NUREG/CR-3026
BNL-NUREG-51609

FEASIBILITY STUDY ON THE ACQUISITION OF LICENSEE EVENT DATA

W.Y. Kato, R.E. Hall, T. Teichmann, J. Taylor,
W.J. Luckas, Jr., P. Saha, P. Samanta and J. Fragola

October 25, 1982
Revised May 25, 1983

DEPARTMENT OF NUCLEAR ENERGY, BROOKHAVEN NATIONAL LABORATORY
UPTON, NEW YORK 11973

Prepared for the U.S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research
Contract No. DE-AC02-76CH00016

NUREG/CR-3026
BNL-NUREG-51609
AN

FEASIBILITY STUDY ON THE ACQUISITION OF LICENSEE EVENT DATA

OCTOBER 25, 1982
REVISED MAY 25, 1983

by
W.Y. Kato, R.E. Hall, T. Teichmann, J. Taylor,
W.J. Luckas, Jr., P. Saha, P. Samanta and J. Fragola*

*Science Applications, Inc., New York, N.Y.

DEPARTMENT OF NUCLEAR ENERGY
BROOKHAVEN NATIONAL LABORATORY
UPTON, NEW YORK 11973

Prepared for
OFFICE OF NUCLEAR REGULATORY RESEARCH
UNITED STATES NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555
CONTRACT NO. DE-AC02-76CH00016
FIN A-3230

Available from
GPO Sales Program
Division of Technical Information and Document Control
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
and
National Technical Information Service
Springfield, Virginia 22161

ABSTRACT

Brookhaven National Laboratory's Department of Nuclear Energy (DNE) has performed a study of the Licensee Event Report (LER) system. The objective of the study was to assess the feasibility of modifying the LER reporting system as proposed by NRC-AEOD, and/or developing an alternative plan that would in addition collect information about significant events amenable to statistical analysis, such as multi-case, multi-variate analysis.

To carry out the study, BNL formed a multi-disciplinary team of engineers and consultants that included individuals with experience in LER case studies, plant operation and systems, core physics and thermal-hydraulics, statistical analysis, PRA, human factors, and data analysis.

The study indicated that the LERs constitute reports from a large variety of events which have in most cases many different plant parameters, both measured and currently not measured, to characterize the event. In order to determine event-specific plant parameters required for statistical and deterministic analysis, a data matrix approach was used to identify those parameters which are currently being recorded, those which could be measured and recorded, and those which are required for certain types of events involving thermal-hydraulics and neutronics as illustrative of events requiring in-depth analysis.

Also included in the study was a review of INPO's Nuclear Plant Reliability Data System; NASA's Problem Reporting and Corrective Action (PRACA) program; Electricité de France's KIT system, an automatic computer-based reactor parameter monitoring and recording system; and the regulatory relationship between the FAA and the commercial airline industry.

FOREWORD

A multi-disciplinary team of engineers formed an LER study team to assess within a short time period (about 12 weeks) the feasibility of modifying or developing an alternative to the NRC LER reporting system, which would be more amenable to statistical analyses.

The study team had many discussions regarding the collection, storage and utilization of LER data with NRC staff and contractors, INPO, EPRI, utilities, reactor vendors, other U.S. government agencies, and foreign utilities and safety authorities. This report, based on the survey of various organizations and on an in-depth review of the LER data requirements by the study team, presents the results of the study in the form of: a data matrix identifying plant parameters required for significant event analysis for trend and accident precursor determination, a discussion of deterministic and statistical analysis methods for significant event analysis, summary of findings, and conclusions.

The team received excellent cooperation from all individuals and organizations that it contacted. All parties appeared to fully provide as much information on a forthright and comprehensive basis as the team could utilize in the short time available. This study could be accomplished only with such cooperation by many different individuals and organizations.

SUMMARY

In response to an NRC request, Brookhaven National Laboratory's Department of Nuclear Energy (DNE) has performed a study of the Licensee Event Report (LER) system. The objective of the study was to assess the feasibility of modifying the LER reporting system as proposed by NRC-AEOD, and/or developing an alternative plan that would in addition collect information about significant events amenable to statistical analysis. The purposes of an LER system are (1) to provide a data base for the identification of accident precursors, trends and patterns; (2) to provide input for a component/system reliability data base; and (3) to help provide input for probabilistic risk assessment (PRA) studies.

To carry out the study, BNL formed a multi-disciplinary team of engineers and consultants that included individuals with experience in LER case studies, plant operations and systems, core physics and thermal-hydraulics, statistical analysis, PRA, human factors, and data analysis. The LER study team carried out its study in the following manner:

1. It contacted representative organizations within and outside the nuclear power field in the United States and abroad regarding the collection, storage, retrieval, and analysis of LER data or similar incident report data. These organizations included various NRC divisions and contractors, U.S. and foreign utilities, INPO, EPRI, NASA, NBS, and FAA/NTSB.

2. In parallel, the team reviewed statistical and deterministic methods of analysis as applicable to LER analysis.

3. The team developed a data matrix approach to identify plant parameters which would be required and could be utilized for statistical and deterministic analysis of events.

4. The team prepared a summary of findings and conclusions, with the details of the basis for the findings and conclusions being placed in the appendices.

The types of data required for event analysis can be grouped into four categories:

1. A complete and accurate narrative description of the event, including event scenario and quantitative data;

2. plant-specific information, including component/system specifications, engineering (mechanical, electrical, etc.) drawings;

3. normal operational data, including maintenance records, and

4. event-specific plant parameters as a function of time from just preceding until termination of the event.

The study indicated that the LERs constitute reports from a large variety of events which have in most cases many different plant parameters, both measured and currently not measured, to characterize the event. In order to determine event-specific plant parameters required for statistical and deterministic analysis, a data matrix approach was used to identify those parameters which are currently being recorded, those which could be measured and recorded, and those which are required for certain types of events involving thermal-hydraulics and neutronics as illustrative of events requiring in-depth analysis. The data matrix also identified those parameters which could be used in the statistical analysis of events. It was also recognized that event tree/fault tree analysis and/or FMEA techniques on a plant-specific basis, which are used in probabilistic risk assessment (PRA) and which may be required of all nuclear power plants in NREP (National Reliability Evaluation Program) by the NRC, would be a highly useful tool to help identify parameters required for statistical and deterministic analysis of events for accident precursor identification. Event tree/fault tree analysis and/or FMEA could also be used to help identify those events which are significant on the basis that they are more directly accident precursors.

A brief summary of the findings and conclusions are given below.

1. An accurate and complete narrative description of every reportable event, including the event scenario and quantitative data, is essential for the analysis of an event. A structured narrative description such as required by FAA/NTSB for aircraft incidents would be a significant aid in developing a

complete description of an event. A comprehensive event analysis data base may take three to five years in development. Although the proposed LER Rule does not necessarily provide a structured narrative of the event, it generally represents an important step toward the development of such a comprehensive data base.

2. The types of quantitative data required for statistical and deterministic analysis have been outlined using a data matrix approach. To implement this approach, significant improvements would have to be made in the collection of relevant event-specific nuclear power plant parameters immediately preceding and during some events for later in-depth analysis. All such event specific parameters need only to be collected and stored and available for use by event analysts, but not necessarily reported with each LER.

3. Although much operational data are currently being collected, significant improvement in the mode of collection and storage, as well as collection of additional data could be accomplished by the installation at each nuclear plant of an Incident Parameter Recorder (IPR), which possibly includes a voice recorder similar to a flight recorder required by the FAA/NTSB in aircraft. An IPR would automatically collect and store key plant parameters and the status of key plant components and systems as a function of time from just preceding until termination of the event for event reconstruction and analysis. The study suggests that the Safety Parameter Display System (SPDS) required by the NRC for all plants modified with the addition of a computer based data storage facility could be the basis for an IPR. Electricité de France, the French utility, does have an automatic plant parameter recording system called KIT installed on all of their operating PWRs, which aids plant operations staff and event analysts to accurately reconstruct events.

4. The utilities are the key to the collection and analysis of operational data, including event data, since they have personnel who are most knowledgeable about the details of components and systems in their nuclear power plants, as well as having all other required parameters directly available to them. It is essential that event analysts, whether they are NRC staff or contractors or INPO staff, for the analysis of events on an industry-wide

(nationally and internationally) basis, be competent engineers knowledgeable about the details of nuclear power plants and have the capability of making direct contact with plant operations staff for the accurate reconstruction of events.

5. The LER system should provide economic and safety incentives for complete and accurate reporting. The utilities may benefit from LER reporting and component reliability data collection and analysis, for example, if, by proving the reliability of their plant systems, longer time intervals for in-service inspection and testing become acceptable.

6. Various data banks utilizing computers for the collection of plant component and system specifications, operational data, reliability and event-specific data have been or are being established. Improved coordination of the various data banks so that they utilize identical definition of components, component boundaries and component failure, and have the same or compatible formats is important to improve event and reliability analysis.

TABLE OF CONTENTS

TABLE OF CONTENTS
(Cont'd)

1. INTRODUCTION

The Department of Nuclear Energy (DNE) of Brookhaven National Laboratory (BNL) was requested by the U.S. Nuclear Regulatory Commission to assess the feasibility of modifying the LER reporting system proposed by AEOD and/or developing an alternative plan to collect information about significant events in the operation of nuclear power reactors so the resultant data base will be appropriate for multi-case, multi-variate analyses. The program was geared to have its major tasks completed within a twelve week period from its inception. By having this short turnaround, the conclusions of the study could be used in the decision making process in the present Licensee Event Report (LER) rulemaking. In order to fulfill the requirements of the program, BNL assembled a multidisciplinary ad hoc team of engineers to investigate the needs and potential direction of the industry. Due to the short time frame, the study, as reported in this document, relied heavily on extensive fact finding through personal contacts in the nuclear as well as other high technology fields.

1.1 OBJECTIVES

At the present time, the U.S. NRC is attempting, through both deterministic and statistical analyses, to review the level of designed safety of nuclear power plants and, where practical, identify accident precursors. Through the application of multi-case, multi-variate analyses and other statistical methods, it is hoped that accident precursors can be identified and steps taken to either avoid or minimize the effects of future significant events. A major problem that the NRC and industry faces at this time is the severe lack of a consistent industry-wide operational data base. In order to conduct the deterministic and statistical analyses for precursor identification, probability of accidents, and plant response to an accident, a data base that consists of detailed plant specifications, operational status of equipment and operations staff, and thermal-hydraulic and neutronic parameters is needed.

One of the primary usages of a data base such as the Licensee Event Reports (LERs) is in the identification of the significant events which require further in-depth studies. A broad definition of the significant events from the NRC perspective could be: "events with the highest potential risk to public health and safety." These events could range from a loss-of-coolant accident to an operational transient such as a turbine or reactor trip. Typical examples of such events are those that are analyzed in an FSAR for every commercial nuclear power reactor.

The analyses that are presented in the FSARs may be grouped into three categories. They are:

1. Scenarios for which the pressure and temperature in the reactor increase but do not result in an uncontrolled release of radioactivity. Examples of such incidents are:

   - uncontrolled withdrawal of the control rod assembly
   - boron dilution incident
   - loss of coolant flow incident
   - loss of feedwater incident
   - loss of load incident

   The events in the above category are also called "abnormal operational transients."

2. Scenarios where a pressure and temperature increase in the reactor system could lead to an uncontrolled release of radioactivity. Examples of such events are:

   - large or small break loss-of-coolant accident
   - steam line break accident
   - steam generator tube rupture accident
   - control rod assembly ejection or drop accident

   The events in the above category are customarily called "accidents."

3. Scenarios which do not involve the reactor system but could lead to the release of radioactivity. Examples of such events are:

- fuel handling incident
- radioactive waste gas incident

External events such as loss of off-site power, earthquake, tornado, flood, fire, airplane crash, etc. have the potential to cause some of the above malfunctions or accidents, thereby causing the release of radioactivity. Thus, many external events also fall into the general framework of "Significant Events."

The study focuses on the collection and storage of the needed operational data to conduct deterministic and statistical analyses of events such as those exemplified above.

1.2 SCOPE

The scope of this study is to address the feasibility of developing a conceptual and operational design for a method of collecting and storing operational data of reportable events. This framework includes, but is not limited to, those events as listed in the proposed LER rule. For each such event identified, the information needed to conduct engineering case studies should also serve as a data base for multi-case, multi-variate analysis. The feasibility of identifying the plant parameters needed and available in each case is discussed. In order to complete the scope of effort, first the analytical methods required to analyze significant events were identified. Next, a data system was conceptualized and documented with respect to the significant events. The system includes sources of relevant information within operating power reactors, as well as data available from external sources. As an outgrowth of the conceptual design, an identification was made of the parameters that cannot be measured at this time. The final product consists of a list of potential operational data needed to perform safety analyses and a feasible implementation strategy for the collection and storage of a realistic amount of data.

1.3 STUDY APPROACH

A multidisciplinary ad hoc team of engineers of BNL staff and consultants was assembled. The experience base represented by this team included:

- data analysis
- LER case study work
- statistical analysis
- probabilistic risk assessment
- human factors expertise
- plant operations/systems experience
- thermal-hydraulic analysis
- core physics calculations

In addition to using the team's expert opinions on the subject of developing a data base and recommended implementation strategy, the study made extensive use of fact finding meetings with representatives of the nuclear and other high technology industries. Appendix A lists those organizations contacted by members of the study team which had an influence on the conclusions of the project. Representatives of the U.S. NRC staff, its contractors, other government agencies, utilities, industry, commercial air carriers, and foreign agencies were interviewed on this subject of data collection and storage.

The results of these two approaches, systematic expert opinion and fact finding, were then applied to a conceptual model, discussed later in Section 3.1, that allowed the synthesis of the results. This is displayed in Figure 1.

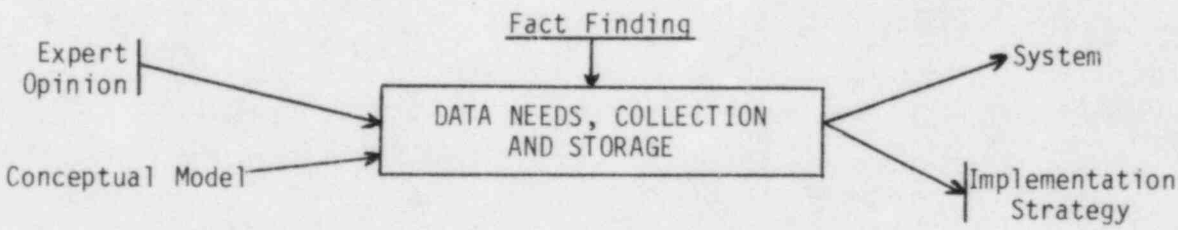


FIGURE 1. STUDY APPROACH

Through the application of this approach, a consensus opinion of the study team was reached. It should be noted that the final direction of the program as reported here is, where applicable, supported by the numerous interviews conducted. This adds confidence to the conclusions, in that individuals representing the nuclear industry, as well as other government agencies controlling high technology commercial industries, seem to be moving towards or have already developed a data base for event analysis.

1.4 REPORT OUTLINE

The remaining sections of this report will highlight the principal results of the study. The technical appendices provide the supporting detailed technical information. They document the material collected, developed and reviewed during the approximate 12 weeks of the project.

Chapter 2 addresses a conceptual data system that could be used to measure, collect, and store all potentially needed information to conduct both deterministic as well as statistical analyses of events in power reactors. The section is strongly based on a matrix of events and reactor parameters developed during the study and presented in Appendix B. Chapter 3 reviews the practicalities of implementing such a system as described in the preceding chapter, and applies a conceptual framework developed by the study team. In this way an immediate, interim solution and a near term future system are recommended. Chapter 4 presents the summary of the findings of the survey conducted of different organizations during this study. Chapter 5 presents the conclusions of this study.

2. A CONCEPTUAL DATA SYSTEM

2.1 DISCUSSION OF SYSTEM

The needs of any high technology industry that can have an impact on the quality of life of its customers must consider both system availability and public safety. These factors are not necessarily mutually exclusive in that a decrease in availability reduces industry profit but also can affect safe operation. On the other hand, a public safety problem, generally as a result of an accident, also impacts the profit margin. Availability and safety are, therefore, very closely interrelated, and utilities that operate the nuclear power plants and provide the event data should see a direct benefit for the effort in providing the data.

In the commercial airline industry (reference Appendix I), benefit can result from using the event data by allowing a proven highly reliable system longer times between scheduled test and maintenance as compared to a unit with a poor reliability data record. In this way, the availability and safety aspects can be directly tied together. When reviewing the interface between these concepts, it is important to be cautious in defining which events have potential safety impacts. Until the abnormal operating conditions of the system are fully known, data should be collected on all systems and components that could be important to safety. In this way no significant event data will be omitted due to a too restrictive definition of the term "safety-related". The data system should include information when there is a question as to its future usefulness.

There are four types of data which may be required for event analyses.

1) First, the up-to-date plant specific information, which include detailed component data, design and construction drawings, normal operating data, etc., are required.

2) Second, the collection of the raw quantitative plant parameter data preceding and following an event should rely as much as possible on the direct measurement and recording of the parameter to remove possible human bias. This directly recorded and stored (possibly at the plant) information may make

up the bulk of the needed quantitative information for some significant events. If and when the raw plant data are required in order to conduct an analysis, it can be extracted from its storage location at the unit site. This allows the information to be available on request.

3) It is conceivable that data recorded manually by the operational staff of the plant will also be required, such as test and maintenance logs which constitute a third type of data. In these cases the handwritten hard copies should be available to the event analyst within a reasonable time frame.

4) A structured narrative with quantitative data specifically to provide a clear understanding of the event sequence or scenario should make up the fourth type of data needed. The narrative must be as complete and accurate as possible in order to be able to reconstruct the event in detail.

In all four cases the data are best collected by plant staff trained in the technique of data collection. It should be noted that each type of data is required to carry out a complete analysis of an event. The types of data are closely interrelated, and the event analyst must have access to all types. It is extremely important that the event analyst, who must be knowledgeable about the details of a specific plant at which the event has occurred, have the ability to contact the operations staff of the plant for detailed interviews regarding an event. In cases when the data are collected, reviewed or codified remotely to the station, a "closed loop approach" should be applied where the codified data are reviewed by the affected plant personnel such as in the NASA-PRACA system, reference Appendix F. Uncertainties introduced by interpretation of the analysis can be minimized by having the staff who prepared the event report review the coded information for correctness.

It should be noted that throughout the above discussion on the management scheme needed to collect the information, both hardware and human performance data are considered. The hardware generally lends itself to direct automatic recording techniques. However, the human data, other than perhaps in the area of response time and procedure following capability, must rely on indirect observations and on a narrative reporting scheme. Since the human is a key factor in both availability and safety, the data collected should be based on a systematic set of observations.

The use of a central data processing system, managed by an organization such as NRC or INPO and accessible by industry and NRC, should be employed to store and retrieve the needed information on events from all U.S. and foreign nuclear plants. All the details of each parameter for each event need not be stored in the central unit, as long as an access method exists to obtain all needed information. The additional data could well be in hard copy, depending on the data type; perhaps strip chart recorder tapes are good enough for data rarely used. This could be stored at the respective plants. It is important not to fill the central data processing with all information, since most of the anticipated large volume of information may rarely be used. It is important that a central organization manage the system to guarantee a full and accurate data set. A decentralized approach cannot exercise the needed control on the many types of data anticipated.

2.2 DATA MATRIX REVIEW

As noted in Chapter 1 of the report, the study utilized data matrices to help in the identification of the needed data and potential ways of collecting it. The use of the matrix display technique and systems analysis based on a data matrix is not new. By applying matrix analysis to reduce large volumes of related data to the minimum set of important points, a data review can become focused. The actual approach that would be required in reviewing nuclear plant operational data for trends and accident precursors relies on plant specific data matrices, as illustrated in Figure 2. By developing such an *a priori* graphical representation of the specific identified events of importance versus a standardized set of plant parameters, the analysis could identify which parameters or combination of parameters are essential for the analyses of most credible events. Thus, it will be possible to envelop most events that conceivably could occur during the life of a power plant.

As an example, this study developed matrices that were used to draw some of the conclusions. The complete analysis used three matrices, each having the same set of Boiling Water Reactor (BWR) and Pressurized Water Reactor (PWR) parameters which were developed from a systems review. The first compares the parameters to their availability, the form that they are in at this time (recorded, not recorded), and where they are located. The second is a

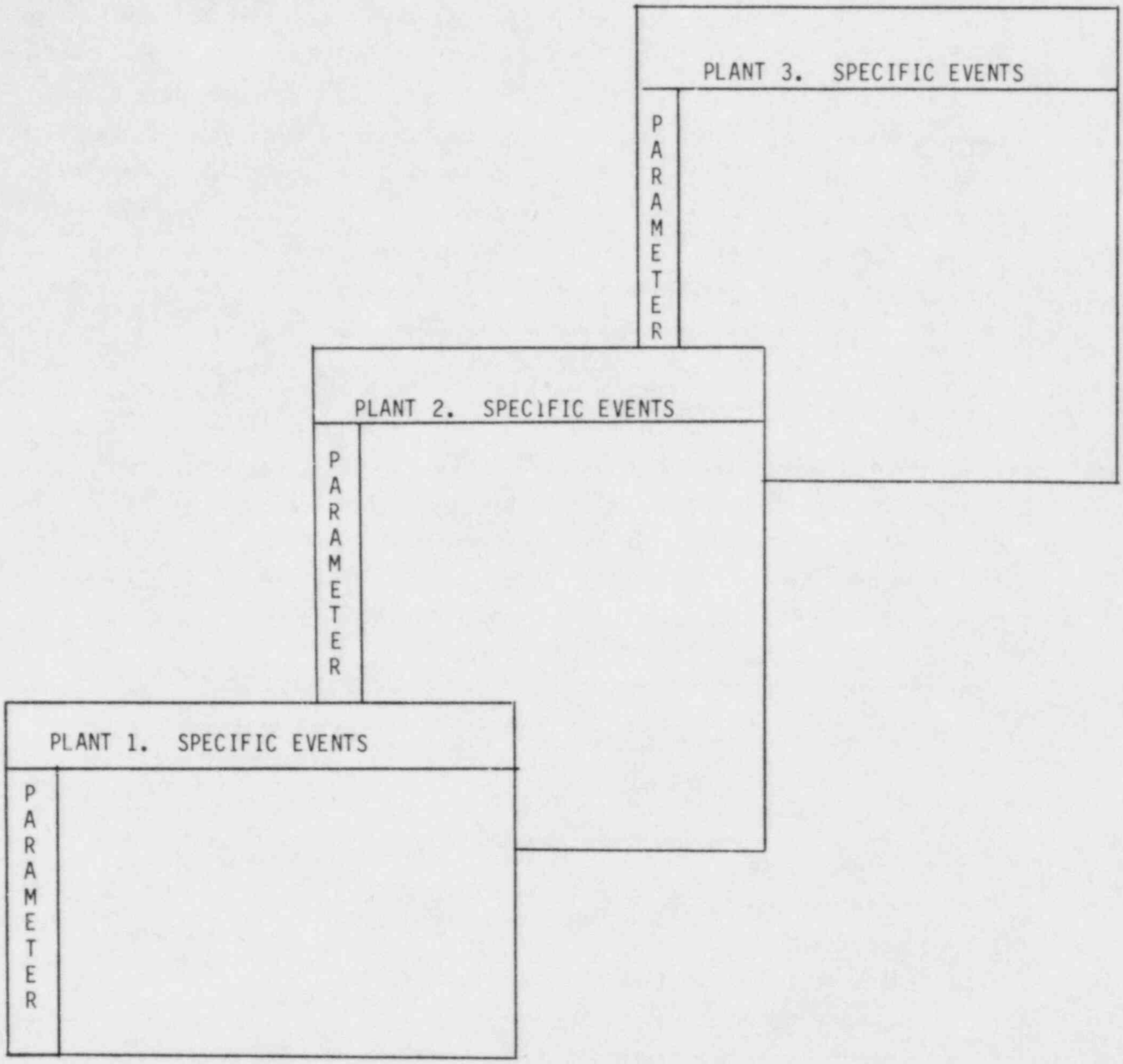


Figure 2. The Data Matrix

representative example of the needed parameters for a statistical analysis of a selected set of events, and the last a matrix for a representative deterministic evaluation. The third matrix illustrates how to proceed, in a plant specific manner, to review the needed parameters for representative events. It does not represent a complete analysis at this time since all important significant events have not been identified. This would require a systems analysis such as a FMEA or an event tree. All three independently developed matrices have been combined into one figure for PWRs and one for BWRs and can be found in Appendix B. By using this graphical approach, the excessively large number of events, uses, availability, and parameter combinations can be analyzed in a meaningful way.

The top level systems of both the PWR and BWR were divided into eight generic types, and then each was subdivided into the principal parameters that are presently annunciated. Table 1 represents a listing of the number of potentially needed major parameters for each plant type, and Table 2 the actual major parameter listing as extracted from Appendix B.

TABLE 1
PLANT PARAMETERS BY FUNCTION

		BOILING WATER REACTOR	PRESSURIZED WATER REACTOR
I.	Nuclear Systems	25	26
II.	Engineered Safety Systems	16	22
III.	Containment	17	14
IV.	Electrical Systems	8	8
V.	Power Conversion Systems	6	9
VI.	Process Auxiliary Systems	13	12
VII.	Plant Auxiliary Systems	4	6
VIII.	Plant External	5	5
	Total	94	102

This is not to say that all parameters will be needed for all events, but on the contrary, each event will only require a subset of the listing. The selection of this subset is the difficult question presently on hand, and

TABLE 2
PARAMETER LISTING

SYSTEM/PARAMETER (PWR)

NUCLEAR SYSTEMS

REACTOR CORE/VESSEL
Parameter
1. Neutron Flux
   - Source Range
   - Intermediate
   - Power Range
2. Reactor Water Level
3. Core Exit Temperature
4. Degrees of Subcooling
5. Water Chemistry
6. Core Cooling Flow

CONTROL ROD DRIVE SYSTEM
Parameter
1. Control Rod Position
2. System Status

REACTOR COOLANT SYSTEM (RCS)
Parameter
1. RCS Hot Leg Temperature
2. RCS Cold Leg Temperature
   RCS Average Temperature
3. Reactor Coolant System Pressure
4. Soluble Boron Concentration
5. RCS Radioactivity
6. Reactor Coolant Pump Status

PRESSURIZER
Parameter
1. Pressurizer Level
2. Pressurizer Pressure
3. Pressurizer Temperature
4. Pressurizer Heater Power
5. PORV Position
6. PORV Flow
7. Pressurizer Quench Tank Level
8. Pressurizer Quench Tank Pressure
9. Pressurizer Quench Tank Temp.
10. Safety Valve Position
11. Safety Valve Flow
12. Safety Valve/PORV Exhaust Temp.

CHEMICAL AND VOLUME CONTROL SYSTEM/
EMERGENCY BORATION SYSTEM
Parameter
1. System Status/Mode
2. Boric Acid Charging Flow
3. Volume Control Tank Level
4. Makeup Flow
5. Letdown Flow
6. RCP Seal Flow in/out
7. Accumulator Level
8. Accumulator Pressure
9. Accumulator Isolation Valve Position
10. Refueling Water Storage Tank Level

RESIDUAL HEAT REMOVAL SYSTEM
Parameter
1. System Status
2. System Flow
3. System Radioactivity
4. RHR Heat Exchanger Outlet Temp.

REACTOR PROTECTION SYSTEM
Parameter
1. System Status

ENGINEERED SAFETY SYSTEMS

LOW PRESSURE SAFETY INJECTION
Parameter
1. System Status
2. System Flow
3. System Temperature

HIGH PRESSURE SAFETY INJECTION
Parameter
1. System Status
2. System Flow
3. System Temperature

AUXILIARY FEEDWATER SYSTEM
Parameter
1. System Status
2. System Flow
3. System Temperature

TABLE 2 (CONT'D)
(PWR)

CONTAINMENT

GENERAL
Parameter
1. Pressure
2. Temperature
3. Sump Water Level
4. Radioactivity

ISOLATION
Parameter
1. Isolation Valve Positions

CONTAINMENT SYSTEMS
Parameter
1. Purge System Status
2. Containment Spray Flow
3. H2,O2,N2 Concentration
4. Effluent Radioactivity
5. Containment Ventilation System Status
6. Ice Condensor System Status
7. H2 Recombiner System Status

ELECTRICAL SYSTEMS

GENERAL
Parameter
1. Breaker Positions
2. Voltages
3. Currents

EMERGENCY POWER
Parameter
1. Diesel Generator Status
2. Diesel Generator Fuel Supply
3. Battery & Inverter Status

LIGHTING
Parameter
1. Status

GENERATOR
Parameter
1. Generator Output (MWe)

POWER CONVERSION SYSTEMS

STEAM GENERATOR
Parameter
1. Water Level
2. Pressure
3. Dump Valve Position
4. Dump Valve Flow
5. Vent Discharge Radioactivity
6. Safety Valve Position
7. Safety Valve Flow

MAIN STEAM
Parameter
1. Steam Flow

CONDENSATE/FEEDWATER
Parameter
1. Feedwater Flow
2. Condensate Storage Tank Level

TURBINE BYPASS SYSTEM
Parameter
1. Bypass Valve Position
2. Bypass Valve Flow

PROCESS AUXILIARY SYSTEMS

CONDENSER AIR REMOVAL SYSTEM
Parameter
1. Effluent Radioactivity

LIQUID RADWASTE SYSTEMS
Parameter
1. Systems Status
2. Storage Tank Levels
3. Effluent Radioactivity

SERVICE WATER SYSTEMS
Parameter
1. System Status
2. Water Temperature
3. System Flow
4. Effluent Radioactivity

COMPONENT COOLING WATER SYSTEM
Parameter
1. System Status
2. Water Temperature
3. System Flow
4. Effluent Radioactivity

TABLE 2 (CONT'D)
(PWR)

PLANT AUXILIARY SYSTEMS

FIRE PROTECTION
Parameter
1. System Status

COMMUNICATIONS
Parameter
1. System Status

CONTROL ROOM HVAC
Parameter
1. System Status

AUXILIARY BUILDING VENTILATION SYS.
Parameter
1. System Status
2. Effluent Radioactivity

SEISMIC
Parameter
1. Accelerometer Output

PLANT EXTERNAL

RADIATION MONITORING
Parameter
1. Radioactivity at all Licensed Release Points
2. Radioactivity at Plant Perimeter

METEOROLOGY
Parameter
1. Wind Direction
2. Wind Speed
3. Atmospheric Stability (vertical temperature differences)

TABLE 2 (CONT'D)
PARAMETER LISTING

SYSTEM/PARAMETER (BWR)

NUCLEAR SYSTEMS

REACTOR CORE/VESSEL
Parameter
1. Neutron Flux
   - Source Range Monitor & Position
   - Intermediate Range & Position
   - Average Power Range Monitor
2. Reactor Water Level
3. Reactor Water Temperature
4. Reactor Pressure
5. Radioactivity
6. Core Temperatures
7. Core Flow
8. Water Chemistry
9. Metal Temperature
   - Upper Flange
   - Lower Head
   - Transition Piece

CONTROL ROD DRIVE SYSTEM
Parameter
1. Control Rod Position
2. System Status
3. Scram Discharge Volume Level

RECIRCULATION SYSTEM
Parameter
1. System Status
2. Recirculation Pump Speed
3. Flow

STANDBY LIQUID CONTROL SYSTEM
Parameter
1. Storage Tank Level
2. Storage Tank Temperature
3. System Status

RESIDUAL HEAT REMOVAL SYSTEM
Parameter
1. System Mode
2. System Status
3. Heat Exchanger Outlet Temp.
4. System Flow
5. Heat Exchanger Flow

REACTOR PROTECTION SYSTEM
Parameter
1. System Status

REACTOR CONTROL SYSTEM
Parameter
1. Mode Switch Position

ENGINEERED SAFETY SYSTEM

REACTOR CORE ISOLATION COOLING
(or Isolation Condenser)
Parameter
1. System Status
2. System Flow
3. System Temperature
4. Isolation Condensor Shell Side (water level)
5. Isolation Condensor Valve Position

HIGH PRESSURE COOLANT INJECTION
Parameter
1. System Status
2. System Flow
3. System Temperature

LOW PRESSURE COOLANT INJECTION
Parameter
1. System Status
2. System Flow
3. System Temperature

LOW PRESSURE CORE SPRAY
Parameter
1. System Status
2. System Flow
3. System Temperature

AUTOMATIC DEPRESSURIZATION SYSTEM
Parameter
1. Safety Valve
2. ADS Valve Position
3. Flow Through Valve
4. System Status

TABLE 2 (CONT'D)
(BWR)

CONTAINMENT

DRYWELL

Parameter

1. Pressure
2. Temperature
3. Sump Levels
4. Airborne Radioactivity Level
5. H2,O2,N2 Concentration, as applicable
6. Spray Flow
7. Effluent Radioactivity

WETWELL (Suppression Pool, Torus)

Parameter

1. Water Level
2. Water Temperature
3. Spray Flow

ISOLATION

Parameter

1. MSIV Valve Positions
2. System Status

CONTAINMENT SYSTEMS

Parameter

1. H2 Recombiner Status
2. Purge System Status
3. Containment Ventilation System Status

SECONDARY CONTAINMENT (Reactor Bldg)

Parameter

1. Pressure

ELECTRICAL SYSTEMS

GENERAL

Parameter

1. Breaker Positions
2. Voltages
3. Currents

EMERGENCY POWER

Parameter

1. Diesel Generator Status
2. Diesel Generator Fuel Supply
3. Battery & Inverter Status

LIGHTING

Parameter

1. Status

GENERATOR

Parameter

1. Generator Output (MWe)

POWER CONVERSION SYSTEMS

MAIN STEAM

Parameter

1. Steam Flow
2. Main Steam Isolation Valve Leakage Control System Pressure

CONDENSATE/FEEDWATER SYSTEM

Parameter

1. Feedwater Flow
2. Condensate Storage Tank Level

TURBINE BYPASS SYSTEM

Parameter

1. Bypass Valve Position
2. Bypass Flow

PROCESS AUXILIARY SYSTEMS

OFF-GAS SYSTEM

Parameter

1. Off-gas System Status
2. Effluent Radioactivity

LIQUID RADWASTE SYSTEMS

Parameter

1. Systems Status
2. Storage Tank Levels
3. Effluent Radioactivity

SERVICE WATER SYSTEMS

Parameter

1. System Status
2. Water Temperature
3. System Flow
4. Effluent Radioactivity

TABLE 2 (CONT'D)
(BWR)

REACTOR BUILDING CLOSED COOLING

Parameter

1. System Status
2. Water Temperature
3. System Flow
4. Effluent Radioactivity

PLANT AUXILIARY SYSTEMS

FIRE PROTECTION

Parameter

1. System Status

COMMUNICATIONS

Parameter

1. System Status

CONTROL ROOM HVAC

Parameter

1. System Status

SEISMIC

Parameter

1. Accelerometer Output

PLANT EXTERNAL

RADIATION MONITORING

Parameter

1. Radioactivity at Licensed Release Points
2. Radioactivity at Plant Perimeter

METEOROLOGY

Parameter

1. Wind Direction
2. Wind Speed
3. Atmospheric Stability (vertical temperature differences)

will be further discussed in Section 3. For the conceptual data system, access is desirable in one form or another to all the listed parameters depending on the event specifications and the type of analysis being conducted. It should be noted that each generic system type has a subcategory referred to as "System Status." This is meant to be a catch-all subdivision that includes the physical status (on/off, open/closed) of all the pumps, valves, instrument and controls, and electrical power that make up the secondary components in the plant. An example of such secondary components would be pilot air solenoid valves that control the actuator of a containment purge system valve. It is this so-called secondary component status that could dominate the parameter listing by the magnitude of numbers and mask the needed information. It is for this reason that this limited study used the subdivision of "system status" along with an attempt to define the primary components in a way that the component boundary encompasses as many of the secondary components as is practical.

To move slightly away from the conceptual list toward a realistic parameter list, the data matrix analysis shows whether or not each parameter is presently recorded, and where the reading is located. It appears that a large number of the parameters are presently available in one form or another, but not always recorded. This matrix of Appendix B represents the generic information available to BNL during the study, and should not be construed to be fact for all specific power plants. The matrix is by necessity general in nature. In addition, the study attempted to review the deterministic and statistical uses for each parameter, as represented in the matrices of the Appendix. The deterministic example used known, standard events to review the needed parameters. These include:

- Large Break Loss of Coolant Accident (LBLOCA)
- Small Break Loss of Coolant Accident (SBLOCA)
- Control Rod Drop Accident (CRDA)
- Steam Generator Tube Rupture (SGTR)
- Anticipated Transients Without Scram (ATWS)

As can be seen in the matrix, most parameters are needed in these cases to perform a deterministic thermal-hydraulic core neutronic safety analysis. It is anticipated that any severe event of a known physical phenomenon would basically require the same level of detail. However, time did not permit us to further expand the matrix for other currently analyzed events based on FMEA or event tree analysis, nor was it within the scope of this study. In the less serious singular events for trend or precursor analysis, such as typically reported in an LER, the detail would probably not be needed. The exact level of needed information is difficult to identify at this time since the development of the initiator list and system response spectra is outside the scope of this study. This aspect, which has a dominant role on the conclusions, is further discussed in Chapter 3.

The statistical analysis section of the matrix relies heavily on Appendix C and addresses the type of data and analysis needed (see Table 3). The technical definitions of terms found in Table 3 can be found in Appendix C. The statistical analysis methods are also described in Appendix C.

TABLE 3
STATISTICAL ANALYSIS DATA TYPES (Examples)

Statistical	Physical
Nominal (e.g., component name, type)	Constant (e.g., component size, cost, capacity)
Binary/Polytomic (e.g., switch "on-off", switch position 1,2...n)	Historic (e.g., time of incident or maintenance)
Ordinal (e.g., fully charged, discharged for battery)	Dynamic (e.g., pressure or temperature as a function of time)
Interval (e.g., numerical variable without zero point)	
Ratio (e.g., temperature, voltage, pressure)	

Therefore, the results of the matrix analyses guide the data system towards building a complete matrix to identify parameters to be recorded, and the type and form of the data.* The matrix must be a living document that

*To aid the reader in understanding the matrix analyses, the matrices have been combined into one figure for PWRs and one for BWRs in Appendix B.

is regularly updated on the basis of the industry's growing understanding of potential initiators of off-normal operation and the plant's response spectrum to these initiators.

2.3 DATA ANALYSIS

The utilization of the event data discussed in the previous sections will be considered here. A complete and accurate narrative with appropriate plant parameters will provide the basis for event analysts to reconstruct the event scenario and conduct trend and precursor analysis using data from previous events in the file. In many cases engineering judgment, coupled with event tree or FMEA analysis, will provide direct conclusions regarding the cause of the event and required corrective action.

It should be recognized that many events such as those involving corrosion of piping or components, fuel degradation due to water jet impingement, external events, loose parts, biofouling, and fires, which may be significant and accident precursors, are more appropriately described in a narrative type format than trying to characterize the event with quantitative parameters. In many such events quantitative parameters to characterize the event are unknown or are extremely difficult to measure.

On the other hand, there are significant events whose analysis for accident precursors may be aided by deterministic and statistical analysis. Statistical analysis does, however, require the analysis of repetitive occurrences of more than a few similar or identical events in order to make the analysis meaningful.

An approach to the analysis of LERs is with the aid of event tree/fault tree analysis or failure mode and effect analysis (FMEA) for specific nuclear power plants. Assuming event trees/fault trees or FMEA were available for every plant, whenever an event occurred the relevant event trees/fault trees could be identified. Statistical analysis of the collection of identified event trees/fault trees for PWRs and BWRs could be performed to search for patterns and trends and accident precursors.

Two general types of analysis can be performed with event data: statistical and deterministic. Statistical analysis of repetitive occurrences is an aid in identifying patterns and trends and accident precursors. Deterministic analysis is used as an aid in 1) better understanding a specific event; 2) understanding the effects of additional equipment failures or operator action, and 3) development of mitigation procedures and correct design or procedural deficiencies.

Statistical Analysis

The statistical methods proposed here (i.e., reflected in Appendix B and outlined in Appendix C) are intended to be integrated with and properly adapted to the salient characteristics of the problems faced here. These include:

- well-defined (deterministic) behavior of certain aspects of plant operation;
- a variety of statistical data types;
- constant, historic and dynamic information; and
- a large number of variates relative to the number of events in some areas of investigation.

Consequently, the statistical approach is multi-step and multi-faceted. It addresses categorical data using discriminatory, graphical and (where appropriate) numerical methods, and quantitative data with multivariate techniques, both correlative and associative. Concomitant variables are included, and time series analyses are involved in a variety of depths. Questions of censored data and competitive risks are also touched on. The general approach is one of changing detail and aggregation and increasing comprehensiveness as significant statistical features of the system(s) emerge from the analyses. An example of how statistical analysis may be utilized is given in Appendix C.

The report of a subcommittee of the American Statistical Association Ad Hoc Advisory Committee on Nuclear Regulatory Research is appended as Appendix D. It encourages increased effort to develop adequate statistical methodology for the identification of trends and patterns from LERs. Also encouraged is more active working contact between statisticians outside of NRC and NRC staff having statistical problems.

Deterministic Analysis

For deterministic analyses of events which involve thermal-hydraulics and neutronics, advanced systems codes such as TRAC and RELAP5 can now be used to understand many of the significant events such as steam voiding in the reactor coolant system, steam generator tube rupture, loss of shutdown cooling and positive reactivity addition, etc. The codes are based on the nonhomogeneous nonequilibrium formulation of two-phase flow and employ the latest best estimate constitutive relations to describe the wall-to-fluid and vapor-to-liquid transfer terms. The codes are applicable to a wide range of accident scenarios starting from a large break loss-of-coolant accident (LBLOCA) to many operational transients such as turbine trip, loss-of-feedwater, etc. These codes are being assessed or verified extensively with the experimental data as well as plant incidents. Based on the assessment results, the codes are being constantly improved.

With the above background, it can be said that more quantitative evaluations of the significant plant events should be pursued. This will provide a better understanding of the event. Since additional equipment failure and the operator actions can also be simulated with these advanced codes, they may be used to determine the consequence of coupling these additional events to the original one for identifying serious accident precursors. Deterministic analyses will also aid in the development of mitigation procedures as well as correct possible design or procedure deficiencies. However, it must be kept in mind that many plant parameters (as illustrated in Appendix B) must be recorded and be available for performing such quantitative analysis.

3. PROPOSED IMPLEMENTATION STRATEGY

Not all the plant incidents that are required to be reported under the existing or proposed LER rule are "significant events." On the contrary, only a few percent (less than about 5%) of all the LER incidents are serious or significant enough to warrant further in-depth studies or investigation. The diversity of incidents which were reported to the NRC during the period January 1 to August 31, 1982 within the framework of the current reporting requirements is illustrated by the titles of selected LERs listed in Appendix E. The 95 events listed in Appendix E constitute about 3.5% of all the LERs reported during this period, and only a few of those listed appear to be amenable to thermal-hydraulic or neutronic deterministic analysis. The events which are listed are those which were screened by AEOD from all reported LERs during this period and appear to require some further in-depth analysis. It is estimated that approximately 1% are considered to be serious enough to require in-depth analysis. A screening procedure must, therefore, be followed to identify the significant events from all reported. This is by no means a trivial task. Good engineering judgement and thorough understanding of the nuclear power plant operation are needed to separate the more serious plant incidents from the routine-type events of no adverse consequences. If the approach discussed in Chapter 2 were to be applied indiscriminately, the important events could be masked by the voluminous numbers of additional data. This should be noted when considering that the present NSIC file on RECON has approximately 31,000 LER and LER predecessor generated abstracts on file. The needed screening procedure presently proposed by AEOD, reference Appendix F, can help in focusing the present system. However, it may not be capable in all cases to expand the sequences reported to the low probability/high consequence area. The approach of using a data matrix, multicase, analysis based on detailed systems analysis such as FMEA or other PRA techniques does, however, appear capable of increasing the systems approach.

Additionally, the proposed conceptual data system approach is manpower intensive and therefore the a priori screening of events is needed. Discussions with NASA, Johnson Space Flight Center, indicated that the space shuttle, which has not yet been placed on a continuous operating schedule, requires 90 to 120 people tracking the reliability of approximately 2,300 components without doing detailed statistical analysis of failures and trends.

Lastly, the requirement to automatically record all the parameters of Table 2 may not be totally necessary. The use of readily accessible plant files for the needed parameters in place of a central computer base file appears not only reasonable but follows the practices of other government agencies such as NASA and FAA.

3.1 THE EVENT DATA COLLECTION

Figure 3 represents a framework with which an event data system can be logically constructed. Two sides of the framework represent the expected number of each type of event on a per year basis and the relative volume of information needed by the amount of information on a per event basis. As one moves from the apex of each triangular model to the foot, this relative number increases. Progressing from a data source of plant specific information, which includes as built and as operated information about the plants, through "failure events" and "significant events" to the "serious events", more and more information on a per event basis is required in order to conduct the needed analysis. However, it is expected that the events become increasingly rare as the more serious events are approached. In this way the framework guides the collection and storage of operational data based on the significance, by definition, of each event.

The serious event, which is assumed to occur once or twice per year, requires rapid notification to the regulatory authorities, but the event specific data for in-depth analysis need not be transmitted immediately but should be available as analysis proceeds.

The next level of events is called "Significant Events" and have less of a potential significant consequence. It might be expected that the industry will see 50 to 100 of these such events per year. These events may warrant a detailed analysis for understanding the event or just a tracking analysis for precursor review. In these cases the data required are smaller in volume and need not be available on an immediate basis.

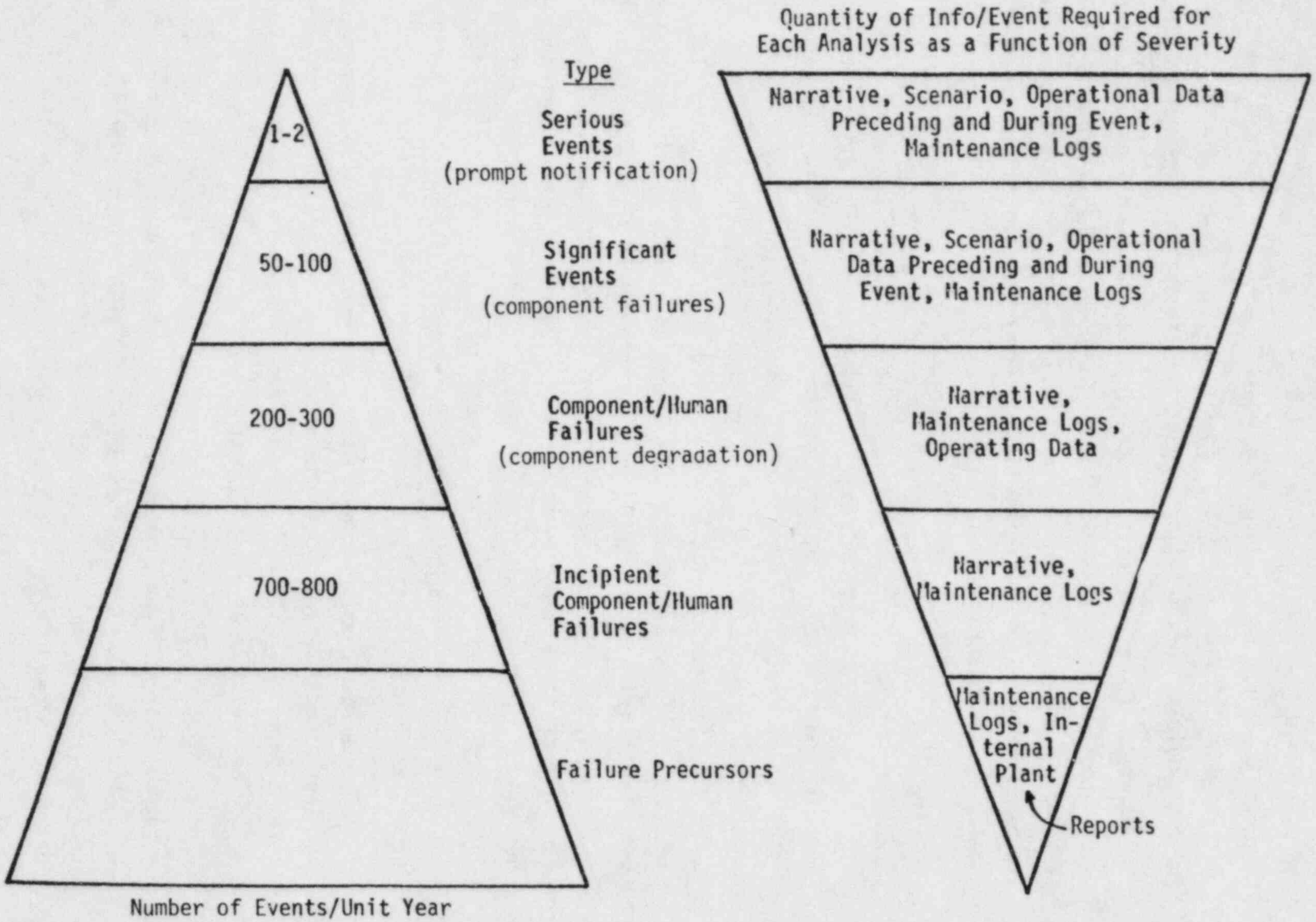


FIGURE 3. EVENT DATA COLLECTION FRAMEWORK BASED ON SIGNIFICANCE

The third category, "Component/Human Failure", includes components such as a pump and system unavailability due to catastrophic failure. "Incipient Component/Human Failure" includes such events as pump oil cooling failure, which could lead to bearing failure and hence to a pump failure. "Failure Precursors", which are usually not reported, are such events as pump bearing overtemperature. These last three categories contain the largest amount of operating data and are usually considered to be a reliability and risk data base. This type of data usually requires the application of a system model to analyze the plant response to the component or subcomponent failures. Due to the lower significance, the single failure of the device should not directly affect safety; these data need only be available on a longer time interval basis. We set once per three months as an estimate.

The last level of data consists of all the support documents such as as-built drawings, technical specifications, and equipment specifications. This type of detailed plant specific information, which is not event specific, is essential to conduct any of the analyses described above, but is only needed on an "on-call" basis and most probably can be handled in microfilm form.

Each category of data builds and adds on to the preceding data level so that the model is additive. Serious Events require all other lower data; Significant Events require failure event data and plant specific information, and so on. The serious event analysis can be considered the accident post-mortem; the significant events more of a precursor analysis; failure events as reliability information; and the plant specific information as supportive information. Attempting to fit current data efforts into the framework would result in a table such as Table 4. This table clearly shows that the data sources to meet the requirements of the framework potentially exist. However, they are presently in non-compatible form and may not be readily accessible for audit or actual use for an event.

3.2 PRESENT

At the present time, it does not appear to be reasonable to expect an LER system to contain all the needed information as discussed in this report. Instead, better use of the many different data sources can be achieved. A logical interface, and therefore a starting point, appears to be an administrative

TABLE 4
Current Data Efforts as Related to the Framework

Category / Data Source	NRC LER	TDC	INPO NPRDS	NRC IPRDS	Plant Files
No. of Plants in System	All	1	61	6	All
Plant Specific Information		X			X
Failure Events	X		X	X	X
Significant Events	X		X		X
Serious Events	X				X

link between the narrative form of the LERs, with INPO's NPRD system; NRC/ORNL's IPRD system, and NRC's Nuclear Plant Data Bank system. By making these four current efforts compatible, it is possible to move towards the framework as described in Section 3.1.

In addition, the capability of the NRC to obtain plant historical operating files should be fine-tuned so that the needed information available only at the plant site can be obtained in a reasonable time frame. In order to expedite this integrated effort, the feasibility of establishing an owners/users group outside of the licensing arena should be investigated. This would allow reporting inconsistencies to be resolved and the data could be accessed from a central point.

While this integration effort is underway, the concept of completing the matrix type of data display, as described in this report, should be attempted. As Figure 4 shows, the application of currently available plant specific system logic models, FMEA or event tree/fault tree type, should be used to identify the needed parameters to be measured and recorded on a plant specific

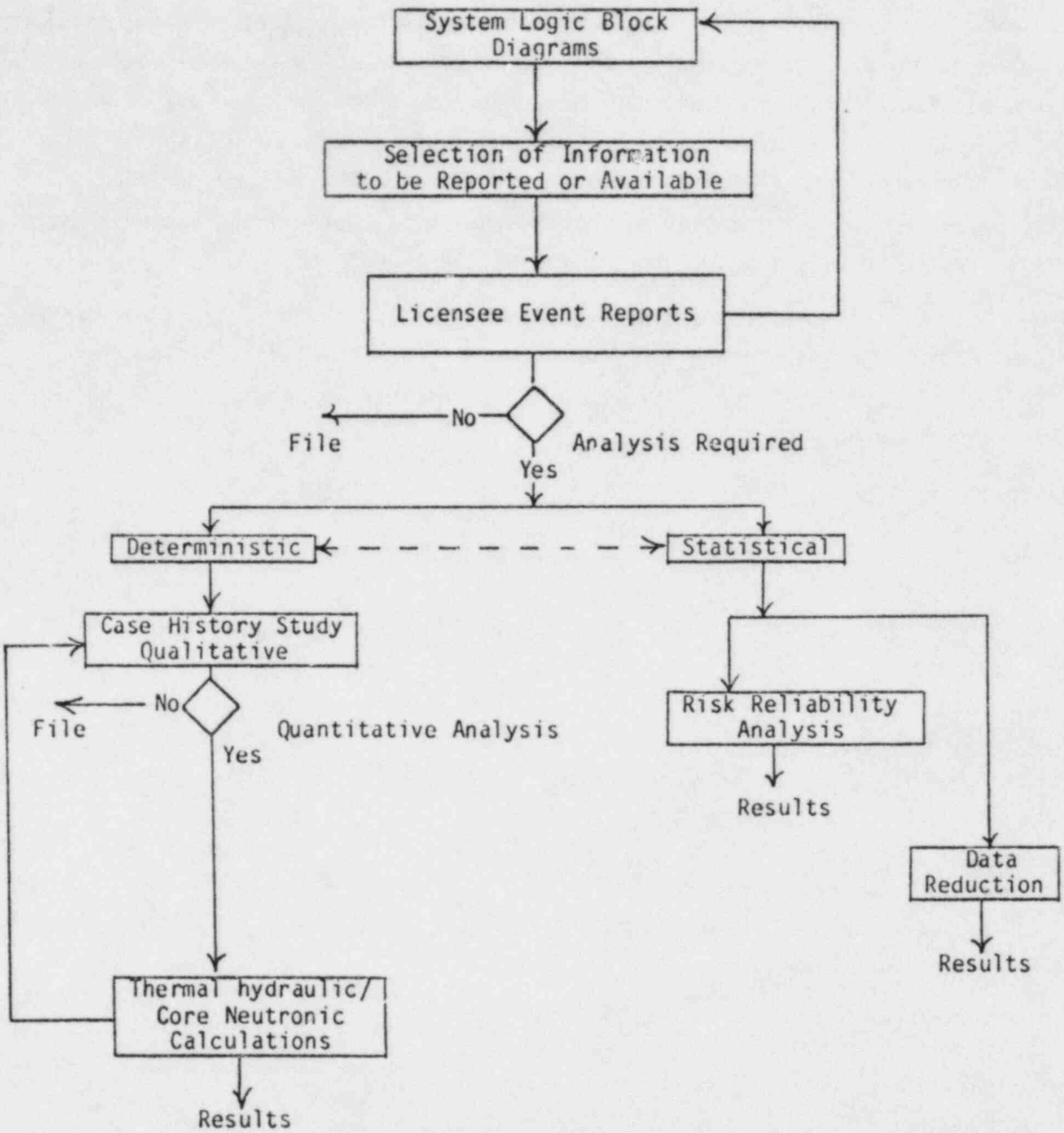


FIGURE 4. LERs Applied to Analysis

basis. This will begin to focus the matrices of Appendix B on an event level. A pilot study on 2 to 4 select plants should help identify the quantitative parameters that might be required to be reported, along with the narrative LER which should at least be retained at the plant site. This effort should then, working closely with the utility, determine the availability and location of the parameters. Where available, representative statistical and deterministic analysis should be tried to identify the usable techniques.

Both of these efforts can proceed independently of the LERs and therefore least disturb the ongoing collection of operating data. They will, however, represent the beginning of a systematic, logical, usable data system of which the LERs would be a part.

4. SUMMARY OF FINDINGS

4.1 DATA REQUIREMENTS

1. The analysis of events requires four types of data: (a) a complete and accurate narrative description of the event; (b) plant specific information including component specifications, drawings, etc.; (c) normal operational data including maintenance data, and (d) plant parameters specific to the event, possibly as a function of time, from just preceding until termination of the event.

A detailed analysis of a significant event (SE), especially involving neutronics or thermal-hydraulics, may require more quantitative data regarding the event. Such data include pertinent items from the following list: component, system, and piping specifications from as-built engineering drawings; reactor core specifications, including power history and distributions and neutron cross sections; maintenance records which provide the operational history of involved components or systems; time-dependent sequence of events including component and system operation and operator action; and time-dependent plant thermal-hydraulic and neutronic parameters from just preceding the event to the termination of the event.

Although statistical analysis has been the basis for developing a reliability data base for inputs (component failure rates, dependent failure rates, etc.) to probabilistic risk assessments, its use as a means for determining trends and precursors has been rather limited and isolated. Effort is needed to develop a proper framework for significant event statistical analysis, such as multivariate analysis and comparative risk analysis, on a small scale initially to determine its usefulness and applicability to nuclear systems.

2. Major improvements can be made in the collection and storage of relevant nuclear power plant performance data immediately preceding and following some events. These improvements can be made in the area of additional quantitative event data.

Due to the extraordinarily large number of plant variables that can be potentially measured for an event, and the numerous types of plant specific events that can be postulated, a systematic process must be used in identifying the specific requirements. Systems analysis techniques such as FMEA, as applied by NASA, or event tree/fault tree analysis, as used in the nuclear industry, should be used to supplement existing actuarial data in the development of the parameter identification matrix. Thus, the data system can focus on collecting the valuable parameter data needed for accident precursor analysis and not be overwhelmed by sheer numbers. In addition, much of this event-specific data need only to be collected and stored and be available when needed for in-depth event analysis. It need not necessarily be reported in each LER.

The FAA/NTSB uses a highly structured data gathering system (Appendix I), ("Manual of Code Classifications - Aircraft Accidents and Incidents", August 1981, and "NTSB Accident/Incident Report"), for investigating incidents and accidents that could be reviewed for guidance in the nuclear industry for the development of a more accurate and complete LER reporting system.

The development of an integrated data collection and storage effort, which includes the use of narrative descriptions of the event, should prove to be both feasible and cost effective if all the presently available data are utilized to build a workable system over the next three to five years.

3. Utility reporting requirements are currently located or described in different Rules, Regulatory Guides, and Technical Specifications, so that it is difficult to determine the information being collected which is applicable for LER analysis. Bringing together all of the reporting requirements in one document would aid in eliminating possible duplication.

4.2 NRC LER SYSTEM

1. The proposed LER rule requiring a narrative description of a reportable event and encoding it into the Sequence Coding and Search System (SCSS) is well suited for the identification of significant events which require in-depth studies. This assumes removal of any ambiguities regarding the definition of reportable events, and assumes that the utilities will provide an accurate and complete report. Although the proposed LER Rule does not necessarily provide a structured narrative of the event, it generally represents an important step toward the development of such a comprehensive data base.

2. The LERs are being used by many different groups, such as: NRC contractors, BNL, ORNL and INEL; EPRI-NSAC and INPO; NRC regional offices, program offices, and staff offices; utilities; Nuclear Power Experience (Petroleum Information Corp.); as well as foreign organizations such as the French Institute for Protection and Nuclear Safety, the West German Gesellshaft für Reaktorsicherheit, and the Commission of European Communities (CEC) Joint Research Center (JRC) at Ispra, Italy. The LER reports are exchanged with the OECD countries under the auspices of the Committee for Safety of Nuclear Installations (CSNI) for such purposes as trend and precursor analyses, reliability analyses and human error rate determination. In many cases these groups are using only the abstracts without the detailed supplements which accompany the LER for analyses. The LERs are being used although there may be deficiencies because these event reports are the only ones which exist in the public domain.

3. One of the prime requirements of an LER for it to be useful for trend analysis or accident precursor study is that it represent a factually complete account of the event with an accurate description of the sequence of events, including quantitative data relevant to the event. There should be economic and safety incentives to the utilities for complete and accurate reporting. The LER reporting system should be used as a data base for trend and accident precursor analysis and reliability analysis.

4. If consistent narrative LERs could be prepared and encoded in the SCSS format by utility personnel, then utility personnel should have the prime responsibility for its encoding. If this is not possible, the encoded LER in the SCSS which has been done by NRC staff or NRC contractor staff should be sent to the plant staff for review and comment before considering the encoded LER to be in a final form.

4.3 INCIDENT PLANT RECORDER (IPR)

Operator action during an event is currently reconstructed for the LER by memory, log entries, and in some cases with the aid of a process computer or strip chart recorders. Under some stressful events, it may be difficult to accurately reconstruct operator action. The requirement for accurate reconstruction of events could, thus, be aided significantly by an automatic recording of event-specific plant parameters and plant component status by an Incident Plant Recorder (IPR) with features similar to the flight recorder in the airline industry.

Electricité de France (EdF), the French utility with twenty-three operating 900 MWe nuclear power plants and eleven 900 MWe and seventeen 1300 MWe NPP under construction, has or is installing an automatic computerized plant parameter monitoring and recording system, KIT (see Appendix J) in each of their 900 MWe nuclear power plants. The objective of this system is to aid in plant operation and in the reconstruction of incidents or events. They are also backfitting to each plant a Safety Parameter Display System (SPDS) with a data link to EdF headquarters.

For their 1300 MWe NPP, EdF has developed and is implementing an integrated reactor protection system called SPIN (Système de Protection Integre Numerique -- Digital Integrated Protection System (see Appendix J)), which includes a logic and analog variable data monitoring and recording system (KIT), a safety parameter display system (SPDS), and a nuclear data link (NDL) to EdF headquarters. Consideration is also being given to extend the NDL to CEA-IPSN, the technical arm of the French Safety Authority (Service Central de Sûrete des Installations Nucléaires (SCSIN)). The 1300 MWe KIT system monitors and records approximately 5,000 logic variables and about 1,200 analog variables as a function of time on a permanent basis. Logic variables are those which indicate such conditions as position of valves and control rods, pump operation, limit switch action, circuit breaker action, etc., whereas analog variables are those which measure such quantities as temperature, pressure, flow rates, neutron flux, water level, etc. Since EdF found it difficult to select *a priori* which variables might be required to reconstruct an incident or event, they chose to monitor and record almost all logic and analog variables available in the control room. EdF estimates that the R&D costs were about $700,000 and the hardware costs about $560,000 for the SPIN system. Since the terminals for the logic and analog variables already exist in the control room, they do not include costs due to wiring from the sensors.

The French KIT system and the FAA/NTSB flight recorder systems with parametric data, and the latter also with voice recording, may be used as guides in the development of an Incident Parameter Recorder (IPR) for automatically recording event parameters at nuclear plants to aid in reconstructing events.

An IPR to provide time-dependent plant parameters such as thermal-hydraulic and neutronic parameters could be developed in conjunction with the proposed Safety Parameter Display System (SPDS). The SPDS, as described by NUREG-0696 which BNL studied, has key reactor plant parameters brought to a central CRT. Since a SPDS is required in the future for all nuclear plants (SECY-82-111b), it appears to be a logical step to require the SPDS to record and store the plant parameters in a standard format for ease in event reconstruction. The information could be stored for a reasonable time and then erased if no significant event has occurred. If an event does occur, the computer could store the quantitative data and make them available in a predetermined form for NRC and INPO analysis.

Discussions with a vendor indicated that it would be a relatively easy matter to attach a parameter recording device so that the values of key parameters from just preceding an event to termination of the event could be stored. One specific SPDS has provision for indicating the action of approximately 400 key plant components such as pumps and valves. An IPR, similar to a flight recorder in the airline industry, that preserves the time sequence action of these parameters from just preceding the event to termination of the event would enable an analyst to reconstruct accurately the important operator actions during this period.

Another vendor indicated that his SPDS system already incorporates an automatic 16 hour 2 second interval input recording system for all 150-500 inputs. There does, however, appear to be some ambiguity in NRC requirements for a SPDS; therefore, there is some hesitancy on the part of utilities to implement an SPDS. Early clarification of NRC requirements for SPDS is highly desirable.

Discussions with the representatives of the commercial airline industry and its regulatory agency, reference Appendix I, indicated that the raw parametric data may not capture the color of the event. In this case the NTSB relies heavily on the voice recorder to fill in the needed happenings (through a narrative form). The concept of voice recording of the operators should be considered as a part of the IPR.

There does not currently appear to be a requirement that utilities have the capability of automatically recording key plant parameters just preceding and during the course of a significant event in a unified manner, although SECY-82-111b appears to imply that parameters required to reconstruct an event must be collected and stored in the Technical Support Center. If ANSI/ANS 4.6 Standard on "Functional Criteria for Data Acquisition and Recording for Transient Reconstruction in Nuclear Power Plants" becomes established and adopted in the near future, the standard could be used as a basis for an event data collection and storage requirement. An industry and NRC consensus is needed to determine the plant parameters and their accuracy, which should be recorded and reported in a standard format to facilitate reconstruction of event scenarios. A starting point for this consensus may be the BNL recommended parameters. The utility should be required to maintain recorded event data for some period of time after the event, such as for a minimum of about three years, unless otherwise requested by NRC or INPO.

4.4 DATA SOURCES

1. There currently exist various sources of qualitative and quantitative data which, together with the narrative LER and SCSS, could be used for multivariate analysis to form the basis for trend analysis and accident precursor study. These include INPO's NPRDS, INPO's plant specification file, utility plant incident reports, NRC Resident Inspector inspection reports, NRC-sponsored seismic and dynamic qualification for plant equipment data bank (INEL), In-Plant Reliability Data System (IPRDS) at ORNL, and the utility maintenance records upon which IPRDS is based.

2. The Institute of Nuclear Power Operations (INPO) has taken over the management of the Nuclear Plant Reliability Data System (NPRDS), a system essential for the development of a reliability data base for safety-related components of nuclear power plants. Although the NPRDS has been in operation since about 1974, there was a significant drop in the reporting of component malfunctions or failures in the last two or three years by the utilities from over 1500/yr in 1976 and 1977 to 860 in 1980 and 755 in 1981. INPO's assuming

the management of NPRDS is an attempt to strengthen the reporting of the component malfunctions or failures. It is important that all nuclear power plants be included in the reporting system. Although INPO currently has agreements with 47 out of 55 utilities for voluntary participation in the NPRDS program, there is some concern among the NRC staff that the utilities will not fully provide input into the NPRDS. Recent information from NPRDS, however, indicates that the utilities may have begun to more fully report failures, since the reported component failures for the first half of 1982 total 1,182. INPO has identified about 7,000 components (safety-related pumps, valves, etc.) out of a total of about 35,000 components per plant, whose specifications and operating status will be routinely monitored and tested for failures or malfunctions. Ambiguities apparently still exist regarding the definitions of failures and components which cause uncertainties on what should be reported. In addition, the NPRDS is limited in scope, and systems such as the vital HVAC, and air conditioning and control and Class 3 systems are not included in the system. These ambiguities appear to lead to a significant number of component malfunctions or failures that are unreported. There is, therefore, need to establish uniform criteria and consistent application of these criteria for the reporting of component malfunctions or failures for utility guidance. A uniform definition of a component and its boundaries is also very important. INPO has developed working plans for the collection, storage and evaluation of NPRDS data with this requirement in mind; however, it is premature at this time to judge the progress of this program. NRC currently carries out periodic audits of this program. Continued careful auditing of the NPRDS program is essential.

3. EdF has developed and is implementing a well coordinated, realistic reliability data acquisition system for all of their nuclear power plants (see Appendix J for details). The system called Systéme de Recueil de Données de Fiabilité (SRDF) routinely monitors approximately 800 components per two NPP at each nuclear power station. (EdF builds multiple, i.e., paired, NPPs at each site.) EdF has assigned one engineer on a full time basis to monitor the 800 components per two NPP. Three types of data are collected at each site and stored in a central computer facility. The three types of data for each of the components are: (1) component description and engineering characteristics,

(2) yearly, operating history including demands, and (3) failure information which is obtained each time a work order has been initiated for each component. In 1981 the SRDF file received about 1,000 component failure reports (300 for valves, 300 for pumps, and 400 for other components) from six plants per year, or about 170 component failure reports per plant per year. This number can be compared to 1,182 component failures reported to NPRDS during the first half of 1982 from about 62 operating plants (i.e., about 34 failure reports per plant per year). In comparing these numbers it should be recognized that SRDF includes approximately 400 components per plant, while the existing reportable scope of NPRDS includes about 4,000 components per plant.

4. The Commission of European Communities (CEC), Joint Research Center (JRC) at Ispra, Italy has a program called European Reliability Data System (ERDS), which is a centralized computer based system for collecting and organizing information related to the operation of LWRs (see Appendix K). ERDS has four main data banks: Component Event Data Bank (CEDB) for component reliability data; Abnormal Occurrence Reporting System (AORS) for incident reports; Operating Unit Status Reports (OUSR); and Generic Reliability Parameter Data Bank (GRPDB).

The CEDB contains technical specifications, operational histories, failure, repair, and maintenance action data for components. The data from about 2,000 components are currently in CEDB from five power plants, with about 500 failure reports on these components as a pilot program. JRC would like to monitor between 1000-2000 components from each plant for CEDB.

In addition to providing a service as a data bank for operating data for LWRs for the European Community, the JRC staff of about 7-10 people also conducts analysis of the AORS data which will have about 1,500 events in a homogenized AORS data bank by the end of 1983. They have tried multi-variate analysis methods on human errors or failures with the AORS data, but did not find anything significant because of the lack of data. They plan to use multivariate analysis on component failures as well as other statistical analysis techniques on the data in CEDB.

5. NRC contractors, when conducting detailed analysis of real or hypothetical events, have experienced considerable difficulty in obtaining plant

specific as-built component and system specifications from utilities and vendors. In some cases, this is because of unavailability of as-built engineering drawings at utilities, or proprietary status of some vendor data.

NRC-RES has a program with Technology Development of California (TDC) and INEL to develop a computer program for storing plant-specific component and system as-built engineering specifications. At the present time this system contains plant-specific data for one PWR. NRC-RES is initiating a program at INEL to obtain plant-specific data for six additional plants for inclusion in this computer system. The plant-specific design data should be from current or up-to-date plant specifications.

6. During this study, BNL has found many sources of nuclear power plant data, as shown in Table 5, as well as RES and NRR programs where data useful for licensee event evaluation are being developed. It does not appear to be the lack of data, but rather the accessibility and the resources to analyze the data, which is lacking. Where applicable, the data should be incorporated into a centralized data file such as the SCSS so that all the data to form a complete picture of an event is in one place.

7. There appear to be a number of different data banks in operation or being initiated. There should be coordination, but not necessarily consolidation, of the various data banks to avoid duplication of effort, and to have a common component identification format and output format for ease in application to LER trend analysis and accident precursor study.

8. One of the most important pieces of information regarding an important safety-related component failure is the time at which failure or abnormal operation occurred, and the length of time this component was unavailable. It is also equally important to know whether a redundant component was operational during the time the first component was out of service. The operational time history of important safety-related components currently does not appear to be collected by INPO or NRC. This type of data should be included in the NPRDS.

TABLE 5

DATA SOURCES

Type/Name	Source
1. Detailed Plant Specifications	Utility Architect-Engineer Vendor
Computerized Plant Specifications	TDC-INEL
2. Maintenance Records	Utility
In-Plant Reliability Data System (IPRDS)	ORNL-NSIC
3. Licensed Operating Reactor Status Summary Report NUREG 0020	Utility NRC
4. Nuclear Plant Reliability Data System (NPRDS)	INPO-SWRI
5. Licensee Event Report (LER)	NRC-AEOD
Sequence Coding & Search System (SCSS)	ORNL
6. Significant Event Report (SER)	INPO - SEE-IN
Significant Operating Experience Report (SOER)	
7. Plant Incident Report	Utility
8. Corrective Action Report	Utility
9. Resident Inspector's Inspection Report	NRC-I&E
10. Seismic and Dynamic Qualification of Mechanical and Electrical Equipment	INEL
11. Environmental Qualification of Mechanical and Electrical Equipment	Franklin Res. Inst.
12. Radiation Release and Exposure	Utility NRC
13. Meteorological Data	Utility

4.4 DATA ANALYSIS

1. Component malfunction or failure (such as those in the NPRDS and IPRDS data bases), inappropriate operator action, and certain exogenous factors must be treated on a statistical basis. Appropriately adapted multivariate analyses of events, plant parameters and operational data (including procedural and exogenous information) can aid in identifying trends and precursors of deteriorating performance and accidents. Such analyses also enable a more comprehensive view of individual, interplant and plant ensemble performance, and thus facilitate coordinated, effective control of safety problems by the utilities (and review by the NRC).

2. The analysis of significant events where multiple component or system failures occur, coupled with inappropriate operator action, should be analyzed on an engineering basis using realistic thermal-hydraulic and neutronic computer codes as required. The physics (e.g., neutronics, thermal-hydraulics) of nuclear plant performance are well understood, and accurate deterministic analysis can currently be performed up to the time of fuel damage, assuming plant specific data are available. Deterministic analyses would aid in identifying and understanding unusual or abnormal events.

3. Although EdF will be collecting large quantities of operating data through their KIT system, they are only using the KIT data for aid in reconstructing events. Neither the EdF Department of Operation and Nuclear Safety (DONS) staff nor the CEA-IPSN's Services d'Analyse de Sûrete des Reacteurs (SASR) appear to have developed any sophisticated statistical analysis techniques to routinely analyze the logic and analog variable data to be collected at their NPPs. EdF conducts conventional statistical analysis with their SRDF reliability data. They attempt to do trend and precursor analysis with their data in the significant event file. EdF estimates that they have about 2,000 events per 23 plants per year, of which about 200-300 are significant events. Of these they estimate that 150-250 are due to reactor trips, since all reactor trips are considered significant events.

4. One of the key factors in being able to determine event trends and precursors of accidents is in having highly competent and plant system knowledgeable engineers to conduct analysis of the LERs. They must have the

capability to communicate directly with plant operating personnel to clearly determine the event sequence or scenario to aid in determining the cause and required corrective action.

5. The NRC is considering a requirement that the utilities make a probabilistic risk assessment (PRA) for each operating nuclear power plant under the National Reliability Evaluation Program (NREP). In conducting a PRA study, it is necessary to develop a detailed event tree/fault tree analysis and, in some cases, failure mode and effect analysis (FMEA) for each plant. The availability of this analysis, together with the component or system failure or operator error reported in the LER, would provide a mechanism for identifying significant events (SE). The component failure or operator error would identify a particular tree. The probability of other malfunctions or errors in this tree would determine the seriousness of the reported LER. This approach would aid nuclear engineers analyzing LERs in the identification of SE.

6. An In-Plant Reliability Data System (IPRDS) based on the analysis of maintenance records of six nuclear power plants has been initiated at ORNL under NRC sponsorship. Currently only the data on pumps and valves have been encoded in IPRDS. The thorough analyses of maintenance records of all nuclear plants would provide a valuable data base for component reliability determination. There should be coordination between the INPO NPRDS and ORNL IPRDS programs, since the data complement each other.

4.5 DATA COLLECTION AND ANALYSIS RESPONSIBILITY

1. The collection, analysis (including trend and statistical analysis), and corrective action for component failure, system malfunctions and operator error, resulting in reportable events, should be the primary responsibility of the utilities and INPO on an industry-wide basis. They have personnel who are most familiar with the components, systems and operating characteristics of the plant and have direct access to plant operating personnel to determine most easily the event scenario and event cause. In addition, they can most quickly and efficiently take corrective action.

One large utility that BNL interviewed has organized an Office of Nuclear Safety, reporting to the CEO, to do precisely the above to meet post-TMI requirements. This group has access to plant incident reports which represent reports on all incidents in the plant and which become the basis for reportable LERs. It also has access to operator logs and maintenance records. These records represent more complete data for trend and precursor analysis and reliability analysis if performed. The results of the utility analysis could be provided to INPO for industry-wide dissemination and trend analysis. It is premature at the present time to judge the efficacy of this utility approach to trend and precursor analysis.

INPO has indicated it plans to analyze licensee events on an industry-wide basis with its SEE-IN program (originated at EPRI-NSAC), which produces significant event reports (SER) and significant operating event reports (SOER) for dissemination on an industry-wide basis. Again, it is premature to judge its effectiveness since it has only recently gotten started.

2. If the utility and INPO programs are successful and readily available, NRC need only act in an audit function, which could include independent analyses of selected significant events, to insure compliance with this program.

3. The analysis of the collected data, whether conducted by NRC and its consultants, INPO, or the utilities, will, however, require a significant increase in program support because of the increased number of analysts required, as well as the current cost of neutronic and thermal-hydraulic analysis. NRC-RES has on-going programs for the development of interactive fast running nuclear power plant analyzers. The fruition of these research activities in one or two years will provide the tools for considerably less expensive analysis of neutronic and thermal-hydraulic phenomena applicable to some of the events.

5. CONCLUSIONS

1. Accurate and complete narrative descriptions, including event scenario and quantitative data, are essential for the analysis of events. A comprehensive event analysis data base may take three to five years in development and implementation. Although the proposed LER Rule does not necessarily provide a structured narrative of the event, it generally represents an important step toward the development of such a comprehensive data base.

2. For statistical and deterministic analyses, significant improvements would have to be made in the collection of relevant nuclear power plant performance data immediately preceding and following some events. The types of quantitative data required for some event analyses have been scoped using a data matrix approach. Much of this event-specific parametric data needs to be collected and stored at the plant, available when required for in-depth event analysis, but not necessarily reported in each LER.

3. Although much event specific data are currently being collected at most plants, collection of such data in a more systematic manner and more easily amenable for event reconstruction and analysis could be accomplished by installing at each nuclear plant an Incident Parameter Recorder (IPR), possibly including a voice recorder, similar to a flight recorder on aircraft.

4. The utilities are the key to the collection and analysis of operational and event specific data in a complete and accurate manner. Event analysts, whether they are NRC staff or contractors or INPO staff, must be knowledgeable about the details of nuclear power plants and must have the capability of directly contacting plant operations staff for accurate reconstruction of events.

5. The LER system should provide economic and safety incentives for complete and accurate reporting and analysis. The utilities may benefit from LER and component reliability data collection and analysis by proving the reliability of their plant systems, for example, if longer time intervals for in-service inspection and testing become acceptable.

6. Improved coordination of the various reliability and event-related (NRC and industry) data banks, which have or are being established so that they

use the identical definition of components, component boundaries, and component failures, and have the same or compatible formats, is important to improve event and reliability analysis.

7. EdF, the French utility, has developed an integrated automatic computer-based operating data monitoring, recording (KIT), and display (SPDS) system (see Appendix J) with a nuclear data link (NDL) to headquarters to aid operation during normal and abnormal conditions and for the reconstruction of events. This integrated system is being implemented on all of their 1300 MWe PWRs. Hardware with the same capability is being backfitted or installed on all of their 900 MWe PWRs as well. In addition, EdF has developed a well-coordinated reliability data acquisition system (SRDF) to be implemented on all of their PWRs to aid in design, component maintenance, and to increase plant reliability.

8. When the backfitting with the improved KIT and SPDS systems is complete on their nuclear plants, EdF will be collecting large quantities of logic and analog variable data on a continuous basis. Except for incident reconstruction, EdF does not currently have any plans for routine analysis of the large quantities of available operating data, possibly because of the effort required. The large quantities of analog and logic variable data which will be available would be well suited for statistical analysis using such techniques as multivariate analysis to search for incident precursors. As a minimum, the data from each incident (about 2000 incidents per year from 23 reactors, which includes significant events -- about 200-300 per year per 23 reactors) should be processed statistically with previous incidents in addition to deterministic analysis. The integration of SRDF (reliability data) analysis with KIT incident data analysis would improve incident precursor and trend analysis.

In order to minimize the effort required, computer-assisted data scanning and analysis methods can and should be developed to scan the large quantities of data off-line for statistical analysis to identify abnormal operator procedures, abnormal component or system action. Routine scanning and assessment of human and component operation should be able to detect and alert operations staff to the precursors of such events as that which occurred at the Salem Nuclear Power Station.

9. The CEC-JRC at Ispra, Italy has developed a well coordinated integrated reliability data, operating history, and incident report acquisition system (ERDS) (see Appendix K) for the European community. This system makes possible the easy retrieval of component failure, repair, and maintenance information, together with component specifications and operating history, incident report and analysis, and reactor operating history from one system for an integrated analysis. The ERDS can be interrogated in a systematic way for identical or similar component or human failure and/or incident characteristics to aid the analyst conduct statistical analysis. In addition to conventional deterministic analysis, they plan to use statistical analysis techniques, such as multi-variate analysis on component failures, human errors and abnormal events in the ERDS data bank to identify accident precursors and trends, assuming funding resources are available.

APPENDIX A

ORGANIZATIONS CONTACTED

ORGANIZATIONS CONTACTED

U. S. Nuclear Regulatory Commission

- Office of Analysis and Evaluation of Operational Data
- RES Division of Risk Analysis
- NRR Division of Licensing
- Office of Inspection and Enforcement
- Region III Office

U. S. Nuclear Regulatory Commission Contractors

- ORNL - NSIC
- INEL
- Sandia National Laboratory

Other Government Agencies

- NASA Johnson Space Center, Reliability Division
- National Bureau of Standards, Engineering Statistics Division
- National Transportation Safety Board
- Federal Aviation Administration

Utilities

- Commonwealth Edison
- Northeast Utilities
- EPRI - NSAC
- INPO (NPRDS, SEE-IN)

Industry

- Westinghouse
- Combustion Engineering
- Technology Development of California
- Petroleum Information Corporation

Aircraft Industry

- United Aircraft
- TWA
- Delta
- Pan American
- Eastern
- ARINC
- Los Alamos Technical Associates
- AERO Data Inc.
- Trans Systems Corp.

Foreign Agencies

- Gesellshaft für Reaktorsicherheit
- Electricité de France
- Institute for Protection and Nuclear Safety (CEA), France

Consultants

- Joseph R. Fragola, Science Applications Inc.
- Donald P. Gaver, Naval Post Graduate School
  American Statistical Association
- Joseph H. Levine, Reliability Division, NASA

APPENDIX B

MATRIX ANALYSIS

APPENDIX B - MATRIX ANALYSIS

The matrices are organized in the following manner:

- Reactor Type - all Boiling Water Reactors then all Pressurized Water Reactors
- System/Parameter - for each Major Plant Function, namely

  I. Nuclear Systems

  II. Engineered Safety Systems

  III. Containment

  IV. Electrical Systems

  V. Power Conversion Systems

  VI. Process Auxiliary Systems

  VII. Plant Auxiliary Systems

  VIII. Plant External

There are plant systems and associated parameters for which there are columns in each matrix as follows: AVAILABILITY, PARAMETER LOCATION, USES.

For the USES columns, please note the following explanation. These columns indicate the data types and typical statistical methods which enter the further analysis in a matrix framework relating reactor, plant and exogenous parameters and "events". The notation is defined below. Several explanatory remarks should be noted.

1. The data types and statistical methods listed are the ones that appear most suitable initially. In the course of the work more (or less) detailed data and techniques may arise.
2. Not all events or event classes require the same (or same amount of) variates, or type of analysis. In each case (or class of cases) the appropriately adapted statistical inputs and methods must be used. In particular, clearly different types of treatment are called for in at least the following cases:

   (i) events involving physical perturbations of the primary system, such as, for example, LOCAs.

(ii) "administrative" events, which do not affect primary system performance, such as, for example, violations of certain technical specifications relating to ESFs which do not lead to any untoward physical effects; and

(iii) events which do not affect primary system performance, but which involve degraded or anomalous physical behavior of some kind (including human error).

In events of type (i) essentially the entire gamut of available parameters must enter the initial considerations, though deeper and more extended investigation should eventually lead to more discriminating and restricted data requirements.

For events of type (ii) the situation is different. While detailed information on the particular system involved is required, additional information will generally only be called for on associated, neighboring, and related equipment.

The case of type (iii) events is intermediate, and the useful and usable data inputs will depend strongly on the specifics of the incident.

In all cases, however, the full gamut of general plant external data may need to be included.

With each set of columns in each matrix (Availability, Parameter Location and Uses) a fourth set of columns, examples for deterministic evaluation has been provided. The events that head the vertical columns are abbreviated and the asterisks indicate that a definition of these events can be found in this appendix.

NOTATION

Data Types - Statistical

Nominal	N
Binary/Polytomic	B
Ordinal	O
Interval	I
Ratio	R

Data Types - Physical

Constant	K
"Historic"	H
Dynamic	V

Statistical Methods

Categorical (Discriminatory & Graphical)	DG
Associative	A
Correlative	C
Time Series	T

These terms are described in detail in Appendix C entitled "Statistical Analyses".

Parameter Location and Availability

Indicates Location and Availability	X

*USES

LB LOCA	Large Break Loss of Coolant Accident
SB LOCA	Small Break Loss of Coolant Accident
SGTR	Steam Generator Tube Rupture
CRDA	Control Rod Drop Accident
ATWS	Anticipated Transient Without Scram

I. MAJOR PLANT FUNCTION: NUCLEAR SYSTEMS BOILING WATER REACTOR

SYSTEM/PARAMETER	AVAILABILITY/LOCATION							EXAMPLES OF USES						
	AVAIL NOW	LOC/CONTOL ROOM		RECORD METHOD		NOT RECORDED	ALARM IN CONTROL ROOM	LB* LOCA	SB* LOCA	CRDA*	TURB TRIP*	ATWS*	DATA TYPES	STATIS ANALYS
		IN	OUT	AUTO	MAN									
REACTOR CORE/VESSEL														
Parameter														
1. Neutron Flux								X	X	X	X	X	R,V	A,C
- Source Rng Mon & Pos.	X	X		X			X	X	X	X	X	X	R,V	A,C
- Int Rng & Position	X	X		X			X	X	X	X	X	X	R,V	A,C,T
- Avg Power Rng Monitor	X	X		X			X	X	X	X	X	X	R,V	A,C,T
2. Reactor Water Level	X	X		X			X	X	X	X	X	X	R,V	A,C,T
3. Reactor Water Temp	X	X		X			X	X	X	X	X	X	R,V	A,C
4. Reactor Pressure	X	X		X			X	X	X	X	X	X	R,V	A,C,T
5. Radioactivity	X		X		X			X	X	X	X	X	R,V	A,C
6. Core Temperatures						X							R,V	A,C,T
7. Core Flow						X							R,V	A,C,T
8. Water Chemistry	X		X		X			X	X	X	X	X	R,V	A,C
9. Metal Temperature														
- Upper Flange	X	X		X									R,V	A,C
- Lower Head						X							R,V	A,C
- Transition Piece						X							R,V	A,C
CONTROL ROD DRIVE SYSTM														
Parameter														
1. Control Rod Position	X	X		X				X	X	X	X	X	R,V	A,C
2. System Status	X		X			X		X	X	X	X	X	B,H,K	DG,T
3. Scram Disc Vol Level	X	X				X	X	X		X		X	B,H,K	DG,T
RECIRCULATION SYSTEM														
Parameter														
1. System Status	X		X			X		X	X	X	X	X	B,H,K	DG,T
2. Recirculation Pmp Spd	X	X				X		X	X	X	X	X	R,V	A,C,T
3. Flow	X	X			X			X	X	X	X	X	R,V	A,C,T

I. MAJOR PLANT FUNCTION: NUCLEAR SYSTEMS (cont'd)

BOILING WATER REACTOR

SYSTEM/PARAMETER	AVAILABILITY/LOCATION: AVAIL NOW	LOC/CONTOL ROOM: IN	LOC/CONTOL ROOM: OUT	RECORD METHOD: AUTO	RECORD METHOD: MAN	NOT RECORDED	ALARM IN CONTROL ROOM	EXAMPLES OF USFS: LB* LOCA	SB* LOCA	CRDA*	TURB TRIP*	ATWS*	DATA TYPES	STATIS ANALYS
STANDBY LQD CONTL SYSTM														
Parameter														
1. Storage Tank Level	X		X			X	X	X	X	X	X	X	B,H,T	DG,T
2. Storage Tank Temp	X		X			X	X	X	X	X	X	X	R,H	A,C
3. System Status	X		X			X		X	X	X	X	X	B,H,K	DG,T
RESIDUAL HEAT REMVL SYSM														
Parameter														
1. System Mode	X	X	X			X	X	X	X	X	X	X	B,H,K	DG,T
2. System Status	X					X		X	X	X	X	X	B,H,K	DG,T
3. Heat Exchng Out Temp	X	X			X			X	X	X	X	X	R,V	A,C
4. System Flow						X	X	X	X	X	X	X	R,V	A,C
5. Heat Exchanger Flow						X		X	X	X	X	X	R,V	A,C
REACTOR PROTECTION SYSTM														
Parameter														
1. System Status	X	X		X				X	X	X	X	X	B,H,K	DG,T
REACTOR CONTROL SYSTEM														
Parameter														
1. Mode Switch Position	X	X			X			X	X	X	X	X	B,H,K	DG,T

II. MAJOR PLANT FUNCTION: ENGINEERED SAFETY SYSTEMS

SYSTEM/PARAMETER	AVAILABILITY/LOCATION							EXAMPLES OF USES						
	AVAIL NOW	LOC/CONTRL ROOM IN	LOC/CONTRL ROOM OUT	METHOD OF RECORDING AUTO	METHOD OF RECORDING MAN	NOT RECRD	ALARMED IN CONTL ROOM	LB* LOCA	SB* LOCA	CRDA*	TURB TRIP*	ATWS*	DATA TYPES	STATIS ANALYS
REACT CORE ISOLAT COOLING (Or Isolation Condensor)														
Parameter														
1. System Status	X					X		X	X	X	X	X	B,H,K	DG,T
2. System Flow	X	X				X		X	X	X	X	X	R,V	A,C
3. System Temp	X		X			X		X	X	X	X	X	R,V	A,C
4. Isol Cond Shell Side water Level	X	X				X	X						R,V	A,C
5. Isol Condensor Valve Position	X	X				X	X						B,H,K	DG,T
HIGH PRESSURE COOLANT INJECTION														
Parameter														
1. System Status	X					X		X	X	X	X	X	B,H,K	DG,T
2. System Flow	X	X		X				X	X	X	X	X	R,V	A,C,T
3. System Temp	X	X		X				X	X	X	X	X	R,V	A,C
LOW PRESSURE COOLANT INJECTION														
Parameter														
1. System Status	X					X		X	X	X	X	X	B,H,K	DG,T
2. System Flow	X	X		X				X	X	X	X	X	R,V	A,C,T
3. System Temp	X	X		X				X	X	X	X	X	R,V	A,C
LOW PRES CORE SPRY														
Parameter														
1. System Status	X					X		X	X	X	X	X	B,H,K	DG,T
2. System Flow	X	X		X				X	X	X	X	X	R,V	A,C,T
3. System Temp	X	X		X				X	X	X	X	X	R,V	A,C
AUTO DEPRESSURIZATION SYSTEM														
Parameter														
1. Safety Valv Pos						X		X	X	X	X	X	B,H,K	DG,T
2. ADS Valve Pos	NT(1)	X				X		X	X	X	X	X	R,V	A,C,T
3. Flow Thru Valve						X		X	X	X	X	X	R,V	A,C,T
4. System Status	X					X		X	X	X	X	X	B,H,K	DG,T

(1) NT = Near term availability.

III. MAJOR PLANT FUNCTION: CONTAINMENT

SYSTEM/PARAMETER	AVAILABILITY/LOCATION: AVAIL NOW	LOC/CONTRL ROOM: IN	LOC/CONTRL ROOM: OUT	METHOD OF RECORDING: AUTO	METHOD OF RECORDING: MAN	NOT RECRD	ALARMED IN CONTL ROOM	EXAMPLES AND USES: LB* LOCA	SB* LOCA	CRDA*	TURB TRIP*	ATWS*	DATA TYPES EVENTS	STATIS ANALYS
DRYWELL Parameter														
1. Pressure	X	X		X				X	X	X	X	X	R,V	A,C
2. Temperature	X	X		X				X	X	X	X	X	R,V	A,C
3. Sump Levels	X		X		X		X	X	X	X	X	X	R,V	A,C
4. Airborne Radioactivity Level	X		X	X				X	X	X	X	X	R,V	A,C
5. H2,O2,N2 Concetration, as Appl	X	X		X				X	X	X	X	X	R,V	A,C
6. Spray Flow							X	X	X	X	X	X	R,V	A,C,T
7. Effluent Radioactivity	X	X		X				X	X	X	X	X	R,V	A,C
WETWELL (Suppression Pool, Torus) Parameter														
1. Water Level	X	X		X				X	X	X	X	X	R,V	A,C
2. Water Temp	X	X		X				X	X	X	X	X	R,V	A,C
3. Spray Flow	X	X				X	X	X	X	X	X	X	R,V	A,C,T
ISOLATION Parameter														
1. MSIV Valve Pos	X	X			X			X	X	X	X	X	B,H,K	DG,T
2. System Status	X					X		X	X	X	X	X		
CONTAINMENT SYSTMS Parameter														
1. H2 Recomb Stat	X					X							B,H,K	DG,T
2. Purge Syst Stat	X					X							B,H,K	DG,T
3. Containment Ventilation System	X					X							B,H,K	DG,T
SECONDARY CONTAINMENT (Reactor Bld) Parameter														
1. Pressure	X		X				X	X	X	X	X	X	R,V	A,C

BOILING WATER REACTOR

IV. MAJOR PLANT FUNCTION: ELECTRICAL SYSTEMS

	AVAILABILITY/LOCATION							EXAMPLES AND USES						
SYSTEM/PARAMETER	AVAIL NOW	LOC/CONTRL ROOM		METHOD OF RECORDING		NOT RECRD	ALARMED IN CONTL ROOM	LB* LOCA	SB* LOCA	CRDA*	TURB TRIP*	ATWS*	DATA TYPES	STATIS ANALYS
		IN	OUT	AUTO	MAN									
GENERAL Parameter														
1. Breaker Position	X	X	X		X	X							B,H,K	DG,T
2. Voltages	X	X	X		X	X							R,V	A,C,T
3. Currents	X	X	X		X	X							R,V	A,C,T
EMERGENCY POWER Parameter														
1. Diesel Gen Status	X	X	X		X		X						B,H,K	DG,T
2. Diesel Generator Fuel Supply	X		X		X								B,H,K	DG,T
3. Battery & Inverter Status	X					X	X						B,H,R	DG,T
LIGHTING Parameter														
1. Status	X					X							B,H,K	DG,T
GENERATOR Parameter														
1. Gen Output (MWe)	X	X		X				X	X	X	X	X	R,V	A,C,T

BOILING WATER REACTOR

V. MAJOR PLANT FUNCTION: POWER CONVERSION SYSTEM

SYSTEM/PARAMETER	AVAILABILITY/LOCATION							EXAMPLES AND USES						
	AVAIL NOW	LOC/CONTRL ROOM IN	LOC/CONTRL ROOM OUT	METHOD OF RECORDING AUTO	METHOD OF RECORDING MAN	NOT RECRD	ALARMED IN CONTL ROOM	LB* LOCA	SB* LOCA	CRDA*	TURB TRIP*	ATWS*	DATA TYPES	STATIS ANALYS
MAIN STREAM Parameter														
1. Stream Flow	X	X		X				X	X	X	X	X	R,V	A,C,T
2. Main Stream Isolation Valve Leakage Control Systm Pres	X	X			X								R,V	A,C
CONDENSATE/FEEDWATER SYSTEM Parameter														
1. Feedwater Flow	X	X		X				X	X	X	X	X	R,V	A,C,T
2. Condensate Storage Tank Level	X	X			X								R,V	A,C,T
TURBINE BYPASS SYSTM Parameter														
1. Bypass Valve Pos	X	X				X		X	X	X	X	X	B,H,K	DG,T
2. Bypass Flow	X	X				X		X	X	X	X	X	R,V	A,C

BOILING WATER REACTOR

VI. MAJOR PLANT FUNCTION: PROCESS AUXILIARY SYSTEMS

SYSTEM/PARAMETER	AVAILABILITY/LOCATION							EXAMPLES OF USES						
	AVAIL NOW	LOC/CONTRL ROOM		METHOD OF RECORDING		NOT RECRD	ALARMED IN CONTL ROOM	LB* LOCA	SB* LOCA	CRDA*	TURB TRIP*	ATWS*	DATA TYPES	STATIS ANALYS
		IN	OUT	AUTO	MAN									
OFF-GAS SYSTEM														
Parameter														
1. Off-gas Systm Stat	X		X	X				X	X	X	X	X	B,H,K	DG,T
2. Effluent Radioact	X	X		X				X	X	X	X	X	R,V	A,C
LIQUID RADWASTE SYSMS														
Parameter														
1. Systems Status	X		X			X		X	X	X	X	X	B,H,K	DG,T
2. Storange Tank Levels	X		X		X			X	X	X	X	X	R,V	A,C
3. Effluent Radioact	X	X		X			X	X	X	X	X	X	R,V	A,C
SERVICE WATER SYSTEMS														
Parameter														
1. System Status	X												B,H,K	DG,T
2. Water Temperature	X		X			X							R,V	A,C
3. System Flow			X			X								
4. Effluent Radioact	X	X		X			X							
REACTOR BUDG. CLOSED COOLING Parameter														
1. System Status	X												B,H,K	DG,T
2. Water Temperature	X		X		X								R,V	A,C
3. System Flow			X			X							R,V	A,C
4. Effluent Radioact	X	X		X			X							

VII. MAJOR PLANT FUNCTION: PLANT AUXILIARY SYSTEMS

SYSTEM/PARAMETER	AVAILABILITY/LOCATION: AVAIL NOW	LOC/CONTRL ROOM: IN	LOC/CONTRL ROOM: OUT	METHOD OF RECORDING: AUTO	METHOD OF RECORDING: MAN	NOT RECRD	ALARMED IN CONTL ROOM	EXAMPLES OF USES: LB* LOCA	SB* LOCA	CRDA*	TURB TRIP*	ATWS*	DATA TYPES	STATIS ANALYS
FIRE PROTECTION Parameter														
1. System Status	X					X							B,H,K	DG,T
COMMUNICATIONS Parameter														
1. System Status	X					X							B,H,K	DG,T
CONTROL ROOM HVAC Parameter														
1. System Status	X					X							B,H,K	DG,T
SEISMIC Parameter														
1. Accelerometer Output	X		X	X									R,V	A,C

VIII. MAJOR PLANT FUNCTION: PLANT EXTERNAL

SYSTEM/PARAMETER	AVAILABILITY/LOCATION: AVAIL NOW	LOC/CONTRL ROOM: IN	LOC/CONTRL ROOM: OUT	METHOD OF RECORDING: AUTO	METHOD OF RECORDING: MAN	NOT RECRD	ALARMED IN CONTL ROOM	EXAMPLES OF USES: LB* LOCA	SB* LOCA	CRDA*	TURB TRIP*	ATWS*	DATA TYPES	STATIS ANALYS
RADIATION MONITORING Parameter														
1. Radioactivity at Licensed Release Pnts	X	X	X	X				X	X	X	X	X	R,V	A,C
2. Radioactivity at Plant Perimeter	X		X		X			X	X	X	X	X	R,V	A,C,T
METEROROLOGY Parameter														
1. Wind Direction	X		X	X				X	X	X	X	X	R,V	A,C
2. Wind Speed	X		X	X				X	X	X	X	X	R,V	A,C
3. Atmospheric Stability (Vertical Temperature Differences)	X		X	X				X	X	X	X	X	R,V	A,C

I. MAJOR PLANT FUNCTION: NUCLEAR SYSTEMS — PRESSURIZED WATER REACTOR

AVAILABILITY/LOCATION — EXAMPLES OF USES

SYSTEM/PARAMETER	AVAIL NOW	LOC/CONTRL ROOM IN	LOC/CONTRL ROOM OUT	METHOD OF RECORDING AUTO	METHOD OF RECORDING MAN	NOT RECRD	ALARMED IN CONTL ROOM	LB* LOCA	SB* LOCA	SGTR*	TURB TRIP*	ATWS*	DATA TYPES	STATIS ANALYS
REACTOR CORE/VESSEL														
Parameter														
1. Neutron Flux														
- Source Range	X	X		X			X	X	X	X	X	X	R,V	A,C
- Intermediate	X	X		X			X	X	X	X	X	X	R,V	A,C
- Power Range	X	X		X			X	X	X	X	X	X	R,V	A,C,T
2. Reactor Water Level	NT(1)	X		X			X	X	X	X	X	X	R,V	A,C,T
3. Core Exit Temperature	X	X			X			X	X	X	X	X	R,V	A,C,T
4. Degrees of Subcooling	X	X			X			X	X	X	X	X	R,V	A,C
5. Water Chemistry	X		X		X			X	X	X	X	X	R,V	A,C
6. Core Flow	X	X		X			X	X	X	X	X	X	R,V	A,C,T
CONTROL ROD DRIVE SYSTEM														
Parameter														
1. Control Rod Position	X	X		X				X	X	X	X	X	R,V	A,C
2. System Status	X					X		X	X	X	X	X	B,H,K	DG,T
REACTOR COOLANT SYSTEM (RCS)														
Parameter														
1. RCS Hot Leg Temperature	X	X			X			X	X	X	X	X	R,V	A,C,T
2. RCS Cold Leg Temperature	X	X			X			X	X	X	X	X	R,V	A,C,T
3. RCS Average Temperature	X	X			X		X	X	X	X	X	X	R,V	A,C,T
4. Reactor Coolant System Pressure	X	X			X		X	X	X	X	X	X	R,V	A,C,T
5. Soluble Boron Concentration	X		X		X			X	X	X	X	X	R,V	A,C,T
6. RCS Radioactivity	X		X		X			X	X	X	X	X	R,V	A,C
7. Reactor Coolant Pump Status	X	X				X		X	X	X	X	X	B,H,K	DG,T
PRESSURIZER														
Parameter														
1. Pressurizer Level	X	X		X			X	X	X	X	X	X	R,V	A,C,T
2. Pressurizer Pressure	X	X		X			X	X	X	X	X	X	R,V	A,C,T
3. Pressurizer Temperature	X	X		X				X	X	X	X	X	B,H,K	DG,T
4. Pressurizer Heater Power	X		X		X			X	X	X	X	X	R,V	A,C
5. PORV Position						X		X	X	X	X	X	B,H,K	DG,T
6. PORV Flow						X		X	X	X	X	X	R,V	A,C
7. Pressurizer Quench Tank Level	X	X			X		X	X	X	X	X	X	R,V	A,C
8. Pressurizer Quench Tank Pressure	X	X			X			X	X	X	X	X	R,V	A,C
9. Pressurizer Quench Tank Temp.	X	X			X			X	X	X	X	X	R,V	A,C
10. Safety Valve Position						X		X	X	X	X	X	R,V	A,C
11. Safety Valve Flow						X		X	X	X	X	X	B,H,K	DG,T
12. Safety Valve/PORV Exhaust Temp.	X	X			X			X	X	X	X	X	R,V	A,C

(1) NT - Near term availability

PRESSURIZED WATER REACTOR

I. <u>MAJOR PLANT FUNCTION</u>: NUCLEAR SYSTEMS

	AVAILABILITY/LOCATION							EXAMPLES OF USES						
SYSTEM/PARAMETER	AVAIL NOW	LOC/CONTRL ROOM IN	LOC/CONTRL ROOM OUT	METHOD OF RECORDING AUTO	METHOD OF RECORDING MAN	NOT RECRD	ALARMED IN CONTL ROOM	LB* LOCA	SB* LOCA	SGTR*	TURB TRIP*	ATWS*	DATA TYPES EVENTS	STATIS *NALYS
<u>CHEMICAL AND VOLUME/</u>														
<u>EMERGENCY BORATION</u>														
<u>SYSTEM</u>														
<u>Parameter</u>								X	X	X	X	X	B,H,K	DG,T
1. System Status/Mode	X					X								
2. Boric Acid Charging								X	X	X	X	X	R,V	A,C
Flow	X	X			X									
3. Volume Control Tank														
Level	X	X			X		X	X	X	X	X	X	R,V	A,C
4. Makeup Flow	X	X				X		X	X	X	X	X	R,V	A,C
5. Letdown Flow	X	X					X	X	X	X	X	X	R,V	A,C
6. RCP Seal Flow in/														
out	X	X			X		X						R,V	A,C,T
7. Accumulator Level	X	X					X	X	X	X	X	X	R,V	A,C
8. Accumulator Pres-													R,V	A,C
sure	X	X					X						R,V	A,C
9. Accumulator Isola-														
tion Valve Position	X	X			X			X	X	X	X	X	B,H,K	DG,T
10. Refueling Water														
Storage Tank Level	X	X			X		X	X	X	X	X	X	R,V	A,C
<u>RESIDUAL HEAT REMOVAL</u>														
<u>SYSTEM</u>														
<u>Parameter</u>														
1. System Status	X					X		X	X	X	X		B,H,K	DG,T
2. System Flow						X	X							
3. System Radioactiv-													R,V	A,C,T
ity			X		X			X	X	X	X	X	R,V	A,C
4. RHR Heat Exchanger			X		X									
Outlet Temp	X							X	X	X	X	X	R,V	A,C
<u>REACTOR PROTECTION</u>														
<u>SYSTEM</u>														
Parameter								X	X	X	X	X	B,H,K	DG,T
1. System Status	X	X		X										

II. MAJOR PLANT FUNCTION: ENGINEERED SAFETY SYSTEMS

SYSTEM/PARAMETER	AVAILABILITY/LOCATION							EXAMPLES OF USES						
	AVAIL NOW	LOC/CONTRL ROOM		METHOD OF RECORDING		NOT RECRD	ALARMED IN CONTL ROOM	LB* LOCA	SB* LOCA	SGTR*	TURB TRIP*	ATWS*	DATA TYPES	STATIS ANALYS
		IN	OUT	AUTO	MAN									
LOW PRESSURE SAFETY INJECTION														
Parameter														
1. System Status	X	X				X		X	X	X	X	X	B,H,K	DG,T
2. System Flow	X	X			X		X	X	X	X	X	X	R,V	A,C,T
3. System Temp	X	X			X			X	X	X	X	X	R,V	A,C
HIGH PRESSURE SAFETY INJECTION														
Parameter														
1. System Status	X	X				X		X	X	X	X	X	B,H,K	DG,T
2. System Flow	X	X			X		X	X	X	X	X	X	R,V	A,C,T
3. System Temp	X	X			X			X	X	X	X	X	R,V	A,C
AUXILIARY FEED-WATER SYSTEM														
Parameter														
1. System Status	X	X				X		X	X	X	X	X	B,H,K	DG,T
2. System Flow	X	X			X		X	X	X	X	X	X	R,V	A,C,T
3. System Temp	X	X			X			X	X	X	X	X	R,V	A,C

PRESSURIZED WATER REACTOR

III. MAJOR PLANT FUNCTION: CONTAINMENT

	AVAILABILITY/LOCATION							EXAMPLES OF USES						
	AVAIL NOW	LOC/CONTRL ROOM IN	OUT	METHOD OF RECORDING AUTO	MAN	NOT RECRD	ALARMED IN CONTL ROOM	LB* LOCA	SB* LOCA	SGTR*	TURB TRIP*	ATWS*	DATA TYPES	STATIS ANALYS
GENERAL														
Parameter														
1. Pressure	X	X		X			X	X	X	X	X	X	R,V	A,C,T
2. Temperature	X	X		X				X	X	X	X	X	R,V	A,C,T
3. Sump Water Level	X	X			X		X	X	X	X	X	X	R,V	A,C
4. Radioactivity	X		X	X			X	X	X	X	X	X	R,V	A,C
ISOLATION														
Parameter														
1. Isolation Valve Positions	X	X			X			X	X	X	X	X	B,H,K	DG,T
CONTAINMENT SYSTEMS														
Parameter														
1. Purge System Status	X					X	X	X	X	X		X	B,H,K	DG,T
2. Containment Spray Flow	X	X			X			X	X	X		X	R,V	A,C
3. H2,O2,N2 Concentration	X		X		X			X	X	X		X	R,V	A,C
4. Effluent Radioactivity	X		X		X			X	X	X		X	R,V	A,C
5. Containment Ventilation System Status	X					X		X	X	X			B,H,K	DG,T
6. Ice Condenser System Status	X					X							B,H,K	DG,T
7. H2 Recombiner System Status	X					X	X						B,H,K	DG,T

IV. MAJOR PLANT FUNCTION: ELECTRICAL SYSTEMS

	AVAILABILITY/LOCATION							EXAMPLES OF USES						
SYSTEM/PARAMETER	AVAIL NOW	LOC/CONTRL ROOM IN	LOC/CONTRL ROOM OUT	METHOD OF RECORDING AUTO	METHOD OF RECORDING MAN	NOT RECRD	ALARMED IN CONTL ROOM	LB* LOCA	SB* LOCA	SGTR*	TURB TRIP*	ATWS*	DATA TYPES	STATIS ANALYS
<u>GENERAL</u>														
<u>Parameter</u>														
1. Breaker Positions	X	X	X		X	X							B,H,K	DG,T
2. Voltages	X	X	X		X	X							R,V	A,C,T
3. Currents	X	X	X		X	X							R,V	A,C,T,
<u>EMERGENCY POWER</u>														
<u>Parameter</u>														
1. Diesel Generator Status	X	X	X		X		X						B,H,K	DG,T
2. Diesel Generator Fuel Supply	X		X		X								B,H,K	DG,T
3. Battery & Inverter Status	X					X	X						B,H,R,	
<u>LIGHTING</u>														
<u>Parameter</u>														
1. Status	X					X							B,H,K	DG,T
<u>GENERATOR</u>														
<u>Parameter</u>														
1. Generator Output (MWe)	X	X		X				X	X	X	X	X	R,V	A,C,T

V. MAJOR PLANT FUNCTION: POWER CONVERSION SYSTEMS

SYSTEM/PARAMETER	AVAILABILITY/LOCATION							EXAMPLES OF USES						
	AVAIL NOW	LOC/CONTRL ROOM		METHOD OF RECORDING		NOT RECRD	ALARMED IN CONTL ROOM	LB* LOCA	SB* LOCA	SGTR*	TURB TRIP*	ATWS*	DATA TYPES	STATIS ANALYS
		IN	OUT	AUTO	MAN									
STEAM GENERATOR														
Parameter														
1. Water Level	X	X			X		X	X	X	X	X	X	R,V	A,C,T
2. Pressure	X	X			X		X	X	X	X	X	X	R,V	A,C,T
3. Dump Valve Position	X	X			X		X	X	X	X	X	X	B,H,K	DG,T
4. Dump Valve Flow	X		X			X		X	X	X	X	X	R,V	A,C
5. Vent Discharge Radioactivity	X		X		X		X	X	X	X	X	X	R,V	A,C
6. Safety Valve Position						X		X	X	X	X	X	B,H,K	DG,T
7. Safety Valve Flow						X		X	X	X	X	X	R,V	A,C
MAIN STEAM														
Parameter														
1. Steam Flow	X	X		X				X	X	X	X	X	R,V	A,C,T
CONDENSATE/ FEEDWATER														
Parameter														
1. Feedwater Flow	X	X		X				X	X	X	X	X	R,V	A,C,T
2. Condensate Storage Tank Level	X	X			X			X	X	X	X	X	R,V	A,C,T
TURBINE BYPASS SYSTEM														
1. Bypass Valve Position	X	X				X		X	X	X	X	X	B,H,K	DG,T
2. Bypass Valve Flow	X	X				X		X	X	X	X	X	R,V	A,C

VI. MAJOR PLANT FUNCTION: PROCESS AUXILIARY SYSTEMS — PRESSURIZED WATER REACTOR

SYSTEM/PARAMETER	AVAILABILITY/LOCATION							EXAMPLES OF USES						
	AVAIL NOW	LOC/CONTRL ROOM		METHOD OF RECORDING		NOT RECRD	ALARMED IN CONTL ROOM	LB* LOCA	SB* LOCA	SGTR*	TURB TRIP*	ATWS*	DATA TYPES	STATIS ANALYS
		IN	OUT	AUTO	MAN									
CONDENSED AIR REMOVAL SYSTEM														
Parameter														
1. Effluent Radioactivity	X	X		X			X						R,V	A,C
LIQUID RADWASTE SYSTEMS														
Parameter														
1. Systems Status	X					X							B,H,K	DG,T
2. Storage Tank Levels	X		X		X								R,V	A,C
3. Effluent Radioactivity	X	X	X	X			X						R,V	A,C
SERVICE WATER SYSTEMS														
Parameter														
1. System Status	X					X							B,H,K	DG,T
2. Water Temperature	X					X							R,V	A,C
3. System Flow						X							R,V	A,C,T
4. Effluent Radioactivity	X	X		X			X						R,V	A,C,T
COMPONENT COOLING WATER SYSTEM														
Parameter														
1. System Status	X					X							B,H,K	DG,T
2. Water Temperature	X					X							R,V	A,C
3. System Flow						X							R,V	A,C,T
4. Effluent Radioactivity	X	X		X			X						R,V	A,C,T

PRESSURIZED WATER REACTOR

VII. MAJOR PLANT FUNCTION: PLANT AUXILIARY SYSTEMS

SYSTEM/PARAMETER	AVAILABILITY/LOCATION: AVAIL NOW	LOC/CONTRL ROOM: IN	LOC/CONTRL ROOM: OUT	METHOD OF RECORDING: AUTO	METHOD OF RECORDING: MAN	NOT RECRD	ALARMED IN CONTL ROOM	EXAMPLES OF USES: LB* LOCA	SB* LOCA	SGTR*	TURB TRIP*	ATWS*	DATA TYPES EVENTS	STATIS ANALYS
CONDENSED AIR REMOVAL SYSTEM														
Parameter														
1. Effluent Radioactivity	X	X		X			X						R,V	A,C
LIQUID RADWASTE SYSTEMS														
Parameter														
1. Systems Status	X					X							B,H,K	DG,T
2. Storage Tank Levels	X		X		X								R,V	A,C
3. Effluent Radioactivity	X	X	X	X			X						R,V	A,C
SERVICE WATER SYSTEMS														
Parameter														
1. System Status	X					X							B,H,K	DG,T
2. Water Temperature	X					X							R,V	A,C
3. System Flow						X							R,V	A,C,T
4. Effluent Radioactivity	X	X		X			X						R,V	A,C,T
COMPONENT COOLING WATER SYSTEM														
Parameter														
1. System Status	X					X							B,H,K	DG,T
2. Water Temperature	X					X							R,V	A,C
3. System Flow						X							R,V	A,C,T
4. Effluent Radioactivity	X	X		X			X						R,V	A,C,T

PRESSURIZED WATER REACTOR

VIII. MAJOR PLANT FUNCTION: PLANT EXTERNAL

SYSTEM/PARAMETER	AVAILABILITY/LOCATION							EXAMPLES OF USES						
	AVAIL NOW	LOC/CONTRL ROOM IN	LOC/CONTRL ROOM OUT	METHOD OF RECORDING AUTO	METHOD OF RECORDING MAN	NOT RECRD	ALARMED IN CONTL ROOM	LB* LOCA	SB* LOCA	SGTR*	TURB TRIP*	ATWS*	DATA TYPES	STATIS ANALYS
RADIATION MONITORING														
Parameter														
1. Radioactivity at all Licensed Release Points	X	X	X	X				X	X	X	X	X	R,V	A,C
2. Radioactivity at Plant Perimeter	X		X		X			X	X	X	X	X	R,V	A,C,T
METEOROLOGY														
Parameter														
1. Wind Direction	X		X	X				X	X	X	X	X	R,V	A,C
2. Wind Speed	X		X	X				X	X	X	X	X	R,V	A,C
3. Atmospheric Stability (vertical temperature differences)	X		X	X		X		X	X	X	X	X	R,V	A,C

USES | GENERAL

SYSTEM/PARAMETER	DATA TYPES	STATISTICAL ANALYSIS
SYSTEM STATUS POSITION FROM PWR/ BWR LISTS IS DEFINED AS FOLLOWS:		
1. Positions on all AOV's, MOV's and Dampers	B,H,K	DG,T
2. Positions on all Breaks	B,H,K	DG,T
3. Equipment Inservice	B,H	DG,T
4. Pump/Fan Vibration, Flow, Inlet and Outlet Pressure, Temperature	R,V	A,C
HUMAN FACTORS		
1. All Operator Actions	B,H	DG,T
2. Times of Actions and Events	R,V	A,C,T
EVENTS INFORMATION		
1. Sequence of Any Action/Event	O,V	DG,T
2. Equipment/Component Failures	B,H,K	DG,T
3. Causes of Failures	N	DG
4. External Events/Acts of Nature, Personnel	N	DG
5. Personnel Radiation Exposure	R	A,C
PLANT EXTERNAL DATA		
1. Additional Meteorological	R,V	A,C
2. Hydrological	R,V	A,C
3. Demographic	R	A,C
4. System Electrical Demands and Trends	R,V	A,C,T
HISTORICAL RECORDS		
1. Equipment Maintenance	H	DG,T
2. Equipment Test	H	DG,[illegible]

APPENDIX C

STATISTICAL ANALYSIS

CONTENTS
APPENDIX C: STATISTICAL ANALYSIS

APPENDIX C. STATISTICAL ANALYSIS

1. Introductory Remarks*

The objectives of an LER system are the elucidation and concomitant control of anomalous nuclear power plant behavior in order to ensure its safe operation both in the short and long term. In most cases this is intimately connected with the efficient and reliable power generating capacity of the plant, and the achievement of desirable levels of plant output over the long term is essentially inseparable from orderly safe operation.

The safety criteria apply both to static and dynamic plant characteristics, to short- and long-term behavior variations, and to intra- and inter-plant phenomena.

The factors underlying these criteria display a great variety and range of physical and statistical characteristics, and a systematic analysis of safety-related events thus requires a close and interactive application of a broad mixture of engineering and statistical methods. These must deal both with individual phenomena (using mainly engineering analyses), and with the aggregated data (using appropriate statistical techniques).

The judicious integration of such analyses enables a descriptive, prescriptive, and to a useful degree predictive representation of overall nuclear power plant behavior combining both deterministic engineering and statistical phenomenological features.

This chapter discusses (in relatively general terms) the main features and requirements of such integrated analyses. Section 2 describes the underlying data and nomenclature from both the statistical and engineering viewpoints, while Section 3 deals with the various analyses that can be carried out and

---

*A recent report entitled "Data-Related Issues in Nuclear Safety Analysis", prepared by the Data Subcommittee of the American Statistical Association Ad-Hoc Advisory Committee on Nuclear Regulatory Research (July 1982), has commented on the character and treatment of the data used in the analysis of nuclear plant safety problems. This appendix outlines the utilization (and development) of appropriate statistical methods, both standard and novel, which address many of the major concerns of this document in the context of the general integrated approach of the present study.

(some of) the results they may be expected to yield. Brief and somewhat schematic descriptions of the associated mathematical formulations are included here. A selected list of general and specific references is also included. Superscripts in the text indicate specific references where it seems appropriate.

2. Data and Nomenclature

In order to simplify and condense the following discussion, it is necessary to give a short description of the type of data considered, and to define the associated terminology. It is most convenient to start with the statistical aspects.

2.1 Statistical Nomenclature[14]

The data which appear in the analyses come in a variety of forms which call for different statistical and engineering treatments. The major division is between qualitative and quantitative data. Qualitative data may be subdivided into two classes:

a) Nominal variables are characterized simply by their names or types (e.g., PWR, BWR, GCR, ...; "on", "off", ...; etc.) and have no intrinsic or logical ordering or enumeration. In some cases it may be adequate to treat these variables as "concomitant observations",[9] i.e., they may simply be regarded as characterizing a class within which more detailed statistical and other calculations are carried out. In other situations, depending on the mechanisms involved and the questions that arise, it is necessary to include them in an integral way in the overall analysis, and it is then necessary to enumerate them, for example, by the introduction of artificial ("dummy") binary or other variates. The actual statistical manipulations which can then be executed are touched on later (see 3.3 below).

b) Ordinal variables are also qualitative, but have a natural ordering, for example, by size, class, etc. (without, however, reference to the absolute quantitative values). Such variables are directly assessible to a variety of quantitative statistical methods, using such methods as rank correlations.[7]

Quantitative data may also be subdivided into two classes:

c) Interval data are characterized by quantitative measures of equality of intervals or differences, and are thus accessible to most standard statistical techniques. However, since they have no absolute zero, and hence lack an absolute scale, no numerical relation can be established between the standard deviation (σ) and the mean (μ).

d) Ratio data are numerical data in the commonly understood mathematical sense, and are thus amenable to all statistical operations. (Their scale has an absolute zero, and thus the "coefficient of variation", $\sqrt{\sigma}/\mu$, can be defined.)

Two comments in particular are in order at this point. Firstly, it may be noted that each class of data defined above includes all the preceding ones, and depending on the need may be treated in greater or lesser detail. For example, interval data may be treated simply as ordinal data, or even as nominal data in applicable circumstances.

Secondly, as the following description of engineering data and terms shows, all these different data types appear in one or other context. It is therefore to be expected that a great variety of statistical techniques (involving greater or lesser complexity) must be called on to provide a proper statistical picture of the problems considered.

2.2 Engineering Data

The complex mass of engineering data which is eligible for consideration in these analyses is conveniently described under four interconnected (and to a degree overlapping) headings: equipment, functional systems, operational data, and "events".

a) Equipment comprises all structural and operating components on which records can separately be kept, such as pipes, vessels, pumps, valves, instruments, generator sets, invertors, etc. (In some cases, important "subcomponents" such as switches, filters, etc. may also be included.) The data available or accessible include:

i) qualitative static data such as manufacturer, type, cost, size, etc., and

ii) quantitative operational data such as age, duty, maintenance and repair cycles, number of failures, and date of last maintenance, etc.

b) Functional systems fall into two classes, for the present purposes, though again there is a degree of overlap.

i) The major functional systems consist of the primary system comprising the nuclear core, the steam generator and the associated controls (which also appear below) and, as appropriate, the secondary system supplying working fluid to the turbine-generator set. The parameters and operations of these systems are well defined and substantially completely deterministic in nature, and their role in statistical and other safety analysis is:

- To define limiting initial and boundary conditions which are (or may be) hazardous to major system operation and hence should be avoided; and

- in the event that such situations do arise, to prescribe the necessary operation of the plant safety systems (see (ii) below to rectify the situation.

ii) Associated and integrated with these major systems are a variety of safety systems, replete with redundant features, which are designed to avoid the potentially hazardous situations indicated in i) above, and to correct them when they do occur. These too are well defined engineering systems, with underlying deterministic character, but they are rarely amenable to complete quantitative deterministic analysis for the following reasons:

- the "on-off" (binary) nature of many of their operations;
- subsystem complexities and non-uniformities;
- parameter and variable uncertainties;
- the statistical nature of component degradation and failure;
- the role of inappropriate or erroneous procedures.

c) Operational data covers a great variety of different types of, and differently characterized (described) variables. They include:

i) exogenous data (e.g., meteorological information)
ii) plant state data (e.g., power level, refueling)
iii) quantitative major functional parameters (e.g., pressure, temperature

iv) quantitative and qualitative safety systems parameters (e.g., on-off status, fluid levels)

v) operating conditions (e.g., maintenance and repair activities).

All this information will generally be a function of time during any incident of interest.

Clearly, it is neither feasible nor necessary to utilize every available (or accessible) piece of information for either deterministic or statistical analysis. However, for the deterministic plant control, a substantial amount of (in principle) redundant and/or dependent information is highly desirable, if not essential, because the pattern it presents makes possible more rapid comprehension and control than would be possible using deductive procedures on minimal information.

For statistical analyses (whether retrospective or prospective), the situation is different. The introduction of a number of deterministically dependent variates into multivariate analyses ("multicollinearity") not only leads to mathematical difficulties, but when these are overcome, leads to results which are equivocal and often lacking in physical significance. For these investigations, therefore, it is important to restrict those variables which are deterministically related to a minimal set (see, however, Section 3.4). On the other hand, safety systems parameters and operating data which are subject to substantial uncertainties should be included to the extent feasible.

d) "Events" - In the light of the objectives stated in the Introductory Remarks, the main emphasis in the data and analyses must center on threats to safe plant operation. As already implied in (b) above, such threats are defined to a large extent by the behavior of the nuclear thermo-hydraulic (i.e., primary) system under conditions involving transients and/or LOCAs, though ancillary activities such as refueling, spent fuel storage and radioactive waste treatment also play a role.

Such system perturbations are in turn the results of certain initiators (events, event sequences or situations) to which the primary system is subjected and to which it is particularly sensitive.

In principle, the primary system response to such initiators is deterministic, and generally amenable to quantitative calculations, such as, for example, using the TRAC code. These calculations can serve to define critical and important initiators, and the associated static and dynamic primary system characteristics.

A number of such calculations have been carried out in a variety of contexts. However, not all possible initiators (and their effects) have been calculated or defined in this way, and a number of them are included on the basis of more restricted engineering and probabilistic evaluations (mainly based on event and fault tree analyses).

The relevant events themselves can (in the first instance) be defined in more practical detail in two ways:

i) The primary way is by the examination and codification of detailed plant and subsystem behavior during those incidents which lead (or potentially lead) to initiating sequences. In particular, this may be accomplished by the SCSS (Sequence Coding and Search System) now being exploited.

ii) A secondary method of definition, which is desirable for a broader and more comprehensive view, is to augment the SCSS by the addition of hypothetical events based on the so-called "dominant sequences" derived from the fault tree analyses of the individual plants. (These are subsets of overall anomalous plant behavior which contribute most substantially to dangerous primary system conditions.) This method can also be extended to include a number of other, more limited situations of general concern, such as, for example, multiple component or systems failures.

At the present state, "events" defined by either of these procedures are characterized by nominal data types. However, the dominant sequences could directly be put into ordinal form and the sequence coded, and general concern items could also be so treated when sufficiently complete fault tree analyses become available.*

*For conciseness, events described by the SCSS will be denoted by SCE, and those defined by "dominant sequences" or "general concern" by GCE.

3. Statistical Methods

3.1 General Comments

The previous discussion has already indicated that the physical nature of the systems and phenomena involved in nuclear plant operation, and their characterization, while intimately connected from an operational point of view, vary widely in their attributes and descriptions (both physical and mathematical). It is therefore not to be expected that a comprehensive analysis can be based on homogeneous data or on uniform methods, even if one is prepared to sacrifice physical significance to attain statistical homogeneity.(6)

Nevertheless, an extensive, illuminating and adequately quantitative statistical description of the overall situation can be attained by the application of appropriately adapted multivariate methods to the various aspects of the problem.

The remainder of this section addresses the statistical analysis of the (isolated) components (Subsection 3.2), and the treatment of the events in relation to the components, operational data, and time (3.3). Subsections 3.4 and 3.5 deal briefly with some peripheral, but important, potential applications of multivariate analysis to the major functional systems and to the question of system reliability in the (practical) competitive risk situation.

3.2 Component* Analysis (Equipment Analysis)

It is most convenient (and simplest) to begin by discussing the treatment of the components. Most of the presently available component data are nominal, and static in character, though there does exist statistical information on failure (and repair) rates, usually on a generic basis. The IPRD (and allegedly the NPRD) program will provide a substantial amount of quantitative information, particularly of a temporal character, dealing with maintenance, test and

*There is an unfortunate but unavoidable overlap of terminology in this subsection. "Component" denotes equipment "elements", e.g., pumps, etc., while "principal component" denotes a linear combination of variates (e.g., age, cost, etc.) which play a preferred and simplified role in the statistical analysis.

repair histories as well as some additional quantitative failure level data. In relation to the statistical analysis contemplated here, this will have to be augmented by specific dynamic performance and duty/maintenance cycle data.

This type of information lends itself directly to a gamut of multivariate analyses, including temporal as well as other features.* In particular, the first phase of such analyses will involve the search for principal components[6] (i.e., linear combinations of variates which characterize the overall statistical behavior of the data in a condensed and simplified way), and time series characteristics,[11] e.g., failure rate variations. Nominal (and ordinal) data will, in the first instance be treated as "concomitants", though as the data base increases it may prove desirable to quantify them by appropriate discriminatory techniques.

It is clearly desirable to put the component data into a "reduced" (e.g., principal component) form before embodying them into the more complex subsystems and events analyses. However, this should not be regarded as the last word involving the components. In more complex situations apparently unimportant component parameter combinations may play a non-trivial role, and the statistical format must therefore allow for the non-reduced data to be used as well as the analysis progresses.

From the viewpoint of the components alone, this collation and analysis will provide information on such things as failure rate of components and component types as a "function" of nominal characteristics (e.g., manufacturer, size, etc.), and of quantitative data such as operational cycles and life. Proceeding in the reverse direction, it should also be possible to obtain quantitative measures of association (clustering or grouping) of the nominal characteristics in terms of the performance variables of interest.[4]

In addition to its intrinsic importance, such information plays a significant role in the event analyses described below.

---

*There are indications that substantial parts of such analyses may be carried out by the IPRD and NPRD programs, in which case only the results and certain necessary elaborations and extensions need be addressed here.

3.3 Event Analysis

a) Introduction: The event analyses, in all their aspects, play a central role in establishing an overall explanatory (and, to a reasonable degree, predictive) picture of nuclear power plant operation on an individual level, as a time function, and in relation to inter-plant statistics.

The sequence coding method, SCSS, (briefly indicated in a previous section) provides an essential basis for a number of statistical (and in some cases deterministic) analyses ranging from the disriminatory (i.e., qualitative) to the largely quantitative.

The general method outlined below proceeds in two main stages which are designed to simplify and clarify the mathematical and statistical features of the problem, and to take fully into account the physical and deterministic aspects of the phenomena that occur.

b) Categorical Analysis: The first and very illuminating and useful stage in these analyses consists of the examination of these SCEs in relation to

- the plants in which they occur,
- their causes,
- their potential effects,
- GCEs (as defined above), and
- time.

Although these data are nominal, except for the time series, discriminatory[7] and graphical[2] techniques provide very effective tools for revealing important patterns of behavior, and possible event groupings which may facilitate the following more quantitative considerations. The time series analysis, of course, shows temporal variations in behavior and possible temporal trends.

c) Quantitative Approaches: The second, more comprehensive and quantitative stage of the analyses, involves the introduction of

i) generic (and, where available, plant specific) component parameters, and

ii) selected non-redundant plant operational data significant for plant performance and control.

The manner in which this is done depends to some degree on the results of b) above. If these results show a substantial amount of association (approximate correlation) between SCEs and GCEs, only the former need to be considered as "individuals" in the ensuing multivariate analysis. If such association is not found, it may be desirable, at least to begin with, to include the GCEs as individuals as well in order to explore more fully the statistical relations of the entire system.

A second initial simplification involves

i) identifying as factors any principal components which revealed themselves in the equipment analysis, and

ii) similarly, utilizing any grouping or clustering of the SCEs which showed itself in the categorical analysis, and carrying out the next stage of multivariate analysis separately on an intragroup (cluster) and intergroup (cluster) basis. This is shown schematically in 3.3(e).

Both these factor and cluster groups will, of course, be augmented by similar combinations based on engineering considerations.

Several comments must be made about these simplifications:

i) While important objectives of this approach are the improvement of mathematical tractability and the more rapid attainment of operational perspicuity, the factors and groups which emerge from the initial investigations must be carefully reviewed in the light of the underlying physical phenomena and those deterministic relations which are known to apply both to components and to system interactions. The appearance of inexplicable combinations requires detailed engineering and probabilistic studies, since they may be due to unrecognized dependencies. The identification of these may require that the relevant aspects of the statistical analysis be carried out in substantially greater detail.

ii) While the aggregated mass of statistical material which accumulates is large, and may thus appear readily amenable to "standard" multivariate techniques,[6] the preceding discussion has shown that both the individual data (events) and the variates are quite heterogeneous in nature (and, in fact, actual more limited studies so far carried out have confirmed this). They also involve a lot of nominal information. The reduction described earlier improves this situation, in that both the event clusters and variable factors (to the extent that they exist) may be expected to be much more homogeneous. This is at the cost of dealing with smaller members of "individuals" (i.e., clusters of events, or members of a cluster), which in turn means that the appropriate quantitative statistical methods involve "association" rather than "correlation"[4]; i.e., one is concerned with the "distance" or "similarity) between events rather than the correlation between variates. It has been shown, however,[4] that there is a close and logical connection between these two interpretations, and under appropriate circumstances, associative results can be translated (mathematically) to correlations in a meaningful way.

Another important avenue of analysis concerns temporal phenomena. These may be divided into long term (i.e., point data separated in time, and related to the individual events or groups of events) and the short term variations which occur during the "life" of a single event (i.e., from shortly before its onset until normal conditions have returned).

The long term time series may be analyzed both on an individual and multiple basis for temporal variations and trends. Of particular significance in the present context is the search (of the multiple time series) for recurrent or sequential series of events* which show an appreciable degree of correlation (either on an in-plant or interplant basis). This is an integral part of precursor studies, since such temporal patterns indicate a trend of deteriorating plant performance requiring remedial action of some kind.

*The term here includes the groups or clusters mentioned earlier.

The short term time variations, particularly of the operational data, may also serve to provide important statistical and deterministic information on reactor performance, especially in the light of the (previously identified) event and component factor relations. In fact, it should be possible to connect the mechanized output of such analyses interactively with the SPDS and DASS systems (see Appendix F) to effectuate speedier and preventive plant control.

There is an important final remark to be made regarding the role of the SCEs and the quantitative methods described above. By the nature of the SCSS there is the possibility of some subjective factors entering the definition of the SCEs. The application of the various quantitative methods outlined above (with their mass of objective data) serves to objectively confirm the appropriateness of the SCE identification, or perhaps, in some cases, to indicate any ambiguities or inconsistencies which can then be rectified.

d) Summary: The general statistical methods described above then yield the following types of information relative to safe plant performance.*

i) Categorization and discrimination of SCEs (sequence coded events) in relation to GCEs, perceived causes, conjectured consequences, plants, and as a function of time, and vice versa, i.e., the establishment of a comprehensive qualitative contingency table for these quantities.

ii) The identification of event and variable clusters (groupings) based on the above.

iii) "Factorization" or clustering of plant component data.

iv) Determination of quantitative associations between event clusters, component factors, operational and plant data.

v) Determination of quantitative associations within event clusters in relation to component, operational and plant data.

---

*Only major aspects of the results are listed here. With the potentially large mass of input information available, it is neither feasible nor appropriate to attempt a complete listing here. The matrix analyses outlined in Appendix B exemplify the type of data and methods to be employed.

vi) Examination, verification and explication of the <u>physical and engineering significance</u> of such groupings (and the attendant elimination or treatment of statistical multicollinearities).

vii) Conversion, where feasible, of quantitative associative relations to correlational form.

viii) Long term time series analysis to extract recurrences, sequences, and other aspects of possible precursor behavior.

ix) Analysis of short term dynamics of events in the framework of the previously developed statistical relations.

x) Integration of the results of (ix), if applicable, with SPDS and DASS parameters.

xi) Verification of the definition of the SCEs in the light of the qualitative and quantitative statistical relations developed above.

e) Statistical Analysis Schematics: The following discussion is designed to supplement in briefly, schematic, partly mathematical form the general description of the statistical analyses given in 3.3.

(i) The Connection Between Correlation and Association

Suppose that x_{ip} denotes the value of the p-th variate for the i-th individual (e.g., the age of a certain kind of pump in the i-th event). For "standard" multivariate analysis it is convenient to normalize these x_is so that their mean (over i) is 0

$$\sum_{i=1}^{n} x_{ip} = 0$$

and their dispersion unity

$$\frac{1}{n} \sum_{i=1}^{n} x_{ip}^{2} = 1$$

The correlation matrix R is defined by

$$R_{pq} = \frac{1}{n} \sum_{i=1}^{n} x_{ip} x_{iq}$$

(in matrix notation $R = X'X$, where X is the matrix (x_{ip}) and X' its transpose). R is a $v \times v$ matrix, v being the number of variates, $p,q = 1,\ldots v$.

The method of principal components searches for the characteristic vectors of R, with the largest characteristic values. These correspond to linear combinations of the form

$$y_{ui} = \sum_{p=1}^{v} b_{up}\, x_{ip}$$

such that one, or several ($<v$) account for most of the dispersion of the x_{ip}, viz.,

$$\sum_{u=1}^{w}\sum_{i=1}^{n} {y_{ui}}^2 \sim \sum_{p=1}^{v}\sum_{j=1}^{n} {x_{ip}}^2 = nv \qquad \text{with } w < v$$

Such vectors y_{ui} $u=1\ldots w$, then represent the variate which accounts for most of the dispersion of the x_{ip}, and in a statistical sense can represent most of what is going on.

This is the preferred procedure when the data are all quantitative and n, the number of individuals, is much larger than v, the number of variates.

If these conditions are not met, it is more convenient and revealing to place the accent on the individuals (e.g., events) and to examine their relation (in particular, their "distance") in terms of the aggregate of the variates.

One then proceeds in the reverse direction, forming the association matrix $Q = XX'$, i.e.,

$$Q_{ij} = \sum_{p=1}^{v} x_{ip}\, x_{jp}$$

(which is an $n \times n$ matrix). The distance between two events, i,j, is given by

$$\begin{aligned} {D_{ij}}^2 &= \sum_{p=1}^{v} (x_{vp} - x_{jp})^2 \\ &= Q_{vi} + Q_{ij} - 2Q_{ij} \\ &= 2(1 - Q_{ij}) \end{aligned}$$

(with appropriate normalization).* It has been shown[4] that the characteristic vectors of Q are directly related to those of R.

---

* i.e., with $Q_{ii} = 1$, etc.

Since the i,j enumeration can be arbitrary, this method is a very useful and appropriate tool for dealing with binary (and hence nominal) data.

(ii) Analysis of Components (Equipment)

In the first instance most of the nominal data (e.g., manufacturer, type, etc.) connected with equipment components must be taken as concomitant, and the different items analyzed separately. (Retrospectively, it may prove desirable to carry out an association analysis on different kinds of equipment to search for any unexpected similarities.)

The data then available fulfill most of the requirements for standard multivariate analysis. However, there is a certain amount of qualitative data involved, and this is best treated (in a partially concomitant manner) by simply constructing a qualitative contingency table, i.e., for a given piece of equipment (e.g., pumps), examining the quantitative data in the light of manufacturer and plant. If any particular pattern reveals itself, either a separation or a grouping may be called for in the following analysis.

Basically, one can carry out a multivariate analysis on the n individuals, with variates such as cost, age, duty cycle, number of failures and other quantitative measures. It may be that significant "principal components" are found for one or another piece of equipment, either in aggregate or for one or other of the concomitant classes. For example, one might find for a certain kind of pump that 90% of the variation is accounted for by a combination of "failure rate", (-) "age", (+) "cost"; this combination may then conveniently be used for further analyses as a single variate, unless clear cut reasons to the contrary arise.

(iii) Event Analysis

The event analysis involves both qualitative and quantitative aspects and rests strongly on graphical and associative methods. While quantitative techniques eventually tend to subsume more qualitative approaches, at the present stage the latter are essential because of the ability to display multidimensional features of the problem and indicate patterns of relationships.

Figure 1 shows one possible (completely hypothetical) pictorial representation of a series of events, characterized on the one hand by the major effect

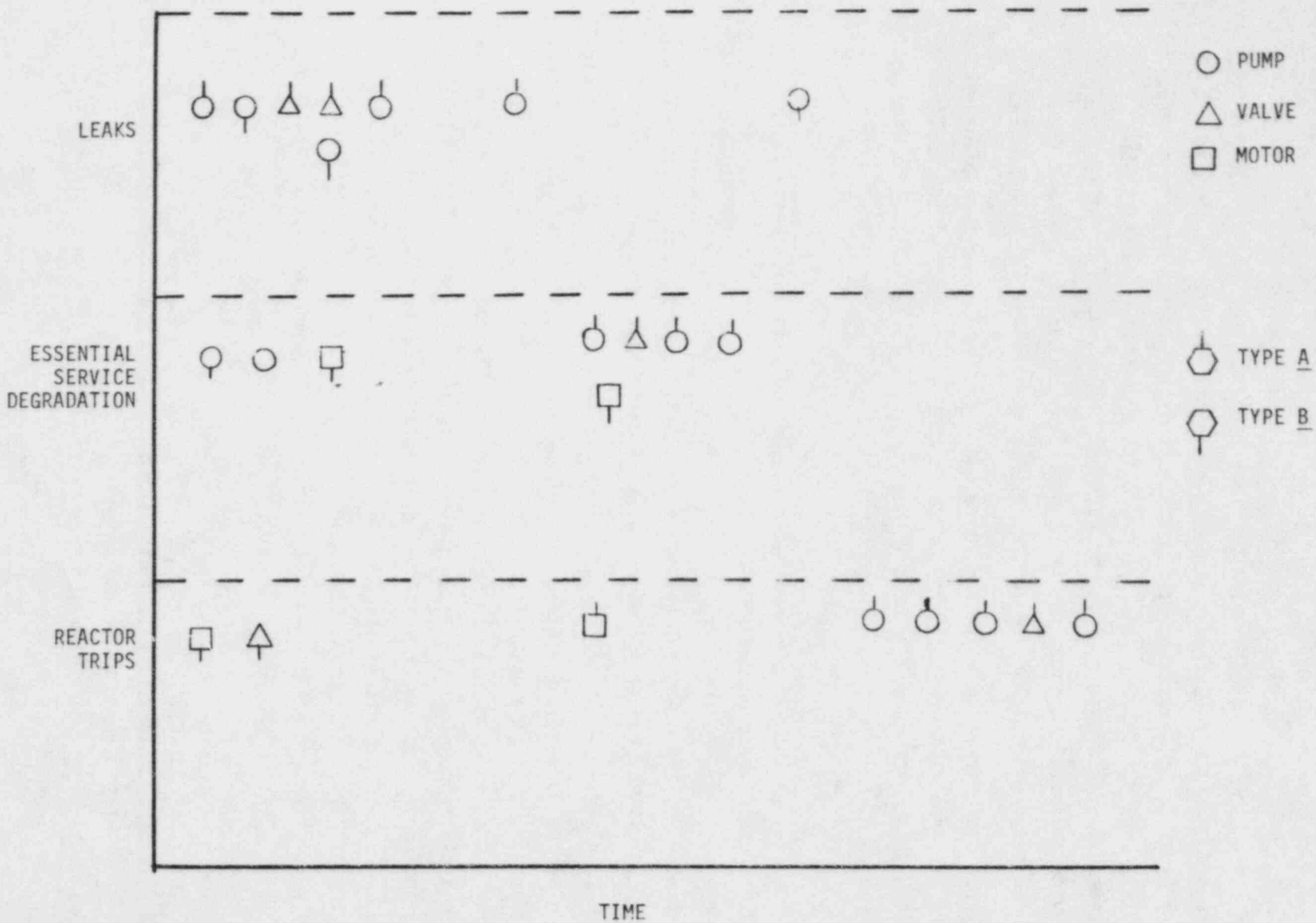


FIGURE 1. SCATTER DIAGRAM FOR ONE KIND OF DEFICIENCY PATTERN

occurring, and on the other hand by the component, type of plant, time, etc. involved. In the speculative sequence of events pictured in the figure, there is a clear trend of system deterioration in Type A plants involving pumps and valves. Further patterns might be revealed using more complex symbols (arrows, slanted lines, different sizes, etc.).[2,9] Representations of this type provide an immediate guide to the construction of qualitative contingency tables and groupings for use in the initial associative evaluations.

In order to proceed further, more quantitatively, some type of arbitrary (but preferably binary or 2^n-ary or polytomic) enumeration of the qualitative data must be introduced.* One may thus construct a statistical "observation" matrix

$$x(i,s)$$

where i is the individual (usually event) identifying index variable, constructed, for example as indicated above; while s identifies variates which may be qualitative (and translated to 2^n-ary form), clustered or factored, as determined by the component (equipment) analysis, or by preliminary graphical study (as above) and direct quantitative measurement.

As indicated in 3.3(c) above, the aggregated mass of $x(i,s)$, and in particular the number of individuals i, may appear to be large enough to attempt standard multivariate analysis, at least over the long term. Over shorter periods this is not likely to be the case, nor are the many intrinsically qualitative and heterogeneous characteristics of the $x(i,s)$ likely to take kindly to the indiscriminate and promiscuous application of standard multivariate techniques.** Instead, it is appropriate to proceed in four steps, which in their totality fully reveal the important statistical features of the $x(i,s)$ system, but yet do not attempt the indiscriminating application of standard methods. These steps are as follows:

---

*If desired, such an enumeration can be mapped in a unique and statistically useful (if physically opaque) way on to the interval (0,1) using Rademacher series.

**See particularly the relevant comments in Refs. (4) and (6).

i) Based on graphical and/or physical analysis of the data, the individual and variate sets, i,s, may be divided up into significant groups, clusters or classes (see, however, Section 3.3(e)) I_α, S_v, which are associatively analyzed as groups ($\Sigma I_\alpha \equiv i, \Sigma S_v \equiv s$).

ii) Within each (or some) of these groups, a similar associative analysis may be carried out, guided by graphical and physical considerations.

iii) Based on the results so obtained, correlation analyses may be carried out using the quantitative variables available to establish more detailed quantitative connections where possible.

iv) For many of the initial investigations the time of the incident may simply be taken as one of the variates s. However, to complete the global picture of the overall system behavior, it will be desirable to examine the various significant or interrelated groupings as time series to determine

- temporal fluctuations
- changing failure rates, and
- varying subsystem relationships.

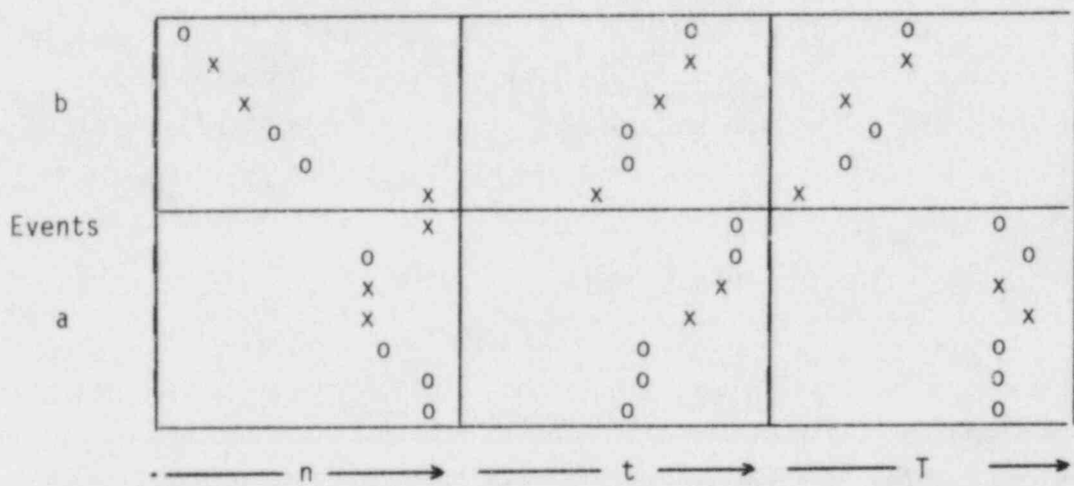
The results of such procedures are, in principle, equivalent to the (relatively) exhaustive analysis of the statistical matrix x(i,s). However, instead of automatically applying standard multivariate techniques at one fell swoop, they involve reliance on measured stages of analysis, each one taking full advantage (or cognizance) of the physical and mathematical limitations of that stage.

To the extent that they exist, statistical dependencies, temporal trends, interplant patterns, and other aspects of systems behavior will manifest themselves in a particularly natural way in such an approach.

e) Hypothetical Example: The statistical analyses described above cover a large range of incidents, input data and mathematical techniques, and it is possible to clarify the approach by means of a completely hypothetical example, which illustrates the multi-step, multi-faceted nature of the analyses (in a greatly simplified way.)

Consider sets of events involving, for example, loss of offsite power (a), and fires due to transformer failure (b) during some fixed period of time. The data available for each incident will include the plant, the plant type (PWR, BWR), plant size, age, power level, outside temperature, time of day (or shift), time since last maintenance, number of maintenance men around, and a plethora of other information. For the present simplified discussion, only a <u>few</u> of these variables will be regarded as statistical variates.

The <u>first</u> step consists of a purely qualitative (categorical) view of these events. This may be displayed in a contingency table, but more comprehensively by means of a graphical plot as shown below.



n = number of maintenance men around
t = number of days since last maintenance
T = outside temperature

o = BWR
x = PWR
each symbol represents <u>one</u> event

This figure (which may be regarded as part of a much larger one, or as part of a more comprehensive set) shows a number of important statistical features by simple inspection:

i) There does not appear to be any significant difference between BWRs and PWRs in regard to the events, <u>a</u>,<u>b</u>, insofar as the influences of n,t and T are concerned;

ii) the only common influence on events a and b appears to be t - both a and b events occur when t exceeds half the range plotted;

iii) events a occur preferentially for large n, while the reverse is true for events b;

iv) events a occur preferentially for higher T.

In addition to introducing more variates (such as n,t,T,...), further (qualitative) structure can be introduced into such a display by the use of complex symbols, e.g., larger ones for older plants, and further elaborations (e.g., $\phi\theta$) to denote manufacturers, etc.

This first step serves to focus attention on the more prominent features of the statistical relations, and enables some discrimination to be exercised in the more quantitative following steps: in particular, it may provide a heuristic justification for initially restricting some of the quantitative calculations to separate classes of events and variates.

If there are a large number of events i of a certain type (or apparently influenced by some variates p) and if x_{ip} represents the value of p in event i, their standard multivariate techniques (see Appendix C 3.3(e)) may be applied to the matrix $X = ((x_{ip}))$ to search for linear combinations of the variates which account for most of the observed statistical variation. For example, in the context of the (highly simplified) case cited earlier, one may find for i belonging to class a, that the combination .5n + 2T (ignoring normalization) represents most of the variation in $((x_{ip}))$. This combination may then not only serve as a new (and simpler) variable for further statistical manipulation, but also indicates that restrictions need to be placed on the amount of maintenance activities in warm weather to reduce (statistically) the chance of events a (LOSP).

If the number of events of a given class is not large, while the number of variates p remains substantial, it becomes more appropriate to measure the "distance" or "association" between the events. Mathematically this is tantamount to interchanging the roles of i and p, and physically it means that one is now characterizing the "causes" (variates) in terms of the similarity of their "effects" (events). For example, adverting to the earlier case again, one may find that the classes of events a and b are associated insofar as t (time since last maintenance) and, for example, plant power are concerned, but not in relation to maintenance activities and outside temperature.

These two types of approaches can be mathematically translated into each other, but usually only one or the other has physical significance.

The final, and to some degree crucial steps in the statistical analyses involve the examination of the time series of the events and event classes, both as individuals and in relation to each other. This process may also be carried out at various levels, beginning with the graphical (cf Appendix C, Figure 1). The importance of this aspect lies in its manifestation of changes in plant and system behavior, and in its "predictive" ability, in particular in facilitating the identification of "precursors" to more serious incidents.

It should be pointed out that all these methods, from the graphical through the most elaborate multivariate correlative or associative analysis, are completely adaptable to mechanized computational methods. In fact, the initial, apparently qualitative approaches may be usefully quantified as the amount of data increases.

3.4 Statistical Approach to Major Plant Functions

The original discussion emphasized the deterministic nature of the primary system and its role in "simply" providing definitions of initiating events, and corresponding well-defined ancillary quantitative physical information. In fact, the situation is somewhat more complicated. The primary system behavior is indeed deterministic, but its analysis and quantification are often clouded by static and dynamic parametric uncertainties and mathematical and computational model approximations.

It is well known that the performance of complex systems can be elucidated by examining the input-output relation when the systems are subject to statistical input disturbances.[1] In the present case the actual measurements provide such data, and the comparison of the experimental and calculated relations can serve to better define parametric uncertainties, indicate model deficiencies (if any), and reveal sensitivities that might not have been manifest from initial theoretical calculations.[10] In particular, long term structural deterioration can be more readily recognized by combining such statistical studies with appropriate non-destructive testing.

3.5 Competing Risk Applications

a) General Discussion: The term "competing risk problem" is used to denote studies of any failure process in which there is more than one distinct cause or type of failure present. In most of the LERs, a number of failures take place over a certain time period, resulting in either some type of system failure or transition from a normal operating state to an unacceptable state. The events described by Sequence Coding and Search Procedures (SCSP), SCEs, should fall in this category. The resulting failure state denoted by the event is due to a particular cause, traceable by engineering analysis. This cause may be a single component failure or, more realistically, a combination of various component and operator failures. Categorization of similar events, i.e., events resulting in similar failure states, will possibly reveal different failure causes (or modes). Also, many events may provide partial information, i.e., the event may not have progressed up to the failure state, but augmented by the assumption of one or more component and/or operator failures, could have resulted in the failure state. In addition, one may include sequences causing such failures obtained from fault tree/event tree type of analysis. In looking at this situation, one may argue that these multiple failure causes are operating simultaneously on the system, and a particular failure cause resulting in the failure will preclude the observation of a failure due to any other cause. Based on this type of observation, one would obtain different failure times along with a cause of failure among several possible causes of failure. One easy example is that of events resulting in reactor scram. Analyzing these events, it is possible to obtain various causes or failure modes resulting in the reactor scram and the corresponding operating time.

Over and above the engineering analysis performed to group analyze these events and group them based on the failure state observed or the potentiality of reaching the failure state, statistical analysis may be used to answer certain questions. One may be interested in assessing the importance of each of the causes assumed to act independently and/or the interactive effects of sets of failure causes. The theory of competing risk analysis provides a framework to do this type of analysis based on the analysis of failure data with competing causes of failures. The inherent assumption in such an analysis is that all the various causes are competing to fail the system and the occurrence of the first failure causes results in the failure state. Such an approximation appears to be well applicable in reactor systems.

The competing risk theory has been widely applied in the clinical, epidemiologic, demographic and basic science literature.(13) Application of this theory to reactor systems will possibly require extension of the general methodology in certain areas. Subsection (b) provides certain aspects of the competing risk theory in a more mathematical framework. Specifically, it discusses the basic statistical relationship underlying the competing risk model development and its application to three types of problems. These are:

a) Estimation of the probability density of the failure state due to each of the failure causes,

b) study of the failure distribution if one or more of the failure causes is removed, and

c) obtaining the "net probability" or the hypothetical probability of the failure state, if only specific cause is present. This assumes dependence among various failure causes and shows their importance in the context of the failure state being studied.

b) <u>Reliability and Competing Risk Analysis</u>

The following discussion provides a more mathematical framework for the previous remarks. The literature on competing risks is quite extensive, and no attempt is made here to be comprehensive. Rather, it attempts to provide the basis of such an analysis and discusses particular problems it may address. The discussion here primarily follows Sather's[13] review work and uses his notations.

Let T be the random variable denoting the time to reach the failure state, and let $F_T(t)$ be its cumulative distribution function. It will be assumed that $F_T(t)$ has a continuous derivative given by $f_I(t)$, called the probability density function. The relation between $f_T(t)$ and $F_T(t)$ is given by

$$f_T(t) = \frac{dF_T(t)}{dt}$$

Let $\mu(t)$ be a function on the time scale t, such that $\mu(t)\Delta t$ is the conditional probability that the system will fail between t and $t + \Delta t$, provided it has not failed up to time t. The function $\mu(t)$ is commonly known as the <u>hazard rate</u> or failure rate in the reliability literature and is called the <u>mortality rate</u> in the biological literature.

Standard reliability literature provides the relationship among the hazard rate, the probability distribution function and the probability density function. The relevant important functional relationship among these variables is as follows:

$$\mu(t) = - \frac{f_T(t)}{1 - F_T(t)}$$

$$f_T(t) = \mu(t) \exp\left[- \int_0^t \mu(s)ds \right]$$

$$R(t) = 1 - F_T(t) = \exp\left[- \int_0^t \mu(s)ds \right]$$

where R(t) is the probability that the system will not reach its failure state up to time t and is called its <u>reliability</u>.

i) Estimation of the Probability Density of the Failure State Due to Each of the Failure Causes

In competing risk theory, one studies the various failure causes responsible for the failure state, along with the distribution of failure time. Let $S_1, S_2, \ldots, S_k$ denote k possible failure causes, where S_i can be a combination of failures, both component and operator failures, instead of a single failure. Also, let Y_j be the random variable denoting the potential time of failure from cause S_j, $j=1,2,\ldots,k$. The occurrence of the failure cause, S_j, precludes observation of any other failure cause, and thus, the potential time of failure Y_j is the time of failure if only the failure cause S_j is operating.

For a given failure state, let us assume that $Y_1, Y_2, \ldots, Y_k$ have a joint probability distribution given by

$$G(t_1, \ldots, t_k) = P\left[Y_1 \leq t_1, Y_2 \leq t_2, \ldots, Y_k \leq t_k\right].$$

Assuming G is absolutely continuous, and its joint probability density function, $g(Y_1, \ldots, Y_k)$, exists always,

$$g(y_1, \ldots, y_k) = \frac{\partial^k G(y_1, \ldots\ldots, y_k)}{\partial y_1, \partial y_2, \ldots, \partial y_k}$$

Let us also define the joint probability element, $F(t,j)$, following Sather's approach derived from competing risk literature,

$$F(t,j) = P[T \leq t, C = j],$$

which is the probability of failing from cause S_j by time t. The probability is given in terms of the joint probability density function,

$$F(t,j) = \int_0^t \int_{y_j}^{\infty} \ldots\ldots \int_{y_j}^{\infty} g(y_1, \ldots, y_k) \prod_{\substack{i=1 \\ i \neq j}}^{k} dy_i \, dy_j$$

For $t = \infty$, let

$$Y_j = F(\infty, j) ,$$

which is the probability that a particular observed failure is due to S_j. As Sather[13] points out, one only observes min $(y_1,\ldots,y_k)$, and the observation that failure occurred at time t due to cause S_j relates to partial information about failure time due to other causes, i.e., they are greater than t.

Defining,

$$f(t,j) = \frac{\partial F(t,j)}{\partial t},$$

one can obtain the probability of observed failures from S_j as

$$f_j^*(t) = \frac{1}{\gamma_j}\int_{y_j}^{\infty} \ldots\ldots \int_{y_j}^{\infty} g(y_1,\ldots, y_k) \prod_{\substack{i=1 \\ i\neq j}}^{k} dy_i = \frac{f(t,j)}{\gamma_j}$$

Thus, starting with failure times and failure cause for a particular failure state, one can obtain the probability distribution due to each of the causes resulting in the failure state. The difficulties one is expected to encounter in such an analysis are the assigning of the joint probability distribution, G, and estimation of its parameters. Hoel[14] and Moeschberger and David[15] have dealt with the estimation problem.

Hoel[14] discusses slight variation of the above method by assigning an added failure cause, S_0, which is the collection of all other failure causes not of interest to the analyst. In our case, S_0 can be used to define failure due to causes not traceable by engineering analysis. The addition of this hypothetical cause will not change the computational process.

ii) Study of the Failure Distribution if One or More of the Failure Causes is Removed

The classical problem of competing risk analysis is to study the probability distribution of the failure state, given that one or more of the failure causes is removed. Although the analysis is quite parametric, one can study the relative improvements that may be brought about in a system by eliminating some of the failure causes, if feasible.

This problem, first envisioned by Bernoulli in estimating mortality rate should smallpox be eradicated, has remained the interest of many. Here, a brief mathematical formulation is provided following Sather's[13] review work.

The mathematical formulation for the structure of the remaining potential failure times given that a particular failure cause S_j is removed is to be represented by the joint density of failure variables $Y_1, \ldots, Y_{j-1}$, $Y_{j+1}, \ldots, Y_k$. Thus, the joint density function of all variables except for Y_j is given by

$$g^{(-j)}(\underline{y}) = g^{(-j)}(y_1, \ldots, y_{j-1}, y_{j+1}, \ldots, y_k) = \int_0^\infty g(y_1, \ldots, y_k)dy_j$$

where $g^{(-j)}(y)$ represents the density function with failure cause j removed. Similarly, one may define the associated distribution function by

$$G^{(-j)}(\underline{y}) = G^{(-j)}(y_1, \ldots, y_{j-1}, y_{j+1}, \ldots, y_k)$$

$$= P\left[Y_1 < y_1, \ldots, Y_{j-1} < y_{j-1}, Y_{j+1} < y_{j+1}, \ldots, Y_k < y_k\right]$$

As noted by Sather[13] and others, the process may not necessarily represent actual circumstances of failure cause interaction, given a failure cause is removed; nevertheless, it is mathematically consistent and can provide useful insights where all the interactions may not be adequately known, _a priori_.

One can extend the procedure to remove more than one variable. Since the procedure is to intgrate out the variable in question, the joint density function of failure times, given causes S_i and S_j $(i < j)$ are removed, is

$$g^{(-i,j)}(\underline{y}) = g^{(-i,j)}(y_1, \ldots, y_{i-1}, y_{i+1}, \ldots y_{j-1}, y_{j+1}, \ldots y_k)$$

$$= \int_0^\infty \int_0^\infty g(y_1, \ldots, y_k)dy_i dy_j \ .$$

iii) Obtaining the "Net Probability" or the Hypothetical Probability of Failure State, if Only a Specific Cause is Present

Now, assume a more realistic situation where each of the failure causes has a different hazard rate. Thus, $\mu_j(t)\Delta t$ is the conditional probability that the system will fail between t and t + Δt, from cause S_j, provided it has not failed up to time t.

Following the procedure defined earlier, if one removes all failure causes except the j-th cause, one obtains the marginal density and the marginal distribution function of Y_j denoted by $g_j(y_j)$ and $G_j(y_j)$.

These respective functions are given by

$$g^{(-1,\ldots,j-1,j+1,\ldots,k)}(y_j) = g_j(y_j) = \int_0^\infty \ldots \int_0^\infty g(y_1,\ldots y_k) \prod_{\substack{i=1 \\ i\neq j}}^{k} dy_i$$

and,

$$G^{(-1,\ldots j-1,j+1,\ldots,k)}(y_j) = G_j(y_j) = P\left[Y_j < y_j\right]$$

These functions are called the "net probability" density from failure cause R_j and the "net probability" distribution from the failure cause R_j. They signify the hypothesized probability density and distribution, if only a particular failure cause is operating.

Following Rose[16], one can obtain the "marginal hazard" rate of failure mode R_j in terms of $g_j(t)$ and $G_j(t)$,

$$\mu^j(t) = \frac{g_j(t)}{1 - G_j(t)}$$

In general, where all the failure causes are interacting,

$$\mu^j(t) \neq \mu_j(t)$$

However, if all the failure causes are independent, $\mu^j(t)$ should be equal to $\mu_j(t)$. Thus, by the use of competing risk theory, one obtains a hypothesized hazard rate for a failure cause showing its interrelation with other causes, which is distinct from its independent hazard rate obtained from failure data.

4. REFERENCES

1. Akaike, H., "On the Identification of State Space Models and Their Use in Control," Reports on Directions in Time Series, D. R. Brillinger and G. C. Tiao, Eds., Institute of Mathematical Statistics, pp. 175-187 (1980).

2. Anderson, E., "Efficient and Inefficient Methods of Measuring Specific Differences," in Statistics and Mathematics in Biology, O. Kempthorne et al., Eds., Ames Iowa, pp. 93-106 (1954).

3. Bunge, M., Scientific Research I: The Search for System, Springer, Berlin, pp. 74-96 (1976).

4. Gower, J. C., "Some Distance Properties of Latent Roots and Vector Methods Used in Multivariate Analysis," Biometrika, 53, pp. 325-338 (1966).

5. Gnanadesikan, R., Methods for Statistical Data Analysis of Multivariate Observations, John Wiley & Sons, New York (1977).

6. Kendall, M. G., A Course in Multivariate Analysis, C. Griffin & Co., London (1957).

7. Kendall, M. G., "Discrimination and Classification," Multivariate Analysis, P. R. Krishnaiah, Ed., Academic Press, New York, pp. 165-185 (1966).

8. Kim, J-O and Mueller, C. W., Factor Analysis: Statistical Methods and Practical Issues, Sage Publications, Beverly Hills (1978).

9. Marriott, F.H.C., The Interpretation of Multiple Observations, Academic Press, New York (1974).

10. Olivi, L., "Response Surface Methodology in Risk Analysis," Synthesis and Analysis for Safety and Reliability Studies, G. Apostolakis, S. Garriba and G. Volta, Eds., Plenum Press, New York, pp. 313-328 (1980).

11. Quenouille, M. H., The Analysis of Multiple Time Series, C. Griffin & Co., London (1957).

12. Rubin, J., "Optimal Classification into Groups: An Approach for Solving the Taxonomy Problem," J. Theoret. Biol., 15, pp. 103-144 (1967).

13. Sather, H. N., "Statistical Models for Competing Risk Analysis," UCLA-ENG 7676 (August 1976).

14. Hoel, D. G., "A Representation of Mortality Data by Competing Risk," Biometrics, 28, pp. 475-488 (June 1972).

15. Moeschberger, M. L. and David, H. A., "Life Tests Under Competing Causes of Failure and the Theory of Competing Risks," Biometrics, 27, pp. 909-933 (1971).

16. Rose, D., "An Investigation of Dependent Competing Risks," Ph.D. Dissertation, Univ. of Washington, Seattle (1973).

APPENDIX D

"DATA-RELATED ISSUES IN NUCLEAR SAFETY ANALYSIS"

by

AMERICAN STATISTICAL ASSOCIATION

AMERICAN STATISTICAL ASSOCIATION
FOUNDED 1839
806 · 15th Street, N.W. • Washington, D.C. 20005 • (202) 393-3253

EXECUTIVE DIRECTOR
FRED C. LEONE

MANAGING DIRECTOR
EDGAR M. BISGYER

DATA-RELATED ISSUES IN NUCLEAR SAFETY ANALYSIS

A Report of the American Statistical
Association Ad Hoc Advisory Committee
on Nuclear Regulatory Research

Dr. Carl A. Bennett, Chair
Dr. Donald P. Gaver, Jr., Vice Chair

July 1982

This report was prepared by the Data Subcommittee of the American Statistical Association Ad Hoc Advisory Committee on Nuclear Regulatory Research. Principal authors are Donald P. Gaver, Leo Breiman, and Sylvia G. Leaver. Helpful information and comments were provided by Robert Dennig and Fred Hebdon of the Office for Analysis and Evaluation of Operational Data, NRC, the Probability and Statistics Research Review Group, NRC, Robert Haueter of the Institute of Nuclear Power Operations, and David Worledge of the Electric Power Research Institute.

DATA-RELATED ISSUES IN NUCLEAR SAFETY ANALYSIS

A Report of the American Statistical Association
Ad Hoc Advisory Committee on Nuclear Regulatory Research

July 1982

SUMMARY

This is a report that comments on the nature and evolving quality of data sources for use in nuclear power generation safety analysis. It has been compiled by a subcommittee of the American Statistical Association Ad Hoc Advisory Committee on Nuclear Regulatory Research. Helpful informative discussions have been held with members of the NRC Office for Analysis and Evaluation of Operational Data (AEOD), with a staff member at the Institute of Nuclear Power Operations (INPO), with the NRC Office of Nuclear Regulatory Research, and with a representative of the Electric Power Research Institute (EPRI).

Principal conclusions and recommendations now follow:

Licensee Event Reports

1. The Committee is encouraged by AEOD efforts to improve the accessibility and useability of the information contained in Licensee Event Reports (LERs). In particular, the proposed Sequence Coding activity and the systematized development of watch lists promise to be valuable and substantial system improvements.

The Committee has reviewed 10 CFR 50.73, which contains proposed changes to LER reporting requirements. This review suggests these additional comments (references pertain to SECY-82-3):

2. Certain basic definitional material should be clarified in order to standardize licensee responses to as great a degree as possible.

Example:

(a) "nonconservative interdependence" (appearing on p.24, Enclosure 1). Several specific example situations could be provided demonstrating where nonconservative interdependence is present, and several others where it is not. It should, of course, be emphasized that any suggested list is illustrative and does not exhaust all possibilities. The exercise of respondent judgment should be aided to as great a degree as possible in order to obtain adequate comparability between responses.

This report was prepared by the Data Subcommittee of the American Statistical Association Ad Hoc Advisory Committee on Nuclear Regulatory Research. Principal authors are Donald P. Gaver, Leo Breiman, and Sylvia G. Leaver. Helpful information and comments were provided by Robert Dennig and Fred Hebdon of the Office for Analysis and Evaluation of Operational Data, NRC, the Probability and Statistics Research Review Group, NRC, Robert Haueter of the Institute of Nuclear Power Operations, and David Worledge of the Electric Power Research Institute.

(b) "Any event that results in the nuclear power plant not being in a controlled condition or that results in an <u>unanalyzed</u> <u>condition</u> <u>that</u> <u>significantly</u> <u>compromises</u> <u>plant</u> <u>safety</u>" (from p.14, Enclosure 1). Clean definitions with well-chosen examples of the above underlined concepts, as well as others susceptible to varying interpretations, would improve the comparability of individual reports of similar events.

3. A narrative descriptive format is not in itself conducive to complete, comparable event reports. The present form design shown in Enclosure 4, the proposed regulatory guide, could be expanded upon to include a prompt or check list to assure that complete component descriptions and other objective information which might easily be omitted in a textual narrative are not overlooked.

The following remarks pertain to the access to and uses of data contained in LERs.

4. Experience (of Committee members) has shown that LER follow-up reports provide valuable information. Past accessibility of these reports has been disappointing. Thus, every attempt should be made to assure that originals and associated follow-up reports are clearly and explicitly linked and easily retrieved.

5. The Committee encourages a concerted effort to develop adequate statistical methodology for detecting and analyzing trends and patterns from LERs.

6. The Committee strongly recommends the use of LER information for appraisal and validation of predictions from probabilistic risk analysis. The ongoing study of precursors to severe core damage using LER data shows promise of being a useful device for identifying possible PRA deficiencies.

<u>Nuclear Plant Reliability Data System</u>

The Nuclear Plant Reliability Data System (NPRDS) provides a data base that supplements the LER system by furnishing reliability data concerning systems and components. The voluntary nature of its reporting requirements and the recent history of licensee participation in the system lead the Committee to question the reliability and hence usefulness of information obtained from the NPRDS. Hence,

7. The Committee recommends that a special study be designed and carried out to assess the validity of NPRDS-generated reliability data for use in PRA studies and for other purposes. One approach would be to select a certain set of representative nuclear plants from which to obtain failure histories which would lead to failure rates and even repair, outage, or unavailability duration distributions. The latter information should be compared statistically for compatibility with assumed parameter values utilized in other studies, such as probabilistic risk assessments.

For the LER system in particular, but also for NPRDS, the question of quality and user acceptance are of ultimate interest. Consequently:

8. Periodic audits should be undertaken to assure data base quality, i.e., completeness, accuracy of coding, relevance for purposes intended, and timeliness. These audits should be designed and conducted by personnel outside the agencies directly responsible for the data bases. Methods for insuring high data base relevance and usefulness can in part be borrowed or learned from others with similar experience.

9. The Committee recommends development of a means for encouraging and expediting user commentary and feedback concerning data-base relevance and usefulness. Provisions should be made for user suggestions as to desired information that is not available, and to inadequacies perceived in information that is supplied. An attempt should be made to learn from experiences with other, similar data bases that have been assembled in other organizations.

Finally, the Committee suggests the following which are intended to help shape a more useful interaction between statisticians and other quantitatively oriented specialists and the nuclear power generation enterprise:

10. Expand and encourage active, working contact between statisticians outside the NRC and those with statistical problems within NRC.

11. Actively search for parallel problem areas in other industries or fields that have been dealt with systematically and successfully. Promote experience transfer.

(a) How have data acquisition and quality problems been handled by Census, EPA, commercial market research? Can techniques be borrowed or modified to fit the nuclear area? Non-respondent behavior to requests for data may be an example.

(b) How have data been obtained, interpreted, and used to influence maintenance policies and enhance safety in other industries (e.g., air transportation, hazardous material transport) that must have a great concern for public safety?

12. Examine the analysis and modeling techniques found useful in other fields and activities for applicability to nuclear (safety) problems. Promote technology transfer.

(a) Are the available data being carefully examined without prejudice (pre-conceived models in mind) for hints of unanticipated system performance quirks? Is enough exploratory data analysis in use? Are the results of exploratory data analysis being shared with physicists and engineers who are well acquainted with the relevant technical and operational areas?

(b) What does medical survival analysis have to offer reliability assessment, and PRA construction? Is there a (perhaps hidden) problem of data censoring in the nuclear area? Are needs for robust analyses being recognized? What do the best practitioners <u>really do</u> in the related field, and what can be learned from them? Can they be profitably exposed to nuclear safety problems and issues?

(c) What do artificial intelligence techniques, used in medical diagnosis, offer to watch-listing and other currently used devices for spotting potential problems early?

(d) How can uncertainty in quantitative estimates be expressed and controlled, when data cannot be assumed to be an ideal random sample from a fixed universe?

DATA-RELATED ISSUES IN NUCLEAR SAFETY ANALYSIS

A Report of the American Statistical Association
Ad Hoc Advisory Committee on Nuclear Regulatory Research
July 1982

1. Introduction and Purpose

The purpose of this report is to summarize the present understanding and attitudes and to present recommendations of members of the ASA Ad Hoc Advisory Committee on Nuclear Regulatory Research on the subject of data. The particular data emphasized for discussion here pertain to plant safety-related equipment and activities, but many of the suggestions offered may well have broader applicability, e.g., in waste material management.

To us, data refers principally to quantitative information about failure, testing and maintenance, challenges, unavailability and event initiation experience relevant to nuclear power plant safety systems and their components and subsystems. The meaning and usefulness of data are influenced and enhanced by information concerning conditions that existed when the data were obtained. Such information as external (environmental) conditions and internal (operational) conditions should influence the way in which particular data are regarded and trusted as evidence. Therefore, such concommitant or auxiliary information is an important part of any data source, and should be recorded and kept in mind when the particular data are interpreted and applied.

These comments also apply to data adapted from other plausible but possibly remote sources, e.g., when failure performance of valves in the chemical industry is adapted to infer that of the same valves in a nuclear power plant. Of course, expert opinion or engineering judgment must inevitably be necessary to evaluate data quality and relevance, to adjust or adapt available data to new needs, and to guide the acquisition of new data. Expert opinion should itself be regarded as data worthy of careful checking both by comparison with other experts' assessments and, as often as possible, by critical comparison with observational experience. It is important to recognize that expert opinion may be biased by special experience, and subtle pressures by client communities. It probably requires an additional level of expertise to recognize and deal with such effects.

2. Data Base Purposes

There appear to be two specific purposes for collecting and analyzing nuclear safety system reliability and availability related data: These are

- o to monitor system performance, i.e.,
  - to identify precursors, trends, patterns, and individually significant events
  - to identify practices, policies, and activities which yield more efficient system performance
- o to supply inputs to probabilistic risk assessments (PRA studies)

The first purpose, that of performance monitoring, ideally will quickly reveal technical and operational flaws in systems and, by sharing experience, anticipate the occurrence of these in similar systems. The burden of reporting the monitoring findings is borne by the electric utilities, in return for which they ideally should benefit from shared information leading to reduced chance of violations of plant Technical Specifications or more serious safety-related and financially damaging events. Other near and long term benefits would also include location of spare equipment to avoid unscheduled shutdowns or outages, information assisting in the establishment of more efficient maintenance and repair and spare parts policies, and more efficient and effective surveillance policies. Such monitoring should also benefit nuclear power plant manufacturers, as timely feedback will ultimately result in improved plant design. In order that monitoring be effective, and reporting conscientious, a net return must be perceived by the utilities involved. Punitive style enforcement based on monitoring reports must be carefully considered for its net beneficial effect. A continuing effort to "sell" the sharing of monitoring information should be made, and the suggestion that admission of difficulties inevitably leads to punitive action should be dispelled.

The second purpose, that of PRA support, is in response to a general trend towards quantification of societal risk from nuclear power and many other sources. The technology of PRA is still evolving and its credible application requires system knowledge and scientific technique and judgment that go beyond mere numerical information or data about failure rates and outage distributions of system elements. For example, some present PRA models do not seem to explicitly recognize the influence of system monitoring, and consequent system modifications, upon risk. However, specific data that relate to component and (sub)system reliability and availability, operational performance, and environmental stress certainly are important in conducting PRA studies. Much attention has focused on the quality of data available for such purposes. There seems to be the belief on the part of some observers, however, that deficiencies in the validity and credibility of PRAs are more attributable to structural inadequacies in PRA modeling than to data inadequacies.

3. Features of Effective Data Bases

The general properties of effective data bases have been summarized in a previous Committee session, but bear repeating and some discussion.

(3-a) A good (effective) data base is used frequently, and is perceived to be useful by its client community. Feedback to the clients is important. Aid in interpretation of the data may be required as a supplementary service.

(3-b) A good data base is adequately documented, so contents are readily and unambiguously accessible for users, and new entries can be made easily.

(3-c) Entries to a good data base must not require excessively difficult coding.

(3-d) The input report form should be kept as simple as possible.

(3-e) There should be a mechanism for auditing and quality control of the reported entries to the data base.

(3-f) The data base management must put emphasis on quality of data, and motivate participants to achieve a useful quality level. Some form of automatic screening or editing or "flagging" of suspect data is worthwhile.

(3-g) Often two or more data bases must be used in a complementary manner. Their individual design must reflect that need.

All of these comments point to the fact that "good data are not cheap, and cheap data are not good."

4. Major Centralized Data Bases and Sources

The following data bases and sources of data are of importance in the nuclear regulatory and safety areas particularly related to plant operations.

1) Licensee Event Reports (LERs)--The basic purpose of the LER system is to report "potentially significant events" that could lead to, or be precursors of, a serious accident.

(1-a) General

Currently, about 400 LERs are submitted per month; reporting is a requirement for licensees. A computerized LER abstract file, containing brief event descriptions, has been maintained for NRC by Oak Ridge National Laboratory in the Nuclear Safety Information Center (NSIC). Another computer file of LERs containing all coded data and abstracts has been maintained by the NRC/AEOD in the Washington area; this has been discontinued, but the activity has been picked up by the Institute of Nuclear Power Operations (INPO), at least on an interim basis, for use by INPO, its members, and participants. The two files differ in the format and style in which abstracts are stored and accessed.

(1-b) Uses

AEOD uses the LERs to identify the occurrence and recurrence of threatening events. Engineering analyses performed by AEOD staff of problems identified in LER reviews are the bases for recommendations of remedial actions to other NRC licensing and enforcement offices.

AEOD staff also use LERs to generate files which contain summaries of events which have certain characteristics with which the staff is concerned. These files, called "watch lists" are monitored by AEOD engineers for significant accumulations of events. Current watch listing practices are informal; files are maintained manually by AEOD engineers. A more systematic procedure for identifying common characteristics among reported events is anticipated.

Total LER submission rates will be monitored by AEOD to note changes in submission rates; such changes may give warning of more serious events to come. An extended program of trend and pattern analysis is under development.

The LER system is not intended to supply data for estimating failure rates of components or systems. Therefore there is no direct way of estimating the exposure of such items (e.g., numbers of attempted starts or actuations, or times of successful operation) when the items have a standby function, i.e., are not always on-line while the plant is on-line. If an item is on-line when the plant is on-line then at least temporal exposure can be estimated from monthly operating summary reports ("Grey Books"), compiled from utility licensee submissions. But it would take much more detective work to track down exposure to unusual physical stress, e.g., to external environmental shock, or to item failures induced by other items' failures which lead to an internally generated environmental change. The required records may not be available. In addition, certain failures may not be LER-reported at all if they are not judged significant enough, e.g., if the failure occurs in a mode not reportable under the terms of the plant's Technical Specifications.

A newer use of LER data is being made by the Reactor Risk Branch of the Division of Risk Analysis to examine characteristics of precursors to severe core damage, i.e., events which stopped short of being serious accidents resulting in severe core damage. Initial screening of event reports to identify precursors has relied on engineering judgment and the computerized abstract file maintained at NSIC. It is expected that this analysis will produce estimates of the probabilities of types of core damage accidents which are based on operating experience and which can be compared to estimates from PRA-type studies.

Comments: The quality of the LER examination by engineers is unknown, and probably varies. What training and experience is required? Experiments, with different personnel interpreting the same returns, might well be informative. Can automatic screening of some kind be used?

How do watch list designations grow and change? Some suggestions concerning use of statistical indicators of change, analogous to quality control techniques, have been passed to AEOD: these include V-masks, time-series methods, and logistic regression and log-linear models; other pattern-recognition or clustering techniques may also be useful.

The use of LER data for appraisal and validation of predictions from PRAs is a commendable one. The ongoing precursor study described above shows promise of being a useful device for identifying PRA deficiencies.

(1-c) LER Analysis

When an LER is submitted to the NRC it is examined by engineers to detect individually significant events. A systematic computerized procedure for coding LERs, the Sequence Coding and Search System (SCSS), is being developed by AEOD. This system attempts to assure that all relevant information about an event is coded and entered into a data base where it can then be searched with precision for specific sequences and other event-related information. The contractor responsible for sequence coding is NSIC. The SCSS setup provides definitions of fundamental steps that may take place in a sequence. It then begins with a cause or initiating event, which may be personnel- as well as hardware-related and traces out the effects and other circumstances of the fault or failure. Various occurrences (steps) that took place during the event are described in an event matrix.

A modification of the Energy Industry Identification System (EIIS) has been adopted in order to standardize identification of functionally similar systems and components in different plants. Work continues with INPO and the EIIS committee to develop compatible nomenclature identification systems for use in connection with other data systems. Since coding of a particular sequence involves judgment and interpretation, it would appear that sequences developed from a particular situation can and sometimes will differ between coders; the extent of this difference might be examined experimentally, as might the effectiveness of certain automatic decision aids. Quality assurance procedures have been established by NSIC. Careful examination of such procedures by impartial quality assurance experts may well be desirable.

Comment: Given that the possible difficulties alluded to can be controlled, it appears that SCSS information would be far more complete and useful than that in the current LER data file. The present LER abstract systems are not thought to be well-adapted to the detection of complex patterns of malfunction.

(1-d) Proposed LER System Changes

In September 1981, it was agreed by the Commission and staff that NRC would modify the existing LER reporting requirements contained in licensee Technical Specifications. A new proposed rule, 10 CFR 50.73, has now been formulated, discussed and approved by the Commission, and has been published in the Federal Register to obtain public comments.

The objective of the new set of reporting requirements is to standardize LER reporting. Additionally, reportability of certain events such as individual component failures without serious system consequences are expected to be reported in NPRDS; see SECY-82-3 (Enclosure 1, p.3).

(i) The (new) requirements would apply equally to all operating nuclear power plants, superseding existing requirements that are contained in each plant's (differing) Technical Specifications. Reporting inconsistencies should thereby be reduced.

(ii) The new requirements eliminate existing requirements to report events not individually significant (e.g., setpoint drift, missed surveillance tests).

Comment: The concepts of individually significant event and safety significant event are not easily and clearly defined, but in general are ones whose possible consequences are judged important or potentially safety significant. It is not clear how well such reporting can be standardized across time and space.

There follows a brief but somewhat detailed list of reportable events, obtained from 10 CFR 50.73 (a). These are reportable:

(1) "Any event resulting in manual or automatic actuation, or the need for such actuation of any Engineered Safety Feature (ESF) including the Reactor Protective System (RPS)." The accompanying Regulatory Guide states that actuation which is part of surveillance testing or normal reactor shutdown need not be reported, unless the actuation is in a manner not part of the planned procedure; then report.

Question: Is the need for such actuation unambiguous?

(2) "Any instance of personnel error, equipment failure, procedure violation, or discovery of design, analysis, fabrication, construction, or procedural inadequacies that alone could prevent the fulfillment of the safety function of structures or needed to:

i) shut down the reactor and maintain it in a safe shutdown condition,
ii) remove residual heat, or
iii) control the release of radioactive material."

Comment: The proviso "that alone could," etc., is susceptible to ambiguity of interpretation. As indicated in the Regulatory Guide, engineering judgment is required, and a single hardware or personnel failure by "random mechanism" may or may not be reportable depending upon "reasonable doubt" as to whether a functionally redundant mechanism would remain operational until its safety function is completed.

(3) "Any event caused by failure, fault, condition, or action that demonstrates a nonconservative interdependence associated with essential structures, components, or systems," i.e., those need to perform duties (i), (ii), (iii) above. The Regulatory Guide further elaborates: to be reportable an event must have had the potential to disable more than one train or channel of a safety system; it can identify previously unrecognized common-cause failures and system interactions. Engineering judgment may be used to assess operator action for nonconservative interdependence (report personnel failure). An example of a reportable event provided in discussions with AEOD staff would be a pipe break (initiating event) which floods a pump intended to mitigate the result of a pipe break.

Comments: Judgment will sometimes be required. In general, basic definitional material should be clarified in order to standardize licensee responses to as great a degree as possible. Can nonconservative interdependence be defined more simply and directly? Several specific example situations could be provided demonstrating where nonconservative interdependence is present, and where it is not. It should, of course, be emphasized that any suggested list is illustrative and does not exhaust all possibilities. The exercise of respondent judgment should be aided to as great a degree as possible in order to obtain adequate comparability between responses.

(4) "Any event for which plant Technical Specifications Statement require shutdown of the nuclear power plant or for which a plant Technical Specification Action Statement (contained in a Limiting Condition for Operation) is not met." The Regulatory Guide instructs that noncompliance with a Surveillance Requirement need not be LER-reported, but should appear in the Monthly Operating Report.

(5) "Any event that results in the nuclear power plant not being in a controlled condition, or that results in an unanalyzed condition that significantly compromises plant safety." Examples are given on the regulatory guide and presumably previous specific events could be cited in this category. It is recognized that engineering judgment will often be required to identify such events. The requirement includes reporting material problems (cladding, reactor coolant pressure, containment).

Comment: Again, possible ambiguity in assessing reportability exists. Clean definitions with well chosen examples of this and other concepts which are susceptible to varying interpretations would improve the comparability of individual reports of similar events.

(6) "Any act of nature, event or act by personnel, that explicitly threatens the safety of the nuclear power plant or site personnel in the performance of duties necessary for the safe operation of the plant, or the security of special nuclear material, including instances of sabotage or attempted sabotage." The Regulatory Guide indicates that the licensee must decide if the act actually threatened the plant. Not all bomb threats are reportable as LERs; NRC is, however, notified through other reporting requirements (i.e. 10 CFR 50.72).

(7) "Any radioactive releases that require the evacuation of a room or building." The regulatory guide instructs that precautionary evacuations which are later deemed unnecessary are not reportable.

> Comment: The necessity of evacuation may not always be clear-cut. Can any objective criteria be suggested?

(8) Any (external) radioactive effluent release exceeding Technical Specifications is reportable. Likewise, any quantity of radioactive material in storage facilties exceeding Technical Specifications. Likewise (for boiling water reactors), if the quantity of radioactive materials in gaseous waste transferred from primary coolant system to gaseous radwaste management system exceeds Technical Specifications. This latter condition may signify fuel cladding failures.

(9) Any event for which the quantity of radioactive release during an unplanned offsite release exceeds 1 curie of radioactive waste in liquid effluents, more than 150 curies of noble gas in gaseous effluents, or more than 0.05 curies of radioiodine in gaseous effluents.

In reports, pre-event plant status is to be described, and careful (EIIS) identification of involved components and systems is required. An account of relevant redundancy is also required. Important operator actions during the event are to be described. Manufacturers are to be identified. It is expected but not required by the proposed LER rule that involved component failures will be NPRDS-reported. Corrective actions are to be detailed (although perhaps not their time table).

(iii) The new requirements specify LER reporting of potentially significant events that are not now reported under existing LER requirements (e.g., all unplanned reactor trips).

(iv) The new LER form will require a detailed event narrative, including (assigned) cause (or, presumably causes), plant status before the event, sequence of occurrences during the event, and planned corrective action following the event. Additionally, the NRC staff may require a licensee to submit additional information and assessments beyond what is normally required for an LER. The amount of time allowed for delivery of such follow-up reports has not been determined.

Comments: A narrative descriptive format is not alone conducive to complete, comparable event reports. Expansion of the form design shown in Enclosure 4 to include a prompt or check list would assure that complete component descriptions and other easily omitted objective information are not overlooked.

The experience of some Committee members has shown that LER follow-up reports provide valuable information. Access to these reports in the past has been difficult. It will be important that a concerted effort be made to assure that originals and associated follow-up reports are clearly linked and that appropriate updates to SCSS records are made as new information on events becomes available.

A second data base is often referred to; it is the

2) Nuclear Plant Reliability Data System (NPRDS).--The NPRDS is a data base that is intended to supplement the LER system, i.e., to provide data concerning failure of systems and components at a lower level than is the LER focus. It is intended to supply reliability data, possibly for use in PRA studies.

(2-a) General

Much of the information which follows has come from Robert Haueter of INPO.

The NPRDS was initiated by a pilot project with 6-7 nuclear plants in 1973; the system was originally planned and critiqued by a committee which contained senior reliability engineering personnel from all of the five nuclear steam system manufacturers, with Southwest Research Institute as contractor. The data base is maintained by Southwest Research Institute under contract from INPO and the utilities.

Participation in NPRDS by utility licensees was, and remains, voluntary. At present, the fraction of utilities reporting is estimated to be about at the level of 50-60% of the utilities, and the record of submission of NPRDS failure reports is apparently spotty, even for cooperating plants. It may be inferred that failure data reporting has declined following TMI because utility effort has been spent on post-TMI remedies and backfits, not on data. INPO assumed management of NPRDS in 1982, and is endeavoring to increase and improve participation by the utilities. For example, letters have been sent to chief executive officers of utilities. INPO is under some pressure to "make NPRDS work" on a voluntary basis, since the NRC might pursue the option of making it mandatory if INPO is unable to make it a reliable source of data.

It may be inferred that INPO is working hard to make the products of NPRDS useful to utilities. It is offering the products also to manufacturers of nuclear systems. The products are historical facts about past failures, and are packaged in regular annual and quarterly reports. Online access to NPRD records is also available. INPO has, and will conduct workshops on the use of the NPRDS product; these include results of analyses using the NPRDS by both INPO systems analysts and others as appropriate. INPO personnel generally have nuclear power plant operational experience; some have had Navy nuclear training. "Analyst types" such as statisticians or operations researchers appear to play little or no role in these workshops—perhaps they could.

Comment: There may well be a place for statisticians to contribute to the INPO mission. A visit by an interested individual or group should be arranged.

(2-b) Uses

The NPRDS data base contains (a) population data on various plants, identifying in a detailed manner the various components and systems therein, and (b) failure reports on these system elements. INPO plans to improve and clarify the descriptions of the reportable events by putting out a new reportable scope manual in 1982; this is a move toward easing the job of fully identifying ("pedigreeing") components, and should improve the consistency of reporting and of the final data between utilities. Failure reports are supposed to link the item to the population item in the engineering data base, provide failure descriptors, failure event start (discovery) and stop times (which gives some information on down or repair times), system status at failure time, whether the failure was detected in the maintenance, test, or in-service periods, plus a written description of the failure. Whether information is included that could point to common-cause or correlated failures is not clear.

NPRDS and LER data are shared between all utilities via NOTEPAD, part of a computer system operated by INPO. NRC does not have access to NOTEPAD. Information from utilities is first screened by the Significant Event Evaluation and Information Network (SEE-IN); if an event is judged to be significant it earns a Significant Event Report (SER) which is passed out quickly on NOTEPAD; if significant enough it is further analyzed and the results are published as a Significant Operating Event Report (SOER). The exact meaning of significant is defined in existing documentation at INPO.

(2-c) NPRDS Analysis

The quality control and analysis carried out on the NPRDS submissions and data seem to be mainly of an engineering nature. Incoming reports are each given a computer edit check, and an engineering review by engineers at Southwest Research. As stated earlier, information on significant events is shared via NOTEPAD.

Growing interest in PRA suggests that failure rate data will be in increasing demand; however, NPRDS products may not be entirely appropriate. Summary NPRDS statistics presented in the INPO annual report are derived from pooled data and therefore can be used only for general guidance. For example, the failure rate on a class of valves would include failures from all modes. This statistic would be grossly misleading if, say, data on only valve body integrity were desired. More detailed information can be retrieved from failure reports, but usually only through detailed analysis of the verbal descriptions. INPO representatives have indicated that more INPO analysis of NPRDS data for PRA use is anticipated. They do not seem to have the appropriate personnel for this task.

Comments: INPO is set up to serve the nuclear industry by sharing experience, helping to make changes in designs and procedures. INPO/NPRDS products can be used for some risk calculations, but care should be used; e.g., how are the failure histories for one component at several plants to be used to describe that component's failures at one specific plant? How well do uncertain failure rates (or processes) at a "low" component level (somewhat understandable from NPRDS product) combine by existing technology (fault trees) to describe "high level" system failures?

One approach to assessing the validity of NPRDS-generated reliability data for use in PRA studies would be to select a certain set of representative nuclear plants from which to obtain failure and repair or recovery histories to determine failure rates and repair, outage, and unavailability duration distributions. The latter information should be compared statistically for compatability with assumed parameter values employed in PRA studies.

The following comment applies to both the LER and NPRDS data bases, but more particularly so to the NPRDS since reporting is voluntary. The Committee recommends that periodic audits be undertaken to assure data base completeness, accuracy of coding, relevance for purposes intended, and timeliness. Such audits should be designed and conducted by personnel outside the organizations responsible for the data bases. Methods for insuring high data base relevance and usefulness can in part be borrowed or learned from others with similar experience.

5. Other Data Bases

Although the LER and NPRDS data systems provide the major sources of data on nuclear plant reliability performance, other systems are also proposed, under development and in use.

It appears that interest in additional data bases stems largely from a perceived need to develop credible numbers to use in PRAs. Consequently much attention is devoted to providing summaries of actual data in the form of failure rates and probabilities of successful actuation (e.g., start of an emergency diesel generator).

Comment: Data summaries in terms of rates and probabilities usually assume the relevance of certain simple models, such as the exponential distribution for times to failure, and the log-normal for outages and repair times, the Bernoulli trials model (binomial and geometric distributions for number of successes or trials until a success occurs, etc.). Little diagnostic work appears to have been done to assess systematic deficiencies of model fit. When PRAs are to be constructed, the effects of model deficiencies should be systematically examined, i.e., in a sensitivity-analysis manner. Such an activity must begin with comparison of the raw data and proposed models and the manner of their incorporation into an overall risk statement. This issue involves new statistical technology; it arises also, in a less complex form, in medical survival analysis.

1) IEEE Standard 500

This is a document containing failure rates, failure modes, and environmental factors for generic components. Ranges are given for these numbers. Contributing to the data base were experts' opinions, garnered by Delphi methods, and in addition, statistical data from nuclear facilities and fossil-fuel plants, other industries, and transmission grids.

Comment: The combination of Delphi technique and the policy of pooling data from many disparate sources makes the use of this base for statistical inference somewhat questionable. Also, the data are limited to electrical and electronic components or systems.

2) In-Plant Reliability Data System

This system is producing failure rates and repair or restoration information from actual utility nuclear plant records.

Population (of components), reliability, and maintenance and repair data collection was initiated in 1978 by American National Standards Institute and the IEEE, with contractor and utility support. Participatory funding by NRC began in 1979. Current contract responsibility resides with the Oak Ridge National Laboratory. Ten installations, representing 16 distinct operating nuclear units out of a total of 70 operational nuclear power plants in the U.S. have participated in allowing data collection. Participation is voluntary.

A standard format for encoding plant data was developed. Summary statistical analyses have been prepared for pumps at six units (four plants), and summary analyses are in progress for valves. Plant data do not easily lead to extraction of details on rates of occurrence and durations of corrective actions or repairs when actual failures (operational, rather than scheduled) occurred, and so considerable manual searching and interpretation of records is required to extract the pertinent records, and thence, data.

3) EPRI Data Bases and Analyses

The Electric Power Research Institute (EPRI) has contracted with Science Applications, Inc. (SAI) for data collection and analyses of certain specific types of high-level safety related events. These are the subjects of reports that may be used as PRA inputs. Three of these studies are as follows:

(3-a) ATWS: A Reappraisal--Part 3: Frequency of Anticipated Transients (January 1982).

This report describes events, and their frequencies, at nuclear power plants that have led to rapid reactor (BWR and PWR) shutdowns, or scrams. These events are challenges to the automatic shutdown system, and their rate enters PRA calculations.

The analysis is based on a data collection begun in 1975, and includes categorized transient event data from 52 plants in all. Data breakdowns are done by reactor vendor and by other categories likely to be explanatory.

The data used appear to be voluntarily contributed in part; some are from LERs. Transient rates are computed as if they were the parameters of a Poisson process, but some attempt is made to estimate "learning curve" effects, so that transient rates go down with plant experience.

Comment: There is interesting information here, but, like NPRDS, the data collected are of a partly voluntary nature and one could question their representativeness, timeliness, and hence the validity or applicability of inferences made using them. Will this type of analysis, or improvement, be systematized and kept current? The analysis is really direct exponential model fitting, with some Chi-square confidence levels. This is acknowledged, and more could be done.

(3-b) Loss of Off-Site Power at Nuclear Power Plants: Data and Analysis (March 1982).

This report describes the frequencies and durations of incidents of loss of offsite power (LOSP) at 47 nuclear power plants. Such losses are of potential safety significance, for power is needed to operate safety systems.

Data were obtained from utilities (and NRC-utility correspondence), from LERs, and from the EPRI SCRAM data base. Events were categorized as to cause, such as human error, and weather. Exponential distributions were fitted to intervals between LOSP events. Recovery times were fitted to log normal distributions. The raw data available are apparently included.

Comment: Participation by utilities was not complete, so the representative nature of the data is questionable. The actual data analysis is not of great incisiveness or sophistication, and the data probably could yield more if pressed. These data will likely be used in PRAs.

(3-c) Diesel Generator Reliability at Nuclear Power Plants: Data and Preliminary Analysis (April 1982; to appear).

This report deals with data on the reliability of the emergency diesel generators that supply power to actuate nuclear reactor safety systems in case off-site power becomes unavailable. The data employed are from various sources: plants, utilities, and LERs. An interesting discussion of the properties (mostly deficiencies) of the various data sources is provided. Reliability estimation is complicated, even under simple assumptions, by the fact that diesels are on standby but are inspected and tested at intervals. The NRC has published guidelines for testing; the protocols are adaptive and complicated, and may not be widely adhered to.

These data were then used to derive estimates of probability of failure to start (13 plants). Probability of failure to start is apparently to be thought of as a success (failure) probability in a Bernoulli trials model, and failure to run rate is the rate parameter of an exponential distribution. Independence is tacitly assumed everywhere, except when common mode (or cause) analysis is attempted. Both "sampling theory" (classical, maximum likelihood) estimates and Bayesian estimates (using a type of non-informative prior) are given; they differ little for the same data, but appear to differ more between plants. Multiple (common-mode or common-cause) failure analysis is given. A somewhat comparable analysis has been made by EG&G, Idaho, which is principally the work of Dr. C. Atwood, a statistician. The results are intended for PRA use.

Comment: The data come from a few actual plants, and may well be unrepresentative overall. Plant-to-plant variations cannot be well estimated because different data sources were available, and used, for different plants.

6. Recommendations

The following are some recommendations intended to help shape a more useful interaction between statisticians (and other quantitatively oriented specialists—and generalists—such as operations researchers, decision analysts, cognitive psychologists and human factors experts, systems engineers, etc.) and the nuclear power generation enterprise.

1) Expand and encourage active, working contact between statisticians outside the NRC (Research) and those with statistical problems within NRC.

2) Actively search for parallel problem areas in other industries or fields that have been dealt with systematically and successfully. Promote experience transfer.

   (a) How have data acquisition and quality problems been handled by Census, EPA, commercial market research? Can techniques be borrowed or modified to fit the nuclear area? Non-respondent behavior to requests for data may be an example.

   (b) How have data been obtained, interpreted, and used to influence maintenance policies and enhance safety in other industries (e.g., air transportation, hazardous material transport) that must have a great concern for public safety?

3) Examine the analysis and modeling techniques found useful in other fields and activities for applicability to nuclear (safety) problems. Promote technology transfer.

   (a) Are the available data being carefully examined without prejudice (pre-conceived models in mind) for hints of unanticipated system performance quirks? Is enough exploratory data analysis in use? Are the results of exploratory data analysis being shared with physicists and engineers who are well acquainted with the relevant technical and operational areas?

   (b) What does medical survival analysis have to offer reliability assessment, and PRA construction? Is there a (perhaps hidden) problem of data censoring in the nuclear area? Are needs for robust analyses being recognized? What do the best practitioners really do in the related field, and what can be learned from them? Can they be profitably exposed to nuclear safety problems and issues?

   (c) What do artificial intelligence techniques, used in medical diagnosis, offer to watch-listing and other currently used devices for spotting potential problems early?

   (d) How can uncertainty in quantitative estimates be expressed and controlled, when data cannot be assumed to be an ideal random sample from a fixed universe?

INPO

D-21

Institute of
Nuclear Power
Operations

1820 Water Place
Atlanta, Georgia 30339
Telephone 404 953-3600

July 21, 1982

Ms. Sylvia G. Leaver, Research
Assistant
Ad-Hoc Advisory Committee on
Nuclear Regulatory Research
American Statistical Association
806 - 15th Street, NW
Washington, DC 20005

Dear Ms. Leaver:

Thank you for providing INPO with a draft copy of the report, "Data Related Issues in Nuclear Safety Analysis." You have permission to reference my remarks in your report.

The report appears to correctly assess the situation regarding nuclear plant data sources except for the OPEC-2 and GADS data bases which were not addressed. We generally agree with the comments and recommendations. Specific comments are as follows:

1. Principal Conclusion and Recommendation No. 5

   Trending, Time-Series Analysis, and selected functions of SPSS are an integral part of INPO's Analysis and Engineering Division programs and are being applied to both LERs and NPRDS failure reports as well as OPEC-2 records. Identification of candidate components is via the OPEC-2 Plant Capacity Factor Loss Determinations and the INPO SEE-IN Program wherein LERs and NPRDS failure reports are screened for generic significance.

2. Principal Conclusion and Recommendation No. 6

   We agree that analyses of significant operating events can provide valuable validation for postulated PRA sequences. The need for accurate data at the component level is often overstated since modeling inadequacies and human performance uncertainties overshadow the data inadequacies. The use of significant operating events to predict the frequency of potential PRA sequences will tend to integrate these uncertainties which enter at each step in a sequence.

3. Principal Conclusion and Recommendation No. 7

We have established an NPRDS Users Group to assist INPO in assessing the usefulness and adequacy of the data base as well as to provide a useful forum for the exchange of ideas. This Users Group - representing utilities, NSSS Suppliers, Architect/Engineers, NRC, DOE, EPRI and possibly a few INPO international participants - should provide the type of reviews recommended here.

4. Principal Conclusion and Recommendation No. 8

It should be recognized that NPRDS statistics presented in the annual report are derived from "raw" data rather than analyzed data and, therefore, can be used only for general guidance. For instance, the failure rate on a class of valves would include failures from all modes. Use of this statistic would be grossly misleading if data is needed only on valve body integrity, for example.

The more detailed information can be retrieved from the failure reports, but usually only through detailed analysis of the verbal descriptions.

5. Principal Conclusion and Recommendation No. 9

Please refer to our Comment No. 3. In addition, INPO, through its SEE-IN Program, is also a major user of both LERs and NPRDS data.

6. Section Two, "Data Base Purposes"

The purposes of NPRDS are much broader than noted in this section. Some of the purposes for collecting equipment and component engineering and failure data are as follows:

A. Near-Term Uses

- o Location of spare equipment to avoid unscheduled shutdown or outage
- o Maintenance planning and repair activities
- o Identification of significant failure modes
- o Spare parts decisions

B. Longer-Term Uses

- o More accurate assessment and improved reliability of nuclear plant safety systems
- o Expedited regulatory activities and decreased overall time and cost required for plant operation
- o Evaluation and adjustment of protection system testing scheduled based on actual performance
- o Identification of failure trends and detection of wearout patterns
- o Statistics supplied to manufacturers on product performance

7. Section 4.1.a

The last two sentences in this section should be changed to read as follows:

> "Another computer file of LERs containing all coded data and abstracts has been maintained by the NRC/AEOD in the Washington area. This has been discontinued, but the activity has been picked up by the Institute of Nuclear Power Operations (INPO), at least on an interim basis, for use by INPO, its members and participants. The two files differ in content and in the format and style in which abstracts are stored and accessed."

8. Section 4.2.a

Under Paragraph Two of this section you may wish to correct your statement that "almost certainly no professional 'data base' statisticians were involved."

The system was planned and critiqued by a committee which contained senior reliability engineering personnel from all five nuclear steam system suppliers, with Southwest Research Institute as a contractor.

9. Section 4.2.a

Under the last paragraph of this section, NPRDS workshops at INPO will include results of analyses using the NPRDS base by both the INPO systems analysts and by other analysts as appropriate.

We appreciate the opportunity to comment on your report and also the interest you have shown in NPRDS. We believe NPRDS to be a valuable tool which should be used by all segments of the nuclear power industry in improving the safety and reliability of nuclear power plants.

We would be pleased to entertain a visit from American Statistical Association personnel.

Sincerely,

R L Haueter

R. L. Haueter
Manager
Information Services Department
Analysis & Engineering Division

RLH:pab

Attachment

APPENDIX E

SELECTED LICENSEE EVENT REPORTS

JANUARY 1 - AUGUST 31, 1982

Titles of Selected LERs Submitted During January 1 - August 31, 1982

Title

Large Unnoticed Leakage of Service Water from the Containment Fan Cooler Coils and Supply Piping

Loss of 125 V DC Bus

Ignition of Gaseous Waste Decay Tank

Inadvertent Disconnection of Station Batteries

Failure of Main Steam Isolation Valve to Close Due to Failure of Two DC Solenoid Valves to Actuate

Inadvertent Containment Spray Actuation

Steam Generator Tube Rupture

Steam Generator Tube Degradation at TMI-1

Reactor Coolant System Leak

Misalignment of High Head Safety Injection Isolation Valve

Fire Resulting from Transformer Failure

Oil Fire in Diesel Generator

Loss of Both Trains of the Residual Heat Removal System

Inadvertent Discharge of Primary Water to the Containment Sump

Shutdown Cooling System Heat Exchanger Failures

Oil Fire in Diesel Generator

Safety Concern Associated with Reactor Vessel Level Instrumentation in Boiling Water Reactors

Incidents Involving Blockage of Coolant Flow to Safety-Related Systems and Components

Barnacles Restrict Flow in Component Cooling System

Title

Asiatic Clam Buildup in Reactor Building Cooling Coils
Heat Exchanger Failures
RHR Heat Exchanger Failure at Brunswick 1 & 2
Heat Exchanger Degradation Due to Corrosion Product

Incidents Involving the Failure of Main Steam Isolation Valves

Failure of Main Steam Isolation Valve (MSIV) (at Brunswick in January 1981)
Failure of Main Steam Isolation Valve (MSIV) (at Hatch)
Failure of Main Steam Isolation Valve (MSIV) (at Brunswick in March 1981)
Failure of Main Steam Isolation Valve (MSIV) (at Brunswick in July 1981)

Steam Voiding in the Reactor Coolant System

Reactor Scram and Loss of Redundant Safety Signals

Service Water Spill

Bolt Corrosion

Stud Failure in Reactor Coolant System Pressure Boundary - Bolted Closures
Corrosion Damage to the Reactor Coolant Pump Closure Studs Due to Boric Acid Attack
Core Barrel Assembly Thermal Shield Bolts Broken
Crack Indications on Steam Generator Primary Manway Studs
Corrosion of Studs on Valve in Spent Fuel Pool

Contaminated Air Systems

Failure of Gas Turbine Generator to Start Due to Contaminated Control Air
Degradation of Performance of Sample Line Isolation Valve Due to Contaminated Control Air
Failure of Diesel Generator Start Test Due to Contaminated Air Start System
Foreign Material in Air System Blocked Solenoid Exhaust
Failed Air Supply Solenoid O-Ring Disables North Salt Water Cooling Pump

Title

Valve Overtravel Anomalies

Loss of Shutdown Cooling and Positive Reactivity Addition

Load Reduction Transient

Effects of Fire Protection System Actuation on Safety-Related Equipment

- Water in Diesel Generator Fuel Oil Storage Tanks
- Hydrogen Recombiner Discovered Inoperable
- Inadequate Ventilation for Engineered Safety Features Equipment
- Inadvertent Actuation of Fire Suppression System
- Spurious Actuation of Fire Suppression System
- Damage Caused by Fire Suppression System

Seismic Qualification of Safety-Related Systems

Centrifugal Charging Pump (CCP) Miniflow Recirculation Valve Closure Causes CCP to Fluctuate

Spurious Trip of a Generator Lockout Relay Associated With a Diesel Generator Unit

Loss of Reserve Station Service Transformer

Spill of Contaminated Water and Contamination of Personnel in the Auxiliary Building

Cracked Hydraulic Speed Control Cylinders on Main Steam Isolation Valves

Failure of Control Rod Guide Tube Support Pins

Failure of High Pressure Safety Injection System

Inadvertent Isolation of Containment Fan Units

Failure of Main Transformer

Crack in Core Spray Sparger Weld

High Conductivity in the Reactor Coolant System

Defective Manual Initiate ESF Switches

Title

Event Sequences Not Considered in the Design of Emergency Bus Control Logic

- Design Deficiency in Interlocks on the Emergency Feeder Breaker
- Design Deficiency in the Safety Features Actuation System Sequencer
- Inefficient Load Shedding in Bus Logic
- Diesel Generator Overload as a Result of Pre-Accident Nonsafety Loads
- Out of Phase Transfer While Loading the Diesel Generator

Check Valves

- HPCI Gland Seal Condenser Upper Head Gasket Leakage Due to Faulty Check Valve
- Wear in Swing Check Valves
- Diesel Generator Problems (IRS-153)
- Stuck High Pressure Injection System Check Valves
- Cracking in Piping of Makeup Coolant Lines

Loss of Salt Water Cooling System and Flooding in Salt Water Pump Bay

Fuel Degradation

- Fuel Damage Due to Water Jet Impingement
- Leaking Fuel Assemblies
- Degradation of Fuel Cladding

Loose Parts

- Hinge Fragments in Steam Generator
- Missing Thermal Sleeve
- Loose Thermal Sleeves
- Missing Swing Check Valve Securing Nuts
- Steam Generator Tube Leak Possibly Due to Loose Parts

Auxiliary Feedwater Header Deformation

- Auxiliary Feedwater Header Damage at Davis Besse
- Auxiliary Feedwater Header Damage at Rancho Seco
- Auxiliary Feedwater Header Damage at Oconee

Title

Loss of High Head Safety Injection Emergency Boration and Reactor Coolant Makeup Capability

Simultaneous Failure of Three Auxiliary Feedwater Pumps

Unexpected Heatup in Cold Shutdown

APPENDIX F

EXAMPLES OF DATA COLLECTION AND ANALYSIS EFFORTS REVIEWED

- LER (NRC)
- NPRDS (INPO)
- IPRDS (ORNL)
- PRACA (NASA)
- GIDEP (NASA)
- NUCLEAR PLANT DATA BANK

F.1 EXISTING LER INFORMATION

Starting in FY 1982, the Nuclear Safety Information Center (NSIC) of Oak Ridge National Laboratory (ORNL) has been funded by the NRC Office of Analysis and Evaluation of Operational Data (AEOD) to provide the focal points for the collection, storage, analysis and evaluation, and dissemination of operating experience data on NRC licensed activities including Licensee Event Reports (LERs) from U.S. commercial nuclear power plants. The LERs are obtained from the NRC licensee and transformed into ORNL/NSIC abstracts by taking the Event Description and Cause Description narratives directly from the present LER form with supplemental information being added with minimum editing or changing.[1] This transformation process from LERs to NSIC abstracts is performed by two nuclear engineers with nuclear systems and operational background reportedly equivalent to that of NRC Inspection and Enforcement engineers. The abstracts are then QA reviewed and loaded via CRT input into the NSIC File, one of the largest of the almost three dozen information files comprising the RECON (REmote CONsole) system. RECON which is managed by DOE's Technical Information Center in Oak Ridge is reported to be accessible by remote terminal throughout the country and available to US Government agencies and contractors.

Presently the NSIC file on RECON contains more than 163,000 records including in excess of 31,000 LERs and LER predecessor generated abstracts. It should be emphasized that as of January 1982, the NSIC file has become the NRC official LER file with its abstracts. The original NRC LER file (known as the NIH file) is no longer used by the NRC and therefore not given to ORNL. Instead the NIH file of original LERs was given to the Institute of Nuclear Power Operations (INPO).

The NSIC file can be searched by various means with a descriptive keyword system as the primary means for retrieval. A secondary retrieval means comes via the NSIC subject categories. Other search capabilities involve system/component codes which are retained from the original LERs and also text searching in the abstracts. Nevertheless as the number of LERs increase, the size of NSIC file abstracts data base increases. The increase in size, coupled with its design characteristics, limits the adaptability of the NSIC data base for detailed information searches. Therefore, the need for a storage system with more efficient and sophisticated data retrieval methods become evident.[2]

Therefore, NRCs Office of AEOD has developed, through ORNL/NSIC a system for codifying the events reported in the LERs. The primary objective of the Sequence Coding and Search System (SCSS) is to reduce the descriptive text of the LERs to coded sequences that are both computer readable and computer searchable.[3] This system is intented to provide a structured format for detailed coding of component, system, and unit effects as well as personnel errors.

REFERENCES

1. Nuclear Safety Information Center and LERs in the NSIC File on RECON, G.T. Mays, July 1, 1982 (handout).

2. Sequence Coding and Search System: User's Manual for the SCSS Data Base ORNL/NUREG/NSIC-190, (Draft), April 5, 1982.

3. Development of Licensee Event Report Sequence Coding and Search Procedure NUREG/CR-1928, ORNL/NUREG/NSIC-187, February 1, 1981.

F.2 NUCLEAR PLANT RELIABILITY DATA SYSTEM (NPRDS)

The objective of the NPRDS is to collect, store, and make available reliability and failure data on safety related systems and components. This objective is intended to provide failure and engineering data for the near term needs of the plant operators as well as for the longer term needs of the analysts.

Since January 1982 the Institute of Nuclear Power Operations (INPO) has assumed management of the NPRDS. In this manner, the NPRDS has been provided with the following advantages:

- a dedicated user of the data base,
- a full technical manager sensitive to the needs and concerns of the operating nuclear plant staffs,
- an increased awareness of the program at the utility management level, and
- a broad-based, user-oriented, feedback system.

INPO moreover has established the following goals for the NPRDS:

- improve utility participation and use,
- provide component reliability data to support the Significant Event Evaluation and Information Network (SEE-IN) and systems analysis programs and to support industry needs,
- provide a proper home for the industry information system,
- provide a stable industry funding for the system,
- satisfy NRC concerns and permit them to shelve the proposed rule making that would merge NPRDS into a regulatory reporting system.

At present, the NPRDS contains over 9,200 reports of component failure representing 61 nuclear units. From the 47 nuclear utilities participating (out of a total of 55 nuclear utilities) in the NPRDS, the engineering data base contains more than 180,000 components. For a typical nuclear unit which submits failure reports on 30-50 components per year, the number of components in the data base is 3,000 to 4,000 out of a possible 20,000 to 30,000 components in the unit. The data base has, in the past, contained only Class 1, Class 2, and Class 1E components.

Some of the improvements in the NPRDS which INPO has made which may prove quite beneficial to SEA data collection are as follows:

- For improving data usage
  - utilization of failure reports and overall data base in event analysis; significant event reports and trending studies will derive from NPRDS data as appropriate;
  - establishment of USER's Group (with NRC/AEOD representation), and
  - utilization of information on NUCLEAR NOTEPAD to exchange information.
- For improving data access
  - availability of data base at SWRI via on-line access for all INPO members, participants, and the NRC,
  - availability of off-line data searches by SWRI via written request.
- For improving data reporting
  - review of Procedures Manual by Data Reporting Working Group to simplify the forms and to improve the definition and examples,
  - interactive data entry program development is underway, and
  - review of all failure reports is underway for input to the SEE-IN program.

F.3 IN-PLANT RELIABILITY DATA (IPRD) SYSTEM

The IPRD program is developing a component reliability data base from operating commercial nuclear power plants. The objective of this program is to establish a comprehensive data base for risk and reliability analysis.

Since 1978 the Failure Incident Reports Review (FIRR) Committee of the American National Standards Institute (ANSI) has sponsored a voluntary program of visits to nuclear power stations for the collection of component population and equipment maintenance records. Technical support in the data encoding and analysis tasks of the program is being performed by Science Applications Inc. (New York office) under contract to Oak Ridge National Laboratory (ORNL). Partial funding is being provided by the USNRC Office of Nuclear Regulatory Research. The responsibility for selection and coordination of the data collection team and plant visits has been assumed by the Reliability Subcommittee (SC-5) of the IEEE Nuclear Power Engineering Committee.

The IPRD personnel have visited ten nuclear stations (16 units). Following the review of the collectd data from the ten nuclear stations, four plants (six units) were selected on the basis of data completeness for a pilot study. Population, failure, and repair information for pumps from four plants (six units) has been entered into a computer. From these four plants, approximately 120,000 maintenance records have been collected. The pump data base contains 1,468 pumps and 3,100 maintenance records on these pumps spanning almost 24 reactor-years of commercial operation. An additional 900 pump maintenance records for years prior to commercial operation have also been entered. Work is underway for entering data on valves for these six units.

The data base contains three record types:

1. Population Record: The population record contains information about the design, operating environment, operating mode, and functional name of the component. The population record is created whether or not the component has experienced any failures. All components of a particualr type, both safety and non-safety related, are entered into the data base.

2. Failure Record: The failure record contains documentation such as date of failure and report number, failure mode, failure cause(s), failure severity level, and failure description. From the description, the analysts assign the failure mode, cause and severity level. There are three failure severity levels: catastrophic, degraded, and incipient. One failure record is entered for each failure.

3. Repair Record: The repair record contains the repair time, crew size, repair category and repair description. A repair record is entered for each maintenance action.

The data analyses performed to date have been directed toward calculating the failure rates, maintenance frequency, and reviewing the repair time data. Other analyses planned include investigation of common cause failures, human error, trends and patterns in the failure characteristics of components, and evaluation of the effect of the plant's preventative maintenance policy on the component's failure rate.

The IPRD program plans to include additional components as well as increase the number of nuclear plants participating in the project. Revisits to the plants which are currently participating in the IPRD program to collect updated information are also planned. The IPRD system is a unique data base because of its completeness of both population and failure/repair information. IPRD is neither limited to only safety-related components nor to those failures which are, in general, within the scope of a reportable occurrence or a violation of a plant's technical specifications. The completeness of the IPRD system will enable the analysts to develop more accurate reliability estimates as it becomes more fully operational. Analysts will also be able to determine whether a particular component's failure rate is changing with age. When fully operational, the IPRD system will provide a data base for use in reliability and failure analysis that is complete in the operational history of the equipment in nuclear power plants.

BIBLIOGRAPHY

1. "Program Plan for Nuclear Plant Reliability Data System, INPO 80-012, Institute of Nuclear Power Operations, April 1982.

2. R. L. Hauster, "Nuclear Plant Reliability Data System, Progress Report - Final Draft, June 1982.

3. "Nuclear Plant Reliability Data System Reportable System and Component Scoping Manual," Southwest Research Institute, December 1981.

4. J. P. Drago, R. J. Borkowski and J. R. Fragola, "The In-Plant Reliability Data Base for Nuclear Power Plant Components: Data Collection and Methodology Report," NUREG/CR-2641, Oak Ridge National Laboratory (ORNL/TM-8271), July 1982.

5. J. P. Drago et al., "The In-Plant Reliability Data (INPO) System: A Data Bank for Components in Commercial Nuclear Power Plants," a paper scheduled for presentation at the 1982 American Nuclear Society Winter Meeting, November 1982.

F.4 PROBLEM REPORTING AND CORRECTIVE ACTION (PRACA) - NASA

On July 9, 1982 representatives of the Department of Nuclear Energy of Brookhaven National Laboratory met with individuals of the Johnson Space Center of NASA. The purpose of the meeting was to review NASA's methods of handling component and system deficiencies through the "Problem Reporting and Corrective Action (PRACA) Program" and the "Government Industry Data Exchange Program (GIDEP)". This review was directed towards the potential of including aspects of either or both programs into the Licensee Event Report (LER) system to potentially enhance its present capabilities. The NASA representatives present at the meeting were:

M.L. Raines	- Director, Quality Assurance Reliability and Safety Office (QARS) (who reports directly to Chris Kraft, Director of JSC).
C. Harlan	- his deputy.
J.H. Levine	- Chief, Reliability Division
J. Adams	- Chief, Quality Assurance Division
D. Browne	- QA Division
R. Garcia	- QA Division
R. Sheppard	- Reliability Division
D. Hudson	- Boeing Aircraft Company
N.J. Price	- Boeing Aircraft Company

This appendix will first overview the principle conclusions drawn in regard to the applicability of the PRACA program to the LERs and secondly review the PRACA program as it functions at JSC/NASA.

The PRACA program, at this time, is not designed as a quantitative statistical or reliability data base, nor is it used to do trend analyses other than life history of a specific component for recurrence control. Even an attempt to extract mean time to failure would be extremely difficult at this time. Therefore, the program itself is not directly applicable to the needs of this study. It should be noted, however, that the philosophical foundation of the NASA system has many points worth noting when discussing the collection of event data such as in the LER system. The NASA approach to the control of the timely resolution of problems is manpower intensive and relies heavily on the cooperation of the contractors. The NASA representatives feel that the cost of the reporting system is a legitimate cost of ownership and operation of the ultimate product, in this case the orbitor itself. For NASA this can be done since they are the ultimate agency that pays for the product, including the PRACA program. In the case of the nuclear industry, this is not true. If the NRC requires a system as manpower intensive as PRACA the question of who pays for it must be asked. In order to help guarantee the full commitment of its contractors to correct reporting of deficiencies, the PRACA data is <u>not</u> used as a punitive system. The only criticism or penalty placed on the contractor through the system is for inadequate reporting. The NASA representative stated that only in this way could they have confidence that the system would work correctly.

The concept of a closed loop and a complete document trail is applied at JSC. This is accomplished by having each item's engineering resolution returned to the engineer who originally identified the problem, for concurrence. In this way errors of interpretation are limited and <u>all</u> parties agree on the item prior to its being closed out. If this concept were to be adopted by the NRC, it could help assure that the actual codified LER is in fact what the licensee staff found at the plant. In this way the quality of the codified file could be increased. While on the subject of the NASA review process it should be noted that PRACA uses an engineering case study approach to reviewing the failure, its corrective action and its recurrence control. This is accomplished through deterministic engineering analysis based on system importance as identified by a failure model and effects analysis (FMEA).

Lastly, the system is based on a computerized file that is used to access, where necessary, the actual hard copy file for each occurrence. It is the paper copy that is used to conduct evaluations of part specific trends since the computer file is limited in space for description. The computer file is generated by an individual's review of the hard copy and codification of this interpretation from the written narrative. This interpretation is, as described above, returned to the initiator of the problem report to close the loop.

This appendix will now describe the PRACA system and some of its details of operation. The purpose of the JSC PRACA system is to provide a timely notification of problems occurring during or subsequent to a products acceptance test and to minimize its effect on mission safety, success and schedules. This is accomplished through a rigorous deterministic analysis to understand the root causes, to develop a resolution which can guarantee effective recurrence control and full documentation of all steps. (In many ways this is very much similar to current programs of corrective action reporting systems utilized in the nuclear industry during plant construction.) The JSC system features:

- Prompt problem notification to NASA by contractors
- Prompt problem notification to program and element project offices by SR&QA
- Concurrent evaluation of open problems by the hardware supplier and NASA SR&QA program management and engineering
- Visibility of the status of current open problems through weekly open problem lists
- Regular reviews of the status of significant open problems prior to each mission
- Storage of problem information to permit rapid experience retrieval through the problem data system

JSC must be notified of the problem within 24 hours of its isolation with documentation within five days. The problem resolution must be submitted 21 working days after the initial written report. This should include the cause and correcting action or rationale for not implementing corrective action. During this time period the status of the action being taken to resolve each reportable open problem is reported to JSC weekly. Also on a weekly basis, JSC staff notifies its management of significant problems that could have a potential impact on cost and/or schedule or that might require hardware changes. The entire system has an elaborate structure of interfaces within NASA as well as with contractor representatives to help guarantee a closed loop resolution to all problems with the correct level of management being informed.

Attachments 1 through 4 represent an illustrative example of the paper documentation included in the PRACA system. Attachment 1 displays the "JSC Shuttle Open Problem List." It includes all information needed to review the status of current open items that are being processed towards resolution. If a NASA representative sees a questionable item on which he or she needs more information, the computer file can be accessed to produce the specific "Problem Standard Display," see Attachment 2, which in the case of this illustrative example the problem is with a failure of an O_2 Pressure Relief valve. The "Disposition Record," Attachment 3, for the failure describes the part that failed and the failure mode is maintained in hard copy, as are the "Corrective Action Record," "Problem Close Out Summary," and the "Failure and Analysis Report," Attachment 4.

In conclusion, the PRACA system has identified 24,000 potential problems on the shuttle, of which 10,000 were real. At the time of the meeting between JSC and BNL staff, approximately 30 problems were being identified each week with a system backlog, on the first orbitor, of 170 open problems.

ACTION ASSIGNEE: SHEPPARD/MEIER CAE: HOVE SSM/TM: EH5/A.J.FARKAS

PROBLEM IDENTIFICATION:

LEVEL	VEHICLE ON	CAUSE	FAIL MODE	TEST/OPER	PREVAIL COND	LOCATION	INT STATUS	REPORT NUMBER
ELEMENT	095	DES-REQ-	OUTPUT ERROR	CKO	FUNCTIONAL	JSC		A89058-01

WORK UNIT CODE	OCCUR DATE	DATE REC	DATE/TIME UPDT	EST RES DATE	INT RES DATE	ACT RES DATE	REFERENCE NUMBER
	03/22/81	03/24/81	04/01/82 164324				730-425000

HARDWARE IDENTIFICATION:

	PART NUMBER	PART NAME	MANUFACTURER	SERIAL/LOT
TEST ARTICLE	MC434-0283-0001	CNTL ASY ANNUNCIATOR	AERSA	57806
NONCONFORMING ARTICLE	006339	HYBRID		7742
NEXT HIGHER ASSEMBLY	VI70-703604	INSTL FLIGHTDECK	RIDNY	

PROBLEM EFFECTIVITY*

MISSION NUMBER	01-004	05-100	01-100
VEHICLE NUMBER	102	102	9-4
CRIT-STATUS	1R-3-E	1R-3-O	1R-3-O

PROBLEM DESCRIPTION:

1- DURING SYSTEM CHECKOUT TESTS WITHIN SHUTTLE AVIONICS INTEGRATED LAB (SAIL) PER OPS 2-8 RUN 01-064-04 IT WAS OBSERVED THAT THE INDICATOR WITHIN THE X PULSE TRANSLATION MANUAL MODE PUSH BUTTON SWITCH S22 ON PANEL C3 (35V73A3A6-S22) WAS NOT ILLUMINATED (ON) SIGNAL OF ANN CNTL ASSY#3 (30 V 73 A18) CHANNEL 26 WAS LOW; MEASURED INPUT WAS 2 1/2 VAC SHOULD HAVE BEEN 5 VAC. 2- NO PREVIOUS FAILURES OF THIS FAILURE MODE. 3- NO RELATED ANOMALIES IN CHECKOUT TO DATE.

REMARKS:

IC BEING INVESTIGATED AT VENDOR (CTI). ANALYSIS CONTINUING. THERMALLY DAMAGE PART RETURNED TO AUTONETIC FOR FURTHER ANALYSIS.

ACTION ASSIGNEE: SHEPPARD/MEIER CAE: HOVE SSM/TM: EH5/A.J.FARKAS

PROBLEM IDENTIFICATION:

LEVEL	VEHICLE ON	CAUSE	FAIL MODE	TEST/OPER	PREVAIL COND	LOCATION	INT STATUS	REPORT NUMBER
ELEMENT		DES-REQ-	OUTPUT ERROR	ATP	FUNCTIONAL	AERSA		A89952-01

WORK UNIT CODE	OCCUR DATE	DATE REC	DATE/TIME UPDT	EST RES DATE	INT RES DATE	ACT RES DATE	REFERENCE NUMBER
	07/20/81	07/22/81	04/01/82 164648				730-441000

HARDWARE IDENTIFICATION:

	PART NUMBER	PART NAME	MANUFACTURER	SERIAL/LOT
TEST ARTICLE	MC434-0283-0003	ANNUNCIATOR CONTROL	AERSA	0030
NONCONFORMING ARTICLE	006339	HYBRID		8024
NEXT HIGHER ASSEMBLY				

PROBLEM EFFECTIVITY*

MISSION NUMBER	02-004	05-100	01-100
VEHICLE NUMBER	102	102	9-4
CRIT-STATUS	1R-3-E	1R-3-O	1R-3-O

PROBLEM DESCRIPTION:

DURING THE ACCEPTANCE BRIGHT/DIM CONTROL TEST OF THE ANNUNCIATOR CONTROL ASY (ACA) PER ATP 705390 REV. K PARA 5.5.7, CHANNEL #32 (TEST SET ANNUNCIATOR DISPLAY #E-6) OUTPUT REMAINED AT THE BRIGHT INTENSITY LEVEL AS DIAL CONTROL WAS ROTATED TO MAXIMUM DIM MODE.

REMARKS:

PRELIMINARY INVESTIGATION ISOLATED FAILURE TO HYBRID CIRCUIT P/N 006339. SUSPECT PART WAS REMOVED AND SENT TO VENDOR FOR F/A. PI AWAITING F/A FROM VENDOR. ECD 12/07/81. THERMALLY OVERSTRESSED.

Attachment 2

```
DATE 07/09/82       JSC SHUTTLE PROBLEM STANDARD DISPLAY             PAGE 001
           PROJECT:<ORBITER >-<ELECTRIC PWR - PRSD/HPGS  >

   ACTION ASSIGNEE:<MCDOWELL/LACKNER  >        SSM/TM:<EPS/R.R.RICE          >

PROBLEM IDENTIFICATION:
   SUBSYSTEM <PES   >      LEVEL <ELEMENT>      REPORT NO. <AC1510-01    >
   CAE <ELLINGSON      > STATUS <C      >       REFERENCE NO. <7A0-087000>
   INT.STAT. <    >        CRIT. <          >   WORK UNIT <              >
   VEHICLE ON <099>        SUSP/VER <VER >      OCCUR. DATE <02/17/82>
   LOCATION <PARHAN>       PAE REVIEW <Y-X>     DATE REC. <02/19/82>
   TEST/OPER. <ATP>                             D/T UPDATED <06/30/82-1645>
   CAUSE <USE-REQ-ENVR>                         RESOLUTION DATE:
   FAIL MODE <FAILS OPEN .>                        ESTIMATED <         >
   MATL COND <METAL TEMPSN>                        INTERIM   <         >
   PREVAIL. COND. <PRESSURE-HI >                   ACTUAL    <06/22/82>
   TIME/CYC. <          >                       HDW DISP   <         >
   TEST DOCUMENT NUMBER <2PT-5750001     >      CONSTRAINT <             >

HARDWARE IDENTIFICATION:
   TEST/PROC HARDWARE
      PART NAME      <VALVE RELIEF PRES O2>     MANUFACTURER  <PARHAN>
      PART NUMBER    <MC284-0440-0401     >     SERIAL/LOT   <0607        >
   NONCONFORMING ARTICLE
      PART NAME      <VALVE RELIEF PRES O2>     MANUFACTURER  <PARHAN>
      PART NUMBER    <MC284-0440-0401     >     SERIAL/LOT   <0607        >
   NEXT HIGHER ASSEMBLY
      PART NAME      <PANEL ASY           >     MANUFACTURER  <RIDNY >
      PART NUMBER    <V070-454879         >     SERIAL/LOT   <            >
   CONTRACT END ITEM
      PART NAME      <                    >     MANUFACTURER  <      >
      PART NUMBER    <                    >     SERIAL/LOT   <            >

PROBLEM EFFECTIVITY:
   MISN  VEH FCC S    MISN  VEH FC  S    MISN  VEH FCC S    MISN  VEH FCC S
 *01-100*9-4*1R2*C**      *   *  * **        *   *   * **        *   *   *
 *      *   *   * **      *   *  * **        *   *   * **        *   *   *
 *      *   *   * **          *  * **        *   *   * **        *   *   *
PROBLEM DESCRIPTION:
PARA. 5.4 (F) WITH TE  STABILIZED AT -310 DEG F, THE VALVE FAILED TO
 ESEAT AT 980 PSIG
 EMARKS




ENTER CONTINUE COMMAND WHEN READY FOR PAGE 2
```

DATE 07/09/82 JSC SHUTTLE PROBLEM STANDARD DISPLAY PAGE 002
CONTINUED
D/T UPDATED <06/30/82-1645> REPORT NO. <AC1510-01 >
PERTINENT DOCUMENTS:

TYPE	ISSUE SITE	DOCUMENT NUMBER	ISSUE DATE
<PV-FCP >	<Z >	<- >	<06/22/82>
< >	< >	< >	< >
< >	< >	< >	< >
< >	< >	< >	< >
< >	< >	< >	< >
< >	< >	< >	< >
< >	< >	< >	< >
< >	< >	< >	< >

ANALYSIS
THE CAUSE OF FAILURE WAS POPPET ICING AT LOW TEMPERATURE. THE ICE WAS PROBABLY DUE TO MOISTURE INTRODUCED INTO THE TEST SETUP BECAUSE OF A PARTIALLY FUNCTIONING MOLECULAR SIEVE COMBINED WITH THE TEST SETUP BEING VENTED OR LEFT IN AN UNPRESSURIZED CONDITION PRIOR TO COMPLETION OF TESTING.
RESOLUTION
THE FAULTY MOLECULAR SIEVE WAS REPLACED. THE VALVE WAS THEN CLEANED AND DRIED AFTER WHICH THE PERFORMANCE TESTS WERE SUCCESSFULLY REPEATED. THE LABORATORY WILL MONITOR ON A REGULAR BASIS THE FACILITY MOLECULAR SIEVE TO CHECK THE WATER CONTENT OF ITS ELEMENT. IN ADDITION, THE LABORATORY SUPERVISOR HAS CAUTIONED THE TECHNICIAN REGARDING MAINTAINING POSITIVE PRESSURE ON TEST UNIT INLET AT ALL TIMES.

ALL PAGE 3 INFORMATION FITS ON PAGE 2

COMPANY NAME: Parker Hannifin

Rockwell International
North American Space Operations

F

DISPOSITION RECORD (INCOMING MESSAGE)

1. PAGE OF	2. OCN	SPLIT	3. IDR NO.	4. DOC SERIAL NO.
	—			AC1510 — 000

ITEM BEING TESTED/INSPECTED/USED

5. PART NO.	6. MFR'S CODE (SERIAL NO)	7. SEQUENTIAL NO. (SERIAL NO)	8. QTY REJ	9. S/SYS
MC 284-0440-0401	92003	264 E838607	1	7A

ITEM BEING INSPECTED/TESTED/USED — DETECTED IN — INSPECTION/VERIFICATION

10. PART NAME	11. OPRN	12. DEPT	13. STA	14. FACIL	15. BLDG	16. ACTIVITY	17. STAMP NO	18.
Valve Pressure Relief Cryogenic O2 Type Class 1		D30	—	—	SUA —	QPC		

19. PMP	20. E. I. MODEL NO.	21. UNIT	22. REF DOCUMENT NO.	23. ITI CD	24. WRITER'S SIGNATURE	DATE
SY	MV0070A	099	2PTS5750001		LINDA JOHNSON	2-19-82

NONCONFORMANCE ITEM

25. SQK NO.	26. PART NO.	27. MFR'S CODE (SERIAL NO)	28. SEQUENTIAL NO. (SERIAL NO)	29.	30. S/SYS
	SAME AS 5	SAME AS 6,7			7A

31. PART NAME	32. REFERENCE DESIG/LOCATION	33. RESP (CHARGE TO)	34. DEPT	35. C C	36. MV
SAME AS 10					

37. NONCONFORMANCE FAILURE DATE: 2-17-82

PARAGRAPH NO.: 5.4 (F)

With temp stabilized at -310 F, the valve failed to reseat at 980 PSIG - S/B reseat at 980 PSIG minimum at 167 SCCM

REPORT NO: FAR 264-001

38. NONCF CLASS	39. PAC NOTIFICATION DATE	TIME	STAMP	40. PAC ACKNOWLEDGEMENT SIGNATURE	DATE	TIME	41. OBJECT	42. CHAR	43. DEF	44. D QTY
P M (S)	2-19-82	10:03	LJ	G. M. Ellingson	2-22-82	830	294	—	XX	1

PROBLEM ASSESSMENT

NONCONFORMANCE ITEM NEXT ASSEMBLY

55. PART NO.	56. MFR'S CODE (SERIAL NO)	57. SEQUENTIAL NO.	58.
V070-454879	03953		

60. PRELIMINARY INVESTIGATION

59. PART NAME: PANEL ASS'Y

61. REVIEW CAR WRITTEN

62. CAR/RTI/MRB SIGNATURE	63. CAR REQ	64. SYM	65. SC	66. CRIT	67. CAU	68. PC	69. PAC CODE
G. M. Ellingson 2-22-82	YES ☒ NO ☐	090	2	1R2	570	1	7AC 087.000

70. APPROVALS

ORGANIZATION	ORGANIZATION	ORGANIZATION
C. E. Varner 2/23/82		
SIGNATURE DATE	SIGNATURE DATE	SIGNATURE DATE

4. DOC. SERIAL NO.

Caller: Phil Breslin   Phone (714) 851-5354 Ext.

Technical Contact: Phone   Ext.

Rockwell International
Space Division

CORRECTIVE ACTION RECORD 14-55-25-43 F-13

1. PAGE 1 OF	2. CAR NO. AC1510 - 010
3. PART NAME: O_2 PRESSURE RELIEF VALUE	4. PART NUMBER: MC284-0440-0401
5. SERIAL NUMBER: FSCM 92003 SERIAL NO 264E838607	6. SUPPLIER: PARKER HANNIFIN
7. NEXT ASSY NAME: PANEL ASS'Y	
8. NEXT ASSY PART NUMBER: V070-454879	9. NEXT ASSY SERIAL NUMBER: FSCM CODE 03953 SERIAL NO.
10. G.O.	
11. E.I. MODEL NO.: MV0070A	12. E.I. MODEL S/NO.: 099
13. ITEM UNDER TEST NAME: SAME AS 3	14. CRIT.: 1R2
15. ITEM UNDER TEST PART NUMBER: SAME AS 4	16. ITEM UNDER TEST SERIAL NUMBER: SAME AS 5
17. TIME/CYCLE	
18. REF. DOC. NO.: 2PT>575C001	19. ZONE
20. WHERE DETECTED: FAC SUP / BLDG — / DEPT —	21. DATE DET.: 2-17-82
22. DET. DUR.: D30	23. CAT: F
24. PAC CODE: SYS 7AC / PROB CE7 / COUNT CGC	25. OBJ: 284
26. CHAR: ✓	27. DEF: XX
28. SYMP: 090	29. SUB-SYSTEM NAME: CRYO
30. S/SYS: YA	

31. PROBLEM DESCRIPTION

AP 5.4(F)
WITH TEMP STABILIZED AT -310 F, THE VALUE FAILED TO RESEAT AT 980 PSIG.

32. 287-500 LEAD MGR NAME FISHER PHONE	33. DESIGNER NAME MUSTIN PHONE 5177
34. BUYER NAME MARCYES PHONE 1349	
35. CAE NAME ELLINGSON DEPT. 294-102 PHONE 3986 DATE 2-22-82	36. CAR APPROVAL (SIGNATURE) C E Farner 2/23/82

37. PROBLEM EFFECTIVITY END ITEM	FLIGHT	CODE	38. PROB. TIME LINE	ASSIGNEE	SCHED.	ACTUAL
			VERIFICATION			2-23-82
OV102 STS	3,4	N	ANALYSIS	MARCYES	4-1-82	6-11-82
OV099		~~B~~C	CA DECISION	FISHER	4-15-82	6-14-82
OV102	OPS	N	CA RESOLUTION	FISHER	4-30-82	6-14-82
OV103 & SUBS		~~B~~C				

39. SYSTEM PROBLEM: YES ☐ NO ☐

40. RELATED DOCUMENTS
DR AC1510
RAIO - PARKER HANNIFIN REPORT EAR264-001A

N=OV102 STS 3&4 AND OV102 OPS. BBW/TH for E. Rusnak 2-23-82
N-SCREENABLE ATP FAILURE. OV102 RELIEF VALVES HAVE PASSED ATP AND OPERATE SATISFACTORY
a. Sgl 3-3-82 DCAS-NASA

FINAL CODING

41. CAUSE	42. CAT.	43. CRIT.	44. FINAL CA
320	U	1R2	SRC

CLOSEOUT SUMMARY — SEE PAGE 2

45. APPROVALS

COMPANY	DATE	COMPANY	DATE	CUSTOMER	DATE
E Rusnak	6-14-82			RE Osborne	6-22-82

CAR NO.

FORM 3955-G-3 REV. 11-75

ORIGINAL

Rockwell International
F-14
Space Systems Group
12214 Lakewood Boulevard
Downey, CA 90241

CORRECTIVE ACTION RECORD
CONTINUATION SHEET

14.54

PAGE ____ OF ____

1. CAR/SUB-CAR NUMBER
AC1510-010

PROBLEM CLOSEOUT SUMMARY

PROBLEM DESCRIPTION

With the temperature stabilized at -310°F, the valve failed to reseat at 980 psig.

ANALYSIS/CONCLUSIONS

The cause of failure was poppet icing at low temperature. The ice was probably due to moisture introduced into the test setup because of a partially functioning molecular sieve combined with the test setup being vented or left in an unpressurized condition prior to completion of testing.

REMEDIAL ACTION

The faulty molecular sieve was replaced. The valve was then cleaned and dried after which the performance tests were successfully repeated.

CORRECTIVE ACTION

The laboratory will monitor on a regular basis the facility molecular sieve to check the water content of its element. In addition, the Laboratory Supervisor has cautioned the technician regarding maintaining positive pressure on test unit inlet at all times.

Q. M. Ellingson 6-14-82

[signature] 6-14-82
[signature] 6/14/82
R.E. Osborne (NASA) 6/22/82

CAR/SUB-CAR NO.

FORM 3955-Q-4 NEW 11-74

ORIGINAL

Parker

FAILURE & ANALYSIS REPORT

Revised 3 June 1982

DATE 18 February 1982 Page 1

1 - REPORT NO.	2 - INITIAL REPT. NO.	3 - REPORTING ACTIVITY	4 - LOCATION	5 - OBSERVED BY	6 - DATE OF FAILURE
FAR264-001A	RR 39217	Engineering	Engr Test Lab	D. Johnson	DAY 2 MONTH 17 YEAR 82

7 - FAILED ITEM PART NO.	8 - FAILED ITEM SERIAL NO.	9 - FAILED ITEM NOUN	10 - FAILED ITEM MANUFACTURER	11 - LOCATION
5750001-102	264F838607	VLV,PR REL,CRYO O_2,TYL,CLL	Parker Hannifin	Irvine, CA.

12 - NEXT ASSEMBLY PART NO.	13 - NEXT ASSEMBLY SERIAL NO.	14 - NEXT ASSEMBLY NOUN	15 - NEXT ASSEMBLY MANUFACTUR.	16 - LOCATION
N/A	N/A	N/A	N/A	--

17 - FAILURE CODE	18 - OPER. USAGE FAILED ITEM	HOURS	MINUTES	SEC.	CYCLES	STARTS	19 - CUSTOMER	20 - P.O. NO.
--		--	--	--	--	--	Rockwell International	M9H3XSH-485043D

21 - FAILURE DISCOVERED 1 ☒ Acceptance TEST, 2 ☐ STORAGE, 3 ☐ SHIPPING, 4 ☐ SYSTEM/VEHICLE CHECKOUT, 5 ☐ OTHER

22 - DESCRIPTION OF FAILURE EVENT: TEST SPEC. * PARA. **

TEST EQUIP. DESC. & SERIAL NO. Performance Setup

* 2PTS5750001

** 5.4 (f) Reseat Leakage - Low Temperature (-300F)

With test setup moisture at less than 5ppm, the valve temperature shall be stabilized within ±5 degrees at minus 270F to minus 320 F for 1/2 hour. Pressure shall then be decreased from the full flow pressure (1005 to 1033 psig) at 20 psig/minute maximum until the valve reseats at 167 sccm maximum GH_e. Record inlet pressure.

(Continued on page 2)

REPORTED BY D. Johnson DEPT. 208 PHONE 2353

23 - ENGINEERING EVALUATION:

CLASSIFICATION: CRITICAL ☐ MAJOR ☐ MINOR ☐ FAIL. ANAL. REQ'D.: YES ☒ NO ☐

The cause of failure was poppet icing at low temperature. The ice was probably due to moisture introduced into the test setup because of a partially functioning molecular sieve combined with the test setup being vented or left in an unpressurized condition prior to completion of testing. The faulty molecular sieve was replaced. The valve was then cleaned and dried after which the performance tests were successfully repeated.

NAME/TITLE J. Vandewalle, Sr.Proj.Engr. DEPT. 283 PHONE (714)851-3340

24 - FAILURE ANALYSIS & RECOMMENDED CORRECTIVE ACTION:

TEST EQUIP. DESC. & SERIAL NO.

CORRECTIVE ACTION

The laboratory will monitor on a regular basis the facility molecular sieve to check the water content of its element. In addition, the laboratory supervisor has cautioned the technician regarding maintaining positive pressure on test unit inlet at all times.

F-15

DATE ______ LOCATION ______ PERFORMED BY: ______ DEPT. ______ PHONE ______

25 - FAILURE CAUSE
1 ☐ Design Deficiency
2 ☐ Mfg. Deficiency
3 ☐ Unauthorized Adjustment or Disassembly
4 ☒ Other
5 ☐ Test Error
6 ☐ Exceed Spec. Requirements

26 - REPAIR OR DISPOSITION ACTION
1 ☐ Repair in Place
2 ☐ Repair & Re-installed
3 ☐ Repaired & Returned
4 ☐ Adjusted
5 ☐ Analysis
6 ☐ Condemned
7 ☐ Hold
8 ☐ Retest

27 - CORRECTIVE ACTION REFERENCE DATA

28 - CORRECTIVE ACTION COMPLETE ______ REL. ENGR.

29 - PARTS REPLACED DURING REPAIR/REWORK

PART NO.	PART NAME	SERIAL NUMBER REMOVED PART	SERIAL NUMBER REPLACEMENT PART

30 - FINAL DISPOSITION SIGNATURES

QUAL ENGR [signature]

ENGINEERING J. Vandewalle 6/4/82

RELIABILITY D. Peterson 6/3/82

CUSTOMER

USER

DATE REPAIRED ______ REPAIRED BY ______ DEPT. ______ PHONE ______

PHI 183A

22. DESCRIPTION OF FAILURE EVENT: (Continued)

Required: 980 psig minimum at 167 sccm max flow rate.

Recorded: Failed to reseat at 980 psig.

F.5 GOVERNMENT INDUSTRY DATA EXCHANGE PROGRAM (GIDEP) - NASA

The Government Industry Data Exchange Program (GIDEP)* provides its members with unclassified, non-proprietary data on engineering, reliability/maintainability, failure experience and metrology. The data, however, are not in a form suitable to be quantified in a statistical fashion since participation is voluntary. Instead the program is utilized as an alerting system.

The engineering data exchange of GIDEP consists of evaluations and qualification test reports. It includes non-standard parts justification data, procurement specification, and manufacturing processess. The reliability/maintainability data exchange includes failure rates, failure modes, and mean repair time on parts, components, assemblies equipments, subsystems and systems. The data are received from field operational experience, laboratory accelerated life testing, and demonstration tests. This interchange also includes reports on math models, prediction techniques, and FMEA's. The third data interchange is on failure experience and made up of the alert and safe alert system, failure analysis reports and the airforce defective parts and components control program. It is the alert and safe alert system that will be further expanded on later in this appendix. The last interchange is that of metrology which includes calibration procedures, equipment evaluation reports, test equipment maintenance manuals, test instrument specifications and the metrology information service.

The 12 GIDEP operation centers are:

- Department of Energy
- Department of the Army
- Navy
- Department of the Air Force
- National Acronautics and Space Administration
- Industry
- DLA
- United States Postal Service
- NSA
- Department of Labor
- Department of Transportation
- Canada

The alert system is intended to disseminate potential problem data to GIDEP participants. The purpose of this effort is to avoid and minimize recurrences of part and material problems, application problems or safety problems at other facilities. The alert may define an actual occurrence of a failure or potential safety hazard. The types of problems reported are:

- Faulty design or changes in part design or fabrication techniques which cause nonconformance to procurement specifications.

- Faulty production or processing techniques involving operations, such as cleaning, encapsulation, sealing, coating and assembly.

---

*Note: The discussion on the GIDEP is based on a meeting held with staff members of the Johnson Space Center (JSC) of NASA, reference Appendix B of this report.

- Unusual failures and potential failures under normal operating or storage conditions.
- Isolated failures of the same part and material which are indicative of a failure trend.
- Previously unidentified damage or deterioration (degradation or contamination) due to handling, transportation, or storage.

In closing, three illustrative examples of JSC prepared Alerts are shown in the attachments to this appendix. Attachment 1 shows a safe alert for pressure containers, and Attachment 2 an alert for terminal junction blocks. A complete, closed loop package is shown in Attachment 3. This includes an alert on silicon power transistors along with its JSC corrective action record and problem closeout.

Attachment 1

23 JUN 1981

GOVERNMENT-INDUSTRY DATA EXCHANGE PROGRAM

OMB NO. 22-R0328

SAFE-ALERT

Please Type All Information – See Instructions On Reverse

1. NOMENCLATURE: CONTAINERS, PRESSURE, SEALED		2. ALERT/SAFE-ALERT NO.: H9-S-81-01 3. DATE: 1981 June 09
4. MANUFACTURER AND ADDRESS: Generic Design Problem	5. NSN: NA	
	6. PROCUREMENT SPECIFICATION: NA	7. REFERENCE:
	8. MANUFACTURER'S PART NUMBER: NA	9. LOT/DATE CODE OR SERIAL NO.: NA

10. SPECIAL REQUIREMENTS OR ENVIRONMENT

Inadvertent mixture of isolated fluids in vessels or systems where separated by a single barrier. Example: Pressure vessel or container having a bladder or bellows separating two fluids which if mixed could result in a hazardous condition.

11. PROBLEM SITUATION AND CAUSE

An explosion of a test vessel occurred during development testing of a pressure vessel design utilizing Freon 12 as a pressurizing medium on the outside of a bladder containing a methanol base slurry. The pressure shell was seamless 6061 aluminum alloy with a 2000 series aluminum plug rolled into one end. The rolled plug design facilitates attachment of an internal butyl rubber bladder. The vessels have a design burst pressure of 2000 psi and a normal operating pressure of 500 psi. In the application being developed the nominal use pressure was less than 100 psi. The failed vessel had been in storage while containing fluids for approximately three months when the explosion occurred.

The results of the failure investigation showed that Freon 12 and Methanol had intermixed due to bladder permeability. Mixing ultimately resulted in formation of a liquid composition of Freon 12 and Methanol extremely corrosive to certain aluminum alloys. The reaction with aluminum alloys such as 2014, 2024 and 7075 (alloys with significant copper content) is severe releasing copious amounts of hydrogen and methane gas. Generation of gases resulted in pressure sufficient to burst the vessel.

(Continued on next page)

12. ACTIONS TAKEN

Action has been taken to require all sealed containers, pressure vessels and closed systems used in NASA-JSC controlled hardware to be evaluated for the effects of mixed fluids on materials if a single barrier failure can allow fluid mixing. If a corrosive or explosive environment is possible due to mixing of separated fluids the fluid(s) shall be changed or the materials shall be changed or the system redesigned to preclude the possibility of explosion. Implementation of these requirements will serve to eliminate problems such as described above.

13. DATE MFR NOTIFIED	14. MANUFACTURER RESPONSE	15. CONTACT POINTS FOR INFORMATION
NA	NA ☐ CORRESPONDENCE ATTACHED ☐ DID NOT REPLY	R. L. Johnston NASA-JSC (713) 483-5409
16. ALERT COORDINATOR: Ralph E. Keyes - JSC SAFE-ALERT Coordinator		17. SIGNATURE OF ALERT COORDINATOR: Ralph E. Keyes

DD FORM 1938, AUG 79 2

ALL PREVIOUS EDITIONS ARE OBSOLETE

JUL 10 1981

18. NOMENCLATURE: Containers, Pressure, Sealed

19. ALERT/SAFE-ALERT NO: H9-S-81-01

11. Problem Situation and Cause (continued)

The corrosiveness of aluminum by chlorinated hydrocarbon/methanol mixtures is a known phenomenon. However, Methanol or Freon 12 are generally compatible individually with the aluminum alloys used. In this regard there are vessel and system designs where different fluids are separated by single barriers such as bulkheads, bladders, bellows etc. In all probability a materials/fluid compatibility assessment does not include an evaluation for the consequences of combinations of the separated fluids. In the cases of closed containers, pressure vessels or closed systems the results can be catastrophic. It should be standard practice, therefore, to evaluate the effects of combined fluids where any single barrier failure would allow mixture.

F-21

29 OCT 1981

Attachment 2

GOVERNMENT-INDUSTRY DATA EXCHANGE PROGRAM

OMB NO. 22-R0328

ALERT

Please Type All Information – See Instructions On Reverse

1. NOMENCLATURE: Hardware, Terminations, Wire (Terminal Junction Blocks)		2. ALERT SAFE-ALERT NO.: H9-A-81-01 3. DATE (Year, Month, Day): 81 October 20
4. MANUFACTURER AND ADDRESS: Deutsch 700 South Hathaway St. Banning, CA 92220 H4: 11139	5. NSN: 6. PROCUREMENT SPECIFICATION: SG. 459/013 (SPAR) 8. MANUFACTURER'S PART NUMBER: CTJ122E	7. REFERENCE: ALERT C6-A-81-07 TWX ALERT H9-A-81-01 9. LOT DATE CODE OR SERIAL NO.: (cont'd) 7812, 7815, 7830, 7839, 7841

10. SPECIAL REQUIREMENTS OR ENVIRONMENT

The respective module requirements are contained in the applicable specifications. The failure conditions were a result of mismated contacts causing excessive contact resistance.

Note: Problems with these modules have been limited to ones with 22 gauge pins.

11. PROBLEM SITUATION AND CAUSE

This ALERT reports the problems encountered with two systems of Space Shuttle equipment. A. Shuttle Remote Manipulator System (SPAR, Toronto, Canada). In the Space Shuttle Remote Manipulator System, two assembled terminal junction module connections exhibited excessive contact resistance (SPAR P/N SG459/013-002, Deutsch P/N CTJ122E05E-4010). During troubleshooting any slight movement of the wire sealing grommet caused the resistance to fluctuate. Failure analysis of one module revealed that pins A and E were bent hard against the wall of the lower housing and were heavily scored (see figure 1). Three unused pins were found to be bent. Failure analysis of the other module revealed that pins A, E, J, N and T were bent and damaged. (see figure 2).

As a result of the equipment failures, the terminal junction modules in stock were examined and discrepancies were found. The discrepancies included (1) bent pins, (2) silicone barrier material in cavity, (3) debris in cavity, (4) broken retention clips, (5) crack retention clips, (6) excessive epoxy around pin preventing socket locking and (7) misaligned bus bars.

Table 1 is a list of the part numbers and lot date codes of devices exhibiting these discrepancies.

12. ACTIONS TAKEN

A. Existing hardware was checked to insure correct mating and gold to gold contact. Unassembled modules from stock were inspected with a boroscope.

B. Assembled modules were X-rayed, pull tested and had continuity verified during vibration. Modules from stock were inspected with a boroscope, and assembly instructions were revised to assure use of proper plastic tool and a pull test to assure socket retention.

13. DATE MFR NOTIFIED (Year, Month, Day): 81 Sept. 28	14. MANUFACTURER RESPONSE: [X] CORRESPONDENCE ATTACHED [ ] DID NOT REPLY	15. CONTACT POINTS FOR INFORMATION: Robert R. Sheppard EEE Parts Reliability Division, Code NB5 Johnson Space Center Houston, Texas, 77058 713-483-3591
16. ALERT COORDINATOR: Robert R. Sheppard, Johnson Space Center		17. SIGNATURE OF ALERT COORDINATOR: Robert R Sheppard

DD FORM 1938 13

ALL PREVIOUS EDITIONS ARE OBSOLETE

Hardware, Terminations, Wire (Terminal Junction Blocks)

H9-A-81-01

6. Procurement Specification

ME417-0015 (Rockwell)
SV771340 (Hamilton Standard)

9. Lot/Date Code or Serial No.

7843, 7845, 7946, 7947, 8009

11. Problem Situation and Cause

TABLE 1

List of Parts with Discrepancies (SPAR)

USER'S P/N (SPECIFICATION)	MANUFACTURER'S P/N	LDC	QUANTITY	WHERE PROBLEM OCCURRED
SG459/013-002 (SPAR)	CTJ122E05E-4010	7841	2	Equipment
SG459/013-001 (SPAR) (Same as ME417-0015-0313 Rockwell)	CTJ122E10A-4010	7839	3	From Stock
SG459/013-002 (SPAR)	CTJ122E05E-4010	7841 7843	Numerous	From Stock and equipment
SG459/013-003 (SPAR) (Same as ME417-0015-0312 Rockwell)	CTJ122E06B -4010	7720 7850	Numerous	From Stock and equipment
SG459/013-004 (SPAR) (Same as ME417-0015-0315 Rockwell)	CTJ122E02D-4010	7845	Few	From Stock and equipment
SG459/013-005 (SPAR) (Same as ME17-0015-0311 Rockwell)	CTJ122E01C-4010	7815	Few	From Stock

B. Extravehicular Mobility Unit (Space Suit Support Equipment) (Hamilton Standard, Windsor Locks, Connecticut)

During Space Shuttle postflight checkout, one astronaut's space suit circulation fan cut off. The failure was caused by excessive voltage drop across the fan power connection in a terminal junction module. The contact resistance of the terminal junction module was 7.45 K ohms. X-ray of the module indicated that the socket had not mated with the terminal junction pin but had been forced down along side of the pin. Failure analysis of the terminal junction module indicated that the socket had been inserted with a metal tool instead of the recommended Deutsch plastic tool. The use of the metal tool allowed the assembler to force the socket down along side the pin. Investigation of devices from stock revealed that parts were received with bent pins and misaligned bus bars (see figures 4, 5 6 and 7). A combination of bent pin and the use of the metal tool led to making the faulty connection.

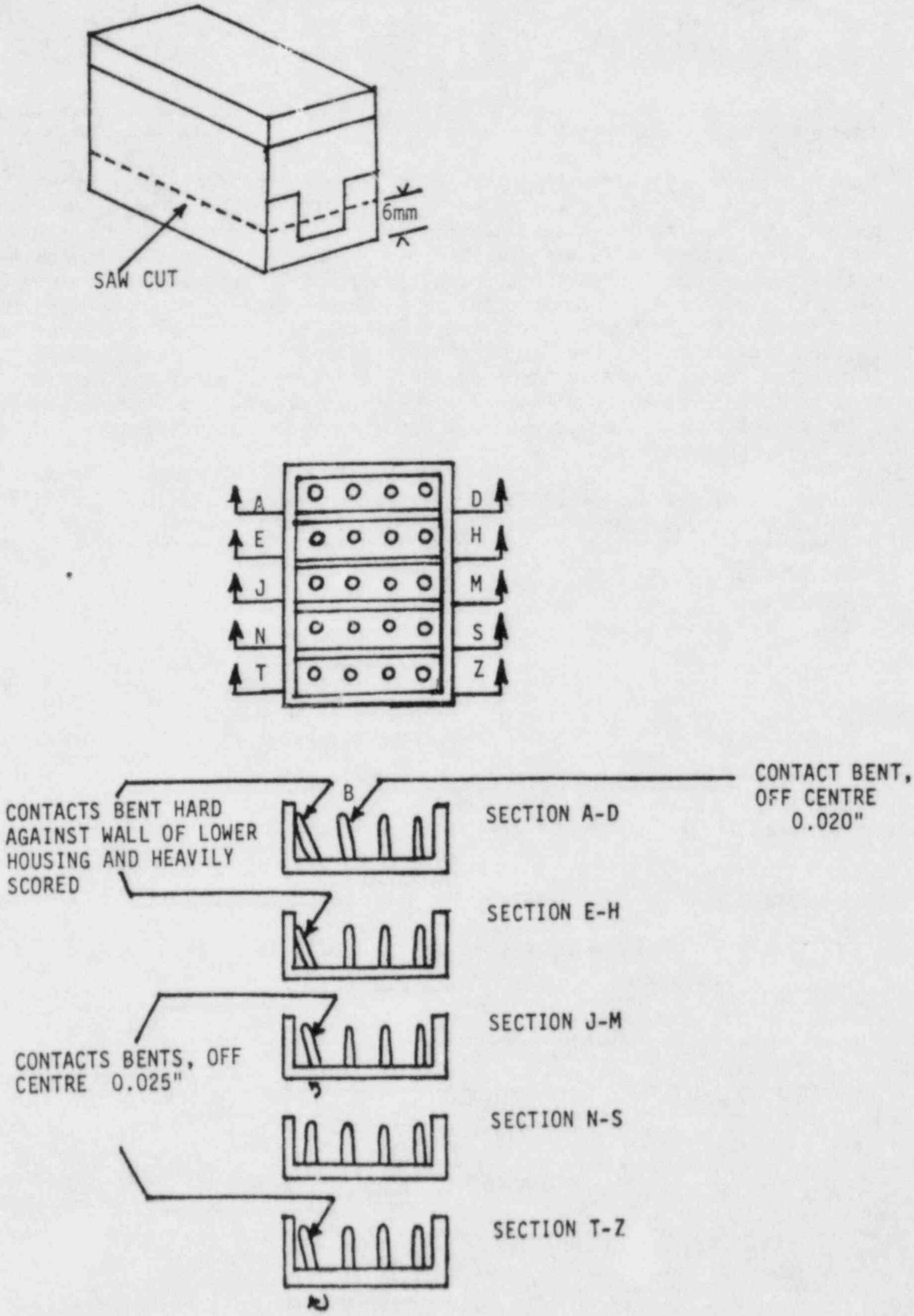
As a result of the equipment failure, the terminal junction modules in stock were examined and discrepancies were found. The discrepancies include (1) offset pins, (2) foreign material, and (3) bent pins. Table 2 is a list of parts exhibiting these discrepancies.

TABLE 2

List of Parts with Discrepancies
(Hamilton Standard)

USER'S P/N (SPECIFICATION)	MANUFACTURER'S P/N	LDC	QUANTITY	WHERE PROBLEM OCCURRED
SV771340-2	CTJ122E05E	7812	1	Equipment
SV771340-1	CTJ122E10A	7946	3	Stock
SV771340-2	CTJ122E05E	7812	2	Stock
SV771340-2	CTJ122E05E	8009	2	Stock
SV771340-3	CTJ122E01C	7947	1	Stock

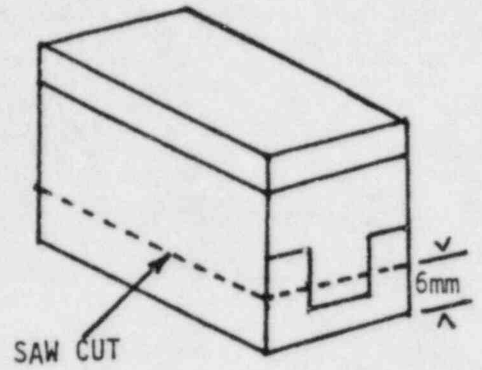
F-24

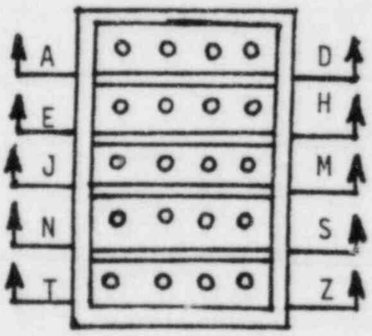


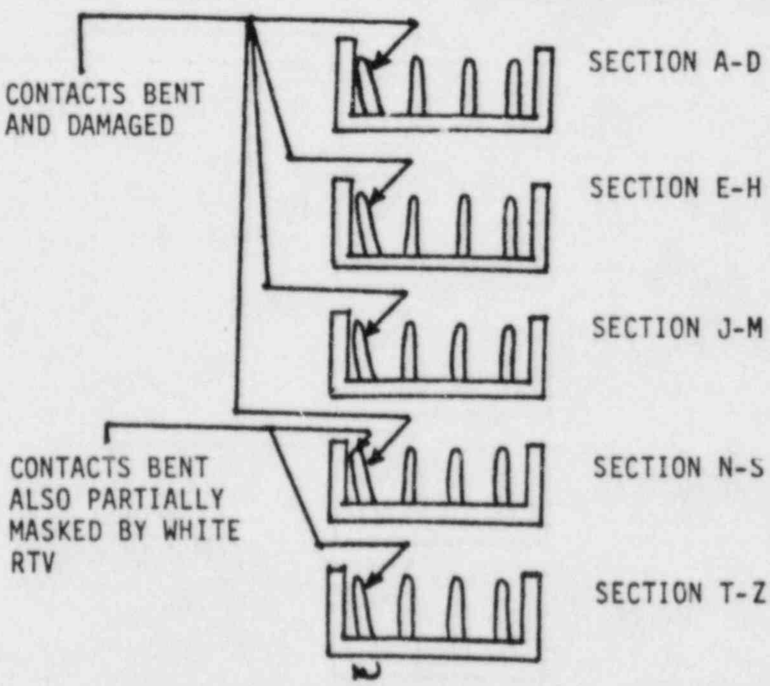
SPAR Sample No. 1

Figure 1

F-25







SPAR Sample No. 2
Figure 2

F-26

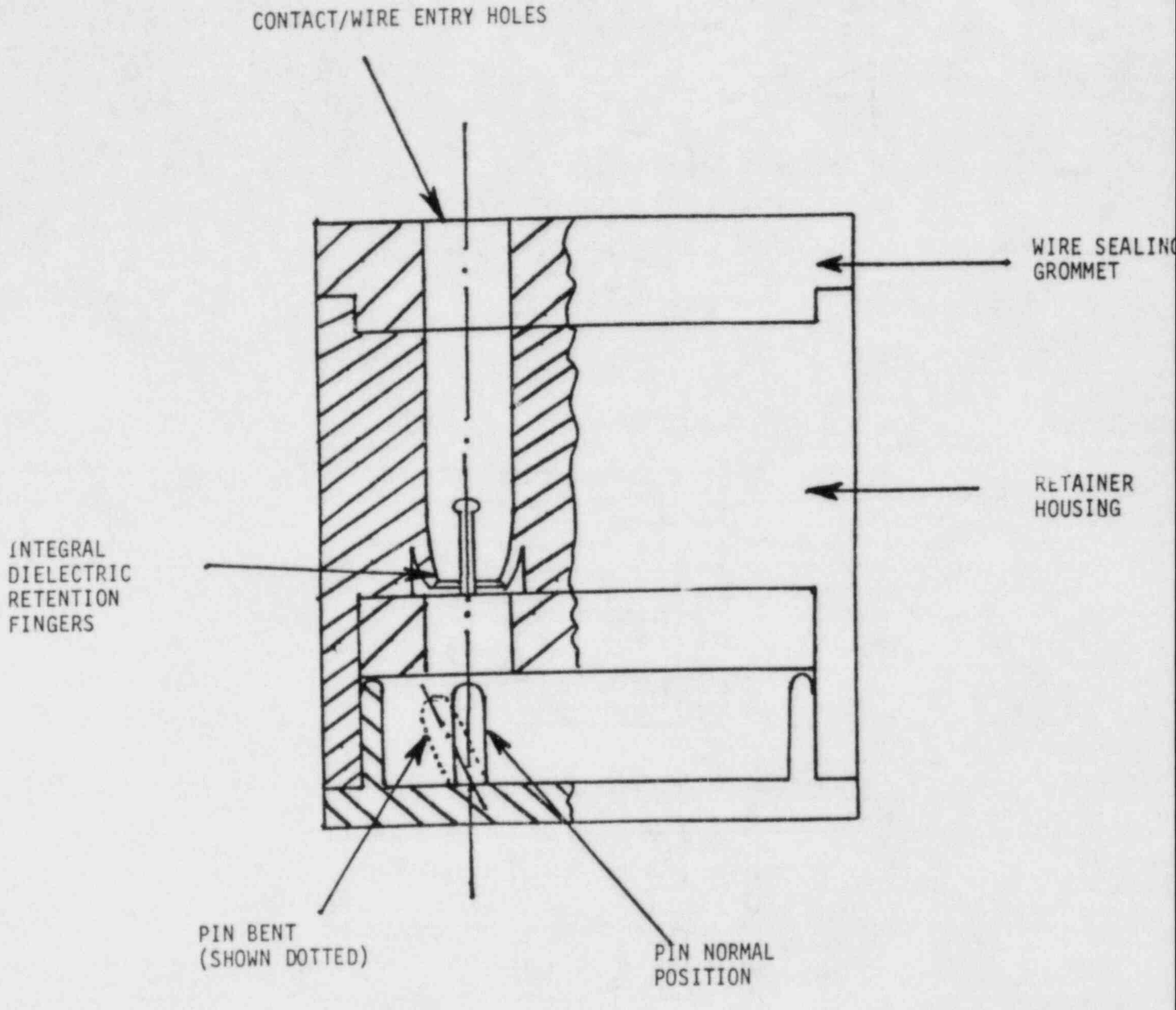

CONTACT/WIRE ENTRY HOLES
WIRE SEALING
GROMMET
RETAINER
HOUSING
INTEGRAL
DIELECTRIC
RETENTION
FINGERS
PIN BENT
(SHOWN DOTTED)
PIN NORMAL
POSITION

FIGURE 3

F-27

25 AUG 1981

GOVERNMENT-INDUSTRY DATA EXCHANGE PROGRAM

OMB NO. 22-R0328

ALERT

Please Type All Information – See Instructions On Reverse

1. NOMENCLATURE (Part/Material/Hazard/Safety Problem) TRANSISTOR, POWER, NPN, SILICON	2. ALERT/SAFE-ALERT NO. D4-A-81-02 3. DATE Year Month Day 1981 August 18

4. MANUFACTURER AND ADDRESS Raytheon 350 Ellis Mountain View, Calif. H4: 49956	5. NSN 5961-01-026-2573	
	6. PROCUREMENT SPECIFICATION MIL 19500/366	7. REFERENCE
	8. MANUFACTURER'S PART NUMBER 2N3501 JANTXV	9. LOT DATE CODE OR SERIAL NO. 7948

10. SPECIAL REQUIREMENTS OR ENVIRONMENT (Requirements placed on, or severe environment to which item was exposed)

11. PROBLEM SITUATION AND CAUSE (State facts of problem and cause—failure mode and mechanism—project and function)

During pre-conformal coating board level test of Radiator Flow Control Assembly, a circuit board (P/N 224-00230-101) failed. Trouble shooting revealed transistor Q14 (JANTXV 2N 3501) was defective. Failure of Q14 was determined to be open base-to-emitter and base-to-collector leads.

Failed parts analysis was performed on failed transistor. Visual examination after decanning revealed that the base lead had broken loose at the ball bond pad. Pull test of the remaining emitter lead failed the lead at the ball bond pad with a force of 0.8 grams. The minimum spec. value is 3 grams.

Photomicrograph of the failed area showed crystalline intermetallic compound. Five additional transistors were subjected to failed parts analysis to determine extent of bonding problem. (Failure analysis Report No. R52747 is included herein as Encl. 1.) The five devices were subjected to electrical test to determine open lead. This device when decanned had a lifted lead at the ball-to-pad junction, similar to the initial failed device.

(See continuation sheet for conclusion)

12. ACTIONS TAKEN (State all actions taken to correct the problem situation and to prevent its recurrence)

Vought has rejected Lot 7948 and obtained JANTXV 2N 3501 from another vendor.

Vought has forwarded the two failed devices and 10 additional samples from Lot 7948 on hand to Raytheon for evaluation.

13. DATE MFR NOTIFIED (Year, Month, Day) 1981.June 24	14. MANUFACTURER RESPONSE [X] CORRESPONDENCE ATTACHED [ ] DID NOT REPLY	15. CONTACT POINTS FOR INFORMATION (Name, Address, Phone) P. R. Provost Vought Corporation Dallas, TX (214)266-7970

16. ALERT COORDINATOR (Name, Address) K. P. Redd, Vought Corp. (214)266-2538	17. SIGNATURE OF ALERT COORDINATOR 8-18-81 Katie Redd D4

DD FORM 1 AUG 79 1938 21

ALL PREVIOUS EDITIONS ARE OBSOLETE

18. NOMENCLATURE TRANSISTOR, POWER, NPN, SILICON

19. ALERT/SAFE-ALERT NO D4-A-81-02

ALERT CONTINUATION SHEET

ITEM 11

Two additional transistors were pulled from stock and subjected to Auger Electron Spectroscopy examination. Pull test on leads resulted in one failing in the chip ball interface and three failing in the wire. Examination of the surface area detected elements of aluminum, gold, silicon and carbon. A copy of the Auger Spectrograph report (Report No. 81-51120-046) is included herein as Enclosure 2.

3. PART NAME: TRANSISTOR, POWER, NPN, SILICON

4. PART NUMBER: JANTX V 2N3501

5. SERIAL NUMBER: FSCM 49956 SERIAL NO. LDC/7948

6. SUPPLIER: RAYTHEON

7. NEXT ASSY NAME: AC OVER/UNDER VOLTAGE SE[illegible]

8. NEXT ASSY PART NUMBER: MC431-0129-~~0301~~ 3002

9. NEXT ASSY SERIAL NUMBER: FSCM CODE 94756 SERIAL NO. MULTIPLE

10. O.O.

11. E.I. MODEL NO.: MV0070A

12. E.I. MODEL S/NO.

13. ITEM UNDER TEST NAME: TRANSISTOR, POWER, NPN, SILICON

14. C[illegible]: IR

15. ITEM UNDER TEST PART NUMBER: JANTXV 2N3501

16. ITEM UNDER TEST SERIAL NUMBER: 49956 LDC/7948

17. TIME/CY

18. REF. DOC. NO.: ALERT D4-A-81-02

19. ZONE

20. WHERE DETECTED: FAC SUP | BLDG | DEPT

21. DATE DETECTED: 02/15/82

22. DET. DUR.: 735

24. FAC CODE: SYS PROB COUNT: 76 00 63 000

25. OBJ

26. CHAR

27. DEF: XX

28. SYMP: 999

29. SUB-SYSTEM NAME: GENERAL AVIONICS

31. PROBLEM DESCRIPTION

THE REFERENCED ALERT REVEALED THAT JANTXV 2N3501 TRANSISTORS MANUFACTURED BY RAYTHEON, LOT DATE CODE 794[illegible] HAVE FAILED AS A RESULT OF THE BASE LEAD BREAKING LOOSE AT THE BALL BOND PAD.

32. LEAD MGR NAME: V.P. OSTRANDER PHONE 1347

33. DESIGNER NAME: ED GRAY PHONE 5554

34. BUYER NAME: G. GLOE PHONE 3112

35. CAE NAME: A.N. WHITE, JR DEPT. 194-01 PHONE 5651 DATE 2-15-82

36. CAE APPROVAL (SIGNATURE): [signature] 2/15/82

37. PROBLEM EFFECTIVITY END ITEM	FLIGHT	CODE	38. PROB. TIME LINE	ASSIGNEE	SCHED.	ACTUAL
OV-102	OFT	N	VERIFICATION	V.P. OSTRANDER	2-15-82	2-15-82
OV-102	OPS	N	ANALYSIS	V.P. OSTRANDER	2-19-82	2-15-82
OV-099		~~C~~	CA DECISION	V.P. OSTRANDER	2-26-82	4-16-82
OV-103		C	CA RESOLUTION	V.P. OSTRANDER	3-5-82	4-21-82
OV-104	SUBS	N				

39. SYST PROBL: YES [ ] NO [ ]

40. RELATED DOCUMENTS

PRC DR AC1481-000

N- Subject Lot Date Codes transistors are not utilized in these units.

R. Sheppard/JSC/Rel } ok to close per
P. Meier/JSC/Rel } telecon 2/18/82
A.E. Eckerman

"N" FOR OV-102 OFT & OPS., AND OV-104 ONLY - [signature] 2-18-82

P. Rubin 2-18-82

FINAL CODING

41. CAUSE: 220 | 42. CAT.: 1 | 43. CRIT.: 1R3 | 44. FINAL CA: RAA

CLOSEOUT SUMMARY — SEE PAGE 2

IED SG 0847 3

45. APPROVALS

CONTRACTOR	DATE	COMPANY	DATE	CUSTOMER	DATE
[signature]	4-30-80				

PROBLEM CLOSEOUT

PROBLEM

Refer to problem description on page 1 of this CAR.

PROBLEM INVESTIGATION

Suspect transitors JANTXV2N3501 LDC7948 manufactured by Raytheon, were found only in Autonetics stock, in kits for OV-103 and in AC sensors delivered for OV-099. No other usage was identified.

Twenty two transistors (from Autonetics stock and from OV-103 kits) were sent to the Autonetics failure analysis lab where they were electrically tested, subject to 30KG centrifuge, -55°C to +150°C thermal shock and bond pull.

Two of the transistors failed the initial electrical test. After centrifuge and ther shock two more failed. When bond pull was performed, three transistors failed bond p with readings of 0.1, 0.6 and 1.8 grams. The bonds are required to withstand 2.0 g pulling force.

In addition to the seven failures mentioned above, potential problems were found, i. cross section of one "good" transistor revealed Kirkendall voiding, and cracks were found under the bond pads on several other transistors.

REMEDIAL/CORRECTIVE ACTION

All suspect transistors were removed from Autonetics stock and from kits. These transistors were scrapped and/or used for problem investigation analysis.

A special Action Requirement SAR # P-2194, was written to return delive AC sensors in 099 for retrofit of the suspect transistors.

All Raytheon transistors have been purged and replaced with acceptable transistors o LDC 8020, manufactured by Motorola.

Failed Part Number: JANTXV2N3501
Part Manufacturer Code No.: 49956
E/I Control: ME431-0129-0002

Name of Part: Transistor, Power, NPN
Part Lot Date Code: 7948
E/I Mfr Code: 94756

J.R. Naranjo
D/294-101
4-30-82

C.W. Dayt 4/27/82

O. Edward Gray
D292-629 4/29/82

R.W. Fields 4/29/82
D/292-620

F6. NUCLEAR PLANT DATA BANK

It has been recognized that the lack of information concerning the physical/geometrical and operating characteristics of the plants poses a serious obstacle in performing safety analyses of LWR plants and in responding promptly to emergencies that may arise.

To remedy this situation, the Office of Nuclear Regulatory Research, Analytical Models Branch of the NRC, has developed through a contractor a computerized data bank to store relevant plant data. The objective of the program was to develop an information library with the capability to describe thermohydraulic and containment systems in order to support both rapid information retrieval and thermohydraulic analysis modeling. The general system design has modular architecture, a data management system, and local or remote terminal access. The program contains tables, sketches, drawings, piping configurations, and power distribution information. At present, the Zion 1 plant has been modeled and demonstrated satisfactorily. There are plans to enter six more plants into this data bank.

APPENDIX G

DATA SOURCES

LIST OF DATA SOURCE TITLES AND CONTACTS

1. Title: In-Plant Reliability Data System (IPRDS)
   Contact: Mr. Joseph P. Drago
   Oak Ridge National Laboratory
   P.O. Box X
   Oak Ridge, Tennessee 37830

2. Title: Nuclear Plant Reliability Data System (NPRDS)
   Contact: Mr. Robert Haueter
   Institute of Nuclear Power Operations
   1820 Water Place
   Atlanta, Georgia 30339

3. Title: Collection and Evaluation of Reliability Data at the Nuclear Power Plant Biblis B
   Contact: Mr. P. Homke
   Gesellschaft fur Reaktorsicherheit (GRS) MbH
   Glockengasse 2.5000 Koln 1
   West Germany (FRG)

4. Title: Root Cause Data Analysis for Combined Cycle Turbines
   Contact: Mr. Richard Duncan
   Electric Power Research Institute
   3412 Hillview Avenue
   Palo Alto, California 94304

5. Title: Failure Data Handbook for Nuclear Power Facilities
   Contact: Mr. C. W. Griffin
   Liquid Metal Engineering Center (LMEC)
   P.O. Box 1449
   Canoga Park, California 91304

6. Title: Reactor Safety Study (WASH-1400 Appendix III Failure Data)
   Contact: National Technical Information Service (NTIS)
   U.S. Department of Commerce
   5285 Port Royal Road
   Springfield, Virginia 22151

7. Title: IEEE Std-500 Reliability Data Manual
   Contact: Mr. Lewis E. Booth
   Fluor Engineers and Constructors, Inc.
   2801 Kelvin Avenue
   Irvine, California 92714

8. Title: Licensee Event Reports
   Contact: Mr. Robert Dennig/Mr. Fredrick Hebdon
   Office for Analysis and Evaluation of Operational Data
   U. S. Nuclear Regulatory Commission
   Washington, D. C. 20555

9. Title: System Reliability Service Data Bank (SYREL)
   Contact: Dr. Ian Watson
   System Reliability Service, UKAEA
   Culcheth, Warrington WA3 4NE
   England

10. Title: Generating Availability Data System (GADS)
    Contact: Mr. Ronald Niebo, Director
    Generating Availability Data System
    North American Electric Reliability Council
    Research Park, Terhune Road
    Princeton, New Jersey 08540

11. Title: Component Failure and Repair Data for Coal-Fired Power Units
    Contact: Mr. Jerome Weiss
    Electric Power Research Institute
    3412 Hillview Avenue
    Palo Alto, California 94304

12. Title: Component Failure and Repair Data: Gasification-Combined-Cycle Power Generation Units
    Contact: Mr. Jerome Weiss
    Electric Power Research Institute
    3412 Hillview Avenue
    Palo Alto, California 94304

13. Title: Diesel Generator Reliabilities at Nuclear Power Plants: Data and Preliminary Analysis
    Contact: Mr. David H. Worledge
    Electric Power Research Institute
    3412 Hillview Avenue
    Palo Alto, California 94304

14. Title: Data Summaries of Licensee Event Reports of Diesel Generators at U.S. Commercial Nuclear Power Plants NUREG/CR-1362
    Contact: Dr. James W. Johnson
    Office of Nuclear Regulatory Research
    U. S. Nuclear Regulatory Commission
    Washington, D. C. 20555

15. Title: Data Summaries of Licensee Event Reports of Pumps at U.S. Commercial Nuclear Power Plants
    Contact: Dr. James W. Johnson
    Office of Nuclear Regulatory Research
    U. S. Nuclear Regulatory Commission
    Washington, D. C. 20555

16. Title: Data Summaries of Licensee Event Reports of Valves at U.S. Commercial Nuclear Power Plants
    Contact: Dr. James W. Johnson
    Office of Nuclear Regulatory Research
    U. S. Nuclear Regulatory Commission
    Washington, D. C. 20555

17. Title: Loss of Off-Site Power at Nuclear Power Plants: Data and Analysis
    Contact: Dr. David H. Worledge
    Electric Power Research Institute
    3412 Hillview Avenue
    Palo Alto, California 94304

18. Title: EdeF Reliability Data System
    Contact: Mr. Henri Procaccia
    Elecricite de France
    25 alle Prives-Carrefour Plajel
    93026 St. Dem'o Cedex 1, France

19. Title: European Reliability Data System (ERDS)
    Contact: Sr. G. Mancini
    Ispra Establishment
    I-21020 Ispra (Varese)
    Italy

20. Title: MIL-HDBK 217D
    Contact: Mr. Lester J. Gubbins
    Rome Air development Center
    Attn: RBET
    Griffiss Air Force Base, New York 13441

21. Title: Nonelectronic Parts Reliability Data (NPRD-2)
    Contact: Mr. Harold Lauffenburger
    Reliability Analysis Center
    Rome Air Development Center
    Griffiss Air Force Base, New York 13441

22. Title: Failure and Inventory Reporting System (FIRS)
    Contact: Mr. L. E. Bennett
    Minerals Management Services (OS-2)
    U. S. Department of Interior
    P.O. Box 7944
    Metairie, Louisiana 70010

23. Title: Government Industry Data Exchange Program (GIDEP)
Contact: Mr. Edwin T. Richards/Mr. William Arnitz
GIDEP Operations Center
Corona, California 91720

24. Title: The Army Maintenance Management System (TAMMS)
Contact: Mr. Raymond W. Beatty/Mr. Kenneth Wasson
DRXMD-MS
U. S. Army DARCOM
Materiels Readiness Support Activity
Lexington, Kentucky 40511

25. Title: Product Performance System - D056
Contact: Mr. Charles W. Gross
HQ AFLC/LOEP
Wright Patterson Air Force Base, Ohio 45433

26. Title: JPL Problem/Failure Reporting System
Contact: Cognizant Engineer
Problem/Failure Control Center
JPL-California Institute of Technology
4800 Oak Grove Drive
Pasadena, California 91103

27. Title: Central Reliability Data Organization (CREDO)
Contact: Mr. H. E. Knee
Oak Ridge National Laboratory
P.O. Box X, Bldg. 6025
Oak Ridge, Tennessee 37830

28. Title: Navy Maintenance, Materiel, Management (3M) System
Contact: Mr. James Kapp
Naval Maintenance Command
P.O. Box 2020, Maintenance Support Office
Code 021
Mechanicsburg, Pennsylvania 17055

29. Title: Microcircuit Device Reliability - Digital Failure Rate Data
Contact: Mr. Harold Lauffenburger
Reliability Analysis Center
Rome Air Development Center
Griffiss Air Force Base, New York 13441

30. Title: Reliability Data From In-Flight Spacecraft
Contact: Mr. Charles Bloomquist
PRC Systems Services
10960 Wilshire Boulevard
Los Angeles, California 90024

The remaining sections of Appendix G document the title, custodian, and contact for selected data sources and give a brief abstract of each for use by the reader.

Title: In-Plant Reliability Data System (IPRDS)

Custodian: Oak Ridge National Laboratory

Contact: Mr. Joseph P. Drago
Oak Ridge National Laboratory
P.O. Box X
Oak Ridge, Tennessee 37830

Abstract: The data base is a comprehensive collection of component population, failures, and repair data for a sample population of operating nuclear generating units. The data were extracted from plant maintenance records and contain the majority of the failure and repair information for non-safety as well as safety class components from the beginning of commercial operation. Preventive maintenance and some contractor-performed maintenance actions are not included.

IPRDS uses a detailed set of generic systems definitions to allow proper aggregation and comparison of components performing the same functions in different plants. The data are selected, encoded and checked by a small group of engineers. Presently, only pump and valve data from 6 nuclear generating units have been encoded.

Title: Nuclear Plant Reliability Data Systems (NPRDS)

Custodian: Institute of Nuclear Power Operations (INPO)

Contact: Mr. Robert Haueter
Institute of Nuclear Power Operations
1820 Water Place
Atlanta, Georgia 30339

Abstract: NPRDS is unique as it results from a self-imposed requirement of all operating nuclear plants within the U.S. The NPRDS collects engineering and failure data on systems and components of Safety Class 1 and Safety Class 2 equipment as classified in ANSI Standard N18.2 for pressurized water reactors, and in ANSI Standard 52.1-1978 for boiling water reactors. Also included is Electrical Class 1E equipment as designated in IEEE Std. 380-1975. Information is collected on 29 major categories of components of mechanical and electro-mechanical designs. From the data base, estimates of components and system failure rates can be derived which can be used to estimate performance of safety systems in operating environment. The NPRDS provides 3 types of output reports to industry participants:

1) Annual Summary Reports of System Reliability (Report A03): provides safety-related system reliability statistics. Data in the report include the normal operating mode to be applied, the period for which the statistics were obtained, the total population of the nuclear unit systems being reported and calculated in service hours, number of failures reported for the period. Other types of information on time (shutdown hours, etc.) are also reported.

2) Summary Report of Component Reliability (Report A04): contains the same type of information given in Report A03 but on a component rather than a system level.

3) Quarterly Component Failure Listing (Report Q02): is distributed quarterly to the industry to provide summary information on all significant component failures.

Title: Collection and Evaluation of Reliability Data at the Nuclear Power Plant BIBLIS B

Custodian: GRS and RWE

Contact: Mr. P. Homke
Gesellschaft für Reaktorsicherheit (GRS) MbH
Glockengasse 2.5000 Koln 1, West Germany (FRG)

Abstract: The Gesellschaft für Reaktorsicherheit MbH (GRS), in cooperation with the Rheinisch-Westfalisches Elektrizitatswerk AG (RWE) on behalf of the Ministry of Research and Technology of the Federated Republic of Germany (FRG), has been developing a reliability data bank in components and systems for risk and reliability analysis. A comprehensive data collection has been carried out in the nuclear power plant (NPP) BIBLIS B since 1977.

The project covered the investigations of 114 process, electrical and control systems. The collected data are stored in a data bank system. A description of the data bank structure and the content of the different data banks is given in the report, "Fuverlassigkeitskenngrossenermittlung im Kernkraftwerk BIBLIS B", GRS-A-532 (December 1980).

SYSTEM 2000 is being used as data base information system, offering the possibility of calculating reliability data on components and systems in NPP under different aspects from the available raw data. The data base information system, their structures and the mechanisms of logical data base links as well as the software developed are described in the report "Ein Informationsystem fur Ermittlung von Fehlerlassigkeitskenngrossen im Kernkraftwerk BIBLIS B", GRS-A-560 (February 1981).

Title: Failure Data Handbook for Nuclear Power Facilities

Custodian: Liquid Metal Engineering Center (LMEC)

Contact: Mr. C. W. Griffin
Liquid Metal Engineering Center
P.O. Box 1449
Canoga Park, California 91304

Abstract: The data in this handbook were taken from six plants, three of which contributed data only on sodium related system component events. A total of 1188 failures were reported and itemized according to: component/part, system/subsystem, facility, location, operating hours, and a description of the failure with a narrative preceding each component data section and summary. A summary of sodium leak information is provided in Section III. Sections covering reliability/availability analysis and maintainability are also included.

Title: Reactor Safety Study (WASH-1400, Appendix III, "Failure Data")

Custodian: U. S. Nuclear Regulatory Commission

Contact: National Technical Information Service (NTIS)
U. S. Department of Commrce
5285 Port Royal Road
Springfield, Virginia 22151

Abstract: Appendix III of WASH-1400 contains the failure rate data and methodology used to compute the system models used in the WASH-1400 study. The goal of this study was risk assessment and reliability analysis. Range values along with point estimates and failure mode frequency were reported. The advantages of WASH-1400 are that it recognizes the importance of failure mode data, standby failure rates and demand probability, as well as the prsentation of ranges in addition to single point estimates. The disadvantages are that WASH-1400 provides data for less than 30 component types. Component descriptions are too general to use the corresponding failure rates for the purposes of any reliability analysis other than the broad type of general assessment attempted WASH-1400 is a useful tool for exploring reliability analysis techniques and applications. The incorporation of ranges and failure mode information is a useful consideration for the developers of reliability data bases.

Title: IEEE STD 500-1977 Reliability Data Manual

Custodian: Institute of Electrical and Electronics Engineers (IEEE)

Contact: IEEE Standards Office
345 East 47th Street
New York, New York 10017

Abstract: The IEEE Reliability Data Manual appears as Appendix D in IEEE STD 500-1977, "Guide to the Collection and Presentation of Electrical, Electronic, and Sensing Component Reliability Data for Nuclear Power Generating Stations." This document contains reliability data in the form of hourly and cyclic failure rates and failure mode information for over 1,000 electrical, electronic and sensing components used in nuclear plants. The data are arranged by generic component listings with separate table and environmental factors to be used in conjunction with the failure rates.

The data include a combination of estimated failure rates by over 200 experts and a data analysis of approximately 25 data sources. The failure rates are presented in low, recommended, high and maximum values for system-related incipient, degraded and catastrophic failure modes to give a range of failure rate information.

The 1977 edition data manual is being updated and expanded to include the mechanical components. Information from individual data sources will be included, along with the synthesized failure rate data. The document is expected to be ready for processing by IEEE Standards Office in December 1982.

Title: Licensee Event Reports (LERs)

Custodian: Nuclear Safety Information Center (NSIC) of Oak Ridge National Laboratory; also Institute of Nuclear Power Operations (INPO)

Contact: Mr. Robert Dennig/Mr. Fredrick Hebdon
Office for Analysis and Evaluation of Operational Data
U. C. Nuclear Regulatory Commission
Washington, D. C. 20555

Abstract: The LER system is designed for licensed nuclear power plants to report "potentially significant events" that could lead to, or be precursors of, a serious accident. Information is reported to the U.S. Nuclear Regulatory Commission (NRC) by utilities; currently about 400 LERs are submitted per month. The LERs include narrative descriptions of events and cover most failures of safety-related components and systems.

A computerized LER abstract file, containing brief event descriptions, has been maintained for NRC by Oak Ridge National Laboratory in the Nuclear Safety Information Center (NSIC). Another computer file of LERs containing all coded data and abstracts has been maintained by NRC Office of Analysis and Evaluation of Operational Data (AEOD). This has been discontinued, but the activity has been picked up by INPO, at least on an interim basis. The two files differ in the format and style in which abstracts are stored and accessed. The NRC has funded a project, the goal of which was to produce gross component failure rate estimates from the LERA. The project was carried out at the Idaho National Engineering Laboratory (INEC) by its contractor, EG&G. To date, reports have been produced on pumps, control rods and drive mechanisms, diesel generators, valves, primary containment penetrations, and instrumentation and control components.

Title: System Reliability Service Data Bank (SYREL)

Custodian: Systems Reliability Service

Contact: Mr. Ian Watson
Systems Reliability Service, UKAEA
Culcheth, Warrington WA3 4NE
England

Abstract: The data bank is used by the United Kingdom Atomic Energy Authority (UKAEA) Systems Reliability Services. It contains information on approximately 900 categories of components collected from operating reactor plants within the United Kingdom. The data bank provides information to contributors in performance, availability and reliability of their own plants and provides generic reliability data to design and reliability engineers of associate numbers of the system.

The types of performance and reliability information offered by SYREL include: Mean time between failures, mean time to repair, minimum and maximum repair time, mean time between maintenance, mean time to maintain, and minimum and maximum maintenance times. Also listed are man and material hourly information.

Title: Generating Availability Data System (GADS)

Custodian: North American Electric Reliability Council (NERC)

Contact: Mr. Ronald Niebo, Director
North American Electric Reliability Council
Research Park, Terhune Road
Princeton, New Jersey 08540

Abstract: The Generating Availability Data System (GADS) is formerly the EEI Equipment Availability Data System. The North American Electric Reliability Council (NERC) assumed responsibility for the operation of EEI data system beginning in 1979. NERC publishes quarterly reports on the performance of medium and large fossil steam units and nuclear steam units. Three sets of microfiche containing the unit specific data and information for each of the unit groupings are included with the report. Two annual reports are also published; a report on equipment availability for the previous 10 years and a companion report on component cause codes for the same period. All the statistics and information were derived from outage and summary reports of over 500 generating units which had been previously included in the EEI data bank.

Title: Component Failure and Repair Data for Coal-Fired Power Units (EPRI AP-2071)

Custodian: Electric Power Research Institute (EPRI)

Contact: Mr. Jerome Weiss
Electric Power Research Institute
3412 Hillview Avenue
Palo Alto, California 94304

Abstract: The failure rates and average restore time for coal-fired power plant equipment were developed using published EEI data, a failure mode analysis procedure, and expert consensus methods. The equipment for which these data were developed is described in the Process Flow diagrams, and the total plant is shown in the Overall Block Flow Diagram.

The report provides tables of equipment failure rates and average restoration times for approximately 100 components. In each component, the relative frequency of occurrence, repair time, startup time, and shutdown time are listed by several principal failure modes. From these an average failure rate is developed and expressed as failures per million hours and mean time between failures (MTBF) on the basis of a time period of one year, including scheduled outages. An average mean time to restore is developed and expressed in hours, which includes startup, shutdown and actual repair time.

Title: Component Failure and Repair Data: Gasification-Combined-Cycle Power Generation Units (EPRI AP-2205)

Custodian: Electric Power Research Institute (EPRI)

Contact: Mr. Jerome Weiss
Electric Power Research Institute
3412 Hillview Avenue
Palo Alto, California 94304

Abstract: The failure rates and average repair times tables were developed for coal-gasification-combined-cycle power plant equipment in the same format as those for coal-fired plants in EPRI Report AP-2071, "Component Failure and Repair Data for Coal-Fired Power Units".

Title: Diesel Generator Reliability at Nuclear Power Plants: Data and Preliminary Analysis. EPRI NP-2433 RP1233-1

Custodian: Electric Power Research Institute (EPRI)

Contact: Mr. D. H. Worledge, Project Manager
Electric Power Research Institute
3412 Hillview Avenue
Palo Alto, California 94304

Abstract: This project covers the collection and analysis of data pertaining to diesel generator reliability in nuclear power plants. The data sources are:

1) Data collected through an on-site review of plant records at 2 plants.

2) Data collected from 4 plants through a review of plant maintenance records.

3) Data supplied by utilities on diesel start attempts and failures for 10 plants.

4) Failure data through a review of Licensee Event Reports (LERs) for 23 plants.

The report gives point estimates of diesel failure to start probabilities at 13 plants and the failure to continue to run at 3 plants based on plant or utility-supplied data. It also provides a composite point estimate for failure to start probability derived from data from all 13 plants.

The report also compares the above estimates with point estimates of diesel failure rates given in NUREG/CR-1362, "Data Summaries of Licensee Event Reports of Diesel Generators at U.S. Commercial Nuclear Power Plants".

Title: Data Summaries of Licensee Event Reports of Diesel Generators at U.S. Commercial Nuclear Powr Plants, NUREG/CR-1362

Prepared by: EG&G Idaho, Inc.

Prepared for: U. S. Nuclear Regulatory Commission (NRC)

Contact: Dr. James W. Johnson, USNRC

Abstract: This report selectively analyzed Licensee Event Reports (LERs) of various diesel-generator events that were submitted to the NRC between January 1, 1976 and December 31, 1978. The pertinent information contained in each LER that described a diesel generator event was coded into a one-line description of the event and then stored in a computer-based data file for obtaining various LER summary statistics.

The report estimated various standby, demand, and operating LER rates for the diesel generators used by all operating nuclear power plants with certain exceptions. These estimates were then averaged to obtain various LER rates for four NSSS vendors considered. Finally, specific plant failure data were averaged to obtain various rates for Pressurized Water Reactors (PWRs), Boiling Water Reactors (BWRs), and for the aggregate population.

Title: Data Summaries of Licensee Event Reports of Pumps at U.S. Commercial Nuclear Power Plants, January 1, 1972 to September 30, 1980. NUREG/CR-1205, Revision 1, EGG-EA-5524

Prepared by: EG&G, Idaho, Inc.

Prepared for: U. S. Nuclear Regulatory Commission (NRC)

Contact: Dr. James W. Johnson, USNRC

Abstract: The Licensee Event Report (LER) Computer File data bank summarizes events reported to the U. S. Nuclear Regulatory Commission. The LERs are sorted according to failure mode, failure mechanism, common cause failures, and recurring failures. Encoding techniques, as well, are described in some detail so as to clarify the sorting process. The codes used for components and systems are identical to NPRDS. Information is listed by plant and by cause of failure if known. Reported failures are used to estimate gross standby and operating failure rates, in units of per hour and per demand, for the selected pumps. Explanation and summary tables of all results are provided.

<u>Title</u>: Loss of Off-Site Power at Nucler Power Plants: Data and Analysis

<u>Custodian</u>: Electric Power Research Institute (EPRI)

<u>Contact</u>: Mr. David H. Worledge
Electric Power Research Institute
3412 Hillview Avenue
Palo Alto, California 94304

<u>Abstract</u>: The report presents loss of offsite power (LOSP) data collected from 47 nuclear power plant sites. The data include 45 events identified as complete losses of offsite power, occurring over 370 site-years of plant operating experience. The data are used to derive estimates of the frequency of total LOSP at plants and the time required to regain offsite power after LOSP, called "recovery time".

As weather conditions were a major cause of LOSP events, and since sites that are geographically close should have similar weather patterns, the data from plant sites in the same geographical region were pooled. The geographical groups chosen were NERC regional reliability councils. LOSP frequency and recovery time estimates were derived for each regional council.

<u>Title</u>: Military Standardization Handbook. MIL-HDBK 217D

<u>Prepared for</u>: Rome Air Development Center

<u>Contact</u>: Mr. Lester J. Gubbins
Rome Air Development Center, Attn: RBRT
Griffiss Air Force Base, New York 13441

<u>Abstract</u>: Military Standardization Handbook for Reliability Prediction (MIL Handbook 217D) is the third update (4th handbook) of reliability data collected by the military on components used by them in different environments. It has had historically about a 5 year reprint cycle. Compoents are grouped in general categories. Factors are supplied for conversion of the overall part failure rate to a more specific type used in a particular environment multiplying it by constants. There are also equations whereby hourly failure rate information can be translated to a cyclic mode by multiplicative factors. Basically, failure rate information is given for the broadest generic categories with information for the subcategories being derived by use of the aforementioned factors. Point estimates are used for the failure rates with information given on components used in military environments. The amount of information in MIL HDBK 217D is useful for calculating failure rates for the same type of equipment. The use of environmental factors for modifying failure rates are important.

Title: Failure and Inventory Reporting Systems (FIRS)

Custodian: Minerals Management Services, U.S. Department of Interior

Contact: Mr. L. E. "Gene" Bennett
U. S. Dept. of Interior, Minerals Management Services (OS-2)
Post Office Box 7944
Metairie, Louisiana 70010

Abstract: The FIRS program was developed by the Geological Survey Division of the U.S. Department of Interior for Safety and Pollution Prevention Devices on offshore structures which produce or process hydrocarbons. The system is composed of two programs. The Safety Device Inventory Reporting program provides information depicting the number of safety and pollution devices by type, manufacturer, and model which are in service on the offshore platforms. The Safety Device Failure Reporting program provides information relative to failures of these devices by failure causes, corrective measures, device types, manufacturer, model and frequency of failure. Failure percentages, reliability and quality trends, mean time between repairs, and mean time between failures, along with their statistical information, are derived from these data.

The FIRS program furnishes an industry-wide exchange of experience and information in the offshore oil industry. The program will demonstrate the effectiveness of an aggressive corrective action policy and should significantly shorten the period of time required to identify problem areas.

Title: Nonelectronic Parts Reliability Data (NPRD-2)

Prepared by: Robert G. Arno, IIT Research Institute

Prepared for: Rome Air Development Center (RADC)

Contact: Mr. Harold A. Lauffenburger
Reliability Analysis Center, RADC
Rome Air Development Center (RBRAC)
Griffiss Air Force Base, New York 13441

Abstract: This data base was developed by the Reliability Analysis Center at Griffiss AFB providing failure rate information on non-electronic parts. Failure rate information is supplied as generic point estimates with 60% chi-square bounds as a range. This data source recognizes that inhomogeneous data classes should not be merged, and uses the Fisher F test to determine homogeneity. This report is organized into four major secions; Generic Data, Detailed Data, Application Data, and Failure Modes and Mechanisms. Reliability information for more than 250 major non-electronic part types is based on test, field operation, and dormant state conditions.

Data are collected on a continuous basis from a broad range of sources including test laboratories, device and equipment manufacturers, government laboratories, and equipment users, both government and non-government. Automatic distribution lists, voluntary data submittal, and field failure reporting systems supplement an intensive data solicitation program.

Title: Government Industry Data Exchange Program (GIDEP)

Custodian: GIDEP Operations Center

Contact: Mr. William Armitz/Mr. Edwin T. Richards
GIDEP Operations Center
Corona, California 91720

Abstract: GIDEP is a cooperative program for exchanging data and has approximately 650 participants from both government agencies and industrial organizations. The program provides a means of exchanging technical data used in research, design development, production, and operation of systems and equipment used mainly in electronic or electro-mechanical application.

GIDEP incorporates the Failure Rate Data Program (FARADA) which is jointly sponsored by the Army, Navy, Air Force, and NASA. The FARADA program comprises the collection, analysis, compilation, and distribution of failure rate and failure mode data.

Participants in GIDEP are provided with access to four major data interchanges: (1) engineering data, (2) methodology data, (3) reliability-maintainability data, and (4) failure experience data. The data bank includes field experience data, laboratory accelerated life testing data, and reliability demonstration data.

GIDEP produces "Summaries of Failure Rate Data" and "Summaries of Replacement Rate Data". The first includes failure rate information, population and failure mode information, when known. The latter includes similar information on replacement data.

APPENDIX H

SAFETY PARAMETER DISPLAY SYSTEM (SPDS)

AND

DISTURBANCE ANALYSIS AND SURVEILLANCE SYSTEM (DASS)

SAFETY PARAMETERS DISPLAY SYSTEMS/DISTURBANCE ANALYSIS AND SURVEILLANCE SYSTEM (SPDS/DASS)

Regulatory Background

The safety parameter display system (SPDS) was a natural outgrowth of Appendix E to 10 CFR 50, which defined the requirements for an onsite technical support center and a near site emergency operations facility (as well as the control room) from which effective direction can be given and effective control can be exercised during an emergency. In order for these facilities to be able to perform their intended functions a data display system was required. NUREG-0696 identified the criteria for the SPDS, as well as for those facilities referenced above.

A summary of the significant points of NUREG-0696 is as follows:

- Its purpose is to assist control room personnel in evaluating the safety status of the plant.
- It will be an operator aid, by concentrating a minimum set of plant parameters in one place.
- It shall provide continuous indication of plant parameters, during both normal and emergency operating periods.
- It shall have a real time display.
- Human factors shall be incorporated into the design (4).
- It shall be capable of presenting the magnitudes and trends of parameters.
- The system shall be located in the control room with displays in the technical support center and the offsite emergency operations facility.
- There shall be a primary display which addresses five minimum plant functions (reactivity control, core cooling/primary system heat removal, reactor coolant system integrity, radioactivity control and containment integrity).
- There shall be secondary displays which provide additional detail on each of the primary display functions.

Prototype Testing

Westinghouse performed a study for the Electric Power Research Institute using two SPDS panel prototypes (6). The objectives of the program were to assess the benefits and potential problems with SPDS in the control room, to evaluate the potential aid in decision analysis, and to assess the use of a training simulator as a tool for proposed control room modifications.

As previously mentioned two SPDS panel prototypes were tested on a training simulator during operator training. The panel types were first, a 30 minute time history of key variables and second, a polargraphic display. Selected events were introduced into the simulator according to a test plan. Examples of events were: LOCA feedwater break, loss of FW, stuck open PORV and steam generator tube rupture. The operator crews were given some initial exposure time and then were tested on each accident/event only once.

The test results indicated that SPDS panels were useful in aiding problem recognition, although not in analysis and decision making.

The shift supervisors used the panels more than the operators. When the operators were implementing specific procedures, the panels were not consulted. Some necessary improvements in panel design were also uncovered during the testing.

Although unrelated to the panel usage, some interesting points about crew behavior and decision analysis were noticed during testing. It was also concluded that, for the SPDS to be successful, a usage pattern must be specified, incorporated into the design, into procedures, and into training.

Commercial Systems

Over twenty vendors are offering SPDS designs, from reactor vendors to architect engineers, to designs by individual utilities. The number of parameters displayed ranges from 35 to 1000. The costs of these systems vary from $0.5 to $8.0 million (7).

The display types used are horizontal and vertical bar charts, polargraphic, pressure-temperature plots, alarm boxes and alphanumeric tables.

Some of the common design features are as follows:

- The parameters are organized by plant function.
- Measured as opposed to derived variables are used.
- CRT's are the preferred method of dislay, although a hard wired system is available.
- Lower level dislays use P&ID mimics or trend graphs.
- Alarm conditions are indicated by color changes, blinking lights, audible signals and limiting conditions on graphs and charts. (Most operators oppose the use of audible alarms, which can be confused with the main control board alarms).

An EPRI sponsored SPDS is presently being installed at the Yankee Rowe plant. Software development has been the major cost factor (45%) while interface with existing plant equipment (28%) and hardware procurement (19%) are the other significant cost items.

The SPDS systems that are presently being offered vary from the type that comply with the minimum requirements of NUREG 0696 up to sophisticated systems with the flexibility to become a integral part of larger data acquisition systems, such as a disturbance analysis and surveillance system.

DISTURBANCE ANALYSIS AND SURVEILLANCE SYSTEM

The purpose of a disturbance analysis and surveillance system (DASS) is to assist operators with the timely identification and correction of plant disturbances that otherwise might impact safety and availability. It is a central data based computer system which employs a multi-level analysis methodology. Plant data is processed and made available to the plant operator in a prioritized fashion.

EPRI has issued two reports on this subject. The first report, Phase I DASS (8) was issued in May 1980. For this report, a prototype DASS was developed for two plant subsystems and tested with operators at a simulator. The systems that were modeled were the feedwater control system and the component cooling water system. It was hoped that DASS could aid and assist the operators in identifying the nature of the disturbance and possible corrective actions, in reducing extraneous alarms, and in predicting the future propagation of disturbances if uncorrected. The test results indicated that DASS provided the operator with an earlier warning than conventional alarms and that the operators were able to reduce the deviation of key plant parameters from normal. The tests also showed that operators initiated control action very rapidly in response to either a DASS message or alarm. However, incomplete models did create some problems, by giving some incorrect and incomplete messages. It must be kept in mind that this test was optimized in that the operators performing this test only had to monitor these two systems. At the time of this project, it was estimated that 5-10 man years would be required for DASS development.

The second EPRI report, Phase II DASS (9) was issued in July 1982. The purpose of this project was to assess the scope and feasibility of developing a plant wide DASS, with the objectives of aiding operators in preventing plant disturbances, terminating them if they occur, and in mitigating the consequences should they occur.

DASS models were developed for plant operators, for plant processes and subsystems, and for plant disturbances. The development of these models led to the following program results:

- Systems and equipment functional relationship charts for safety and availability.

- Assessment of engineering talent necessary to develop a DASS design.

- A set of well defined DASS functions.

- Detailed engineering models of each of the DASS functions.

- Development of elementary human factors models.

- Informational requirements of the operator's mode of behavior.

- Preliminary cost/benefit ranking of the identified DASS functions.

It was estimated that 25 man years would be required for the engineering, 15-20 man years for the software with a computer hardware cost of $1-2 million.

The next step in the EPRI programs will be to develop a more modest DASS, a system that will be consistent with previous findings, but will monitor a limited set of parameters.

BIBLIOGRAPHY - APPENDIX H

1. American National Standard, "Functional Criteria for Data Acquisition and Recording for Transient Reconstruction in Nuclear Power Plants," ANSI/ANS - 4.6, Draft 8.

2. U.S. Nuclear Regulatory Commission, "Instrumentation for Light Water Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident," Regulatory Guide 1.97, Revision 2, December 1980.

3. U.S. Nuclear Regulatory Commission, "Functional Criteria for Emergency Response Facilities, NUREG-0696, Final Report, February 1981.

4. U.S. Nuclear Regulatory Commission, "Human Factors Acceptance Criteria for the Safety Parameter Display System," NUREG-0835, Draft Report, October 1981.

5. Daryl L. Harman, "SPDS Review," for EPRI by DASS Phase III Design Group, November 1981.

6. Westinghouse Electric Corporation, "Evaluation of Safety Parameter Display Concepts," EPRI Final Report NP-2239, February 1982.

7. A.B. Long and D. Cain, "Safety Parameter Display Systems: Criteria for Success," presentation before ACRS, March 17, 1982.

8. Combustion Engineering Inc., "On Line Power Plant Alarm and Disturbance Analysis System," EPRI Final Report NP-1379, April 1980.

9. Westinghouse Electric Corporation, "Disturbance Analysis and Surveillance System Scoping and Feasibility Study," EPRI Final Report NP-2240, July 1982.

10. Technology Development of California, "Nuclear Plant Data Bank," presentation before Nuclear Rgulatory Commission, May 1982.

APPENDIX I

NATIONAL TRANSPORTATION SAFETY BOARD (NTSB)

FEDERAL AVIATION ADMINISTRATION (FAA)

SAI/NY R 82-9-18

Commercial Air Industry Operations Regulation
and its Relation to
Commercial Nuclear Power Industry Operations Regulation
A Quick Comparison

Prepared by:

Joseph R. Fragola
Principal Investigator
Science Applications Inc.
274 Madison Ave.
New York, N.Y. 10016

Prepared for:

Dr. Walter Kato
Deputy Chairman
Department of Nuclear Energy
Brookhaven National Laboratory
Upton, N.Y.

29 September 1982

Revised 12 October 1982

2nd Revision 14 October 1982

TABLE OF CONTENTS

FOREWORD

This study was undertaken for Brookhaven National Laboratory in support of a broader based NRC study in which they are engaged, whose objective was to review the overall data needs, requirements and current capabilities of the commercial nuclear power industry as they relate to nuclear regulation. During the course of the study it was decided to review alternative government agency approaches to the problem of data collection. Initial attention was given to the activities of NASA in this regard. However, it was quickly discovered that while the NASA PRACA system was well suited for a developmental technology, it was decidedly unsuited for an operational commercial technology.* The attention of the effort was then turned toward the commercial aviation industry. Initial contacts with this industry and its regulators indicated a greater degree of comparability to commercial nuclear power. For this reason, it was decided to investigate the problems, the history, and the current status of commercial aviation regulation as they relate to data collection and use, and to compare the experiences and approaches to commercial nuclear power regulation.

The study indicated that, while it would be far from true to suggest that the situations are identical, there are enough similarities** of a fundamental nature to indicate that a transfer of regulatory technology might be fruitful. By the very nature of the study the results would be expected to be somewhat one-sided, and the reader might get the impression that commercial aviation has solved all the problems and has all the answers. This impression is far from correct. What is correct is that while the problems addressed by commercial aviation are similar, they have been addressing them for a longer time and have developed regulatory approaches which would probably be considered novel in the commercial nuclear power industry.

The novelty of the approaches, of course, does not guarantee their correctness, nor even their transferability if correct, but it does make them worthy of consideration especially in light of the nuclear industry's investigation of alternative regulatory approaches in response to recent executive initiatives such as Executive Order 12291.

---

*It is interesting to note that NASA appears to be coming to a similar conclusion concerning the operational phases of the space shuttle program. This fact is witnessed by the award of a recent $50K contract between the shuttle prime contractor, Rockwell International, and Pan American. This study is intended to apply the commercial aviation approach to the space shuttle system.

**The similarities of the two extend to the issue of safety goals. The FAA has recently issued a notice of proposed rulemaking that would change the FAA approach of regulating airline safety to one of "Regulation by Objective" (RBO). This approach specifies safety goals for airline operations and provides the industry with the option of devising innovations to meet the specified goals.[7]

1.0 Purpose

This study was directed at investigating the relationships between the regulatory bodies and the commercial operators involved in the commercial aviation industry. The investigation was undertaken in an attempt to understand the relationship between these two groups at the present time and the history of its development over the last 10-15 years, and to attempt to draw parallels between and to gain insights from this relationship and the relationship between the U.S. Nuclear Regulatory Commission and the commercial nuclear power industry.

2.0 Scope

The study was restricted by time and funding constraints to telephone contacts between the principal investigator and a representative group of major domestic air carriers, and their associated regulatory bodies, that is, the Federal Aviation Administration (FAA) and the National Transportation Safety Board (NTSB). The study considered only the operational aspects of the air carriers and therefore did not attempt to address the aircraft air worthiness certification activities of the FAA.

3.0 General Observations

The domestic commercial air industry is regulated by several government agencies. The two agencies which are most relevant to this study are the FAA and the NTSB. The FAA has been organized as a part of the Department of Transportation since 1967, and the NTSB has been an independent agency since 1975. The FAA is primarily responsible for certifying the airworthiness of an aircraft type, and monitoring air carrier operations. The NTSB is responsible for accident and significant incident investigation.

Over the past decade and a half the FAA has worked in cooperation with the commercial carriers in an attempt to find a way to allow demonstrated operational performance to be substituted for hard and fast regulatory rules without sacrificing legitimate regulatory needs. This cooperation has resulted in a regulatory approach which has been embodied in several FAA regulatory guidance documents (in particular, advisory circulars 120.17 and 121.22). Both sides agree that this approach has brought order and stability to their regulatory environment. Both sides also agree that this was accomplished because the FAA provided for direct economic advantages to be given to operators whose performance had demonstrated improvement as judged via a pre-agreed upon criterion or criteria. This aspect of the program provided an ever present incentive for each carrier to improve performance beyond their current level (rather than reach some pre-set fixed limit and then stop). Both agreed that, while it would greatly over-simplify the situation to say that the introduction of this cooperative approach alone has been responsible for the greatly improved performance and safety record during the period, there is no disagreement that the program was a significant contributor.

The NTSB exercises its reponsibility through use of an intensive after-the-fact incident report (NTSB Form 6120.4F), and through the data collected via two onboard instruments, the Digital or Analog (Oscillographic) Flight

Data Recorder, and the Cockpit Voice Recorder. The requirements for these devices have been developed over a number of years via joint discussions between the regulators, the aircraft manufacturers, and the air carriers under the auspices of ARINC. The current requirements are embodied in three ARINC standards (717, 573 and 557). Contacts were made with three individuals at the NTSB. Each was familiar with the requirements of, and the analysis of, data from the individual recording device within their purview. The results of these contacts are presented in Section 4.3.1.

4.0 Major Study Conclusions

As a result of the study, the following major conclusions have been reached. Where appropriate, the conclusions have been separated between FAA and NTSB. The general basis for these is discussed and explained in a subsequent section of the study report.

A. General Conclusions

The FAA/NTSB relationship with the commercial air carriers appears to be in many respects analogous to the relationship between the NRC and the plant operators (licensees).

B. FAA Conclusions

1. In the commercial aviation industry, the relationship has moved from an adverserial one to a more cooperative one over the past decade and a half.

2. This change in relationship has provided for the development of an orderly process for stabilizing the regulatory environment.

3. The initiation of FAA approved reliability programs on the part of the carriers has been a key aid in this transition.

4. The carriers were economically motivated to initiate these programs because they were assured they would receive direct regulatory relief from fixed operational limits by having an approved program in place.

5. This change in the regulatory environment has played a major role in the significant improvement in overall passenger safety, aircraft utilization, and performance which has occurred over the past decade and a half.

6. Whie there are significant differences between the two industries, there are enough similarities, and the potential benefits of regulatory stability are of such importance that the application of air carrier experience to commercial nuclear power regulation should be explored further.

7. The success of this application will be directly proportional to the directness of the tie between licensee participation and consequent regulatory relief to provide an economic incentive for the participants based upon their degree of participation.

C. NTSB Conclusions

1. The NTSB post-accident or incident investigation relies heavily on two sources of information:

a) Recorded real time information collected on board the aircraft,

b) NTSB Accident/Incident Reports filed after the accident.

2. Both of these sources of information include both numerical information as well as narrative information.

3. While each of these forms of information is valuable, it is the correlation between the two which is of greatest value and the value of an individual source would be greatly diminished without the existence of the other.

4. The availability of recorded real time information of aircraft data and cockpit voice communication and the contemporaneous correlation of the two provide key insights into post-accident analysis.

5. The combination of real time recorded plant state vector data and control room voice would appear to have, based on the analogy to the aviation industry, very significant advantages over recording of state vector data alone. On this basis it is strongly recommended that it be considered.

4.1 General Conclusion Basis

The regulatory environments of the commercial air operations and the commercial nuclear power industry are believed to be comparable due to the following similarities:

1. Both are commercial industries providing services to the general public.

2. Both are regulated by federal agencies and operate under government licensure.

3. In both cases the operators/licensees are not the designers and builders of the systems which they operate.

4. Each licensee has its own approach toward operation which has been developed to fit its own corporate style and fleet/plant complement over a number of years.

5. The ultimate responsibility for safety rests with the licensees in both cases.

6. There is a high public awareness of accidents in both cases.

7. In both industries economic success is based upon maintaining high levels of utilization on existing major capital investments.

8. A safety problem on the part of one licensee affects all licensees.

There are, of course, differences between the two which are by no means insignificant. Among these are:

1. Differences in perceived vs. actual risk, and the voluntary vs. involuntary risk argument.

2. The economics of the air industry are regulated by a federal agency which has recently attempted deregulation. In the nuclear industry the economics are regulated by state utility regulatory bodies which have not shown this attitude to any significant degree.

3. The public perceives a real and current need for air travel, the need for nuclear power is less clear to them, and there exists a considerable anti-nuclear lobby.

4. The capital investment per aircraft is at most in the $60-70M range (747) and most often much lower. The capital investment in a nuclear plant is upwards of $2B.

5. The lost downtime for an aircraft is directly felt, and while recoverable via replacement aircraft, this increases fleet size and thereby operating cost without any corresponding increase in revenue. This means increased availability can be measured in real dollars. For a nuclear plant the cost of downtime is considerably more (maybe $500-750M per day), but the cost of replacement power is oftentimes recoverable through rate adjustments. Thus, increased availability is only measured in real dollars under certain circumstances.

6. A nuclear plant (single unit) has more than 25,000 components (line replaceable units); an aircraft has at most 5,000-6,000.

However, despite the above (as well as other) differences, it was felt that the similarities are such that much could be gained from reviewing the commercial air regulatory environment. It is believed that the results of this short study have borne this out.

4.2 FAA Conclusions Basis

During the days prior to the introduction of jet aircraft into the commercial fleets, the FAA regulated the carriers by mandatory specific fixed intervals for certain overhaul operations. These overhaul intervals were based upon extrapolations from the early automotive industry experience in which the air industry had its roots. Subsequent to the introduction of jet aircraft, it became obvious that a new philosophy needed to be developed. Both the industry and the FAA recognized that the fixed time approach was counter-productive to the overhaul of many components (as witnessed by their increased unscheduled removal rate following overhaul). However, "hard time" extensions were grudgingly and unsystematically awarded based upon regional preferences and the judgments of individuals involved in the decision making. This approach produced disorder, instability, and inconsistencies in the regulatory environment, forcing each side to protect and defend their decisions based upon argument. The development of an alternative systematic approach was undertaken by some of the major carriers to set the regulatory decision making on a firmer data base. This base included semi-quantitative and statistical quantitative information and analytical decision making features that were structured in an organized "Reliability Program". The philosophy of the approach was embodied in the dual concepts of Maintenance Steering Groups (MSG), and Maintenance Review Boards (MSB). These concepts were agreed to by both the FAA and the industry and were documented in a series of FAA advisory circulars. The acceptance of this approach converted industry/regulatory discussions into whether or not the individual carrier's program was acceptable and how it could be made acceptable. Once the program was implemented, the carrier was free to operate essentially as he wished as long as he stayed within the requirements of his proposed program. If he performed better than expected (according to pre-agreed criteria), he could take immediate steps to take advantage of this performance with the FAA performing an oversight function.

To take advantage of these benefits, the carrier had to make an investment in the establishment of a reliability program and its associated program elements (alerts, failure review and analysis, reliability control review meeting, data collection and data reporting), but he was provided incentive to do so because he knew this would allow him to remove some of his components from strict hard time limits and thus improve his aircraft utilization. Carriers that did not wish to participate were not penalized, but were required to stay under the prior "hard time" system. This allowed the FAA to apply regulation in proportion to cooperation, and regulatory relief based upon demonstrated performance according to pre-agreed criteria. For these reasons all carriers were encouraged to establish programs (except when their small fleet size made the investment uneconomical), and those that had them established were encouraged toward ever better performance, whereas in the past they had no economic incentive to do better than the performance which was the direct result of the application of the strict limits.

This new emphasis allowed the FAA to concentrate on regulating the performance of the carriers under its jurisdiction rather than on the specific means by which this performance was achieved. The means were left to the carriers with the understanding that the FAA would audit their programs on a continuous basis and that they would be required to have in place an in-house system which would ensure continuing analysis and surveillance of the implementation of their approach. They were also responsible for reporting on a regular basis items of significance to the FAA. Once the program was in place, the carriers were free to implement operational changes on their own, provided that these changes were made in accordance with their program and that the FAA was advised of the reasons for and the nature of the changes. In the beginning many changes were suggested and accepted by the FAA on this basis; however, now the carriers contacted indicated that very few changes take place.

The system is not perfect, and in fact a recent study by the National Academy of Sciences [5] indicates that although the carriers maintain and monitor records on failures and significant events, the FAA's own data systems are deficient. In particular they stated:

> "The information gathering mechanisms presently used by the FAA are a collection of individual systems that have come into being at different times in response to the identification of particular problems. In the past Congress and the General Accounting Office have found that the FAA's data base and communications system are inadequate both in scope and practice for the modern aviation system.

The individual systems have little or no common basis for cross-correlation of information. Consequently, information in these data systems is often not available in a timely fashion, not able to be cross-referenced, and not presented in a format that can be easily used."

This problem could be a direct result of the FAA reliance on the carriers to maintain their own data bases in-house, and should be recognized as something to be guarded against if a system is implemented in the nuclear industry. (Note: The FAA has recognized this problem and is in the process of developing a modern, comprehensive information and data processing system.[5,7]

In the nuclear industry some utilities have already established reliability organizations (e.g., Duke Power Co.[8]. The idea of measuring the reliability performance of a unit is by no means a new one, at least as far as plant availability is concerned.[9] What may appear new is the investigation of relaxing regulatory requirements based upon reported performance (e.g., increasing the allowable maintenance time on a redundant unit before plant shutdown is required based upon the demonstrated past performance of the unit). However, even this idea is included, at least qualitatively, in some nuclear documents such as IEEE Std. 279-1971.[10]

4.3 NTSB Conclusions Basis

The National Transportation Safety Board is an independent government agency separate from the FAA. It is responsible for investigating, determining accident cause, making safety recommendations, and reporting the facts and circumstances of all U.S. civil aviation accidents, as well as other accidents within its scope. In addition, the Board makes recommendations on matters pertaining to transportation safety. Contacts were made with three individuals at the NTSB, as well as other individuals who had interfaced with the NSTB in the development of standards, and in accident investigations. These contacts indicated that the NTSB interest is limited to accidents and incidents which could be described as accident precursors. They do not get involved in the detailed historical data analysis process except on an ad hoc basis after an accident occurs.

Over the years, the Board has established two general methods of providing them with the information necessary to conduct their investigation:

1. The collection of a real time on-board information on a continuing recycle basis.

2. The collection of past-accident information via investigator reporting and interviews with witnesses.

4.3.1 On-Board Data Collection

The NSTB requires that two devices be carried on board commercial aircraft. These devices are the Cockpit Voice Recorder (CVR) and the Flight Data Recorder (FDR).

Cockpit Voice Recorder (CVR)

The first device records all cockpit to cockpit (via headset microphone and cockpit via microphone) cockpit to ground, and ground to cockpit communication on a recycling basis for post-accident analysis. The use of CVRs had been proposed as early as 1959, but serious discussion concerning making them a regulatory requirement occurred in 1963. By 1966 they were required to be carried on all commercial aircraft. The first readout of a CVR also occurred in 1966 as a result of a 707 crash investigation. The NTSB currently engages in 30-40 analyses of CVR tapes per year (world-wide). The analysis of the tape involves the cooperation of the FBI magnetic tape processing lab, which possesses extensive expertise and has unique hardware capabilities in this field. The FBI helps in enhancing and separating out various features recorded on the tape. Originally the devices were designed to record all sound in the 350-3500 Hz range. These specifications were developed to match the limits of human voice capabilities. However, it was found that sounds other than voice were of extreme value and NTSB is now rewriting the specification to include everything between 100-6000 Hz. The capacity of current recorders is approximately 200-300 hours prior to recycle.

At most only 10% of the recorders are lost. These are pimarily when the crash occurs over water of such depth that recovery is impossible. Only 5 recorders have been lost due to the results of a crash (i.e., fire). The NTSB felt that CVR data is a significant contributor to 90% of the accident investigations undertaken.

The recorder is basically a commercial type multi-track tape recorder, but it is built to standard specifications that ensure retrievability, reliability, survivability, and accurate post-accident time correlation. The standard for this device was developed over time jointly by the NSTB, FAA, air carriers, aircraft manufacturers, and device manufacturers via a consensus process under the auspices of ARINC Inc. of Annapolis, Maryland. The standard, which is designated ARINC-557, is reviewed periodically and updated as required. The device is manufactured by Fairchild and Sunstrand.

The information contained on this device has been of considerable value in post-accident investigation (as can be seen from reading the transcriptions of the tape of Air Florida Flt. 90 accident at Washington National Airport.[4] However, by itself the data can sometimes be misleading. The NTSB, in recognition of this fact, always attaches a warning to the readers of CVR transcripts. A representative warning is as follows:

> "The reader of this report is cautioned that the transcription of a CVR tape is not an exact science but is the best product possible from an NTSB group investigative effort. The transcript or parts thereof, if taken out of context, could be misleading. The attached CVR transcript should be viewed as an accident investigation tool to be used in conjunction with other evidence gathered during the investigation. Conclusions or interpretations should not be made using the transcript as the sole source of information."

Flight Data Recorder (FDR)

1. Analog (Oscillographic) Recorders "Scratch Recorders"

Devices designed to record aircraft parameters for post flight analysis have been available since the early days of aviation. Charles A. Lindberg carried an early foil recorder on his historic flight in 1927. This device provided the documentary evidence required to prove his accomplishment. This early design (which is now on display in the Smithsonian) utilized pen scratches in metallic foil that was slowly but continually advancing. The pens recorded the analog output of instrument readings such as altitude and heading, thus providing a permanent record of the trip. This basic design was improved upon and developed into a device by an engineer employed by General Foods Corporation in the 1950's. This 1950's design is the basis for both the Fairchild and Sunstrand "Scratch Recorders" (so called because the record is still made by oscillographic scratches by a pen in metallic foil). In 1960 recorders were required on all turbine aircraft. These scratch recorders record basic aircraft parameters such as altitude, magnetic heading, and vertical acceleration on a foil which advances at a rate of 0.1 inches per minute. These are the devices carried on all current aircraft other than the wide body aircraft (747, DC10, L1011). This includes even the newer designs such as the 737 because it was not designated a "wide body". The devices are built to ARINC standard 573 (with the exception of British aircraft which carry scratch recorders with 0.2 inch per minute resolution and record pitch, roll, and engine parameter in addition to the standard set).

When the standard was originally set, the analysis of accidents was developing. For this reason the original parameter set included navigation parameters which are no longer a problem. The NTSB now recognizes they need parameters which are more performance related. Originally the microscopic analysis of FDR foils was done by the National Bureau of Standards for the NTSB, but now they do their own analysis. The current feeling is that scratch recorders are not adequate for current post accident analysis and they hope to replace all scratch recorders on aircraft with digital devices using more advanced recording media.

2. Digital Flight Data Recorder (DFDR)

This device is built again to an ARINC Standard, ARINC-717, and records digital data on aircraft performance, and systems activation parameters. The parameters which are required to be recorded have been adjusted over the years and the specific required parameter list on current devices was not available to the principal investigator at the time of the study. However, it was determined that current regulations require that 19 parameters be recorded. These are recorded on a 25 flight hour recycle basis. The recording medium is currently magnetic tape and the record rate is 64, 12 bit word per sec. The sampling rate depends on the actual number of parameters chosen, and is specified by the aircraft operator. The 19 required parameters are specified by 14CFR25 and 14CFR121, and include altitude, air speed, heading, pitch, roll, vertical acceleration, longitudinal acceleration, lateral acceleration, engine thrust or power, control surface position or control inputs, and microphone keying information. In addition to these required parameters, the operators add as many as 70 or 80 additional voluntary parameters. On the average, the voluntary additions are about 30-35. Also, it should be noted that many U.S. domestic carriers record only the required 19. This is because of the economic impact of adding instrumentation to their aircraft. The most active voluntary contributors are government-sponsored non-domestic carriers.

The current research of NTSB involved looking into alternative recording media such as bubble memory and solid state memory, and increasing the number of required parameters. The latter research is the result of the development of digital flight instrumentation in new aircraft. Since this instrumentation does not leave "witness marks", there is a real and current need to record the instrument readings. This need is also present due to the more complicated interaction between the flight crew and the auto-pilot system on modern aircraft. Interviews conducted with individuals involved in the development of the standard and in the use of the data for post accident investigation attested to the value of the data recorded from an accident investigation standpoint. But again the data by itself can be somewhat misleading and it would be dangerous to base conclusions or interpretations on the FDR data alone. The individuals contacted all indicated how important the recording of event timing was because of its value in contemporaneous post accident analysis.

4.3.2 Post Accident Information Collection

The post accident/incident data collection activities of the NTSB are essentially two-fold:

1. NTSB Accident/Incident Reports using NTSB Form 6120.4F (1/82)

2. Interviews with individuals involved and eyewitnesses to accidents or incidents

NTSB Form 6120.4F (1/82)

The NTSB has developed an intensive post-accident investigation form over the years. It has been reviewed and revised periodically, with the latest version dated January 1982 and designated 6120.4F. The previous version was revised in September 1980, but the basic information base dates back to the 1970 time frame. The data collection is an attempt at the development of structured analytical data and narrative in all areas pertinent to the accident or incident. In its current form the report includes the following data areas:

Section I - Aircraft Information

- Aircraft data (registration number, year, make, model, S/N, etc.)
- Power plant data
- Aircraft performance equipment
- Fuel/load data
- Aircraft weight and balance
- Aircraft weight and balance at accident
- Sketch of crash site (plan view and elevation view)
- Impact sequence
- Principal impact
- General damage assessment

- Narrative of impact sequence
- Aircraft exit data
- Cockpit documentation
- Emergency locater transmitter
- Emergency lights and survival equipment
- Aircraft wreckage documentation
- Tests and examinations
- Aircraft system malfunction/failure and/or incorrect part

Section II - Environment Operations

- Search and rescue, firefighting and medical treatment
- Basic accident/incident data
- Airport/airstrip data
- Runway data
- Facilities (enroute and airport/airstrip)
- Air traffic control
- Operational aspects
- Weather briefing and weather forecasts
- Weather conditions at accident site
- Weather at airport/airstrip

Section III - Personnel Data

- Inquiry summary
- Pilot-in-command data
- Air traffic controller(s) data

Narrative Statement of Facts, Conditions and Circumstances

Supplement I - CVR/FDR on Aircraft
Identification and Post-Accident Condition

Supplement B - Occupant Injuries and Survivability

Post-Accident Interviews

Not much information on the form and substance of these interviews was able to be determined in this study due to the constraints. However, it is known that these do take place via both testimony at formal hearings and via on-site interviews. The data collected are utilized to provide for some information contained in 6120.4F and as supplemental information to support the other investigatory tools.

4.3.3 Summary and Conclusions NTSB/NRC

Although the time and effort available were not extensive, the principal investigator was able to come to the following conclusions:

1. The NTSB system works because of the availability of diverse tools which supplement and complement one another. The NTSB has concentrated on function diversity in the specification of its investigatory tools. It is the combination of all of them that makes the system effective. An investigation using any one taken out of context could be misleading.

2. In both the real time and post-accident tools, both structured data collection and narrative information are collected, and it is the opinion of the analysts that while in an individual accident one or the other may prove most valuable, it is the cotemporaneous analysis of both of these types of information that allows for accurate and adequate accident investigation.*

3. If the NTSB analogy holds for the nuclear industry, then the following conclusions are obtained:

a) For significant nuclear industry accidents/incidents (i.e., those occurring on a several times a year basis or less), a systematic accident/incident investigation approach should be taken. This approach should include all the equivalent real time and post-incident investigatory tools of the NTSB to ensure the functional diversity required (i.e., both data and narrative).

b) That a real time recording system by established for all nuclear units. That this system include both voice and plant state vector information, to be recorded on a recycle basis in a form which will allow for post-incident cotemporaneous analysis.

c) That plant control room operators be instrumented (i.e., provided with headsets), and that control room area conversations as well as input/output conversations be monitored (both phone and page systems) to provide input to this Control Room Voice Recorder. (Note: There is already precedent for this in the load dispatch centers of many U.S. utilities.)

d) That this recorded information be maintained at the plant and provided to the NRC upon request following a significant accident or incident.

e) That the detailed implementation of these recommendations, including the decisions concerning parameter identification, parameter format, recycle times, storage times and allied issues, be decided on a consensus basis under the auspices of some broad based standards coordinating body such as the American National Standards Institute.

---

*See, for example, the Air Florida 737 Accident Report of the NTSB [11].

5.0 Study Approach

Because of the short time available for the gathering of the information necessary to complete this study, it was decided that the principal investigator would rely on telephone interviews for the source of his information. The spectrum of groups to be contacted was decided jointly by the PI, BNL staff and NRC staff; however, the choice of the particular individuals was the PI's alone. These telephone inquiries were supplemented by the review of the documents contained in the bibliography and referenced throughout the report. The study concentrated on breadth rather than depth, and as such may suffer from errors in some of the details. However, an attempt was made to contact the entities involved, and these attempts were successful. In addition to the contacts, significant supplemental documentation was available. Also, three of the non-government individuals contacted (as well as the PI) had experience with the NTSB process.

As a result, it is felt that the study approach did produce an adequate informational base both to give the readers of the report an understanding of the commercial aviation industry regulatory process, and to support the conclusions arrived at as a result of the study. The following is a list of the organizations contacted; summaries of the contact conversations are given in Section 7.0.

- Government Agencies
  - Federal Aviation Administration
  - National Transportation Safety Board
- Commercial Air Carriers
  - United
  - American
  - TWA
  - Delta
  - Pan American
  - Eastern
- Other Organizations
  - ARINC Inc.
  - Los Alamos Technical Associates (performing a study for EPRI on an allied subject)
  - Aero Data Inc.
  - Trans Systems Corporation

The supporting documents reviewed are listed in the References in Section 8.0.

6.0 Relevant Commercial Aviation Regulatory Agency - Responsibilities and Organization

6.1 Federal Aviation Administration (FAA)

The FAA is chartered with the responsibility to regulate air commerce to foster aviation safety, to promote civil aviation and a national system of airports, to achieve efficient use of navigable airspace, to develop and operate a common system of air traffic control and air navigation for both civilian and military aircraft.

Enabling Legislation: The Federal Aviation Administration, formerly the Federal Aviation Agency, became a part of the Department of Transportation in 1967 as a result of the Department of Transportation Act (80 Stat. 932).

As shown in Figure 1, the FAAS is organized under the direction of the administrator into six divisions. Aside from the Administration Division, which manages FAA internal affairs, each division cooperates towards the purpose of the FAA Charter. The Airports Section administers programs to identify the type and cost of development of public airport and assists in their planning and growth via grants of funds to public agencies. This division also develops standards by which airports serving air carriers certified by the Civil Aeronautics Board are sanctioned.

The Air Traffic and Airway Facilities Division operates a network of airport and air route traffic control towers and centers, plus flight service stations to ensure the safe and efficient utilization of navigable airspace. Rules and regulations for allocation of airspace and security control of air traffic for national defense also come under the jurisdiction of this division.

Safety regulation is overseen by the FAA's Aviation Standards Division through the issuance and enforcement of regulations, rules and standards on aircraft manufacture, operation and maintenance. In addition, standards are set for the rating and certification (including medical) of airmen. The Engineering and Development Section provides the systems, procedures, facilities and devices necessary to see that air navigation and air traffic control meet the needs of both the civil aviation and air defense systems. Development and testing for improved aircraft, propellers, engines and appliances are additional responsibilities of the Engineering Division.

Finally, the Policy and International Aviation Affairs Division promotes the exchange of information with foreign countries through technical representation at international conferences, the training of foreign nationals, and participation in the International Civil Aviation Organization, among other groups.

6.2 National Transportation Safety Board (NTSB)

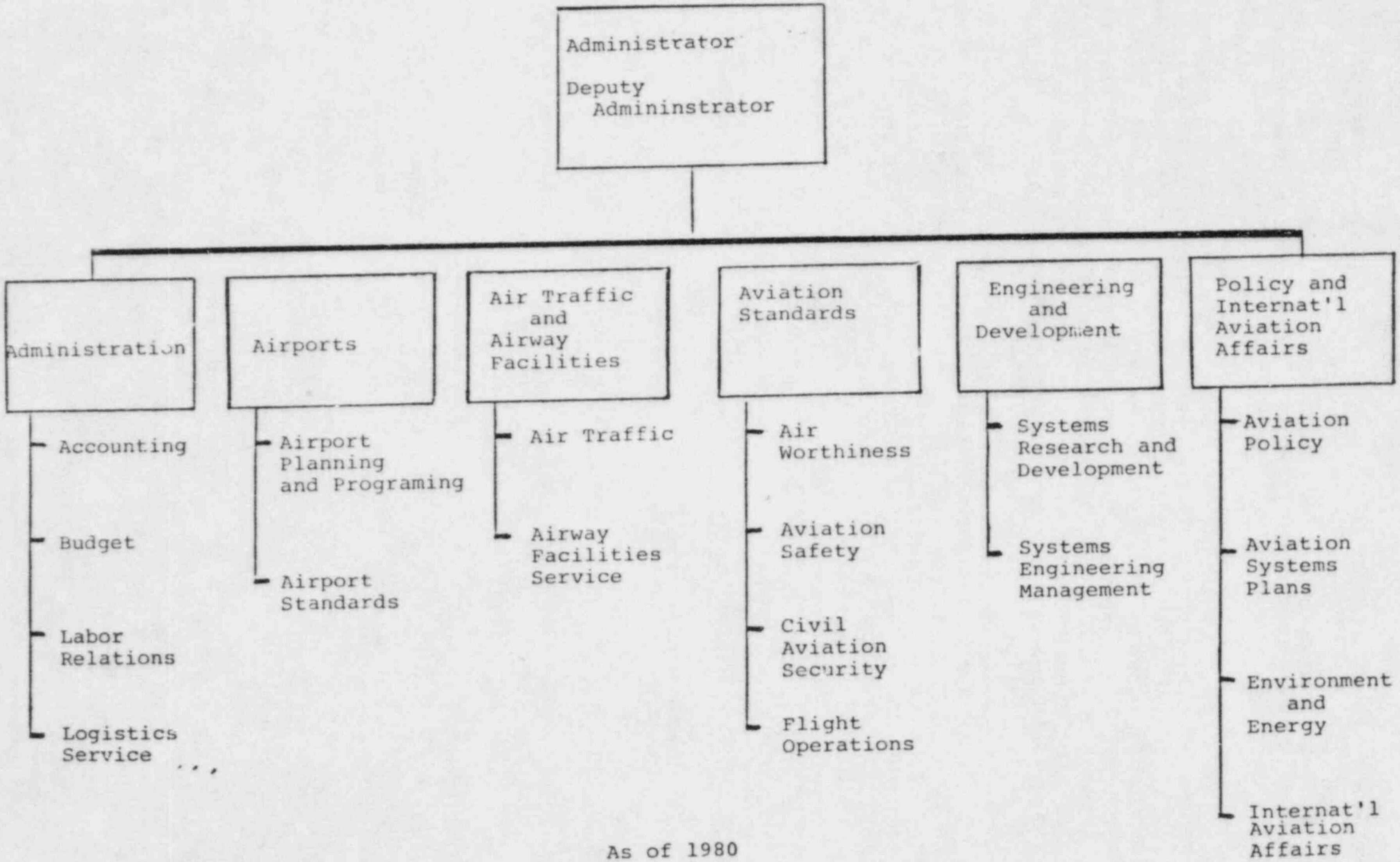
The NTSB is chartered with the responsibility to promote transportation safety by conducting independent investigations of accidents and other safety problems by formulating safety improvements.

Enabling Legislation: The NTSB was established as an independent agency of the Federal Government on April 1, 1975 by the Independent Safety Board Act of 1974 (88 Stat. 2156; 49 U.S.C. 1901).

The NTSB consists of five members appointed by the President, by and with advice and consent of the Senate, for five-year terms. Two of these members

Figure 1

Federal Aviation Administration



As of 1980

are designated as Chairman and Vice-Chairman by the President for two-year terms, with selection of the Chairman requiring consent of the Senate. The Board's structure is shown in Figure 2.

For all U.S. civil aviation accidents, the Board has the responsibility for the investigation of each accident, the determination of its cause, reporting the facts and surrounding circumstances and making safety recommendations. This process is carried out for all railroad and pipeline accidents which result in a fatality or substantial property damage, railroad accidents involving passenger trains, highway accidents selected in cooperation with the states, major marine accidents involving a public and a non-public vessel and/or casualties and other transportation accidents which, in the judgment of the NTSB, should be investigated.

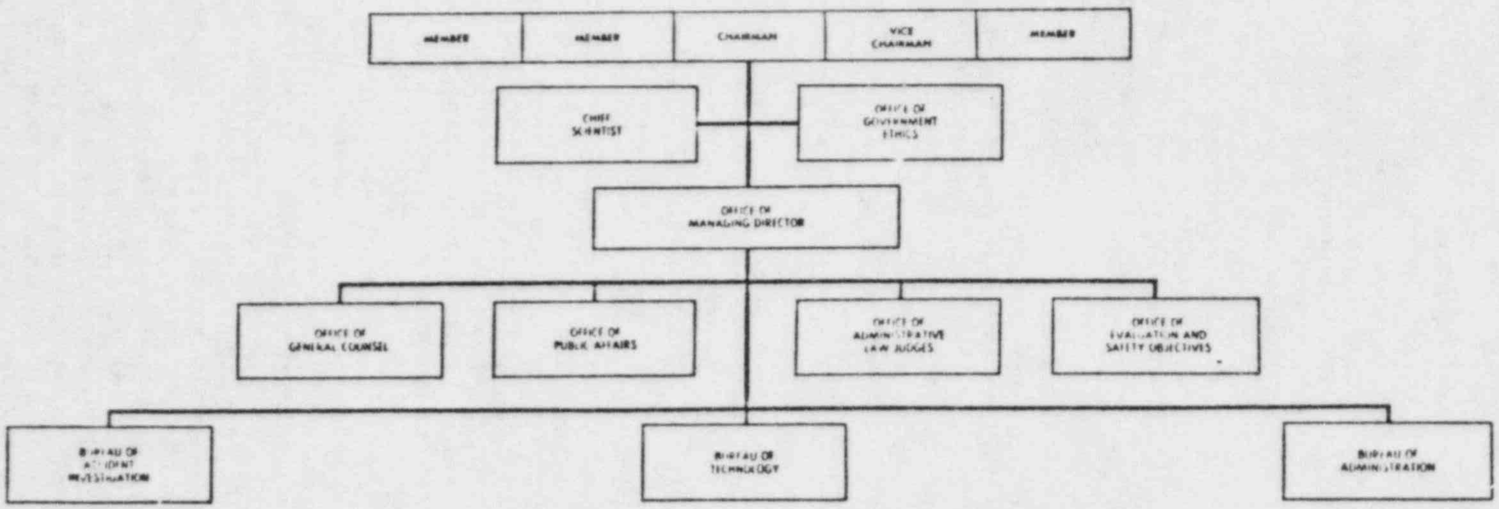
The Board acts to promote transportation safety in a variety of ways, such as assessing techniques for accident investigation and establishing procedures thereupon; formulating regulatory requirements for accident reporting, and evaluating the awareness of transportation safety of other government agencies with respect to their accident prevention responsibilities. It is also a responsibility of the NTSB to monitor the adequacy of hazardous materials transportation safeguards and procedures, and the performance of other government agencies in this area. Reports are given annually to the Congress on NTSB activities.

7.0 <u>Individual Interview Reports</u>

To be supplied.

Figure 2

NATIONAL TRANSPORTATION SAFETY BOARD



7.0 Individual Interview Reports

7.1 Government Agencies I- 18

7.1.1 Federal Aviation Administration

1. Government Agency: Federal Aviation Administration (FAA)

2. Contact: Mr. Ed Schilke
Aircraft Maintenance Division
FAA Building, AWS-300
Federal Aviation Administration
800 Independence Ave.
Washington, DC 20591
(202) 426-3440

3. Responsibilities: To review submitted reports to determine if regulatory action is required concerning aircraft maintenance. To review and approve carrier Reliability Programs.

4. Discussion:

The FAA regulates the industry through both its headquarters offices and through regional offices around the country. In the 1950's and 1960's they were actively involved in the development of the Maintenance Steering Group (MSG) and Maintenance Review Branch (MRB) philosophy and in the development and review of the individual air-carrier proposed Reliability Programs. These reviews involved both headquarters staff and the Principal Maintenance Inspectors (PMI) in the relevant region. The impression was given that during this period a great deal of personnel time was spent on these activities, but now the activity is minimal. The primary activity is the performance of the oversight function relative to individual air carrier maintenance. The FAA relys primarily on the PMI to review the carriers in his region and to report unusual trends. There is currently in place a data system to track reliability performance but this is directed at only items considered significant. The carriers develop two types of reports and submit them to their PMI. The first is the Mechanical Reliability Report (MRR). This is a daily report on failures of 6 specific items (e.g. landing gear, brakes, engine Foreign Object Damage (FOD)). The second report submitted every 10 days is called the Mechanical Interruption Summary (MIS). This report includes all causes of difficulties which result in delay or cancellation of a flight. It is the responsibility of the PMI to convert this new material into Service Difficulty Reports (SDRs) and to submit them to the FAA District Office which in turn transmits them to the FAA Maintenance Analysis Center in Oaklahoma City. The Center sends out weekly reports based upon the submittals of all districts and sends these to 300 recipients including all the air carriers. The FAA in turn reviews these reports on a regular basis investigates trends and develops a System Analysis Summary Report (SASR) which is distributed to both headquarters and regional staff. The information gathering and distribution process has fallen short on occassion (e.g. the Chicago American Airlines DC-10 crash May 25, 1979) and has been criticized both internally and outside the FAA.(s) As a result the FAA has requested the Department of Transportation's Transportation Systems Center in Cambridge MA to develop a more comprehensive system. This system, which is expected to be operational in the near future, is called the Aviation Safety Analyses System (ASAS). In addition, at the request of the FAA, NASA has developed an experimental Aviation Safety Reporting System (ASRS).

Since 1975, NASA has operated this system which permits confidential reporting of safety problems and violations of procedures within the aviation system, including information on human error. Anyone is permitted to file a confidential report of observed or experienced safety problems but pilots and air traffic controllers have been the principle sources. As of 1980 over 22,000 reports were received. NASA publishes quarterly reports containing both the statistical group of items and analyses of the more significant ones.

7.1.2 National Safety Transportation Board

1. Government Agency: National Transportation Safety Board (NTSB)

2. Contact: Mr. Paul Turner
National Transportation Safety Board
Audio Lab TE60
Washington, D.C. 20594
(202) 382-6691

3. Responsibilities: Cockpit Voice Recorder Analysis (CVR)

4. Discussion:

The NTSB (actually its equivalent since it was not yet created) began to tak about placing voice recorders on aircraft in the 1958-1959 time frame. The talk became serious in the early 1960's, and commercial aircraft were required to have CVRs on board. The first analysis of a CVR tape occurred in 1966 subsequent to a 707 crash. At present the NTSB analyses about 30-40 tapes per year. They perform post incident analysis on tapes for the world over not just the U.S. This analysis is performed in cooperation with the FBI labs. The FBI has some of the most sophisticated tape analysis devices in the world, and has the bulk of the talent in the field also. They and the NTSB do work for the Air Force, Navy, Washinton Metro, and the New York Police Department among others. Contrary to popular myth, less than 10% of the recorders are unavailable or the tapes rendered unusable after an incident. The bulk of those lost around the world are a result of ocean or other deep-water crashes when retrievability is not possible. Throughout the history of the program only 2 Fairchild and 3 Sunstrand recorders have been lost due to the results of a crash (i.e. fire).

CVRs were originally designed to capture the entire band with capabilities of the human voice (350-3500 Hz). But as they began to analyze tapes they found the recorders picked up many other useful noises besides voice (e.g. engine noise, control activation noise, landing gear noise). For this reason the standard (ARIMC 557-1966) is being rewritten to expand the record range from 100-6000 Hz. The tape records and recycles every 30 minutes. Reliability is insured by the fact that an aircraft cannot take off without an operating CVR. These observed mean time between failure is about 200-300 hrs. The biggest cause of failure is improper maintenance of the device.

1. Government Agency: National Transportation Safety Board (NTSB)

2. Contact: Mr. Billy M. Harper
Flight Recorder Lab TE60
National Transportation Safety Board
Washington, D.C. 20594
(202) 382-6689

3. Responsibilities: Analog (Oscillographic) Flight Recorders - "Scratch" Recorders

4. Discussion:

The NTSB contact indicated that devices designed to record aircraft parameters for post flight analysis have been available since the early days of aviation. Charles A. Lindberg carried an early foil recorder on his historic flight in 1927. This device provided the documentary evidence required to prove his accomplishment. This early design (which is now on display in the Smithsonian) utilized pen scratches in metallic foil that was slowly but continually, advancing. The pens recorded the analog output of instrument readings such as altitude, and heading thus providing a permanent record of the trip. This basic design was improved upon and developed into a device by an engineer employed by General Foods Corporation in the 1950's. This 1950's design is the basis for both the Fairchild and Sunstrand "Scratch Recorders" (so called because the record is still made by oscillographic scratches by a pen in metallic foil). In 1960 recorders were required on all Turbine aircraft. These scratch recorders record basic aircraft parameters such as altitude, magnetic heading, and vertical acceleration on a foil which advances at a rate of 0.1 inches per minute. These are the devices carried on all current aircraft other than the widebody aircraft (747,DC10,L1011). This includes even the newer designs such as the 737 because it was not designated a "wide body". The devices are built to ARINC standard 573 (with the exception of British aircraft which carry scratch recorders with 0.2 inch per minute resolution and record pitch, roll, and engine parameter in addition to the standard set).

When the standard was originally set the analysis of accidents was developing. For this reason the original parameter set included navigation parameters which are no longer a problem. The NTSB now recognizes they need parameters which are more performance related. Originally the microscopic analysis of FDR foils was done by the National Bureau of Standards for the NTSB, but now they do their own analysis. The current feeling is that scratch recorders are not adequate for current post accident analysis and they hope to replace all scratch recorders on aircraft with digital devices using more advanced recording media.

Concerning the value of CVRs to post incident analysis, the comment made was that over 90% of the time the CVR tape (if available) has made a significant contribution to and has affected the course of an investigation. Many times it is the key element. The suggestion was made that serious consideration be given to employing the device in Nuclear Plant Control Rooms. The comment was made that many other agencies (i.e. Metro, NYPD etc.) with just this type of a problem and the CVR concept has been successful for the solution of their problem. It was suggested that even if the operators were not outfitted with microphones, consideration should be given to recording phone calls, page calls, and control room conversations (using area microphones) on a single device with time synchronization on a recycle basis.

1. Government Agency: National Transportation Safety Board (NTSB)

2. Contact: Mr. Dennis Grossi
   Flight Recorder Lab TE60
   National Transportation Safety Board
   Washington, DC 20594
   (202) 382-6692

3. Responsibilities: Digital Flight Data Recorder (DFDR)

4. Discussion:

The NTSB contact indicated that this device is built to ARINC Standard, ARINC-717 and records digital data on aircraft performance, and systems activation parameters. The parameters which are required to be recorded have been adjusted over the years and the specific required parameter list on current devices was to be mailed to the principal investigator. However, current NTSB regulations require that 19 parameters be recorded. These are recorded on a 25 flight hour recycle basis. The recording medium is currently magnetic tape and the record rate is 64, 12 bit words per sec. The sampling rate depends on the actual number of parameters chosen, and is specified by the aircraft operator. The 19 required parameters are specified by 14CFR25, and 14CFR121 and include; Altitude, Airspeed, heading, pitch, roll, vertical acceleration, longitudinal acceleration, lateral acceleration, engine thrust or power, control surface position or control inputs, and microphone keying information. In addition to these required parameters the operators add as many as 70 or 80 additional voluntary parameters. On the average the voluntary additions are about 30-35. Also it should be noted that many U.S. domestic carriers record only the required 19. This is because of the economic impact of adding instrumentation to their aircraft. The most active voluntary contributors are government sponsored non-domestic carriers.

The current research of NTSB involved looking into alternative recording media such as bubble memory and solid state memory, and increasing the number of required parameters. The latter research is the result of the development of digital flight instrumentation in new aircraft. Since this instrumentation does not leave "witness marks" there is a real and current need to record the instrument readings. This need is also present due to the more complicated interaction between the flight crew and the auto-pilot system on modern aircraft. Interviews conducted with individuals involved in the development of the standard and in the use of the data for post accident investigation attested to the value of the data recorded for an accident investigation standpoint.

7.2 Commercial Air Carriers

1. Airline: United

2. Contact: Mr. Thomas Edwards
   Administrator of Maintenance Programs Development
   United Maintenance Operations Center
   SFOML
   San Francisco International Airport
   San Francisco, CA 94128
   (415) 826-6343

3. Fleet Composition:

1.	18 - 747	*number on order
2.	47 - DC10	
3.	3 - 767 (19)*	
4.	49 - 737	
5.	125 - 727	
6.	83 - DC8	
	325 Total	

4. Reliability Program:

United has had extensive experience with Reliability Programs several of the key individuals who developed the overall philosophy for deciding the methods and criteria for categorizing components as hard time, on Condition, and Conditon monitored, and some of the more general requirements for failure analysis and corrective action were originally United employees. In particular Stan Nowland, and Tom Mateson lead the industry in arguing against the original piston aircraft overhaul policy of the industry to a more "if it works - leave it alone" philosophy embodied in the MSG-2 program. Their experience led to the publication of a well-known pioneering document by Nowland (with Howard Heap as co-author) entitled: "Reliability Centered Maintenance" (NTIS A-066-579 29 December 1978) which provided the baseline MSG-2 approach.

United's feeling is that they have learned much since the early attempts. As a result the implementation of their program which used to rely rather heavily on actuarial analysis as a basis for alerting their engineering staff to problems now has eliminated all alert's based upon statistics. This "No Alert" policy is a result of several factors:

1. They noted for several years that never was an alerted item not already known to their engineering staff.

2. They have a comparatively large engineering staff so they are able to track problems on more of an individual basis.

3. They place heavy emphasis on person to person communication links between the pilots, the maintenance crews, and the engineering staff

In summary they felt:

Once you know your equipment and you have good communication between your people statistical alerts are superfluous.

7.2.2 American

1. Airline: American

2. Contact: Mr.Paul Wilson
   Manager of Quality Assurance Programs
   American Airlines Maintenance and Engineering Center
   Mail Drop 117
   P.O. Box 51009
   Tulsa, OK
   (918) 832-2152

3. Fleet Composition:

1.	14	-	747
2.	36	-	DC10
3.	179	-	727
	229	-	Total

4. Reliability Program:

American has had a systematic reliability program for 15 years. There program predates the development of MSG.2 The motivation for the development of the program was economic. They wanted to take advantage of statistical techniques to remove many components from the hard time requirements of the FAA. Their program is based upon tracking removals of equipment for cause but they also use pilot reports per 1000 flight hours. They monitor and alert on a statistical basis (i.e. mean value+X-). Any component which penetrates the alert level causes it to be flagged and it is reviewed by data analysis & engineering personnel at a reliability control meeting. The program conforms to and is in compliance with FAA advisory circular 120.17. Originally the statistics were used to help justify removing components from hard time or for extending the overhaul time for those which remained but after 5 or 6 years this process stabilized and for the last 2 years there have been no changes.

7.2.3 Trans World Airlines

1. Airline: TRANS World Airlines

2. Contact: Mr. George Heflin
   Manager Reliability Control Analysis
   Trans World Airlines
   P.O. Box 20126
   Kansas City International Airport
   Kansas City, MD 64195
   (816) 891-4643

3. Fleet Composition:

1.	50	-	707 (29)*
2.	90	-	727
3.	32	-	L1011
4.	18	-	747
5.	(10)**	-	767
	190	-	Total

*number currently

4. Reliability Program

TWA has had a Reliability Program for over 10 years. They have developed a data analysis, tracking, and alerting system called the "Overpar Program." This system tracks the number of removals per unit flight hour and stores the previous 11 months of performance. The so called PAR Value (Alert Limit) is based upon the 11 month mean plus a factor time If the PAR value is exceeded the last 3 months of calculations are reviewed and if the item has been over PAR for the last 3 mos. then it is "flagged" and sent to their engineering group for review.

While experience has indicated to TWA that Over Par system very seldom identifies a problem that their engineering staff does not already know of they feel that it is valuable as a confirmatory mechanism, and as an oversight system. In a practical sense it also provides their engineers with the statistical evidence to back up design or operations changes they suggest. Currently about 1% of the components (about 35) are alerted by the system each month. The system also includes a system alert each month employing a system overpar feature based upon a review by ATA chapter. This sometimes produces a system alert even when no component is overpar.

The system was extremely valuable several years ago in providing them with the information which allowed them to get FAA agreement for Hard Time, on condition, and condition monitoring assignments and changes thereto. It also was useful in extending the hardtime limit. However over the past few years this has been less significant since the assignments are very seldom charged now.

7.2.4 Delta

1. Airline: Delta

2. Contact: Mr. Jerre O. Williams
Supervisor of Maintenance Specification Development
Delta Airlines Inc.
Harts Field
Atlanta International Airport
Atlanta, GA 30320
(404) 765-3596

3. Fleet Composition:

1.	36	- DC9	
2.	13	- DC8	
3.	41	- L1011	
4.	129	- 727	
5.	(20*)	- 767	*number on order
6.	(60*)	- 757	
	219	- Total	

4. Reliability Program:

Delta has had a program in force for 14 years. Although they started out with an alert system on component parameters they no longer use this. The alerts occur now only on a systems basis (i.e. basically by ATA chapter) for this alert they track the parameter of: delays and cancellations per 100 flight hrs. (or departures). They alert on the 12 month mean value of this parameter whenever it exceeds a preset limit which they establish independently of but with the oversight of the FAA. They depend more on operating reports now to maintain their operational availability level rather than statistics. Reports such as the Fleet Operations analysis report, and the engine operations anal sis report supplemented by pilot reports provide them with what they consider to be the most effective Reliability Program in the industry. They feel that although every carrier probably feels their own program is best Delta's is actually the best because Delta is the airline that has been most successful financially (NB: other airlines disputed the reason but also agreed that Delta is the most successful). In general the belief was that data collected on components was useful for analysis once a problem is detected but at present alert values based upon component performance parameters are no longer useful.

IMAGE EVALUATION
TEST TARGET (MT-3)

150mm

6"

7.2.5 Pan American

1. Airline: Pan American

2. Contact: Mr. Ray Valeika
Systems Director of Engineering and Quality Control
Pan American World Airways
JFK International Airport - Bldg. 208
Jamaica, N.Y. 11430
(212) 632-5220

3. Fleet Composition:

1.	45	-	747
2.	9	-	737
3.	55	-	727
4.	16	-	DC10
5.	12	-	L1011
	137	-	Total

4. Reliability Program:

Mr. Valeika started the discussion by indicating that Pan Am spends about $400M per year on maintenance. This $1M per day number appears to be somewhat representative for the industry . The program started in 1969 and has been in place for the 13 years since. Originally the program utilized a data system with alerts on every component. The alerts were discontinued in 1974 and they are only developed on a system basis using a 12 month average of the parameter: delays per 100 departures. The component failure numbers were useful in the beginning primarily to prove assertions to the FAA. This was during the time when the industry was changing from an overhaul philosophy to a fly to failure philosophy. Two factors were involved in the elimination of this system. First it was recognized early that if you needed numbers to tell you you had a problem with a component you were in real trouble because by then it was too late. Thus alerts never occurred on components that were not already known as problems. The second reason was cost. The economic climate in the industry has reduced the manpower available for this type of review from 40 at the high to 4 or 5 today. At present there is no longer any automatic (edp compatible) collection of component failure data as there was in the past except for warrantee items. However they do continue to collect and store hard copies of the component shop cards.

Mr. Valeika chaired the committee which developed MSG3. He believes the approach has universal applicability. He is currently under ($50K) contract to Rockwell International to investigate the feasibility of applying the approach to the space shuttle operations. He believes that Pan Am will be involved next year in the actual application of the approach to the Space Shuttle. He indicated that Pan Am would be interested in doing the same thing for the commercial nuclear industry, but only on a funded basis.

7.2.6 Eastern

1. Airline: Eastern

2. Contact: Mr. Donald T. Crosby
Director of Quality Assurances and Chief Engineer
Eastern Airlines
Miami International Airport
Miami, FL 33148
(305) 873-2792

3. Fleet Composition:

1.	28	-	L1011
2.	127	-	727
3.	80	-	DC9
4.	30	-	A300
	260	-	Total

4. Reliability Program:

Mr. Crosby indicated that Eastern has been involved in the development of Reliability Programs since the advent of the jet age (almost 15 years). Eastern developed its own approach called REAP (Reliability Engineering Analysis Program). This program originally included data collection alert limits and tolerances. It was used to convert from the hard time concept which then applied to the whole airplane to the current concept where almost no components (except those with demonstrated life limitation such as landing gear) are now on hard time. Today Eastern no longer uses component alerts. But they do alert on system performance when any system contributes more than 1 1/3% of the delays encountered. In addition they have people reviewing the performance of components on a regular basis and these people have enough experience to recognize a real problem when it occurs.

8.0 REFERENCES

1. 49 CFR Chapter VIII - National Transportation Safety Board Part 830 - Notification and Reporting of Aircraft Accident or Incidents and Overdue Aircraft, and Preservation of Aircraft Wreckage, Mail, Cargo and Records, Secs. 830.1 - 830.35.

2. National Transportation Safety Board, Manual of Code Classifications - Aircraft Accidents and Incidents, August 1981 (4th Edition), Washington, D. C.

3. National Transportation Safety Board, "NTSB Accident/Incident Report", NTSB Form 6120.4F, January 1982.

4. Turner, P. C. et al., "Specialists' Factual Report of Investigation of Cockpit Voice Recorder," reported in Aviation Week & Space Technology, 22 February 1982, pp. 81-91, "Air Florida 737 Voice Recorder Transcribed," McGraw Hill, New York.

5. National Academy of Sciences, "Improving Aircraft Safety - FAA Certification of Commercial Passenger Aircraft," Committee on Airworthiness Certification Procedures - Assemby of Engineering - National Research Council, Washington, D. C., 1980, Library of Congress 80-82605, ISBN zero -309-03091-9.

6. Office of the Federal Register et al., U. S. Government Manual, 1 May 1980, Washington, D. C.

7. Kozicharow, E., "FAA Proposes Safety Rule Changes," Reported in Aviation Week & Space Technology, 27 September 1982, p. 31, McGraw Hill, New York.

8. Rose, S. T. and Abraham, P. M., "Safety Evaluation of Operational Occurrences as Applied to Oconee Nuclear Station," ANS/ENS International Meeting on Thermal Reactor Safety, August 1982, Chicago, Illinois.

9. Haddad, E. E. et al., "IEEE Trial-Use Standard Definitions for Use in Reporting Electric Generating Unit Reliability, Availability, and Productivity," ANSI/IEEE Std. 762-1980, IEEE, New York.

10. Russ, J. et al., "IEEE Standard Criteria for Protection Systems for Nuclear Power Generating Stations," ANSI/IEEE Std. 279-1979, IEEE, New York.

11. NTSB, "The National Transportation Safety Board Report of the January 13, 1982 Air Florida 737 Accident at Washington National Airport," reported in Aviation Week & Space Technology, 27 September 1982, pp. 78-89 (Part 1), McGraw-Hill, New York.

APPENDIX J

ELECTRICITÉ DE FRANCE

INCIDENT REPORTING SYSTEM IN FRANCE

APPENDIX J

INCIDENT REPORTING AND ANALYSIS AND RELIABILITY DATA SYSTEM IN FRANCE

It is of interest to study the French system of incident or event reporting because they appear to have a highly developed incident data collection and storage system whose approach may be adapted so as to significantly enhance the utility of the U.S. LER system.

Before looking at the incident reporting system (IRS), it is important to briefly look at the nuclear industry organization in France because this directly impacts their IRS.

France has one nationalized utility, Electricité de France (EdF), which operates all of their commercial electricity generation power plants. EdF, employing about 100,000 people, has an electricity generation capacity of about 44 GWe broken down as follows: Nuclear (PWR) - 19.8 GWe (45%); Nuclear (non-PWR) - 2.2 GWe (2.2%); and Fossil 22 GWe (50%). Of the 22 GWe from fossil fuels, oil produces about 11.9 GWe (54%); coal 9.7 GWe (44%), and gas 0.4 GWe (2%). They have twenty-three operating 900 MWe PWRs (Westinghouse-type built by Framatome); eleven 900 MWe PWRs under construction, and thirteen 1300 MWe PWRs under construction or ordered. They have endeavored to make all of their PWR nuclear plants as identical as possible, except for the higher power rating for the 1300 MWe plants.

Incident Reporting and Analysis

EdF has always had a practice of incident or event reporting from its fossil fueled plants before they entered the nuclear power era. They have, therefore, continued the practice from their nuclear plants with some modifications. Incidents or events are divided into two categories, the first being those, which taken individually, do not have any particular safety significance but which with repetition may become precursors of serious incidents. The second category represents those which have safety significance and may be precursors of serious incidents. The French safety authorities, which are the Service Central de Sûrete des Installations Nucléaires (SCSIN), a department of the Ministry of Industry and Energy; the Institute of Protection and Nuclear Safety (IPSN) of the French Atomic Energy Commission (CEA), which is the technical arm of SCSIN and EdF, developed a set of criteria to define "significant incidents". These criteria are Attachment A to this Appendix J. In addition, plant operations must report all unplanned reactor trips (scrams), since this represents loss of electric power generation and is considered a significant incident. It is the plant superintendent's responsibility to determine whether an incident is a "significant incident" (SI) or not. The occurrence of an SI must be reported by telex immediately to the SCSIN, IPSN and the Department of Operations and Nuclear Safety (DONS) of EdF. A report on the SI, based on a uniform structured narrative format (see Attachment B), must be sent to SCSIN, IPSN and DONS no later than one month after the incident. The SI may also include the printout from KIT, which is EdF's automatic operating reactor parameter recording system used for incident reconstruction, and described later in this appendix.

The DONS of EdF encodes SI reports into a computer file based on a standard format provided as Attachment C. In addition, information regarding incidents which are not SI are computerized using the same format. They have had about 2,000 incidents per year for the 23 reactors, of which about 200-300/year were considered significant and 20/year which were considered very significant incidents. Approximately 150 to 250 of the significant incidents are a result of reactor trips in the 23 plants.

DONS has direct links to INPO's NOTEPAD and provides SIs to INPO. LERs (NRC) and SERs (INPO) from the United States are translated into French and then encoded and entered into their computer file for incidents.

All incident reports, whether significant or not, are reviewed by review groups in DONS of EdF and IPSN-CEA. The IPSN review is conducted on behalf of SCSIN, the French safety authorities. Both DONS and IPSN have engineers who are knowledgeable about plant operations and who conduct any required in-depth review and analysis of significant events. DONS and IPSN each have about twelve staff people assigned full time to the analysis of significant events who have direct access to the computerized data file on incidents. IPSN has one person assigned to monitor the events from each EdF site. In addition, both organizations, including the incident analysts, are able to directly contact the operations staff of any plant by telephone or plant visits to obtain or confirm details about incidents in order to develop a clear understanding of the scenario and cause of the incident.

Because of the variety of incidents, the DONS and IPSN carry out case by case studies of their significant incidents to identify anomalies which may be used to determine trends and accident precursors. These studies principally consist of deterministic analysis of the incidents to determine the sequence of events and the cause or initiator of the incidents. They have not developed any special statistical analysis methods for analyzing incident reports. During the conduct of SI review they do look through their computerized file for similar events to aid in the identification of trends and accident precursors. When all of the KIT systems are updated as described below with a permanent recording system, EdF will have a very large source of operating data which could be used for such statistical analysis as multi-case and multi-variate analysis. They did not, however, indicate any plans to develop or carry out such statistical analysis to search for accident precursors or trends.

KIT System

EdF has, and is implementing, a computer-based automatic operating data acquisition system called KIT (Control (K) Information Treatment), sometimes also referred to as TCI (Le Traitement Centralise des Informations), on all of their PWR power plants and 700 MW fossil power plants. KIT has two purposes:

(1) to aid in the control of the nuclear power plant, and (2) to aid in the reconstruction and analysis a posteriori of operations and incidents or significant events. They have five main designs of the KIT system which have evolved with experience. They can be represented by the systems on the 700 MW fossil plants, Fessenheim (900 MWe) nuclear power plant (NPP), Bugey (900 MWe) nuclear power station, CP1-2 (900 MWe), and Paluel (1300 MWe) NPP. In addition, EdF is currently designing an advanced control room for the next generation (1500 MWe) NPP which incorporates an advanced KIT system. This discussion will concentrate on the details of the advanced 900 MWe and the 1300 MWe NPP KIT systems, with special emphasis on the 1300 MWe because this represents the current state-of-the-art KIT system in operation.

EdF has divided the NPP plant parameters which are scanned and recorded into two categories: (1) the state of different plant components such as valves, pumps, relays, etc. called logic variables, to which EdF applies the acronym "TOR" (tout ou rien, all or nothing), and (2) the readings from various detectors or sensors, which they designate as analog variables.

The first category of parameters -- logic variables or TOR -- represent the state of such devices as pressure regulators, thermostats, threshold measuring relays, travel limits (limit positions) of valves, interlock positions for circuit breakers, relay contacts, valve positions, pump status, etc. KIT can scan up to 4,064 of the logic or TOR variables. In actual practice about 4,000 logic variables are actually monitored. It has a scanning rate of 50 millisecs for normal TOR, 10 millisecs for TOR of in-core devices, and 10 millisecs or 200 millisecs for TOR of devices which measure the perturbations of the state of the components of the turbine generator.

Although KIT has the capability of scanning up to 1,080 analog variables, in practice only about 1,000 analog variables are actually monitored.

All of the changes in the logic or TOR variables are recorded on a printer called the "operations log" in chronological order with a resolution of 50 msec. The information which is printed specifies (1) the time that the change in state occurred, (2) the reference of the sensor, (3) function of the sensor, and (4) the state of the variable. The KIT system with the logic or TOR variable records may be used to determine the operating discrepancies relative to operator actuator actions. This, however, has not been used and will be cancelled. KIT has a built-in comparison system for comparing the actual state of an actuator or physical criteria with theoretical status as envisioned by the authors of the operating instructions. This also has not been operational. Repeated changes or excessive fluctuations in TOR above a predetermined value will produce an alarm on the printer. The operator can also request the printer to recall those TOR which have changed their state by at least n times over a 24-hour period. In addition, the TORs from the control and protective devices of the turbine generator are scanned, recorded and may be analyzed. Fast changes in state and fast changes in physical values in the turbine generator control and protection system trigger rapid scanning and recording for a 30 second interval.

The second category, analog variables, represents plant parameters such as temperatures, flow rates, water level readings, pressure, neutron flux, etc. KIT has the capability to scan up to 1080 of the analog variables. The scanning rate chosen by the operator for the analog variables depends upon the speed of variation of the physical state being measured. KIT has three possible scanning rates for analog variables: (1) rapid scan rate every 5 seconds with a maximum of 60 variables, (2) medium scan rate every 20 seconds with a maximum of 480 variables, and (3) slow scan rate every 60 seconds up to a maximum of $(1080 - [n_{5\text{ secs}} + n_{20\text{ secs}}])$.

It should be noted that although the analog variables are scanned at the aforementioned scanning rates, the data from the scanning process are not necessarily recorded. Only the data from up to 20 analog variables (in the Bugey type KIT) and up to 40 analog variables (in the CP1-2 type KIT) can be stored and printed as a permanent history.

The analog variables which are scanned every 5 seconds are stored in the computer memory for 5 minutes, whereas the variables scanned every 20 or 60 seconds are stored for 30 minutes. Under normal operation the analog variables are erased every 5 or 30 minutes and replaced by analog variables measured during the next 5 or 30 minutes. There is, therefore, continuous replacement every 5 or 30 minutes of the variables being stored in the memory. If an event occurs and certain criteria are met, the variables stored during the preceding 5 and 30 minutes in the computer memory are printed. In addition, 5 minutes of data following the event of the analog variables in the 5 minute category and 30 minutes of data following the event of the variables in the 30 minute category are printed and become a permanent record. In the early KIT systems the operator could determine which analog variables could be stored and recorded. Since this led to significant differences in the data available to reconstruct an event, EdF has pre-determined a standard set of 40 variables and is planning to standardize the variables to be stored and printed. The KIT system will thus store and print analog variables from 5 minutes before an event to 5 minutes after the event for variables scanned every 5 seconds, and 30 minutes before to 30 minutes after an event for variables scanned every 20 or 60 seconds. EdF, however, is backfitting to all 900 MW KIT systems a magnetic tape recording system which will store all 4064 logic and approximately 1080 analog variables scanned over a 24-hour period. Although these data will not be available to the operator during operation, they will be available for event reconstruction or operation analysis by processing the tape off-line.

The KIT system, which is located in a room adjacent to the control room but considered a part of the control room, currently is not classified as a safety-related component; however, it is connected to a buss which is connected to the emergency power source. Since it is not safety-related, it is not subject to IPSN review, nor are there technical specifications regarding its use or availability. They estimate the KIT system development for all plants has cost about \$1.6 million, while the hardware construction cost for each plant is about \$0.5 million. Since the wiring terminals for the monitored logic and analog variables are already in the control room, they do not charge additional costs for providing the variables to the KIT system.

EdF has developed a Safety Parameter Display System (SPDS) for all 900 MW NPP. They plan to take the logic (TOR) and analog variables from the KIT computer and process the data in a second computer, and display the information on four CRTs; two for the operator, one for the shift technical adviser, and the last at the technical support center. They also plan to transmit data from the SPDS via a data link to EdF headquarters. The SPDS has four main functions: (1) to display the actions of the safety protection system; (2) to display the results of the actions; (3) to confirm automatic action of the safety protection system; and (4) to aid in the diagnosis of the event. They are currently implementing the first SPDS system. They plan to have 12 SPDS units implemented by the end of 1984. They believe that they will be able to implement one per month after they get started.

For the 1300 MW NPP, EdF has made major improvements to the KIT system (also called the ICI [le Traitement Centralise des Informations] system). The KIT system is now a part of a Digital Integrated Protection System, SPIN (Systeme Protection Integrated Numeric). SPIN uses programmable microprocessors called Controbloc to acquire, process, monitor, and transmit operational data from the sensors to the operator, shift technical advisor (STA), technical support center, and EdF headquarters. In effect it is an integrated reactor protection, SPDS, and incident data monitoring and recording system. the microprocessors utilize solid state devices instead of conventional relays and switches to switch and transmit data. The data are multiplexed from one unit to another using optical fibers.

In SPIN the KIT system receives and records approximately 5000 logic (TOR) data and about 1200 analog data, of which about 200 analog data come from the reactor protection system. Data in the SPIN are multiplexed from one unit to another such as from the Controbloc to KIT. The analog data are monitored and recorded using analog-to-digital conversion. About 100 analog variables are scanned every 2 seconds, 160 analog variables every 20 seconds, and about 600 analog variables every 60 seconds. SPIN has two computer levels for handling the data. The first level computer, which has a 64K word internal memory and a 24 megabyte disk memory (used principally for programming), is used for acquiring the logic and analog variable data. The first level computer puts the logic data into chronological order and also processes the analog data. The CRT displays in the control room obtain their data from the first level computer. The second level computer, which has a 256K word memory and 50 megabyte disk memory, is used to transmit data to four separate CRTs which constitute the SPDS. In-core instrumentation output is pretreated at the microprocessors and is multiplexed to the second level computer. This computer has as peripheral equipment a floppy disk, magnetic tape, electrostatic printer and the four CRTs. The four CRTs go to the STA, Technical Support Center, and two to the data link to EdF headquarters. The disk will store all the logic and analog variable data received for a 24-hour period. The data will be transferred to magnetic tape for permanent storage once every 24 hours. The data will, however, be available for recall to the operator only as long as it is on the disk. EdF plans to store the tape for the life of the plant. Since they believe it will require about one reel of tape per 24 hours, they anticipate a significant storage problem. The EdF staff anticipates that there will be significant advances in the state-of-the-art for data storage in the next few years to help solve the problem of plant data storage.

The EdF staff estimates that the research and development of this integrated plant data monitoring and storage system (SPIN) will cost about 5 milion FF or about $700K. The first level hardware costs 1.5 million FF or about $210K per plant, and the second level hardware costs 2.5 million FF or about $350K. They stated that there was no additional cost as far as the KIT stem was concerned because all of the logic and analog data were already at the Controbloc.

Since 1980 EdF has been working on the development of a new type control room for their new nominal 1500 MWe PWR. This project, called S3C, has three objectives: (1) extensive integration of facilities for control and presentation of data, (2) efficient data processing which supplies the operator with relevant data, and (3) consistency between operating procedures and maintenance or periodic test procedures.

They plan to have a control room where operational control and data display will be obtained using computerized facilities. They will have redundant computers so that the computer control system can be classified safety grade components. They plan to reduce the number of controls and displays in the control room. EdF is currently building a simulation control room to test their design, which will be completed by 1985.

SRDF (Systèm de Recueil de Données de Fiabilité) - Reliability Data Bank

EdF has developed SRDF, a reliability data collection system which has been implemented on the six nuclear power plants of Fessenheim and Bugey for prototypic study. They are now implementing the system on all twenty-three 900 MWe PWRs. It was estimated that it would take about one year to implement the SRDF program on all 23 plants. The SRDF system has three objectives: (1) to provide reliability and availability data to aid in design, (2) to rationalize the technical specification time limits on the safety systems unavailability, and (3) to optimize maintenance and testing policies.

The SRDF has been designed to provide the following data for each group of identical components:

1. Total number of failures
   a) failures during operation
   b) failures during standby
   c) failures on demand
2. Operating history
3. Number of demands on component
4. Operating failure rate
5. Failure rate during standby
6. Failure rate on demand
7. Mean time between failures

8. Mean outage duration
9. Mean time to repair
10. Modes and origins of failure
11. Details on failing sub-components

EdF initiated a reliability data collection system at Fessenheim (two NPP) by collecting data on a total of about 4000 components in 1977. It was recognized very early that it was too difficult to keep track of that large a number of components, so that the total number was reduced to about 800 components for the two units.

EdF has developed three forms: (1) descriptive, (2) operation, and (3) failure, which are used for site data collection on the 800 components. The descriptive form contains the description and engineering characteristics of each of the components being followed. the operation form reports the operating history, including the number of demands, of each component each year. The failure form is completd whenever there is a work order for the component. The type of information required in the failure form is shown in Attachment D. One individual, who is generally a former shift supervisor, is assigned the responsibility to collect this information on a full time basis for each pair of units.

The approximate 800 components in the two NPP are distributed as follows:

Electrical Components	
Circuit Breakers	142
Motors	127
Miscellaneous (transformers, inverters, batteries, rectifiers, alternators, panel boards, etc.	51
Total	320
Active Mechanical Components	
Pumps	120
Valves	320
Turbines	6
Diesel Engines	4
Compressors	12
Rotating Filters	4
Total	466
Passive Mechanical Components	
Pressure Vessels	27
Heat Exchangers, including steam generators	20
Total	47
Total Components	833

These SRDF components were selected either because they were directly related to safety systems or had an effect on the availability of the units.

The data are collected at each site and then entered into a central computer by means of a computer terminal. Each form is verified before input into the computer and there are consistency and completeness checks of the data by the computer. The central computer is located at the EdF, Region d'Equipment Clamart, 2 et 4 Avenue de General de Gaulle, BPN 47, 92140 Clarmart, France. In 1981 the SRDF file received about 1,000 component failure reports (300 valves, 300 pumps and 400 others) per six plants per year, or about 170 component failures per plant per year.

The analysis of the data is conducted by the EdF Studies and Research Department staff at Clamart, consisting of 3-5 analysts, and the results are provided to DONS and the Construction Department. Because of the lack of data, they consider the data as time-independent. Failure data are analyzed using the exponential distribution law. They have published a third revision of the Recueil Provisorie de Données de Fiabilité (RPDF), which is a handbook of reliability data. The third version of RPDF contains results of analysis of reliability data collected from the units at Fessenheim and Bugey.

Conclusions

1. EdF and IPSN appear to have a well coordinated, systematic approach to the collection, storage, retrieval, and analysis of incident reports to determine the cause of incidents, to identify accident precursors, and to prevent the occurrence of serious accidents.

2. EdF has developed and is implementing an integrated microprocessor based logic and analog variable data monitoring and acquisition system (KIT), safety parameter display system (SPDS), and nuclear data link (NDL) to EdF headquarters for their 1300 MWe PWR nuclear power plants. The system, called Système de Protection Integre Numerique (SPIN [Digital Integrated Protection System]), has three purposes: (1) to act as a part of the reactor protection system, (2) to aid safe reactor operation, and (3) to aid in the reconstruction of events. SPIN collects logic and analog variables, processes the data, displays the processed data, initiates reactor protection alarms and actions, and records the data.

EdF is also backfitting the KIT, SPDS and nuclear data link on to all of their 900 MWe PWRs.

3. The 1300 MWe SPIN system monitors and stores approximately 5000 logic and about 1200 analog variables. Since it was difficult to determine a priori which variables might be required for reconstruction of an incident, EdF has decided to monitor and store almost all logic and analog variables available in the control room.

4. EdF has developed and is implementing a well coordinated realistic reliability data acquisition system on all of their nuclear power plants (NPP) which monitors routinely approximately 800 components per two NPP. The system, called Système de Recueil de Données de Fiabilité (SRDF), collects reliability data from each site and stores the data in a central computer.

5. EdF carries out deterministic analysis of incidents on a case-by-case basis. They do not appear to have developed or have any plans for developing sophisticated statistical analysis methods for analyzing incidents to determine accident precursors or trends.

DEFINITION OF "SIGNIFICANT INCIDENTS"

There are ten criteria to define "significant incidents":

1. Any incident which leads to the actuation of the protection function "Emergency Shutdown" (SCRAM) either automatically or manually, including spurious actuation, except emergency shutdowns resulting from a trip of the main turbine. Voluntary actuations of emergency shutdown, in the course of programmed activities, are exceptions to this criterion.

2. Any incident which leads to the actuation of an engineered safety system, either automatically or manually, including spurious actuation. Voluntary actuations of such systems, in the course of programmed activities, normal startups or shutdowns, periodical tests, are exceptions to this criterion.

3. Loss of an engineered safety system. Any incident leading to an excursion outside of the operating technical specifications or which could have so resulted for a different status of the plant:

   - complete loss of a safety system

   - partial loss of a system fulfilling a safety function, thus leading to a "safe operational status" of the unit (§ 3 of technical specifications)

   - violation of one or more safety limits (§ 2 of technical specifications)

   - common mode failure which has caused or which could cause multiple failures in one or more safety systems.

   This criterion applies especially to common mode failures resulting from:

   - close environment conditions of systems or components (fire, flooding, temperature, radiation, etc.)

   - interactions of systems, which are not identified beforehand

   - errors in operation or maintenance

   - errors in design, manufacturing or erection.

4. External aggression from a natural (earthquake, flood) or man-made phenomenon (explosion, airplane crash,...) which could affect the safety of the plant.

5. Sabotage or sabotage attempt which could affect the safety of the plant.

6. Incident leading to a release of radioactive products, either uncontrolled or outside the regulatory release limits.

7. Incident leading to an ionizing radiation exposure of a plant personnel (permanent or not) higher than the regulatory limits.

8. Incident of nuclear origin which caused death, or a severe injury which required evacuation to a hospital of the injured person(s).

9. Identified anomaly in design, manufacturing or operation, leading to an operating condition which has not been analyzed and could not be enveloped within the design conditions.

10. Incident which the operator has declared of significance since he wishes to perform a thorough analysis of this incident in order to obtain all useful feedback information as regards safety.

Attachment B

EDF - SPT	TRANCHE :	Page
GRPT :	COMPTE-RENDU D'UN INCIDENT SIGNIFICATIF	3/5
Centrale :	SURVENU LE	

S O M M A I R E

EDF - SPT	TRANCHE :	Page
GRPT :	COMPTE-RENDU D'UN INCIDENT SIGNIFICATIF	4/5
Centrale :	SURVENU LE	

1 - GENERALITES

- Date et heure
- Centrale et tranche
- Origine présumée de l'incident

  Le texte doit faire apparaître clairement, lorsque cela est possible, la cause originelle de l'incident de façon à pouvoir orienter facilement l'analyse vers le groupe B ou le groupe F (origine "matériel" ou non).

- Installation concernée

2 - NATURE DE L'INCIDENT

Résumé succinct (en quelques lignes) de la cause, de la localisation et de la nature du matériel, circuit ou système élémentaire concerné. Indiquer systématiquement le code AM, le constructeur, le type, le code fonctionnel.

3 - DESCRIPTION DE L'INCIDENT

3.1.- Etat initial avant le début de l'inciden'

- de la tranche
- du matériel ou des systèmes en cause.

3.2.- Chronologie de l'incident

- heures, minutes, secondes
- phénomènes physiques apparus, perturbations successives, manoeuvres automatiques engendrées, manoeuvres manuelles réalisées ...
- protections, alarmes, sécurités ayant fonctionné et paramètres les ayant actionnées
- mises en application des R.G.?
- observations diverses.

3.3.- Etat final

- de la tranche
- du système en cause

3.4.- Chronologie de la reprise du service (date et heure)

- redivergence
- recouplage
- retour à la puissance initiale

EDF - SPT	TRANCHE :	Page
GRPT :	COMPTE-RENDU D'UN INCIDENT SIGNIFICATIF	5/5
Centrale :	SURVENU LE	

4 - COMMENTAIRES

4.1.- Causes profondes

- défaillance de matériel ou erreur de conception
- défaillance humaine
- consigne inadaptée
- etc...

Donner le raisonnement qui a conduit à identifier une cause.

4.2.- Commentaires sur les anomalies observées

- à l'origine de l'incident
- pendant le déroulement de l'incident
- au redémarrage ou au retour à une situation normale.

5 - CONSEQUENCES (réelles ou potentielles)

5.1.- Sur la disponibilité

5.2.- Sur le matériel

5.3.- Sur les performances

5.4.- Sur la sûreté nucléaire et notamment sur les barrières

5.5.- Sur l'environnement

5.6.- Sur la radioprotection

6 - ACTIONS ENTREPRISES

6.1.- Au plan humain

- Action de formation complémentaire.

6.2.- Au plan technique

- Modification envisagée sur l'installation (matériel ou conditions d'exploitation) ou sur un document (consigne ou autre)
- Demande d'étude particulière
- etc...

7 - DOCUMENTS COMPLEMENTAIRES ETABLIS

Autres que ceux indiqués sur la première page.

8 - DOCUMENTS ANNEXES

Schémas d'appareils ou de circuits facilitant la compréhension du rapport.

CENTRALE de : Tranche :

RAPPORT D'INCIDENT SIGNIFICATIF
SURVENU le

RI - 2 - 015 - 82

D 5062 pages annexes

Résumé :

Le Chef de Centrale,

Documents ayant traité du même sujet :

- Télex d'information à l'Administration n° du
- Fiche 221 N° du
- Fiche 222 N° du
- Note

Conservation :

Qualité surveillée : oui
non

J-16

G.R.P.T. CENTRALE DE	RAPPORT D'INCIDENT N° (TRANCHE) Incident du (date)	INDICE	PAGE

Dernier réexamen effectué le :	Conditions du prochain réexamen par : en :	Durée de Conservation

Rédaction - Modification

Ind	REDACTEUR		VERIFICATEUR		EXAMEN	DATE	N° PAGES MODIFIEES
	Nom	Visa	Nom	Visa			

Documentation de reference - Documentations satellites

Lieu de conservation	Code doc.	Nb	Lieu de conservation	Code doc.	Nb

Documents de travail - Diffusion interne

Destinataire	Service	Nb	Destinataire	Service	Nb

Copies - Diffusion externe

Destinataire	Service	Nb	Destinataire	Service	Nb

E.D.F. Production Thermique
G. R. P. T.
Centrale Tr.

J-17

AVARIE DE MATÉRIEL

constatée le └┴┘ └┴┘ └┴┘

1-1-82

nt 222 N°

I. - MATERIEL EN CAUSE

Accidenté : directement ☐ ; par répercussion ☐ { Fiche 222 N° / Fiche 221 N°

Désignation du matériel :

Appareil :

Caractéristiques :

Constructeur :

II. - DESCRIPTION SOMMAIRE DE L'AVARIE

(Tranche en service ☐, *à l'arrêt* ☐*)*

survenue en exploitation ☐ découverte au cours d'une visite ☐

III. - RENSEIGNEMENTS STATISTIQUES

Nombre d'heures de marche ☐ du matériel, ☐ de l'appareil		Nombre de démarrages ☐ du matériel, ☐ de l'appareil	
depuis la mise en service	depuis la dernière visite	depuis la mise en service	depuis la dernière visite

IV. - DESCRIPTION DE L'INCIDENT - CONSTATATIONS FAITES *(anomalies enregistrées en exploitation, résultat de l'examen ou de l'expertise du matériel, dégâts observés)* **- CAUSES PRESUMEES DE L'AVARIE**

Repères schémas photos, etc...

V. - TRAVAUX EFFECTUES - MODIFICATIONS APPORTEES

VI. - FONCTIONNEMENT DES PROTECTIONS

VII. - ENSEIGNEMENTS A TIRER - MESURES PRISES OU A PRENDRE

VIII. - CONSEQUENCES ET REPERCUSSIONS

☐ Séparation du réseau, passage à charge nulle, coupure des feux, chutes des barres de manœuvre - Fiche 221 N°

☐ Prolongation de jours d'un arrêt de tranche programmé (☐ Valeur réelle - ☐ Valeur prévue)

☐ Avarie d'autres matériels, Fiche 222 N°

☐ Indisponibilité de tranche

☐ Totale MW j h mn, ☐ réelle - ☐ prévue

☐ Partielle MW j h mn, ☐ réelle - ☐ prévue

☐ Immobilisation

☐ Matériel j h ☐ réelle - ☐ prévue

☐ Appareil j h ☐ réelle - ☐ prévue

Secours ou rech^{ge} disponib. ☐ Oui - ☐ Non

COUT DE LA REPARATION : Nombre d'heures : Coût : F. - Val. réelle ☐ - Val. estimée ☐

Pièces jointes : ☐ Schémas, ☐ Photos, ☐ Croquis, ☐ Autres ______________

______________, le ______________

Le Chef de centrale

JACOT & LORIN

1-1-1982

INCIDENTS D'ORIGINE INTERNE ET EXTERNE

SÉPARATIONS DU RÉSEAU, PASSAGES A CHARGE NULLE, COUPURES DES FEUX, CHUTES DE BARRES, A-COUPS RÉSEAU

G.R.P.T. :
Centrale :
Tranche :

Document 221 N°
INCIDENT du … à … h … mn
Jour de la semaine :

IV - NATURE DE L'INCIDENT

(tel que défini dans le titre)

- ☐ A-coups sur le réseau sans séparation de la tranche
- ☐ Passage à charge nulle ou coupure des feux ou chute de barres sans séparation du réseau
- ☐ Marche sur réseau séparé ou clientèle prioritaire
- ☐ Ilotage sur auxiliaires
- ☐ Déclenchement total en général (ou arrêt volontaire) sans ilotage sur auxiliaires
- ☐ Déclenchement total en général (ou arrêt volontaire) après ilotage

V - SITUATION AVANT INCIDENT

- ☐ Tranche couplée au réseau général
  - ☐ en régime normal
  - ☐ en cours de démarrage
  - ☐ en cours de variation de charge
- ☐ Tranche sur réseau séparé ou clientèle prioritaire
- ☐ Tranche ilotée sur auxiliaires
- ☐ Tranche en autonome
- ☐ Tranche en téléréglage
- ☐ Chaîne de régulation concernée exploitée en "manuel"

CONDITIONS A L'INSTANT DE L'INCIDENT

MACHINE n° 1		MACHINE n° 2	
P_o	MW	P_o	MW
Q_o	Mvar	Q_o	Mvar
U_o	kV	U_o	kV

Autres tranches en service à la Centrale n°
Nature du combustible :
Conditions atmosphériques :

VI - CAUSES PRÉSUMÉES

a b c

a - Nature du premier défaut
b - Cause de la coupure des feux, du passage à vide, de la chute de barres, de la marche en réseau séparé, de l'ilotage ou du déclenchement total sans ilotage
c - Cause du déclenchement total après ilotage

- ☐☐☐ Avarie matériel principal
- ☐☐☐ Avarie matériel C^{ts} C^{des}, Prot., Régul.
- ☐☐☐ Essais
- ☐☐☐ Fausse manœuvre
- ☐☐☐ Défaut fileria
- ☐☐☐ Défaut fonctionnement de protections
- ☐☐☐ Défaut fonctionnement autom., régul.
- ☐☐☐ Défaut fonctionnement divers
- ☐☐☐ Défaut réseau
- ☐☐☐ Autres causes ou divers (à préciser)

VII - CONSÉQUENCES ET RÉPERCUSSIONS

Remise à disponibilité de la tranche le … à … h … mn
Recouplage ou reprise du parallèle le … à … h … mn
Motif du maintien à l'arrêt ou retard à la reprise du régime normal :

- ☐ Indisponibilité de tranche ☐ totale de … MW pendant … j … h … mn ☐ partielle de … MW pendant … j … h … mn
- ☐ Avarie de matériel - détail sur fiche 222 n°
- ☐ Conséquences sur autres tranches — Tranches n° / Fiches n°

Autres répercussions :

CONDITIONS du passage à charge nulle

- immédiat - volontaire ☐
- immédiat - automatique par protection ☐
- différé (reportable) ☐

VIII - ORIGINE DE L'INCIDENT

Emplacement du premier défaut

- ☐ Interne à la tranche
- ☐ Autre tranche de la centrale
- ☐ Auxiliaires communs
- ☐ Liaison centrale-poste
- ☐ Poste d'interconnexion sur lequel débite la tranche
- ☐ Réseau

Installation à l'origine du défaut

- Chaudière ou Réacteur et ses auxiliaires ☐
- Turbine et ses auxiliaires ☐
- Alternat. et Transformateur ☐
- Auxil. électriques de tranche ☐
- Auxiliaires Généraux ☐
- Externe ☐

IX - ÉTUDES DES ILOTAGES

Résultat	Attendu	Obtenu	
Pas de séparation	☐	☐	effectué au bout de :
Ilotage réalisé	☐	☐	durée :
Déclenchement total : après ilotage	☐	☐	au bout de : après ilotage
direct	☐	☐	au bout de : après début du défaut

En cas de mesure ou de court-circuit interne ou externe à la centrale

Forme: ☐ monophasé ☐ évolutif ☐ polyphasé — Durée
Caractère: ☐ fugitif ☐ permanent — Élimination ☐ correcte ☐ incorrecte

Nombre de feuilles complémentaires : Pièces jointes - Nombre : ☐ Schémas ; ☐ Autres

Vu, le Chef de centrale : , le 19

I - DESCRIPTION SOMMAIRE ET CAUSES DE L'INCIDENT (précisez les causes, la localisation et les caractéristiques du matériel incriminé)

II - CONCLUSIONS SUR LE COMPORTEMENT DE LA TRANCHE (MATÉRIEL ET CONDUITE) - MESURES PRISES OU A PRENDRE - ENSEIGNEMENTS A TIRER

III - INFORMATIONS PARTICULIÈRES FOURNIES PAR LES APPAREILS D'ENREGISTREMENT

(Oscilloperturbographe, tachyperturbographe, détecteur chronologique d'événements) autres que celles figurant en XI et XII.

XI - DÉROULEMENT DE L'INCIDENT (MÉCANIQUE, THERMIQUE, ÉLECTRIQUE, etc.)

h	mn	s	Phénomènes physiques apparus et perturbations successives observées (nature, valeurs, durée)	Alarmes, protections et sécurités ayant fonctionné	Déclenchements et manœuvres automatiques ou manuels intervenus et conséquences sur les installations de la centrale

XII - COMPORTEMENT DES PROTECTIONS - SÉCURITÉS ET RÉGULATIONS AYANT FONCTIONNÉ OU QUI AURAIENT DU FONCTIONNER

Désignation, caractéristiques et réglages (seuil et temporisation)	Temps réel de fonction'	Fonction' intem-pestif *	Fonction' explo-itation *	Origine des fonctionnements incorrects

Mentionner : c = correct, i = incorrect.

FICHE EVENEMENT

Filière · Groupe Palier · Site · Tranche · Date de l'événement · Numéro événement

Rédacteur de la fiche :

Identité de l'événement

Date Fin événement — Jour / Mois / An

Nature de l'événement

Documents de saisie ou origine

Matériel défaillant — Syst.Elém. · Rép.Mat. · Matériel · Code AM · Constructeur du matériel

Situation de la tranche Avant événement — Etat tranche · Puiss.Elect.(MW) · Puiss.Ther.(%) · Etat réacteur · Essai en cours

Circuit Primaire — Pression(Bar) · Température(°C)

Conséquences

Sur la tranche : — Action (A:auto. M:manu.) · Etat de Repli · Pression(Bar) · Température(°C)

Sur le fonctionnement de la tranche ou du système :

Puissance indisponible . MW — Durée Heures

Application des règles générales d'exploitation ou d'une consigne de conduite. — Code

Sur le matériel :

Syst.Elém. · Rép.Mat. · Matériel · Code AM (Matériel affecté) · Nombre matériel affecté · Durée de la réparation du matériel initiateur (Heures)

Sur la sûreté :

Sur le personnel et l'environnement :

Conséquence · Montant · Unité · Conséquence · Montant · Unité

Information fournie à l'extérieur — SCSIN · IPSN DSN-CEA · SCPRI · Préfecture · DII · Police ou Gendarmerie · Mairie · Parquet — O =Oui N =Non

Accessibilité : A.S. · A.E. — O=Oui N=Non

Causes de l'événement :

Numéros de fiches de suivi :

Mots clefs :

Résumé :

N° de Microfiche

Etat de la fiche

A : attente

T : terminée

ATTACHMENT D

			1st page
1	... DT FICHE DEFAILLANCE MATERIEL ULGC 03 ECRAN 1	1	SRDF FAILURE FORM
2.	CODE OPERATION	2	OPERATION CODE
3	- A AFFICHAGE - E EMISSION	3	- A DISPLAY - E EDIT
4	- M MODIFICATION - S SUPPRESSION	4	- M MODIFICATION - S DELETION
5	350 CLE TRANCHE-ANNEE-NUMERO (TAANNNNN)	5	350 UNIT,YEAR,FORM NUMBER
6	352 REFERENCE FONCTIONNEL	6	352 FUNCTIONAL CODE
7	354 NUMERO DT (GC)	7	354 WORK ORDER NUMBER
8	1?2 NUMERO CONSIGNATION	8	WITHDRAWAL FROM OPERATION ORDER NUMBER
9	100 REFERENCE DOCUMENTATION	9	100 DOCUMENTATION REFERENCES
10		10	
11	351 DATE DECOUVERTE ANOMALIE : JJMMAA	11	351 ANOMALY DECTECTION DATE :
12.	490 DATE DEBUT DEFAILLANCE : JJMMAA	12	490 BEGINNING OF FAILURE DATE :
13	371 ETAT DU MATERIEL SITUATION DU MATERIEL	13	371 ITEM OPERATIONAL MODE ITEM STATUS
14	- A ARRET - E ENTRETIEN/REQUAL.	14	- A STAND BY - E MAINTENANCE
15	- F FONCTIONNEMENT - N SERVICE NORMAL	15	- F OPERATION - N NORMAL OPERATION
16	- S SOLLICITATION - T ESSAI PERIODIQUE	16	- S ON DEMAND - T PERIODIC TESTING
17	355 DESCRIPTION SOMMAIRE DE LA DEFAILLANCE :	17	BRIEF DESCRIPTION OF THE FAILURE

FIGURE 6

J-22

D 1 FICHE DEFAILLANCE MATERIEL BLOC 00 <u>ECRAN</u> :

377 SITUATION DE LA TRANCHE	. 01 EN PUISSANCE 2 % PN
. 03 ATTENTE ARRET A CHAUD	. 04 ARRET POUR RECHARGEMENT
. 05 ARRET A FROID CUVE F.	. 06 ARRET INT. NON CONNECT. DU RRA
. 10 ARRET INT. SUR RRA	. 12 ARRET POUR INT. CUVE
359 MATERIEL ENTRAIN. INDISPO. MAT.	. - 0 OUI
379 CONSEQUENCE DE LA DEFAILLANCE	. 01 DECLENCHEMENT GTA
. 02 CHUTE DE BARRES	. 04 ILOTAGE
. 06 PASSAGE ATTENTE/ARRET A CHAUD	. 07 RETARD AU COUPLAGE
. 11 PERTE PARTIEL. SYSTEME OU VOIE	. 12 PERTE TOTAL. DU SYSTEME
. 30 REDUCTION DE CHARGE	. 40 APPLICATION Io
. 41 PASSAGE A L'ETAT DE REPLI (Io)	NOTA :
339 MODE OF DEFAILLANCE	:
340 COMPOSANT INTERNE AFFECTE	:
341 CAUSE PHYSIQUE DE DEFAILLANCE	:
358 DUREE REPARATION (H)	:
356 DUREE DEFAILLANCE (H)	:
365 DUREE INDISPONIBILITE TRANCHE (H)	: 364 INDISPO. TRANCHE (MWH)
367 NOMBRE D'HEURES MO CUMULEES	: 101 DOSE ABSORBEE (H.REM)
496 MESURES PRISES	: . 01 REMPLACEMENT TOTAL MAT.
. 04 MODIFICATION DU MATERIEL	: . 06 CONTROLES MAT. IDENTIQUES
. 20 [illegible]	: . 21 REPARATION PROVISOIRE
[illegible]	VERIFICATEUR :

2[nd] page

1	D 1 FAILURE FORM	
2	377 REACTOR OPERATIONAL MODE	: 01 POWER OPERATION
3	. 03 START UP - HOT STAND-BY	: 04 REFUELING
4	. 05 COLD SHUT DOWN	: 06 HOT SHUT DOWN (RHR N. OP.)
5	. 10 HOT SHUT DOWN (RHR OP.)	: 12 HOT SHUT DOWN (RCS OPEN)
6	359 ITEM UNAVAILABLE ?	: - 0 (YES)
7	379 FAILURE CONSEQUENCES	: 01 TURBINE TRIP
8	. 02 : REACTOR TRIP	: 04 SEPARATION FROM NETWORK
9	. 06 : START UP/HOT STAND BY	: 07 COUPLING DELAYED
10	. 11 PARTIAL LOSS OF FUNC. SYSTEM	: 12 COMPLETE LOSS OF F.S.
11	. 30 POWER REDUCTION	: 40 USE OF TECHN. SPECIFICATIONS
12	. 41 SHUT DOWN (REQUIRED BY TECH. SPEC.)	
13	339 GENERAL FAILURE MODE	:
14	340 FAILING COMPONENT	:
15	341 CAUSE OF THE FAILURE	:
16	358 REPAIR DURATION	:
17	356 FAILURE DURATION	:
18	365 UNAVAILABILITY DURATION	: 364 (LOSS OF GENERATION MWH)
19	367 NUMBER OF TOTAL WORK HOURS	: 101 RADIATION PROTECTION CONSEQUENCES (H. REM)
20	496 ACTION TAKEN	: 01 ITEM REPLACED
21	. 04DESIGN CHANGES	: 06 IDENTICAL ITEMS CHECKED
22	. 20 MANUFACTURER OF REF. CHANGES	: 21 PROVISIONAL REPAIR
23	056 WRITTEN BY	CHECKED BY

Attachment E

Reports Pertaining to Appendix J

1. "SRDF, The Reliability Data Collection System of EdF," by J. P. Schweitz.

2. "Bilan du SRDF, jusqu'au 31 Decembre 1981," by C. Hot, EDF Report DPT-SPT D544, 22 Fevrier 1983.

3. "Paluel Control Organization," by J. Grisollet.

4. "Data Processing and Data Display in Electricite de France PWR 1300 MW Nuclear Power Plants," by C. Hermant and G. Guesnier, IAEA Specialists Meeting, Dec. 5-7, 1979, Munich, FRG.

5. "A Distributed Architecture in the Control of the PWR 1300 MW Nuclear Plants of Electricite de France," by G. Guesnier, P. Peinturier, G. Varaldi, IAEA Specialists Meeting, May 14-16, 1980, Chalk River, Ontario, Canada.

6. "Electronic System of Power Station Control with Modules and Distributed Software Based on Controbloc Elements," by P. Peinturier, D. A. Mayrargue and G. Guesnier, IAEA Symposium, Cannes, France, April 24-28, 1978.

7. "Controbloc: An Advanced Programmable Relaying System for Large Generating Power Stations," ENKOR-Seoul, November 1980.

8. "Digital, Integratd Protection System (SPIN) Qualification Process," by J. M. Colling, J. Loubet, J. L. Brunet and L. Remus, IAEA Symposium, Munich, FRG, October 11-15, 1982, IAEA-SM-265/58.

9. "Project N4, Studies of Control Room and of Control/Command System (S3C Project), Overview."

APPENDIX K

EUROPEAN RELIABILITY DATA SYSTEM (ERDS)

APPENDIX K

EUROPEAN RELIABILITY DATA SYSTEM (ERDS)

The Joint Research Centre (JRC) at Ispra (Italy) of the Commission of the European Communities (CEC) has developed a centralized system called European Reliability Data System (ERDS) for collecting and organizing information related to the operation of LWRs. The ERDS project was started in 1977 and is now in the final design and implementation stages.

At JRC the ERDS project is a part of the reliability and risk evaluation program, which has a technical staff of between 19 and 20 individuals. This program has the following five components:

1) Development and implementation of ERDS, a centralized data bank which will provide information for LWR risk assessment to utilities, constructors and licensing authorities.

2) Analysis and processing of information in ERDS to implement a continuous feedback to reactor operations.

3) Development of PRA methodologies, including the completion of SALP, a fault-tree analysis computer code.

4) To conduct benchmark exercises for the comparison of PRA methods to build up a set of compatible and consistent procedures.

5) To conduct research on accident sequence simulation and control by developing techniques and models to simulate various phases of accidents, including operator response and emergency action.

ERDS is structured into four main data banks:

1) Component Event Data Bank (CEDB)

2) Abnormal Occurrences Reporting System (AORS)

3) Operating Unit Status Reports (OUSR)

4) Generic Reliability Parameter Data Bank (GRPDB)

CEDB

The CEDB is a data bank which collects failure, repair, and maintenance actions data for major LWR components, together with their technical specifications and operational histories. CEDB plans to rely upon the reliability data acquisition programs in Europe and the United States, such as the ATV system of Sweden, SRDF system of EdF France, the Caorso power station of ENEL, Italy, the Biblis power plant of the RWE/Gesellschaft für Reaktorsicherheit (GRS) of the Federal Republic of Germany (FRG), and INPO's NPRDS in the United

States. The JRC has set up a reference classification system in three parts in order to be able to clearly define components and to homogenize the data received from different national organizations and in different languages. The first is called the Reference System Classification (Tables I and II), which is an attempt to classify LWR components in more than 200 systems very similar to the IEEE Energy Industry Identification System (EIIS) and the system codes used in the AEOD Sequence Coding and Search System (SCSS). For each system there is given a description of its functions, boundaries, and interface with other systems and a list of the main components belonging to the system.

The second category is the Component Family Reference Classification, whose aim is to group components of similar engineering characteristics. They have identified up to 60 different types of components with a specification of its boundary, a set of 20 attributes describing its engineering characteristics. The last category is failure classification, which uses nine attributes to define such effects as failure modes, failure causes, etc.

The CEDB is still a pilot program which has collected engineering data on about 2000 components and about 500 failure reports. They anticipate receiving about 200 failure reports per plant per year. In the future they plan to obtain data from existing national programs such as EdF's SRDF and direct plant visits by JRC staff. The types of statistical analysis available can be seen from reports listed in Attachment B.

AORS

The Abnormal Occurrences Reporting System (AORS) consists of two types of abnormal occurrence data banks. The first consists of the operating national data banks such as the French Fichier d'Incident of CEA/EdF, the Italian event reporting system of Caorso (ENEL), the Swedish safety-related occurrence reporting system of SKI, and the USNRC LER system. The JRC also receives incident reports directly from five nuclear power plants -- three from Belgium, one from Holland, and one from FRG's Obrigheim. The second data bank is the AORS centralized data bank (AORS/CDB), which contains events selected from national data banks according to a selection criteria and predetermined format. AORS/CDB data is in the English language, having been translated from the original language. The structure of AORS can be seen by examining Figure K-1.

The purpose of AORS is twofold: 1) coordination of the various national incident reporting systems, and 2) homogenization of the reported data in the national systems as input for the AORS/CDB. Since there are differences in language and in the information content as well as in the criteria for reporting, JRC set up a mechanism for storing homogenized national data as well as a retrieval system for detailed analysis and comparison of the information in the different national systems. At the present time they have 40 Italian, 100-150 Swedish, and 50 U.S. reports in the homogenized (AORS/CDB) data bank. By the end of 1983 they estimate that they will have about 1500 selected incidents in AORS/CDB. They estimate that 700 reports/year/person can be transformed from the national incident data bank into the homogenized format. They've estimated

TABLE I - Reference System Classification: list of assemblies

(A)	Nuclear Heat System
(B)	Engineered Safety Features
(C)	Reactor Auxiliary System
(D)	Fuel Storage and Handling Systems
(E)	Radioactive Waste Management System
(F)	Steam and Power Conversion System
(G)	Power Transmission System
(H)	Electric Power System
(I)	Instrumentation, Supervision, Monitoring System
(L)	Protection and Control System
(M)	Plant Buildings HVAC System
(N)	Service Auxiliary Systems
(O)	Structural Systems

TABLE II - Reference System Classification: list of systems for assembly B

(B)	Engineered Safety Features
B1	Reactor Containment System (PWR)
B2	Reactor Containment System (BWR)
B3	Containment Spray System
B4	Containment Isolation System
B5	Containment Pressure Suppression System (BWR)
B6	Pressure Relief System (PWR)
B7	Hydrogen Venting System
B8	Post-accident Containment Atmosphere Mixing System
B9	Containment Gas Control System
B10	Auxiliary Feedwater System (PWR)
B11	Reactor Core Isolation Cooling System (BWR)
B12	Emergency Boration System (PWR)
B13	Standby Liquid Control System (BWR)
B14	Residual Heat Removal System (PWR)
B15	Residual Heat Removal System (BWR)
B16	High Pressure Coolant Injection System (PWR)
B17	Accumulator System (PWR)
B18	Low Pressure Coolant Injection System (PWR)
B19	Nuclear Boiler Overpressure Protection System (BWR)
B20	High Pressure Core Spray System (BWR)
B21	High Pressure Coolant Injection System (BWR)
B22	Low Pressure Core Spray System (BWR)
B23	Low Pressure Coolant Injection System (BWR)

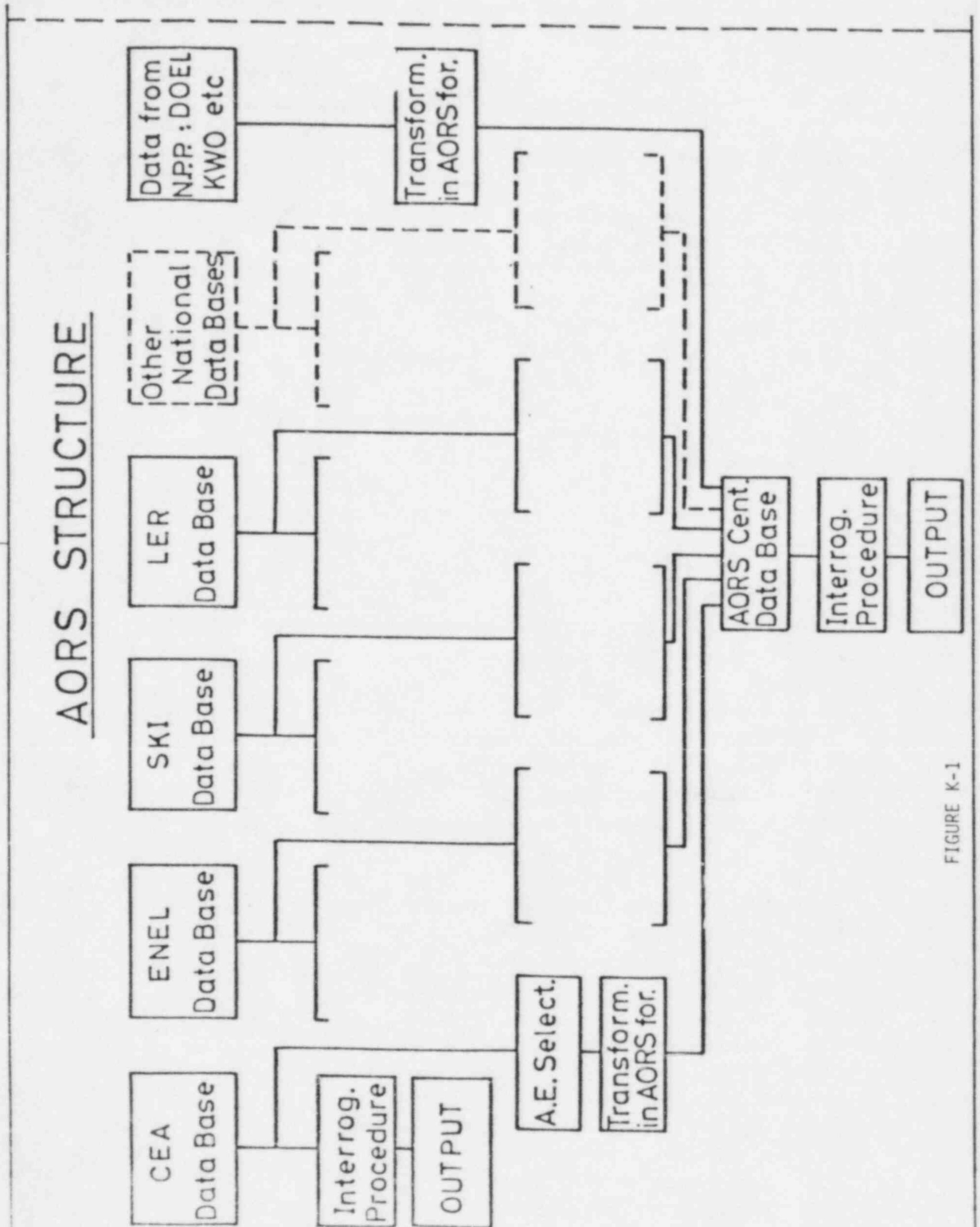


FIGURE K-1

FIGURE K-1

that they will put about 20-30 incidents/plant/year in the AORS/CDB bank. They have a staff of 7-10 people who carry out inputting of data into AORS and the analysis of the data. The selection categories are given below:

1. Release of, or exposure to, radioactive material
2. Degradation of safety-related systems
3. Deficiencies in design, construction, operation or evaluation with regard to safety
4. Generic problems of safety interest
5. Consequential actions
6. Events of potential safety significance
7. Effects of unusual external events, either of man-made or natural origin
8. Events which attract public interest

JRC has developed a standard incident reporting format as shown in Attachment A, which is a combined structured and narrative format reporting scheme. This is used as a basis for transforming the national incident reports into standard format for the JRC AORS/CDB data bank.

The AORS system has been designed so that the computer can aid in the analysis of the stored data by interrogation of the data. The following types of analyses can be carried out:

- Analysis for searches to be made for:
  - events or occurrences at similar units,
  - faults by system or component involved,
  - identification of trends or patterns,
  - common mode faults,
  - events involving personnel errors.
- Analysis for safety studies, such as:
  - abnormal occurrences selection for in-depth study,
  - consequence analysis,
  - event-tree and initiating event analysis,
  - plant operating experience analysis for feedback to utilities.
- Analysis for statistical studies according to well defined sample types, i.e.:
  - overall homogenization throughout countries and reactors,
  - partial homogenization per country or reactor,
  - identification according to coded information (system involved, cause of failure, etc.),
  - identification according to key-words in the free-text (initiating events, consequences, etc.).

In addition to the AORS, the JRC has established for the OECD Nuclear Energy Agency (NEA) a data bank called Incident Reporting System (IRS) for the NEA collected incident reports. These reports are those submitted by the OECD countries which, in addition to the Western European countries, include countries such as United States, Japan, Canada and Australia. The NEA-IRS data bank, although separate from ERDS, has the same format as the AORS-CDS data bank.

OUSR

OUSR is a centralized data bank containing information on outages in nuclear power plants. It is a collection of operating data from European nuclear power plants. JRC has developed three reporting forms: Event Report Form, Monthly Performance Report Form, and Daily Generation Report Form, which are completed by power stations and sent to JRC on a quarterly basis. A pilot program was completed using these new reporting forms involving three plants (Caorso, Doel and Fessenheim). The data from these reports are then computerized at JRC.

GRPDB

Since 1972 JRC has been placing into GRPDB reliability parameters of reactor components found in the literature. GRPDB uses the component classification codes developed for CEDB. GRPDB will be filled with processed data from the failure reports stored in CEDB.

A.O.R.S. **Abnormal Event Reporting Format** E.R.D.S.

A.E. Reference Number

National Reporting Ident. Code

Date of event

Categories

Total number of occurrences

Ref. code C.E.D.B.

Ref. code O.U.S.R.

Ref. code I.R.S.

TITLE: ______________________________

FACILITY STATUS (at the moment of event)

- ☐ Zero power / Hot stand by
- ☐ Starting - up
- ☐ Reduced power
- ☐ Full power
- ☐ Cold shut - down
- ☐ Hot shut - down
- ☐ Shutting - down
- ☐ Refuelling/Revision
- ☐ Raising power
- ☐ Under construction
- ☐ Unidentified
- ☐ Others

Power level in MWel

EFFECT ON OPERATION (after event)

- ☐ No significant effect
- ☐ Delayed coupling
- ☐ Plant outage
- ☐ Power reduction
- ☐ Reactor trip
- ☐ Turbine trip
- ☐ Hot shut - down
- ☐ Cold shut - down
- ☐ Loss of heat sink
- ☐ Loss of F.W. to S.G.
- ☐ Unidentified
- ☐ Others

Power level in MWel

ACTIVITY RELEASE ☐ No release

Personnel
- ☐ Within authorized limits
- ☐ Exceeding authorized limits

Environment
- ☐ Within authorized limits
- ☐ Exceeding authorized limits

SIGNIFICANCE DISCUSSION ______________________________

A.E. Reference Number

Event and Sequence description *(with detailed information about activity release, plant parameters variation, common cause, human error, initiating event, etc)*

A.E. Reference Number |_|_|_|_|_|_|_|_|_|_| Occ. number |_|_|

SYSTEMS INVOLVED DURING THE COURSE OF THE OCCURRENCE

|_|_|_| ______________________________
|_|_|_| ______________________________
|_|_|_| ______________________________
|_|_|_| ______________________________
|_|_|_| ______________________________
|_|_|_| ______________________________

FAILED SYSTEM OR EQUIPMENT

|_|_|_| ______________________________

FAILED COMPONENT OR PART

|_|_|_|_| ______________________________

EFFECT ON FAILED SYSTEM/COMPONENT

- ☐ No significant effect
- ☐ Loss of component function
- ☐ Degraded component operation
- ☐ Induced failure of another component
- ☐ Unavailability of another system/component
- ☐ Loss of system function
- ☐ Degraded system operation
- ☐ Loss of one redundancy
- ☐ Loss of more than one redundancy
- ☐ Others

CAUSE OF FAILURE

- ☐ Personnel
- ☐ Mechanical
- ☐ Electrical/Instrument
- ☐ Environmental
- ☐ Hydraulic
- ☐ Previous failure
- ☐ Common cause
- ☐ Unknown
- ☐ Others

DETAILED INFORMATION:

____
____
____
____
____
____
____
____
____

WAY OF DISCOVERY

- ☐ Audio/Visual alarm, Monitoring
- ☐ Rout. surveillance, Observation
- ☐ Testing
- ☐ Review of procedure
- ☐ Calling system into operation
- ☐ Inspection
- ☐ Maintenance
- ☐ Repair
- ☐ Unidentified
- ☐ Others

ACTION TAKEN

- ☐ No action taken
- ☐ Component/part replacement
- ☐ Component/part repair
- ☐ Adjustment/Recalibration
- ☐ New procedure
- ☐ Training
- ☐ Redesign/Modification
- ☐ Control of similar equipment
- ☐ Temporary repair/by pass
- ☐ Unidentified
- ☐ Others

Attachment B

Reports Pertaining to Appendix K

1. "The European Abnormal Occurrences Reporting System (AORS)," by J. Amesz, G. Francocci, R. Primavera and T. Van der Pas, 4th Euredata Conference.

2. "Operating Unit Status Report (OUSR), A Pilot Experiment for a Centralized Data Bank," by P. Bastianini and J. Soro, CEC-JRC Technical Note 1.06.01.82.52, May 1982.

3. "The European Reliability Data System: An Organized Information Exchange on the Operation of European Nuclear Reactors," by G. Mancini, J. Amesz, P. Bastianini and S. Capobianchi, IAEA Inter. Conf. on Nuclear Power Experience, IAEA-LN-42/311, Vienna, September 13-17, 1982.

4. "BIDIPES, A Conversational Computer Program for Point and Interval Estimation of Constant Failure Rate, Repair Rate and Unavailability," by A. G. Colombo and R. J. Jaarsma , EUR-7645EN, 1981.

5. "Bayesian Estimation of Constant Failure Rate and Unavailability," by A. G. Colombo and R. J. Jaarsma, IEEE Transactions on Reliability.

6. "State of Development of Statistical Methods for the European Reliability Data Systems," by A. G. Colombo, 14th Expert Meeting on Risk & Reliability, Ispra, May 28, 1982.

7. "An International Benchmark Exercise on System Reliability," by A. Amendola, IV EuRe Data Conference, Venice, March 23-25, 1983.

8. "DYLAM-1, Description and How-to-Use, Part I: Outlines of Event Sequences and Consequences Spectrum Methodology," by A. Mendola and G. Reina, CEC-JRC Tech. Note 1.05.01.82.147, October 1982.

9. "Human Models and the Problem of Data," by G. Mancini and A. Mendola, IV EuRe Data Conference, PER 654/82, Venice, March 23-25, 1982.

10. "Reliability in Electrical and Electronic Components and Systems," by E. Lauger and J. Moltoft, 5th European Conference in Electrotechnics - EUROCON 82, Copenhagen, Denmark, June 14-18, 1982.

11. "The Problem of Data Homogenization in Reliability Data Banks, A Scheme of Reference Classifications," by S. Capobianchi, T. Luisi, G. Mancini and M. Melis, PER 487/81, ANS/ENS Meeting on PRA, September 20-24, 1981, Port Chester, New York.

NRC FORM 335 (11-81)

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

1. REPORT NUMBER (Assigned by DDC)
NUREG/CR-3026
BNL-NUREG-51609

4. TITLE AND SUBTITLE (Add Volume No., if appropriate)
Feasibility Study on the Acquisition of Licensee Event Data

2. (Leave blank)

3. RECIPIENT'S ACCESSION NO.

7. AUTHOR(S) W. Y. Kato, R. E. Hall, T. Teichmann, J. Taylor, W. J. Luckas, Jr., P. Saha, P. Samanta and J. Fragola

5. DATE REPORT COMPLETED
MONTH May | YEAR 1983

9. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)
Brookhaven National Laboratory
Upton, New York 11973

DATE REPORT ISSUED
MONTH December | YEAR 1984

6. (Leave blank)

8. (Leave blank)

12. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)
Office of Policy Evaluation
Office of Nuclear Regulatory Research
U. S. Nuclear Regulatory Commission
Washington, D. C. 2055

10. PROJECT/TASK/WORK UNIT NO.

11. FIN NO.
A-3230

13. TYPE OF REPORT
Formal

PERIOD COVERED (Inclusive dates)

15. SUPPLEMENTARY NOTES

14. (Leave blank)

16. ABSTRACT (200 words or less)

Brookhaven National Laboratory's Department of Nuclear Energy (DNE) has performed a study of the Licensee Event Report (LER) system. The objective of the study was to assess the feasibility of modifying the LER reporting system as proposed by NRC-AEOD, and/or developing an alternative plan that would in addition collect information about significant events amenable to statistical analysis, such as multi-case, multi-variate analysis.

The study indicated that the LERs constitute reports from a large variety of events which have in most cases many different plant parameters, both measured and currently not measured, to characterize the event. In order to determine event-specific plant parameters required for statistical and deterministic analysis, a data matrix approach was used to identify those parameters which are currently being recorded, those which could be measured and recorded, and those which are required for certain types of events involving thermal-hydraulics and neutronics as illustrative of events requiring in-depth analysis.

Also included in the study was a review of INPO's Nuclear Plant Reliability Data System; NASA's Problem Reporting and Corrective Action (PRACA) program; Electricité de France's KIT system, an automatic computer-based reactor parameter monitoring and recording system; and the regulatory relationship between the FAA and the commercial airline industry.

17. KEY WORDS AND DOCUMENT ANALYSIS

17a. DESCRIPTORS

Licensee Event Report
Statistical Analysis
LER Reporting System
Events Analysis
Reliability Data
NPRDS

17b. IDENTIFIERS/OPEN-ENDED TERMS

18. AVAILABILITY STATEMENT

19. SECURITY CLASS (This report)

21. NO. OF PAGES

20. SECURITY CLASS (This page)

22. PRICE
$

NRC FORM 335 (11-81)

*U.S. GOVERNMENT PRINTING OFFICE: 1985 515 034 10015