^{i} \Delta t_j \quad \text{ago.}$$

The variables b_{ti} can be used in the binary alarm expressions formally at the same way as any other variables b_i.

We have now reduced the complicated arbitrary alarm limit expressions $a_i(\bar{X}',t)$ of n analogue and/or binary variables and time into boolean expressions of a few binary variables that define the conditions for different alarms. However, these still represent the multivariate alarming principle which differs fundamentally from the conventional one-sensor- one-alarm method or the single variable alarming technique.

PRESENTING PROCESS OPERATING AND ALARM STATUS

Importance of a Good Interface

It is not sufficient that the alarm system recognizes that the process is in a failure mode. This information is useful only when the operator has perceived it. If the process is not a trivial one, it is also important that the operator gets some information of the nature of the failure mode. In this way the alarm system can direct him to the source of further detailed information about the process state and help him to decide on appropriate actions.

It is important that the way of information presentation is adjusted to the requirements for the speed of perceiving it. Also the possibilities for misinterpretations should be minimized. This chapter describes a novel method for presenting alarm information to the control room operators.

Coding of Information in Alarm Presentation

There are generally speaking other more efficient means of coding repeatedly used information than using text. Use of traffic signs along road sides is perhaps the most prominent example of this. The following coding methods are suggested as suitable for use in CRT-presentation [2]:

- colour
- location on screen
- geometrical form of the object
- intensity
- blinking

The function of alarm presentation in a complicated process is twofold: To give the operators an overview of the process status, and to display details of alarm messages for fault diagnostic purposes.

To make it possible to satisfy the conflicting requirements of a fast overview and detailed alarm information, a hierarchical alarm display concept is proposed. This consists of an overview picture, that utilizes other information coding possibilities than text, that is symbols and colours; and a hierarchy of defail pictures where the alarm information is integrated to other process information. In addition the concept includes ordinary alarm text displays.

The overview picture consists of a symbolic diagram that has always the same layout form on the CRT-screen.

In this diagram the process is divided into functionally separate parts. Each part is represented by a symbol that has a fixed position and a specific form on the screen. Figure 4 shows a possible layout for the overview diagram ofa PWR-plant. In this way the properties: *location on the screen* and *form of the object* are used to identify the parts of the process.

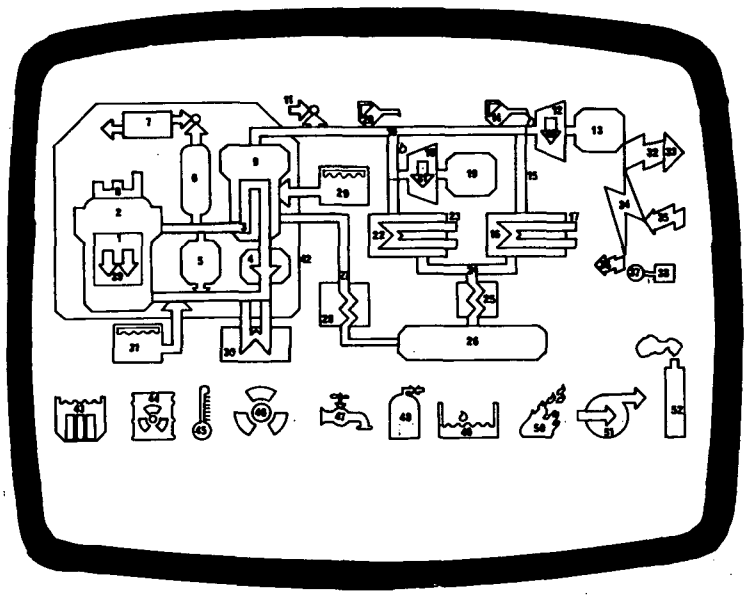


Figure 4. List of suggested alarm groups:

1. *Reactor*
2. *Reactor pressure vessel*
3. *Primary circuit*
4. *Reactor coolant pumps*
5. *Chemical and volume control system*
6. *Pressurizer*
7. *Pressurizer relief tank*
8. *Control rod system*
9. *Steam generators*
10. *Steam lines*
11. *Secondary circuit relief system*
12. *Turbine 1*
13. *Generator 1*
14. *Lubrication system, T-G 1*
15. *Bypass line 1*
16. *Condenser 1*
17. *Cooling water system 1*
18. *Turbine 2*
19. *Generator 2*
20. *Lubrication system, T-G 2*
21. *Bypass line 2*
22. *Condenser 2*
23. *Cooling water system 2*
24. *Condensate system*
25. *Low pressure pre-heaters*
26. *Feed water tank*
27. *Feed water system*
28. *High pressure pre-heaters*
29. *Auxiliary feed water system*
30. *Residual heat removal system*
31. *Safety injection systems*
32. *Main electric power bus*
33. *Main outer grid*
34. *Auxiliary power systems*
35. *Secondary outer grid*
36. *Auxiliary power systems (diesel backed)*
37. *Diesel plant, generators*
38. *Diesel plant, motors*
39. *Scram indication* } *Shown only when function initiated*
40. *Turbine 1 trip* } *Shown only when function initiated*
41. *Turbine 2 trip* } *Shown only when function initiated*
42. *Containment isolation (shown only when func. initia.)*
43. *Irradiated fuel storage systems*
44. *Radioactive waste systems*
45. *High room temperature*
46. *High radiation level*
47. *Process water delivery system*
48. *Pressurized gas delivery system*
49. *Water on the floor*
50. *Fire alarm*
51. *Ventilation systems*
52. *Off-gas systems*

The properties *colour* and *intensity* are used to code the updated information on the overview picture. Two colours from the blue end of the spectrum and of distincly different intensity, for example light blue and dark grey, are used to display the normal operating status of the process [3]. In this method each part of the process that is represented in the overview by a symbol can be in two different normal statuses: "on" or "off". A suitable criterion for choosing one of these is developed for each part. For example steam lines are on when there is flow in them. Turbine is on when running etc.

When an alarm relating to a certain part of the process is given, the corresponding symbol in the overview turns into a high intensity red or yellow depending on the urgency of the alarm. Every possible alarm in the system is related to one of the symbols in the overview picture. Thus an alarm colour in a symbol indicates that one or more of the alarms related to that symbol are active. The alarm colours are superimposed to the background information colours on the display.

The possibility to use *blinking* to transmit information to the operators has been reserved to indicate that new, unacknowledged alarms are present in a process part. When a new alarm is indicated, the symbol on the overview starts semiblinking in the actual alarm colour. At the same time an audible annunciation signal is given. Semiblinking means a slow oscillation between two intensities or tones of the same colour. When the operator acknowledges the alarm, the colour becomes steady.

In addition to the general process operating and alarm status information the operators need detailed information about the alarms as well as the actual values of the different process parameters and the states of the components. The purpose of the detail pictures in the display hierarchy is to provide this information in a consistent way.

In them the alarm information is superimposed on displays each of which shows a part of the process. In a complicated process it may be useful to have more than two levels of hierarchy in the displays.

The alarm text displays form the third way of presenting alarms. These are especially usable for understanding the time development of events when there are not too many alarms activated in a short time interval.

Connection between the Theory and the Praxis

As mentioned in the introduction, the multivariate alarming theory was not derived from mathematical or system theoretical considerations, but has rather emerged from attacking practical problems in designing concepts and systems. Therefore, it is no wonder that such theoretical concepts as system state space or binary alarm vectors can be directly identified with items in the software structure for a computer based alarm system called HALO (Handling of Alarms using LOgic). This system is under development in the OECD Halden Reactor Project. Further details of the system and of some practical application results of parts of it can be found in references [4, 5 and 6].

Application of Multivariable Alarming to Nuclear Processes

The principles of multivariate alarm handling and display have been preliminary tested in two application projects. One of these is developing a complete HALO-system for a simplified PWR-simulator,and the other is a post trip alarm handling logic for a 660 MW BWR power plant. The displays in Figures 5-8 are taken from the PWR simulator displays. Both of these projects indicate very promising results in terms of ability to reduce the amount of irrelevant alarm information [5, 6]. Some tests have also been run on the effect of HALO-alarm handling to the accuracy and speed of fault diagnostic of very little trained operators. Preliminarily, the results indicate a significant improvement in accuracy.

CONCLUSIONS

Process alarms form an indispensable part of the man-machine interface in complex processes. To help the operators to act as a part of the overall process control system, the alarm system needs two abilities: It has to recognize process abnormalities and to present them to the operators in an efficient way. These two aspects of the alarm systems have been discussed.

A framework for a theory of forming process alarms has been presented. Based on that the functions of process alarms are to alert the operators and to direct their attention to abnormal or undesired process conditions this theory shows that an optimal alarm system for complex processes has to utilise the *multivariate alarming* principle. This principle is, in fact, a natural extension of today's single variable alarm systems.

A simple method to apply the multivariate alarm theory by using vectors of binary variables and boolean alarm expressions has been outlined. This simplification makes it possible to use the theory in computer based alarm systems.

A novel method of presenting the process alarms to the operators is described. This aims for providing the operators with means to get alarm information for different purposes at the appropriate speed of perception. A general overview of the process operating status and any alarm situations may be obtained at one glance from a symbolic overview picture. More detailed information for diagnostic purposes is contained in detail pictures and alarm message lists.

REFERENCES

1. P. Visuri and F. Øwre, "Forming and Presenting Process Control Room Alarms Using Computers," *HPR-283*, March (1982).

2. J. Foley and V. Wallace, "The Art of Natural Graphic Man-Machine Conversation," *Proceedings of the IEE*, Vol. 62, No. 4.

3. J. Hol and G. Øhra, "Development of Guidelines and Recommendations for Colour Display Based Information Presentation Systems," *HPR-263*, May (1980).

4. P. Visuri and F. Øwre, "A Candidate Approach to a Computer Based Alarm Handling System. Functional Description," *HWR-23*, May (1981).

5. P. Visuri et al., "Handling of Alarms Using Logic," Technical note to be published in Nuclear Safety.

6. P. Visuri, F. Øwre, and B. B. Thomassen, "Handling of Alarms with Logic (HALO) and Other Operator Support Systems," *HWR-24*, May (1981).

THE STAR-CONCEPT

A Method for the Definition and Generation of Computer-Based Systems to Support the Operator During Normal and Disturbed Plant Situations

L. Felkel, H. Roggenbauer*

Gesellschaft für Reaktorsicherheit (GRS) mbH
D-8046 Garching, Germany F.R.

ABSTRACT

The paper describes a variety of functions to improve man-machine communication in nuclear power plants by advanced use of process computers. Special functions of interest here are:

- Computerized Operational Manual
- Post Trip Analysis
- Alarm Reduction
- Disturbance Analysis and Surveillance
- Improved Plant Information Processing, Retrieval and Display.

All these functions use complex combinations of plant signals. The combinations (discrete process models) have to be described in a homogenous and formal way. The methodology used as well as the functions and examples are given. Experience from a pilot application in a nuclear power plant is also reported.

INTRODUCTION

To date the information the operator is provided with in the control room of a nuclear power plant is mainly based on the "one-sensor one-signal" philosophy [1]. This means that even though computers are used at numerous places in a nuclear power plant in most cases their capabilities to transform data into information are not really exploited. Consider, for example, loss of preferred power; this emergency situation requires the emergency diesels to be started. The initiating event may be of some minor significance so that the power supply is available soon thereafter. What happens in the control room? A large number of indicators will light most of them disappearing only after the proper acknowledge button has been pushed. And on the plant computer? At the first moment up to a thousand messages are initiated about no longer operating components and upon return of the power supply hopefully all of those thousand are reported to have returned to an admissible status. The most critical situation, however, occurs if there are just a few missing. How should the operator be able to scan a listing containing almost two thousand messages (lines) to find the one or two that are missing?

*Affiliated with Österreichisches Forschungszentrum Seibersdorf GmbH, A-1082 Vienna, Austria, presently with GRS.

This is just a very simple example to which a very simple solution exists but it shows clearly that something intelligent has to be done with the data in order to improve the man-machine interface.

An interesting finding is that many of the problems of the kind described in the example may represented by some graphical method which is on a level of abstraction permitting to cover other problems or functions as well.

For all messages possibly triggered in the example an individual treatment must be provided.

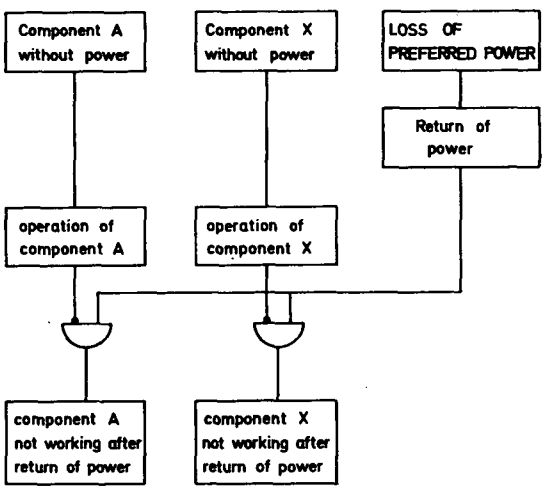


Figure 1 shows intuitively the way information is produced from raw data. In this situation the operator is only interested in messages originating from the bottom row and the right-hand-side column boxes.

In general the algorithmic problems to be covered are limited to a few. The most important of these are (and can be drawn from figure 1):

- sequences (in time)
- sequences (causality)
- logical combination
- parallelism

The following chapters refer to the functions and problems presently discussed. For each one of these the algorithms and their graphical representation are pointed out.

Fig. 1: Graphical description of information generation from data

COMPUTERIZED OPERATIONAL MANUAL

Many situations as they are described in the operational manual consist only of checking the values of specific plant variables, combining them in a logical way and performing the operator action required when the situation has been identified. Two examples of such parts of the operational manual are explicited here. The first example refers to the identification of medium LOCA's in a PWR (1300 MWe KWU-type) and the second to the availability and repair time requirements of the safety system of a BWR.

Before determining the cause of a medium LOCA an initiating event is defined in the operational manual. This event is the high pressure injection signal. The presence of the high pressure injection signal requires the operator to go through a complex checking procedure in order to find the cause and to take action according to the information in the manual. While the action may require a variety of different activities the checking procedure is entirely based on signals from the instrumentation. The data therefore can be made available to a computer with the checking procedure represented appropriately in it. The representation need encompass only the logical operators AND, OR, NOT, m OUT OF n and arithmetical relations to turn numeric values into logical ones (e.g. $a<b$, $a\neq b$ etc.). The procedures usually are to be scanned sequentially even though the inherent structure may well be a set of possible mutually exclusive parallel subprocedures. The small set of algorithmic representations described thus far should enable to automize checking procedures of this kind. As a result the computer would identify the situation, determine the action to be taken and inform the operator about the action ifself or at least where a description of it can be found. A gain in speed of determination and a reduction of the probability of human error is obvious.

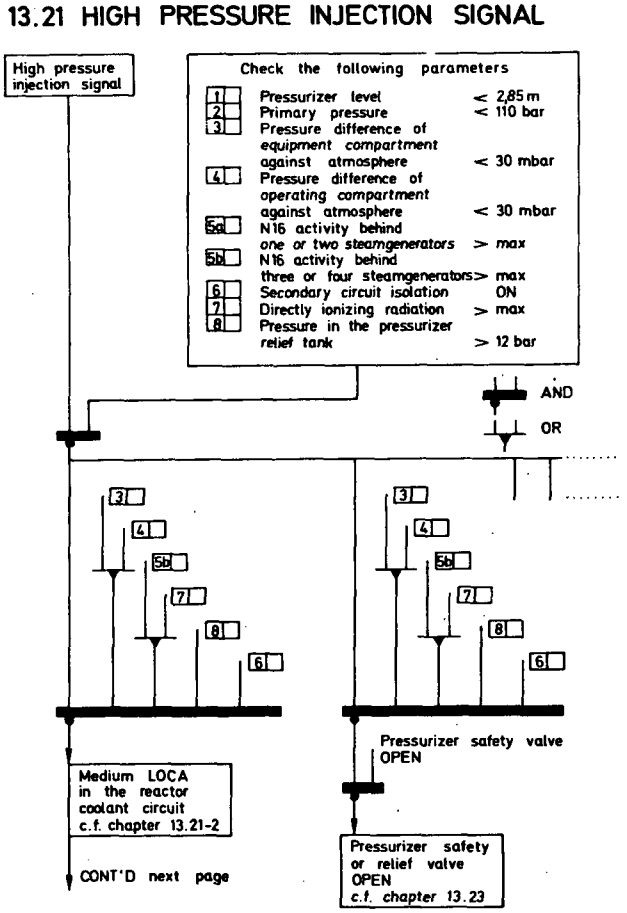


Fig. 2: Operational manual of a 1300 MWe PWR

Figure 2 shows a part of the original procedure in the operational manual. The operator is required to check all the parameters (1...8) against the criteria indicated and tag them accordingly. These criteria are referenced further down in the diagram to facilitate the logical scanning which is performed manually. The diagram splits into several possible combinations all of which are mutually exclusive. As a result only one of the boxes on the bottom of figure 2 may be obtained as a description or reference to the present emergency situation.

It is also noteworthy that some of the parameters to be checked (1,2) are never referenced in the diagram. These parameters should only be looked at by the operator to confirm major assumptions about the plant status. In a computerized version these variables would have to be checked and displayed to the operator.

It is needless to say that all the procedure steps can be described by a logical diagram of the kind shown in figure 1. If the signals are available on the plant computer the logic may be executed automatically giving the text in the result boxes to the operator. The procedure the operator is required to step through is exactly the way an algorithm would perform. Figure 3, then, shows which information is to be given to a computer to accomplish the same task.

The logical network of fig. 3 could possibly be reduced so as to minimize the number of gates and thus optimize the speed of computation. It should be noted, however, that this reduces the readability of the diagram as compared to the one in fig. 2. On the other hand, all these descriptions have to be tested and verified only once and even this may be computer-supported.

The second example concerning the safety system of a BWR [2] is outlined in figure 4. Since the algorithm and the logic is basically the same as in figures 2 and 3 only the differences will be described.

Usually safety actions of the reactor protection system are triggered according to some logic as shown in figure 4. A channel is said to be failed if at least one of its transducers is failed. If two or more channels are failed a safety action will be performed. The maximum allowable repair time of the transducers may be obtained from the respective descriptions in the operational manual. The example requires a repair time of 10 hours. Should there be other failures in the mean time the repair time may change drastically or even safety actions may be initiated. The operator must therefore always be informed about the status of the safety system.

A computerized system should facilitate keeping track of failed transducers, channels etc., and the respective repair times. Status changes and their impact on the repair times or existence of impending difficulties should be reported.

Basically there are two possibilities realizing such a safety system status surveillance. One is operated off-line requiring the operator to interact with the computer and enter all information about failed transducers enabling the system to determine the actual status. More elegant and reliable would be obtaining the information about failed transducers on-line. In any case the required repair time could be decreased according to the time elapsed thus always having the actual repair time at the operator's disposal.

The meaning of what is expressed in figure 4 can again be represented graphically and interpreted by the same computer program as would be used for all functions described thus far. The graphical representation is outlined in figure 5.

Note that it is not information delivered by the safety system but information about the degradation of the safety system itself.

POST TRIP ANALYSIS

The most important task of the operator or plant engineer after a reactor or turbine trip has occurred is to check whether all signals have been activated correctly, completely and in the right time sequence. During a major upset, assuming a time resolution of 10 milliseconds, the messages obtained may very well fill some meters of computer print-out. The only order of the messages so far available is a chronological one. This means that messages logically dependent may be separated by a whole bunch of data originating from other parts of the instrumentation. It is therefore a time-consuming and error-prone task first to find out whether the messages belonging together were in the correct order and secondly whether some messages are missing at all.

Reducing the time spent on examination of the print-out impacts plant availability significantly since the plant may be started-up again only after confirmation that everything occurred as it was designed (of course, the cause for the incident must be found, too).

Starting-up the plant while some required actions had not been performed but failed to be detected may severely impact plant safety. The following example (again from a 1300 MWe PWR) is used to point out the requirements of a system performing post trip analysis automatically.

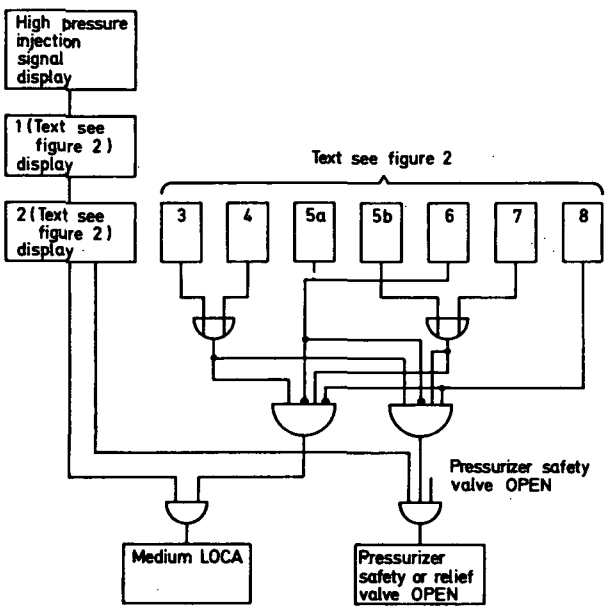


Fig. 3: Necessary description to perform task of fig. 2 automatically

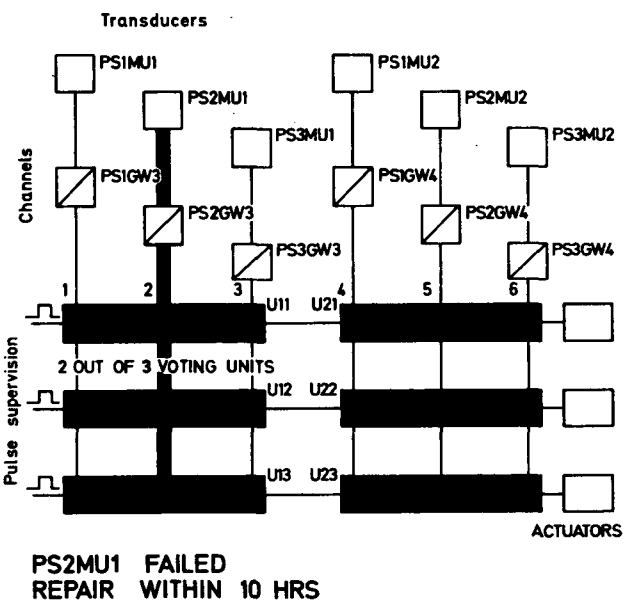


Fig. 4: Safety system of a BWR

A turbine trip necessitates three different signals each of which must be present one second after the trip has occurred. These signals are:

(1) ADDITIONAL MEASURES AGAINST OVERSPEED VIA POWER RELAY
(2) TURBINE TRIP RELEASE
(3) PRESSURE TURBINE TRIP HYDRAULIC OIL TOO LOW

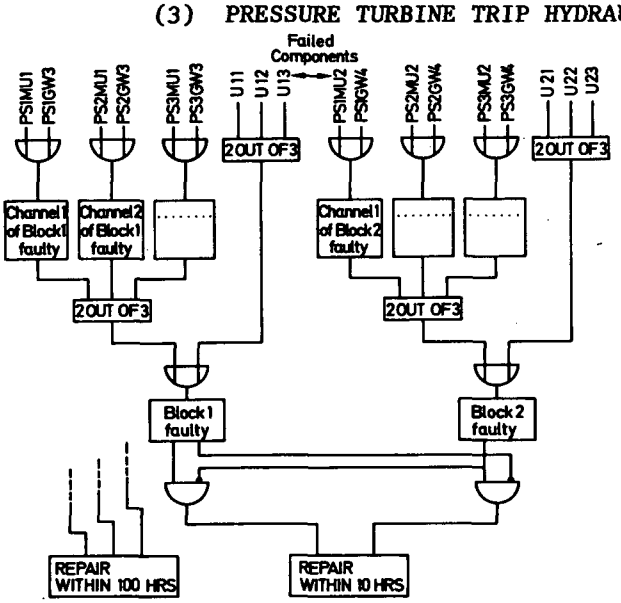


Fig. 5: Safety system status surveillance

All of these signals are secured by redundant channels which have all to be activated in order to trip the turbine. Any of the signals, however, may be used as an initiating event starting the post trip sequence surveillance.

After two seconds another set of signals must be present:
TURBINE CONTROL SYSTEM OFF
CONTROL VALVES OPEN
HIGH PRESSURE TURBINE TRIP VALVES CLOSED
MAIN STEAM MOTOR OPERATED VALVES CLOSED
VACUUM BREAKERS COND. PRESS. CONTROL OPEN
TURBINE TRIP BYPASS VALVES NOT CLOSED
MAIN STEAM BYPASS CNTRL VALV. NOT CLOSED.

After three seconds:
GATE VALVE PRESSURE BALANCE LINE CLOSED
MAIN STEAM FOR HEATING GATE VALVES CLOSED
LOW PRESSURE BYPASS VALVES OPEN

Before seven seconds are elapsed all of the vacuum breakers must have returned to their original position. Figure 6 shows how the required information may be produced algorithmically, basically using the same tools as for the previous functions. There is but one extension to be made: the introduction of time delays. Note that the operator gets the information be most urgently needs: the signals unexpectedly missing.

ALARM REDUCTION

During major plant upsets there is a large amount of alarms displayed to the operator. 500 alarms within five minutes may be expected according to experience reported [3]. Many of these alarms bear little or even no information at all (e.g. low oil pressure at some pumps which are not and need not be operating). Also alarms may be a direct consequence of a primary alarm or imply the preceding one. In any case, to determine whether or not an alarm should be displayed, the plant situation must be examined. In many cases simple logic can be used to suppress an alarm where the basic algorithmic functions described in the previous chapters may be applied.

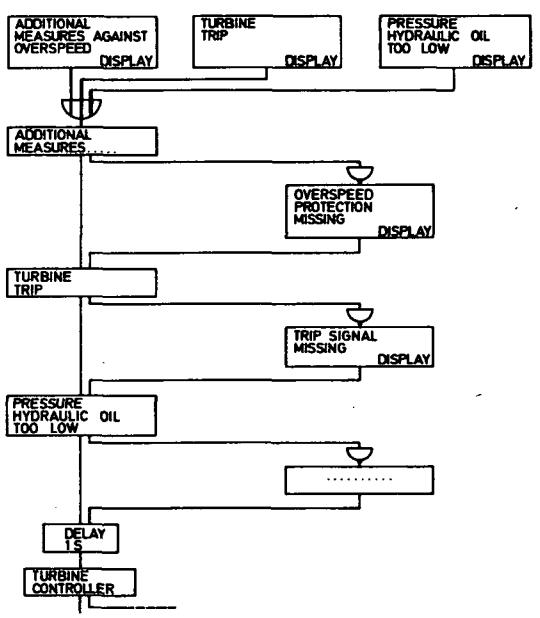


Fig. 6: Post trip alarm sequence

Figure 7 shows an example where an operating pump must for some reasons be switched off and the stand-by pump turned on. Usually the switch-over takes some seconds while the instrumentation reports two pumps not operating. This situation, however, requires an alarm solely if it persists longer than the expected duration of the switch-over.

Basically the example of figure 7 incorporates more than just suppressing three alarms replacing them by one in case it is really necessary. This method also allows for the identification of the cause of the alarm. For this reason further explication of alarm reduction, apart from very simple situations, is postponed until the discussion of disturbance analysis in the next chapter. The simple kind of alarm handling is published in [4,5].

DISTURBANCE ANALYSIS

Many publications have been issued on disturbance analysis (DAS) [6,7,8,9]. The main goal of disturbance analysis is to identify a disturbed situation, determine the primary causes and to gather important information about the expected propagation of disturbances. Again, as in the example shown in the introduction the analysis is based on primary process data consisting of binary status indications, limit excess information or analog values (physical variables). However, to produce information useful for the operator additional data have to be entered to allow a computer to determine specific situations and collect and present the respective information. These data are usually called the "process model" because they describe how the raw data are expected to behave.

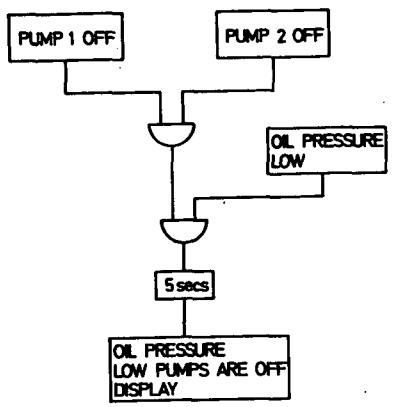


Fig. 7: Simple alarm tree

As mentioned in the discussion about alarm reduction the plant situation and the causes leading to it must be properly determined. This is done by so-called cause-consequence diagrams an example of which is shown in figure 8.

This diagram shows a small part of a cause-consequence diagram for a disturbance concerning the main condensate pumps of a 1300 MWe PWR.

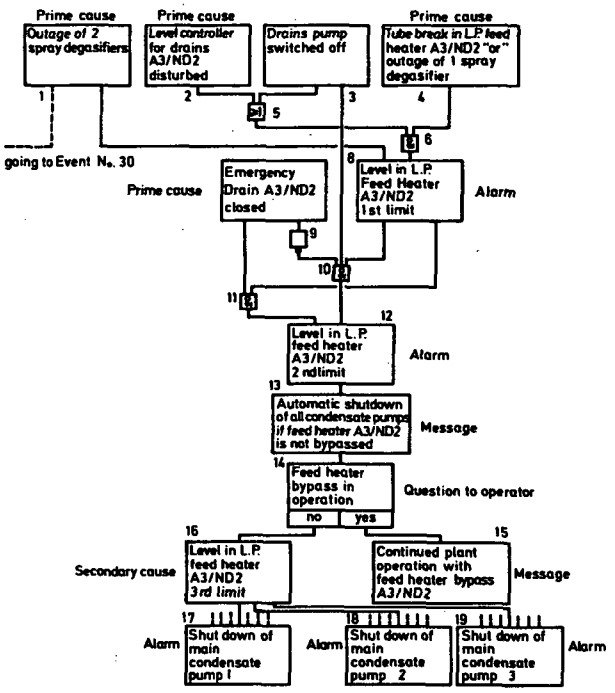


Fig. 8: Sample cause-consequence diagram

The basic assumption is that the drains pump for the low pressure feedheater is either switched-off or in repair (event 3). If there is a tube break in the low pressure feedheater or a spray degasifier in the feedwater tank is lost. Subsequently, there will be an increase in the water level of the feedheater. This increase will continue until the first limit is reached (event 8). This is the first observable event from which the disturbance analysis system will conclude that the primary cause can only be the tube break in the low pressure feedheater (event 4). At this point already, appropriate corrective actions could be taken. In case the corrective action is not taken, the water level will continue to rise and will exceed a second limit (event 12).

The control system automatically isolates the defective low pressure feedheater after the second limit has been exceeded and the appropriate preheater will be by-passed. This may not be successful, however, in which case an emergency shut-down of all three main condensate pumps is imminent. The operator

will be notified about this situation by appropriate messages. In the Grafenrheinfeld nuclear power plant the status of the valves for the pre-heater by-pass is not available on the process computer and there is only the operator to know whether or not the pre-heater by-pass was successful. The disturbance analysis system therefore asks the operator an appropriate question (event 14). The question is answered by means of a special keyboard in the disturbance analysis system. If the pre-heater by-pass was unsuccessful there will still be continued increase of the water level in the low pressure feedheater which after the excess of a third limit causes the automatic shutdown of the two operational main condensate pumps and prevents that the stand-by condensate pump is started. As a consequence the feedwater tank will be emptied by and by, which eventually leads to the shut-down of the main feedpumps and reactor scram.

Please note that apart from the question to the operator all descriptive means are already used by the simpler functions of the previous chapters. The difference so far is mainly one of quantitative complexity.

A system performing disturbance analysis has been designed and installed in the Grafenrheinfeld nuclear power plant (1300 MWe KWU-PWR). It has been coupled on-line to the process and tested throughout the commissioning phase and during the first weeks of normal 100 percent operation. Detailed information about the tests are published in [10].

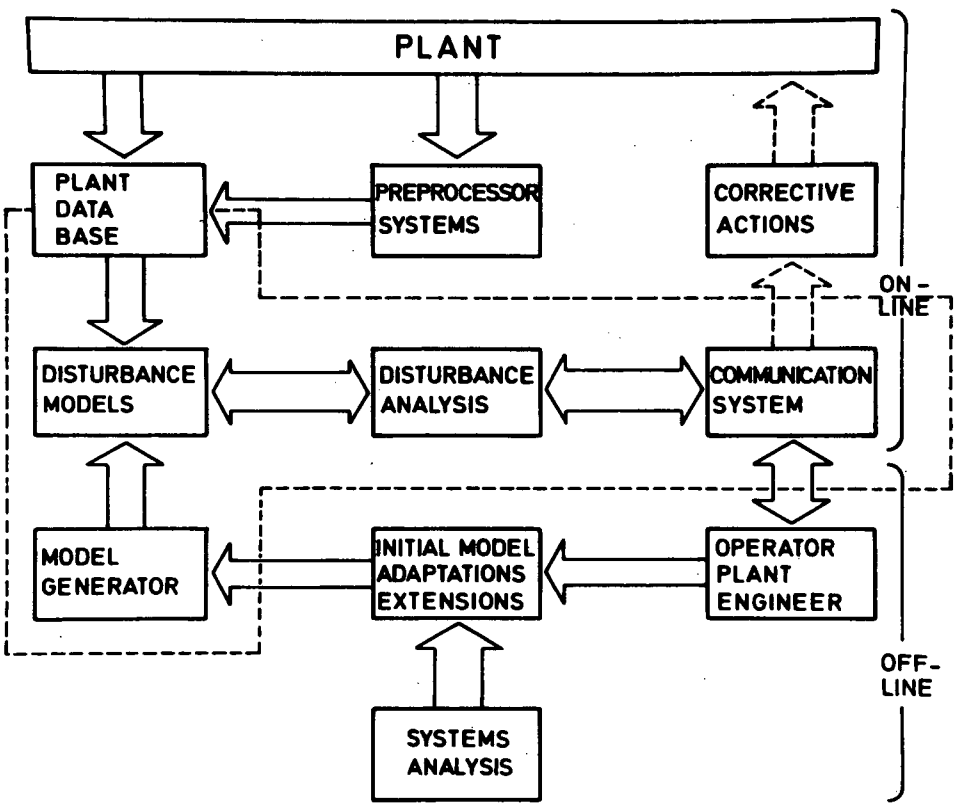


Fig. 9: Modules of the STAR-DAS

The STAR-system (abbr. from Störungsanalyserechner (disturbance analysis computer)) is outlined in figure 9. It consists of several modules each of which performs a specific function described in the sequel.

The plant data gathered from the instrumentation are preprocessed so as to form the plant data base. Preprocessing comprises limit checking, data validation, filter-

ing and deriving variables from other plant signals. Dedicated preprocessor modules for noise analysis and loose-parts monitoring may also contribute to the plant data base.

To detect disturbances, so-called disturbance models (represented by cause-consequence diagrams) are used. These are stored in a background data base and are readily accessible by the disturbance analysis routines. The models contain the anticipated flow of events during disturbances. The disturbance models are overlaid by the actual plant data available from the plant data base. After association of predefined disturbance models with acutal data the models are considered activated.

The disturbance analysis routine scans the activated models and detects disturbances, if there are any, at their very beginning. After determining the status of the process, the further possible consequences will be evaluated and if possible and feasible, corrective actions suggested as well as primary causes detected. Since the disturbance analysis module is a computer program, results delivered by it have to be transformed into a readable form according to ergonomic standards. This task is performed by an operator-communication system. The communication system also provides means for retrieving and supplying information from and to the disturbance analysis system.

The models (CCD's) used by the disturbance analysis routine are mainly produced by systems analysts. The information required stems from engineering judgement as well as from plant design models. There is a significant amount of experience though, gained during operation of the DAS, by which most likely new insights evolve and may result in modifications, adaptations and extensions of the existing models. The DAS data background may thus be enhanced continually.

The DAS system therefore comprises an off-line tool (model generator) for preparing, testing and modifying the CCD's.

It is the existence of such a model generator which made possible the realization of functions like post trip analysis, alarm handling etc. with the STAR-DAS. How this is achieved is outlined in the next chapter.

GENERIC FUNCTIONS

All the functions described in this paper require a basic set of so-called semantic primitives (generic functions). Most of these primitives have already been shown informally. However, in order to make a computer system understand and correctly interpret a complex collection of on-line data, a formal concept must be provided.

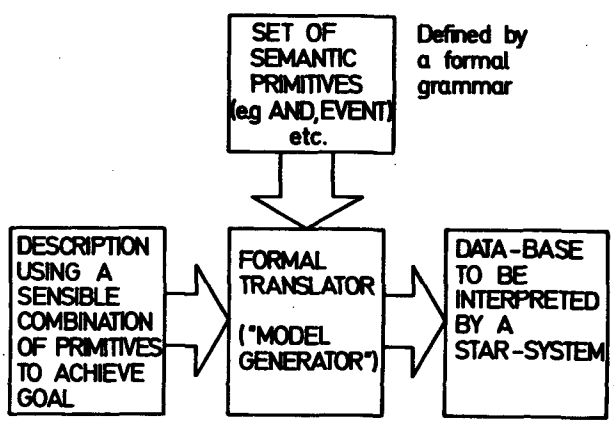


Fig. 10: The STAR-Concept

This concept is called the STAR-concept as opposed to the STAR-system which is able to interpret descriptions of data transformation. The concept provides the set of semantic primitives necessary to produce complex descriptions of how the data are to be interpreted. It is interesting, though, that this set is rather small as was already intuitively clear from the previous chapters. Therefore the descriptions may be derived rather easily without deep understanding of how computer systems work.

It is the plant engineers, systems analysts and may be even operators who benefit from this fact since they are able to incorporate their knowledge about situational contexts or complex plant conditions into a computerized system utilizing this know-

ledge when the situations occur or the conditions impend. This only makes it possible to turn data into information. Moreover, a formal tool which turns engineering knowledge into complex computer-interpretable data bases facilitates easy adaption or backfitting since it is entirely based on software. The only hardware changes may be necessitated by enhancing the data acquisition when additional signals are required.

Figure 10 shows the main parts of a system with which complex data interpretations can be specified.

With the presently existing spectrum of generic functions [11] a great number of problems concerning the improvement of information for the operator can be solved. However, there are extensions to be made as new requirements (c.f. safety parameter display system (SPDS) [12]) or experience with DAS systems pointed out in the next chapter, evolve.

CONCLUSIONS

From experience with the application of the STAR-DAS in the Grafenrheinfeld plant the following recommendations for further development as well as commercial use of such a system in a nuclear power plant are given:

- For good display of analysis results at least two, preferably coloured, cathode ray tubes (CRT) are required. The display should be alphanumeric, with graphical support.
- Fully graphic display systems (as opposed to semigraphic ones) are to be preferred on the grounds of better resolution and software portability.
- The selection of disturbances to be detected, identified and processed must be based on a systematic task analysis of the operators and should not be limited or even based on available plant instrumentation.
- Which systems are to be analysed and at what level of detail requires the same careful considerations.
- DAS-like systems may easily be upgraded so as to allow functions of the kind described in this paper, without extending the need of additional hardware.
- The process descriptions (generic functions, see resp. chapter) need be extended so as to allow dynamical problems (trend-curves, balances, history) to be described.
- The basic concept of top-down design (represented by the STAR-concept and realized by the model generator (figure 10) has proven its feasibility and should be further developed.

In conclusion more emphasis must be put on the display of information (not necessarily only on CRT-based systems) and on including additional means for describing dynamical problems without necessitating dynamic modelling on the basis of differential equations.

Presently work is being carried out to enhance the system based on this experience which as a further goal will also make it possible to specify extended SPDS's within the STAR-concept.

ACKNOWLEDGEMENT

Thanks are due to Miss Johanna Weindl for the careful typing of the manuscript and Mr. Peter Bartel for doing the artwork.

REFERENCES

[1] A.B. Long, "Technical Assessment of Disturbance Analysis Systems", Nuclear Safety Journal, Vol. 21, 1(1980)
[2] H.Roggenbauer, "Basic Ideas for the Development of a Computerized Reactor Operation Manual", Proc. Enlarged Halden Programme Group Meeting, June 5-9, Loen, Norway, (1978)
[3] Personal Communication With German Utilities (1981)

[4] P.C.M.Kay and P.W.Heywood, "Alarm Analysis and Indication at Oldbury Nuclear Power Station", IEE Conf.Publ.16, Part I (1966).
[5] F.Øwre, et al., "A Software Structure for Handling of Alarms Using Logic (HALO)", Halden Work Report HWR 45, Halden, Norway (1982)
[6] W.Bastl and L.Felkel, "Disturbance Analysis Systems", In: Human Detection and Diagnosis of System Failures, J.Rasmussen, W.B.Rouse, Eds., pp. 451-473, Plenum Publ. Corp. (1981)
[7] L.Felkel, R.Grumbach et al., "Analytical Methods and Performance Evaluation of the STAR Application in the Grafenrheinfeld Nuclear Power Plant, IAEA Specialists' Meeting on NPPCI, Dec. 5-7, Munich, Germany, (1979)
[8] L.Felkel, "STAR Disturbance Analysis System, Answers to regulatory review questions", paper submitted to the IEEE Standards Workshop on Human Factors and Nuclear Safety, Myrtle Beach, S.C., (1981)
[9] C.H. Meijer and B.Frogner, "On-Line Power Plant Alarm and Disturbance Analysis System", EPRI-Report NP-1379, Palo Alto, (1980)
[10] L.Felkel et al., "Results from the STAR-Application at Grafenrheinfeld", (1982), to appear
[11] L.Felkel, R.Manikarnika, "The Modelgenerator MOGEN", GRS-internal report, Munich, Germany (1982), (in German)
[12] USNRC, NUREG-696, NUREG-814, NUREG-835, (selection), (1981)

A MONITORING AND DIAGNOSTIC SYSTEM OF FISSION PRODUCT TRANSPORT AND RELEASE IN NUCLEAR POWER PLANTS

H. Kodaira, S. Kondo, and Y. Togo

University of Tokyo
7-3-1, Hongo, Bunkyo-ku, Tokyo, Japan

ABSTRACT

A monitoring and diagnostic system (MADS) of fission product (FP) transport and release in nuclear power plants (NPPs) is proposed and the conceptual design for MADS is studied in this paper. A MADS can be described in the most general way as a computer-based information processing system which takes in plant data, processes it and displays the results to the NPP's operating crew.

Our major concern for MADS is, however, not to evaluate general plant dynamics, but to monitor the distribution of whole radioactive materials such as FP, and to diagnose the plant state in the view of FP transport during the NPP's lifetime.

Several functions demanded of MADS are : (a) during normal operation, to certify the fuel integrity and the effectiveness of the purification systems, (b) in an unusual event, to identify the event and to monitor the amount of FP release with accuracy, and (c) in case of a rare occurrence, to estimate the maximum potential release.

INTRODUCTION

In the aftermath of Three Miles Island Accident, various kinds of man/machine systems in NPPs have been proposed and developed in the world [1,2]. These systems can be described as computer-based information processing systems which take in plant process and control data, analyze the plant dynamics, estimate the resulting damage to fission product barriers, and display the results to the NPP's operating crew to help their control of the plant.

As the high power levels and fuel exposures of modern nuclear reactor plants have resulted in core inventories that may exceed 10 billion curries (Ci) of radioactive material, the potentially severe consequences of the release of a major part of them are serious problems that must be addressed if nuclear reactors are to be used successfully as a large-scale source of power for the near future.

During normal operation of NPPs, a major part of the FP inventories is retained in the core and the very small fractions of them escape to the primary coolant. The radioactive materials in the primary coolant then escape to the secondary coolant and/or to the reactor containment and the major part of them is removed by the purification systems. The radioactive materials cannot, however, disappear in the plants except for radioactive decay, and when an unusual event will happen, all of them may become the source terms of the environment. As the occurrence of an unusual event may

be hardly forecasted, we must be prepared for the events.

A monitoring and diagnostic system (MADS) of FP transport and release in NPPs is proposed, and our primary objective of MADS is to monitor the distribution of the radioactive FP and to diagnose the plant state in the view of FP transport during the NPP's lifetime. MADS can provide the NPP's operating crew with the information of the distributions of the whole radioactive FPs at all times, and in case of an unusual event, these informations may become the accurate initial conditions for the evaluation of the radiological consequences.

Two projects have been initiated in the study of MADS, one is the development of the computational code which can simulate the detailed phenomena of the FP transport and release in NPPs, and the other is the conceptual design of MADS.

The objectives of the development of the computerized simulation code are as follows.

(a). to evaluate the FP distribution in various situations,
(b). to lead the understanding of the phenomena,
(c). to make the radiological data for MADS, and
(d). to determine the threshold values of MADS.

COMPUTERIZED SIMULATION CODE SACHET

PWR plants are chosen to simulate FP transport and release in our study and computerized code SACHET has been developed, in which PWR plants are devided into more than thirty compartments. The multiple compartment system as shown in Table I, cannot describe the phenomena in PWR plants completely, but it is enough for the simulation of the major phenomena. As the computerized model is intended to evaluate the distribution of the whole radioactive FPs in NPPs, there is no way to reduce the radioactive FPs in the multiple compartment system with the exception of radioactive decay. The radioactive FPs which are removed from one compartment, are always transported into another compartment. Therefore compartments such as purification system, filtration system, and reactor containment wall are considered in SACHET.

The interrelation of the compartments is shown in Table II as a form of the transport coefficient matrix. Transport coefficient from j to i is expressed as H(i,j) and if it is not essentially zero, it is simbolized as F, G, E, D, P, etc., according to the properties of the transport. The determination of the coefficient is described in the following sections.

Simulation code SACHET is a computerized mathematical model for calculating the transport and release of radioactive FPs in PWR plants during normal operation and in case of unusual events. During normal operation, the calculations are based on a series of generically applicable parameters which describe the appearance rates of FPs in the primary coolant, the transport and release mechanics resulting in their appearance in liquid and gaseous wastes, and the effectiveness of design considerations incorporated to reduce the quantity of radioactive materials that may be released to the environment [3]. In case of unusual events, additional releases of FPs From the core to the primary coolant, from the primary coolant to the secondary coolant, and/or from the primary coolant to the reactor containment are considered, and various engineered safety systems can operate to remove FPs from containment atmosphere; i.e., aqueous spray systems, recirculating filter units, annulus air cleanup system [4].

The characteristics of SACHET are as follows.

(a). dynamical transport and release of FPs in PWR plants,
(b). detailed time-variable data input at more than one hundred steps,
(c). more than thirty compartments of PWR plants
(d). transport and release in both gaseous and liquid phase,
(e). transport and release in both normal and anomalous conditions.

Equations of The Multiple Compartment Model

As the flow terms assume uniform mixing within each compartment, the changes of FP

inventories are described by a set of equations of the form :

$$dC_i/dt = \sum_j H_{ij}C_j + P*U \qquad (1)$$

where C_i = inventory in compartment i

H_{ij} = transport coefficient from compartment j to compartment i ($i \neq j$)

$H_{ii} = -\sum_j H_{ji} - \lambda = -H_{\tilde{i}i} - \lambda$

λ = decay constant

P = constant according to the thermal power and fission yield

U = 1 if compartment i is the core region
0 if compartment i is not the core region

These equations are solved exactly and the FP distribution after Δ is obtained as follows.

$$C(t) = \exp(H*\Delta)*C(t_0) - (1 - \exp(H*\Delta))*H^{-1}*P*U \qquad (2)$$

$$= (I + H*\Delta + \frac{1}{2}H^2*\Delta^2 + \frac{1}{6}H^3*\Delta^3 + \ldots)*C(t_0) + (\Delta + \frac{1}{2}H*\Delta^2 + \frac{1}{6}H^2*\Delta^3 + \ldots)*P*U$$

FP Inventory in Core

As the estimation of whole FP core inventories needs a relatively large computer code such as ORIGEN, and a long computational time, FP core inventory matrix is used in SACHET, which is previously calculated by ORIGEN code. FP inventories at a certain time are interporated from the elements of the matrix.

In normal operation, radioactive FP which leaks to the primary coolant is very small as compared with the FP in core, and the assumption of the constant core inventory during a short period of computation may be reasonable except for the reactor shutdown. In other words, the input source term vector U and the transport coefficient H(i,i), if compartment i is the core region, are zero in such a case. As the power related constant P is zero in case of either accidental or normal reactor shutdown, we are given homogeneous equation (3) in matrix notation.

$$\frac{dC}{dt} = HC \qquad (3)$$

And the solution of it is obtained as follows.

$$C(t) = \exp(H*t)*C_0 = (I + H*t + \frac{1}{2}H^2*t^2 + \frac{1}{6}H^3*t^3 + \ldots)*C_0 \qquad (4)$$

FP Leak from The Core to The Primary Coolant

In normal operation, operating power equilibrium FP source term and FP escape rate coefficient are used in SACHET [3].

Iodine spiking phenomena after the reactor shutdown are considered in SACHET, in which original empirical model obtained by Davidon-Fletcher-Powell Method, using the data of the experiments in OWL-1 in-pile loop of JMTR, is used [5]. The model is a nonlinear function with such variables as reactor power, fuel burnup, FP inventory, and change of linear heat rate, coolant temperature and coolant pressure as

$$FF = 0.1678*\{1 - \exp(-0.0303*CB)\}*[\{1 - \frac{2}{\exp(0.00823*\Delta Q) + \exp(-0.00232*\Delta Q)}\}$$
$$+ \{1 - \frac{2}{\exp(0.02488*\Delta T) + \exp(-0.02748*\Delta T)}\}$$
$$+ \{1 - \frac{2}{\exp(0.006457*\Delta P) + \exp(-0.003329*\Delta P)}\}]*C, \qquad (5)$$

where FF = Number of nuclides/hr/10^{15}, CB (MWD/ton), C = inventories/10^{17}, ΔQ (W/cm), ΔT (°C), ΔP (kg/cm²G).

In case of further fuel defect, from gap release to core explosion, the release fractions of the core inventories are referred to the data from Ref.[4,6].

Purification System

In NPPs, several systems purify the inlet liquid flow by demineralization and the effectiveness of them is defined as a decontamination factor (DF), which is the ratio of the initial to the final amount in terms of concentration or activity of radioactive material.

If compartment i is a purification system with the value of DF and the liquid flow goes out of the compartment j at the rate FI, through the compartment i, and goes into the compartment l at the rate FO, transport coefficients of these compartments are as follows.

$$H_{ij}=(FI - FO/DF)/V_j,\ H_{li}= 0,\ \text{and}\ H_{lj}= FO/DF/V_j. \tag{6}$$

Demineralizer, secondary coolant blowdown system,condenser, and boron recovery system are considered as purification system in SACHET (Fig.1,3).

Filtration System

To reduce the radioactive materials in gaseous flow, demineralization is not effective, and some filtration systems are used in NPPs. The effectiveness of filtration system is defined as filter efficiency (EF), and it is the ratio of trapped materials to the total inlet materials.

If the compartment i is a filtration system with the efficiency of EF and the radioactive materials in gaseous phase flow out of the compartment j, through the compartment i, to the compartment l at the rate G, transport coefficients of these compartments are as follows.

$$H_{ij}= EF*G/V_j,\ H_{li}= 0,\ \text{and}\ H_{lj}= (1 - EF)*G/V_j. \tag{7}$$

Containment air cleanup system, annulus air cleanup system,filter unit, and PCA filter are considered in SACHET (Fig.1,3,4).

Partition Factor (Stripping Factor)

Partition factors (PFs) are referred to the data from Ref.[3] during normal operation. As for the iodine partition factor, we can evaluate it as a function of temperature, pressure and partition coefficient in SACHET optional mode.

There are some pairs of compartment such as secondary coolant system (liquid) & (gas), CVC tank (liquid) & (gas), and reactor containment building & reactor containment sump in SACHET, where we assume that the liquid and gas are at equilibrium. A leak flow F from the compartment j to the pair of compartment i(gas) and l(liquid), is partitioned as follows.

$$H_{ij}= PF*F/V_j \ \text{and}\ H_{lj}= (1 - PF)*F/V_j. \tag{8}$$

Tank systems, where gas and liquid are at equilibrium, are not considered pairs of compartment in SACHET, therefore outlets from such compartments are both gaseous and liquid, and transport coefficients of them are

$$H_{ki}= PC*G/V_i^l \ \text{and}\ H_{li}= (1-PF)*F/V_i^l = (1-PC*V_i^g/V_i^l)*F/V_i^l. \tag{9}$$

Transport coefficients mentioned above are summalized in Fig. 5.

Radwaste Treatment System

In SACHET, liquid waste such as chemical waste and detergent waste are not included. Schematic diagrams of gaseous and liquid waste treatment system used in SACHET are shown

in Fig. 1,2 respectively.

Off-gas flows from tank vent to gaseous waste treatment system are not shown in Fig. 2.

Accident

In case of accident, natural deposition and containment sprays are considered in SACHET. Those removal rate from containment air inventories are referred to the models from Ref. [4].

Primary coolant leak rate to the containment in small LOCA and the containment air leak rate to the environment are also calculated in SACHET optional mode and the models of them are referred to the model from Ref. [7,8] respectively.

DESIGN OF MADS

Schematic flow diagrams of MADS and SACHET and the interrelation of them are given in Fig. 6. The MADS software consists of codes as follows.

Data Input

In process of data input, three kinds of data set are took in, plant process data, control data, and radiological data. Process data such as temperatures, pressures, flow rates, etc. are used to determine the transport coefficients. Control data such as valve open/close, pump on/off, etc. are used to recognize the NPP's state, and also to determine the transport coefficients. The process data used in estimation of the transport coefficients is not always the one measured, but also the one averaged during the time cycle. There are several parameters which are not measured directly, such as vapor mole fraction, leak rate between the compartments, etc. We evaluate some of them from other measured process data and others are assumed initially. But the values of them are adjusted in adaptation phase of MADS step by step.

Radiological data are took in after evaluating the inventories of radioactive materials at the next step, and comparison between the two data are done in diagnosis phase.

Solution of The Coupled-differential Equation

The equations to be solved are the ones described in the previous chapter, and the solution of them are also given previously. As SACHET is not a code intended to use in online process, computational time of the solution is longer than real time if smaller computer system is used. Numerical approximations by the truncation of the higher order matrix are used as shown in equation (10).

$$\begin{aligned} C(t) &= \exp(H*\Delta)*C(t_0) \\ &\tilde{=} \left(I + H*\Delta + \frac{1}{2}H^2*\Delta^2 \right)*C(t_0) \\ &\equiv \tilde{C}(t) \end{aligned} \tag{10}$$

These approximations are invalid if the product of t by the norm of the matrix is not small. But in MADS, the product is far less than unity and these approximations are valid.

In an unusual event, the FP distribution after long period can be evaluated and especially in case of a rare occurrence, the potential release in addition to a loss of 1 of 3 FP barriers is also evaluated.

The computed results are displayed in CRT to the NPP's operating crew.

Diagnosis of The Plant States

Radiological data such as inventory vector of radionuclide m (C^m) and the estimated value of it ($\tilde{C}^m$) are used to diagnose the plant condition and identify the occurrence by the pattern recognition method. The threshold of each condition is given by the results of SACHET code.

Adjustment of The System Parameters

In the adjustment phase, a functional of the system parameters and measured data is defined as follows.

$$Q(\bar{C},x) = \frac{1}{2}\{\bar{C} - \tilde{C}(x)\}^2 \tag{11}$$

where $\bar{C}$ is the measured data and $\tilde{C}$ is the estimated data using the system parameter x. When the data is measured, system parameter is adjusted according to the following equation (12).

$$x[n] = x[n-1] - r[n]\nabla_x Q(\bar{C}[n],x[n-1]). \tag{12}$$

As for MADS, $\bar{C}$ is the radiological data, and $\tilde{C}(x)$ is expressed in equation (10), we have

$$Q(\bar{C}[n],x[n-1]) = \frac{1}{2}(\bar{C}[n] - \tilde{C}(x[n-1])^2, \tag{13}$$

$$\begin{aligned}\tilde{C}(x[n-1]) = C[n-1] + (& \Delta \sum_{l}^{l\neq ij} H_{il}C_l - \Delta H_{i\tilde{i}}C_i - \Delta\lambda C_i - \frac{\Delta^2}{2}H_{i\tilde{i}} \sum_{l}^{l\neq ij} H_{il}C_l \\ & - \frac{\Delta^2}{2} \sum_{l}^{l\neq ij} H_{il}H_{l\tilde{i}}C_l - \Delta^2\lambda \sum_{l}^{l\neq ij} H_{il}C_l + \frac{\Delta^2}{2}H_{i\tilde{i}}C_i \\ & + \Delta^2\lambda H_{i\tilde{i}}C_i + \frac{\Delta^2}{2}\lambda^2 C_i + \frac{\Delta^2}{2} \sum_{l} \sum_{m}^{m\neq ijl} H_{im}H_{ml}C_l) \\ & + (\Delta C_j + \frac{\Delta^2}{2} \sum_{l}^{l\neq j} H_{jl}C_l - \frac{\Delta^2}{2}H_{i\tilde{i}}C_j - \Delta^2\lambda C_j - \frac{\Delta^2}{2} \sum_{k}^{k\neq ij} H_{kj}C_j) * x[n-1] \\ & - \frac{\Delta^2}{2} C_j * x[n-1]^2\end{aligned} \tag{14}$$

$$\begin{aligned}x[n] = \; & x[n-1] - r[n]*\{\bar{C}[n] - \tilde{C}(x[n-1])\} \\ & * \{(\Delta C_j + \frac{\Delta^2}{2} \sum_{l}^{l\neq j} H_{jl}C_l - \frac{\Delta^2}{2}H_{i\tilde{i}}C_j \\ & - \Delta^2\lambda C_j - \frac{\Delta^2}{2} \sum_{k}^{k\neq ij} H_{kj}C_j) - \Delta^2 x[n-1]C_j\}\end{aligned} \tag{15}$$

where $x = H_{ij}$

The system parameters adjusted are :
(a) parameters of every nuclide : leak rate from fuel to the primary coolant, decontamination factor of demineralizer, stripping factor of CVC system,
(b) parameters of every element : leak rate with cladding failure, removal rate by sprays or natural deposition, transport coefficient with evaporation, and
(c) parameters in common : power ratio of failed fuel, leak rate from the primary to the secondary coolant, leakage from the primary coolant to the containment, etc.

RESULTS AND CONCLUSION

As MADS is not installed in an actual NPP yet, the validity of the MADS software is tested in combination with SACHET code.

Some results are shown in Fig. 7~10, where additional fuel cladding failure is occurred at the third time step, and the inventories of I-131,133 in the primary coolant increase gradually. In those figures, little circles show the results of MADS estimation. The difference of the condition between Fig. 7 and Fig. 8 is the length of the time step, and in both cases the adjustments of the system parameter by MADS are well. In Fig. 9, fuel cladding failure increases gradually and the MADS adjustment is fairly good. In Fig. 10, the result is according to the inventory of I-133, where adjustment of system parameter tends to oscilate as compared with the case of I-131. The reason of the oscilatory tendency is that the function of $\Gamma[n]$ in equation (15) is not optimized in case of I-133, as we use the same function of $\Gamma[n]$ in both I-131 and I-133.

Computerized code SACHET which simulate the dynamical FP transport and release in PWR plant is developed, and the conceptual design of MADS is proposed and the effectiveness of MADS is shown in this study.

As for MADS, one of the outputs is the FP release from NPP to the environment and we are going to combine it with another system which predicts realtime atmospheric radionuclide concentration and associated doses caused by an accident release from NPP to realize an automated emergency response system in the near future.

REFERENCES

1. A. B. Long et al, "Summary and Evaluation of Scoping and Feasibility Studies for Disturbance Analysis and Surveillance Systems (DASS),"Report EPRI NP-1684, (1980).

2. F. Honeycutt et al, "Design and Hardware Alternatives for a Safety Parameter Display System (SPDS)," Report NSAC-34, (1981).

3. "Calculation of release of radioactive materials in liquid and gaseous effluents from pressurized water reactors (PWRs)," DRAFT REGULATORY GUIDE 1.BB, (1974).

4. " Release of radioactivity in reactor accidents, Appendix VII to reactor safety study," Report WASH-1400, (1975).

5. H. Kodaira, "Analysis of Iodine Spike Activity in ATR Primary Coolant by Togo-Kondo-Kodaira (TKK) Model," (in Japanese) NEUT Report 80-09, (1980).

6. R. A. Lorenz et al, "Fission product source terms for light water reactor Loss-Of-Coolant Accident,"*Nucl. Tech.* 46, (1979).

7. R. O. Wooton and H. I. Avci, "MARCH (Meltdown Accident Response CHaracteristics) code description and user's manual," Report NUREG/CR-1711, (1980).

8. A. Kenigsberg, "Parametric study of radioactive release from a breached containment," *Nucl. Tech.* 50, (1980)

Table I Multiple Compartment System in SACHET

1. Reactor Core
2. Primary Coolant System
3. Demineralizer
4. CVC Tank (liquid)
5. CVC Tank (gas)
6. Holdup Tank
7. Boron Recovery System
8. Hydrogen Recombiner System (gas)
9. Hydrogen Recombiner System (liquid)
10. Continuous Off-gas Decay Tank
11. Gas Decay Tank
12. Secondary Coolant System (liquid)
13. Secondary Coolant System (gas)
14. Condenser (Demineralizer)
15. Air Ejection System
16. PCA Filter
17. Containment Air Cleanup System
18. Filter Unit
19. Pressurizer Relief Tank
20. Reactor Coolant Drain Tank
21. Auxiliary Building Drain Tank
22. Reactor Containment Sump
23. Auxiliary Building Sump
24. Turbine Building Sump
25. Waste Evaporation System
26. Waste Holdup Tank A
27. Waste Holdup Tank B
28. Secondary Coolant Blowdown System
29. Reactor Containment Building
30. Auxiliary Building
31. Turbine Building
32. Reactor Containment Annulus
33. Annulus Air Cleanup System
34. Reactor Containment Wall
35. Environment (gas)
36. Environment (liquid)

Table II Transport Coefficient Matrix

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16-18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33-36
1	Σ																														
2	V	Σ		F		pd																									
3		D	Σ																												
4		fd		Σ																											
5		Fd			Σ																										
6		d				Σ											p	p	p												
7						pD	Σ																								
8					P	PP	PP	Σ		PP	PP						PP	PP	PP				PP								
9					p	pP	pP		Σ	pP	pP						pP	pP	pP				pP								
10					G			G		Σ																					
11					G		P	G			Σ							P	P				P	P	P						
12		pL										Σ			P																
13		PL											Σ																		
14													D	Σ																	
15													d		Σ																
16										EP	EP				EP	λ												E	E		
17	X															λ											E				
18																λ											E				
19		L															Σ														
20		L																Σ													
21		L						F	p	p	d								Σ						F						
22		pL															ppL	ppL		Σ							S				
23		pL																	ppL		Σ			ppL	ppL						
24												pL										Σ									
25																							Σ	p	p						
26																	p	p	p					Σ							
27			F				p							F						F	F			p	Σ						
28												D														Σ					
29		PL															PpL	PpL									Σ				
30		PL								PL	PL								PpL					PpL	PpL			Σ			
31													PL																Σ		
32																											L		Σ		
33																													E	λ	
34																											N			λ	
35										eP	eP				eP								P				eL	eL	eL	eL	λ
36						pd						d									F	F	p								λ

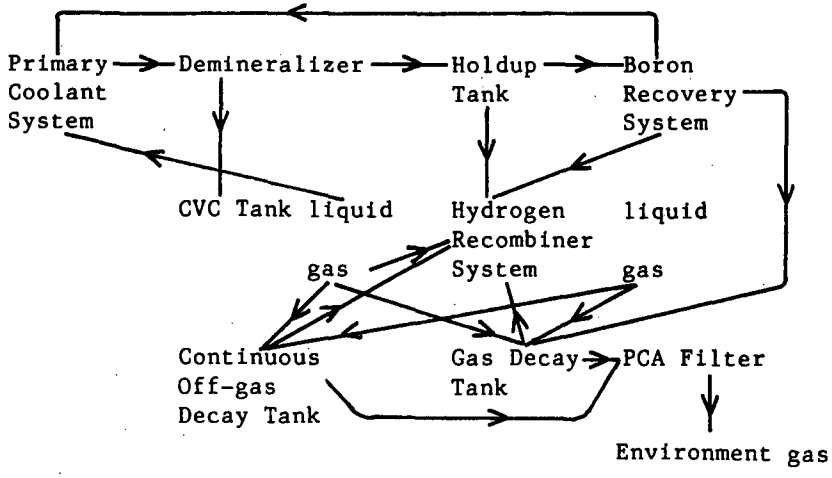


Fig. 1 Primary Coolant Purification System and Gaseous Waste Treatment System

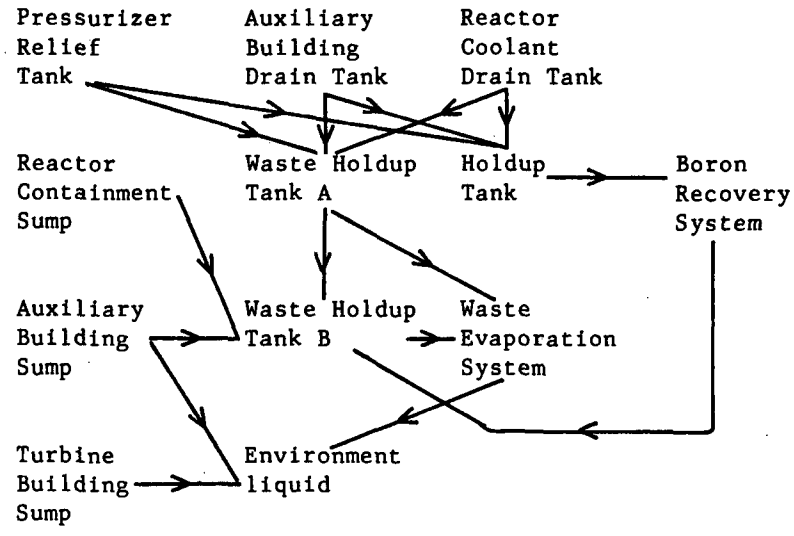


Fig. 2 Liquid Waste Teatment System

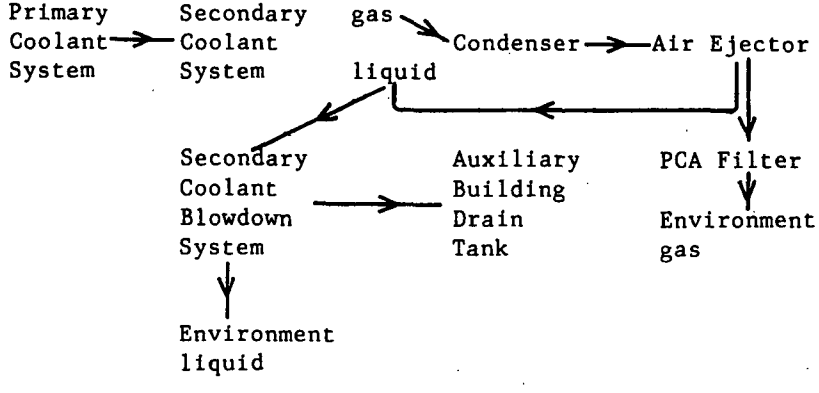


Fig. 3 Secondary Coolant System

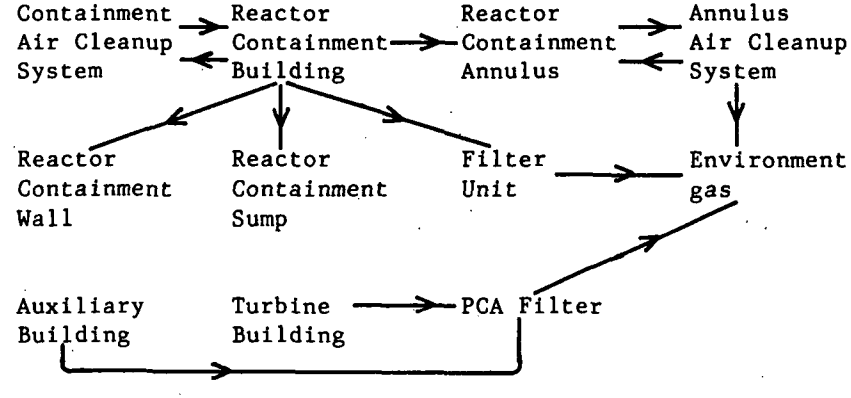


Fig. 4 Accidental Air Containment System

Purification system i (DF)

$j \xrightarrow{FI} i \xrightarrow{FO} l$

$H_{ij} = (FI - FO/DF)/V_j$

$H_{li} = 0$

$H_{lj} = FO/DF/V_j$

Filtration system i (EF)

$j \xrightarrow{F} i \xrightarrow{F} l$

$H_{ij} = EF*F/V_j$

$H_{li} = 0$

$Hlj = (1-EF)*F/V_j$

Partition factor i:l (PF)

$j \xrightarrow{F}$ i (gaseous), l (liquid)

$H_{ij} = PF*F/V_j$

$H_{lj} = (1-PF)*F/V_j$

Tank (Partition coefficient PC)

$j \xrightarrow{FI} i$ (gaseous) $\xrightarrow{G} k$, (liquid) $\xrightarrow{FO} l$

$H_{ij} = FI/V_j$

$H_{ki} = PC*G/V_{il}$

$H_{li} = (1-PF)*FO/V_{il}$

$= (1-PC*V_{ig}/V_{il})*FO/V_{il}$

Fig. 5 Examples of Transport Coefficient

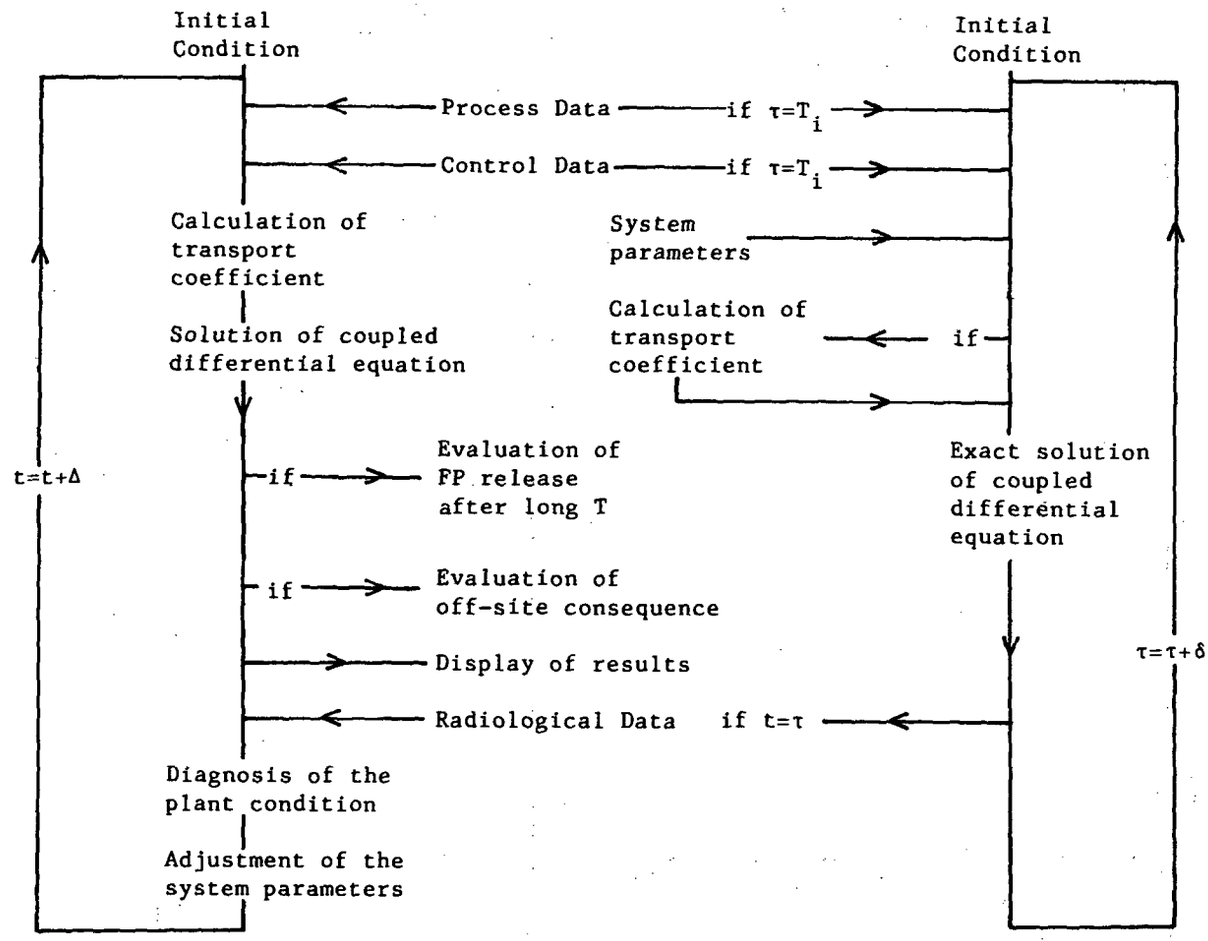


Fig. 6 Schematic Flow Diagrams and Interrelation of MADS and SACHET

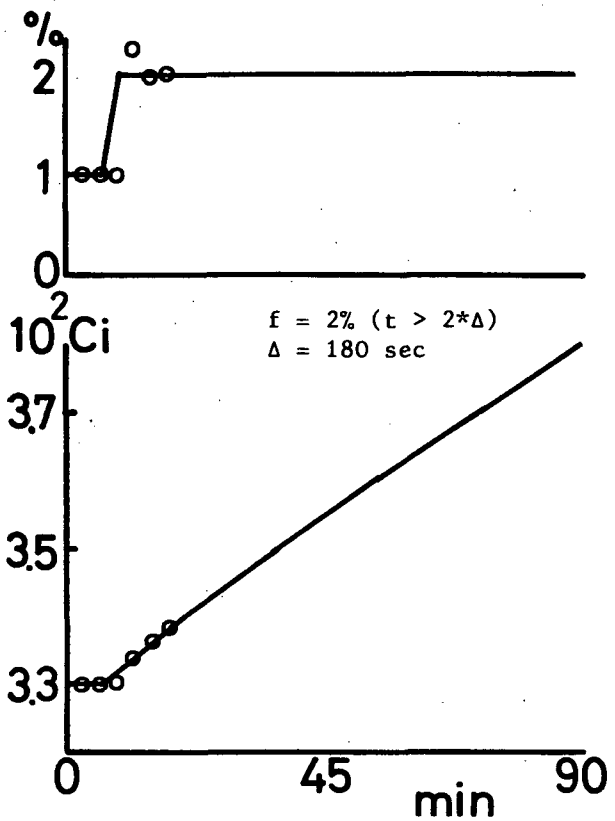


Fig. 7 Inventory of I-131 in the 1ry coolant and adjusted fuel failures in MADS

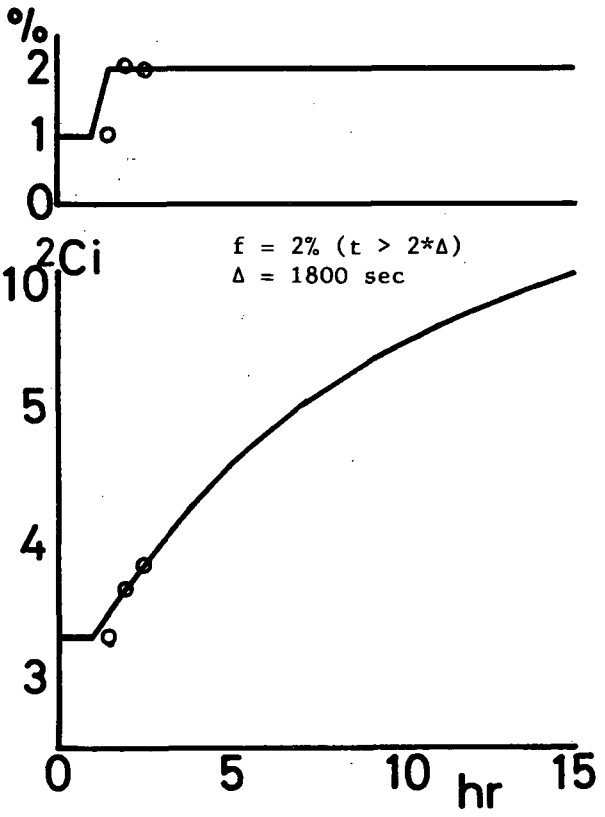


Fig. 8 Inventory of I-131 in the 1ry coolant and adjusted fuel failures in MADS

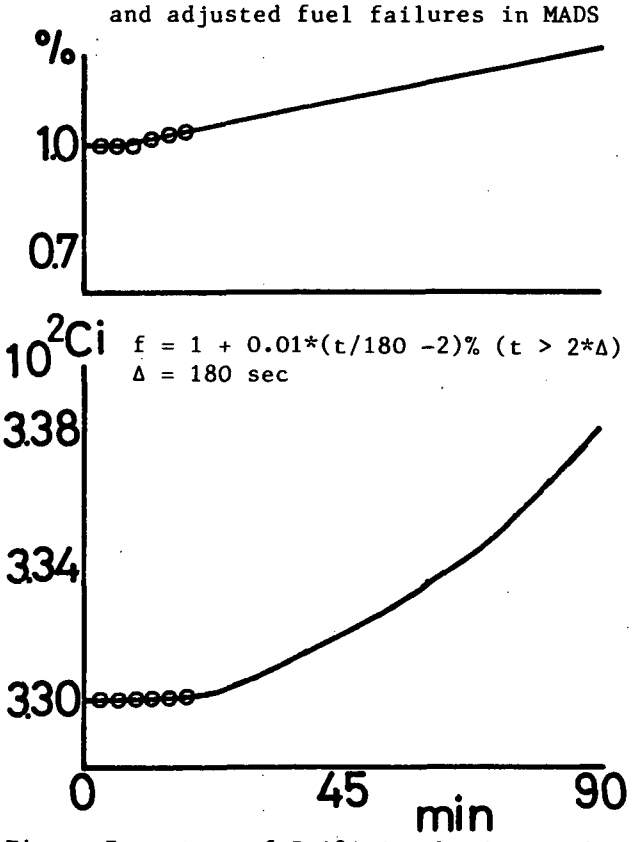


Fig. 9 Inventory of I-131 in the 1ry coolant and adjusted fuel failures in MADS

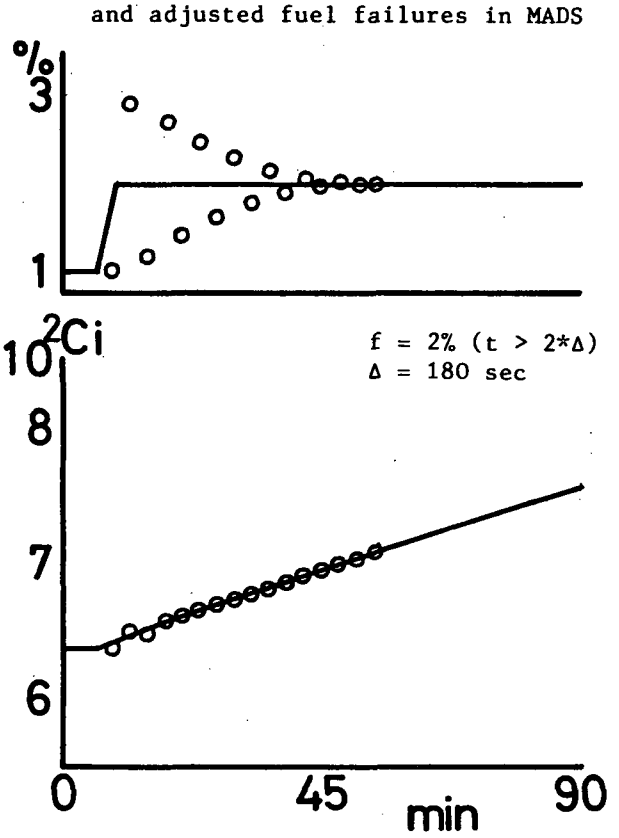


Fig. 10 Inventory of I-133 in the 1ry coolant and adjusted fuel failures in MADS

SESSION 11

PRESSURIZED THERMAL SHOCK - 2

Chair: R. Bello *(CNSNS)*
G. Whitman *(ORNL)*

Panel Discussion on

PRESSURIZED THERMAL SHOCK

Chair: G. Whitman *(ORNL)*

Panelists

R. Cheverton *(ORNL)*
V. Chexal *(EPRI)*
K. Kuszmaul *(USt)*
A. Lucia *(JRC)*
R. Noel *(EdF)*
M. Vagins *(NRC)*

THE CONSEQUENCE OF THE COINCIDENCE OF IRRADIATION EMBRITTLEMENT; SURFACE CRACKING AND PRESSURIZED THERMAL SHOCK (PTS) IN RPVs OF LWRs

K. Kussmaul, J. Jansky, and J. Föhl

Staatliche Materialprüfungsanstalt (MPA)
University of Stuttgart
Pfaffenwaldring 32
D-7000 Stuttgart 80, W. Germany

ABSTRACT

One important project within the German Research Programme "Integrity of Components" focusses on the consequences of a small break LOCA with respect to the Pressurized Water Reactor (PWR) pressure vessel integrity. To answer the question of possible failure modes resulting from overcooling transients, a lower bound approach had to be developed as a preventive tool to demonstrate the safety margin for extremely long range operation, and a necessary step to a better understanding of the effect of superimposed mechanical, thermal and residual stresses. Therefore, a conservatively severe pattern of thermal transients was evaluated and correlated to an embrittled component-like thick walled hollow cylindrical specimen. The validation of theoretical fracture mechanics analyses for the RPV and the model by means of large scale experiments will be performed under realistic conditions of temperature (absolute and differential) pressure, crack pattern, and material embrittlement.

DEFINITION OF "PRESSURIZED THERMAL SHOCK" ON PRESSURE-RETAINING COMPONENTS

Adequate safety measures against catastrophic failure in a PWR primary system (156 bar) are designed into the operating procedures for system temperature transitions (e.g., start-up, shutdown), which are specified so that pressure remains at about 50 bar above the saturation line for the maximum operating temperature (T = 326 °C). Leaks that cannot be compensated for by the pressurizer result in a rapid drop in system pressure to the saturation pressure determined by the system temperature. Under certain conditions, the emergency core cooling (ECC) system will come into action which cools down the RPV core region under retaining pressure leading to "pressurized thermal shock".

Experiments on "depressurized thermal shock" have been carried out at the Oak Ridge National Laboratory /1/ and at Framatome /2/, the load and material conditions that satisfy the aforementioned requirements have become well known in the meantime. The loading where emergency coolant injection under high pressure is required as given by a small leak in the primary system (e.g. leak size of NW 50 mm) is substantially different from the case of depressurized thermal shock.

TOUGHNESS DEGRADATION THROUGH IRRADIATION

It is therefore necessary to establish material toughness data through the thickness of the vessel wall.

Pressurized thermal shock is characterized by both loading in the elastic-plastic range, where the material toughness behaviour can be described by the upper shelf Charpy impact energy, and in the transition region, where linear-elastic fracture mechanics applies.

In the Federal Republic of Germany, thermal shock during ECC was only under consideration with regard to failure in the linear-elastic range, Fig. 1. Ductile failure

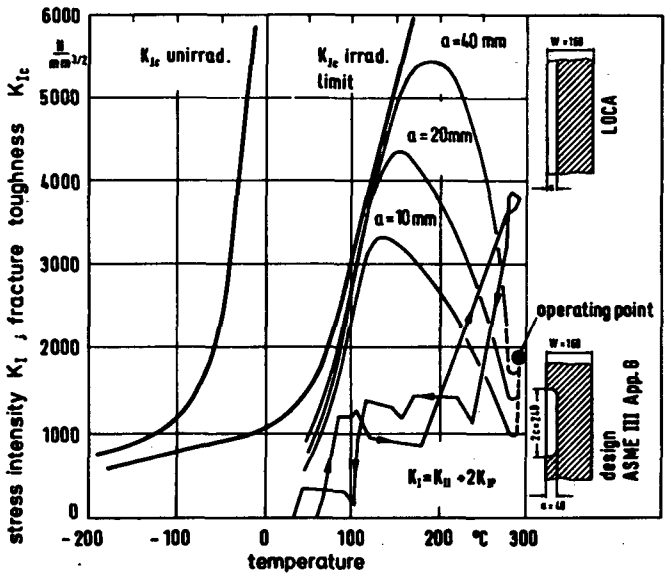


Fig. 1: Loading path during heat-up and cool-down and ECC for different crack depths

has not been regarded as a problem because:

- in no case of toughness degradation has the upper shelf Charpy energy dropped below the 50 ft-lb (68J) lower limit allowed by US regulations (10 CFR 50) and also adopted by German rules
- the results of large-scale specimen tests /3/ show that even material with an upper-shelf Charpy energy of about 40 J has a loading capacity at least equal to or even exceeding the collapse load (yield stress) calculated on the basis of the plane stress conditions, Fig. 2.

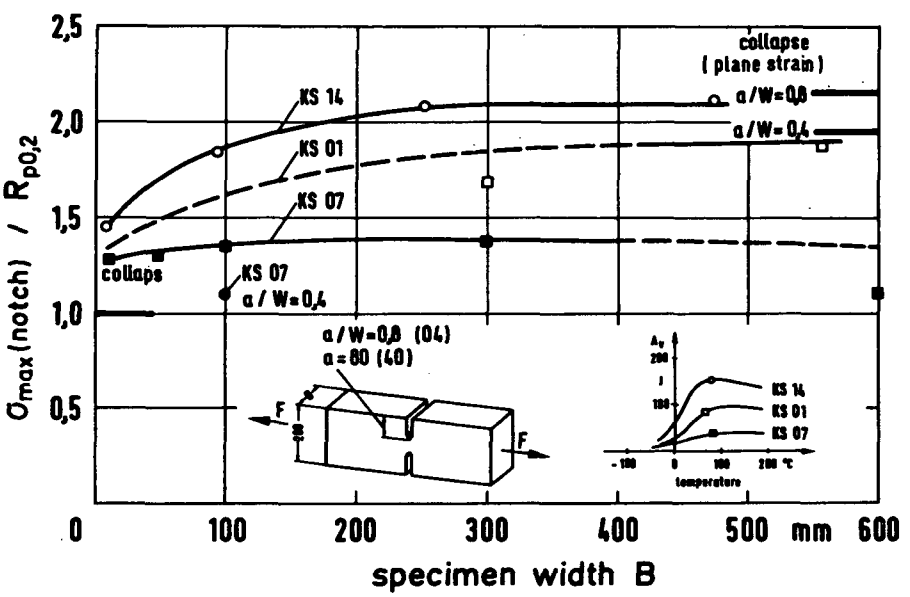


Fig. 2: Plastic limit load for materials with different upper shelf toughness levels and different specimen size

From the boundary conditions of stress intensity during ECC for different crack depths, material requirements can be established from the stress intensity curves (load path) as shown in Fig. 1.

Because surveillance programmes according to current specifications include only Charpy V-notch and tensile specimens, the main problem is to transform results from Charpy impact testing into fracture mechanics properties. The reference temperature concept following the ASME code and related rules leads to a lower limit of fracture toughness, however in a rather conservative way.

The following discussion will include more realistic boundary considerations for different types of material.

Plants Under Special Concern

Two reactor pressure vessels (345 MWe and 625 MWe) built during the mid-1960's contain a circumferential weldment in the core region with a weld material having relatively high sensitivity to neutron embrittlement. Furthermore, these vessels are exposed to a relatively high neutron fluence at the end of life.

On the basis of code trend curves for neutron embrittlement, the toughness degradation can be conservatively predicted. This is shown in Fig. 3 for an assumed EOL fluence of 3.5×10^{19} cm^{-2} (E > 1 MeV) and a weld material representative for older vessels. The shift in transition temperature amounts to approximately 200 K and the drop in upper shelf energy (USE) to about 50 %.

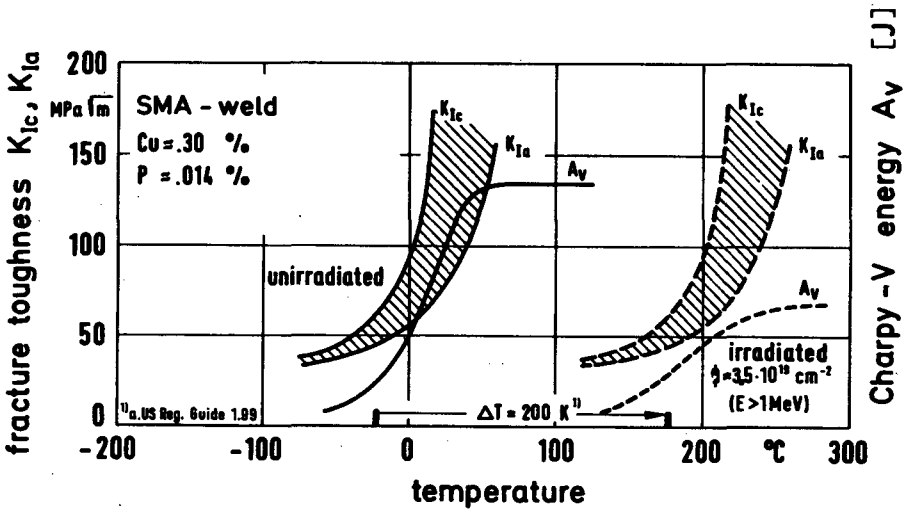


Fig. 3: Toughness degradation due to neutron irradiation for high copper weld material

The reference fracture toughness for the irradiated material indicates that due to the high NDT-Temperature crack initiation will be followed immediately by fast brittle fracture even at temperatures in the range of 200 °C.

Results from surveillance specimens taken from the 345 MW PWR plant exhibit a much smaller shift in ΔT, about 55 K, than that predicted from the US Regulatory Guide trend curves, Fig. 4.

Following the procedures of ASME Section III, Appendix G, and ASME Section XI, the fracture toughness curves also shown in Fig. 4 can be established.

This consideration is restricted to the linear-elastic range only. Realistic component behaviour in the upper shelf and transition region cannot be derived from this basis.

The German research programme "Integrity of Components" investigated in detail the failure mechanism in the elastic-plastic range for different lower-bound materials. The extensive test results combined with data from open literature yielded a correlation between Charpy energy and fracture toughness (crack initaition J_i,

instability K^{**}_{Ic}) as shown in Fig. 5. In this trend curve, material with an upper shelf energy of 35 J as a lower bound for all possible and realistically postulated material conditions in a reactor pressure vessel including EOL is represented.

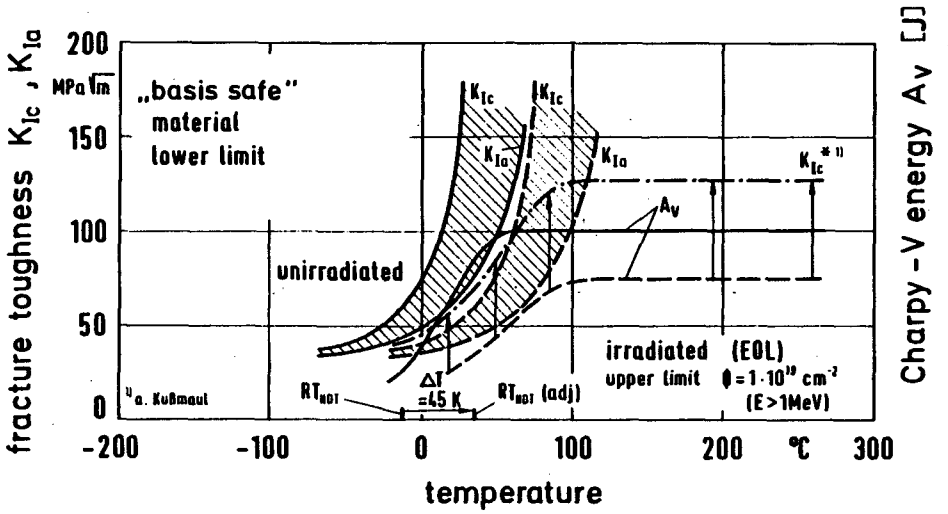


Fig. 4: Evaluation of fracture toughness from Charpy-V surveillance specimens of a 345 MW plant

The fracture toughness of the weld material with a "medium high" copper and phosphorous content derived from this correlation is also plotted in Fig. 4. However, the transition behaviour between the linear-elastic and the elastic-plastic regime is still a remaining problem.

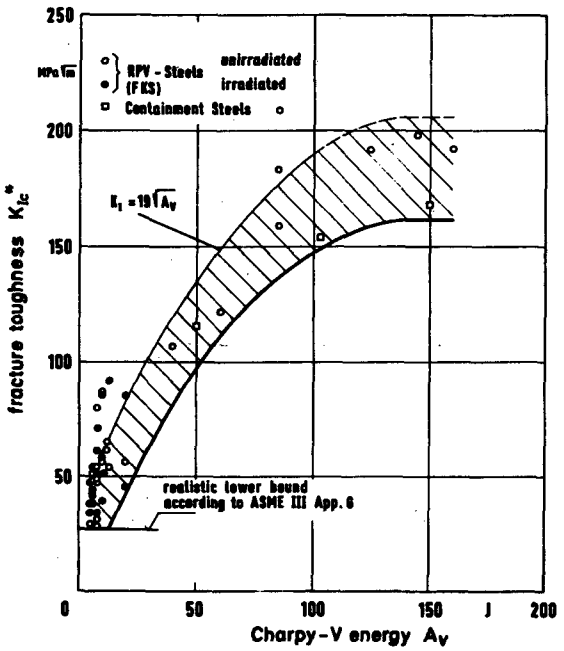


Fig. 5: Correlation between Charpy-V energy and fracture toughness K^{**}_{Ic}

To reduce the EOL fluence as much as possible, changes in the fuel elements arrangement, including the placement of steel dummy elements in positions near the vessel wall have been adopted /4/ several years ago.

Other Plants

In the Federal Republic of Germany, the use of optimized materials of high toughness is required since the early 1970`s. The reduction of accompanying and trace elements as well as a balanced content of alloying elements in the base material affect the sensitivity of the material to neutron embrittlement in a positive way. The deposited weld metal is out of any concern due to the good prerequisites for an extremely high toughness. The EOL fluence is limited to $1{,}0 \times 10^{19}$ cm^{-2} (E > 1 MeV) and will even be somewhat less in practice due to an enlarged water gap.

A lower limit for the Charpy energy temperature curve can be "calculated" from the specified properties of the optimized steel for the BOL and the EOL states, Fig. 6. The transition temperature shift amounts to about 45 K according to Regulatory Guide 1.99, and the upper shelf energy drops from the current lowest allowable level of 100 J to about 75 J (a decrease of about 25 %).

The corresponding fracture toughness curve is also plotted in Fig. 6, according to the procedure previously described.

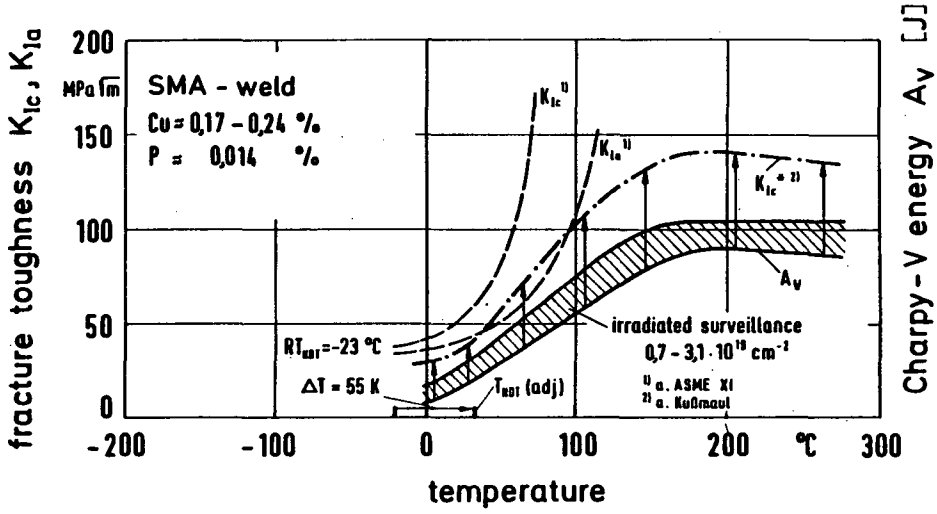


Fig. 6: Toughness degradation through neutron irradiation for optimized RPV material at EOL

REALISTIC SIMULATION OF PRESSURIZED THERMAL SHOCK

In Fig. 7 the stress state of the reactor pressure vessel wall is shown for 80 bar saturation pressure. Realistic tests should represent as nearly as possible the actual stress state and component configuration thereby, the comarability of the component and test wall thickness play a particularly important role. On this basis, a 200 mm wall thickness of the test specimen was selected. In order to include a possible effect of a corrosive medium on crack initiation and partial monotonic growth under PWR conditions, the inner side of the test pieces are subjected to heated water at a pressure of 240 bar which is then exchanged by cold water under retaining pressure.

The circumferential stress in the test specimen resulting from the internal pressure of 240 bar is on a level with 40 N/mm^2 about half of the circumferential stress in the RPV. If the thermal shock test specimen proposed here is loaded in longitidunal direction with an additional axial force of 26.6 MN (resulting in a stress of 80 N/mm^2), the circumferential stress occurring in the real RPV is achieved in the axial direction

of the test specimen. The axial stresses in the RPV wall corresponds roughly to the circumferential stress in the test specimen.

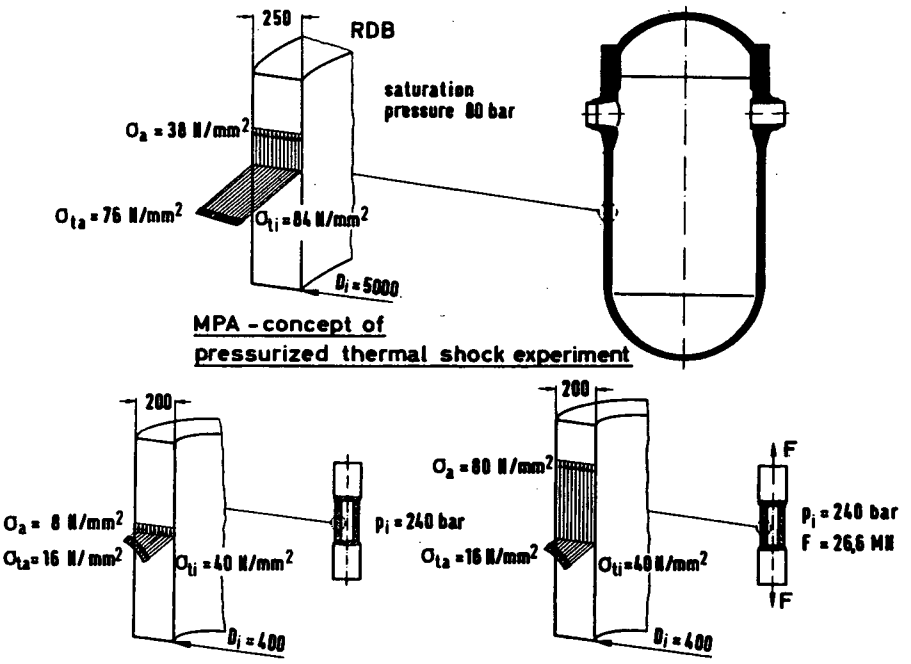


Fig. 7: Comparison between stress state in a reactor pressure vessel and MPA thermal shock test specimen

In comparison to the stress state in the RPV wall, the sense of the principal stresses in the test specimen is rotated by 90°. This implies that an axial crack in the RPV experiences a comparable stress state as it is for a crack in the circumferential direction of the specimen. The toughness of the test specimen will be chosen comparable to the old vessels in the EOL state.

COMPARISON OF OPERATIONAL AND SIMULATED TRANSIENTS

The thermal stresses superimposed on the membrane stresses indicate high positive stresses on the RPV inner surface for sufficiently large heat transfer coefficients. As shown in Fig. 8, heat transfer coefficients over 10 000 W/m² ·K lead to a saturation in temperature differences through the wall thickness.

In time, the stresses acting in the vicinity of the cooled surface (due to force equilibrium over the wall cross-section) decrease as shown in Fig. 9, so that a reduction of the thermally-induced stress peaks at the RPV inner wall occurs. Depending on the duration of cooldown, the wall depth over which positive thermal stresses act increases, whereby the corresponding stress intensity factors at a given wall depth become larger. The influence of the heat transfer coefficient on the temperature differences decreases with wall depth, so that the temperature dependent fracture mechanics parameters, such as COD, J-Integral, K_{Ic} and $K_{Ic}^{\cdot\cdot}$ are affected less. The determination of realistic transfer coefficients between the coolant and the RPV wall has instigated controversial discussions about the conservatism of different investigations in this field. Figure 10 shows the temperature history measured on a nozzle of the experimental HDR plant cooled by thermal shock while under nominal operating conditions (T=306 °C, p = 106 bar) /5/. The nozzle was cooled using a specially designed spray sparger assembly. The heat transfer coefficients in the HDR tests were higher than the aforementioned boundary value of 10 000 W/m³ K. A comparable cooling set-up will be used for the planned tests discussed in this paper.

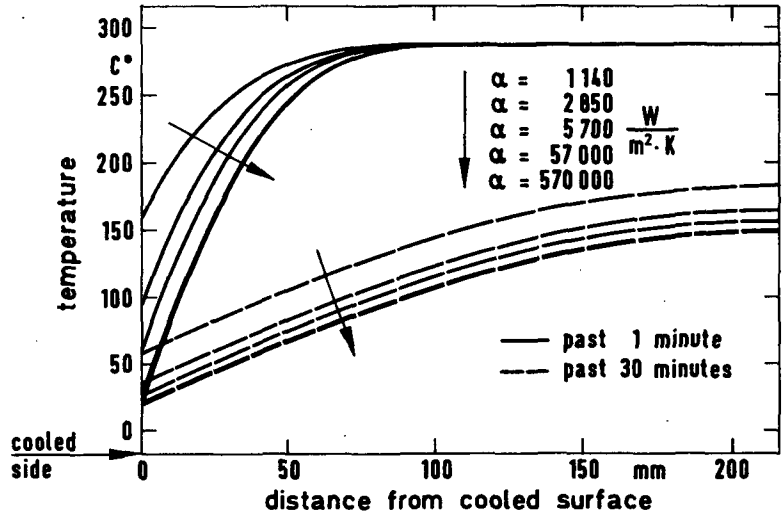
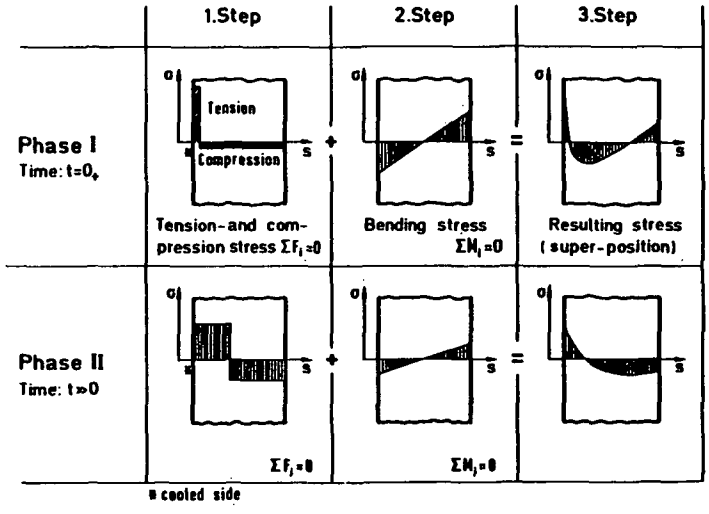


Fig. 8: Temperature distribution as a function of heat exchange coefficient



Stress state through the wall thickness by one-sided cooling

Fig. 9: Stress state through the wall thickness caused by one-sided cooling

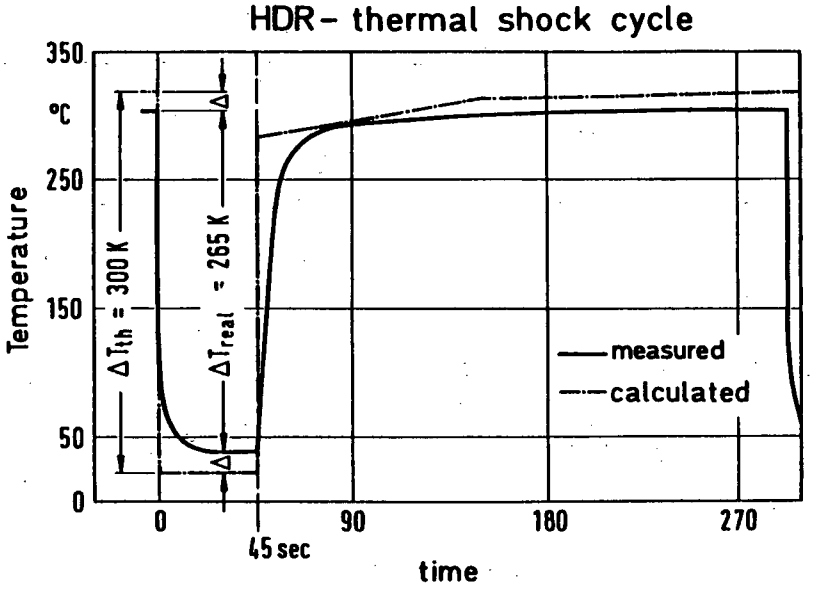


Fig. 10: Surface temperature during HDR-thermal shock experiment at nozzle corner

FRACTURE MECHANICS ANALYSIS FOR MPA THERMAL SHOCK

During the cool-down of the specimen wall, a time-varying temperature profile through the wall results, and therefore, part of the temperature-dependent deformation takes place as a consequence of local stresses rather than global strains. Because local effects are concerned that do not lead to gross deformation of the structure, these stresses must equilibrate over the wall thickness. Should a crack be present in the wall (e.g., an infinitely long axial crack), then the already separated crack edges will be loaded by the thermally-induced stresses (causing crack edge translation) and a moment (causing crack edge rotation).

The stress intensity resulting from pressurized thermal shock superimposed on the membrane stresses cause a rise in the overall K_I level not only in the peak region but also across the entire wall.

Figure 11 shows how this superimposed "driving force" can be affected by changing the relevant parameters. The drop of K_I in thickness direction, and therefore, the possibility to arrest the crack is reduced as the internal pressure increases.

Should a running crack reach a depth where the stress intensity induced by internal pressure alone exceeds the local material fracture toughness either a leak (initiation in radial direction) or rupture (initiation in axial direction) will occur.

Calculations of the temperature field show that almost 600 sec are needed until the cooling front clearly penetrates the wall thickness. At this time, the maximum thermal stress level (stress intensity) is attained, Fig. 12. A comprehensive consideration of the crack tip loading is given by Fig. 13, in which the stress intensity K_I is plotted as a function of crack tip temperature. The fracture toughness values in the same figure allows the evaluation of individual crack depths.

If one considers a flaw with a depth of 50 mm (i.e. an ASME design flaw), it can be seen that the crack tip already senses an increase in stress intensity at a tip temperature of 30 °C ($K_I = K^{*}_{Ic}$). Because the stress intensity at the crack tip further increases with cooling time, propagation of the crack tip takes place with a time-dependent velocity da/dt to effect a decrease in the thermal strains (relaxation process in the structure). High da/dt rates can cause corresponding increases in crack tip loading due to increasing crack depth, as indicated by the arrow 1 in Fig. 13. If while "on the way" to the largest stress intensity value the crack tip reaches a region where the laws of linear-elastic fracture mechanics apply (as would be the case below temperatures of about 170 °C for critical materials at EOL), spontaneous crack propagation in the direction of increasing depth, Fig. 13, arrow 2, can occur with possible crack arrest at a given wall depth due to decreasing thermal stresses.

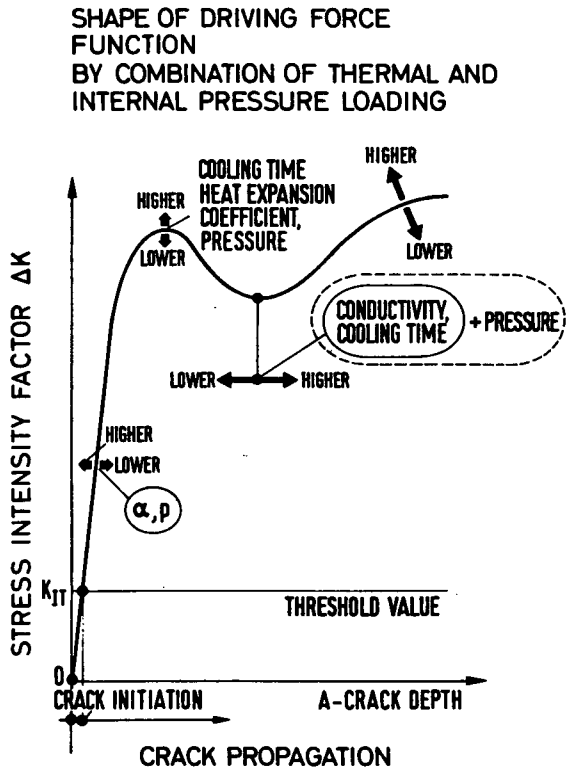


Fig. 11: Parameters influencing the crack during force

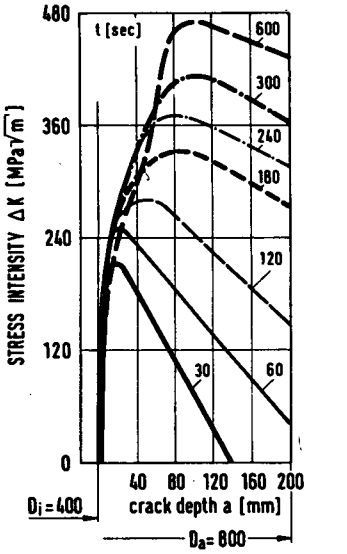


Fig. 12: Driving force (K) during pressurized thermal shock experiment (circumferential crack)

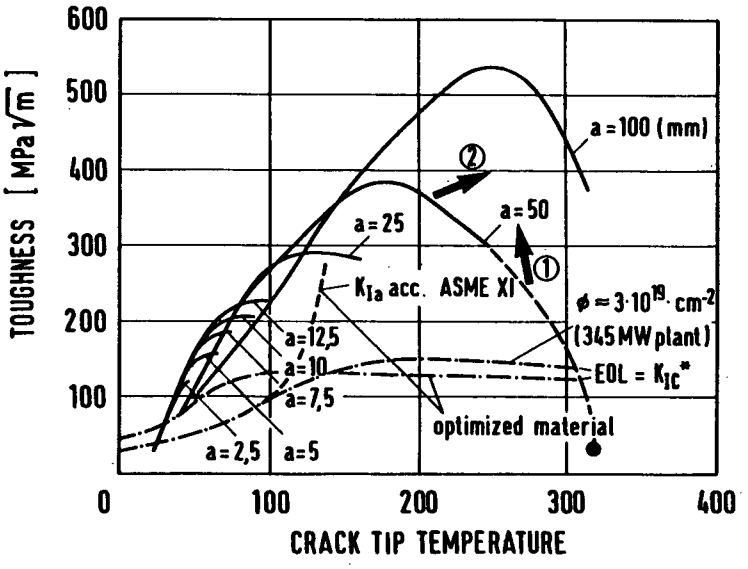


Fig. 13: Comparison of stress intensity and fracture toughness evaluated from Charpy-V results of surveillance specimens

The largest plastic deformation -- separation of the crack edges (translation and rotation)-- occurs when the stress intensity maximum is attained. A reversal in the direction of crack edge displacement (i.e., crack closure) results in a reduction of the stress intensity on the crack tip as well as in a build-up of compression ahead of the crack tip. Under these conditions further crack initiation and propagation cannot occur (warm prestressing effect). This effect can advantageously be used by reversing

the direction of crack edge displacement once again in positive direction (as would be the case, for example, for repressurization by ECC). As can be clearly seen in Fig. 13, on the one hand, cracks deeper than 50 mm can deepen only through monotonic growth into the region of potential brittle fracture. Crack jumps (initiation and arrest processes) on the other hand, can occur for crack depths less than 50 mm, particularly under EOL conditions in welded joints with high copper content. The same is also relevant for optimized materials for crack depths under 25 mm.

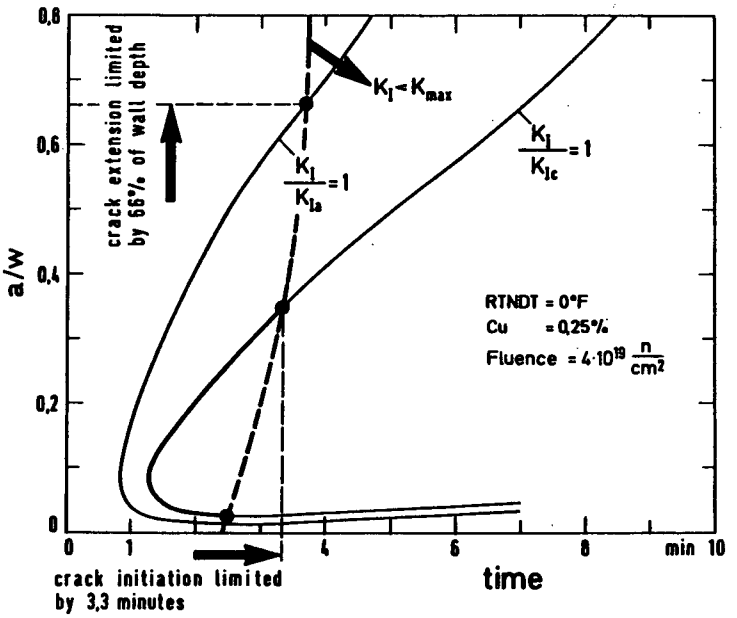


Fig. 14: Theoretical evaluation of crack arrest considering warm-prestress effect according to OCA-1

It must be noted that the smaller the crack depth, the lower the temperature must be for crack initiation with subsequent crack jump. The time period in which the warm pre-stressing conditions occur decrease with smaller crack depth, as it is clearly demonstrated by analyses with OCA-1 /6/, in Fig. 14.

To what extend the actual behaviour of the crack tip is governed by elastic-plastic processes must be evaluated by sophisticated theoretical analysis and consequently be verified experimentally.

CRACKING DUE TO PRESSURIZED THERMAL SHOCK IN A CU-ALLOYED HIGH STRENGTH STEEL DRUM

Following a rapid shutdown of a coal fired power plant in 1965 that had been operated at a temperature and pressure of 290 °C and 80 bar, several leaks occurred near the downpipes roll-in of a boiler drum. Examinations of the drum inner surface indicated surface cracks of 50 mm length on each of four tube holes. The defects were all located at about the same circumferential position below the level at which feed-water was injected.

Destructive examination showed maximum crack depths up to about 82 mm, and that cracks towards the inner surface were shorter than those deeper in the wall thickness, Fig. 15. The fractographic investigations indicated spontaneous crack propagation.

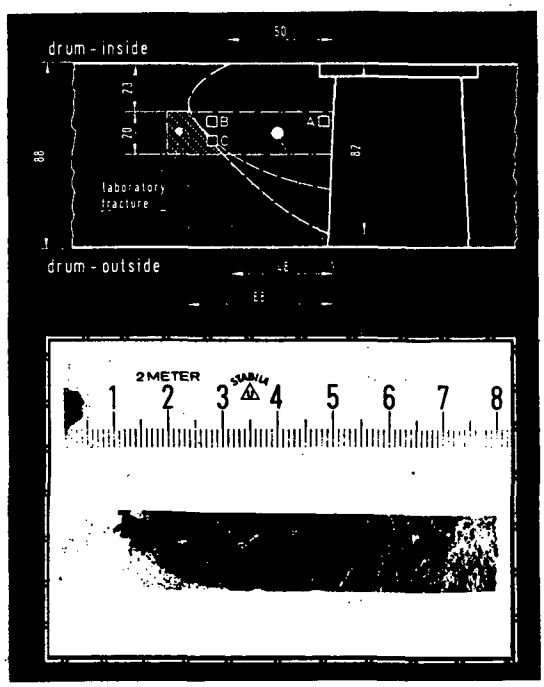


Fig. 15: Fractography of crack in a boiler drum resulting from pressurized thermal shock

It can be concluded that the running crack was arrested not by higher material toughness (onset of upper shelf energy of about 40 J in the range of 200 °C), but rather because of the decrease in crack driving force.

Additional evidence was provided by a foundary calculation of the dependence of K-value on cooling time; these calculations were based on similar ones carried out for a HDR-nozzle. The notch impact energy was transformed and compared with the calculated K-values, Fig. 16.

The results of these calculations indicate that crack propagation of about 75 mm in the direction of the outer wall surface has to be expected when internal pressure thermal and stresses act together. In the load direction where the thermal stresses act alone, an initial crack would achieve a final depth of only about 60 mm due to the lower stress intensity.

Because of the assumptions required for the calculation, the agreement with the actual findings can only be regarded as coincidental. Nevertheless, it does give a qualitative indication of the events occurring during pressurized thermal shock, and furthermore, confirms the potential danger of such kind of loading pressure retaining components.

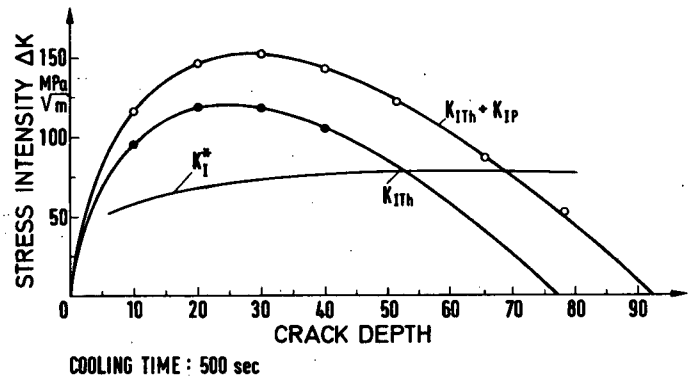


Fig. 16: Calculated stress intensities and fracture toughness of the boiler drum in case of failure during pressurized thermal shock

CONCLUSIONS AND RECOMMENDATIONS

The analyses to date show that the possible consequences of pressurized thermal shock (e.g., failure of RPV) must be reckoned with only if all boundary conditions considered in this contribution -- internal pressure, thermal shock loading of the RPV wall, depth of crack capable of crack initiation, embrittled material in front of the crack tip, and repressurization -- are present during the cooldown phase.

The most economical measures lie in the operation and design areas. Prevention of repressurization during the thermal transient and reduction of thermal shock loading in the embrittled core area are included in these measures. The first requirement can be realized with appropriate intervention in the control system. The greatest temperature difference, and consequently, the highest thermal shock loading (which only occurs in case of high pressure cooling), can be kept away from the embrittled RPV wall by introducing the emergency cooling pipe into the primary nozzle adjacent to the hot outlet nozzle (hot leg). The piping material is not embrittled by irradiation, and therefore, failure is not possible because of high toughness in this area. A higher temperature of the coolant can also contribute to solve the problem of fast fracture. The most expensive measure to prevent the consequences of this transient is to anneal the RPV and thereby at least partially restore the original toughness.

Concerning two older reactor pressure vessels in Germany, which would be the first to come into a critical situation according to the lay out, a sufficient safety margin could be demonstrated. This could be achieved by means of results obtained from additional research programmes supported by a modified operation scheme and repeated inservice inspection. With regard to an extremely long-range operation, and the need to basically validate the methods for fracture analysis in case of superimposed thermal and mechanical residual stresses, theoretical and experimental studies of component behaviour are under way.

REFERENCES

1. R.D. CHEVERTON, "Pressure Vessel Fracture Studies Pertaining to a PWR LOCA-ECC Thermal Shock: Experiments TSE-1 and TSE-2", ORNL/NUREG/TM-31, September 1976

2. PELLISIER-TANON, "Framatome Thermal Shock Experiment"; presented paper to Section G at SMiRT-Conference, Paris, 1981

3. K. KUSSMAUL, "The Integration of the Tensile and C_V-Tests in an Experimentally Verified Engineering Fracture Mechanics Approach - Sicherheit der druckführenden Umschließung von Leichtwasserreaktoren", 7th MPA Seminar - 8/9 October 1981

4. K. KUSSMAUL, "German Approach to the Structural Integrity of Irradiated Nuclear Light Water Reactor Vessels", IAEA Specialists' Meeting on Irradiation Embrittlement and Surveillance of Reactor Pressure Components", Vienna, 19 - 21 Ocotber 1981

5. JANSKY, J., et al, "HDR-Sicherheitsprogramm; Ergebnisse der HDR-Thermoschockversuche V66.0 und V66.1, 5. Statusbericht des HDR-Sicherheitsprogrammes des Kernforschungszentrums Karlsruhe, 10. Dezember 1981

6. S.K. ISKANDER et al, "OCA-1, A code for Calculating the Behaviour of Flaws on the Inner Surface of a Pressure Vessel Subjected to Temperature and Pressure Transients. NUREG/CR-2113, ORNL/NUREG-84, August 1981

THE EPRI PROGRAM CONCERNING REACTOR VESSEL PRESSURIZED THERMAL SHOCK

V.K. (Bindi) Chexal, T.U. Marston, and Bill K.H. Sun
Electric Power Research Institute
Palo Alto, CA 94304

The long-term potential for neutron embrittlement of reactor vessels has been a recognized concern for a number of years. Recently, significant attention has been focused on the performance of certain vessels during overcooling transients.[1] Such an overcooling system transient can occur in a variety of ways. These include primary system breaks, secondary system breaks, and excessive feedwater flow. The likelihood of such a transient posing a real challenge to the reactor vessel is related to the simultaneous occurrence of several conditions. These necessary, but not sufficient, conditions are:

- The reactor vessel has become highly embrittled and thus the brittle to ductile transition region of the vessel material has shifted to higher temperatures.
- There is a crack or flaw in the vessel of sufficient size to propagate.
- There are large induced thermal stresses in the vessel beltline region that are caused by cold water cascading by this region.
- The reactor remains pressurized or is repressurized during a time of decreasing temperatures.

The pressurized thermal shock issue is unique because of:

i) Technical complexity (involves many disciplines, i.e., thermal-hydraulics, neutronics, materials, and fracture mechanics).

ii) Dynamic nature--vessel conditions change with age (neutron embrittlement, annealing).

iii) Reactor vessel failure consequences not currently part of safety analyses.

iv) Economic incentive to assure reactor vessel integrity.

v) Political and media popularity.

The Electric Power Research Institute (EPRI) has been supporting research on reactor vessel integrity for a number of years. This work in the past focused mainly on materials and dosimetry. In June 1981, thermal hydraulics research also was expanded and accelerated. In addition, a cooperative program with four utilities was initiated to evaluate reactor vessel thermal shock for four specific plants.

The pressurized thermal shock issue is being addressed at EPRI using matrix management to coordinate and apply the program results. In its program, EPRI is:

- Developing the capability to predict accurately reactor vessel wall transient temperatures
- Developing the capability to determine accurately vessel wall radiation exposure
- Developing the capability to determine accurately reactor vessel toughness
- Developing a linked set of analytical codes so that utilities or their contractors can assess independently the effects of reactor vessel thermal shock with high accuracy
- Investigating ways to extend a reactor vessel's life.

PREDICTING TRANSIENT TEMPERATURES

To accurately determine the impact of reactor vessel wall temperature transients on the reactor vessel, it is essential to know the magnitude of the transients. To this end, EPRI has an effort underway to determine more precisely the fluid temperature and the heat transfer coefficient at the downcomer beltline region of reactor vessels during various transient conditions. These are important inputs to vessel capability calculations.

EPRI already has completed fluid and thermal mixing tests using one-fifth scale, transparent models, of reactor cold leg and downcomer geometries that are representative of B&W, W, and CE plants. Tests have also been completed in a two-dimensional, transparent, full height test facility. In addition, tests are planned using a one-half scale facility that can operate at up to 200 psia.[2] The objective of this facility is to:

- provide steady-state and transient data on thermal mixing for
  - phenomenological understanding
  - development of heat transfer correlation
  - code assessment
- provide scaling rationale to apply data to reactor conditions
- help develop, assess, and improve turbulent mixing models in computer codes.

EPRI is continuing to improve a three-dimensional computer code, COMMIX[3], that can predict the mixing of fluid streams. It is being used to analyze the mixing of emergency cooling water (injected into the reactor) and reactor water.

Figure 1 shows a sketch of the one-fifth scale facility representative of W and CE plants. Figure 2 shows the effect of loop flow to HPI flow ratio on fluid temperature at thermocouple location #1. Figure 3 shows a comparison of the test data with the code predictions for one of several tests run in this facility. The physical trends are reproduced correctly and good quantitative agreement is observed, especially for the temperature distribution in the downcomer. The EPRI program provides for continuously improving the accuracy of the codes as new data become available.

VESSEL WALL EXPOSURE

To determine how much ductility a reactor vessel wall has lost, one must know how much neutron exposure it has had. EPRI is sponsoring analytical and experimental programs to predict more accurately the reactor wall fluence level and its energy spectrum from dosimetry measurements.

A number of observations and recommendations have resulted from the EPRI dosimetry program:

- There is a 50% uncertainty in determining vessel wall neutron fluence from foils when making generic analyses and 20-30% for plant specific analyses.
- It appears that damage is predicted best by including all neutrons, not just those with energy greater than 1 MeV, as has been past practice. The neutrons are weighted by an energy-dependent function to determine their damage to the vessel wall material.
- Detailed multigroup neutron transport calculations are needed to obtain accurate information about the neutron spectrum, reaching the foils and vessel wall, and to translate results from test and surveillance samples to material conditions at locations in vessel walls.

Analytical methods must be used to estimate the fluence throughout the reactor vessel wall from foil data because the foils may be located some distance away. Foil data help establish the magnitude of the fluence. There has been a continuing concern about the accuracy of these calculations. This is important where the flux from the core through the wall and to the foil has a steep slope. EPRI has a number of programs to improve these calculational methods including an experiment with foils both inside and outside of the vessel wall.

VESSEL'S INTEGRITY ASSESSMENT

In the vessel capability effort, EPRI will integrate its results with findings from the NRC, the manufacturers programs, and elsewhere. There are three major elements to EPRI's program for determining the capability of reactor vessels. These are: a) the prediction of radiation damage, b) the measurement of fracture toughness of irradiated materials, and c) the measurement of crack arrest properties of irradiated materials.

The research activities that have been launched in support of the vessel capability effort are aimed at:

- accurately determining vessel material properties
- developing advanced elastic and plastic fracture mechanics methods
- improving the understanding of vessel irradiation damage mechanisms and the level of damage that occurs for various exposure levels
- determining what causes cracks to arrest, and how crack arrest capability can be enhanced
- learning more about structural analysis for reactor pressure vessels

- extracting all possible information from surveillance capsules that are taken from reactors
- learning how to determine more accurately the reactor vessel wall irradiation from dosimeter readings
- improving the capability to find, and to determine the size and character of flaws and defects in reactor vessel walls using nondestructive methods.

The results of EPRI testing confirm the conservatism in determining toughness properties of these vessels. Figure 4 shows a plot of RT_{NDT} (reference temperature for brittle to ductile transition region) and 30 ft-lb Charpy temperature for high upper shelf welds. The plot also shows the branch technical position and the trendline based on high shelf data. The shaded region shows the improvement in estimating initial RT_{NDT}. The EPRI recommendation based on these high shelf data is RT_{NDT} = -50°F or the temperature corresponding to 30 ft-lb Charpy, whichever is higher, instead of the conservative branch technical position.

Figure 5 shows the result of one experiment on a high shelf, high copper content weldment to show the conservatism in the irradiated and unirradiated conditions between the data and branch technical position as well as the Reg. Guide 1.99.[4] All of the data are from the EPRI research project 886-2 with the Naval Research Laboratory. The capsules contained Charpy, precracked Charpy and one-inch thick J integral specimens with 20% sidegrooves. The measured fracture data was compared with the predicted fracture toughness values. The prediction can be made using (1) the measure RT_{NDT} and the measured Charpy shift or (2) the inferred RT_{NDT} and the Reg. Guide 1.99.1 (3) predicted shift. Figure 5 shows the various predictions. For the purposes of comparison, the 100 Ksi $\sqrt{in}$ toughness level is selected because it approximates the mid-transition toughness.

Figure 6 compares the results from crack arrest toughness experiments with the predictions using ASME Section XI procedures. Crack arrest toughness determines the conditions (and position) for the arrest of a propagating crack in a LEFM type of analysis and test. The material is a high shelf, low copper SA 533 B1 material irradiated to approximately 1 x 10^{19} n/cm^2. In the figure, the predicted K_{Ia} curves and the test data are shown. The scatter is typical for this type of test. It can be seen that the margin between the data and the predictions are roughly the same for both irradiated and unirradiated materials.

The vessel integrity analysis procedures described above conservatively model the vessel as a brittle elastic material with no credit to the ductility of nuclear pressure vessel steels. In fact, vessel steel is chosen for its high fracture toughness and ductility. It may only be brittle during a PTS event in the cold inside wall. It is probable that existing surface cracks that initiate during the PTS transient, arrest in the hot tough interior vessel wall. To confirm (and claim credit for) this behavior, EPRI research project 2180 is investigating crack arrest in ductile steel, and other ductile material related issues such as the limitations of warm prestressing, and the role of vessel cladding. The objective is to upgrade the current elastic analysis procedures by including plasticity and probabilistic behavior into the computer models.

The objective of the non-destructive examination (NDE) effort is the development and thorough demonstration of an underclad crack detection instrument ready for field use. The emphasis must be on positive proof of reliable detection of underclad cracks of critical size, if NDE is to afford a means of negating the pressurized thermal shock issue. Current activities include the fabrication of a number of underclad crack test samples for screening and qualification and evaluations of

current and emerging technology. Test samples containing about 100 underclad cracks have been completed. Current technology is adequate for strip clad, but is not sufficient for multiwire and manual arc clad (on older vessels). An extensive test program of emerging technologies is now underway.

After identification of the optimum transducers and signal analyses and/or displays, a field useable instrument will be built and integrated into existing PAR inspection tools. The resulting tool will be thoroughly tested to establish detection reliability on a statistically verifiable basis. The resulting tool will be available on a lease basis to utilities and in-service inspection (ISI) vendors.

PLANT SPECIFIC VESSEL EVALUATION

EPRI has an integrated approach to analyze a reactor vessel's ability in response to a pressurized thermal shock event. Cooperative programs have been initiated with four utilities to analyze reactor vessels at four plants, including one from each of the PWR vendors. This cooperative program will give EPRI a chance to perfect and demonstrate this analytical capability. It will also show how the package can be fashioned to make it most valuable and most easily used by the utilities.

Utilities will have the capability to determine, with realistic assumptions and best estimate calculations, the integrity of reactor vessels over their design lifetimes. They will be able to determine limiting events, analyze plant behavior and vessel capability, evaluate the need for and benefit for system modifications, develop improved operating strategies, and investigate the effects of multiple failures and operator errors.

Figure 7 shows the plant analysis task flow chart of how the various computer codes link together in performing the analysis.

The exact chemical composition, and the irradiated and nonirradiated material properties throughout a reactor vessel, are paramount in determining the vessel's ability to resist pressurized thermal shock events. EPRI initiated a major effort to obtain these data from the NRC's material surveillance data base, MATSURV.[5]

EPRI found MATSURV difficult and slow to use. Consequently, EPRI developed and applied a retrieval command systems methodology MENDER-MATSURV[6] in order to efficiently retrieve data from MATSURV. EPRI can now retrieve information for any plant from MATSURV concerning:

- Reactor pressure vessel materials
- Baseline surveillance program materials that were tested prior to irradiation
- Surveillance program materials that have been irradiated.

EPRI has also developed two large nuclear reactor pressure vessel steel data bases and is in the process of determining if its extensive unirradiated and irradiated pressure vessel steel data base can be combined with MATSURV to provide a standardized unified data base, to be used by all concerned in RPV integrity assessment. This would reduce the inconsistencies in integrity assessment caused by data from different materials data bases.

Figures 8 and 9 show the three-dimensional temperature and velocity profiles during a transient calculation in the downcomer obtained using the COMMIX code to

better predict the transient temperature history at the vessel wall for thermal stress calculation. These three-dimensional calculations help remove conservatism from the one-dimensional calculations in the lower end region of loop velocity to safety injection flow velocity.

The vessel integrity analysis requires both a thermal and stress analysis of the reactor vessel wall. Temperatures are calculated through the wall as a function of time for a given transient as shown in Figure 10.[7] These temperatures cause thermally-induced stresses in addition to the pressure stresses in the vessel wall. From the calculated stresses in the wall, a fracture mechanics analysis is performed to determine stress intensity factors for the various assumed crack depths, as shown in Figure 11. At a given time in the transient the stress intensity and the fracture toughness vary with crack depth as shown in Figure 12-a. The fracture toughness, K_{Ic}, is available from Section XI of the ASME Code. When the stress intensity, K_I, exceeds the material toughness, a crack of a given depth (point A) is determined to initiate. If the material toughness is significantly reduced due to embrittlement or reduced temperature, a range of flaws (between points A and B) could initiate as indicated in Figure 12-b. If the stress intensity for an initiated crack falls below the arrest toughness, K_{Ia}, the crack is determined to arrest at a depth as indicated by point D in Figure 12-c. By comparing the material toughness and crack driving force curves at many points in time during a transient, a critical crack depth diagram can be constructed as shown in Figure 13. This curve changes with increasing plant life and is used to evaluate the behavior of flaws of various assumed depths subjected to a particular pressure and temperature transient.

REMEDIAL ACTION EVALUATION

Preliminary results to date have been very encouraging. EPRI believes that the current program will demonstrate that even the older reactor vessels with high copper content welds will be safe for their design lifetimes, without the need for fixes. But this is not yet an established fact and EPRI is backstopping its efforts with programs that seek ways to extend vessel lifetime.

Modifying a plant's operating procedures is one such approach. Warming and reducing the emergency injection water flow and automatically reducing excessive feedwater flow, are ways to reduce overcooling. These are being investigated so that utilities can determine the effectiveness of this technique for each plant.

The safety panel display system has the potential to help the operator avoid shocking the reactor vessel. This is being evaluated.

Another approach to extending vessel lifetime is to reduce the number of neutrons reaching the vessel wall. This can be achieved by fuel management strategies that move the most active fuel away from the edge of the core. But there can be a cost penalty and there are many questions to be answered. The EPRI program examined (1) the types of fuel management changes that can be made, (2) the resulting effects on vessel flux, (3) the effects on fuel cycle costs, (4) the lead time required, (5) the effects on safety margins, (6) the experience in Europe, and (7) the vessel wall toughness benefit of reduced flux.

Figure 14 illustrates the effect of flux reduction on RT_{NDT} through the use of an example. For this purpose, a reactor with a sensitive weld (Cu = 0.35, Ni = 0.75) with an initial RT_{NDT} of 0°F, and a nominal end of life fluence of 4×10^{19} n/cm^2 is proposed. This reactor has seven years of operation and two flux reduction schemes are proposed for immediate implementation. The first is a fuel shuffling method that reduces the flux by a factor of 2. The second is a much more drastic action that includes the replacement of outer fuel assemblies with reflector

assemblies that reduce the flux by a factor of 10. This is accompanied by a loss of thermal margin and a substantial derate of the plant. Figure 14 illustrates the results of the two schemes. In Figure 14(a) the fluence is plotted as a function of effective full power years (EFPY) of operation and the associated RT_{NDT} is plotted in Figure 14(b). The variation in end of life RT_{NDT} is small, despite the substantially reduced flux.

It is clear that the time of flux reduction scheme implementation relative to EFPY is extremely important with regard to limiting RT_{NDT}. In addition, vessel-specific analyses are essential for making any decisions. The benefits of flux reduction are dependent on plant-specific factors, e.g., chemical composition of reactor pressure vessel materials, initial RT_{NDT}, initial vessel flux, age of plant, etc.

If calculations ultimately show that a vessel has become too embrittled to remain in service, thermal annealing of the reactor vessel can be considered. A four year program by EPRI on thermal annealing is complete.

This research indicates that annealing the vessel at 850°F for about 170 hours successfully recovers ductility and minimizes further reembrittlement. Figure 15 illustrates the upper shelf behavior through an embrittlement, anneal, and reembrittlement cycle of a low initial upper shelf (68 ft-lb) high copper (0.36 wt%) weldments. Figure 16 shows the transition temperature behavior. These laboratory experiments illustrate the benefits of using a high (850°F) temperature anneal, but they say absolutely nothing about the feasibility or practicality of performing such a thermal treatment on a reactor vessel.

EPRI's vessel annealing assessment has addressed many matters including reactor vessel dsnign, metallurgical considerations, reactor vessel insulation, primary shield concrete, reactor coolant piping, equipment supports, reactor vessel internals, fuel storage, and health physics. Although the evaluation indicates that there are no generic plant design restrictions that preclude annealing, plant-to-plant variations are important. In addition to the requirement for a plant specific evaluation, several vital ASME Boiler and Pressure vessel code and licensing requirements must be addressed and resolved.

It has become evident that thermal treatment of a reactor vessel will be a complex operation with many ramifications. At this time it is untried and unproven, and not yet an available alternative.

A pilot project to choose between the above proposed remedial actions based on decision analysis is nearing completion.

THE BOTTOM LINE

Reactor vessel thermal shock is not a new problem. But with a growing number of plants approaching their mid-lives, it is a problem that must be understood and dealt with. The effort to gain that understanding is now underway.

It is too early to have the final answer, but the dimensions of the thermal shock problem and ways of dealing with it are becoming discernible. From what we now see, it is a moderate problem, not trauma. It is unlikely that any plant should have to cease operation because of it. At most, some plants may have to make small concessions to mitigate the effects of thermal shock in the way that they operate.

ACKNOWLEDGEMENTS

The work reported here is a synopsis of the effort being carried on by several individuals of the EPRI staff. The authors gratefully acknowledge the contributions of A. Billy, D. Cain, J. Chao, G. Dau, D. Franklin, T. Griesbach, J. Kim, C. Lin, A. Long, R. Nickell, D. Norris, O. Ozer, T. Passell, J. Quinn, W. Reuland, J. Sursock, and H. Wyckoff.

REFERENCES

1. T. Marston, B.K.H. Sun, and B. Chexal, "EPRI Pressurized Thermal Shock Program: Status and Review," presented at the USNRC 9th Water Reactor Safety Research Information Meeting, Gaithersburg, Maryland, October 28, 1981.

2. B.K.H. Sun, et al., "The Thermal-Hydraulic Aspects of the Pressurized Thermal Shock Problem: EPRI Program Status," presented at the USNRC Advanced Code Review Group Meeting, Bethesda, Maryland, April 21-22, 1982.

3. W.T. Sha, et al., "COMMIX-1: A Three-Dimensional Transient Single-Phase Component Computer Program for Thermal-Hydraulic Analysis," USNRC Report NUREG/CR-0785, September 1978.

4. "Effect of Residual Elements on Predicted Radiation Damage to Reactor Vessel Materials," USNRC Regulatory Guide 1.99, July 1975 and Revision 1, April 1977.

5. J. Strosnider, C. Monserrate, L.D. Kenworthy, and C.D. Tether, "Computerized Reactor Pressure Vessel Materials Information System," NUREG-0688, U.S. Nuclear Regulatory Commission, October 1980.

6. A.F. Billy and T.U. Marston, "Role of the Computerized Material Surveillance Information System on Reactor Vessel Integrity Assessment," ASME/ANS Second Joint Nuclear Engineering Conference, Portland, Oregon, July 26, 1982.

7. D.M. Norris, et al., "Integrity Analysis of a Pressurized Water Reactor Vessel Subjected to a Pressure-Temperature Transient," to be presented at the 1982 ASME Winter Annual Meeting, Phoenix, Arizona.

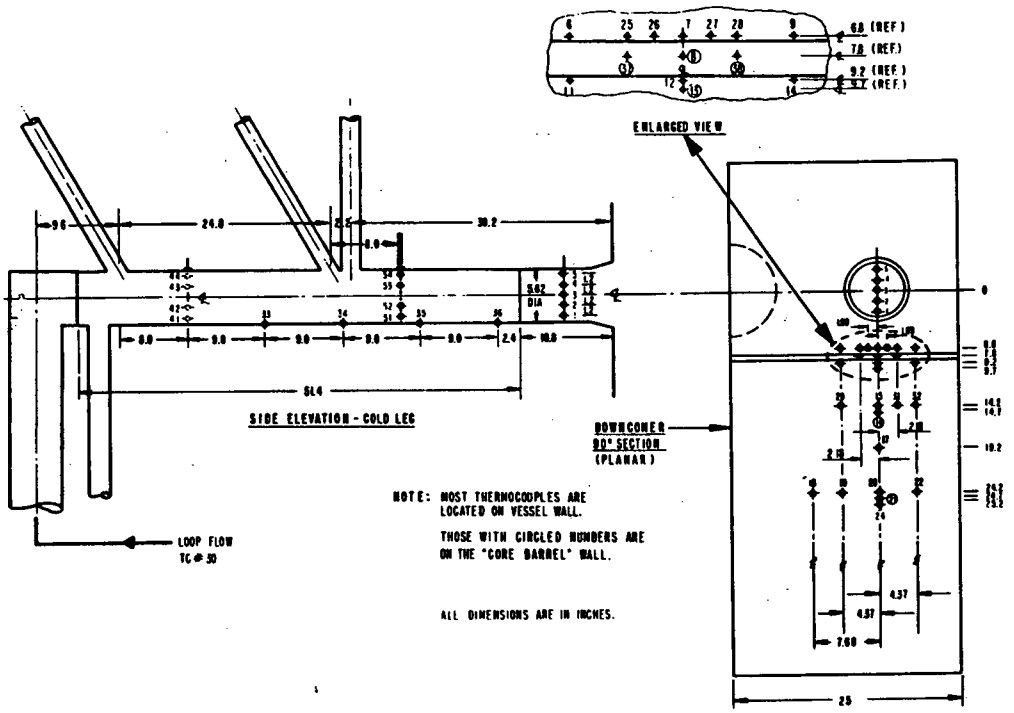


Fig. 1. Mix Rig Thermocouple Locations, Phase II

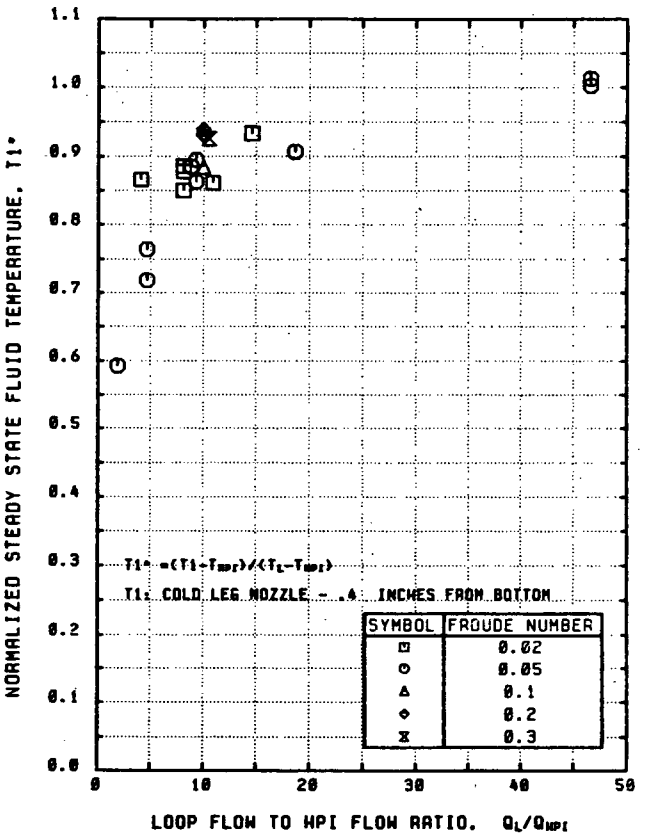


Fig. 2. Effect of Loop Flow to HPI Flow Ratio, Q_L/Q_{HPI} on Normalized Steady State Fluid Temperature, T1

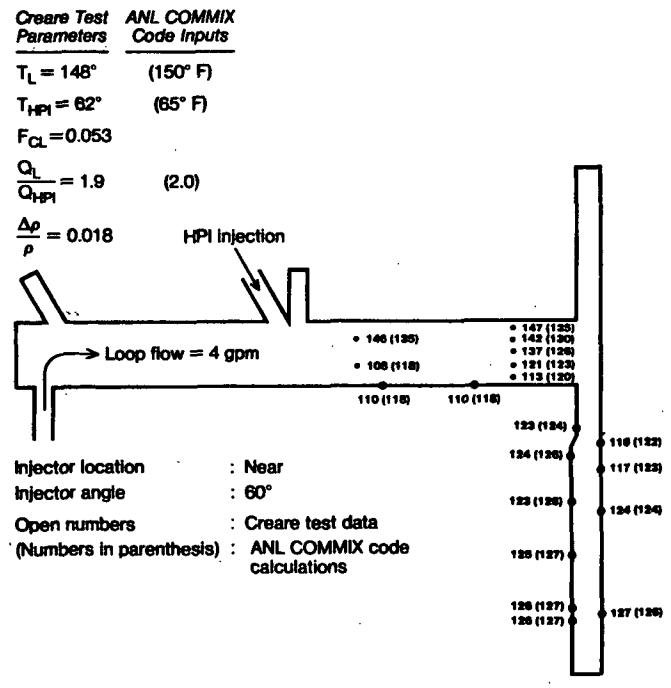


Fig. 3. Temperature Grid (°F), Test Number 51

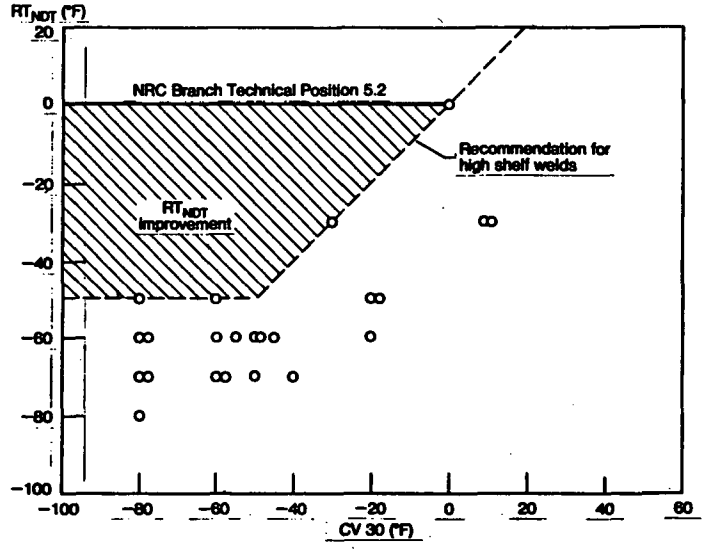


Fig. 4. Plot of RT_{NDT} and 30 ft-lb Charpy Temperature for High Upper Shelf Welds

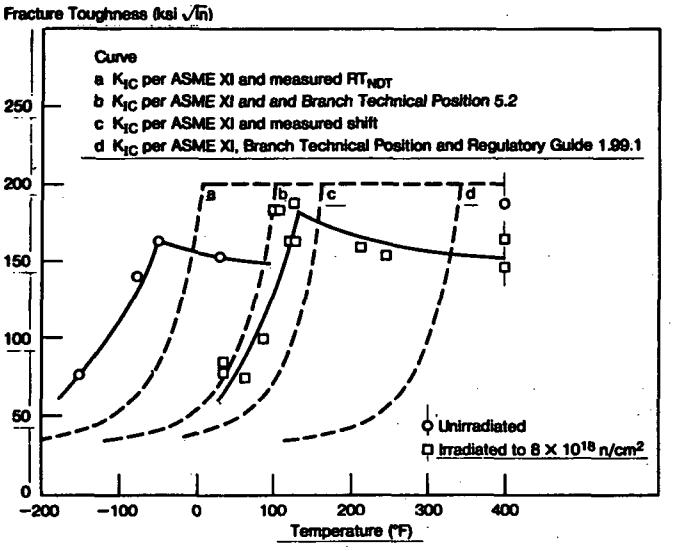


Fig. 5. Comparison between Measured Initiation Fracture Toughness (K_{IC} and K_{JC}) and Predictions for a High Shelf, High Cu Content Weld

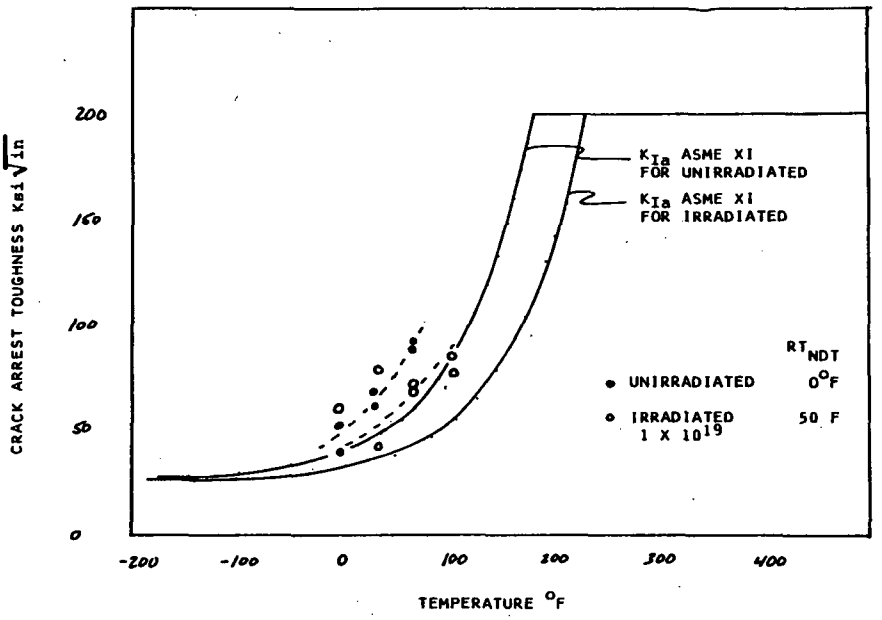


Fig. 6. Comparison between Measured Crack Arrest Toughness (K_{Ia}) and Predictions Using ASME Section XI Procedures

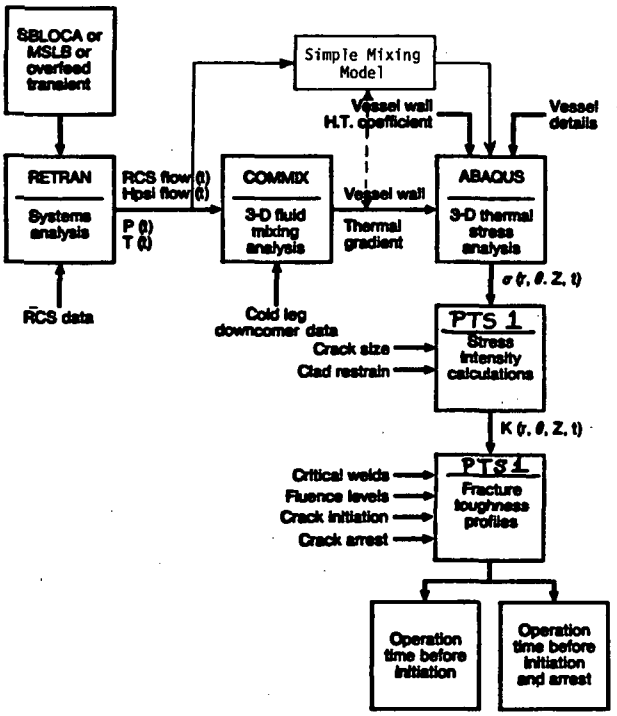
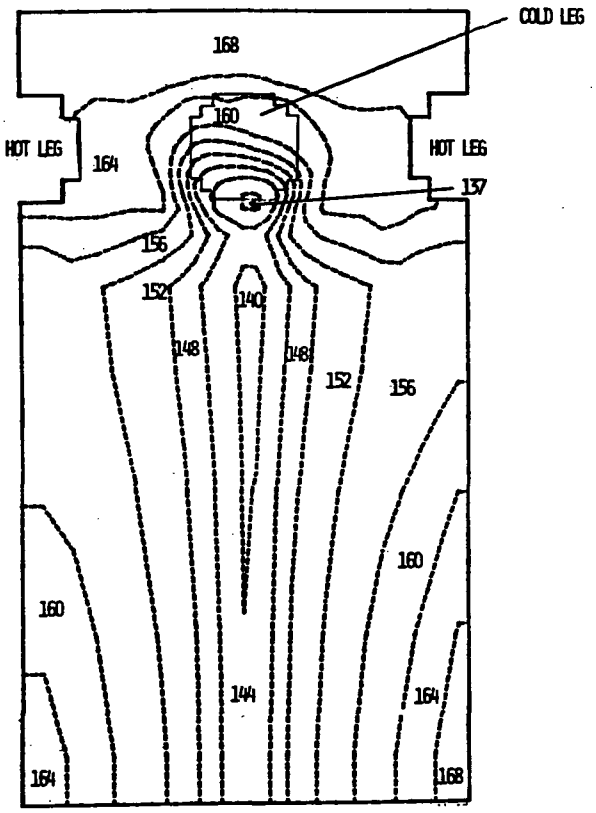


Fig. 7. Plant Analysis Task Flow Chart

Fig. 8. Isotherm Plot for Downcomer Region Near the Vessel Wall [T = 500 sec (C)]



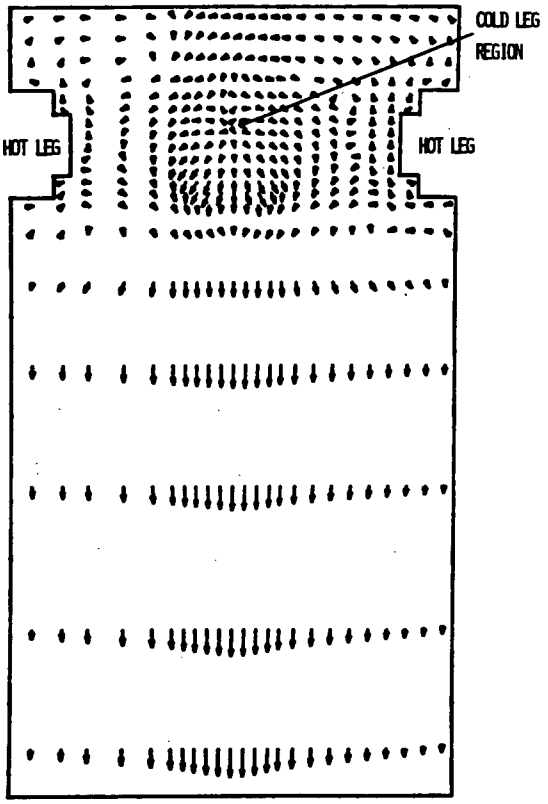


Fig. 9. Velocity Distribution in Downcomer Next to Vessel Wall (T = 500 sec)

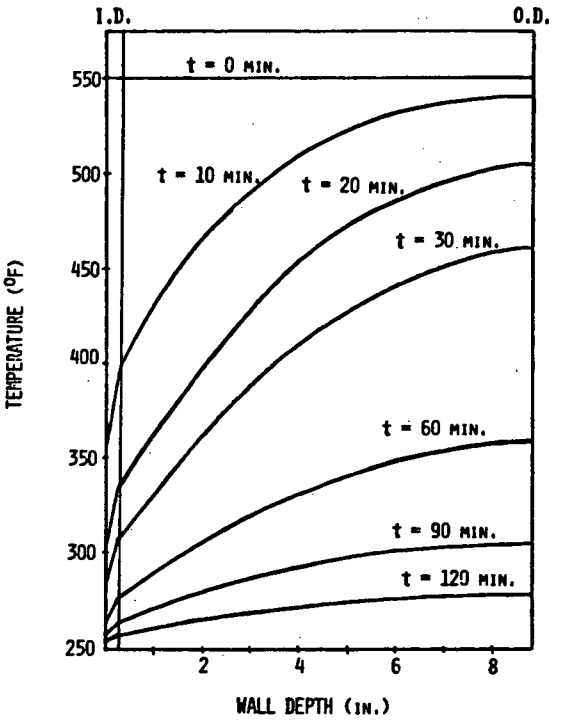


Fig. 10. Temperature vs. Depth in Vessel Wall

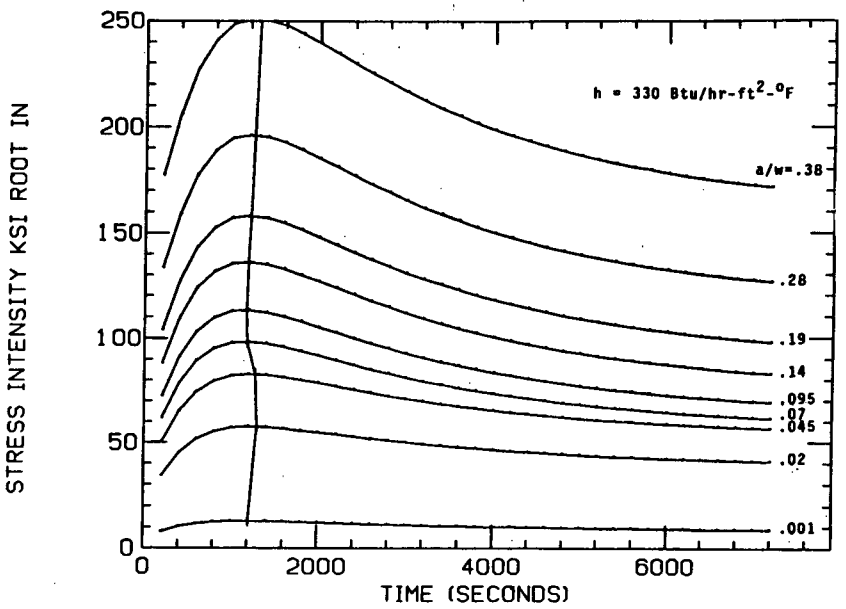


Fig. 11. Stress Intensity vs. Time

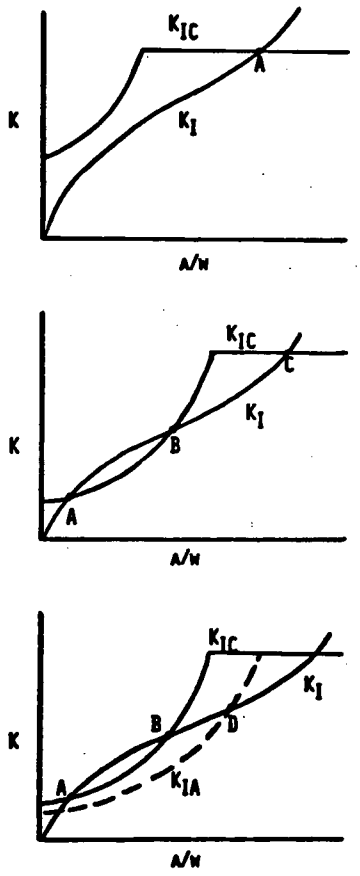


Fig. 12. Toughness and Crack Driving Force Curves

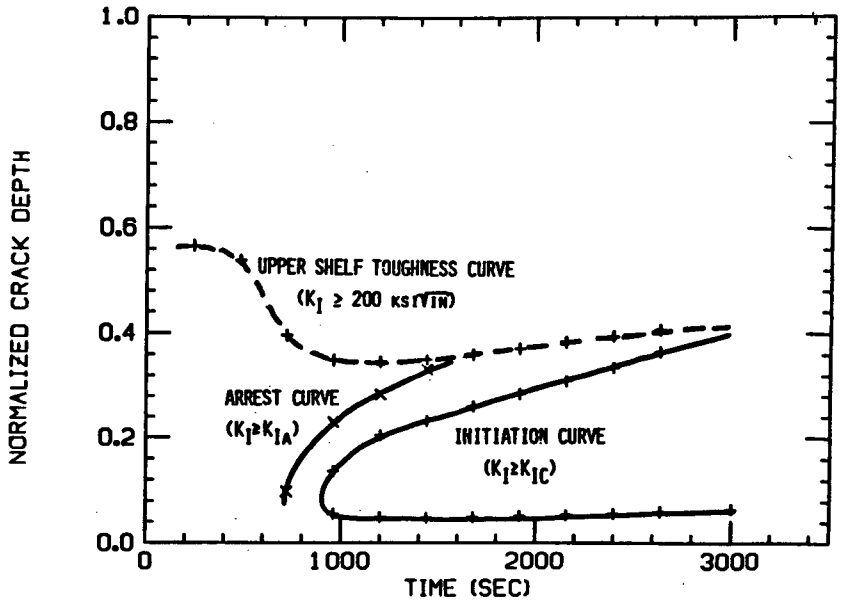


Fig. 13. Critical Crack Depth Diagram

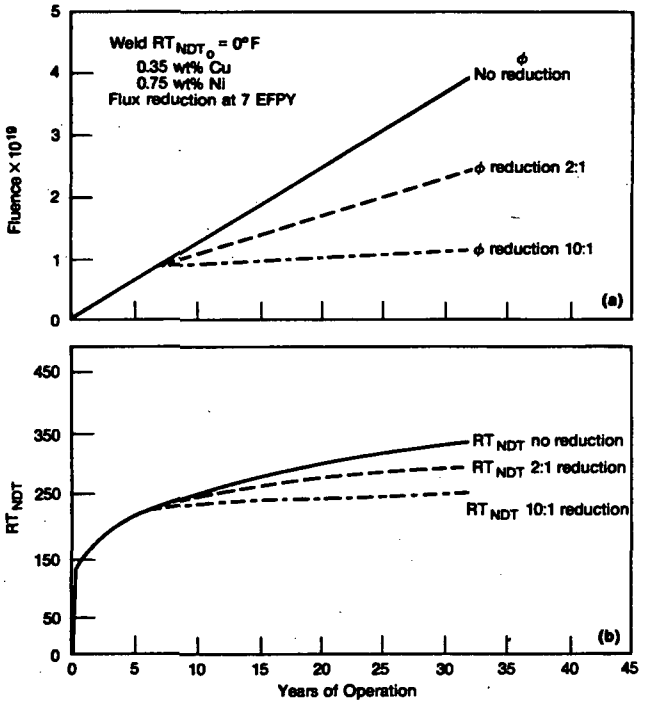


Fig. 14. (a) The Effect of Two Flux Reduction Schemes on the Accumulation of Fluence as a Function of Years of Plant Operation. (b) The Resultant RT_{NDT}'s for the Two Flux Reduction Methods Compared with Those of No Flux Reduction

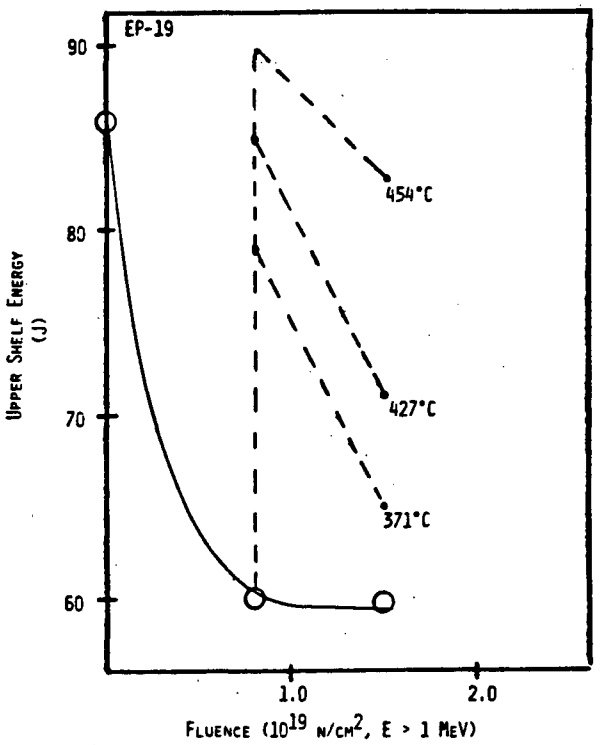


Fig. 15. Upper Shelf Behavior on Irradiation, Anneal, and Re-irradiation of a Low Shelf, High Copper Content Weld

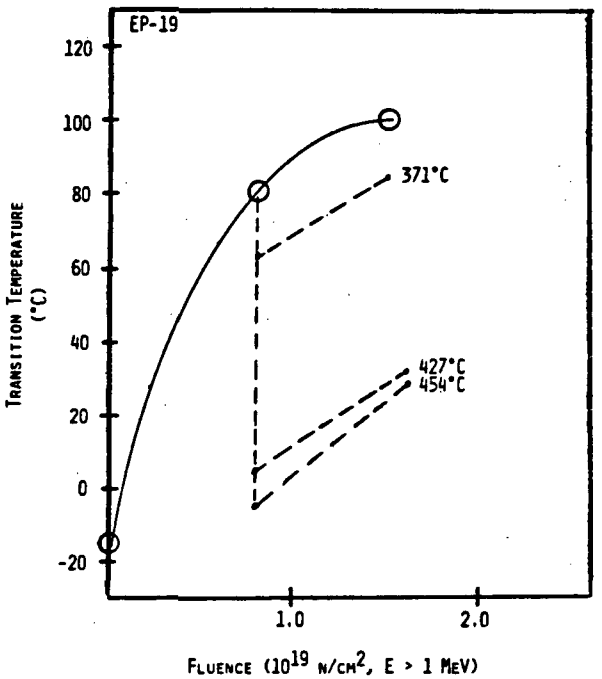


Fig. 16. Transition Temperature Behavior on Irradiation Anneal and Re-irradiation of a Low Shelf, High Copper Content Weld

SESSION 12

PRA-3: DATA BASES AND SPECIAL APPLICATIONS

Chair: G. Flanagan *(ORNL)*
M. Hayns *(UKAEA)*

SYNTHESIS OF THE DATA BASE FOR THE RINGHALS 2 PRA USING THE SWEDISH ATV DATA SYSTEM

Gunnar Johanson
Swedish State Power Board
Vallingby, Sweden

Joseph R. Fragola
Science Applications, Inc.
New York, New York

ABSTRACT

The Swedish State Power Board is undertaking a Probabilistic Risk Assessment (PRA) of the Ringhals 2 PWR. One of the unique features of this PRA is the availability of over four years of operating history for the unit contained in the ATV data system. This paper describes the cooperative process by which this operating data system information was converted into a data base for use in the risk assessment. The paper discusses the problems encountered, the methods of solution, and the unique features of the resulting data base including the scope and content of the ATV system, data validation, data translation, data structuring from a risk oriented perspective, extraction of population operating time and demand information, calculation of failure rates, and component unavailable times.

INTRODUCTION

The Swedish State Power Board is conducting a risk assessment program for the Ringhals plant. One step in that program is a PRA for the Ringhals Unit 2. A plant-specific data base has been developed in order to enhance the accuracy and reduce the uncertainty of the event sequence probability assessments in the PRA by incorporating actual Ringhals 2 operating experience.

PLANT SPECIFIC DATA BASE, SCOPE AND CONTENT

To develop this plant-specific data base, the Swedish Thermal Power Reliability Data System (ATV) has been used.[1] At present, information has been collected from Ringhals Unit 1, Barseback Units 1 and 2, Oskarshamn Units 1 and 2, Forsmark Unit 1, (all BWR-units), and from Ringhals Unit 2 and 3, (PWR-units).

In order to obtain the basic quantitative values needed (operating times to failure, repair times, successful and unsuccessful activations, etc.) to assess reliability characteristics, the failure reporting is complemented by operating data recording. This information is collected from the existing unit availability information system, which gives the operating history of the unit as well as its primary components, the reactor and the dual turbine systems. The history is transformed into points of time for transactions between defined operating states. The identified states are cold shutdown, hot standby, starting and power production.

In addition, turbine trips and reactor scrams are also noted. The ATV system also includes the informational base necessary to indicate which systems are required for each of the states. This indication allows the assignment of components to each operating state. Consequently, their operating history was deduced from the plant operating profile. As of summer 1981, about 60,000 components were contained in the ATV-system.

DATA BASE DEVELOPMENT

Data Transfer and Translation

Creating the Ringhals Unit 2 PRA data base required the transfer of data from the ATV system to the data structure developed for the ORNL in Plant Reliability Data program.[2] All failure reports for Ringhals 2, from October 1, 1976 until May 1, 1981 were sorted according to a system, component, date hierarchy and then printed out. The original reports are written in Swedish and code according to the Swedish system. Before conversion into the new "data base," the Ringhals 2 reports were translated into English.

The translation into English was inhibited by the nature of the failure reports. As in the U.S., each report is brief and to the point. To save space and time, the individuals documenting a maintenance action, use in-house technical shorthand and extensive technical abbreviations.

This problem was further exacerbated by truncations resulting from data encoding of each event. For this reason a straight Swedish to English translation was not acceptable even with the use of a technical dictionary. Thus, a "failure report dictionary"[3] was created by a joint Swedish-U.S. effort.

The first step to creating this dictionary was the review of U.S. plant failure reports and the extraction of technical terms and shorthand commonly used by U.S. maintenance technicians for the component types of interest in the Ringhals 2 study. The extracted terms were then systematically categorized by similar class distinctions.[4] The categorized list was reviewed and modified by a Swedish-U.S. technical team by matching it against the terminology utilized in the ATV system. As a result, corresponding Swedish terminology was developed for each technical term. The "dictionary" thus constructed was sent to Sweden for an additional review and approval by SSPB technical staff. Once the failure report dictionary was agreed upon by both parties, translation of the ATV records was begun.

Even with the dictionary, some of the records required discussion between technical staffs before an adequate translation could be agreed upon. However, the discussions were greatly simplified by the availability of the dictionary, and it therefore proved to be an invaluable tool throughout the data encoding process.

The next step was to transmit portions of the component data library to the data base. For this, no translation was required. The data were just prepared to fit into the corresponding positions in the data files.

Data Validation

Since the ATV system is encoded from the maintenance records by the utility (SSPB), and since experience with the IPRD system indicated that in some cases the

encoded data failed to faithfully represent the actual maintenance history, a data validation experiment was conducted.[5] The experiment indicated that 85% of all the identified maintenance records were recorded in the ATV system. As the accuracy of the system had significantly improved over the past few years, it was concluded that it would be conservative to say that over 90% of the relevant maintenance actions from Ringhals 2 are included in the ATV data system.

Plant-Specific Failure and Maintenance Data Development

Once the base of information was available from the ATV system, the failure rate and maintenance unavailability information was developed for the fault tree quantification. To ensure proper interface between the fault trees and the data, each fault tree analyst reviewed their initial trees with the data base task team. The review focused upon the basic events used by the analysts to verify that data would be available for quantification of each event. In cases where data was not available, the analysts agreed upon modification of the basic events (either decomposition or combination) which would allow the fundamental integrity of the tree to be maintained and yet be compatible with the data available. Component boundaries and interfaces, and the failure rate type (i.e., either time related or demand related), and the failure modes for which required quantification, were agreed to so that they were consistent from tree to tree, and data base compatible.

Consistency required that complete specification be provided for each component failure basic event utilized in the fault trees. This specification included the failure mode of interest in addition to the generic component type. In the fault trees this specification is accomplished by developing a coding system. In order to allow for the direct connection between the data base and the fault trees required to provide for adequate traceability, the coding scheme selected must be acceptable from the data base viewpoint as well. The coding scheme jointly agreed upon provided the additional feature of minimizing errors occurring in interface between the tasks.

The data coding used for components is given in Tables 1 and 2. A combination of these codes allowed for the component failure basic events to be specified in a complete, traceable fashion.

At this point, the ATV data was searched to extract failure records for the components identified within the systems modelled in the fault trees. All extracted failure records were then reviewed and categorized (catastrophic, degraded, incipient, non-failure) as to their failure severity and their impact on the component function, and by whether the failures were time or demand related.

Next the demand spectrum was calculated for each component as the sum of the test, auto initiated, failure related, and interfacing maintenance demands. The total exposure time was obtained from the combination of the plant operating time in mode data, and the system operating requirements per mode. In those cases where fractional equipment components were employed for a particular mode (e.g., 1 of 3 pumps), the exposure time was modified appropriately. From the above information, the demand related failure rate was calculated as the ratio of the number of catastrophic demand related failures (n_D) to the appropriate demand spectrum (D), and the time related failure rate as the ratio of the equivalent n_t to the total exposure time (T).

The maintenance rate (or maintenance frequency), which was required as an input to the human error and common cause quantification was calculated as the number of total maintenance actions which required the disabling of the component of interest.

This total was estimated by the sum of the catastrophic and degraded failures with the portion of the incipients which required the disabling of the component also included.

Traceability and review procedures required that the input data and the calculations made to generate the individual rates of failure be systematically organized. In order to satisfy these requirements, a form was constructed by the data analysts. The form allowed for calculations of both the time related and demand related estimates of the failure rate mean value for the identified components.

An example of the form used for the demand related failure rate calculation for valves is given in Figure 1.

Maintenance Unavailability Data

The ATV system is unique in that it gives four time points (t_1 to t_4) associated with each maintenance action:

t_1 = Time of failure discovery
t_2 = Time the component was unavailable
t_3 = Time the repair was initiated
t_4 = Time at which the component was again available

In addition to these time points being very useful in aiding in the failure severity classification, they also allowed for individual unavailable times per repair to be calculated. In particular, the difference between t_4 and t_2 provided the unavailable time. When these were categorized by component type, they provided a basis for estimating the average unavailable time which could be expected to occur given a failure.

ALTERNATIVE DATA SOURCE DEVELOPMENT

Even though the plant specific information available on Ringhals 2 from the ATV system was excellent in form, quality, and quantity, it was necessary to supplement this with alternative information. This use of alternative sources was required both to provide information on components which were unavailable in the ATV system, and to reduce the uncertainty bounds around the failure rate values for components which were available. The ATV system allowed calculation of rates for pumps, valves, batteries, diesels, and inverters. These were supplemented by U.S. LER data for pumps, valves and diesels. For other electrical components, data was available from the Ringhals 1 risk assessment data base, and from an SSPB system-wide data base on electrical components. Data on heat exchangers was provided from U.S. plant information and French operational data on PWR, RHR systems.[6] The data on the remaining components (such as sensors, fuses, and switches) were obtained from U.S. published sources (such as IEEE-500[7] and the RAC[8] notebooks).

DATA BASE SYNTHESIS

The data base obtained from the Ringhals 2 ATV records was incorporated and conditional information (likelihood distribution) with prior information to produce

a posterior mean estimate for eacn component failure basic event for which there existed ATV data. The approach utilized involved two steps:

1. For pumps, valves, and diesel generators by the LER Data Summaries[9],[10],[11] produced by EG&G for the USNRC were utilized for mean values of the prior distribution of the failure rate for each component failure mode of interest. The means were expressed as failures per hour for time related modes and demand probabilities for demand related modes. The error range due to uncertainty in the estimates was developed by EG&G considering the population of plants to have produced a homogeneous data set. For this reason the range calculated was oftentimes rather narrow and not thought to be truly representative of the ranges which should be applied to allow for plant to plant variations. Thus the error range applied to the mean point values was that defined by WASH 1400 for the component and failure mode of interest. The range estimate allowed the 5 and 95 percentile ranks to be roughly established for the corresponding WASH 1400 lognormal. These percentile values were utilized to characterize the appropriate prior distribution (gamma for failure rate, and beta for demand probabilities).

2. The Ringhals 2 ATV data parameters developed as part of the data analysis task were then utilized as likelihood information to update the parameters of the prior distributions developed in Step 1 using Bayes' Theorem. This second step allowed the posterior mean values and error bounds to be defined.

These posterior values developed as a result of this process were then utilized to quantify the fault tree component failure basic events for those events which had relevant ATV data available.

For those components for which no Ringhals 2 data was available the data and the asociated error bounds contained in the primary sources were used directly. In many cases the WASH 1400 point values and error bounds were used when no other data was available.

INTERFACES WITH OTHER PRA TASKS

The existence of plant data allowed for a unique interface to be developed between the fault tree analysts and the data analysts. The data analysts were guided in their thrust by the fault tree emphasis, and the fault tree analysts could make decisions as to whether to include events and at what level to include events, based upon their actual historical occurrence. In several ihstances, data questions elicited a comprehensive system review from an operational viewpoint which gave greater insight into actual system operation to all participants. In the case of the human error task, the ATV data provided an estimate of the number of opportunities for events such as "failure to restore." In the case of common cause, the existence of the multiple time points allowed times when safety components were simultaneously unavailable to be identified, and in concert with the maintenance interaction matrix and actual estimates of maintenance frequency allowed indirect simultaneous tech spec violations to be uncovered (e.g., disabling of two trains by the "tag out" of interfacing components required by two different components).

During the course of the development of the data base, an interesting and important interface between the fault tree analysts and the data analysts was

discovered. This interface occurs due to the two different perspectives involved in the specification of a component failure event.

The fault tree analyst attempts to understand the plant system he has been assigned in terms of both its normal operating behavior, and its behavior under abnormal operating conditions. The analyst then attempts to characterize the behavior of his assigned system in response to a spectrum of initiating events. From the fault tree standpoint, this is accomplished by decomposing the undesirable events applicable to the combination of initiating event and systems response (i.e., a particular accident sequence). This decomposition is then a "top down" process in which the analyst continues the decomposition until each of the branches of his binary logic tree ends in a basic or elemental event. The point at which this termination occurs is determined, in part, by the availability of and form of the data to be utilized to quantify the event. The availability of significant amounts of operational data can significantly reduce the amount of fault tree detail required.[12]

The data analyst, on the other hand, is concerned with establishing the population, failure, and repair history of the relevant components, and their associated demand and time exposure in a manner which allows the history to be utilized to project forward in time the behavior of these components in response to future initiating events. The data analyst performs this task by reviewing individual plant records. Since the task of the data analyst is to synthesize an undesirable event from lower level events (i.e., individual records), his approach is essentially "bottom-up" in nature.

Due to these different viewpoints there must be agreement between the two analysts on which failures should be assigned to which basic event, and whether data is available to support all the elemental events indicated in the fault tree. During the courses of the Ringhals 2 PRA, the agreement was achieved via individual conversation and meetings between the two groups. However, in order to allow for traceability, the decisions reached were required to be documented. This documentation was rather simple for most components, because clear distinctions could be made between the component and the rest of the system (e.g., for switches, batteries, inverters, battery chargers, manual valves, tanks, transformers). However, in the case of some components, the distinctions were not so clear cut. These components required somewhat detailed specification of the interface boundaries so that the reviewers would understand which failures were considered within the boundary of a particular, basic event and which were not. In particular the following component boundaries required specification:

1. Diesel Generators
2. Pumps
3. Operated Valves

The specifications included:

1. Functional Interface
2. Energy or Driver Interface
3. Command Interface
4. Lubrication and Cooling Interface
5. Control Interface
6. Monitoring Interface

A summary of the interface boundaries established for the Ringhals 2 data base is given in Figure 2. These boundaries were applied both to the elemental event termination point on the part of the systems analysts, and to the ATV data categorization on the part of the data analysts. This agreed to application

minimized the possibility of the miscommunication between the two groups of analysts, and the PRA reviewers.

CONCLUSIONS AND RECOMMENDATIONS

As a result of the performance of the effort reported upon in this paper the following conclusions and recommendations are proposed:

1. The Swedish ATV system is a significant source of data for use in a risk assessment. It compares very favorably with the data systems available in U.S. utilities in both breadth of coverage, quantity of data and data quality.

2. Since the ATV system identifies a failure event with the component which has been maintained it should not be used as a source of data without some correlation being made between fault tree basic events and the maintenance events.

3. The ATV system of including the 4 times associated with each event is extremely valuable and often adds great insight into the severity of individual failures and the coincidence of multiple failures. It is recommended that this feature be incorporated into other data bases which are intended to be used as sources of risk and reliability data.

4. The ATV system does not at present include information identifying components by their functional name (e.g., main steam shut off valve) but only by their number and generic types. This ommission presents no problem within the Swedish utility system. However, it makes comparisons between ATV data and data from other nations more difficult. Therefore it was recommended that consideration be given to adding the functional name to the component population record at least for pumps and major valves.

5. In general the availability of well structured in-plant maintenance records contributed a great deal to the overall risk assessment not only in quantifiable terms such as allowing for in-plant failure rate calculations, but in qualitative terms such as allowing both the data analysts and the systems analysts to gain a great deal of insight into the actual plant operating and maintenance history. This insight was reflected in the fault tree construction task as well. For this reason it is recommended that any in-plant maintenance records available be used whenever a PRA is attempted even when sufficient operating history is not available to allow for reasonable failure rate calculations to be made.

ACKNOWLEDGEMENTS

The work reported on in this paper was supported under a contract between the Swedish State Power Board and NUS Corp. The authors wish to thank both the Power Board and NUS for their assistance in the preparation of this paper. In particular, Mr. T. Lilja of SSPB and Mr. M. Evans and G. Parry of NUS have been helpful. Finally, the authors wish to thank Ms. M. Fienemann, Mr. A. McBride, and Ms. C.

Mason of SAI for their assistance in the performance of the work upon which this paper has been based.

REFERENCES

1. EKBERG, K. The Swedish Thermal Power Reliability Data System; 9-25-80, SSPB Ref. VET-KE-ON, Swedish State Power Board, Vallingby, Sweden.

2. DRAGO, J. P. and FRAGOLA, J. R. "The In-Plant Reliability Data System - History, Status, and Future Effort." ANS International Meeting on Thermal Reactor Safety, Chicago, IL, August 1982.

3. JOHANSSON, G. SSPE Ref. KSP-GUJ/EK-3483.

4. FIENEMANN, M. and MASON, C. Nuclear Plant Component Nomenclature Hierarchy for Failure and Repair Reporting, June 12, 1981, SAI/NY-R-81-4.

5. GYLLENBAGA, H. SSPB Ref. VTH-EG/MAI.

6. GROS, G. and LAMORA, L. M. "Comparison of the Calculated Availability of Safety Functions with Operational Data," C.E.A.-I.P.S.N., C.B.N. FAR B.F.6 92260 Fontenay-Aux-Roses, France, in the Proceedings of the International ANS/EMS Topical Meeting on Probabilistic Risk Assessment, September 20-24, 1981.

7. ANSI/IEEE Std. 500-1977, IEEE Guide to the Collection and Presentation of Electrical, Electronic, and Sensing Component Reliability Data for Nuclear Power Generating Stations, IEEE, New York, 1977.

8. FULTON, D. W. Nonelectronic Parts Reliability Data. IIT Research Institute, Summer 1978.

9. Data Summaries of Licensee Event Reports of Pumps at U.S. Commercial Nuclear Power Plants, EG&G, Idaho, Inc., January 1, 1972 to April 30, 1978.

10. Data Summaries of Licensee Event Reports of Valves at U.S. Commercial Nuclear Power Plants, EG&G, Idaho, Inc., January 1, 1976 to December 31, 1978.

11. Data Summaries of Licensee Event Reports of Diesel Generators at U.S. Commercial Nuclear Power Plants, EG&G, Idaho, Inc., January 1, 1978 to December 31, 1978.

12. MINARICK, J. W. and KUKIELKA, C. A. "Precursors to Potential Severe Core Damage: 1969-1979, A Status Report," NUREG/CR-2497, ORNL/NSIC-182, June 1982.

Table 1

COMPONENT CODE

Components:	Code
Pumps	
Motordriven	PM
Turbine driven	PT
Valves	
Motor operated valve	MV
Air operated valve	AV
Check valve	CV
Relief valve	RV
Manual valve	XV
Tank	TK
Strainer or Filter	FL
Heat Exchanger	HE
Busbar	BS
Rectifier or Diode	DE
Battery	BY
Cable	CA
Diesel Generator	DG
Inverter	IV
Switch	SW
Relay	RE
Sensor Pressure, Level	PR, LE
Transformer	TR
Circuit breaker	CB

Table 2

FAILURE MODE CODE

Code	Failure mode	
A	Normally closed fails closed	(NCFC)
	ex. Does not operate	(general)
	Fails to start	(pump)
	Fails to open	(valve, relay)
	Fails to lift	(checkvalve)
B	Normally open fails open	(NOFO)
	ex. Does not operate	(general)
	Fails to close	(valve, relay)
C	Normally closed fails open	(NCFO)
	ex. Wrong configuration	(valve)
D	Normally open fails closed	(NOFC)
	ex. Wrong configuration	(valve)
	Fails to run	(pump)
M	Test/Maintenance	
S	Short circuit	
O	Open circuit	
W	Loss of function	
P	Plugged	
L	Leakage/Rupture	
X	Operational error	

IN PLANT DATA ANALYSIS FORM

PLANT _____ PRA DEMAND DATA ANALYSIS

I. Identification Information

Component Type: Valve Date: 10-6-81

System No./Name: Safety Injection System #323 Analyst: McF

II. Input Information

	Population: N	Component Sub Type: Check	Motor	Sol.	Air	Man.
Demand Spectrum Analysis:						
1. Test Demands:						
2. Auto Initiates:						
3. Corrective Maintenance: (for each type of component)						
4. Interfacing						
(1,2,3) X # of Components of Type: D =						

III. Calculations

	Check	Motor	Sol.	Air	Man.
$q_d = n_d \quad D = {}^{n_d}$					

IV. Output Data

	q_d (per demand)	N	D	n_d
Check				
Motor				
Solenoid				
Air				
Manual				

Figure 1 In Plant Data Analysis Form

Boundary Specified	Interface Areas					
Component Type	1. Functional	2. Energy or Driver	3. Command	4. Lubrication and Cooling	5. Control	6. Monitoring
1. Diesels	From air intake, and outlet of fuel inlet valve to the output busbar interface excluding the first transformer	Same as Functional	Input contacts to starting air system. Entire system including accumulation and compressor, but not command signal to input contacts	Entire lubrication and cooling system with the exception of the inlet cooling water	Include all local control. Control and command circuits to starting air compressor included	All monitoring instrumentation excluded
2. Pumps	From outlet of inlet isolation valve to inlet of output isolation valve	a. Motor Driven: Input connect to motor control center including MCC switch gear and relays b. Steam Turbine: Outlet of steam inlet control valve	Same as Energy	a. Small and Medium Pumps: Entire lubrication and cooling interface b. Large Pumps: Local portions only. Heat sink and lubrication supply excluded	a. Motor Driven: Same as Energy b. Steam Turbine: Governor circuits and interface with steam inlet and throttle valves included	
3. Operated Valves	From outlet of inlet piping to inlet of outlet piping including all fittings, flanges, seals, bolts, and other devices necessary for piping connection	a. Air Operated: Inlet air to operator b. Motor Operated: Input connect to motor control center including MCC switch gear and relays	Input signal to MCC. Input signal to solenoid valves, but not command signal	Not applicable	Local limit switches included	

Figure 2 Component Boundary Specification Matrix for Ringhals 2 PRA Data Base

THE IN-PLANT RELIABILITY DATA SYSTEM (IPRDS) HISTORY, STATUS, AND FUTURE EFFORT*

Joseph P. Drago
Oak Ridge National Laboratory
Oak Ridge, Tennessee

Joseph R. Fragola
Science Applications Inc.
New York, New York

ABSTRACT

Since 1977 the American Nuclear Standards Institute/Failure and Incidents Reports Review (ANSI/FIRR) committee has sponsored a voluntary program of visits to nuclear power stations for maintenance record collection at the plant site, and the conversion of these records into a comprehensive data base to be applied to risk and reliability analyses. At present, ten plants have been visited and data have been collected on 16 units. These data have been reviewed and the information from four plants (six units) has been encoded for two plant components (pumps and valves). This paper reviews the history of the program, the lessons learned, and the insights gained. The present status of the information in the data base is discussed and initial observations are documented. A comparison with other systems is included as well as future developments and cooperative efforts.

1. INTRODUCTION

In performing a Probabilistic Risk Assessment, an adequate base of reliability information is required. The Nuclear Regulatory Commission (NRC) has attempted to respond to this requirement by constructing a component informational base from the Licensee Event Reporting System (LERS). But the representativeness of this data is dependent on how faithfully the LERS represents actual operational experience. In addition, the creation of a component failure rate base from the failure frequency information contained in the LERS requires assumptions which bring into question the credibility of the results. Further, the unavailability calculations common to the risk assessment models require estimates of component down time including an estimate of the frequency of component unavailability. Some analysts have voiced a concern whether these estimates obtained from LER data are reasonable.

A feasibility study utilizing the maintenance work request records was initiated in 1977 by the Reliability Data Working Group Subcommittee (SC5.3) of the Institute of Electrical and Electronics Engineers (IEEE). This effort was directed at the collection of in-plant records by visits of volunteer teams under the auspices of the ANSI/FIRR Committee, and the conversion of these collected records into an In-Plant Reliability Data System (IPRDS).[1,2]

---

*Research sponsored by U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Division of Risk Analysis, under Interagency Agreement 40-550-75 with the U.S. Department of Energy under contract W-7405-eng-26 with the Union Carbide Corporation.

2. SCOPE OF THE IN-PLANT DATA EFFORT

The IPRDS was intended as a test system which would use data on selected components from selected plants to test the validity of other data systems and to provide data which was representative of U.S. plant experience. Plants considered representative of the U.S. nuclear plant population were selected for team visits. There was never any intention that this data should be used on a plant-specific basis, nor on a manufacturer specific basis. The teams emphasized depth and breadth of collection at each plant visited. The intention was to review every maintenance record at each plant visited and record all documents that could be considered relevant to the final data base. The relevant records were categorized according to failure severity, and then encoded into the data system. The team members attempted to collect population information, exposure time, number of demands, and component identification information during the visits.

The tasks required for data collection and analysis have evolved over time and now include:

1. Data Base Structure
   - Definition of Standard Data Base Subsystems
   - Definition of Population, Failure, and Repair Records Encoding Format
   - Development of Data Entry Software
   - Development of Component Identification Hierarchy
   - Development of Component Boundaries Definition
   - Development of Component Failure Modes and Failure Cause Codes

2. Data Team Visits
   - Contact of Utility Personnel
   - Selection of Team and Team Leader
   - Visit to Plant for Data Collection

3. Data Encoding and Entry
   - Collected Data Records - Review and Selection
   - Encoding Population and Failure/Repair Records
   - Entering Duty Cycle and Demand Spectrum
   - Data - Validation and Verification

4. Data Output Structure
   - Presentation of Information
   - Selection of Primary and Secondary Sorts
   - Interface with PRA Fault Trees

5. Data Handbook Development
   - Determination of Component Definition
   - Determination of Component Functional Characteristics
   - Determination of Frequent Component Failure Mechanisms
   - Determination of Frequent Component Failure Modes
   - Determination of Component Failure Rates and Maintenance Rates

3. PRESENT STATUS AND INITIAL OBSERVATIONS

The present status of the IPRD program is summarized in Table I. The data collected and entered is summarized in the Table II.

From a preliminary review of the data, it is apparent that the data base will provide a significantly greater amount of information per plant than other data systems. The information on the safety and non-safety system components provides for a comparison of the operational performance of components of equivalent design and operating environment. Also the inclusion of degraded and incipient failures in this data base allows for a comparison of maintenance philosophies. Already, it can be seen that some units have a greater number of incipient failures than others and

TABLE I

Present Status of IPRD

Plants visited	10
Plant visits	12
Units visited	16
Plants ready for entry	4
Units ready for entry	6
Plants near ready	3
Units near ready	5
Maintenance records reviewed	120,000
Corrective maintenance records extracted	24,000
Components for which entry has been initiated	6 units-pumps and valves
Component failure and repair entry	6 units-pumps and valves
Component population entry	6 units-pumps and valves
Verification and validation completed	Pumps (total) Valves (partial)
Data handbooks to be published	Pump handbook FY82 Valve handbook FY83

TABLE II

Data Entered in IPRD

Data entered	Pump totals	Valve totals
Population	1428	8000
Catastrophic failures	700	800
Degraded failures	1300	1500
Incipient failures	2000	3000
Total failures	4000	5300
Period of observation (reactor years)	20	20

fewer degraded failures. This correlates well with some plants emphasizing preventive maintenance while others choosing to wait until the failure is more significant before repair. The data could also allow for the determination of the safety significance of the differing philosophies (i.e. does a significant preventative maintenance program actually reduce the number of catastrophic failures observed for safety related components). The data also indicate that less than one out of four pump failures is catastrophic, and therefore to use the catastrophic failure rate as the only basis of a maintenance unavailability estimate may be significantly in error. Another interesting observation is that a review of the total time-oriented failure history of a component gives a much clearer picture of what is transpiring than looking at only the catastrophic failures, and a comparison of these histories from unit to unit for the same component is more meaningful when all failures are included.

4. LESSONS LEARNED

Lessons have been learned in this project in all the task areas listed in Sect. 2. Some of the important lessons were:

- The need to create more systematic cause codes based upon nouns and modifiers (adjectives, adverbs);
- The need for and the structure of the comprehensive interviews which must be conducted with each supervisor (Electrical, Mechanical, and Instrumentation) to determine the actual maintenance policy at the unit;
- The need to maintain data traceability from the collection through the encoding stage;
- The requirement for validation and verification of the entered information;
- The importance of developing a consensus on the data output structure between engineers involved in risk and reliability analyses;
- The critical need to supplement the statistical information with engineering information to supply the most useful data output.

5. COMPARISON WITH OTHER SYSTEMS

At present, there exist several data systems from which reliability data can be obtained on nuclear plant components. Some of these sources are not comparable with IPRD system because of their current scopes [such as the Edison Electric Institute (EEI) data system or the current North American Electric Reliability Council/Generating Availability Data System (NERC/GADS)]. Others are comparable for only certain portions of the data. Each data base has individual features which are valuable for purposes other than providing a base of information for the performance of a risk assessment. However, since the IPRD system has been designed specifically for use in reliability and risk analyses, it is compared to several of the other major systems on that basis. The systems chosen for comparison are:

1. The Nuclear Plant Reliability Data System (NPRDS)-Institute of Nuclear Power Operations (INPO).

2. The Licensee Event Reporting System (LERS) - USNRC Office of Analysis and Evaluation of Operational Data (AEOD).

3. EG&G Failure Rate Data from LERs - EG&G Idaho for USNRC.

4. European Reliability Data System (ERDS) - Ispra Joint Research Centre Varese, Italy for the Commission of the European Communities (OECD).

5. The Swedish Thermal Power Reliability Data System (ATV) - Consortium of Swedish Utilities for internal use.

A comparison matrix is provided in Table III.

6. FUTURE EFFORT

The IPRD program is an ongoing program. Further work is planned to increase the breadth of the program in FY83. The proposed valve data from two additional plants are intended to be entered into the data base, as well as data on additional components. At present, it is intended that information on diesels, batteries, battery charges, and inverters will be included. In addition at least one additional revisit is scheduled to bring up to date the data records on one plant currently in the data base.

TABLE III

Comparison of IPRDS With Other Systems

	IPRD	NPRD	LERS	EG&G LER	ERDS	ATV
Standard boundary definition						
System	Yes	Planned	No	No	Yes	Yes
Component	Planned	Future	No	Yes	Planned	No
Components covered						
Safety	Yes	Yes	Yes	Yes	Yes	Yes
Non-safety	Yes	Planned	No	No	Yes	Yes
Information addressed						
Failures	Yes[a]	Yes	Yes	Yes[b]	Pilot data only	Yes
Population	Yes[a]	Yes	No	Yes[b]	Pilot data only	Yes[c]
Plants covered	4	All United States	All United States	All United States	Pilot data only	4
Units covered	6	All United States	All United States	All United States	Pilot data only	8
Failure records	Directly from plant records	Generated from records by plant personnel	Generated from records by plant personnel	From LERS	Pilot data only	All from plant records
Population records	3 plant records 1 drawing review	Supplied by plant with pedigree	None	From FSAR	Pilot data only	All from plant records
Demand spectrum	Plant spectrum estimated	Plant spectrum estimated	No	Estimated generic	Unknown	Estimated from maintenance surveillance schedule
Exposure time	Plant spectrum estimated	Plant spectrum estimated	No	Estimated generic	Unknown	Estimated - some components have clocks
Failure categories included						
Catastrophic	Yes	Yes	Yes	Yes	Unknown	Yes
Degraded	Yes	No	No	No	Unknown	Yes
Incipient	Yes	No	No	No	Unknown	Yes
Unavailable time	No	No	No	No	Unknown	Yes
Corrective maintenance repair time	Some plants	No	No	No	Unknown	Yes
Failure rate	Yes	Yes	No	Yes	Unknown	Yes
Maintenance rate	Yes	No	No	No	Unknown	Yes
UNID[d] compatibility	Yes	No	No	No	Yes	No
Plant visits for verification	Yes	No	No	No	No	Yes
Comments	Covers only selected plants Covers both safety and non-safety components Presently, only pumps and valves encoded	Covers all plants Covers all safety components	Covers all plants Covers all safety components Reporting inconsistent both on number of components covered and types of failures reported	Covers all plants Failures based on LERS criteria Exposure time and demands estimated Covers important components Provides failure rates No repair time	Still in research stage Design cooperation with IPRDS	Some electrical components missing Introduction of time clocks on components will improve exposure time documentation Failure records in Swedish Cause coding not adequate to describe failure/repair text

[a] Presently only for pumps and valves; more planned.

[b] Includes pumps, valves, diesels, control rod drive and penetrations.

[c] Includes pumps, valves, instruments, transformers, filters, diesels, tanks, and heat exchangers.

[d] The Tennessee Valley Authority's Unique Identification of Structure, System, and Component Descriptions.

Work is also ongoing to expand the approach taken to develop the data to include more comprehensive information such as:

a. Component Definition
   - Identification - type definitions
   - Description - parts breakdown
   - Potential boundaries
   - Boundaries used in analysis

b. Component Functional Characteristics

c. Component Frequent Failure Mechanisms
   - General environmental mechanisms and parts affected
   - General operational mechanisms and parts affected
   - Frequent mechanisms in nuclear plant applications

d. Component Frequent Failure Modes
   - Failure observation from a functional view
   - Frequent failure effects in nuclear plant applications

It is expected that the effort in FY83 will include analysis of the collected data. Studies will be undertaken to investigate the human error contribution to corrective maintenance, to investigate the time dependency of the rate of failure occurrence, and to obtain insights into the effects of the actual plant operational environment which might be of significance in the preconditioning of components prior to qualification testing.

7. PROBLEM AREAS AND LIMITATIONS

Although it is believed that the IPRD system will provide a valuable new source of information, the user should be aware of the following problem areas and the limitations.

7.1 Limited Failure and Repair Description

The records used as the source for the encoded data were actual inplant maintenance forms as filled out by the maintenance personnel and their supervisors. As such, the records were not specifically intended to support a reliability and risk assessment data base but to document the maintenance action. For this reason the failure and repair descriptions were sometimes insufficient to indicate exactly the nature of the problem. In order to discern the severity and the cause of the failure, an understanding of the following was necessary (1) the maintenance process involved in the plant, (2) the nature and sequence of other maintenance actions on a particular component, and (3) the history of other maintenance actions occurring in the unit during the time period of interest.

7.2 Failure Cause Codes Applicability

Failure cause codes originally defined in the LER based data were utilized for the encoding of the pump records. During the course of the encoding effort it became evident that a more effective set of cause codes could be derived from the records using an approach which took into account the frequency of occurrence of certain key related words in the text. The cause codes utilized for valves were generated in this manner, and the pump codes were slightly modified to take this into account. However, the pump codes are still, at present, substantially the same as the original LER codes and therefore are, to some degree, not representative of the maintenance record text.

7.3 Limited Sample Size

Currently, the IPRDS includes data from only four nuclear plants (six units) for pumps and valves. Although this sample includes over 20 reactor years of experience, the inherent reliability of most the plant components precludes the occurrence of a statistically significant number of failure events on individual components. Therefore, without aggregation of components across the plants the failure statistics calculated often include wide uncertainty bounds. Since aggregation presumes homogeneity of the subpopulations, and since the subpopulations may not be homogeneous, care must be taken when using the calculated values.

7.4 Estimation of Annual Demands

For many pumps operated in either the alternating or standby mode, the number of annual demands was estimated to be 12; one demand per month. This estimate is the assumed minimum number of demands placed on these components and is probably lower than the actual number by a factor of 2 to 3. This difference arises from both system interfacing demands and transient demands. Interfacing demands are those demands which require the pump to be tested following certain maintenance actions such as replacing a valve in the process piping. Transient demands arise from such actions as a reactor scram or an engineered safety feature actuation signal. The effect of the lower estimate of annual demands is that the calculated failure rates are conservative; that is larger than the true value by a factor of 2 to 3.

7.5 Estimates of Duty Cycle

Engineering judgment was used to estimate the duty cycle of each pump. It is planned to review the operator logs to obtain the number of hours each pump was operated.

8. ACKNOWLEDGEMENT

The effort reported on in this paper was performed under the sponsorship of the USNRC Office of Nuclear Regulatory Research, under Dr. James W. Johnson, Project Manager. The work is being performed under an interagency agreement with Oak Ridge National Laboratory. Science Applications, Inc. is under contract with ORNL. The authors wish to thank Ms. B. Horwedel of ORNL, and Ms. M. Fienemann and Ms. C. Mason of SAI for their support in this effort.

9. REFERENCES

1. J. P. DRAGO, R. J. BORKOWSKI, D. H. PIKE, F. F. GOLDBERG, *The In-Plant Reliability Data Base for Nuclear Power Plant Components: Data Collection and Methodology Report*, NUREG/CR-2641 (ORNL/TM-8271), July 1982.

2. J. P. DRAGO, R. J. BORKOWSKI, J. R. FRAGOLA, J. W. JOHNSON, *The In-Plant Reliability Data Base for Nuclear Plant Components: Data Report - The Pump Component*, NUREG/CR-2886 (ORNL/TM-8465) (to be published).

LIMITED SCOPE PROBABILISTIC RISK ASSESSMENTS (MINI-PRAs) FOR ENVIRONMENTAL REPORTS

R. L. O'Mara and W. T. Hotchkiss

Stone & Webster Engineering Corporation
Boston, Massachusetts 02107, U.S.A

ABSTRACT

The Nuclear Regulatory Commission (NRC) specifies that Environmental Reports (ERs) include a discussion of the risks associated with accidents. Probabilistic Risk Assessment (PRA) is one method of examining postulated accidents. One approach to PRA is the Mini-PRA, which uses the accident risks reported in a comprehensive PRA for one site and examines consequences specific to a different site. By concentrating on specific differences, some preliminary results can be obtained without reviewing all features of the design and site. There are usually many differences between the plant for which a comprehensive PRA has already been performed ("base" plant) and the plant for which an ER is being prepared ("study" plant), but only a few need to be considered because they dominate risks or dominate uncertainty. These factors will be discussed, as will the tasks necessary for preparing a Mini-PRA.

DISCUSSION

Environmental Reports (ER) and Environmental Impact Statements (EIS) should include a discussion of effects of potential accidents. This should cover even highly improbable accidents. A Probabilistic Risk Assessment (PRA) is one possible basis for the discussion of improbable accidents. This paper discusses one approach to Probabilistic Risk Assessment for inclusion in Environmental Reports, the Mini-PRA.

The term "Mini-PRA" is used to distinguish an appropriate limited scope PRA from a comprehensive PRA such as WASH 1400. In its simplest form, a Mini-PRA starts with the radiation release reported in a particular comprehensive PRA from one site and modifies it based on the specific conditions of a different site. A Mini-PRA can thus provide information about accidents that is adequate for an ER or EIS but at a lower cost than a comprehensive PRA.

The following abbreviated version of an NRC Statement of Interim Policy that appeared in the Federal Register (45FR40101) addresses the requirement for risk assessment in Environmental Reports:

"Environmental Reports should include a discussion of the environmental risks associated with accidents ... In-plant accident sequences that can lead to a spectrum of releases shall be discussed and shall include sequences that can result in inadequate cooling ... and to melting of the reactor core ... causes external to the plant which are considered possible contributors ... shall also be discussed. Detailed quantitative considerations that form the basis of probabilistic estimates of releases need not be incorporated ... but shall be referenced."

"The environmental consequences . . . shall also be discussed

- in probabilistic terms . . .
- in a manner that fairly reflects the current state of knowledge."

"Releases refer to . . . exposure pathways including air, water, and groundwater."

A Mini-PRA that is responsive to the NRC notice is a comparison of a particular power plant to a similar one on which a comprehensive PRA has already been performed. By concentrating on specific differences, some preliminary results can be obtained without reviewing all features of the design and the site. These results provide an overview of the risk from a particular plant and show which of the particular plant's features contribute most to that risk.

There will be many differences between the study plant and the base plant. In addition to differences in plants and sites, there are differences in data and models. Differences in only a few vital areas need to be considered, however, because these areas dominate estimated risks or dominate uncertainty. These areas are described below:

- Site Population and Meteorology - This factor dominates the consequences portion of the calculations. Information must be comprehensive, particularly for the nearby population.
- Source Term - This factor dominates the uncertainty in the results from the consequences models. Recent work (see Nuclear Technology - May 1981) shows that source term estimates currently used in PRAs are unreasonably conservative.
- Major Design Features (for example, thermal power, containment, electrical grid reliability) - A base plant is chosen whose major design features are similar to those of the study plant.
- External Events (for example, an earthquake) - The response spectrum and equipment susceptibility may dominate failure likelihood for some systems at some plants.
- Liquid Pathways - Realistic estimates of effects of site geology on the natural processes that inhibit source migration must be made.

Site population density and distribution have the greatest impact on risk because the integrated probability of releasing radioactivity from all the release categories possible is fairly constant from one design of a given power level to another design of a similar power level. That is, any single component or system within the design is not likely to produce as much difference in health effects as a difference in population exposed. By the same token, because a range of meteorological conditions is probable, site meteorology is also not likely to produce a great difference in health effects integrated over a time period unless it is combined with some peculiarity in topography, such as a valley, an ocean, or a lake.

This has been borne out by Sandia research using the Computation of Reactor Accident Consequence (CRAC II) code.

The source term is highly sensitive to a catalog of assumptions regarding fission product aerosol generation and deposition. This has resulted in the selection of multiple factors of conservatism and gross overestimation of potential effects in most comprehensive PRAs. The "worst case" effects dominate the public perception of accident consequences. The NRC has recently institutionalized the worst case accident by an elaborate study of its economic consequences. (See NUREG CR/2591.) The NRC has specified, however, that for ERs the applicant and the staff should "...select those values which would be expected to yield estimates nearest the real case" (Regulatory Guide 4.2.). Therefore, the Mini-PRA should use a more realistic source term than the conservative value used in many comprehensive PRAs.

A Mini-PRA can discern the effects of significant design differences. For example, those postulated accident sequences that include excessive containment leakage rather than massive containment failure will have a much lower or more delayed release if the reinforced concrete primary containment is surrounded by a secondary containment structure. Such design differences as this must be considered in a Mini-PRA. Even more obvious design differences, such as the reactor's thermal power output, must also be included.

External events are significant because of their potential for compromising redundancy. They are "common causes" of failure. Seismic fragility is the most difficult event with which to deal. A severe earthquake, while rare, can be powerful and destructive. The Mini-PRA evaluation of external events consists of checking the design criteria of systems whose failure dominates accident consequences, for example, the auxiliary feedwater system. The system should be checked to determine what design criteria were used to enable the system to accommodate the external event. In particular, the system should be checked to determine if common cause failure is more probable in the study plant than in the base plant.

The model of the liquid pathway can also affect the release estimate. If dilution is the only site-specific factor in the model, the apparent release can be very large. Ion exchange and filtration in the soil should also be included in the model. This is especially important for an inland river site because the transport of radionuclides is chiefly inhibited by these mechanisms.

Figure 1 shows results of a few PRAs that have been published. These are typical of PRAs that could form the basis of a Mini-PRA. The range of serious accident frequency estimates is from 10^{-6} to 10^{-9} per year.

While most PRAs have estimated the results of serious accidents, PRAs can also be used to determine the results of less serious accidents. Figure 2 shows PRA results for events that have actually happened -- unit outages. This figure also shows an extrapolation of the trend: the WASH 1400 core melt frequency prediction and the frequency prediction of core damage accidents from the precursor study, NUREG CR2497. The range of outage frequencies is from 10 to 10^{-3} per year for outages that have occurred. The range has been extended to 10^{-6} per year to include the WASH 1400 core melt frequency estimate.

The tasks necessary to prepare a Mini-PRA are:

- Identification of the scope of the Mini-PRA.
- Identification of the comprehensive PRA on which the Mini-PRA is based.
- Identification of significant differences between the base plant and the study plant. Modify event trees and fault trees to reflect the differences.

- Identification of those events which could result in common cause failures, for example, environmental stresses, systems interactions.

- Determination of source terms from accident sequence for use in the Mini-PRA.

- Determination of site-specific features for use in the mini-PRA, for example, population, meteorology, land use.

- Compilation of accident consequence information with probability information from event and fault trees to produce complementary cumulative distribution functions (CCDF), using the CRAC II code. These CCDFs are in effect derived from the CCDFs in the comprehensive PRA but account for the differences between the base plant and the study plant.

- Preparation of report to describe results, methodology, and assumptions.

Other Benefits of a Mini-PRA

In addition to meeting content requirements of ERs, a Mini-PRA also:

- Provides a framework for subsequent full scope PRA.

- Shows where design improvements can reduce the likelihood or consequences of accidents. This not only enhances safety but reduces potential outage and cleanup costs.

- Quantifies safety of existing design as part of the technical basis for resisting design changes which do not appreciably improve safety.

Uncertainty is an inherent characteristic of, rather than a flaw in, a PRA. Indeed, one objective of a PRA is to deal with uncertainty in a rational way. These assessments are one facet of the general subject of decision making in the face of uncertainty. The alternative to a PRA is a guess -- educated perhaps, but rarely formal and coherent.

CONCLUSIONS

A Mini-PRA is an effective way of addressing the NRC requirements for risk assessment in ERs. By making use of an already-prepared comprehensive PRA and only considering several vital areas of difference between the base plant and the study plant, the Mini-PRA provides information about accidents for ERs at a much lower cost than a comprehensive PRA.

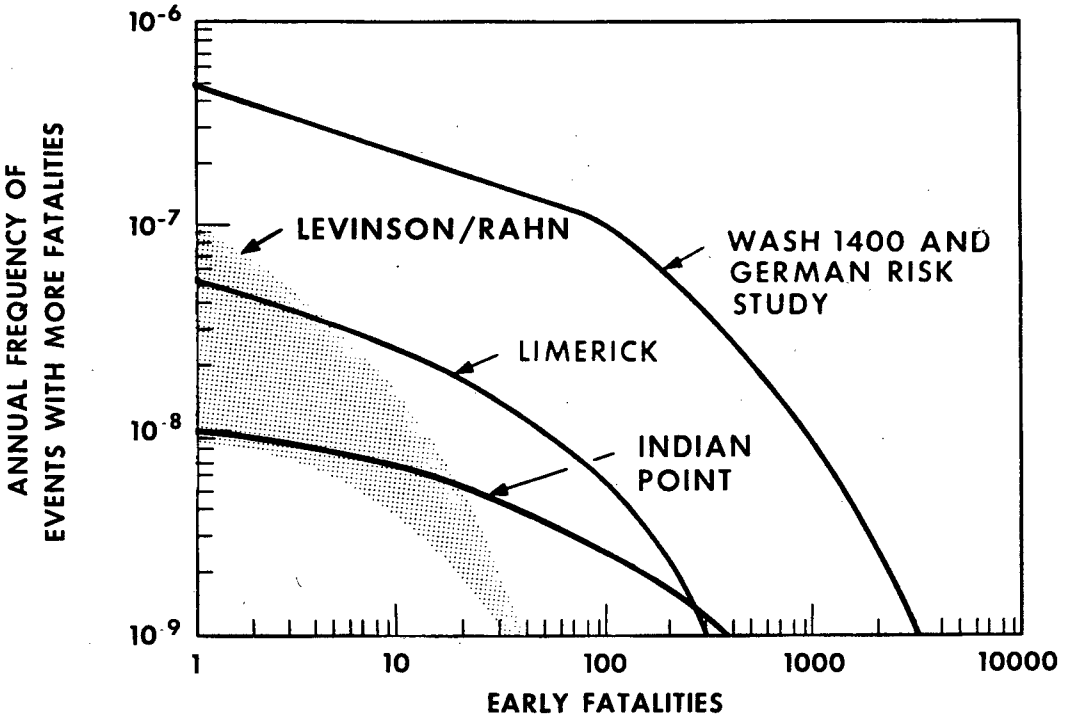


Fig. 1. PRA Results Showing Serious Accident Frequency.

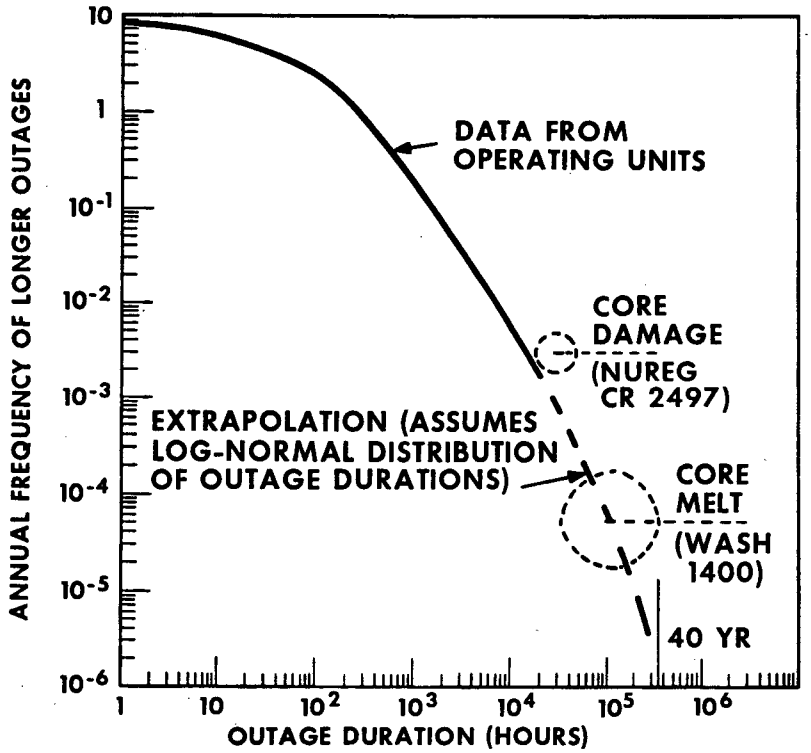


Fig. 2. PRA Results for Less Serious Events.

A PRA-BASED APPROACH TO ESTABLISHING PRIORITIES FOR EQUIPMENT QUALIFICATION NEEDS

D. E. Leaver, W. A. Brinsfield, and J. F. Quilliam

Wood-Leaver and Associates, Inc.
1340 Saratoga-Sunnyvale Road
Suite 206
San Jose, CA 95129 U.S.A.

R. N. Kubik

Nuclear Safety Analysis Center
Electric Power Research Institute
3412 Hillview Avenue
Palo Alto, CA 94303 U.S.A.

ABSTRACT

The evolving nature of environmental qualification requirements and the tight schedule imposed for equipment testing suggest the need for a methodology which can be used to establish priorities for qualification needs. An approach has been developed which utilizes probabilistic risk assessment (PRA) techniques to rank the importance of equipment and instruments in a plant. This ranking can then be used to establish priorities for qualification and to provide a basis for the elimination of unimportant equipment from additional consideration. A demonstration of this PRA-based approach has been completed for an operating plant.

INTRODUCTION

During the last several years the Nuclear Regulatory Commission (NRC) has expanded significantly its environmental qualification requirements for nuclear power plant equipment. The NRC now specifies more detail on methods to be used and on required documentation, specifies a wider range of equipment to be qualified, and specifies a wider range of conditions under which equipment must be qualified. Although the deadline for completion of environmental qualification of safety-related electrical equipment has recently been relaxed by the Commission, an extensive and expensive program in environmental qualification is still anticipated by the utilities. Further, the prospect of expanding requirements, particularly in the areas of seismic qualification, mild environment, mechanical equipment qualification, and equipment survivability in a hydrogen burn environment, creates uncertainty for the future.

Because of these uncertainties, and as a backup to the ongoing industry qualification effort, the Nuclear Safety Analysis Center proposed reviewing a plant's design to determine the importance of various equipment items. This relative ranking could then be used to establish priorities on equipment qualification needs. This would provide a basis for schedule relief or for reconsidering qualification requirements for low importance equipment. The general purpose of the work reported here is to develop and demonstrate a methodology for performing this relative importance ranking.

The methodology utilizes a probabilistic risk assessment (PRA) based approach to the importance calculation for equipment qualification.

The specific objectives of this work are the following: (1) develop and demonstrate a PRA-based methodology for performing a general, plant-wide relative importance ranking of equipment items which are explicitly included in the PRA logic models; (2) develop and demonstrate a methodology for performing a relative importance ranking of instruments which provide information to the operator but are not explicitly included in the PRA logic models; and (3) investigate the potential for use of plant modifications as a substitute for qualification or as a basis for reconsidering qualification requirements. The demonstration of these objectives is performed using the Consumers Power Company Big Rock Point plant as an example. The Big Rock Point plant was chosen for this application for two reasons. First, a complete PRA has been done by Consumers Power Company for Big Rock Point and has been submitted to the NRC as the basis for future licensing considerations. The NRC has reviewed the PRA and the informal response has been favorable. Thus some of the groundwork has been laid for using the PRA in dealing with regulatory issues. Second, Consumers Power Company is considering utilizing some of the concepts in the report in dealing with the environmental qualification issue for Big Rock Point. If carried out, this would provide a demonstration of the usefulness of these concepts to the industry. Although the Big Rock Point plant design is unique, this did not detract significantly from the example calculation since the qualification requirements and the equipment design from a qualification standpoint are similar to a number of operating plants.

BASIS FOR AND USES OF PRA-BASED APPROACH

As noted above, the general purpose of this work was to develop and demonstrate a methodology for calculating a relative importance ranking of equipment. PRA was selected as the basis for the methodology because of its ability to assemble all of the design and operational characteristics of a plant into a unified set of models from which a plant-wide ranking of equipment can be inferred.

The potential uses of a PRA-based approach to importance calculations for establishing priorities on equipment qualification needs are as follows:

- In cases where not all equipment can be tested at the same time, the priority list provides a basis for testing less important items at a later time.
- The priority list and PRA provide a possible basis for reconsidering the qualification requirements for low importance items.
- The PRA provides a basis for depicting the risk implications of continuing operation of a plant pending resolution of an environmental qualification issue.
- The priority list and the PRA facilitate definition of plant design and procedural changes which could significantly decrease the importance of qualification of an equipment item or a system. This suggests the possibility that such plant changes could be used as a substitute for qualification or as a basis for reconsidering qualification requirements.
- Finally, the importance calculation can be used as a basis for defining the specific environmental profile to which a particular equipment item or system should be qualified.

The above uses of a PRA-based approach to establishing priorities on equipment qualification will probably be best applied to older plants. The NRC staff has stated that for older plants a different interpretation of requirements from that in the DOR

Guidelines will be considered where justified. Most operating plants are not committed to comply with any particular industry standard for equipment qualification but rather must meet the General Design Criteria. Also, PRA-based arguments are best applied to older plants because of the better operating experience base and the fact that the unique plant designs provide an incentive to evaluate generic issues on a plant-specific basis.

Application of a PRA-based approach to equipment qualification (or any regulatory issue for that matter) must be done with care and preparation. Such an approach will probably have to be done on a plant-specific basis, particularly for the older plants as noted above. Individual licensees will have to lay the proper groundwork with the NRC staff in order to have assurance that the approach will receive due consideration. The quality of the PRA must be well established with the NRC prior to application of the approach.

RANKING OF ITEMS EXPLICITLY MODELED IN PRA

Several techniques for importance calculations were defined in this work to be used depending on the situation. For the general, plant-wide importance ranking of equipment items explicitly included in the PRA logic models, the Increased Failure Probability Method was used. In this approach the failure probability of the item under consideration is assumed to increase from b to b' and the corresponding increased core damage frequency is calculated (core damage frequency is used as the measure of risk). The importance is

$$I = \frac{cdf(b') - cdf_b}{cdf_b}$$

where cdf(b') is the core damage frequency for item failure probability b' and cdf_b is the baseline core damage frequency. The importance may be interpreted as the fractional increase in core damage frequency due to increased failure probability of the item. In applying this technique to equipment items which are explicitly modeled in the PRA, cdf(b') is calculated simply by exercising the logic models with b replaced by b'. Table I displays the resulting ranking for Big Rock Point with failure probabilities increased to unity. It is noteworthy that eight systems have an importance ranking of less than .1, i.e., complete failure of the system would increase total core damage frequency less than 10%.

RANKING OF INSTRUMENTS NOT EXPLICITLY MODELED IN PRA

For instruments which provide information to the operator but which were not explicitly included in the PRA logic models, a somewhat different technique was used for the importance calculation. The importance was based on an estimate of the core damage frequency decrease due to the operator actions which the information facilitates. For the Big Rock Point example Table II gives the ranking of the ten most important operator actions and the instrument sets associated with those actions. Generally, individual instruments have zero importance using this methodology since successful completion of most operator actions requires more than one instrument.

TABLE I

General Importance Ranking of Systems, Components, and Functions at the Big Rock Point Plant

System, Component, or Function	Importance Ranking
Reactor Protection System, Control Rod Drive System	1281.0
Post-Incident System	25.5
Reactor Depressurization System (RDS)	25.6
Core Spray System	25.6
Emergency Condenser (Valves)	11.8
Emergency Condenser (Makeup)	6.45
Fire Protection	5.8
Early Fire Suppression	3.7
Main Steam Isolation Valve Closure	.8
Enclosure Spray Valve	.64
Restore Instrument Air	.52
Late Fire Suppression	.51
Restore Offsite Power in Short-Term	.39
Emergency A.C. Power	.45
Turbine Bypass Isolation	.190
Re-Establish Main Condenser	.136
Feedwater System	.000[a]
LPS Preventing RDS	.074
Shutdown Cooling System	.095
Turbine Bypass	.050
Recirculation Pump Trip	.010
Control Rod Drive Makeup System	.028
Restore Offsite Power Long-Term	.024
RDS Valve Remains Closed	.000[a]

[a]Failure rate already unity in dominant accident sequences considered.

TABLE II

Importance Ranking of Instrument Groups

Relative Ranking	Importance	Action	Required Instruments
1	4.1×10^{-1}	Repair or restore PIS	EL, YL, CSF, RSP
2	1.8×10^{-1}	Feed and bleed and high pressure recycle following EC failure	RSP, SDL, HL, CST, FWF, VL
3	1.3×10^{-1}	Fire system makeup to EC	RSF, ECL
4	1.15×10^{-1}	Close MSIV following spurious opening of TBPV	SDL, FWF
5	1.14×10^{-1}	Restore FW following spurious opening of TBPV	RSP, 4014, SDL, MSIV
6	8.0×10^{-2}	High pressure recycle following PIS failure	VL, RSP, EL, HL
7	8.0×10^{-2}	Feed system recycle following PIS failure	EL, VL, CSF, RSP, HL
8	7.6×10^{-2}	Inject FW following RDS/CS failure; makeup to hotwell with FPS	VL, RSP, CSF, FWF, EL, HL, CST
9	7.0×10^{-2}	Manually open CS valves	VL, RSP, CSF, CSV
10	7.0×10^{-2}	Use condensate pumps to supply water to core (makeup to hotwell with FPS)	VL, RSP, CSF, FWF, EL, HL, CST, 2B

Glossary of Instrument Abbreviations Used in Table II

Instrument/Parameter	Symbol
Core spray line flow	CSF
Condensate Storage Tank level	CST
Core spray valve positions	CSV
EC level	ECL
EC valve positions	EVL
Enclosure level	EL
Feedwater flow	FWF
Hotwell level	HL
Main Steam Isolation Valve position	MSIV
Reactor system pressure	RSP
Steam drum level	SDL
Vessel level	VL
2B bus voltage	2B
Control Valve 4014 valve position	4014

PLANT MODIFICATION AS A SUBSTITUTE FOR QUALIFICATION

A procedure was developed in which the importance of qualification of an equipment item (or group of items) is calculated and compared for various sets of plant modifications. Results for Big Rock Point are summarized below. These results indicate the following:

- Based on the models used in the PRA for equipment failure rate as a function of environmental condition, equipment qualification to the DOR Guidelines would result in little if any decrease in total core damage frequency.
- Altering these models to incorporate the most extreme assumption of equipment failure (i.e., failure rate of unity under any harsh environmental condition) and including the further assumption that qualification to the DOR Guidelines would return the failure rate to normal, equipment qualification for key systems has very high importance for the plant as-is.
- With the key design modifications listed in Table III, the importance of further qualification is reduced significantly as illustrated below.

Qualification Importance Using PRA Models and With Plant As-Is	Qualification Importance Under Very Extreme Failure Assumption and Plant As-Is	Qualification Importance Under Very Extreme Failure Assumption and with Key Plant Modifications
~ 0	25.6	0.16

TABLE III

List of Big Rock Point Plant Design Modifications
Affecting the Importance of Qualification

Replace a manually operated Emergency Condenser makeup valve with an automatic, motor-operated valve.

Modify manually operated valves in the Post Incident System so that these valves can only be locked in their correct position. Install position indicators for the valves.

Incorporate a procedural change in which the Feedwater System is used for long-term cooling during loss of coolant accidents for which the Feedwater System is capable of supplying makeup at a rate greater than the coolant outflow rate.

Incorporate a signal for automatic closure of the turbine bypass isolation valve at a reactor vessel water level above the level at which the Reactor Depressurization System is actuated.

Develop a procedure for diagnosing the cause of Instrument Air System failure and demonstrate through operator training that at least 99% of system faults can be diagnosed within ~ 2 hours.

Correct the cause of leaking Reactor Depressurization System (RDS) valve and operate with RDS-101 valves open.

Provide double valve isolation at containment interfaces where single valve isolation exists.

TABLE III (Continued)

Sustain load rejection 9 out of 10 times.

Provide indication of containment water level where this indication is not affected by harsh conditions in containment.

CONCLUSIONS

The general conclusion from this work is that the PRA-based approach to importance ranking of safety equipment is feasible. It provides a systematic, logical basis for an ordering of equipment importance. Other more specific conclusions are as follows:

- A tight schedule for testing equipment with the uncertainties in future equipment qualification requirements make a safety equipment priority list very desirable. PRA is a technically feasible approach to providing a safety ranking of equipment. Use of PRA in regulation and licensing will require that individual licensees lay the proper groundwork with the NRC.

- The PRA-based approach to establishing priorities for equipment qualification will probably be best applied to older plants for which the requirements are more flexible.

- It is expected that qualification of certain instruments which provide information to the operator to allow accident sequences to be better managed could play a key role in an overall strategy for equipment qualification at some plants.

- It is expected that, at least for older plants, modifications or procedure changes may be more cost effective and certain in achieving risk reduction than environmental qualification of each item of equipment. This suggests the possibility that such plant changes could be used as a substitute for qualification or as a basis for reconsidering qualification requirements.

THE USE OF OPERATOR ACTION EVENT TREES TO ADDRESS REGULATORY ISSUES

Wesley A. Brinsfield and Robert G. Brown

Wood-Leaver and Associates, Inc.
1340 Saratoga-Sunnyvale Road
Suite 206
San Jose, CA 95129 U.S.A.

Patrick Donnelly

Consumers Power Company
Big Rock Point Plant
R. R. #3
Charlevoix, MI 49720 U.S.A.

ABSTRACT

The functional event trees constructed for the Big Rock Point (BRP) probabilistic risk assessment have been expanded to focus upon and highlight the role of the plant operators during accident sequences. These trees have been used to address regulatory issues as they apply to the BRP nuclear plant. Two examples of their use are the assessment of the need for wide range level instrumentation to monitor inadequate core cooling, and an assessment of shift staffing requirements for the BRP plant. This paper will briefly describe the methodology employed in developing the Operator Action Event Trees (OAETs), as well as the application of these tools to address these specific regulatory issues at BRP. Applications to other issues within the nuclear power industry will be suggested.

INTRODUCTION

Probabilistic Risk Assessment (PRA) is a valuable resource which can be used to help assure continued safe operation of nuclear power plants. One area where PRAs will be most useful is in addressing regulatory requirements that are imposed on plants by the Nuclear Regulatory Commission (NRC). One example of such use is the PRA performed for the Big Rock Point (BRP) nuclear power plant [1]. Typically, generic regulations and requirements address a standard plant which has substantially different systems and operating parameters than BRP. The relatively simple design and small size (75 MWe) of BRP require careful screening and evaluation of such issues to ensure that they are relevant to BRP, and to determine the best response to regulatory requirements from a risk and benefit/cost perspective. The analysis documented in this paper provides an important first step in utilizing the risk assessment to address such issues for BRP. The methodology employed is applicable to other plants as well.

METHODOLOGY

To realistically and efficaciously investigate the impact of regulations and

requirements on plant safety, any evaluation of changes to plant design and/or operation must be based on a firm foundation consisting of:

- An explicit identification of potential accident sequences which could occur and the plant states comprising these sequences.
- A clear understanding of the plant response associated with each plant state.
- A careful delineation of the actions required of the operator at each plant state.

Event trees provide a logical framework upon which this foundation can be constructed.

A major result of any PRA is the development of event trees for the transient and accident initiators which have occurred or could be hypothesized to occur at the plant under examination. These event trees are based upon the fundamental functions which must be performed by the plant safety systems either automatically or through operator action (e.g., maintenance of coolant inventory, decay heat removal, etc.). They provide a systematic identification of the various combinations of component or system failures which result in an inability to perform one or more of these fundamental functions. From these event trees a set of dominant accident sequences are generated using best-estimate probabilistic data. These sequences have been utilized for a more detailed assessment of operator actions and plant response. Focusing on the dominant accidents ensures that events which have the potential to impact the health and safety of the public are addressed, thus satisfying the first criterion noted previously.

The event trees and dominant accident sequences developed in the PRA have been utilized to develop operator action event trees (OAETs). The methodology employed for OAET development is detailed in NUREG/CR-1440 [2]. OAET models follow the same logic paths as those in the PRA, but the role of the operator as the sequence progresses is explicitly highlighted. This required modifying the PRA event trees to focus on the role of the operator as the accident evolves. Each state of the original event tree is examined carefully to determine the appropriate operator response at that particular point in the accident progression. The events which involve operator action are identified, and in some cases broken down into additional events in order to separate and highlight key operator tasks. In addition, the sequences are expanded to include additional operator actions which could be performed to prevent or minimize core damage but were conservatively neglected in the original PRA.

The goal of the OAET construction process is to produce a clear logical representation of the operator's role throughout the accident sequence and to document this model by clearly defining the following information:

- The Key States: The failure events which produce each key state enumerated in the OAET are delineated and their implication to the maintenance of the critical safety functions is described.
- The Required Operator Response: Emergency procedures, guidelines, and other relevant information including input from the reactor operators are used to describe the appropriate operator actions at each state.
- The Key Symptoms Exhibited by the Plant: The physical plant response at each state is described in terms of measurable plant parameters. The necessary and sufficient information required by the operator to unambiguously diagnose each plant state is defined. This is acquired from plant transient and safety analysis performed in support of the design, best-estimate analysis of the dominant sequences, and plant operating experience.

OAETs have been developed for BRP which address all key operator actions necessary to respond to the events comprising dominant accident sequences. An example of an OAET developed for BRP is presented in Figure 1. This sequence is initiated by a loss of offsite power and followed by a failure of the onsite emergency diesel, the emergency condenser, and the core spray system. Operator responses to each of these events are represented in this tree. These include diesel repair, actuation of the standby diesel, providing makeup to the emergency condenser, and manual depressurization. The documentation which accompanies this OAET includes a state-by-state description addressing each of the information areas previously noted.

APPLICATIONS

The set of OAETs developed for the dominant sequences has been used to address the specific issues of the need for wide-range reactor vessel water level instrumentation and the adequacy of shift staffing at BRP. This section highlights the results of these key application projects.

By focusing attention on the operator's information needs during the dominant sequences at BRP, specifically as this information relates to actions taken to prevent or respond to conditions of inadequate core cooling, an assessment of the adequacy of the existing BRP control room instrumenation was made. Particular attention was focused on the need to be able to monitor vessel water level within the active fuel zone of the core (i.e., "wide-range level" instrumentation).

BRP currently has "narrow range" instrumentation which has the capability to monitor vessel water level as low as an elevation of 2 feet above the top of the active core. However, the NRC had requested the plant to specifically address the effectiveness of the wide-range monitoring capability in their inadequate core cooling (ICC) instrumentation assessment. Using the OAET model and documentation, the information required by the operator to unambiguously identify each plant state as well as the information required to implement and verify the appropriate action(s) for each state was specified in terms of the fundamental plant parameters. This list of information needs was compared to the instrumentation available at BRP to assess its adequacy.

It was concluded that the existing BRP instrumentation provides the necessary and sufficient information for the operators to respond to failure events in the dominant accident sequences and bring the plant to a safe shutdown condition. Wide-range level monitoring capability would not enhance the operator's capability to diagnose plant conditions or detect a situation which could lead to ICC. Narrow range level instrumentation supplemented by other plant instrumentation is adequate for this purpose. Extended vessel water level monitoring capability would only provide confirmatory, not essential, information to the operator. Furthermore, wide-range level instrumentation does not provide additional information which would alert the operator to take alternative actions or use additional systems to prevent ICC. The relatively simple BRP design provides the operator with only a few actions to respond to core uncovery conditions -- those which he is instructed to take should level drop below the range of the existing narrow range instrument. Once these are performed (or attempted) there are no other options available to prevent core damage. The existing plant instrumentation is adequate to inform the operator that these actions are required.

Finally, for some accidents wide-range level instrumentation would not provide a reliable indication of adequate core cooling. This was demonstrated by the analysis of reactor coolant piping system breaks below the core elevation. For such LOCAs where the break flow exceeds the core spray makeup flow, vessel liquid level will not recover. However, this does not mean that there is inadequate heat removal from the fuel. It has been demonstrated that the BRP core spray system will effectively remove decay heat from an uncovered core. Reflood is not required to ensure adequate core cooling. Hence, even if wide-range level were available, it could not be relied upon for unambiguous determination of ICC as required by NUREG-0737 [3], since it is

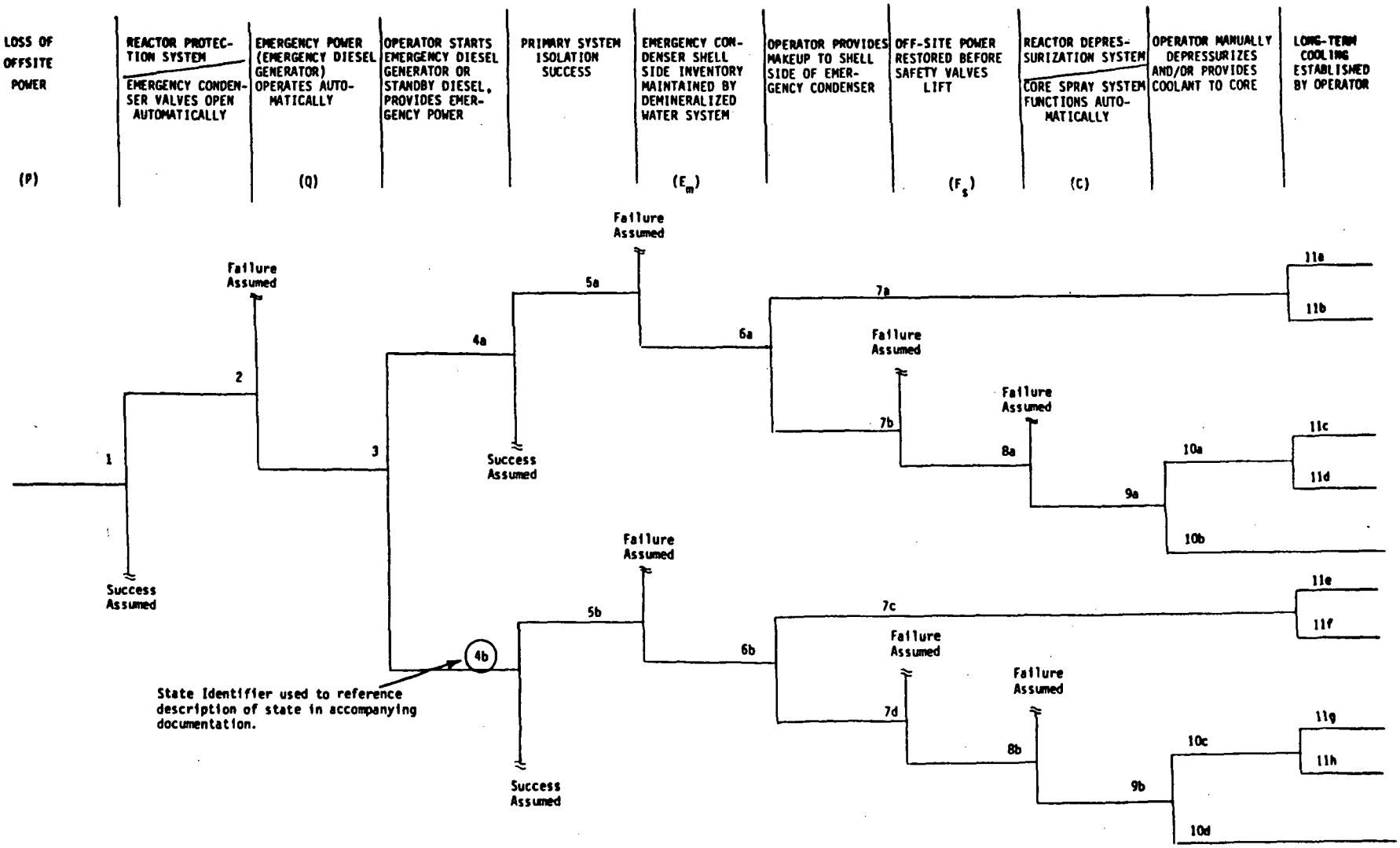


Figure 1. Operator Action Event Tree For a Station Blackout Sequence at Big Rock Point

possible to prevent core damage without recovering water level. For breaks of this type, the operator must rely upon core spray line flow to inform him that adequate heat removal is being provided.

OAETs have also been used at Big Rock Point to assess the adequacy of shift staffing and plant call-up procedures for responding to site emergencies. This assessment was performed in response to NRC Generic Letter 81-10 [4] which specified minimum on-shift staffing levels for operating plants. As noted previously, the development of the OAETs produced a list of actions which should be performed in responding to various failure events in an accident sequence and the specific conditions under which these actions must be taken. Using this information as a foundation, the following approach was used to evaluate the adequacy of BRP shift staffing:

(1) Determine the personnel required to perform the actions identified for the individual states in the OAETs for dominant accident sequences.

(2) Integrate the results of the analyses for the individual states to determine the staffing needs for each sequence as described by the OAET.

(3) Compare the manpower needs specified above to those currently available at BRP.

(4) For any additional staffing needs identified from this comparison, evaluate each case using a risk criterion to assess the need for changes in the BRP shift staffing.

To perform the initial task, additional information was developed for each operator action. This data included:

- The time limitations on the required actions,
- The location and associated environmental conditions where the actions must be performed,
- The time required to diagnose the problem and take the specific action,
- The skills required to perform the specific task.

These key information needs are all interrelated and form the basic data base upon which staffing evaluations were made. Using this information the specific personnel requirements were determined for each dominant sequence. This list of personnel was then compared to the available on-shift personnel at BRP. Call-up procedures were also evaluated based upon the time limitations imposed by the sequences to determine if personnel not on site would be able to respond within these time constraints. Based upon this work, recommendations were made concerning the adequacy of shift staffing and call-up procedures at Big Rock Point, and the role of the Shift Technical Advisor (STA). These include:

- The current staffing at BRP is adequate to respond to the risk significant sequences identified in the BRP probabilistic risk assessment. With the plant in its present configuration, no sequences were identified in which additional personnel were required to respond effectively to the sequence. This analysis showed that only one Senior Reactor Operator (SRO) (not two as stated in Ref. 4) is necessary to respond to risk significant sequences.

- An extra auxiliary operator (AO) would be helpful, but is not essential, in responding to some station blackout sequences. The sequences in which this additional AO would provide support are of very low probability, and the cost of adding a third AO on-shift does not justify the minimal decrease in risk due to this action.

- The existing procedures for call-up of plant personnel are adequate to respond to risk significant sequences. No sequences were identified in which personnel not on-site at the outset of the event would be required before a significant amount of time (i.e., enough time to respond to a call) has passed.

- BRP operators (SRO and RO) are capable of diagnosing plant conditions during potential accidents and taking the correct action. It is not evident that a STA would provide a significant improvement in the diagnostic efficiency of the operating staff during risk significant accident sequences. The relatively simple BRP plant and control room design coupled with the extensive experience of the BRP operators allows the STA to play a smaller diagnostic role than at newer and/or more complex plants.

CONCLUSIONS

This project has demonstrated that OAETs are a very useful tool for applying the results of a risk assessment to enhance the safety of operating plants, and to address regulatory issues. The approach provides a logical foundation for decision-making in the many and varied issues confronting operators of modern power plants. Operator action event trees have proven to be valuable aids for maximizing the use of a plant's PRA and for efficiently, logically, and systematically addressing issues which impact the plant's performance and safety. Two specific issues for which the OAET methodology has been successfully applied have been described in some detail.

In addition to the two examples discussed, other issues have been proposed for which OAETs would be applicable. One example of such a use is a project now underway which is using OAETs to review generic emergency procedure guidelines (EPGs). By using the list of suggested operator actions generated by an OAET analysis for a "generic" plant, along with available "best-estimate" calculations on plant response, a review of the compatibility and completeness of EPGs is being performed. Almost any potential plant modification (hardware or procedural, site specific or generic) can be analyzed with OAETs by changing the focus of the study to evaluate the specific issue(s).

In conclusion, many current regulatory issues address man/machine interface issues. These issues will require significant input from human factors analysts. In order to practically obtain the potentially significant benefits afforded by the various human factors disciplines, there must be a strong interaction between the human factors analysts and the plant thermal-hydraulic analysts. The role of the operator under accident conditions can be effectively investigated only if the plant physical response under these conditions is known, the information flowing to the operator via the plant instrumentation is identified, the effect of postulated operator responses to these conditions is determined, and the necessary diagnosis and response strategies are charted. The OAET methodology systematically develops and presents the realistic thermal hydraulic response of the plant to risk significant accident sequences in a form which can be readily integrated into human factors engineering analysis. Hence, the work reported here is a significant first step in providing this necessary link between the plant response analyst and the human factors analyst.

REFERENCES

1. Consumers Power Company, Probabilistic Risk Assessment, Big Rock Point Plant, Docket No. 55-155, March 1981.

2. J. vonHerrmann, R. Brown, A. Tome, "Light Water Reactor Status Monitoring During Accident Conditions," NUREG/CR-1440, June 1980.

3. "Clarification of TMI Action Plan Requirement," NUREG-0737, November 1980.

4. USNRC Generic Letter 81-10, "Post-TMI Requirements for the Emergency Operation Facility," Daniel G. Eisenhut to All Licesnsees, February 18, 1981.

RISK ASSESSMENT OF FILTERED-VENTED CONTAINMENT OPTIONS FOR A BWR MARK III CONTAINMENT

F. T. Harper and A. S. Benjamin
Sandia National Laboratories
Albuquerque, New Mexico

ABSTRACT

We have recently evaluated the risk reduction achievable in a Mark III containment boiling water reactor (Grand Gulf) by incorporating various types of containment venting systems, as well as other severe accident safety systems. Risk reduction factors of up to 100 were calculated for certain containment venting options. Achievement of this risk reduction potential was found to be dependent upon several factors, including: (1) availability of a service water tie-in to replenish water supplies; (2) ability of the venting system to handle ATWS accidents; (3) ability to eliminate hydrogen burns after significant risk reduction has already taken place; and (4) assumptions made regarding phenomenological uncertainties. The use of high-efficiency filtering media was found to be unnecessary.

I. INTRODUCTION

For the past few years, Sandia has been investigating the merits of filtered vented containments and other safety systems for the mitigation and prevention of severe accidents in light water reactors.[1,2] During this time, we developed a methodology in which probabilistic risk assessment techniques and results are used to evaluate the risk reduction achieved by different accident mitigation and prevention schemes. This methodology was first used to evaluate the effectiveness of filtered vented containment options for a Mark I containment boiling water reactor (Peach Bottom).[3-5] The methodology has now been modified to compare the risk reduction potential of several improved safety strategies, including filtered vented containments, for a Mark III containment boiling water reactor (Grand Gulf).[6] This paper describes the results recently obtained for Grand Gulf.

II. SAFETY STRATEGIES CONSIDERED

The public risk from Grand Gulf Unit 1 was analyzed with and without several design modifications. The improved safety strategies which were considered in this analysis are the following:

1) An additional passive containment cooling system.

2) An additional decay heat removal system.

3) The utilization of an external water supply tie-in to the vessel. (The Standby Service Water System (SSWS) tie-in to the Residual Heat Removal (RHR) System is available for this purpose).

4) The utilization of an external water supply tie-in to the suppression pool. (The SSWS is again available.)

5) Low volume venting capability (vent flow capacity of 15,000 cubic feet per minute which cannot handle Anticipated Transient Without Scram (ATWS) overpressurizations).

6) High volume venting capability (vent flow capacity of 400,000 cubic feet per minute at venting pressure which can handle ATWS overpressurizations).

Several combinations of the above strategies were also analyzed. For the venting cases, three filter options were considered: no additional filter, a crushed rock filter, and a filter train consisting of crushed rock, charcoal, and high efficiency particulate filters.

In combination with the strategies listed above, the following plant system variations were also considered:

1) An improved Reactor Protection System (RPS).

2) Improved Safety Relief Valves (SRV).

3) Improved SSWS reliability.

4) A controlled hydrogen ignition system in containment.

5) A post accident inerting system[7] installed to prevent hydrogen burns, with and without purge capability.

6) A gas turbine combustor system[8] installed to prevent hydrogen burns.

7) A recovery model for long-term loss of RHR sequences which is more optimistic than the one originally used in the Grand Gulf RSSMAP PRA.[9]

Reasonable combinations of the above variations were also considered.

III. EVENT TREES

Event tree logic was used to obtain the accident sequences that were quantified for each strategy. Three event tree stages were necessary. Sequences from initiating event trees led to sequences from a mitigating event tree which led to containment event tree sequences. The initiating event trees were identical to the system event trees developed in the Grand Gulf RSSMAP report with the following exception: A station blackout sequence in which the Reactor Core Isolation Cooling System (RCICS) fails in five to eight hours due to battery depletion or turbine failure, was added and quantified using numbers derived in Sandia's Station Blackout Program.[10] After the improved safety strategies were incorporated into the plant model, the system sequences were requantified.

The mitigation event trees included decision points for all of the improved safety features which were added and choices for recovery at different stages of the accident. These trees also included a decision point for failure of pumps after loss of net positive suction head to deal with pump survivability uncertainties. More information on the mitigation event trees is given in References 3, 5, and 6.

The containment event tree included the traditional WASH-1400 containment failures[11] along with specific containment failures associated with containment venting. The modified containment event tree also includes the possibility of containment survival after core melt.

IV. TREATMENT OF UNCERTAINTIES

An important part of the risk assessment was the treatment of uncertainties. Phenomenological and systemic uncertainties found in the sequences were handled parametrically with a conservative and nonconservative value calculated for each uncertainty. Conservative values generally represented expert opinion as defined by WASH 1400 and other risk assessments while nonconservative values represented the evolving industry position. Bounding risk calculations were then performed for each strategy using first the conservative and then the nonconservative assumption sets. The uncertainties that were bounded in this manner were:

1) Probability of in-vessel steam explosions failing containment.

2) Probability of ex-vessel core water interactions failing containment.

3) Probability of hydrogen burns failing containment.

4) The iodine release form (I_2 or CsI).

5) Particulate deposition on primary system structures.

6) Particulate fallout in unfailed containment.

7) Particulate and I_2 removal in the suppression pool at saturated conditions.

8) Particulate removal in crushed rock at superheated conditions.

9) RPS recovery factors after an ATWS.

10) Containment failure pressure.

11) Location of containment breach; subsequent suppression pool availability.

12) Severity of containment breach; subsequent injection systems survivability.

Sensitivity calculations were performed to judge the relative importance of the different uncertainties on the risk with and without the add-on safety features.

An uncertainty which was handled differently was the nonrecovery model used to quantify the long-term loss of RHR sequences. As mentioned in Section II, RHR recoverability was treated as a plant system variable so that the sensitivity of the results to this variable could be studied individually.

V. RISK QUANTIFICATION

All strategies were initially compared on the basis of expected population dose. The expected population dose for each sequence involved a calculated normalized dose to the public weighted by the sequence probability. The sequence probabilities were calculated using RSSMAP results updated to reflect advances in the state-of-the-art, nominal failure probabilities for mitigative systems, and

updated WASH-1400 containment failure probabilities. The quantification of the normalized dose to the public involved the use of the ORIGEN, CORRAL, and CRAC codes. Selection of the best safety strategies was made on the basis of the overall potential for reducing expected population dose. After the selection was made, additional CRAC code calculations were performed to estimate the potential reduction in early fatalities, latent cancer fatalities, and property interdiction.

VI. RESULTS

Results of the Grand Gulf Filtered-Vented Containment Risk Assessment are shown in Table 1 for five venting strategies and the base case, which represents the modified PRA results without any of the venting options incorporated.

The results are given in terms of expected population dose (man rem/year) and risk reduction factors (based on reduction in expected population dose). The population dose calculations shown in Table 1 assumed a uniform population distribution of 100 people per square mile. CRAC code calculations have since been made for several strategies using the actual population distribution surrounding Grand Gulf, yielding results close to the original approximations. For Grand Gulf, a decrease in population dose of about 25% using the conservative assumption set and a twofold increase in population dose using the nonconservative assumption set is expected when one shifts from calculations using the uniform population distribution to the actual population distribution.

Other venting strategies were considered (high and low volume vents with valves which allow the containment to depressurize down to 15 psia rather than relief valves, high and low volume vents which are closed prior to meltdown and SSWS tie-in to the suppression pool rather than to the vessel), but are not shown in the table because results for those strategies do not differ significantly from the strategies shown.

The expected population dose for each of the strategies was calculated for several different initial plant assumptions. The assumptions involve effectiveness of hydrogen control systems, reliabilities of the Reactor Protection System (RPS) and the Safety Relief Valves (SRV), and the recovery model used for long-term loss of RHR accidents. The hydrogen control system shown in the table is the Post Accident Inerting system (PAIS) with purge capability which was assumed capable of eliminating all hydrogen burn containment failures (PAIS reliability was assumed to be 99%). Hydrogen ignitors and PAIS without purge capability were assumed in this study to be less than 99% effective while the Gas Turbine Combustion System was assumed to be too expensive to be practical.

Calculations using the RPS and SRV reliabilities from the Grand Gulf RSSMAP PRA are shown as well as calculations using improved RPS and SRV reliabilities. Grand Gulf has committed to improving its RPS and will have SRVs which may be more reliable than analysis takes credit for. Calculations with and without the improved SRV reliability are very similar. The results shown in the table for improved SRV and RPS reliabilities are almost identical to results assuming improved RPS reliability only.

Calculations were first made with the exponential nonrecovery model used in WASH-1400 and RSSMAP studies for all accident sequences except ATWS sequences. This nonrecovery term was applied only to components which are considered recoverable. Then calculations were made applying an additional recovery term to the long-term loss of heat removal sequences to account for heroic recovery actions. The nonrecovery factor used, the exponential model multiplied by 0.1, is considered to be optimistic and is applied to evaluate the importance of the recovery model in the assessment of the worth of the different vent filter strategies. Sequences

other than the long-term loss of heat removal sequences were handled in the same manner as in the original calculation.

Calculations were made assuming an improved SSWS reliability, considering the possibility of core recovery before core melts, assuming greater reliabilities for the mitigating systems, and other initial plant assumptions, but results are not shown here because conclusions regarding the merits of venting were identical to those discussed for the plant assumptions shown in Table 1.

VII. DISCUSSION

The following insights have been gained from the Grand Gulf Filtered-Vented Containment Risk Assessment:

a) Venting strategies that eliminate long-term containment overpressurizations, but do not provide makeup water or ATWS mitigation (low volume vents) result in a population dose risk reduction of from 2 to 3 relative to the base case. This risk reduction is predominantly due to the additional time to core melt gained in these situations, which increases the probability of recovery before core degradation. When more optimistic credit is taken for recovery during long-term loss of heat removal accidents in both the base case and low volume vent case, the risk reduction is almost nil.

b) Higher risk reduction (factors of from 3 to 6) can be obtained by utilizing the standby service water tie-in to replenish suppression pool water that is vented (in the form of steam) from the containment. The risk reduction achievable if the optimistic recovery factor for longterm accidents is applied is only a factor of 2.

c) Risk can be reduced significantly more (factors of from 15 to 40) if ATWS fixes are considered along with longterm containment overpressure mitigation (e.g., GE's proposed ATWS Implementation 3A or use of high volume venting with the service water tie-in). The risk reduction factors when the more optimistic long-term recovery factors are applied range from 12 to 18.

d) After ATWS sequences and long-term containment overpressure sequences have been mitigated, risk can be reduced further by a working hydrogen control system (factors of from 18 to 91). Without reducing risk from both ATWS and the long-term overpressure sequences, hydrogen events are unimportant to risk. More optimistic recovery factors bring the risk reduction factors down to between 4 and 25.

e) After significant risk reduction has taken place, accidents involving loss of ECCS injection (predominantly the station blackout sequence with RCIC failure between 5 and 8 hours) drive risk. Hydrogen control brings the consequences of these sequences down by eliminating a large portion of the early containment failure and allowing more time for radionuclide plateout in the containment. Filtered-venting reduces the consequences of these sequences only slightly because containment plateout and deposition in the primary system and the suppression pool occur whether or not there is a vent. These sequences, therefore, form an upper bound of achievable risk reduction.

f) Filters reduce the risk somewhat, but not significantly more than by using only the existing suppression pool as a scrubber.

g) The better a strategy is in reducing the population dose risk, generally the better it is in reducing the probability of core melt. The better strategies reduce the core melt frequency by factors of up to 14.

VIII. CONCLUSIONS

The cost of a simple high volume vent utilizing the suppression pool as a scrubber for a Mark I BWR has been estimated by Holmes and Narver, Inc. (an architect-engineering firm subcontracted by Sandia) to be about $1.2 million. This cost is quoted in 1980 dollars and includes a 15 percent contingency and a 6 percent fee. It will be assumed that the cost of the backfit would be comparable for a Mark III containment. Comparison of this figure with the values of man-rems averted for a high volume vent with the suppression pool scrubber given in Table 2 gives the following insights:

a) At $1000 per man-rem averted, it appears that a vent is cost-effective using the conservative set of uncertainty assumptions for all initial plant assumptions.

b) At $100 per man-rem averted, using conservative uncertainty assumptions, it appears that a vent is borderline cost-effective if one assumes conservative RPS/SRV reliabilities and the conservative nonrecovery model for long-term accidents. If either of these assumptions are not assumed, the vent is not cost-effective.

c) For the nonconservative set of assumptions, a vent is not cost effective for $1000 or $100 per man-rem averted.

It appears that the effectiveness of a vent is determined by the assumptions that one makes, either about system and phenomenological uncertainties or about initial plant conditions.

Using conservative assumptions about unncertainties and recovery models, one can make a case for a cost-effective vent with risk reduction factors of up to two orders of magnitude. Using nonconservative assumptions, it appears that a vent is not cost effective and the reduction in risk achieved is less than one order of magnitude.

The decontamination factors used for the primary system plateout and the probabilities of suppression pool unavailability given containment failure are the major contributors to the large differences between the conservative results and the nonconservative results found in this study. In order to reach a firm conclusion about the cost-effectiveness of venting systems, uncertainties regarding these phenomena must be reduced.

Table 1. Comparative Risk for Filtered Vented Containment Strategies

Initial Plant Assumptions	Base Case		Low Vol. Relief, Gravel Filter		Hi Vol. Relief, Gravel Filter		Low Vol. Relief, Gravel, SSWS Tie-In to Vessel		Hi Vol. Relief, Gravel, SSWS Tie-In to Vessel		Hi Vol. Relief -No Filter, Low Vol. Relief -Gravel, SSWS Tie-In to to Vessel	
	Cons	Non Cons	Cons	Non Cons	Cons	Non Cons	Cons	Non Cons	Cons	Non Cons	Cons	Non Cons
A. No H_2 control, present RPS/SRV reliabilities, (exp-t/19) non-recovery model for all sequences, t in hours	4E2	3E0	1E2 (3)	2E0 (2)	4E1 (9)	2E-1 (14)	7E1 (6)	9E-1 (3)	1E1 (40)	2E-1 (20)	1E1 (40)	2E-1 (20)
B. PAIS with purge capability H_2 control present RPS/SRV reliabilities, (exp-t/19) non-recovery model for all sequences	4E2	3E0	1E2 (3)	2E0 (2)	4E1 (11)	2E-1 (16)	6E1 (6)	9E-1 (4)	4E0 (91)	1E-1 (23)	5E0 (89)	1E-1 (23)
C. No H_2 control, present RPS/SRV reliabilities, (exp-t/19)x.1 non-recovery model for long-term sequences, (exp-t/19) for all others	2E2	2E0	1E2 (1.2)	1E0 (1.1)	4E1 (4)	2E-1 (8)	7E1 (2)	9E-1 (2)	9E0 (18)	1E-1 (12)	9E0 (18)	1E-1 (11)
D. No H_2 control, improved RPS/SRV reliabilities, (exp-t/19) non-recovery model for all sequences	3E2	2E0	3E1 (12)	3E-1 (6)	2E1 (18)	2E-1 (10)	2E1 (19)	2E-1 (9)	9E0 (32)	1E-1 (15)	9E0 (34)	1E-1 (15)
E. PAIS with purge capability H_2 control, improved RPS/SRV reliabilities, (exp-t/19) non-recovery model for all sequences	3E2	2E0	2E1 (15)	3E-1 (7)	1E1 (30)	1E-1 (14)	9E0 (32)	2E-1 (10)	3E0 (89)	1E-1 (18)	3E0 (89)	1E-1 (18)
F. PAIS with purge capability H_2 control, improved RPS/SRV reliabilities, (exp-t/19)x.1 non-recovery model for long-term sequences, (exp-t/19) for all others	5E1	4E-1	1E1 (3)	2E-1 (2)	5E0 (9)	1E-1 (3)	8E0 (6)	2E-1 (2)	2E0 (25)	9E-2 (4)	2E0 (25)	9E-2 (4)

(Top numbers represent population dose - man-rem/year. Numbers in parenthesis are risk reduction factors relative to the appropriate base case.)

Table 2. Value of Man Rems Averted*

Initial Plant Assumption

	At $1000 Per Man Rem Averted(NRC)		At $100 Per Man Rem Averted (AIF)	
	Cons	Non Cons	Cons	Non Cons
A. No H_2 control, present RPS/SRV reliabilities, exp-t/19 non-recovery model for all sequences	$1.2x10^7	$8.4x10^4	$1.2x10^6	$8.4x10^3
B. PAIS with purge capability H_2 control, present RPS/SRV reliabilities, exp-t/19 non-recovery model for all sequences	$1.2x10^7	$8.7x10^4	$1.2x10^6	$8.7x10^3
C. No H_2 control, present RPS/SRV reliabilities, (exp-t/19)x.1 non-recovery model for long-term sequences, exp-t/19 for all others	$4.5x10^6	$4.2x10^4	$4.5x10^5	$4.2x10^3
D. No H_2 control, improved RPS/SRV reliabilities, exp-t/19 non-recovery models for all sequences	$8.4x10^6	$5.1x10^4	$8.4x10^5	$5.1x10^3
E. PAIS with purge capability H_2 control, improved RPS/SRV reliabilities, exp-t/19 non-recovery model for all sequences	$8.6x10^6	$5.1x10^4	$8.6x10^5	$5.1x10^3
F. PAIS with purge capability H_2 control, improved RPS/SRV reliabilities, (exp-t/19)x.1 non-recovery model for long-term sequences, exp-t/19 for all others	$1.4x10^6	$7.8x10^3	$1.4x10^5	$7.8x10^2

*All numbers pertain to a high volume relief strategy with the SSWS tie-in to vessel. A reactor lifetime of 30 years is assumed.

References

1. A. S. BENJAMIN, "Program Plan for the Investigation of Vent-Filtered Containment Conceptual Designs," Sandia National Laboratories, SAND79-1088, NUREG/CR-1029 (1979).

2. A. S. BENJAMIN, et al., "Filtered-Vented Containment System (FVCS) Design Study," in Report of the Zion/Indian Point Study, ed. W. B. Murfin, Chapter 1, Sandia National Laboratories, SAND80-0617/1, NUREG/CR-1410 (1980).

3. A. S. BENJAMIN, F. T. HARPER, and P. CYBULSKIS, "Filtered-Vented Containment System Conceptual Design Study and Risk Assessment for a BWR Mark I Containment," Sandia National Laboratories, to be published.

4. A. S. BENJAMIN, F. T. HARPER, and P. CYBULSKIS, "Probabilistic Risk Assessment of Filtered-Vented Containment Systems: Mark I BWR," Trans. Am. Nucl. Soc., 38, 501 (1981).

5. A. S. BENJAMIN, F. T. HARPER, and P. CYBULSKIS, "Risk Assessment of Filtered-Vented Containment Options for a BWR Mark I Containment," paper given at the 1981 Port Chester, New York, ANS Topical Meeting on Risk Assessment.

6. F. T. HARPER, A. S. BENJAMIN, "Filtered-Vented Containment System Risk Assessment for a BWR Mark III Containment, Sandia National Laboratories, to be published.

7. Allens Creek FSAR.

8. H. J. REILLY, et al., "Conceptual Design of a Core Melt Mitigation System for a PWR with an Ice Condenser Containment," Idaho National Engineering Laboratory, EGG-PR-5633 (1982).

9. S. W. HATCH, P. CYBULSKIS, R. O. WOOTON, "Reactor Safety Study Methodology Applications Program: Grand Gulf #1 Power Plant," Sandia National Laboratories, SAND80-1897/4 of 4, NUREG/1659/4 of 4.

10. A. M. KOLACZKOWSKI, A. C. PAYNE, Jr., "Station Blackout Accident Analyses," Sandia National Laboratories, to be published.

11. N. C. RASMUSSEN, et al., "Reactor Safety Study," WASH-1400, NUREG-75/014 (1975).

RISK REDUCTION ANALYSIS OF SEVERE ACCIDENT PREVENTION AND MITIGATION SYSTEMS

S. W. Hatch, P. R. Bennett,
D. D. Drayer, and A. S. Benjamin

Sandia National Laboratories
Albuquerque, New Mexico 87185 USA

ABSTRACT

The Nuclear Regulatory Commission (NRC) is currently addressing the problem of how regulations might be changed to include consideration of degraded core accidents. In support of this, the Severe Accident Risk Reduction Program is being performed to assess the benefits and impacts of a set of degraded core safety features. This paper describes some initial results of Phase I of the program which includes estimates of the effects which various preventive and mitigative safety features have on the frequencies and consequences of core melt accidents for six reference reactors.

INTRODUCTION

An NRC-sponsored program entitled "Severe Accident Risk Reduction (SARR) Program" is being conducted at Sandia National Laboratories to provide a value/impact assessment of various preventive and mitigative safety approaches on degraded core accidents. This assessment will become part of the data base to be used by NRC in the degraded core rulemaking process.

The Phase I assessment includes a ranking of candidate safety approaches on the basis of their potential for reducing risk. This has been done for each of the six reactors (see Table I) analyzed in the Reactor Safety Study[1] (RSS) and Reactor Safety Study Methodology Applications Program[2] (RSSMAP). This initial ranking is based on the ability of the safety approaches to reduce the core melt frequency and risk associated with the reference plants and does not include the cost of retrofitting or other impacts. These latter considerations are the subject of another paper[3].

The types of safety options analyzed in this program include a wide range of both preventive and mitigative add-on systems along with plant specific fixes which may correct particular vulnerabilities identified by probabilistic risk assessment. Best-case effects were generally attributed to each safety option and in the Phase I analysis no potential adverse or detrimental effects were considered. This will be considered in later analyses. It should be noted that there are other limitations and uncertainties in the risk assessments being used which may affect the types of safety approaches found to be beneficial. These include a lack of explicit consideration of external events and the use of some potentially conservative phenomenological assumptions.

Table I

Reference Plants Analyzed in Phase I

Plant	PRA	Vendor	Containment Type
Surry PWR	RSS	West	Dry subatmospheric containment
Peach Bottom BWR	RSS	GE	Mark I containment
Sequoyah PWR	RSSMAP	West	Ice condenser containment
Oconee PWR	RSSMAP	B&W	Large, dry containment
Calvert Cliffs PWR	RSSMAP	CE	Large, dry containment
Grand Gulf BWR	RSSMAP	GE	Mark III containment

METHODOLOGY

The first step in the Phase I SARR program assessment was to update the reference PRAs to reflect the newest available information. This update included reanalyzing certain containment failure modes, reassessing feed and bleed capabilities, and requantifying some of the accident sequence probabilities. The objective of this review was to bring all the PRAs being used to some common level.

The second step involved making an initial characterization of the potential benefits of the safety approaches for each type of accident identified in the reference PRAs. This was done by grouping the dominant accident sequences for a plant into sequences defined by failures of certain safety functions. Then, each safety approach was analyzed for its effect on the functional sequences. This functional screening provided an initial definition of how the safety options should work in order to be beneficial and provided information and insights on a general level which were easily compared to other plant results. Also, certain safety options were eliminated from further study in plants where they were found to have no effect on any functional sequence.

The initial characterization of safety approaches for Grand Gulf is presented as an example in Table II. Two LOCA and three transient functional accident sequences were found to be important. The BWR safety functions required after a LOCA are reactor subcriticality (RS), emergency core cooling (ECC), containment overpressure protection early and late (COE and COL), and radioactivity removal (RR). For transients, the required safety functions are RS, ECC, reactor coolant system overpressure protection (RCSOP), containment overpressure protection (CO), and RR. These safety functions are identified in Table II as failing either due to an initial system failure (X), post core melt (PCM), or post containment failure (PCF). The Xs to the right of the functional sequences indicate which safety approaches are applicable. For a more detailed discussion of LWR functional accident sequences, refer to Reference [4].

The initial characterization of safety approaches for Grand Gulf showed that containment venting systems were appropriate for accidents involving containment failure before core melting but had limited value for accidents involving early core melting because venting would not prevent the occurrence or significantly reduce the consequences of these accidents. Similarly, hydrogen control systems were found to be appropriate for accidents with core melting in an initially intact containment since only for these accidents will the possibility of hydrogen burning be important.

Table II

Results of Initial Safety Option Characterization for Grand Gulf

Dominant LOCA Functional Accident Sequences					Applicable Candidate Degraded Core Safety Approaches for Grand Gulf									
					Additional Containment Heat Removal Systems[1]	Addition of Hydrogen Control Devices[3]	Addition of Core Retention Devices[4]	Addition of Containment Venting System	Addition of Particulate Removal System	Additional Coolant Injection Systems	Increase RPS Reliability	Increase Containment Design Pressure[6]	Addition of Missile Shields[7]	Other Accident Specific Fixes[8]
IS	ECC	COE	COL	RR										
	PCF		X	PCM	X			X				X		X
	X		PCM	PCF		X	X			X		X	X	X
Dominant Transient Functional Accident Sequnces														
IS	ECC	RCSOP	CO	RR										
	PCF		X	PCM	X			X				X		X
	X		PCM	PCF		X	X			X		X	X	X
X	PCF		X	PCM	X See Note 2.			X See Note 5.			X			X

PCF - Safety function fails post containment failure.

PCM - Safety function fails post core melt.

Notes

1) Prevents containment overpressure from gas generation.
2) CHR system capacity must equal 20-30% of operating power.
3) Prevents containment overpressure from hydrogen burning.
4) May prevent containment failure if device reduces noncondensible gas generation.
5) Vent must be of high flow design for ATWS.
6) Affects probability of containment overpressure from hydrogen burning or gas generation.
7) Prevents containment failure from steam explosions.
8) These include increasing the reliability of emergency AC power systems, safety/relief valve reclosure, and Automatic Depressurization System actuation.

After the initial safety approach characterization was performed, the overall effect of the candidate safety approaches on each plant-specific accident sequence was quantified. This was done by estimating the safety approach unavailability and then calculating the reduction in accident sequence frequency and contribution to risk. The analysis included the effects on dominant and non-dominant accident sequences to ensure that the residual risk after risk reduction was adequately represented. Accident sequence cut sets were also reviewed, when possible, to ensure that the overall effects of a safety option on a sequence were correctly calculated.

Since the RSSMAP PRAs did not include any calculations of consequences, CRAC code runs were made to estimate the relative consequences expected from each RSS release category. These consequence measures have been used to calculate the original risk and risk reduction for each plant. The reduction in population dose in man-rems per reactor year is presented in the result tables of this report.

Once the safety option effects on individual sequences were analyzed, the overall effects on the core melt frequency and risk were evaluated by accumulating the results for all of the accident sequences. Reduction factors were then calculated by dividing the core melt and risk measures before the implementation of the safety approaches by those calculated after the implementation of the safety approaches.

RESULTS

Table III gives results for the six RSS and RSSMAP reactors. Presented for each candidate safety approach is a potential reduction factor for the total core melt frequency and population dose. All possible safety options and combinations of options are not shown. It is the intent of the authors to present typical and interesting results for each plant which perhaps show trends on how the safety options function. The numbers in parentheses after the safety approach description represents the unavailability of the add-on system or the factor reduction in unavailability of an existing system attributable to some improvement.

Sequoyah

The results for Sequoyah show that no single option alone provides large (greater than an order of magnitude) core melt or risk reduction. A hydrogen control device was found to have the largest single effect on population dose with a potential reduction factor of 2.5. Installing an automatic primary system depressurization capability was found to affect the core melt frequency the most as a single option.

By combining options it can be seen that overall effects start to increase. Correcting the drain common-mode failure of the recirculation systems and the interfacing system LOCA provides the starting point for large risk reduction. Subsequent addition of another high-pressure injection and recirculation train and increasing the auxiliary feedwater system reliability may reduce both core melt and risk by factors of 50. Adding a hydrogen control system in addition to the other fixes was found to reduce the population dose by another factor of five.

Containment venting systems were found to be minimally beneficial for Sequoyah in absence of other improvements. This is due to the calculated importance of hydrogen burning containment failure modes and the fact that for most of the dominant sequences, containment cooling systems are operating. Comparing approaches 12 and 14 for Sequoyah in Table III, however, one can see that given certain other fixes, adding a filtered vent reduces the population dose by a factor of 3.

Table III.

Phase I Results

	Candidate Safety Approach Description	Factor Reduction in Core Melt Frequency	Factor Reduction in Population Dose
	Sequoyah Results		
1)	Add hydrogen control system (.01)	1.0	2.5
2)	Increase containment design pressure by 100%	1.0	2.2
3)	Remove drain common-mode failure	1.2	1.4
4)	Add automatic depressurization system (.01)	1.4	1.2
5)	Reduce interfacing system LOCA (.001)	1.1	1.2
6)	Improve auxiliary feedwater system (.1)	1.1	1.1
7)	Credit for feed and bleed	1.1	1.1
8)	Add filtered containment vent (.01)	1.0	1.1
9)	Add high pressure injection train (.01)	1.0	1.0
10)	Add core retention device (.001)	1.0	1.0
11)	Combination of #5, 3, 9, 1, and 6	56	330
12)	Combination of #5, 3, 8, and 1	1.4	93
13)	Combination of #5, 3, 9, and 6	56	58
14)	Combination of #5, 3 and 1	1.3	27
15)	Combination of #5, 3, and 9	8.3	7.7
16)	Combination of #5, 3, and 6	1.6	2.3
17)	Combination of #5 and 3	1.3	1.8
	Grand Gulf Results		
1)	Add high volume unfiltered vent (.01)	13	43
2)	Add containment heat removal train (.01)	4.5	5.5
3)	Add low volume unfiltered vent (.01)	4.4	5.5
4)	Increase containment design pressure by 100%	2.0	2.2
5)	Improve AC power systems (.01)	1.4	1.3
6)	Improve safety/relief valves (.01)	1.2	1.2
7)	Improve reactor protection system (.1)	1.2	1.2
8)	Improve emergency core cooling systems (.1)	1.1	1.0
9)	Add hydrogen control system (.01)	1.0	1.0
10)	Add core retention device (.001)	1.0	1.0
11)	Improve auto-depressurization system (.01)	1.0	1.0
12)	Combination of #1, 7, and 9	13	92
13)	Combination of #1 and 8	45	88
14)	Combination of #1 and 9	13	81
15)	Combination of #7, 8, and 2	34	39
16)	Combination of #3, 7, and 8	29	39
17)	Combination of #3, 7, and 9	11	37
18)	Combination of #2 and 7	11	27
19)	Combination of #3 and 7	11	26
20)	Combination of #2 and 8	6.0	5.9
21)	Combination of #5, 6, 7, and 11	2.1	2.0

Table III Continued

Calvert Cliffs Results

1)	Add HPI train with feed and bleed capability (.01)	24	23
2)	Add automatic depressurization (.01)	23	23
3)	Improve auxiliary feedwater system (.1)	6.6	6.1
4)	Add hydrogen control system (.01)	1.0	2.3
5)	Improve AC power systems (.01)	1.2	1.3
6)	Add containment spray train with CHR (.01)	1.0	1.1
7)	Add filtered containment vent (.01)	1.0	1.0
8)	Add core retention device (.001)	1.0	1.0
9)	Combination of #1, 3, and 6	230	250
10)	Combination of #2, 3, and 6	210	240
11)	Combination of #1, 3, and 7	220	230
12)	Combination of #1, 3, and 5	170	130
13)	Combination of #1, 3, and 4	130	120
14)	Combination of #1 and 3	130	91
15)	Combination of #3 and 4	6.6	14

Surry Results

1)	Add hydrogen control system (.01)	1.0	2.5
2)	Add high pressure injection train (.01)	2.1	1.6
3)	Add auxiliary feedwater train (.01)	1.3	1.4
4)	Reduce interfacing system LOCA (.001)	1.1	1.2
5)	Add filtered containment vent (.01)	1.1	1.2
6)	Credit for feed and bleed	1.2	1.2
7)	Add unfiltered containment vent (.01)	1.1	1.1
8)	Add containment spray train with CHR (.01)	1.1	1.1
9)	Improve AC power systems (.1)	1.1	1.1
10)	Add low pressure injection train (.01)	1.1	1.1
11)	Remove recirculation actuation common mode	1.1	1.1
12)	Combination of #1, 4, 8, 9, and 11	1.3	42
13)	Combination of #1, 2, 4, 9, and 11	4.1	40
14)	Combination of #1, 4, 9, and 11	1.3	30
15)	Combination of #1, 2, 3, 4, and 9	7.3	15
16)	Combination of #1, 2, 3, and 4	7.2	14
17)	Combination of #2, 3, 4, and 8	12	12
18)	Combination of #2, 3, 4, and 11	11	11
19)	Combination of #1, 4, and 8	1.2	7.4
20)	Combination of #4, 6, 9, and 11	1.6	2.0

Peach Bottom Results

1)	Add high volume unfiltered wetwell vent (.01)	3.4	29
2)	Add high volume unfiltered drywell vent (.01)	3.4	3.4
3)	Add low volume filtered vent (.01)	1.4	2.3
4)	Improve emergency core cooling systems (.01)	1.6	1.6
5)	Improve reactor protection system (.1)	1.6	1.6
6)	Add containment heat removal system (.01)	1.4	1.4
7)	Add core retention device (.01)	1.0	1.4
8)	Improve auto-depressurization system (.1)	1.2	1.2
9)	Improve high pressure service water system (.1)	1.2	1.2
10)	Improve emergency service water system (.01)	1.0	1.0
11)	Improve AC power systems (.01)	1.0	1.0
12)	Combination of #1, 4, and 5	30	180
13)	Combination of #1 and 4	27	110
14)	Combination of #1, 5, and 6	35	36

Table III Continued

15)	Combination of #1 and 10	4.0	33
16)	Combination of #1 and 5	3.5	32
17)	Combination of #3, 5, and 10	3.5	15
18)	Combination of #4, 5, and 6	14	14
19)	Combination of #4 and 5	3.7	3.7
20)	Combination of #5, 8, 10, and 11	2.4	2.4
	Oconee Results		
1)	Add hydrogen control system (.001)	1.0	6.3
2)	Improve emergency core cooling system (.1)	7.0	4.3
3)	Improve safety/relief valves (.1)	1.3	1.3
4)	Improve auxiliary feedwater system (.03-0.1)	1.3	1.3
5)	Reduce interfacing system LOCA (.001)	1.1	1.2
6)	Improve reactor protection system (.1)	1.1	1.1
7)	Improve AC power systems (.01)	1.0	1.0
8)	Add filtered containment vent (.01)	1.0	1.0
9)	Add core retention device (.01)	1.0	1.0
10)	Combination of #1, 2, and 5	11	660
11)	Combination of #1, 5, and 9	1.1	120
12)	Combination of #1, 3, 5, and 7	1.5	98
13)	Combination of #1, 4, and 5	1.4	80
14)	Combination of #1 and 5	1.1	72
15)	Combination of #2, 4, and 5	14	15
16)	Combination of #2 and 5	11	12
17)	Combination of #1 and 2	7.0	6.8
18)	Combination of #3, 5, 6, and 7	1.7	2.0

Grand Gulf

The results for Grand Gulf show that the addition of a high-volume, unfiltered primary containment vent may reduce both the core melt frequency and population dose by more than a factor of 10. This is because the high-volume vent (approximately 400,000 cfm) not only reduces the frequency of loss of residual heat removal sequences leading to core melt but also reduces the frequency of core melts caused by anticipated transients without scram (ATWS). No other single option affects both of these dominant accident types. An unfiltered vent is sufficient at Grand Gulf because of the effectiveness of the suppression pool as a fission product scrubber.

A variety of other single options was found to provide some core melt and risk reduction potential. These range from adding another suppression pool cooling train to provide heat removal or increasing the reactor protection system (RPS) reliability. Several systems, however, were calculated to provide no measurable effects by themselves.

Integrating several options together was found to have large effects for Grand Gulf. The best approaches included combinations of adding containment vents, adding containment heat removal trains and increasing the reliabilities of the RPS and/or emergency core cooling system (ECCS). Potentially large core melt frequency and risk reduction may be achieved by integrating these systems into Grand Gulf.

Calvert Cliffs

Sequences involving loss of all feedwater were found to be very important for Calvert Cliffs in RSSMAP. This was primarily due to the high unavailability calculated for the AFWS and the fact that no feed and bleed capability was assessed for the plant. Consequently, increasing the AFWS reliability or adding a high pressure injection line capable of a feed and bleed mode of decay heat removal were found to be effective in reducing the core melt frequency and risk. Incorporating both of these two fixes at Calvert Cliffs was calculated to reduce the core melt frequency and risk by almost two orders of magnitude. It should be noted that Baltimore Gas & Electric Company is currently upgrading the AFWS at Calvert Cliffs. Additional reduction was found to be provided by adding a containment spray train with heat removal capability, adding a filtered containment vent, or improving the emergency AC power systems. The effects of a hydrogen control system were found to be limited at Calvert Cliffs due to the calculated importance of containment failures due to ex-vessel steam spikes.

Surry

The results for Surry show that adding a hydrogen control system provides the largest reduction in population dose of any single safety option. From a reanalysis of the Surry sequences using the MARCH code, containment failure due to hydrogen burning was determined to be more important than originally believed in the RSS and therefore the importance of hydrogen control systems as a potential fix has increased. The largest reduction in core melt frequency from a single option was found to result from adding an additional high pressure injection and recirculation train.

A number of specific plant fixes identified at Surry were found to be needed before large risk reduction was possible. These fixes include reducing the probability of the interfacing system LOCA, removing a common-mode failure of the recirculation systems, and improving the AC power systems. These fixes correct

particular vulnerabilities which, left uncorrected, limit the overall risk reduction that is possible.

The best options to be combined with these specific fixes were a hydrogen control system, an add-on high pressure injection and recirculation train, and an improved auxiliary feedwater system. Similar to the results for Sequoyah, containment venting systems had minimal effects on the Surry accident sequences until after hydrogen control and specific fixes have been implemented. This was due to the importance of hydrogen burning containment failures and the fact that for most of the dominant sequences, containment heat removal systems have succeeded.

Peach Bottom

The results obtained for Peach Bottom were similar to those for Grand Gulf. High volume, unfiltered containment venting of the wetwell was found to be the best single option in terms of both core melt and risk reduction. The effects of venting at Peach Bottom were not found, however, to be as good as those at Grand Gulf due to a higher importance of loss of injection accidents. Loss of injection accidents resulted in core melting in an initially intact containment which limits the risk reduction potential of containment venting. Also, the value of additional containment heat removal systems is diminished due to more overpressures occurring from noncondensable gas generation.

The best approaches for Peach Bottom were those which included combinations of high volume containment venting, improving the ECCS or RPS, adding an additional containment heat removal train, and correcting a common-mode failure in the emergency service water system.

Oconee

The results for Oconee indicate that adding a hydrogen control system or increasing the emergency core cooling system reliability may reduce risk more than any other single approach. This is due to the fact that most of the dominant accident sequences at Oconee involve loss of core cooling and containment failure from hydrogen burning. Improving the ECCS was also found to have the largest effect on the core melt frequency. Since containment venting did not prevent core melting for any dominant sequence and the sequences with overpressure containment failure affected by vents were already of low consequence, containment venting was not found to be beneficial for Oconee.

Other single approaches were found to have minimal effects on core melt and risk by themselves. One of these, reducing the interfacing system LOCA frequency, was important in combination with other fixes. It was found that not correcting the interfacing system LOCA limits the core melt and risk reduction at Oconee to factors of 21 and 7, respectively, regardless of the number of other fixes.

Several combinations of options were found to result in factors of 10 or more reduction in core melt frequency and population dose at Oconee. The best of these combinations included reducing the interfacing system LOCA frequency in conjunction with adding a hydrogen control system or increasing the ECCS reliability.

SUMMARY

It should be noted that the results presented do not include feasibility or cost/benefit considerations. Another paper at this conference addresses these issues[3].

A number of insights and comments can be made based on the Phase I results. It has been found that, for the plants studied, correcting specific accident sequence faults or vulnerabilities (e.g., certain common modes, the interfacing system LOCA, etc.) reduces the core melt frequency and population dose by factors of approximately two. Not correcting these specific vulnerabilities generally limited the overall core melt and risk reduction regardless of the number of improvements added.

For the PWR cases, hydrogen control systems by themselves were found to reduce population doses by factors of two or more. Combining hydrogen control systems with the specific accident fixes mentioned above resulted in large population dose reductions (factors of 20 or more).

Containment venting systems appear to be very effective for the two BWRs in reducing both the core melt frequency and risk. Venting for the PWRs seems of questionable benefit based on core melt and risk reduction potential. This is due to the calculated importance of hydrogen burning and other containment failure modes and the fact that for many of the dominant PWR accident sequences, containment cooling systems are operating.

Some safety options (e.g., core retention devices and missile shields) were found to be effective only after large initial risk reduction and therefore may be of minimal benefit.

Finally, it was found that the results were not easily generalized based on containment type because the overall effects were often driven by plant specific system differences.

REFERENCES

1. Reactor Safety Study - An Assessment of Accident Risks in US Commercial Nuclear Power Plants, US Nuclear Regulatory Commission, WASH-1400, NUREG-75/014, October 1975.

2. Reactor Safety Study Methodology Applications Program, NUREG/CR-1659, SAND80-1897, Sandia National Laboratories, 1981, 1982.

3. A. S. Benjamin, et al., "Value-Impact Analysis of Severe Accident Prevention and Mitigation Systems," Proceedings of the International Meeting on Thermal Nuclear Reactor Safety, American Nuclear Society, Chicago, Illinois, 1982.

4. G. J. Kolb, "Systemic Event Tree Methodology Employed in the Interim Reliability Evaluation Program", Proceedings of the International Meeting on Probabilistic Risk Assessment, American Nuclear Society, Port Chester, New York, 1981.

SOME PERSPECTIVES ON RISK PRESENTATION FROM THE GERMAN RISK STUDY

J. Ehrhardt, A. Bayer

Kernforschungszentrum Karlsruhe, F.R. Germany
Postfach 3640, D-7500 Karlsruhe

ABSTRACT

Results of risk assessments for nuclear power plants and other facilities of the nuclear fuel cycle are so far nearly exclusively presented in the form of frequency distributions and annual expectation values of the number of fatalities. These conventional presentations do not sufficiently reflect the entire nature of risk. A more complete evaluation of risk assessment results is recommended to improve the interpretation of the results and make them consequently more understandable. The results of analysing calculations are shown which provide more insight into the nature of the collective risk and the number of early and late fatalities to be expected after accidental releases of radioactivity. Furthermore the dimension of damage "fatality" is converted into "loss of life expectancy", which is more relevant on a societal level. To present these improvements the German Risk Study (Phase A) has been taken as a basis.

INTRODUCTION

The discussion which followed the publication of the "German Risk Study" - Phase A (GRS) /1,2/ showed that the results of the risk assessments were often interpreted too simplistically or sometimes even misinterpreted. This resulted in part from the fact that the graphical and numerical presentations commonly used in risk studies may cause difficulties in interpretation. Additional presentations which further indicate the nature of risk may provide more insight and help to avoid interpretation problems.

The following topics often arose in the discussions of the results of the German Risk Study:
- number of late fatalities arising from different dose levels
- sensitivity of the number of late fatalities to the dose-risk relationship
- probability of early and late fatalities after accidental releases
- temporal distribution of early and late fatalities
- expected loss of life time as a dimension to present damage
- presentation of total damage (early plus late fatalities) on a common basis.

These and other related topics will be treated in more detail during Phase B of the German Risk Study. However, an attempt has been made to develop preliminary results on the basis of the models and analyses of phase A of this study. These results are indicated in the following presentation.

NUMBER OF LATE FATALITIES ARISING FROM DIFFERENT DOSE LEVELS

According to the dose probability of mortality relationships, early fatalities are calculated in case of relatively high doses (threshold dose: 100 rad within a few days). In contrast to this, late fatalities are predicted at all dose values due to the thoroughly linear dose-risk relationship of the "German Risk Study". In most cases, the overwhelming part of late fatalities is calculated from very low doses applied to a large population group living at far distances from the site. For example, about 23% of the collective risk is caused by late fatalities calculated beyond 540 km from the site /3/.

To demonstrate this in the proper way, it is important to recognize the relationship which may exist between radiation dose levels and number of late fatalities associated with these levels. The nature of such relationships may influence the manner in which individuals perceive risk.

For the following analysis, the dose limits D_o for reactor incidents established in the "German Radiation Protection Law" are used as a criteria to define a high dose and a low dose region. This law limits the dose commitment after a reactor incident to 5 rem for whole body and bone marrow, 15 rem for lung and thyroid and 30 rem for bone surface.

The reevaluation of the risk assessment results calculated with the computer code UFOMOD /4/ showed that all accidental releases cause late fatalities estimated to a large scale from individual organ doses below the above-mentioned limits D_o. The percentages are dependent on the release category in the range of 62% and 100% (see Tab. I). Presentations intended for the future (Phase B) will show probability distributions of radiation doses and the number of early and late fatalities caused by different dose levels.

SENSITIVITY OF THE NUMBER OF LATE FATALITIES ON THE DOSE RISK RELATIONSHIP

As mentioned above, the computation of late fatalities was performed on the basis of an uninterrupted linear dose risk relationship. This differs from the relationship used in the American "Reactor Safety Study" (WASH 1400), where attenuation factors were applied in the range of low doses and low dose rates to simulate a linear-quadratic relationship. Both curves are shown in Fig. 1.

To illustrate the influence of this alternative dose-risk relationship on the risk assessments, supplementary calculations were performed with a modified version of UFOMOD. This version used the piecewise linear dose-risk relationship of Fig. 1 neglecting the dose rate dependency. The results, presented in Tab. I too, show that, dependent on the release category, the collective risk is reduced by a factor between 2,5 and 5,0. For the total risk, this factor is about 4. These numbers reflect once more that late fatalities are calculated to a high percentage from low doses ($\leq$10 rem).

PROBABILITY OF EARLY AND LATE FATALITIES AFTER ACCIDENTAL RELEASES

Early fatalities are predicted only for accidental releases belonging to categories FK1 to FK4 (core melt with steam explosion or leak in containment) in the

presence of a few environmental conditions. In contrast to this, late fatalities can occur at all dose levels due to the linear dose-risk relationship and with this at all releases. Although this fact may influence the manner in which individuals perceive risk, it is insufficiently emphasized in the German as well as in the American Study.

To improve this situation, it is proposed to add to the presentation of results figures which show the conditional probability that early and late fatalities occur after accidental releases at all. Fig. 2 gives the corresponding results of the German Risk Study. Only about 1% to 5% (except FK2 with 24.5%) of the environmental conditions lead to early fatalities. The different percentages can be explained by the category-dependent release data in connection with the protective actions aiming at reducing or avoiding early fatalities.

TEMPORAL DISTRIBUTION OF FATALITIES

Early fatalities occur within several weeks or months after exposure; in contrast, late fatalities (leukemia and cancers) are evidenced years or decades later. Moreover, long-half-life radionuclides released at nuclear accidents cause a chronic exposure which also influences the time dependent incidence of late fatalities.

In this connection the following two questions arise: first, how is the incidence of late fatalities distributed within time after accident, and second, how far lie the incidence rates originating from reactor accidents above the natural incidence rate? These questions cannot yet answered completely. But to meet this aspect to a certain extent with the present version of the computer code UFOMOD, risk assessment calculations were performed separately for the population living at the time of the accident (LG) and the generations born afterwards (FG) /3/. The results for the mean collective damage $\overline{KS}$ are shown in Tab. I. On the average about 89% of the late fatalities occur in the population living at the time of the accident and about 11% in the generations born afterwards. On an absolute time scale the first percentage can be assigned approximately to the first forty years after the accident and the second percentage to the time afterwards. Applying the dose-risk relationship of the "Reactor Safety Study" (Fig. 1), the numbers are similar (about 9% late fatalities in the following generations).

EXPECTED LOSS OF LIFETIME AS A DIMENSION TO PRESENT DAMAGE

Risk assessments which present only the number of fatalities give an incomplete picture of the consequences. This is because they do not represent the loss of life expectancy, which is more relevant on a societal level. This loss of lifetime differs significantly between early and late fatalities.

Each individual has a life expectancy l at birth, which denotes the length of life that this individual will realize. Although it is not possible to know l for an individual, it is possible to derive a probability density function of life expectancy p(l) from population statistics. The set of individuals who have the life expectancy l and the age A at the time of the accident, and eventually die due to radiation exposure resulting from the accident will suffer an expected reduction in length of life $l_v(A,l)$. A derivation of $l_v(A,l)$ is given in /5/.

From $l_v(A,l)$ the "age at time of accident" - dependent individual mean loss of life time per fatality LVT(A) can be calculated in the following way:

$$LVT(A) = \int_A^\infty l_v(A,l)\ p(l)\ dl \ / \ \int_A^\infty p(l)\ dl$$

The probability density function of age q(A) can also be derived from the statistical description of a population. Then, with use of this function, the mean loss of life time per fatality $\overline{LVT}$ can be calculated:

$$\overline{LVT} = \int_0^\infty LVT(A) \cdot q(A)\ dA$$

Early fatalities occur within several weeks or months after the accident. Neglecting this small time span, the reduction in life time $l_v(A,l)$ for an individual is

$$l_v(A,l) = l-A$$

A value of $\overline{LVT}$ = 37,8 a has been derived for the German population /5/.

For late fatalities, loss of life expectancy of individuals living during the accident (LG) or born afterwards (FG) is dependent on the length of irradiation and the duration of latent and manifestation periods. For the German population, the $\overline{LVT}$ are dependent on the type of cancer in the range of 9 a to 15 a for persons living during the accident (LG) and up to 30 a for individuals born afterwards (FG) /5/.

Once the mean loss of life expectancy per fatality $\overline{LVT}$ is known, the total loss of life expectancy GLV is given by GLV = KS·$\overline{LVT}$, where KS denotes the number of fatalities. The GLV was calculated for early and late fatalities and is presented in the form of complementary cumulative frequency distributions (CCFD) in Fig. 3a,b.

The expected loss of life expectancy to an idividual LV is given by /5/

$$LV = \frac{GLV}{P_o} \cdot f \cdot L_o,$$

where L_o denotes the mean life expectancy at birth (L_o = 71,3 a) and P_o is the population collective being considered for the calculation of the collective damage KS after accidents with frequency f. Tab. II shows the results for early and late fatalities within a distance of 540 km from the site ($P_o = 2{,}07 \cdot 10^8$ persons).

The individual and collective loss of life expectancy caused by natural and societal sources of risk are put together from statistical data of the US in /6/; corresponding results for selected diseases within the F.R. of Germany are given in /7/ and reproduced in Tab. III.

PRESENTATION OF THE TOTAL DAMAGE

In both the German Risk Study and in the American Reactor Safety Study, the numbers of early and late fatalities are presented separately. This is necessary as the mean loss of life time for these fatalities differs by a factor of approx. four; hence, the direct addition of fatalities would not be appropriate.

Typically, the calculated numbers of early fatalities and late fatalities of each individual accident sequence are separated and incorporated into different CCFD's. A subsequent combination of these CCFD's is inappropriate and leads to a misrepresentation of risk (e.g., the addition of the maximum number of early fatalities and the maximum number of late fatalities which originate from two different weather-population situations) /2/.

A possible way to present the total damage of accidents in form of CCFD's is to use the loss of lifetime. In such a presentation, the total loss of lifetime is calculated for each accident sequence and used in the construction of the final CCFD. A CCFD of this type is shown in Fig. 4. The abscissa represents the total loss of life time GLV per event and the ordinate represents the frequency of events which have this total loss of lifetime or a higher loss as a consequence.

Since this new dimension is not yet commonly used, a second auxilliary abscissa has been added for better interpretation, which is derived by dividing the total loss of lifetime on the upper abscissa by the mean individual loss of life time for early fatalities ($\overline{LVT}$ = 37,8 a). This lower abscissa shows total loss of lifetime converted to number of "effective early fatalities". This calculation normalizes the total loss of lifetime for early and late fatalities to an "equivalent" number of early fatalities.

FINAL REMARKS

The above mentioned analysing recalculations have been performed with modified versions of the accident consequence model of the German Risk Study (Phase A). In the intervening period new scientific foundings have accumulated. This fact has made it necessary to generate the new version UFOMOD/B3 of the computer code. It contains new values of the deposition velocity and the washout parameter and completely new data within the dosimetry submodel. The recalculated risk assessment results will be published in /8/. Further improvements concerning accident consequence modelling, data-bases and risk presentations will be performed in Phase B of the study.

REFERENCES

/1/ Der Bundesminister for Forschung und Technologie (Ed.), "Deutsche Risikostudie Kernkraftwerke", TÜV Rheinland, Köln, Main Report 1979, Appendix VIII, 1981. Translation into English: "German Risk Study", Report EPRI-NP-1804-SR (1981)

/2/ BAYER, A., et al.: "The German Risk Study: Accident Consequence Model and Results of the Study". Nuclear Technology, in press

/3/ EHRHARDT, J.: "Analysis of the Stochastic Somatic Fatalities Evaluated in the German Nuclear Power Plant Risk Study (in German). Report KfK-3218, October 1981

/4/ SCHÜCKLER, M., VOGT, S.: "UFOMOD - Program to Calculate the Radiological Consequences of Reactor Accidents Within Risk Studies (in German)". Report KfK-3092, January 1981

/5/ EHRHARDT, J.: "Determination of Reduction in Life Expectancy from Stochastic Somatic Fatalities after Accidental Radiation Exposure (in German)". Report KfK-3181, June 1981

/6/ COHEN, B.L., LEE, I-Sing: "A Catalog of Risks". Health Physics, Vol. 36 (June) 1979, pp. 707-722

/7/ GEISSLER, U.: "Verlust an Lebensjahren: ein neuer Gesundheitsindikator". Medizin, Mensch, Gesellschaft, 5, S. 111-118 (1980)

/8/ EHRHARDT, J., VOGT, S.: "Unfallfolgenrechnungen und Risikoabschätzungen für Druckwasserreaktoren mit dem Rechenprogramm UFOMOD/B3. Report KfK-3373, in preparation.

Tab. I Characteristic Quantities of the Late Fatalities Corresponding to the 25 Reactor Units of the German Risk Study

RELEASE CATEGORY	DESCRIPTION	RELEASE FREQUENCY $/a^{-1}/$	MEAN COLLECTIVE DAMAGE $\overline{KS}$ LIVING GENERATIONS LG	FOLLOWING GENERATIONS FG	ALL GENERATIONS AG = LG + FG	PERCENTAGE OF LATE FATALITIES IN THE FG	LATE FATALITIES FROM DOSES $<D_o$ [1] AG	REDUCTION FACTOR [2] AG
FK1	Core meltdown followed by steam explosion	$2 \cdot 10^{-6}$	39065	4361	43426	10,0%	62,0%	2,60
FK2	Core meltdown, large leak in containment (300-mm o.d.)	$6 \cdot 10^{-7}$	15949	2595	18544	14,0%	66,8%	3,24
FK3	Core meltdown, medium leak in containment (80-mm o.d.)	$6 \cdot 10^{-7}$	3674	598	4272	14,0%	84,3%	3,95
FK4	Core meltdown, small leak in containment (25-mm o.d.)	$3 \cdot 10^{-6}$	1068	120	1188	10,1%	94,8%	4,47
FK5	Core meltdown, overpressure failure, failed filter system	$2 \cdot 10^{-5}$	550	39	589	6,7%	98,4%	4,75
FK6	Core meltdown, overpressure failure	$7 \cdot 10^{-5}$	397	19	416	4,5%	99,1%	4,76
FK7	Design basis loss-of-coolant accident, large leak in the containment	$1 \cdot 10^{-4}$	1892	267	2159	12,4%	95,8%	4,77
FK8	Design basis loss-of-coolant accident	$1 \cdot 10^{-3}$	<<1	<<1	<<1	5,9%	-	5,00
all FK		-	-	-	-	11,0%	-	3,92

[1] Dose Limits of the "German Radiation Protection Law"

[2] Ratio of the number of late fatalities calculated in the German Risk Study to those estimated with a nonlinear dose-risk relationship similar to WASH-1400

Tab. II Mean Loss of Life Time per Fatality $\overline{LVT}$ and Mean Individual Loss of Life Expectancy $\overline{LV}$ within a Distance of 540 km from the Site, Corresponding to 25 Reactor Units

RELEASE CATEGORY	EARLY FATALITIES		LATE FATALITIES				
			LIVING GENERATIONS LG		FOLLOWING GENERATIONS FG		ALL GENERATIONS AG
	$\overline{LVT}$ /a/	$\overline{LV}$ /s/	$\overline{LVT}$ /a/	$\overline{LV}$ /s/	$\overline{LVT}$ /a/	$\overline{LV}$ /s/	$\overline{LV}$ /s/
FK1	37,8	0,164	10,14	108,1	22,77	29,2	137,3
FK2	37,8	0,041	10,25	16,5	22,94	7,2	23,7
FK3	37,8	0,001	10,15	4,6	22,79	1,9	6,5
FK4	37,8	0,002	10,08	7,6	22,36	2,0	9,6
FK5	37,8	0	10,52	24,9	22,51	4,2	29,1
FK6	37,8	0	10,86	61,2	22,94	6,8	68,0
FK7	37,8	0	9,82	445,7	22,74	147,1	592,8
all FK	37,8	0,208	10,03	673,0	22,75	199,0	872,0

Tab. III Loss of Life Expectancy due to Various Causes

selected diseases	mean individual loss of life expectancy $\overline{LV}$ /s/
neoplasms	$7{,}9 \cdot 10^{7}$
incl.: n. of respiratory organs	$1{,}2 \cdot 10^{7}$
diseases of circulatory system	$1{,}2 \cdot 10^{8}$
incl.: heart diseases	$5{,}2 \cdot 10^{7}$
diseases of respiratory organs	$2{,}1 \cdot 10^{7}$
incl.: pneumonia	$7{,}3 \cdot 10^{6}$
diseases of digestive organs	$2{,}3 \cdot 10^{7}$
incl.: cirrhosis of liver	$1{,}1 \cdot 10^{7}$
accidents, poisoning, violence	$4{,}7 \cdot 10^{7}$
incl.: motor vehicle accidents	$1{,}8 \cdot 10^{7}$
incl.: suicide	$1{,}2 \cdot 10^{7}$
reactor accidents (German Risk Study)	
early fatalities	$2{,}1 \cdot 10^{-1}$
late fatalities	$8{,}7 \cdot 10^{2}$

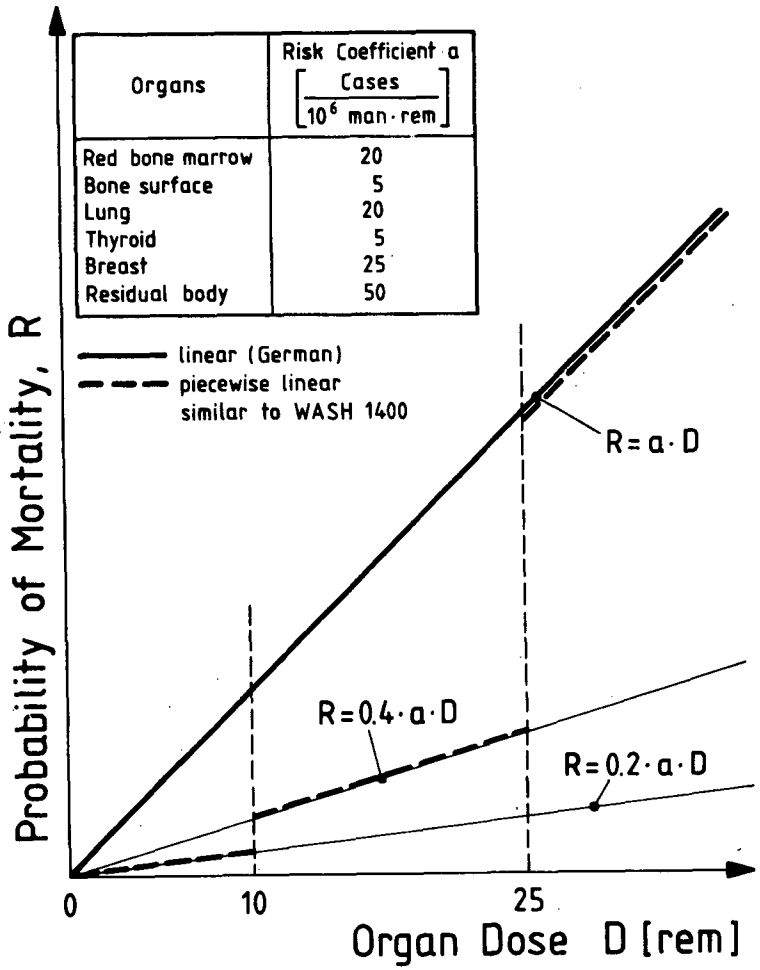


Fig. 1 Dose-Risk Relationships

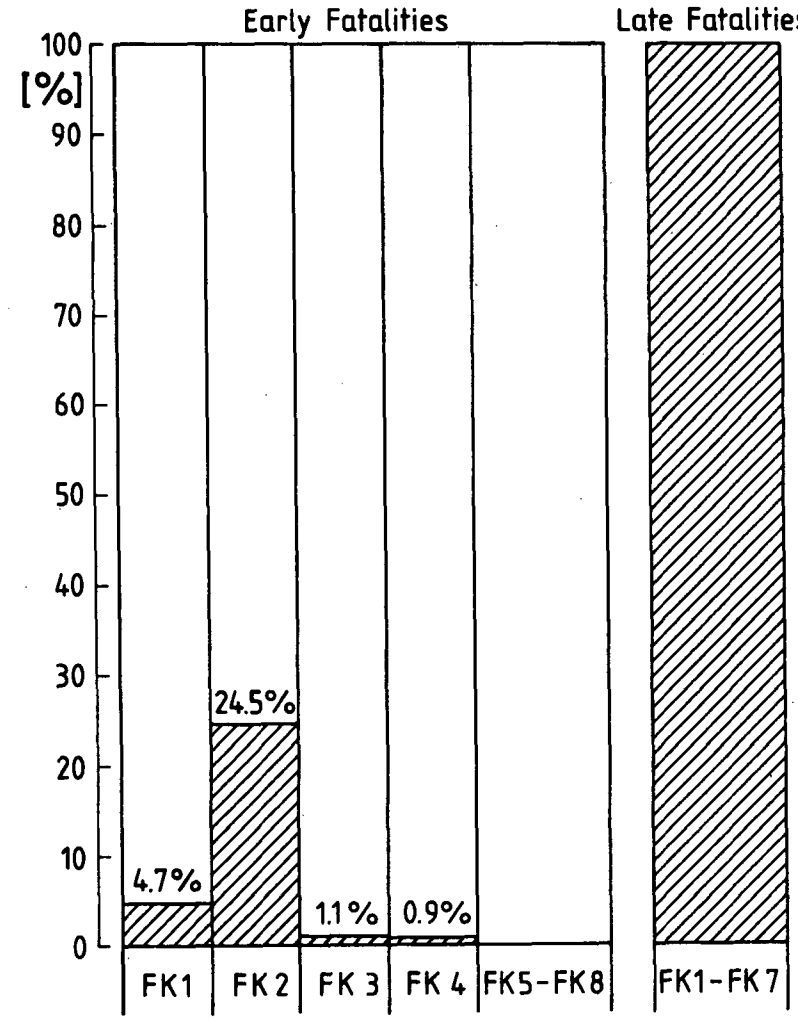


Fig. 2 Conditional Probability of Early and Late Fatalities After Accidental Releases

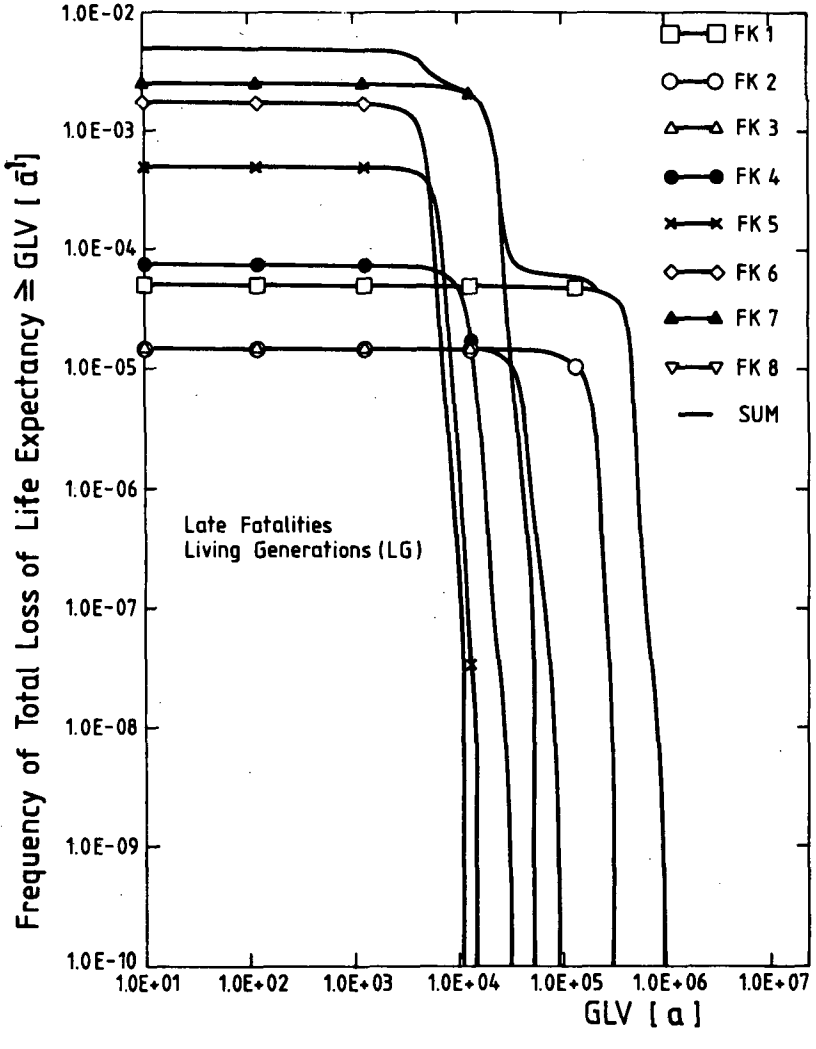


Fig. 3a CCFD of Total Loss of Life Expectancy GLV for Late Fatalities in the Living Generations, Corresponding to 25 Reactor Units

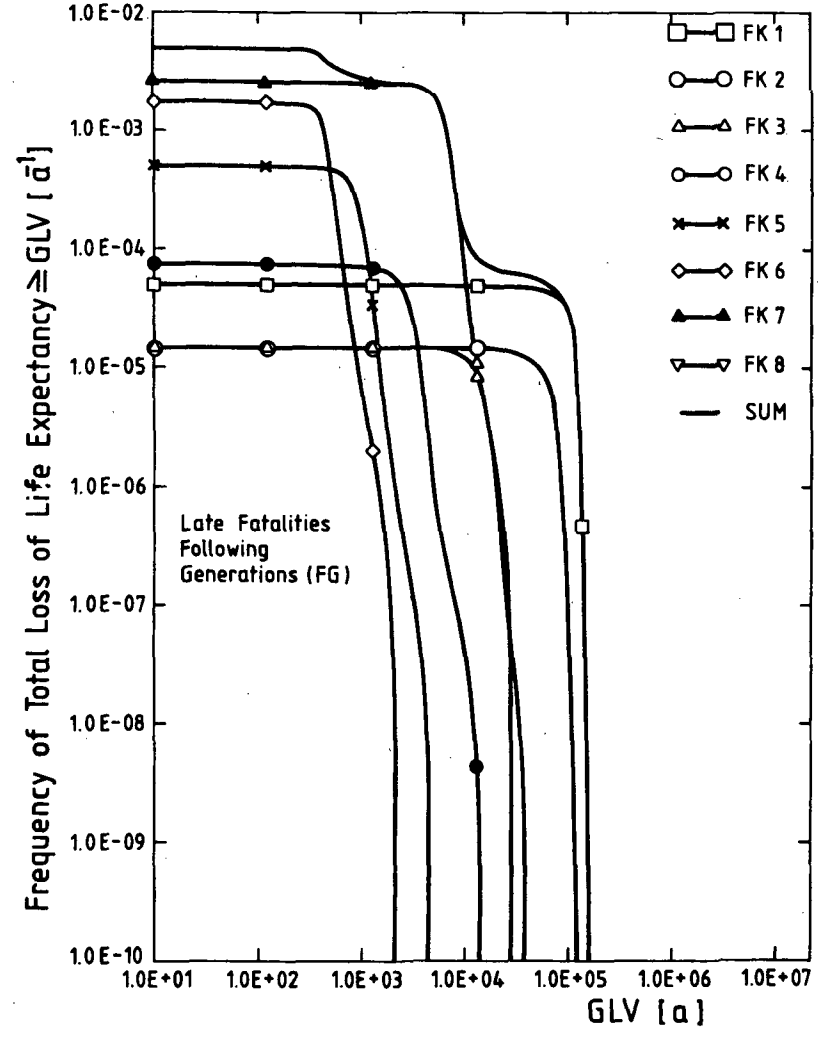


Fig. 3b CCFD of Total Loss of Life Expectancy GLV for Late Fatalities in the Following Generations, Corresponding to 25 Reactor Units

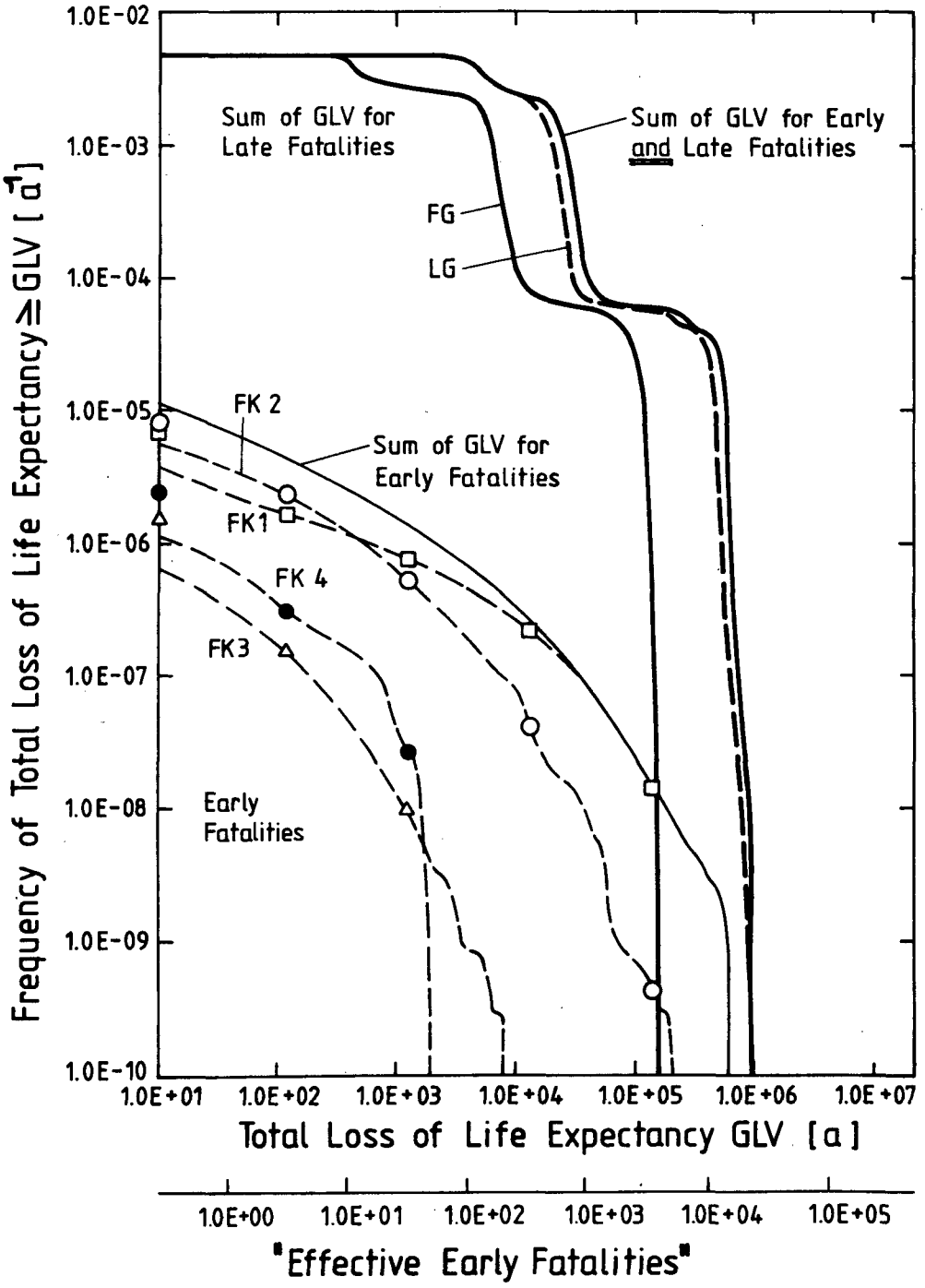


Fig. 4 CCFD of Total Loss of Life Expectancy From Early and Late Fatalities, Corresponding to 25 Reactor Units

NRC FORM 335 (11-81) U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

1. REPORT NUMBER *(Assigned by DDC)*
NUREG/CP-0027 Volume 1

4. TITLE AND SUBTITLE *(Add Volume No., if appropriate)*
PROCEEDINGS OF THE INTERNATIONAL MEETING ON THERMAL NUCLEAR REACTOR SAFETY, Held at Chicago, Illinois, August 29—September 2, 1982

2. *(Leave blank)*

3. RECIPIENT'S ACCESSION NO.

7. AUTHOR(S)

5. DATE REPORT COMPLETED
MONTH | YEAR

9. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS *(Include Zip Code)*
Chicago Section of the American Nuclear Society
c/o Elmer E. Lewis
Dept. of Mechanical and Nuclear Engineering
Northwestern University
Evanston, Illinois 60201

DATE REPORT ISSUED
MONTH: February | YEAR: 1983

6. *(Leave blank)*

8. *(Leave blank)*

12. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS *(Include Zip Code)*
American Nuclear Society, European Nuclear Society, Canadian Nuclear Society, Japan Atomic Energy Society; in cooperation with U. S. Nuclear Regulatory Commission, International Atomic Energy Agency

10. PROJECT/TASK/WORK UNIT NO.

11. FIN NO.

13. TYPE OF REPORT
Conference Proceedings

PERIOD COVERED *(Inclusive dates)*

15. SUPPLEMENTARY NOTES

14. *(Leave blank)*

16. ABSTRACT *(200 words or less)*

The Proceedings of the International Meeting on Thermal Nuclear Reactor Safety, held at Chicago, Illinois, August 29—September 2, 1982, contain the entire collection of papers submitted for presentation at the meeting, as well as two special addresses, and four summarizing review articles. The papers deal with a wide spectrum of subjects pertaining to the area of thermal nuclear reactor safety, including: licensing criteria, safety goals, probabilistic risk assessment, reliability analysis, safety-related operational experience, man/machine interface, human factors, transient analysis, loss-of-coolant analysis, structural analysis, fuel performance evaluation, severe accident analysis, radiological source term evaluation, pressurized thermal shock. In addition to papers on the above technical subjects, the Proceedings contain a number of papers describing safety-related programs in a number of countries, including Argentina, Brazil, Canada, Fed. Rep. of Germany, Finland, France, Greece, Italy, Japan, Mexico, Spain, Sweden, and United Kingdom. The Meeting was jointly sponsored by the American Nuclear Society, the European Nuclear Society, the Canadian Nuclear Society, and the Japan Atomic Energy Society. It was, furthermore, organized and conducted in cooperation with the U. S. Nuclear Regulatory Commission and the International Atomic Energy Agency.

17. KEY WORDS AND DOCUMENT ANALYSIS

17a. DESCRIPTORS

licensing; safety goals; probabilistic risk assessment, PRA; reliability analysis; operational experience; man/machine interface; human factors; transient analysis; accident analysis; loss-of-coolant accident, LOCA; small-break LOCA analysis; large-break LOCA analysis; severe accident analysis; radiological source terms; pressurized thermal shock; degraded core cooling; structural analysis.

17b. IDENTIFIERS/OPEN-ENDED TERMS

18. AVAILABILITY STATEMENT
Unlimited

19. SECURITY CLASS *(This report)*
Unclassified

21. NO. OF PAGES
2140 (3 volumes)

20. SECURITY CLASS *(This page)*
Unclassified

22. PRICE
S