

Johnson #14

The attached report by S. Levy, is being used as a major contribution to two Technical Assessment staff reports, as follows:

- 1) Simulation Adequacy (Chapter 2,3,& 5 of Levy Report)
- 2) Design Margins (Chapter 4 of Levy Report)

These reports, which will include additional material and staff analysis, are still in preparation.

SEP 5 1979

Handwritten signature or initials

8001 220 765

P

SLI-7904
AUGUST 1979

SEP 5 1979

#14
Lounsbury

STAFF DRAFT CONFIDENTIAL
NOT FOR DISTRIBUTION

A STUDY OF SIMULATION AND
SAFETY MARGINS IN LIGHT WATER REACTORS

S. LEVY INC.

1999 South Bascom Avenue
Campbell, California

SEP 5 1979

CONFIDENTIAL
NRC
REGISTRATION

A STUDY OF SIMULATION AND
SAFETY MARGINS IN LIGHT WATER REACTORS

Prepared for the
President's Commission on the Three Mile Island Accident

by
S. Levy and J. E. Hench

SLI-7904

August 26, 1979

S. LEVY INC.

Suite 725

1901 S. Bascom Ave.

Campbell, CA 95008

STATE DEPT. CONFIDENTIAL
EXCEPT FOR DISTRIBUTION

NOTICE

This report was prepared as an account of work sponsored by the United States Government. Neither the United States Government nor any of their employees, nor any of their contractors, subcontractors, or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness or usefulness of any information, apparatus, product or process disclosed, or represents that its use would not infringe privately owned rights.

SLI-7904

ABSTRACT

STAFF DRAFT CONFIDENTIAL
NOT FOR DISTRIBUTION

A study was performed at the request of the President's Commission on the Accident at Three Mile Island to assess the potential for safety enhancement through the expanded use of simulation and to assess the adequacy of margins in today's light water reactors. Many experts were interviewed in both the nuclear and the aerospace disciplines in the process of gathering information on improving nuclear safety. Some recommendations are made for improving margins in nuclear safety by making equipment modifications, by application of improved simulation and by application of some commonly used aerospace techniques.

TABLE OF CONTENTS

	<u>Page</u>
ABSTRACT	
SUMMARY	1
1.0 INTRODUCTION	6
2.0 ANALYTICAL SIMULATION STATUS	9
2.1 <u>General Comments</u>	9
2.1.1 Type of Analyses	9
2.1.2 Segmentation of Analyses	10
2.1.3 Capability for Analyses	15
2.1.4 General Findings and Recommendations	16
2.2 <u>Steady State Analyses</u>	17
2.2.1 Background	17
2.2.2 Findings and Recommendations	18
2.3 <u>Transient Analyses</u>	19
2.3.1 Background	19
2.3.2 Findings	20
2.3.3 Recommendations	29
2.4 <u>Accident Analyses</u>	30
2.4.1 Background	30
2.4.2 Findings	43
2.4.3 Recommendations	57
2.5 <u>Damage Analysis</u>	58
2.5.1 Background	58
2.5.2 Findings and Recommendations	59

	<u>Page</u>
2.6 <u>Training Simulator Models</u>	60
2.6.1 Background	60
2.6.2 Findings	62
2.6.3 Recommendations	64
3.0 HARDWARE TYPE SIMULATORS	66
3.1 <u>Engineering Simulators</u>	66
3.1.1 Concept	66
3.1.2 Applicability	67
3.1.3 Feasibility	69
3.1.4 Implementation Schedule	69
3.1.5 Merit	70
3.2 <u>Control Room Safety Enhancement</u>	71
3.2.1 Concept	71
3.2.2 Feasibility	74
3.2.3 Implementation Schedule	74
3.2.4 Merit	75
3.3 <u>Improved Reactor Training Simulator</u>	76
3.3.1 Concept	76
3.3.2 Applicability	76
3.3.3 Feasibility	77
3.3.4 Implementation Schedule	77
3.3.5 Merit	78
3.4 <u>Simulator for Each Site</u>	79

	<u>Page</u>
3.4.1 Concept	79
3.4.2 Applicability	79
3.4.3 Feasibility	80
3.4.4 Implementation Schedule	80
3.4.5 Merit	81
4.0 SAFETY MARGINS	82
4.1 <u>Approach</u>	82
4.2 <u>Basic Nuclear Safety Philosophy</u>	82
4.2.1 Description of Philosophy	82
4.2.2 Evaluation of Loss of Coolant at Very High Pressure	85
4.2.3 Evaluation of Loss of Coolant at Medium Pressure	87
4.2.4 Evaluation of Means to Improve Probability - Damage Estimates	89
4.2.5 Findings and Recommendations	94
4.3 <u>Design Margins</u>	97
4.3.1 Background	97
4.3.2 Findings and Recommendations	99
4.4 <u>Equipment Margins</u>	102
4.4.1 Discussion	102
4.4.2 Conclusions	111
4.4.3 Recommendations	112
5.0 COMMUNICATION LINK TO REMOTE CENTERS	113
5.1 <u>Concept</u>	113

	<u>Page</u>
5.2 <u>Applicability</u>	113
5.3 <u>Feasibility</u>	114
5.4 <u>Implementation Schedule</u>	114
5.5 <u>Merit</u>	114
6.0 APPLICATION OF AEROSPACE TECHNIQUES TO NUCLEAR SAFETY	116
6.1 <u>Concept</u>	116
6.2 <u>Applicability</u>	117
6.3 <u>Feasibility</u>	118
6.4 <u>Implementation Schedule</u>	118
6.5 <u>Merit</u>	119
APPENDIX I	120

LIST OF FIGURES

<u>Figure</u>	<u>Title</u>	<u>Page</u>
1	Prediction of TMI-2 Turbine Trip With POWERTRAIN	22
2	Prediction of TMI-2 Turbine Trip With POWERTRAIN	23
3	Prediction of Oconee Feedwater Loss With POWERTRAIN	24
4	Prediction of Oconee Feedwater Loss With POWERTRAIN	25
5	Prediction of Oconee Feedwater Loss With CADDS	26
6	Prediction of Peach Bottom-2 D Level Flux Turbine Trip	28
7	Typical Equipment Malfunction Set for LOCA Evaluations	32
8	B&W Analysis of Pressure for Small Break	34
9	B&W Analysis of Core Mixture Height for Small Break	35
10	B&W Analysis of Fuel Cladding Temperature for Small Break	36
11	High Pressure Loss of Inventory Logic Diagram	38
12	Intermediate Pressure Loss of Inventory Logic Diagram	39
13	Low Pressure Loss of Inventory Logic Diagram	40
14	Pressurizer Level Performance for 0.01 ft ² Break	44
15	Natural Circulation Behavior for 0.01 ft ² Break	45
16	Various Pressure Predictions for Small Break	48
17	Various Coolant Escape Rate Predictions for Small Break	49
18	Various Clad Temperature Predictions for Small Break	50
19	Prediction of Pressure for TMI-2 Accident	51
20	Prediction of Hot Leg Temperature for TMI-2 Accident	52

<u>Figure</u>	<u>Title</u>	<u>Page</u>
21	Prediction of Pressurizer Level for TMI-2 Accident	53
22	High Pressure Loss of Inventory Logic Diagram	86
23	Medium Pressure Loss of Inventory Logic Diagram	88
24	New B&W System Response	91
25	Reactor Coolant System Arrangement - Elevation, from TMI-2 FSAR	-- 109
26	Reactor Coolant System Arrangement - Elevation, from Davis-Besse Unit 1 FSAR	 110

<u>Table</u>	<u>Title</u>	<u>Page</u>
1	Codes Availability to NRC for Predicting Reactor Transients and Loss of Coolant Accident (LOCA)	11
2	B&W Codes for Predicting Reactor Transients and Loss of Coolant Accident (LOCA)	12
3	Application of B&W Codes to Analyzed Accidents	13
4	Listing of Possible Small Break Experiments	55
5	Comparison of Key Characteristics of Operating B&W Plants with CE and <u>W</u> Plants for the Loss of Feedwater Transient	103
6	Susceptibility to PORV Lift for B&W, CE and <u>W</u> PWRs As a Result of a Loss of Feedwater Event	104
7	Summary of PWR ATWS Analyses	106

Summary

The result of this two month study of light water reactor safety margins and ways of improving them has been reassuring from the standpoint of the overall degree of safety which exists in current light water reactors. The concept of defense in depth (which has been used to protect against both those events which have been defined, as well as those undefined events, such as TMI-2 accidents) has worked well and should be preserved. The overall conclusions of this study are that, although the present concepts of safety are sound, the event at Three Mile Island has generated new insights for providing an improved level of safety.

The major conclusions of this study, which are discussed in more detail in the main body of this report are summarized below:

- There are some sequences of events, similar to the event at Three Mile Island, in which a small number of equipment failures can lead to very serious fuel damage. (See section 4.2). These cases involve a slowly developing situation, in which the normal and auxiliary feedwater are not available. If no heat can be rejected through the steam generator, the only means of rejecting heat is through the relief valves (plus a small amount through the makeup and letdown system). It then becomes possible for the system to lose inventory through the safety or relief valves, while remaining at a pressure too high for automatic actuation or effectiveness of safety systems, and too high for even manual actuation in some designs.

12

• The discovery of these potentially unacceptable sequences emphasizes the need for a thorough study of degraded normal and abnormal transient events, based upon a probabilistic approach, such as the one in section 4.2 of this report. The probabilistic approach chosen for such a study could be somewhat qualitative, but it should be capable of making the various accident and transient safety margins relatively consistent. The study should not focus on just early loss of coolant events but also on long term cooling, increased reactor power to flow ratios, reactivity changes, ... etc. Such evaluations should be made by following the event in terms of time and defining the possible failures, the information available to operators, and their alternate courses of action. At every step of the sequence, a probabilistic judgement coupled with an approximate damage assessment should be developed to evaluate whether changes are needed in design, information available to operator, or operating procedures. These evaluations should be performed with the involvement of operation personnel so that they can employ the studies to generate malfunction charts and logic diagrams to replace many of the written operating procedures (see section 6).

• Consideration should be given to having a computerized data interpretation system such as the one described in section 3.2, in every control room to interpret the disparate signals coming to the reactor operator. This computerized system would process the control room information in such a way as to make it easier for the operator to know what is happening in his power plant, and therefore be more likely to make the correct decisions in a crisis.

• Communications should be improved (see section 3.2). This could be done by displaying the safety data interpretation system information described above at a remote center in addition to the control room of the nuclear power plant. A dedicated telephone line for voice communication from each site to a remote center should also be utilized.

✓ • Consideration should be given to having a recording device such as the B&W Reactimeter at each site to automatically record data when an upset condition occurs. This could be used to reconstruct the chain of events after serious accidents, as well as a means for collecting valuable data from less serious events for calibration of computer analytical results.

• While NRC action taken to date will reduce the probability and consequences of degraded events, consideration should be given to the following equipment modifications as a means of further increasing safety margins:

- Increase the availability of the steam generator by making the auxiliary feedwater system single failure proof
- Incorporate a means for measuring level or water inventory in the primary system of PWRs and employ this diversified instrumentation for initiating emergency cooling systems
- Incorporate a positive means of knowing when safety and relief valves are open or shut
- Increase the redundancy of Power Operated Relief Valves

- would include interpretation of void fractions present

- Eliminate loop seals from pressurizer lines
- 7 - Design the pressure relief system (safety plus relief valves) to be less dependent upon steam generator heat removal
- Raise the HPI shutoff head to the safety valve pressure range
- Improve the control room design through increased information processing by computers

Detailed evaluations of the proposed equipment modifications should be made to determine which can and should be considered.

• The nuclear industry currently does not have a computer code capable of simulating important control function, plant systems, operator-plant interactions, and loss of coolant. Such calculations are being performed by synthesizing the results of several computer programs, making it very difficult to perform analysis for a variety of fault tree events. Such a code can and should be developed in the next two years.

• Continued development of available computer codes is recommended. Verification of such models with tests is essential, especially in the area of plant transients.

• Consideration should be given to the development of a single high fidelity engineering simulator which implements all aspects of the small break and transient analyses (see paragraph 3.2). This advanced, high fidelity simulator could be used to perform the sequence of events investigations recommended above. A possible drawback to the use of

such a simulator is its very long schedule for implementation (six or seven years) and its high cost. It is suggested that scoping of such a facility be undertaken to assess its software feasibility and schedule. In the meantime, improved analytical models such as discussed in the preceding paragraph or such as are being developed by the NRC, (improved TRAC transient version) should be accelerated.

- Consideration should be given to the use of improved training simulators at reactor sites to be used for ad hoc studies following abnormal events, to verify the maintenance of adequate margins, and to train operators in coping with such new events.

- A mechanism should be developed to improve the feedback from the reactor operators (electric utility) to the reactor suppliers and architect engineers who design the control rooms, plant and equipment. This should result in improved operability and therefore improved overall plant safety.

INITIAL
2V1.0 INTRODUCTION

This report is in response to a request from the Staff of the President's Commission on the Three Mile Island Accident. It provides an evaluation of simulation in the nuclear light water reactor industry and how it might be improved. The term "simulation" is used herein to describe the analytical models and computer programs to predict the detailed performance of light water reactors for reactor design and licensing. It also includes the hardware systems driven by computers which simulate events in the power plant and which are used for operator training and other similar man-machine applications.

The study was performed over a period of two months and was carried out by holding meetings with various organizations in the nuclear and space industry. A complete listing of the meetings and organizations contacted is given in Appendix I. Because of the limited time available and the small number of persons involved, the study cannot be considered comprehensive or complete. However, it is hoped that it is responsive to the following objectives agreed to with the Staff of the President's Commission:

1. Evaluate the analytical models and predictions available in the nuclear light water reactor industry. Assess their capability and accuracy and provide recommendations for improvement.

2. Evaluate hardware type simulators employed in the nuclear industry and compare their status to that of the space industry. Provide recommendations for improvement and, in particular for application to design, accident prevention, accident investigations, and improved operator training of light water reactors.
3. Assess design margins and make recommendations for margin or equipment changes and improvement.

It should be recognized that the above stated objectives are rather broad and that the assessment could focus only upon selected areas for which information was readily accessible. The results of this assessment are presented in five major sections following this introduction.

Section 2 contains a discussion of analytical simulation in the light water reactors industry. It discusses the various types of analyses performed and provide findings and recommendations for each separate area of analysis.

Section 3 deals with the hardware type simulator with man-machine interactions. It describes the simulators available in the nuclear and space industry and describes four different types of simulators which could be considered for improvement.

Section 4 is concerned with design margins and it contains an assessment of the available margins and how they might be improved by improved communications, procedures, and equipment.

Section 5 discusses communication links between reactor sites and other locations, such as a central command center located in Bethesda.

Section 6 discusses the application of some aerospace technology and techniques to enhance safety at nuclear power stations.

The results of the study are presented in terms of findings and recommendations through each of the Sections of the report with principal results reiterated in the Summary.

2.0 ANALYTICAL SIMULATION STATUS

2.1 General Comments

2.1.1 Type of Analyses

A light water nuclear power plant with its many components, subsystems and systems requires the use of a very large number of analytical models, computer programs, and analytical tools for design and licensing. It is not the purpose of this section to cover all such analyses, but rather to focus upon the state of the reactor and water in the primary system. The models available to describe conditions in the reactor can be broken down into several categories.

They are:

1. Steady state analyses. Such models deal with reactivity, fuel enrichment, heat transfer, power, and flow distribution in the reactor on a steady-state basis. They also provide many input parameters to transient computations. Sometimes, they are employed to describe very slow transients which can be evaluated on a quasi-steady state basis.
2. Transient analyses. These models deal with most normal and abnormal plant disturbances. They employ a relatively simple representation of the reactor primary system, but include accurate control and safety functions in their modeling. They tend to deal with small departures from normal conditions and not accidents.
3. Accident analyses. These analyses deal with unexpected events such as a leak or break in the primary system, control blade drop or ejection...etc. They are transient calculations but they analyze

STATE DEPARTMENT
CONFIDENTIAL

conditions more degraded than those in the transient analyses described above.

4. Damage Analyses. Several of the accidents may lead to damage to the reactor core and the calculation of such damage often requires a separate analysis. The accident may alter the reactor configuration and conditions may be quite different than those under normal transient, or the initial stages of the accident.
5. Training Simulator Models. Such simulators often employ different and simplified models than those in design or safety analyses, and they are best dealt with as a separate group.

In this particular section, we shall put special emphasis on transient and accident analyses, and simulator models as they are of greatest importance in avoiding TMI type accidents.

2.1.2 Segmentation of Analyses

The kind of information required and accuracy and details of the calculations can be expected to vary with each kind of analysis. For example, considerable accuracy and details in the reactor core are utilized in steady state calculations while many accident analyses employ a much more lumped representation of the core. This has led to the development of computerized models (or codes) which are applicable only to certain types of events and often to rather limited scenarios. This problem is illustrated in Table 1 which lists the codes available to the NRC for transient and loss of coolant accident (LOCA) analyses, their applicability and non-applicability. Table 2 shows comparable information for the B&W codes. As shown in Table 3, the

TAF-1 - YES - AVAILABILITY - AC FOR PREDICTING REACTOR TRANSIENTS AND LOSS OF COOLANT ACCIDENT (LOCA)

CODE	LAB	WHEN AVAILABLE	APPLICABILITY
RT	BNL	NOW	For PWR transients, not for small breaks. Improvement needed in steam generator modeling. Fast running time. Controls and trips not as good as in RETRAN
RAMONA-III	BNL	December 1979	Good for many BWR transients and accidents. Not for small breaks. Fast running. Some control system by December 1979; Complete controls by September 1980.
RETRAN	BNL, INEL (from EPR)	July 1979	Good for Reactor Transients (PWR and BWR). Not adequate for LOCA or small breaks. Good trips and control logic. Long running time.
-50	BNL	NOW	Adequate for many PWR transients. Not for small breaks. Control logic not as good as that of RETRAN. Long running time.
RELAP-4/ MOD 7	INEL	December 1979	Possibly more adequate than RELAP-4/MOD 6. For PWR LOCA and small break analysis. Long running time. Inadequate controls and trips for reactor transients.
MAC-PIA	LASL	NOW	For PWR LOCA. Excessive Running Time (3 Hrs on large computer) Consequences of collapsing nodes to reduce running time for small breaks not yet assessed. Trips and controls not adequate for reactor transients analyses.
RELAP-5	INEL	NOW	For PWR LOCA. Running time, about equal to that of TRAC-PIA. Insufficient assessment as of now concerning small break capability. Trips and controls not adequate for reactor transients analyses.
MAC-PDI	LASL	December 1979 (PWR)	Good, fast running code, capable of addressing PWR small breaks and reactor transients. Trips and controls as per RETRAN.

*Based on similar version furnished by NRC Research

TABLE 2 - B&W CODES FOR PREDICTING REACTOR TRANSIENTS AND LOSS OF COOLANT ACCIDENT (LOCA)

CODE	TYPE	APPLICABILITY
POWER TRAIN	ANALOG-DIGITAL HYBRID	Good for PWR transients. Detailed control and secondary plant model. Real time results. Not for small breaks and no two-phase flow.
CADDS	DIGITAL	Good for PWR transients. More detailed core model but less detailed control systems. Long Running Time. Not for small breaks and no two-phase flow.
CRAFT	DIGITAL	For PWR LOCA in primary system. Long running time. Controls and trips inadequate for reactor transients.
TRAP	DIGITAL	For PWR LOCA in secondary system. Long running time. Controls and trips inadequate for reactor transients.

NOT CONFIDENTIAL
NOV 19 1970

CONFIDENTIAL

<u>CLASSIFICATION</u>	<u>ACCIDENT</u>	<u>CODE</u>
Decrease in Reactor Coolant Inventory	-LOSS OF COOLANT ACCIDENT (LOCA)	CRAFT
	-MALFUNCTION OF LETDOWN SYSTEM	CRAFT
	-SAFETY VALVE (PSV) STUCK OPEN	CRAFT
Radioactive Release From Subsystem or Component	-WASTE GAS TANK RUPTURE	--
	-FUEL HANDLING ACCIDENT	--
Anticipated Transient Without Scram (ATWS)	-LOSS OF FEEDWATER	CADDS
	-LOSS OF OFFSITE POWER	CADDS
	-ROD WITHDRAWAL	CADDS
	-TWO PUMP COASTDOWN	CADDS
	-SAFETY VALVE STUCK OPEN	CRAFT

application of codes vary with the type of accident analysed. In some cases the results from one code are required as input to another code (i.e. POWER TRAIN/CADDS, TRAP/CADDS). Such segmentation is a serious drawback to being able to calculate the entire course of TMI type accidents. No single code exists that combines a good control system and a good small break model. While such calculations can be performed by combining several available codes, the analyses are not flexible enough to readily evaluate changes in the possible branches of the fault trees. This is all the more true when operator actions are included.

Superimposed upon this segmentation of analyses for different transient and accident types is the fact that many calculations are performed for licensing purposes rather than on a best estimate basis. In other words, as will be discussed later, some of the answers generated by LOCA codes may not be indicative of what the operators will see.

2.1.3 Capability for Analyses

The capability for analysis varies from one organization to another. At present, the best capability resides with the reactor suppliers who can perform the entire range of calculations. Next, in terms of capability, comes the NRC. While the NRC could call upon national laboratories to attain the same level of proficiency as the reactor suppliers, they have chosen often to assess and audit the results from manufacturers analyses rather than reproduce them. This is not a serious drawback except under those special conditions where the NRC might be thrust into a lead role. One exception in NRC capability is the area of analyzing the LOCA with a large line break.

In this area, the NRC codes appear to be at the forefront of technology. However, in other areas such as plant transients or the analysis of the LOCA with a small break, the NRC capability clearly lags that of the reactor manufacturers. The widest spread in range of analytical capability exists among the plant owners or operators. Some utilities such as TVA, Duke Power Company, and others have developed good analytical capability while other utilities have almost none. EPRI, through its RETRAN code and other similar programs, is trying to make it possible for all plant owners to have adequate independent analytical tools. However, analytical independence by all utilities is not true today, and several plant operators have to rely very heavily, if not exclusively, upon manufacturers for most of their analytical evaluations. Under such circumstances, the plant operating engineering support group cannot help but be less responsive and lacking in complete understanding, especially for unexpected type events.

2.1.4 General Findings and Recommendations

1. There is a strong need for analytical simulation of fault tree events which involve control systems, operator actions, and equipment failure such as occurred at TMI. Such calculations need to incorporate man-machine interactions and need to be performed on at least a real time and on a best estimate basis.
2. The NRC needs to accelerate its efforts to develop independent capability to analyze transients and accidents.

3. Utilities should develop the capability to perform transient and accident analyses. This could be accomplished through an acceleration of EPRI efforts to develop codes for utility use; or by giving utilities access through a remote terminal to some of the manufacturers codes; or by giving the utilities the support required for them to effectively use the computer programs developed by the NRC.

2.2 Steady State Analyses

2.2.1 Background

The steady-state reactor analyses are concerned with calculating the three dimensional power distribution, reactivity, exposure, and thermal hydraulic characteristics in the core at start-up and as fuel burn-up progresses. The reactivity computations involve several nuclear group cross sections and many parallel flow paths. They are multinode calculations and often take several hours on the fastest digital computers available. Simplified similar analyses are performed on process computers installed at most nuclear power plants.

The steady-state calculations are of utmost importance to the performance and economics of power plants. They yield the fuel enrichment and operating reactivity strategy, both of which control fuel cycle costs. They also determine the allowable operating power level by computing two important parameters: peak fuel duty (expressed in terms of kw/ft of fuel rod) and the margins to Critical Heat Flux (CHF), also called Departure from Nucleate Boiling (DNB). These two parameters, which will be discussed in more detail

in Section 4, are specified in the plant Technical Specifications together with maximum plant power. Very detailed and extensive steady-state analyses are performed to assure that the Technical Specifications are satisfied.

The methods employed for steady-state calculations have been improved considerably over the years. With increased computer capability, more details have been incorporated in the analyses. Also, comparison with numerous separate effect tests and in-reactor measurements have validated the codes and put them on a sound basis.

2.2.2 Findings and Recommendations

1. Commercial incentives and plant performance warranty pressures are enough to assure the continued development and verification of steady-state models by industry. For that reason, no recommendations are necessary in this area.
2. The steady-state codes are somewhat inconsistent in their approach and details. In some portions of the model, extreme details and accuracy are provided while failing to recognize some of the approximations employed in associated areas such as two-phase flow.
3. Continued evaluation of steady-state models against in-reactor performance is essential to assuring accuracy and improvement in such methods.

4. Several of the outputs from steady state codes are employed in other performance and safety evaluations. Often, such parameters are taken at their bounding values which make ensuing calculations not representative of what the operators might see. It would be desirable to identify all such outputs, their best estimated values and their range of uncertainty. Such a tabulations could be of great assistance in performing best estimate calculations and formulating future model improvements and additional in-reactor tests.

2.3 Transient Analyses

FRAP IGNORED

2.3.1 Background

Most of these analyses are performed through such codes as IRT, RETRAN, POWER TRAIN and CADDs listed in Tables 1 and 2. Many other similar tools are available and they tend to serve two purposes:

1. Investigate total plant dynamics and, in particular, optimize control systems for normal and off-normal operations.
2. Investigate anticipated plant transients and assure that appropriate safety margins are satisfied.

While primary emphasis will be placed in the following discussion upon POWER TRAIN and CADDs, it should be realized that the comments are generally applicable to other available models.

POWER TRAIN is a B&W computer program concerned with total plant simulation. It includes a simplified reactor representation (point kinetics and single control volume for heat transfer), and pressurizer model (three control volumes, heaters, sprays and relief valves), and a transport delay representation of the primary flow recirculation loop. The secondary system is well represented and a very detailed simulation of the once-through steam generator is included. Setpoints and controller gains can be modified on-line and capability exists for automatic or manual change of any control element. POWER TRAIN is used for control system optimization, verification of plant maneuverability and some control and protection system failure and system effects analyses. It is utilized to investigate such anticipated transients as turbine trip with or without reactor scram; load rejection; loss of feedwater; reactor coolant pump trips; and feedwater heater failures.

CADDS is a B&W computer program which performs many of the same analyses as POWER TRAIN except that it contains much less plant control details but an improved reactor core representation. It is employed for many transients where peak fuel conditions become important such as the coastdown or a locked rotor of reactor coolant pump, control rod withdrawal, control rod drop...etc.

2.3.2 Findings

1. There are many limitations to the transient models. For example, POWER TRAIN applies to power levels between 15 and 100 percent and

STATE OF MISSISSIPPI
NUCLEAR REGULATORY COMMISSION

is not suitable for decay power level or low power natural circulation studies. No two-phase condition is allowed in the primary system, i.e. it cannot simulate a system piping break or two-phase natural circulation without a break. The pressurizer cannot go solid or entirely empty (i.e. relief valves always discharge steam) and the modeling of the emergency core cooling systems (ECCS) are not included. In other words, POWER TRAIN application is limited to those transients where the primary system remains relatively close to normal and water solid. Many of the same limitations (no two-phase flow; no system piping break; no ECCS actuations) are applicable to CADDs. In addition, several of the control functions incorporated in POWER TRAIN are not included. On the other hand, CADDs is capable of dealing with low power levels down to decay heat and below.

2. Several comparisons of the models have been made to start-up tests data and reactor transients. The trends in the reactor system behavior are reproduced by the models as shown in Figures 1, 2, 3, 4, and 5. Figures 1 and 2 deal with a turbine trip from 95 percent power at TMI-1. Figures 3 and 4 are concerned with a loss of feedwater at Oconee from 76 percent power. Figure 5 shows the same turbine trip at Oconee as compared to the CADDs prediction. While the correspondence is acceptable, some discrepancies are still noted in Figure 1 and 5 in terms of the predicted power level for both POWER TRAIN and CADDs. These discrepancies deserve further investigation. In the case of POWER TRAIN, the peak pressure level also

FIGURE 1- PREDICTION OF TMI-1 TURBINE TRIP WITH POWER TRAIN

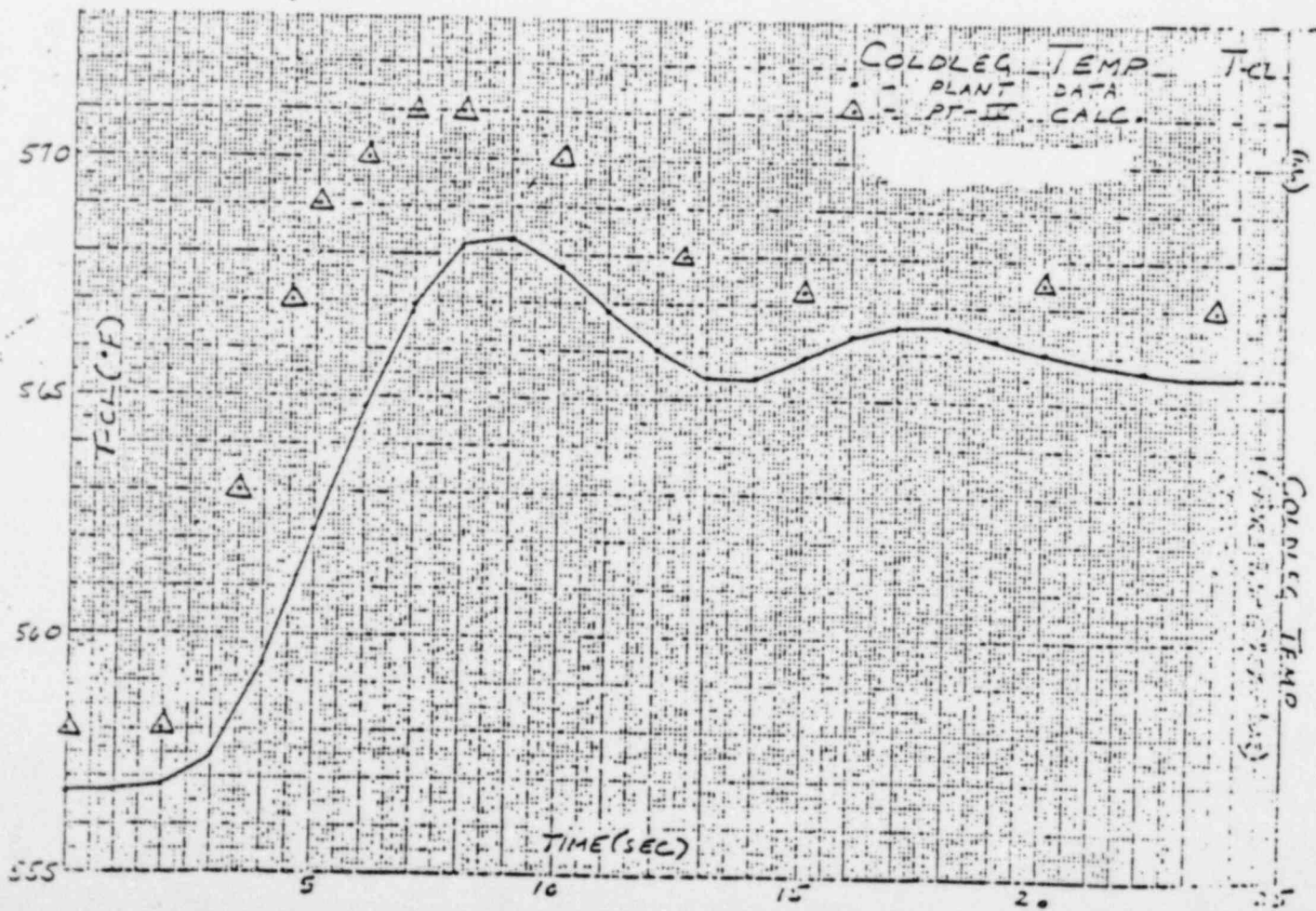
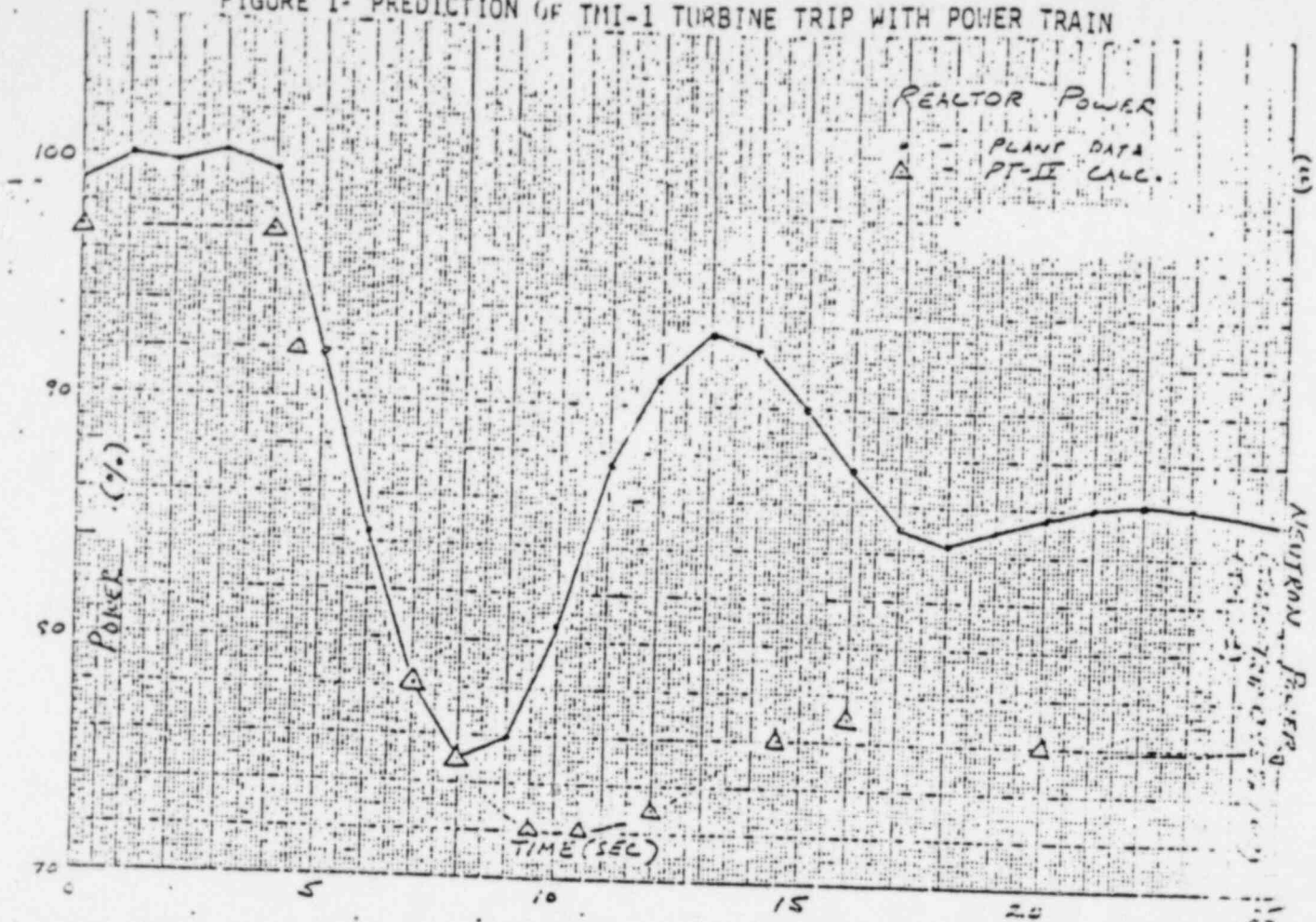


FIGURE 2-PREDICTION OF TMI-1 TURBINE TRIP WITH POWER TRAIN

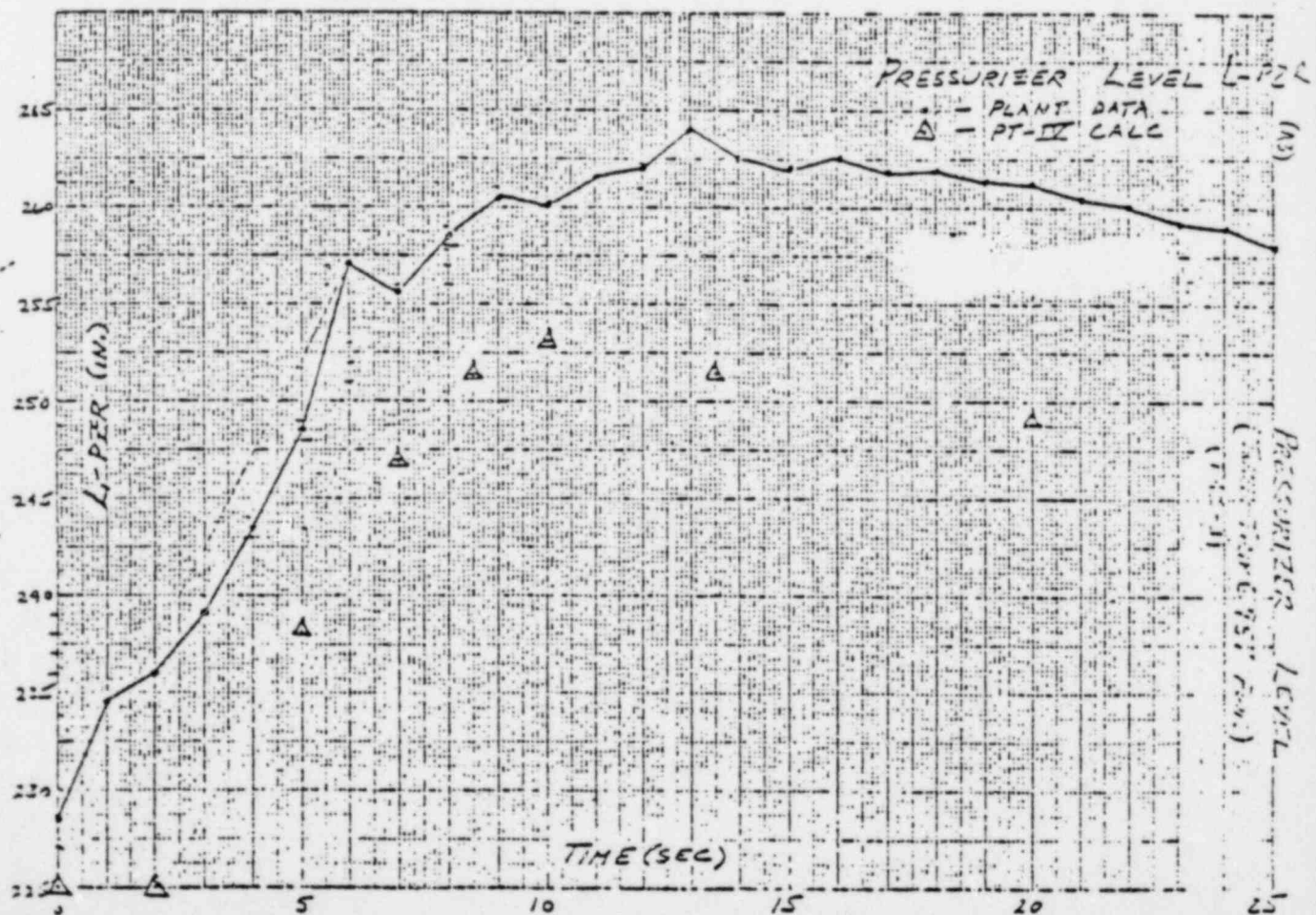
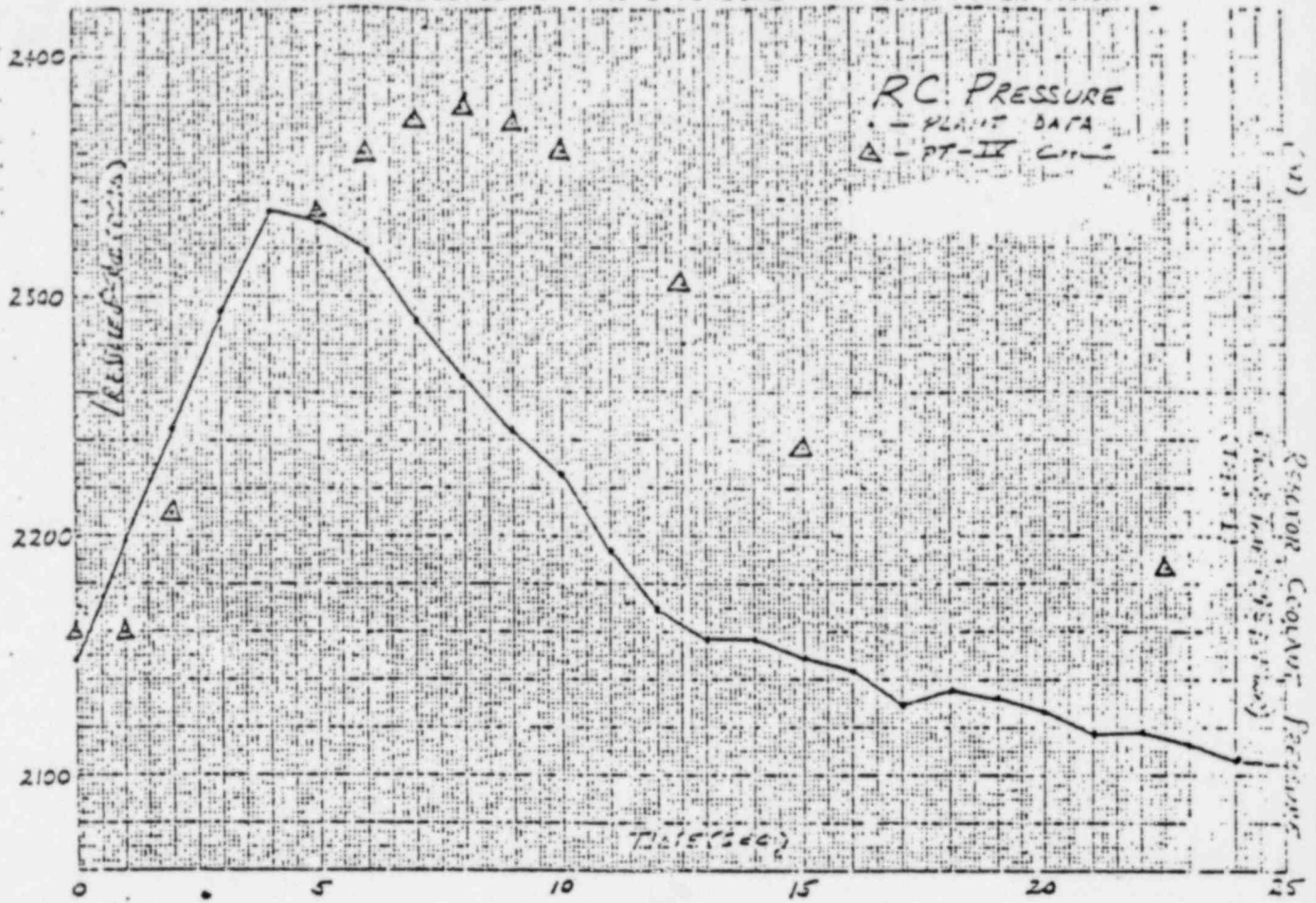


FIGURE 3-PREDICTION OF OCONEE FEEDWATER LOSS WITH POWER TRAIN

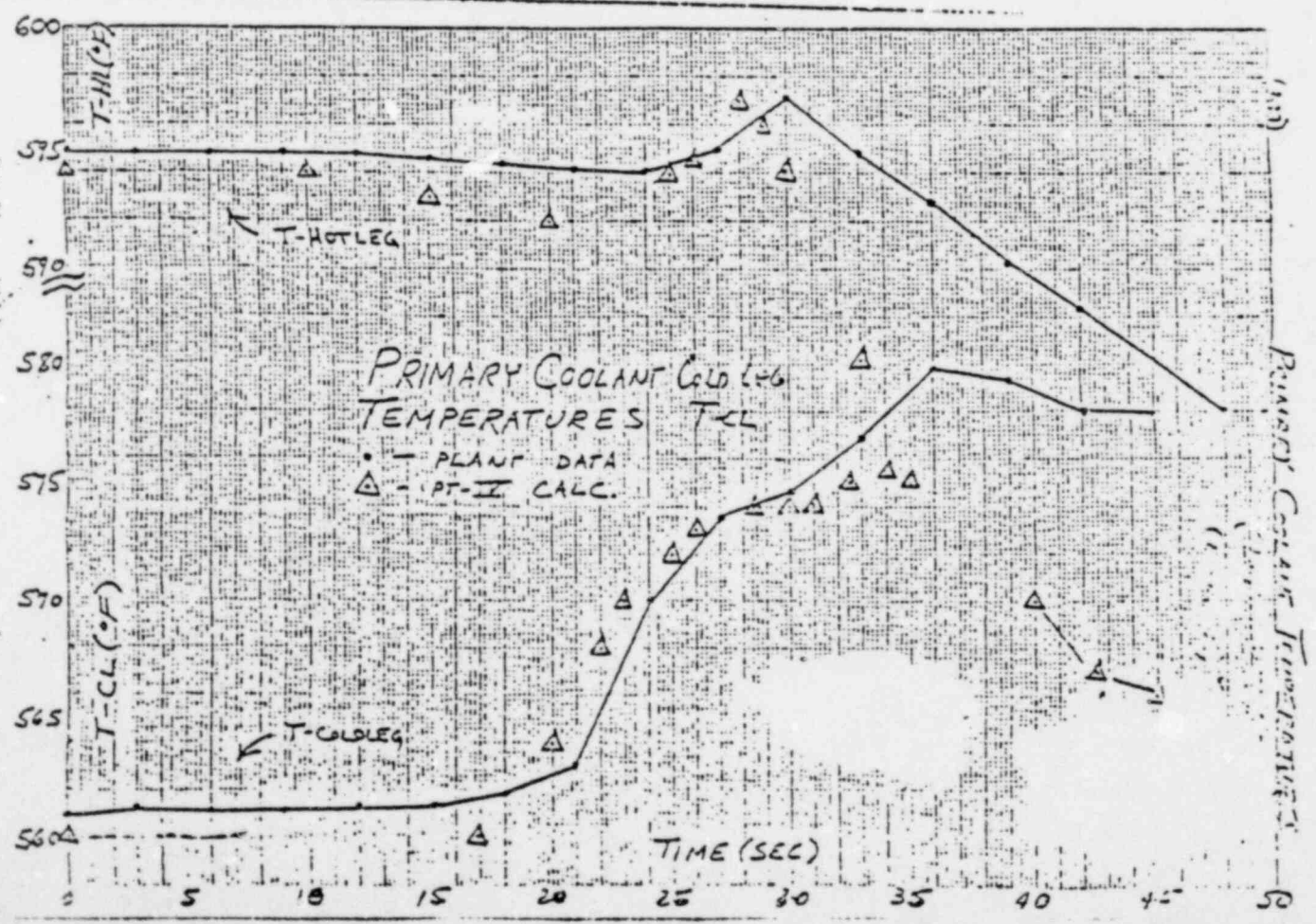
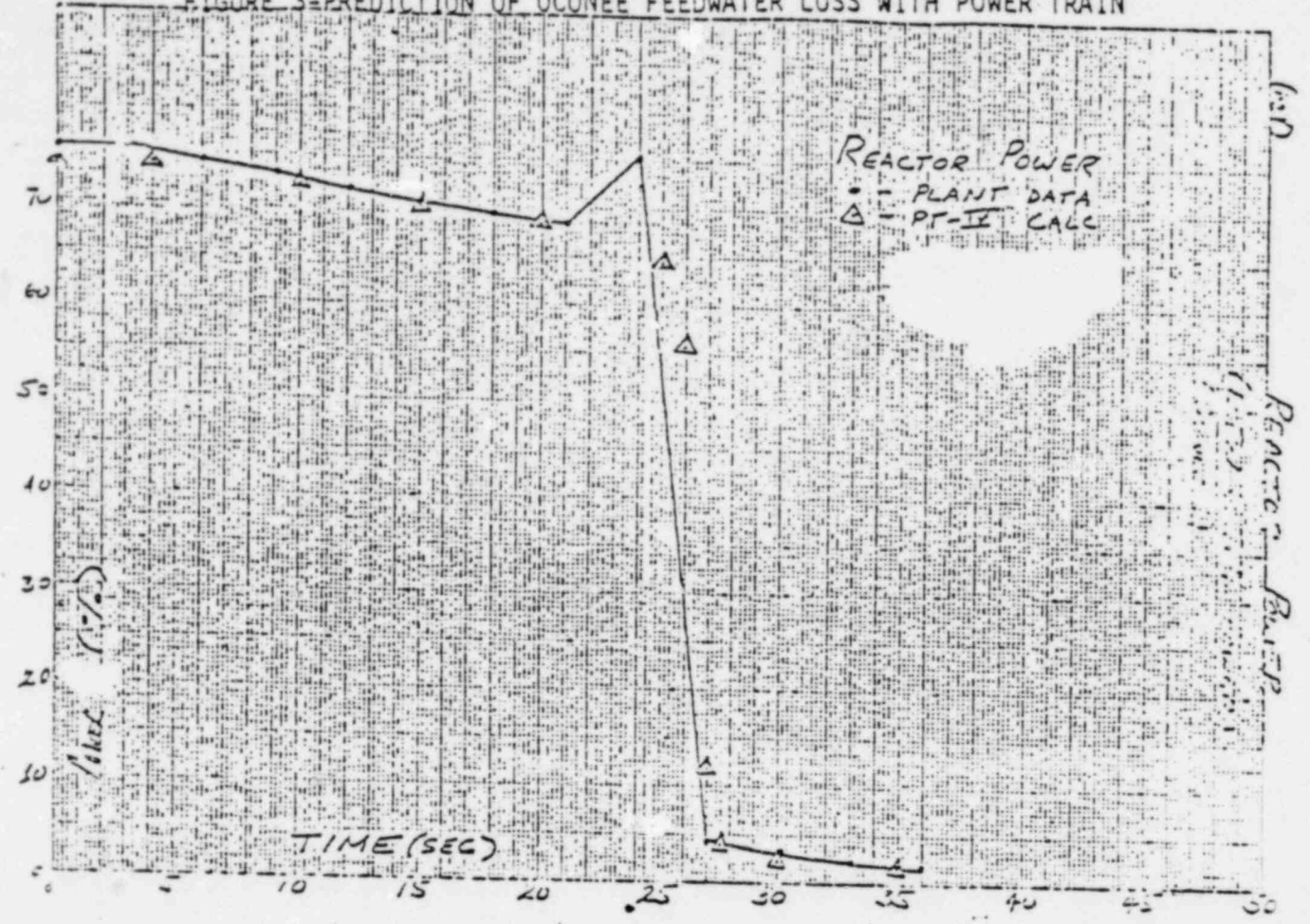
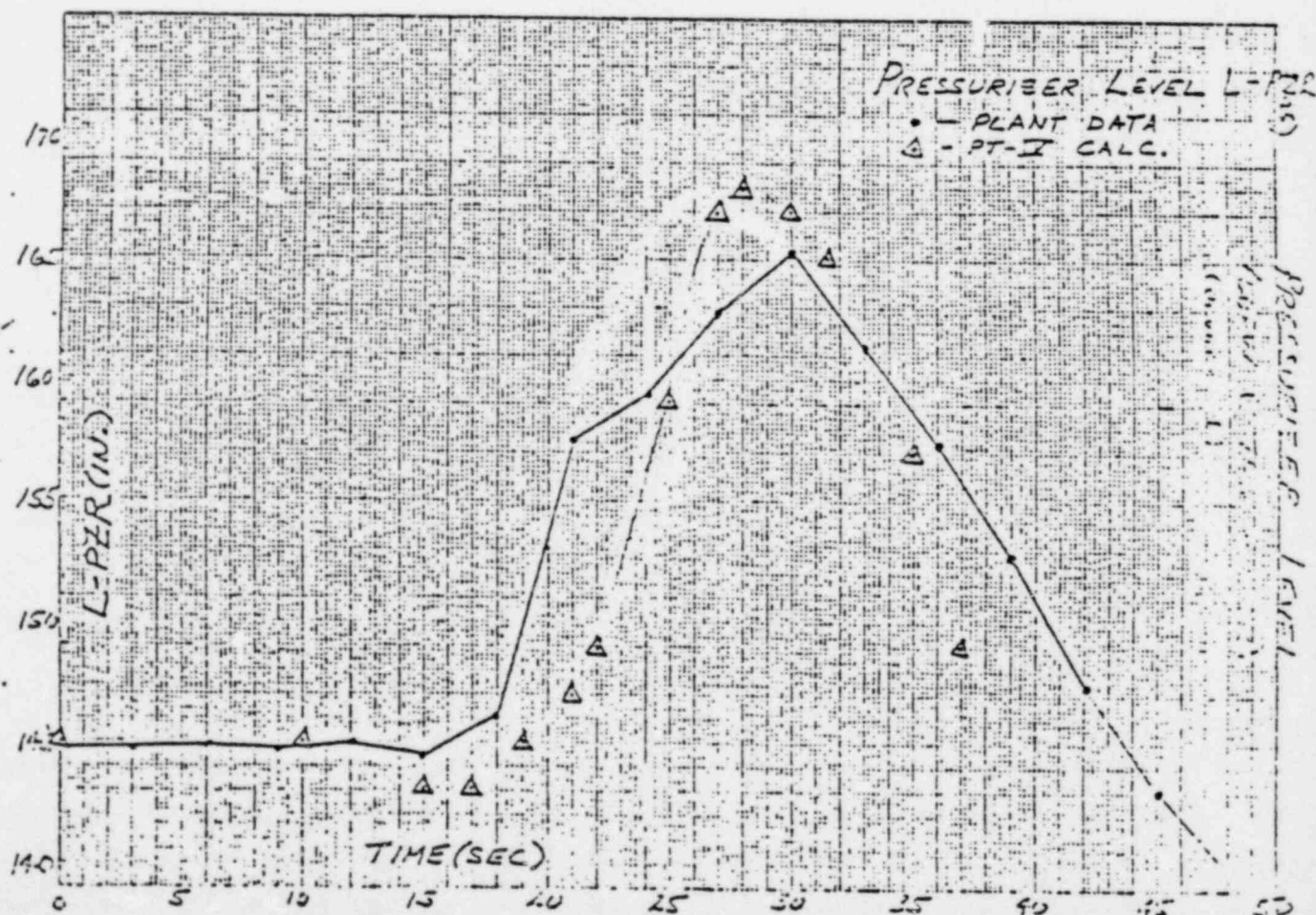
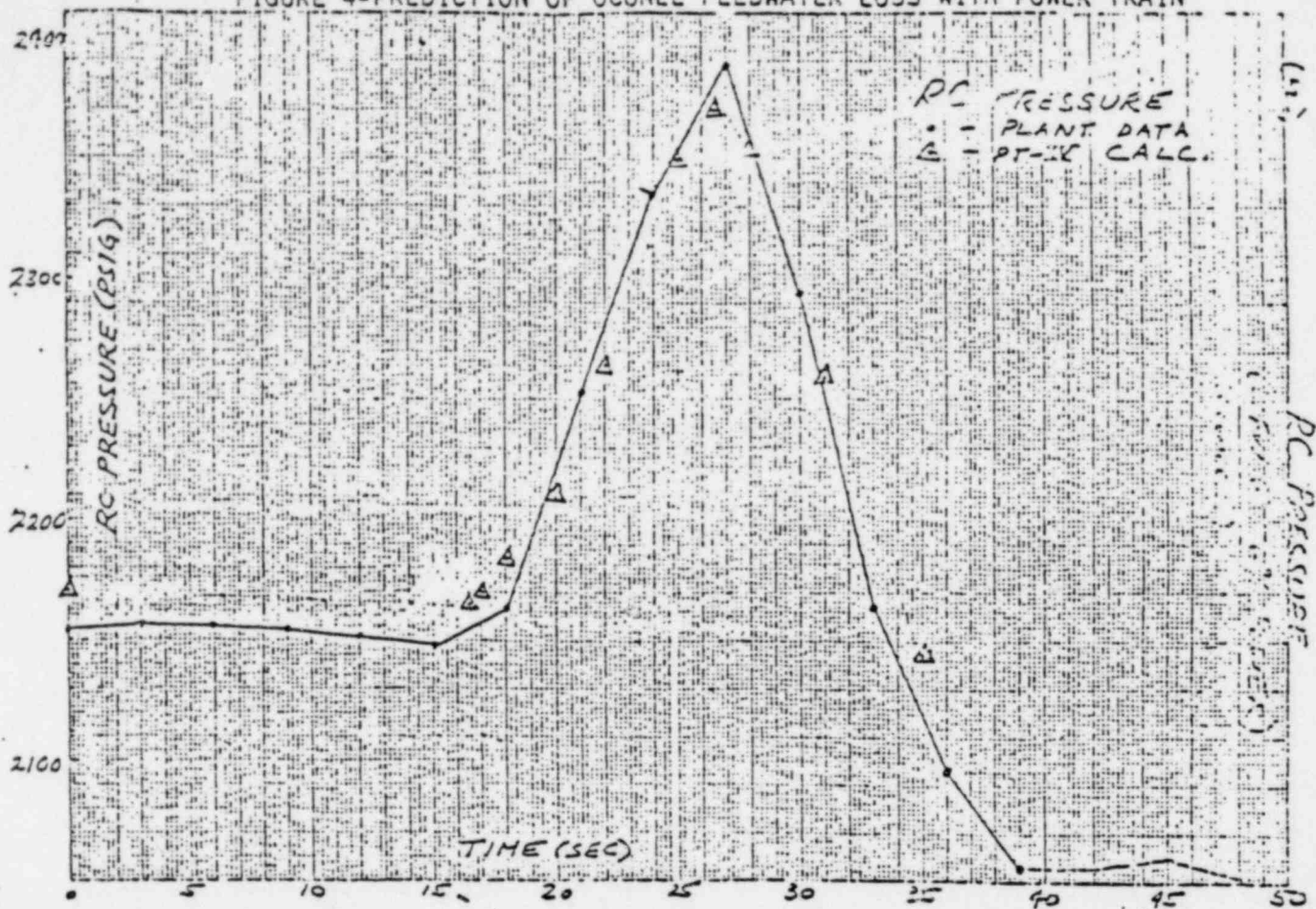


FIGURE 4-PREDICTION OF OCONEE FEEDWATER LOSS WITH POWER TRAIN



Reactor Power % Full Power

50

70

50

50

30

30

20

10

0

-10

Time After Trip of Feedwater Pumps, seconds

CADDS

$$\alpha_m = 1.52 \times 10^{-4} \frac{\Delta K}{\Delta T}$$

O'Connell - Reactor Data

CADDS

$$\alpha_m = 0.66 \times 10^{-4} \frac{\Delta K}{\Delta T}$$

AD = TIME TO "0" (100% "0")

FIGURE 5-PREDICTION OF O'CONNOR FEEDWATER LOSS WITH CADDS

exceeds the measured value, probably due to overpredicting the cold leg temperature by almost 5°F.

3. POWER TRAIN and CADDs can describe the early stages of the TMI-2 accident. Results are given in NUREG-0560 which show that CADDs does a satisfactory job up to 360 seconds when the reactor coolant reaches saturation temperature. Beyond this point, one must employ LOCA models which, unfortunately, do not have adequate representation of the reactor control system, the steam generators, or the balance of the reactor plant. As inferred from Table 1 and 2, no tool exists in the industry to describe the entire TMI-2 sequence of events. This, in part, explains why several months after the accident a complete prediction of what happened at TMI-2 is not available. Another reason is that all necessary information to perform the prediction was not measured or recorded.
4. Many of the transient studies are terminated early, and in so doing do not examine other abnormal conditions that might develop in the course of bringing the plant to cold shutdown, especially conditions brought about through the action of the operator.
5. The comparisons presented in Figures 1 to 5 show the importance of recording information during plant operation. Such data logging gives special opportunities to check analytical models and correct possible discrepancies.

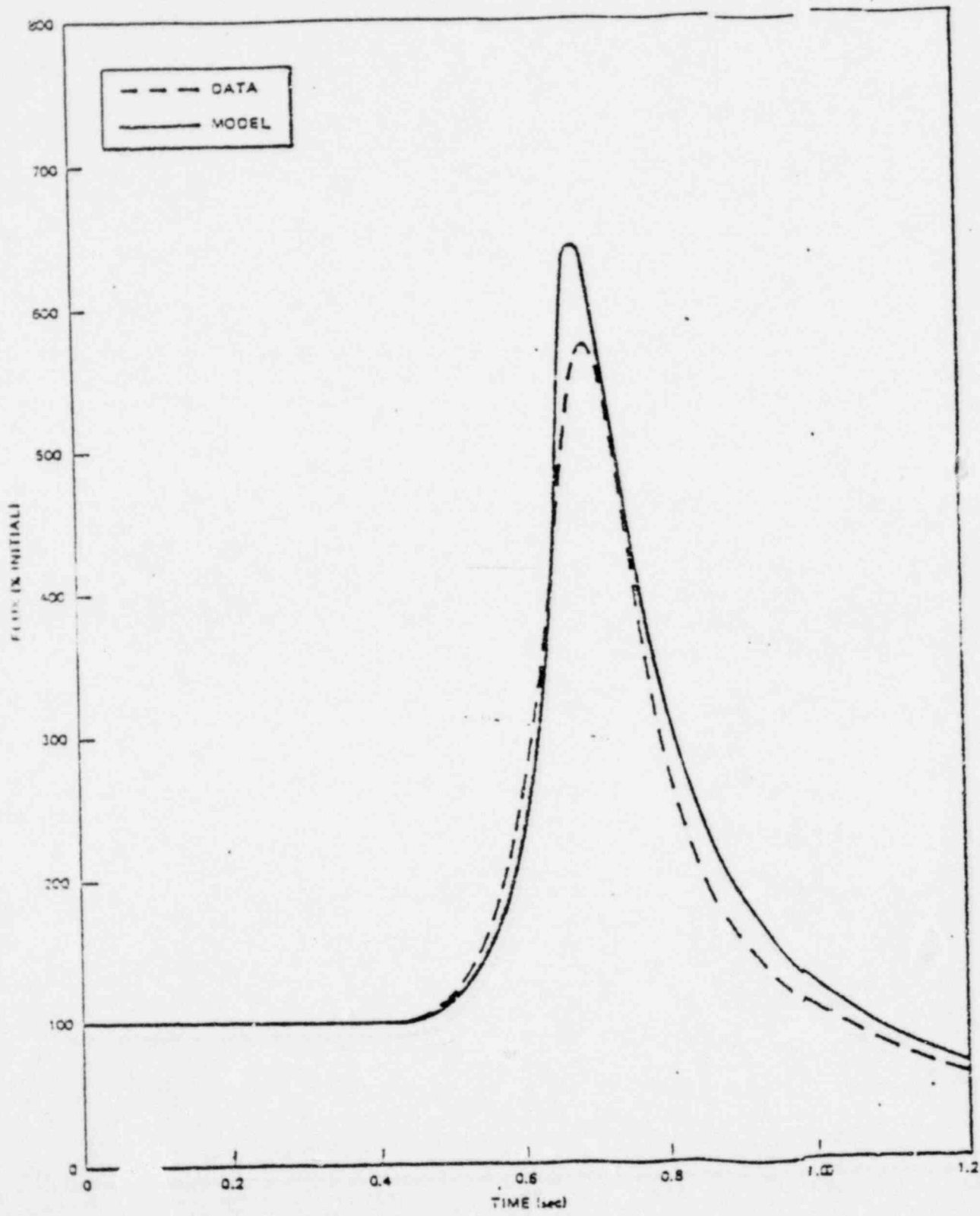


FIGURE 6-PREDICTION OF PEACH BOTTOM-2 D LEVEL FLUX TURBINE TRIP 3

6. Many of the start-up tests are not severe enough to test the analytical models. The capability to perform more severe tests is essential to verifying the models. For example, in-reactor tests at higher pressure rates than during anticipated transients were performed at Peach Bottom in 1977, and they led to substantial improvements in transient modeling*. Figure 6 shows the results predicted by the improved model. One of key changes introduced in the model whose predictions are shown in Figure 6, was to replace the simplified point kinetics core model by a one-dimensional reactor kinetics model.

7. Besides training simulators, POWER TRAIN and equivalent tools offer the only other real time man-in-loop capability presently available in the nuclear industry.

2 3.3 Recommendations

1. Expansion of transient models to include two-phase flow modeling and other such essentials in order to allow these models to simulate small breaks, natural circulation and natural circulation breakdown is recommended to better understand system failures and effects and to study man-in-loop intervention and inappropriate operator actions. Also, all transient calculations should be carried out to cold plant shutdown.

* General Electric Report, NEDO 24154, October 1978

2. A systematic program of well instrumented severe operational transient tests at power plants is recommended. Means must be devised to perform such tests gradually at more severe conditions than anticipated during plant operation in order to give the available models a more stringent verification than accomplished to-date. NRC and the nuclear industry must find a way to encourage such tests. Continuous monitoring of key variables at all plants (see Section 6.0) to simply record the actual plant transients which randomly occur may be the most practical way of accomplishing this task.

3. Rapid modification of such tools as POWER TRAIN or CADDs, under recommendation (1) above may give the industry the earliest way to simulate fault tree events and to develop operating guidelines and malfunction procedures. This is a preferable course of action to employing training simulators in those cases where the training simulator models are very inferior to those included in POWER TRAIN, CADDs, or equivalent codes.

2.4 Accident Analyses

2.4.1 Background

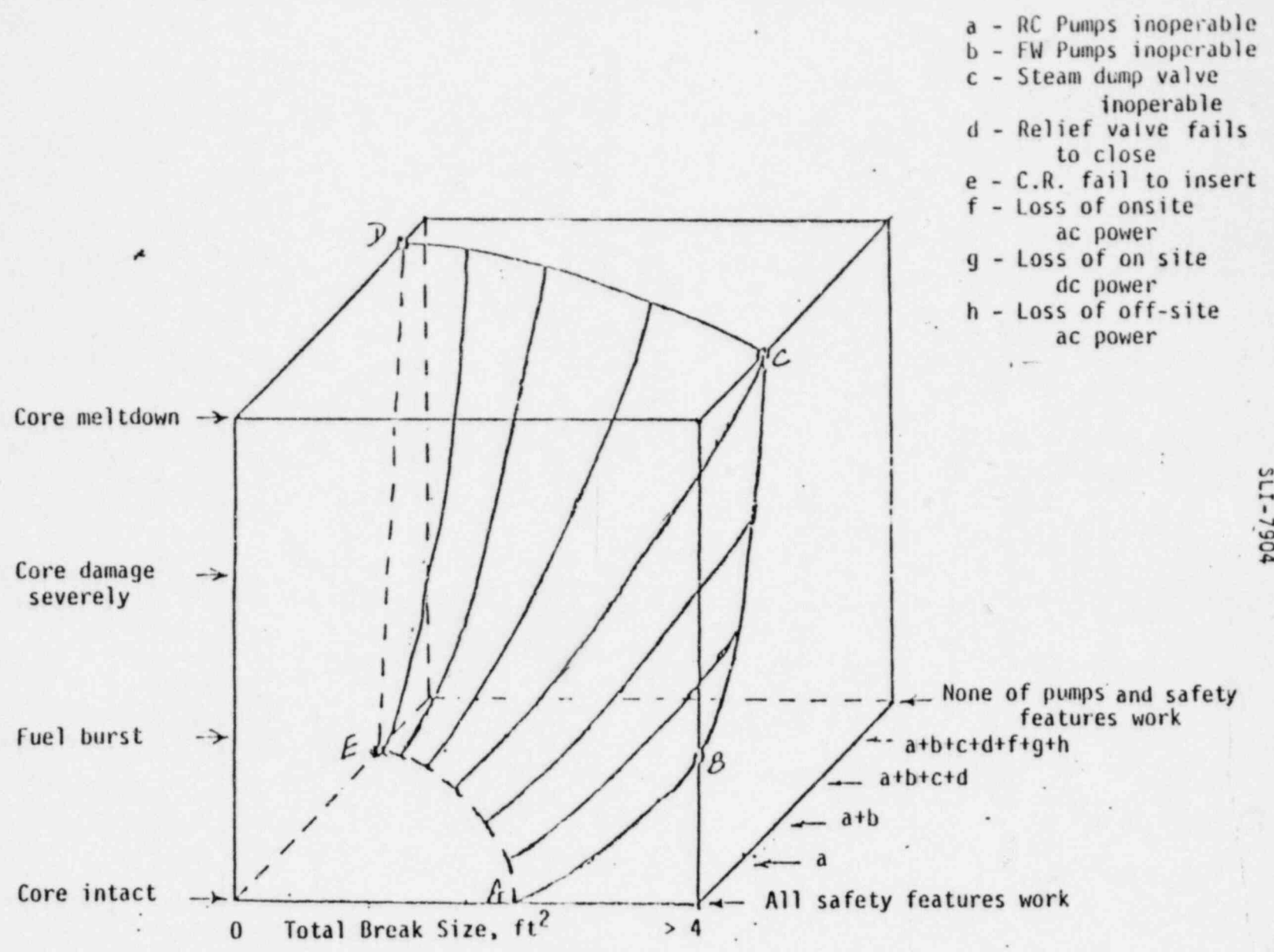
There are many accident analyses performed in the course of safety evaluations and preparations of safety analysis reports for submittal to the NRC. The number of models is also rather large. Some of these accidents are listed in Table 3 and focus will be placed here on those events

which lead to loss of water inventory from the primary system. Such accidents are analyzed at B&W by employing the TRAP and CRAFT codes. Similar codes exist in the BWR/PWR industry and their names are LAMB, CHASTE, SCAT, CHASE, REFLOOD, RELAP 3B, RETRAN, MARVEL, TRANFLO, RELAP 4, RELAP 5, CEFLASH, SATAN, TRAC,, just to mention a few. While the discussion will center upon TRAP and CRAFT, the comments are applicable generally to other codes and they tend to represent the status for other accident models besides those utilized to deal with loss of primary water inventory.

The CRAFT-TRAP codes are integral system models which are capable of simulating various steam-water systems and loops. They provide submodels to simulate such specific system components as reactor core, coolant circulation pumps, emergency coolant systems, steam generators. They are based upon transient and simultaneous solutions of the mass, momentum, and energy equations and provide for considerable flexibility in terms of spatial discretization. The codes also provide for the simulation of assorted trips or control action but these are generally limited in number to a selected set.

The codes are applied to a wide spectrum of events and end results. This is illustrated in Figure 7*. On the bottom axis, the break size through which primary system water is being lost is varied from zero to several square feet. On the axis into the paper, several malfunctions are postulated. On the vertical axis, the end conditions of the reactor core are shown, ranging from intact fuel, to a few fuel rod failures, to fuel burst, to

* Furnished by NRC Research



SLI-7904

FIGURE 7 - TYPICAL EQUIPMENT MALFUNCTION SET FOR LOCA EVALUATIONS

severely damaged core, to core meltdown. The surface A B C D E corresponds to the output from TRAP/CRAFT codes for the specific malfunctions shown. It is apparent that with different malfunctions or combinations thereof one could generate different surfaces A B C D E. It should be recognized from those malfunctions listed in Figure 7, that Figure 7 does not include the operator-plant interactions or possible operator errors. Such operator actions would generate several other sets of surfaces A B C D E. The objectives of the extensive safety studies performed in the licensing process is to define the worst surface A B C D E and to show that it satisfies the requirements of Title 10, Code of Federal Regulations, Part 50 (10 CFR 50), Appendix K.

The Appendix K, 10 CFR 50, specifies many of the details of the LOCA analyses. It not only specifies initial conditions, rates of power generation, and certain model features, but it also identifies the peak fuel clad temperature not to be exceeded and the malfunction characteristics to be employed. Generally, the LOCA analyses are performed for a specific set of break sizes with the plant at 102 percent of power and with the assumptions of reactor trip, no off-site power and one single failure such as one complete train of the emergency water cooling system not being available. Based upon a multitude of evaluations, it was judged that the prescribed set of conditions would generate the worst surface A B C D E in Figure 7. A typical set of such small break calculations performed by B&W is given in Figures 8, 9, and 10 where the pressure, core mixture height, and peak fuel temperatures are plotted versus time. As long as the active core is

PRESSURE

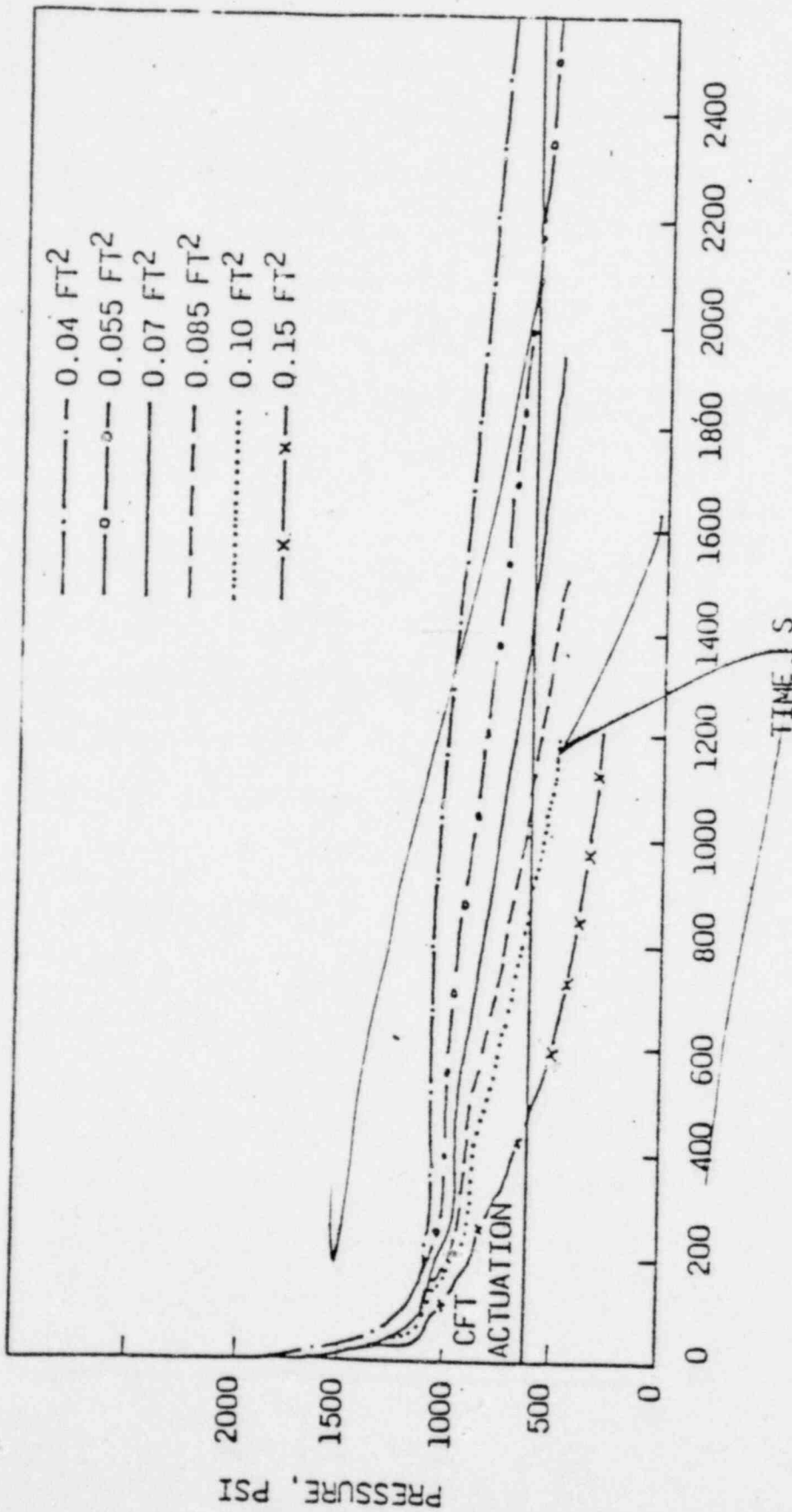


FIGURE 8 - B&W LOCA ANALYSIS OF PRESSURE FOR SMALL BREAK

CORE MIXTURE HEIGHT

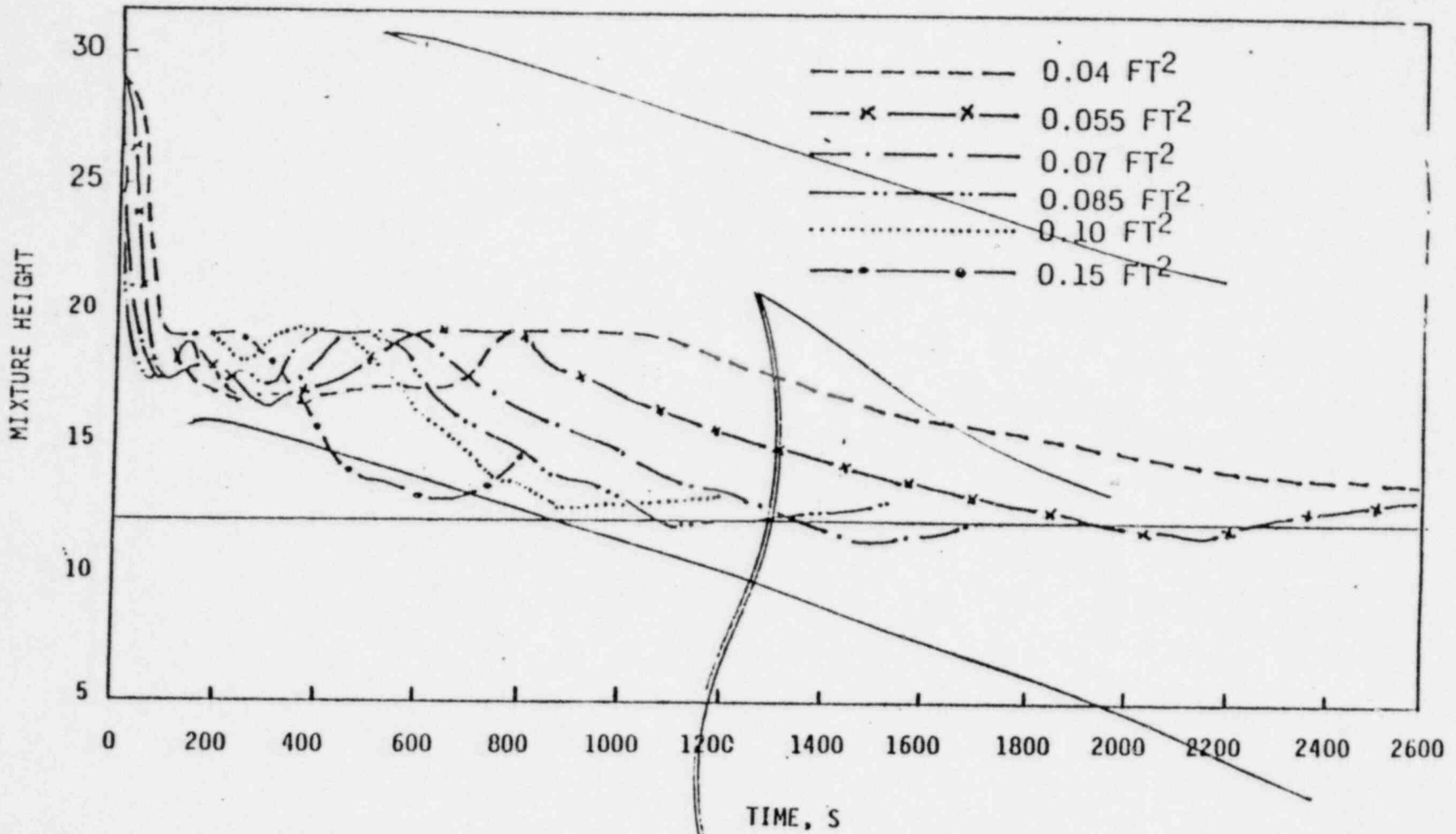
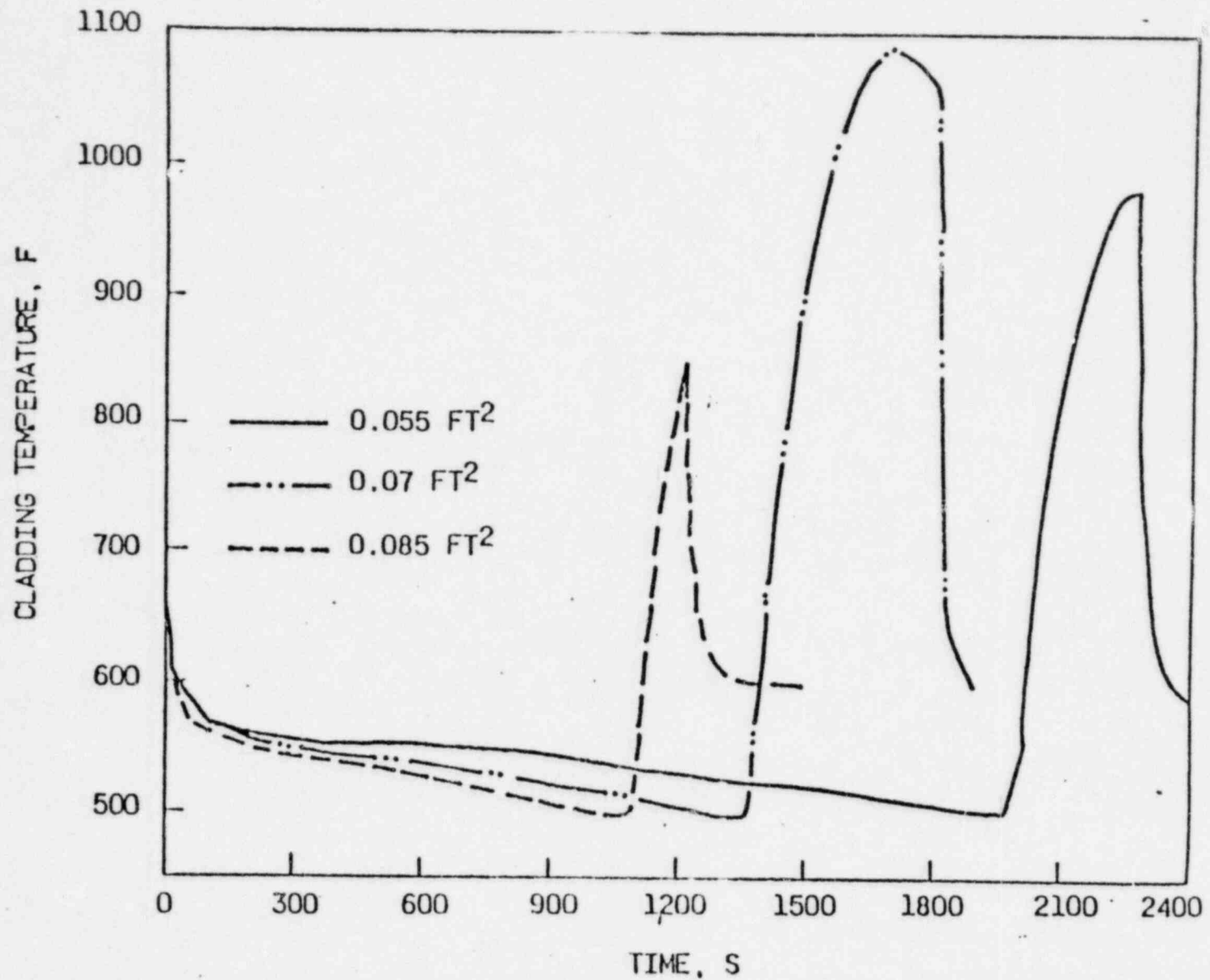


FIGURE 9 - B&W LOCA ANALYSIS OF CORE MIXTURE HEIGHT FOR SMALL BREAK

35

SLI-7904

CLADDING TEMPERATURE VS. TIME



36

SLI-7904

FIGURE 10-B&W ANALYSIS OF FUEL CLADDING TEMPERATURE FOR SMALL BREAK

~~As shown in Figure 9,~~ the resultant peak fuel temperatures will fall below the peak value of Appendix K and will tend to be not too much above saturation coolant temperature. Similar calculations are performed for a range of medium to large breaks up to and including a double ended break of the largest pipe connected to the reactor pressure vessel.

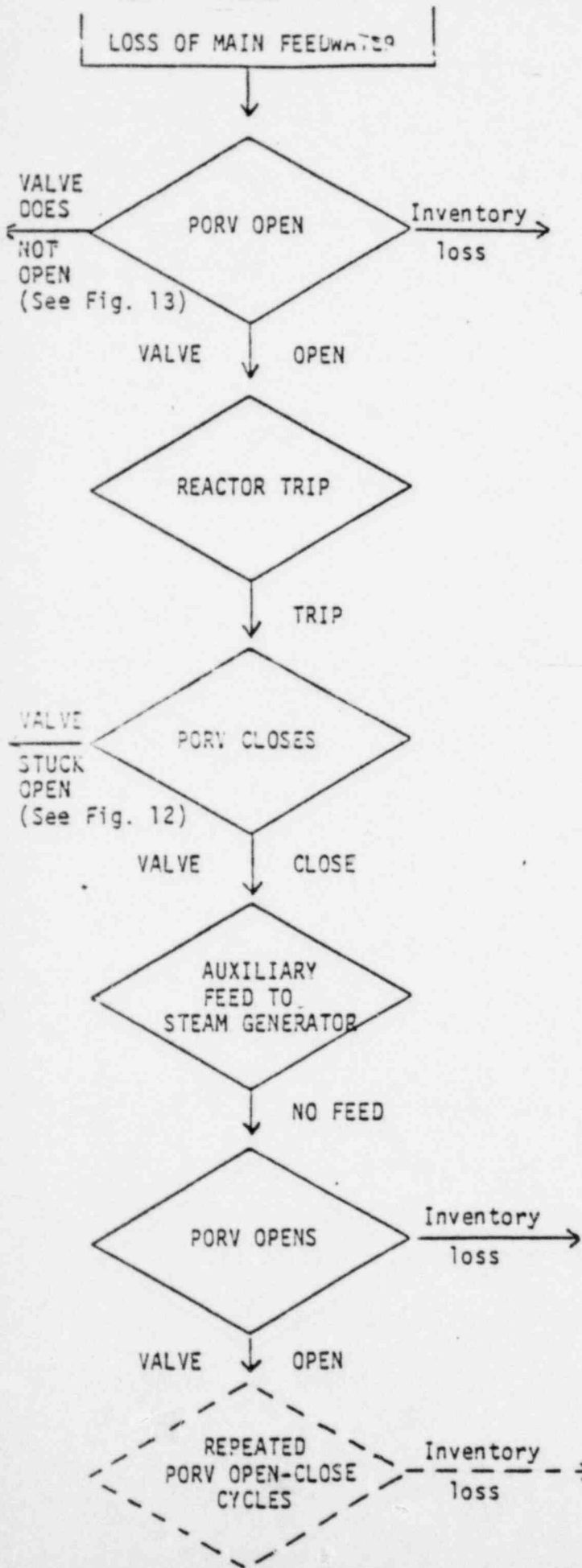
Analyses of loss of inventory from the primary system can be subdivided into three groups. For a PWR, the three groups are (1) the pressure prevailing in the reactor during the accident is above High Pressure Injection (HPI) actuation point and the steam generators provide the primary means of decay heat removal; (2) intermediate pressure after the early stages of the accident and either the High Pressure Injection or steam generators can remove decay heat; (3) low pressure shortly after the accident and the low pressure emergency and shutdown systems as well as HPI can remove decay heat. These three possibilities are illustrated in Figures 11, 12 and 13 for the original TMI-2 design with a loss of feedwater being the initiating event. After the small and medium break in Figures 11 and 12, other event paths could be developed to reach less severe end conditions than those illustrated and they were left out of the Figures.

The calculation methods tend to be more complex as one goes from Figure 11 to Figure 12 and 13 because the rate of change of such parameters as pressure, local flow conditions accelerate from Figure 11 to 12 to 13. For very large breaks, events take place very rapidly and the opportunity for operator actions decreases sharply so that the sequence of events is

EVENT

SLI-7904

DESCRIPTION



- Event is initiated with loss of feedwater to steam generators.

- Loss of feedwater degrades heat sink capacity of steam generators and primary system pressure rises. At 2255 psig the power operated relief valve (PORV) opens.

- Primary system pressure continues to rise with PORV open until it reaches 2355 psig where the reactor is scrammed.

- Once the reactor power is reduced to decay heat level, the PORV depressurizes the primary system down to its close set-point at 2205 psig.

- After start-up delay, the auxiliary feedwater system comes on, but fails.

- Without auxiliary feed, remaining heat capacity in steam generators is boiled away and primary system repressurizes due to decay heat. At 2250 psig, PORV reopens.

- With no feed, PORV will cycle open and closed as decay heat pressurizes primary system between each valve actuation. Inventory loss continues until steam generator heat sink can be re-established or primary system pressure can be reduced to allow HPI to deliver water.

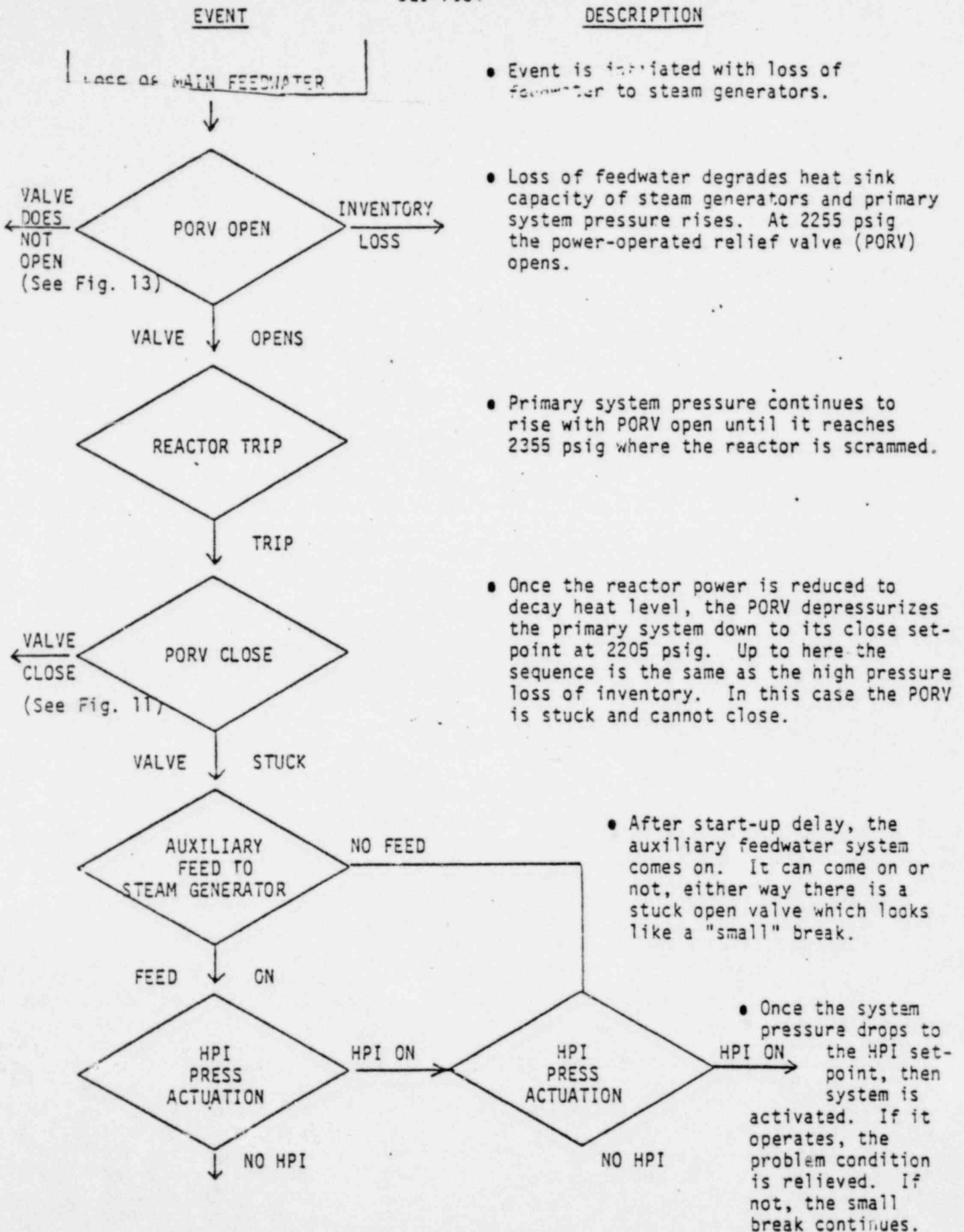


FIGURE 12 - INTERMEDIATE PRESSURE LOSS OF INVENTORY

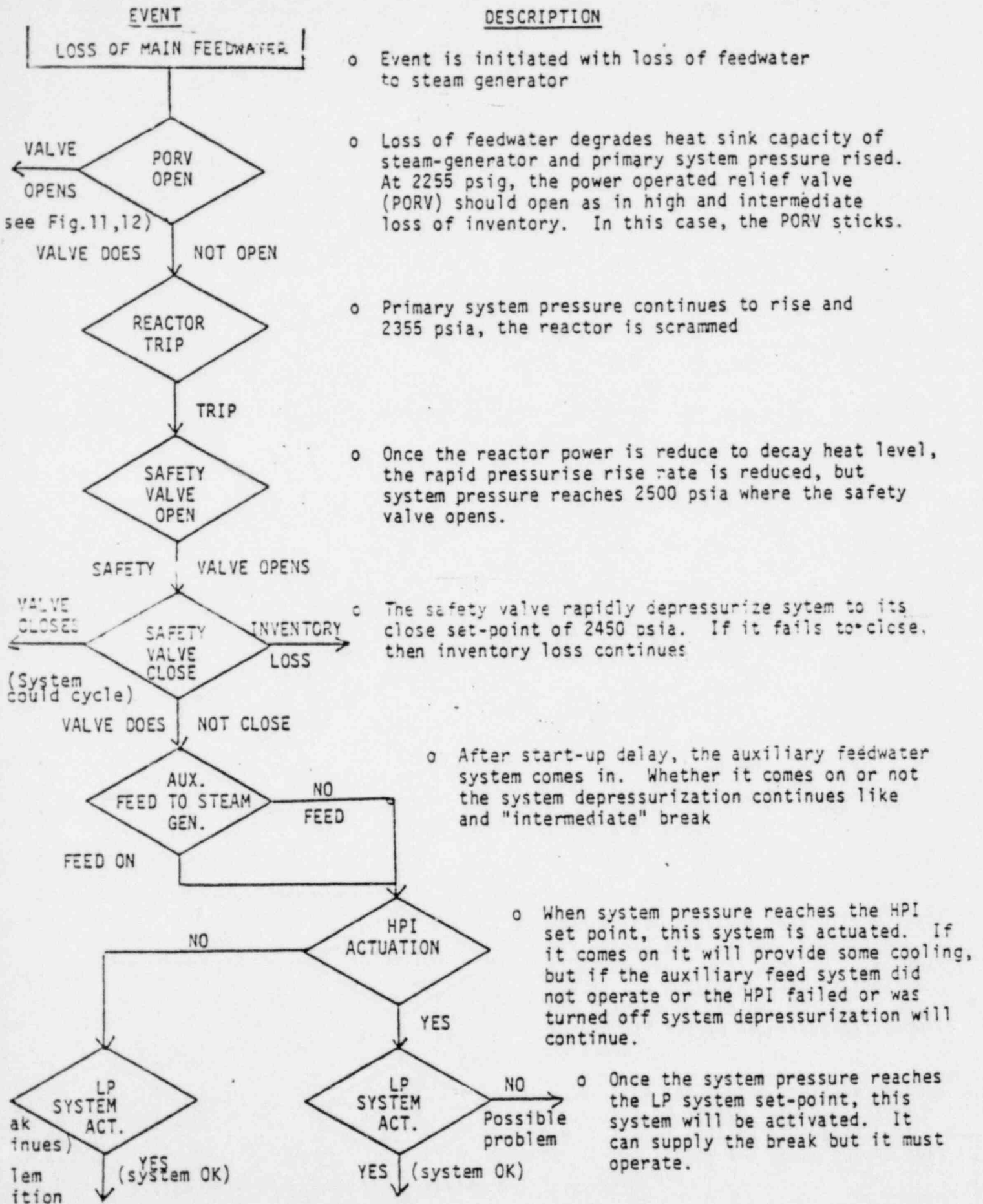


FIGURE 13 - LOW PRESSURE LOSS OF INVENTORY

entirely automatic. Because of the interest in the early phases of such blowdowns, the analysis includes the effect of sonic waves. These calculations are carried out over very small time steps and often take many hours to complete. Many of the important reactor parameters change rapidly in the rapid loss of inventory accident and the models have to be more precise in their representation of the physical processes. During such large breaks, non-equilibrium conditions play an important role. Non-equilibrium refers to both water and steam not being at the same temperature (for example, subcooled water coming in contact with steam) and such non-equilibrium conditions are much more difficult to deal with. For very small breaks, such as shown in Figures 11 or 12, the event takes place over a long period of time, giving the operators a chance to react and intervene. The rate of change in variables with time is smaller and a less precise model can give acceptable answers. Also, non-equilibrium conditions are usually not as important.

In his letter of January 1978, C. Michelson focused upon the small break range of Figure 12 and raised several concerns in his memorandum dealing with "Decay Heat Removal During a Very Small Break LOCA for a B&W 205 Fuel Assembly PWR". Michelson's interest was in the range of small breaks (probably $\leq 0.05 \text{ ft}^2$) where he felt that the reactor pressure would remain high enough so that primary water inventory loss through the break might exceed the HPI water additions. Michelson used the Appendix K postulated conditions of loss of off-site power and unavailability of one train of the HPI. Such a set of circumstances is different from the TMI sequence of events; however, in retrospect, Michelson had the foresight to

identify several problem areas which might have contributed to the severity of the TMI-2 accident. They are:

1. For such a small break, pressurizer level could go up and pressurizer "level indication is not a correct indication of water level relative to the reactor core". A full pressurizer may convince the operator to trip the HPI pump and watch for a subsequent loss of level".
2. "The pressurizer surge line loop seal inhibits steam entry into the pressurizer".
3. "Steam generators must remove a significant portion of the decay heat during the initial phase of blowdown".
4. Due to loss of off-site power, the reactor coolant pumps are not available and heat is transported to the steam generators by natural circulation. Natural circulation may be interrupted by the formation of steam voids within the primary system and a transition takes place from natural circulation to pool boiling in the reactor core and condensing in the steam generator. "The adequacy of this unstable mode (intermittent natural circulation)* for decay heat removal needs to be verified".
5. "Fuel peak clad temperature is the parameter of particular interest for comparison with ECCS acceptance criteria, but stability of the fluid process and adequacy of instrumentation and components should also be considered".

*Added for explanation in this report

Michelson's comments which deal with design and equipment concerns will be discussed in Section 4. In this section, the emphasis will be put upon his modeling and behavior comments. It is worth noting that calculations generated by B&W and submitted to NRC on May 7, 1979* support two of Michelson's points. As shown in Figure 14, pressurizer level would rise with time for a 0.01 ft^2 break at pump discharge. Figure 15 identifies that natural circulation would be lost at about 650 seconds for this same size break. These B&W predictions were performed with their CRAFT code. It is most important to realize that for the ground rules of Appendix K and the assumptions postulated by Michelson, the CRAFT code predicts that the reactor core would remain cool. This fact was presented already in Figure 10 which shows that, indeed, the peak temperature criterion of Appendix K would be satisfied for the entire range of small breaks.**

2.4.2 Findings

1. Calculations of loss of coolant inventory from the primary system are being performed by a prescribed formula. It consists of selecting a spectrum of breaks in the primary system (generally interpreted to be leaks due to material structural failure), loss

*Evaluation of Transient Behavior and Small Reactor Coolant System Breaks in the 177 Fuel Assembly Plant", B&W Report May 7, 1979.

**The broader implications of Michelson's memorandum are covered in Section 4.

PRESSURIZER LEVEL VS. TIME 0.01 FT² BREAK AT
PUMP DISCHARGE - SYMMETRIC AFW

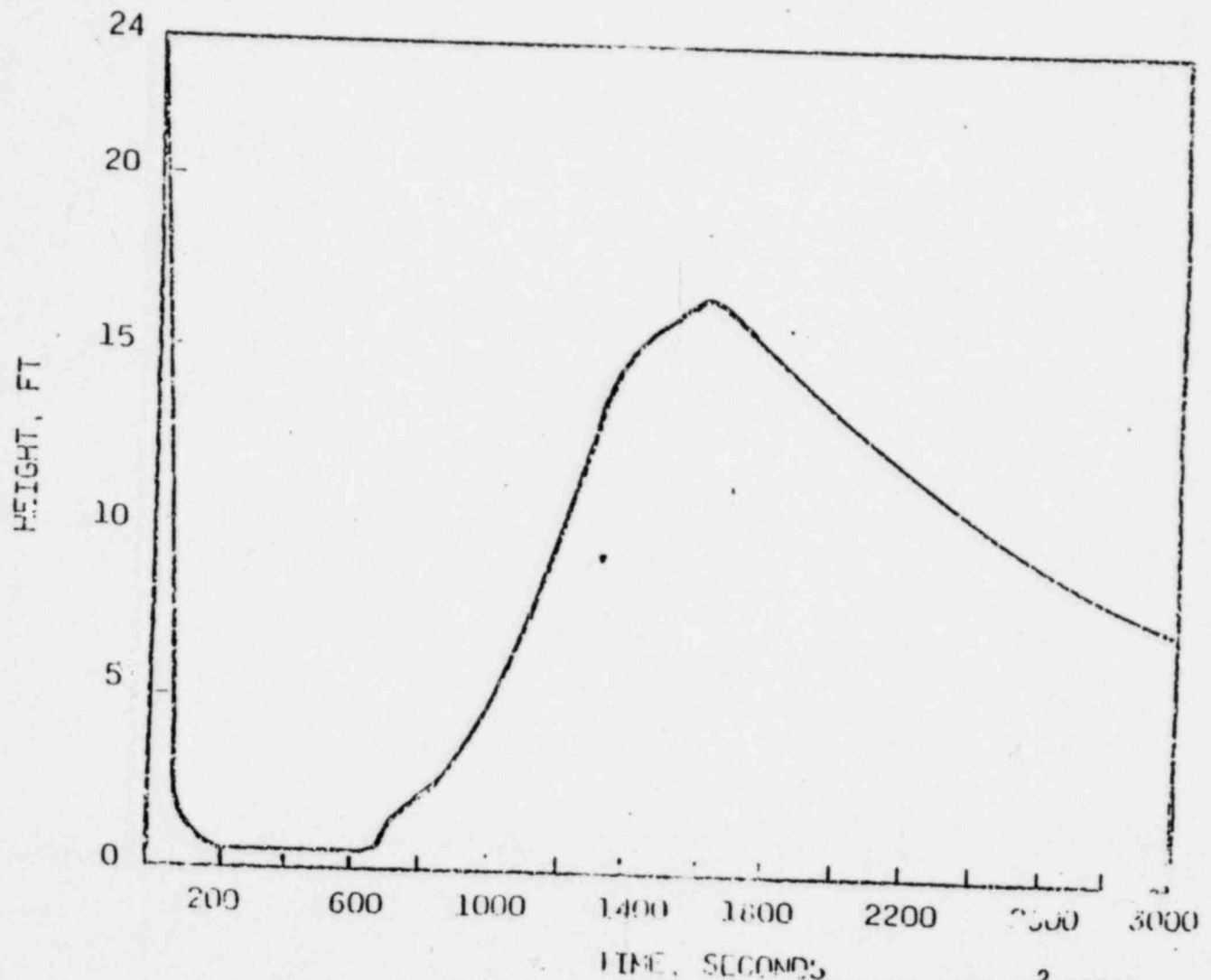


FIGURE 14- PRESSURIZER LEVEL PERFORMANCE FOR 0.01 FT² BREAK

HOT LEG LEVEL VS. TIME-0.01 FT² BREAK AT
PUMP DISCHARGE-SYMMETRIC AFW

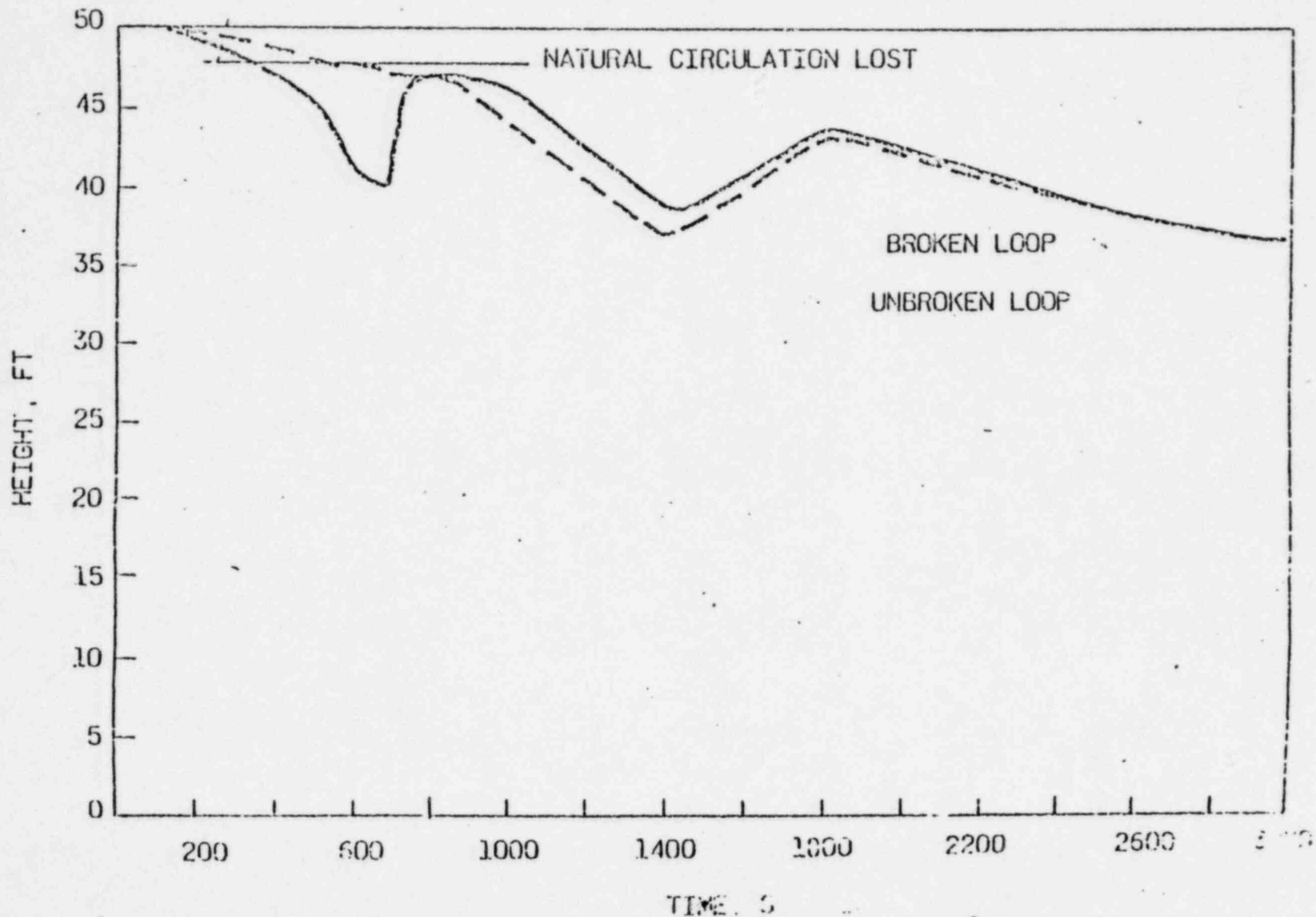


FIGURE 15- NATURAL CIRCULATION BEHAVIOR FOR 0.01 FT² BREAK

45

SLI-7904

of off-site power and a single failure. Under such circumstances, which are judged to be infrequent, peak fuel clad temperature is to be kept below 2200⁰F. As mentioned in subsection 2.4.1, the basic premise in the selected approach was that the prescribed formula would generate the worst surface A B C D E in Figure 7 and that a more frequent set of event combinations would lead to a less degenerated surface A B C D E. This is not the case and this very important finding is discussed at length in Section 4 together with many important recommendations. Let us briefly note here that the sequence of events in the high pressure loss of inventory accident shown in Figure 11 can lead to core uncover and damage for the normal transient of loss of main feedwater coupled with a single failure of the auxiliary feedwater system and no subsequent operator action. Similarly Figure 12 illustrates that a break could be created (by the failing of a relief valve in the open position) as a consequence of the loss of main feedwater. The occurrence of such a "break" could be much more frequent than a break from material structural failure. Also, adverse operator intervention based upon information available to him must be considered and could adversely impact the consequences of the events illustrated in Figure 11 to 13. Finally, failure of off-site power at another time besides the start of the event might have a greater impact. (See section 4 for a gross probability discussion and its implications).

2. The analytical models for accident analyses have been checked in a multitude of separate effects tests and in-reactor tests, (for example, the LOFT and BURST facilities). The models have generally done an acceptable job and the experimental data have been employed where necessary to adjust the models. Comparisons of the models to the NRC standard problem six are given in Figures 16, 17, and 18. Standard problem six was a small break transient performed in the Semi-Scale Test Facility at INEL. Figure 16 shows pressure predictions versus time; Figure 17 plots the mass flow rate escaping from the break; and Figure 18 shows the peak surface temperature. Even though all the calculations are carried out on a best estimate basis, it is observed in Figure 18 that the predictions of peak clad temperature tend to exceed the measured values by varying amounts. Also, it should be pointed out that the differences between the various models may be indicative of the uncertainties that exist in what are complex multi-phase transient calculations. A prediction by CRAFT of the TMI-2 accident up to the point of reactor pump trip is also shown in Figures 19 and 20, and 21. System pressure, temperature and pressurizer level results for the CRAFT simulation are seen to be in good agreement with TMI accident information.
3. The analytical models contain several simplifying assumptions. With the exception of a very limited number of codes such as TRAC, few of the models consider thermal non-equilibrium conditions. In many

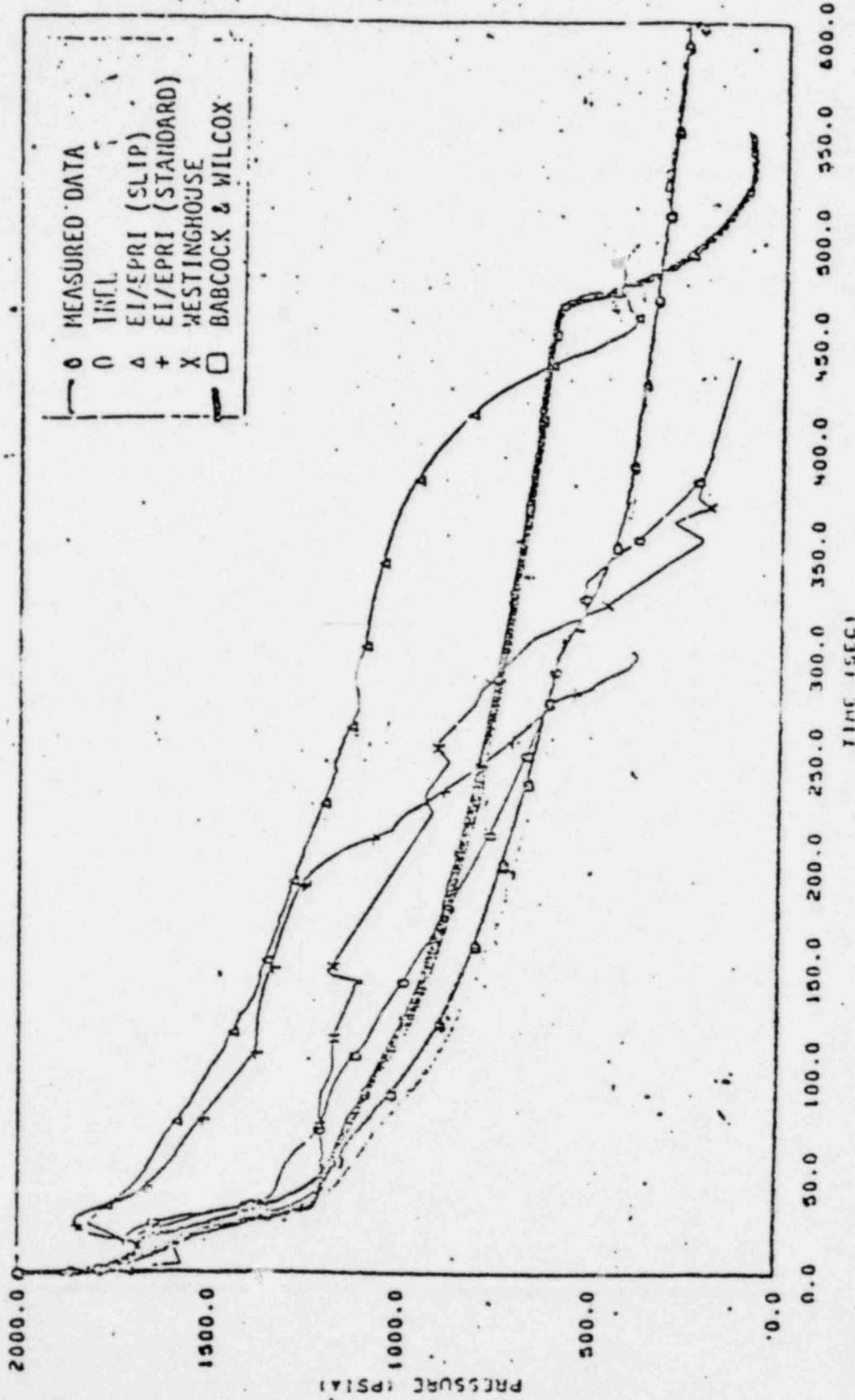
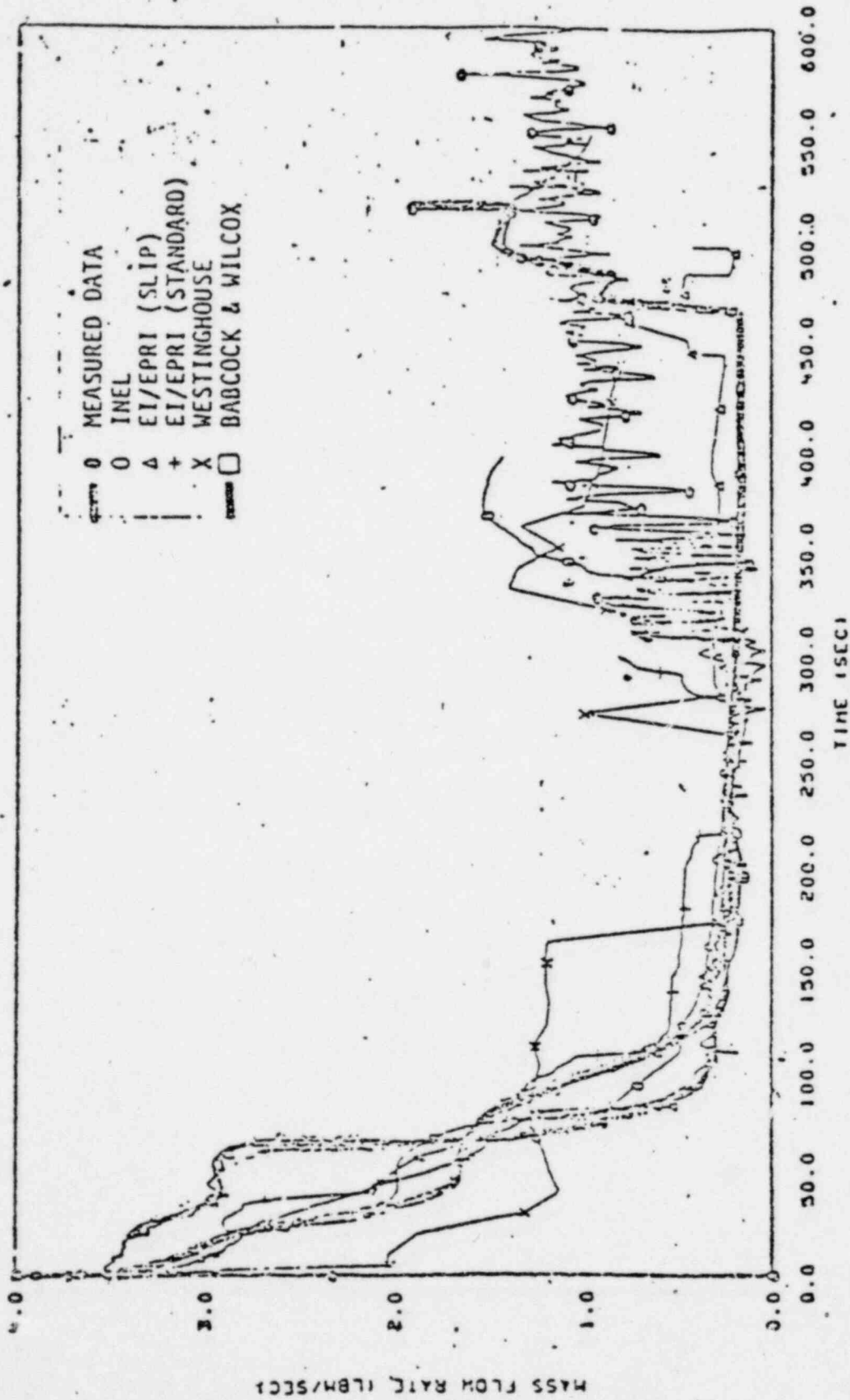


FIGURE 16- VARIOUS PREDICTIONS FOR SMALL BREAK
UPPER PLENUM PRESSURE (PV+10)



MASS FLOW RATE OUT BREAK SIMULATOR (FOO-231)
FIGURE 17- VARIOUS COOLANT ESCAPE RATE PREDICTIONS FOR SMALL BREAK ;

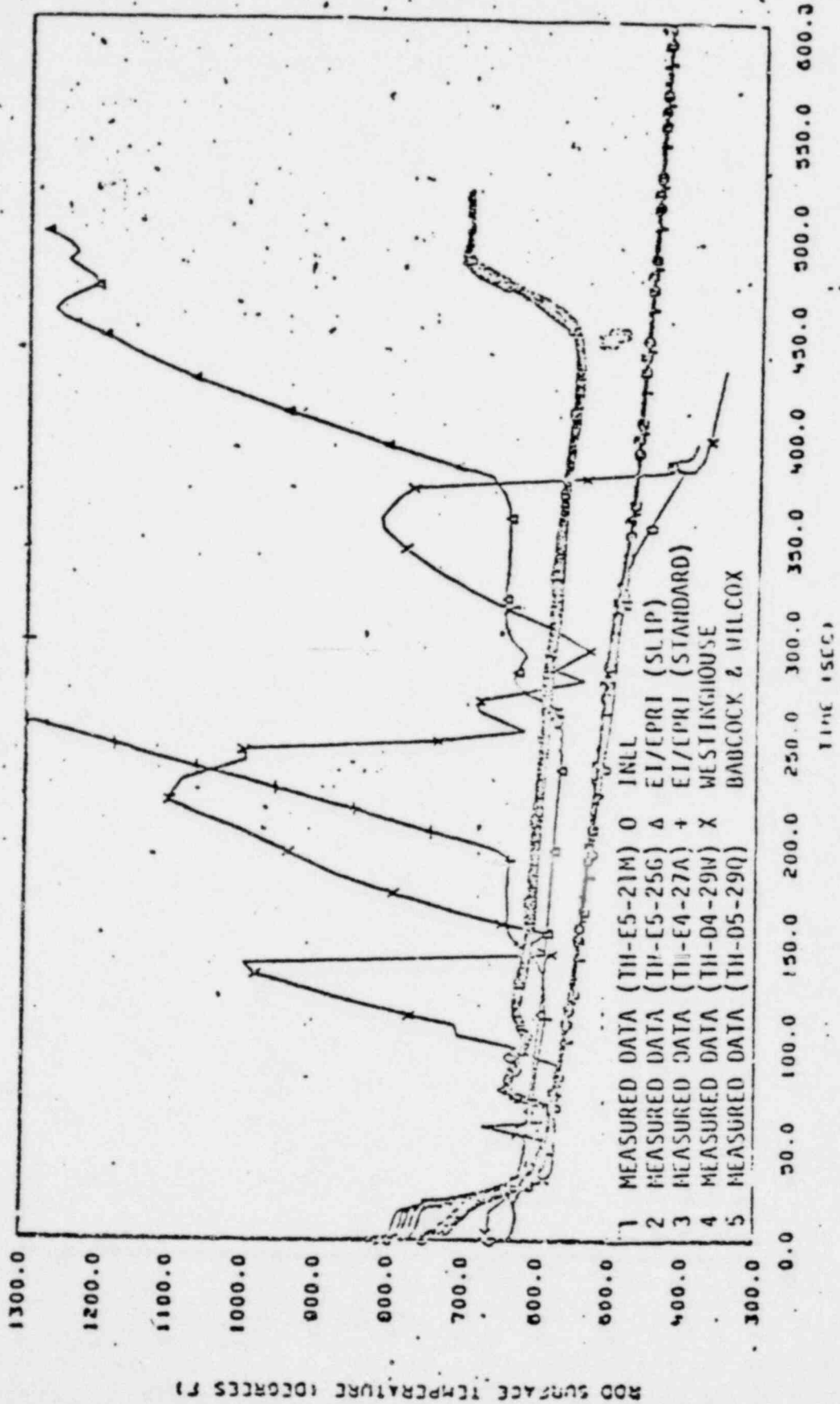


FIGURE 18- VARIOUS CLAD TEMPERATURE PREDICTIONS FOR SMALL BREAK

SYSTEM PRESSURE VS. TIME

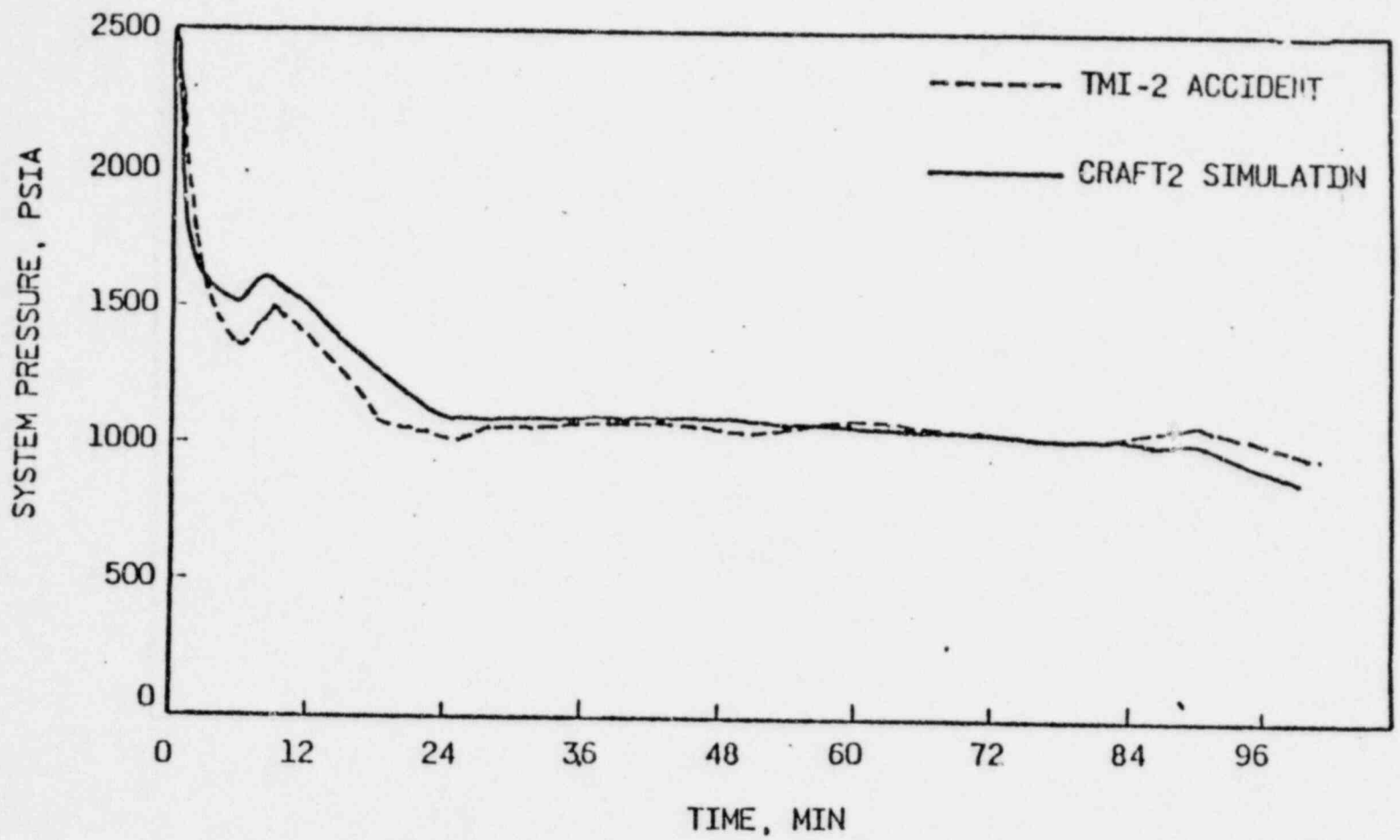


FIGURE 19- PREDICTION OF PRESSURE FOR TMI-2 ACCIDENT

HOT LEG TEMPERATURE

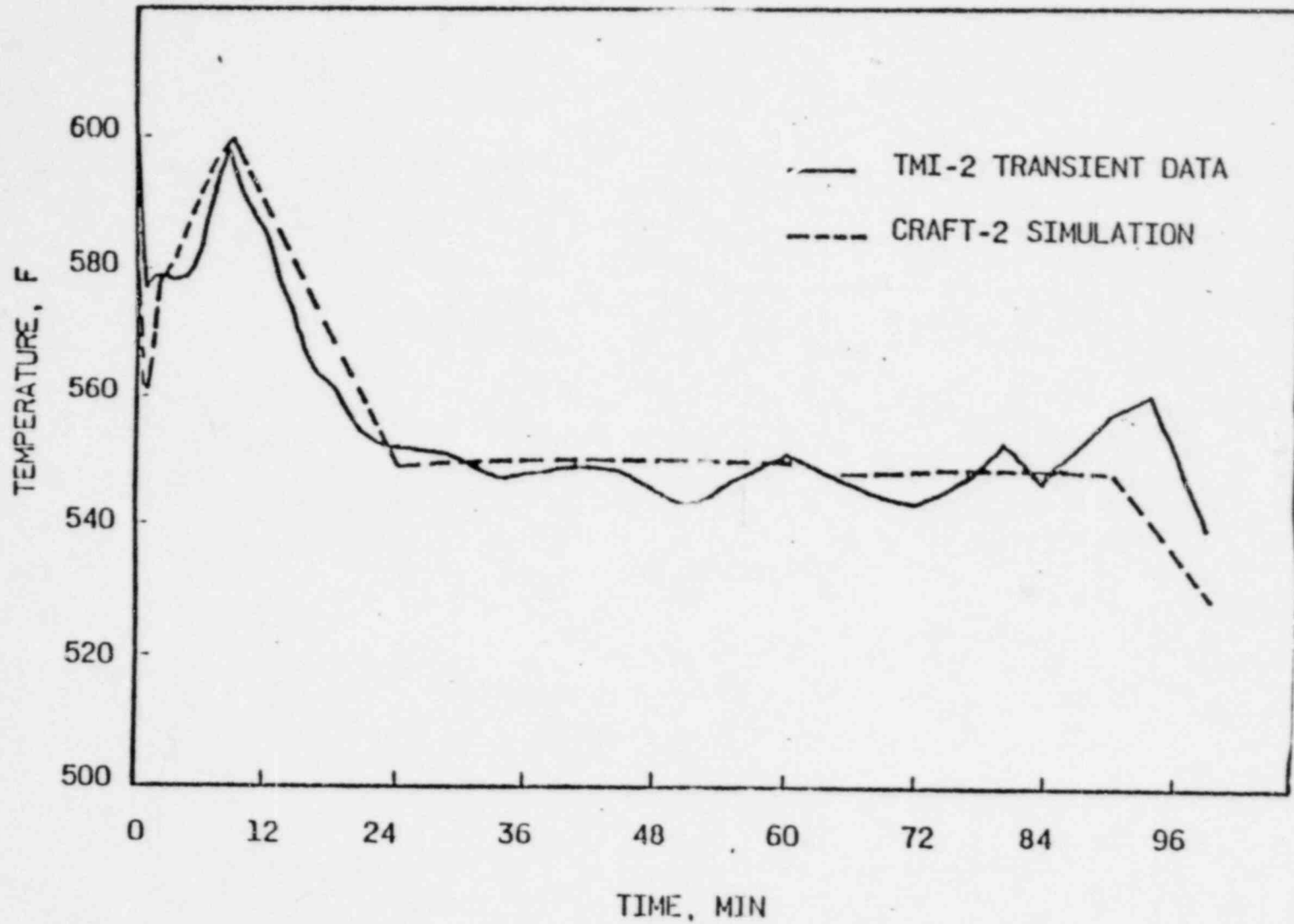
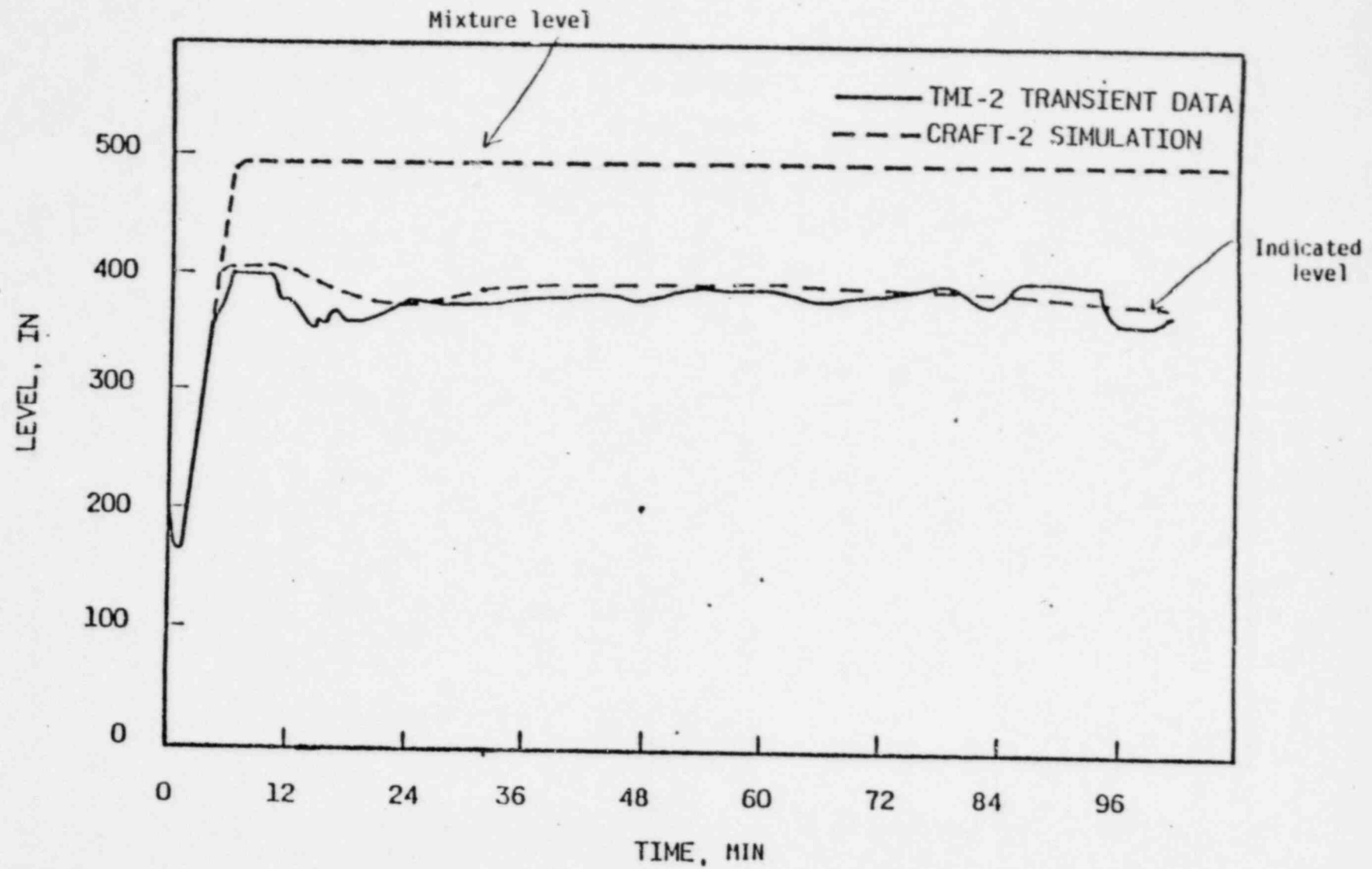


FIGURE 20- PREDICTION OF HOT LEG TEMPERATURE FOR TMI-2 ACCIDENT

52

SLI-7904

PRESSURIZER LEVEL



53

SLI-7904

FIGURE 21- PREDICTION OF PRESSURIZER LEVEL FOR TMI-2 ACCIDENT

SLI-7904

computer codes, one dimensional homogeneous flow with thermal equilibrium is used to represent the recirculation loop. At present, no models deal with non-condensable gases in the primary loop. Finally, many empirical correlations based upon out-of-reactor tests are introduced in the models and for that reason it is believed that accuracy and details may go well beyond those necessary in other segments of the code.* Many elements of the models can and are being improved through efforts sponsored by the NRC, EPRI, and the manufacturers. Table 4, prepared by NRC Research, shows various areas for simulation of the small break LOCA which need to be studied further and the priority assigned to the various areas and corresponding experiments. Table 4 and the preceding comments should not detract from the overall view that the present models are expected to overpredict the accident consequences. In the LOCA case, this results from many conservative aspects of the models which are required by Appendix K.

4. The models do not incorporate detailed control functions and deal with man-machine interactions only in a simplified way. This makes it difficult to readily evaluate all the possible branches in an accident sequence and to assess how operators might react or how their reaction might be improved.

5. Just complying with the peak allowable fuel clad temperature as determining success or failure for LOCA safety evaluations may

*This has been referred by some as "using a laser beam to kill a mouse" in describing some portions of the model.

TABLE 4- LISTING OF POSSIBLE SMALL BREAK EXPERIMENTS

	Semiscale USA	LOFT USA	THTF (BDHT) USA	Flecht- Seaset USA	TLTA USA	PKL FRG	LCBI FRG	CCTF JAPAN	TPTF JAPAN	SCTF JAPAN	ROSA III JAPAN
1) Integral Tests											
a) Free convection 2-phase integral behavior (steady state)	+ 1				S _g ² (BWR)	S _g ¹	+ 2	S _g ²			
b) Reactor Transient (Energy and Mass Transfer)	+ 1	S _n ¹				S _g ¹					
2) Separate Effect Tests											
a) Reflux boiler	S _p ¹					S _p ²		+ 1			
b) Core uncovered heat transfer			+ 1	S _p ¹	S _p ¹						S _p ¹
c) Mixture level (Core, Down-comer)		+ 1				S _g ¹			+ 2		
d) Heat Transfer in SG	S _p ¹					+ 1		S _g ¹			
e) Countercurrent flow in primary horizontal loop pipes									+ 2		
f) Influence of non-condensable gas	+ 1					S _g ¹					
g) flow blockage (core)				+ 1						+ 2	
h) nuclear feedback		+ 1									

- + = first priority (key tests)
 - 1 = early available (before Sept. 1980)
 - 2 = late available, improved instrumentation
 - S = scaling and supporting
 - S_g = scaling with respect to geometry
 - S_p = scaling with respect to pressure
 - S_n = supporting nuclear
-) support tests

overlook other important processes. Michelson referred to the need to consider stability of the fluid process over and above peak clad temperature. This is a valid comment inasmuch as it reflects the ability to accurately calculate the peak temperature. One is concerned with being able to describe all the correct trends in the reactivity, fluid flow and thermal processes in an unstable environment. In order to avoid surprises, correct trends in the controlling processes may be much more important than over-sharpening the value of a single parameter. For example, capability to predict whether natural circulation takes place, when it stops, how it restarts is most important. It should be noted here that models have not been verified in this important area. Similarly, one might have to deal with intermittent condensation or flow instabilities in U-tube and once-through steam generator configurations. In that sense, Michelson's views deserve further evaluation.

6. As noted already, the models are usually conservative even when best estimate results are sought. In the first nuclear power test at LOFT, all best estimate predictions exceeded the reactor measurements. This was due primarily to the models being too conservative in predicting the first fuel rod rewetting during a large LOCA. Another example is that CRAFT still assumes only steam heat transfer during core uncover while, in fact, the presence of water droplets in the steam yield a higher heat transfer rate.

7. The available models take several hours on the fastest computers to carry out the simulation of accidents. As mentioned already, this comes about not only from excessive details in some areas but also from the models trying to generate too many different types of information. For example, to calculate loads on reactor components, very small time steps and very fine special segmentation are needed for the large LOCA. This is not the case for small breaks.

2.4.3 Recommendations

1. Event and malfunction charts such as Figures 11 to 13 need to be developed for reactor transients and accidents. Such charts should consider operator information and operator actions. From such studies could emerge sequences of events which are more frequent or more severe than those presently prescribed in the licensing process (see Section 4).
2. There is a strong need for models capable of carrying out calculations for such events and malfunctions sequences. Such models should include control systems, man-machine interactions and the computations should be performed rapidly and, if at all possible, in real time. The codes should strive for best estimates. The development of such codes is not meant to replace other available codes and their needs for licensing purposes.
3. Development and experimental verification of accident codes must be continued. Emphasis should be put on the capability to model

the processes correctly rather than in oversharpening the accuracy in predicting a single parameter such as peak clad temperature. For example, tests for breakdown of natural circulation, flow instabilities if they occur, condensation with non-condensable gases would fall in such a category.

4. It is suggested that other parameters such as rate of loss of coolant inventory, modes of coolant circulation, periods of core uncover, and time of fuel rod rewetting also be used to complement peak clad temperature as a means of evaluating reactor system safety.
5. It is recommended that licensing evaluations be made on a best estimate basis and that a safety margin be added to the best estimate. This approach is superior to the present mode of adding conservatism in several places of the licensing models. The recommended approach will not only lead to better understanding of phenomena and make more information available to operators, but it also would put the development and experimental verification of such models on a systematic basis.

2.5 Damage Analysis

2.5.1 Background

Following the accident at TMI-2, there was a need to estimate the degree of core damage and, in particular, the reactor core configuration. This knowledge was necessary to evaluate alternate modes of transition to cold shutdown at TMI-2. Models have been developed to deal with such

post-accident damage. These models vary with the type and degree of resultant damage. For example, during a LOCA, the fuel cladding will balloon and fail and lead to flow blockage in the fuel assembly.⁷ If the fuel clad temperature continues to rise, metal (zirconium)-water reaction takes place and brittle clad failure occurs. In the case of a very strong reactivity accident, the fuel clad will rupture and some fuel fragments might be dispersed in the coolant. Many out-of-reactor and in-reactor experiments have been performed to help predict the resulting damage and to verify the many available models.

In performing such predictions, one of the key results is to define the prevailing geometry because it will determine the flow at each location and the fuel capability to transfer heat to the coolant. As expected, uncertainty in geometry increases rapidly with degree of core damage.

2.5.2 Findings and Recommendations

1. Damage models have been developed and they are validated against experimental data (see for example, General Electric NEDO-20566, pages I-76 to I-105 for LOCA). These models tend to deal with the early stages of damage and to overestimate the consequences to satisfy licensing requirements.
2. There are uncertainties in the models and continued experimentation and modeling efforts need to be carried out. Several in-reactor experiments have been performed to simulate LOCA accidents. These experiments are being sponsored by NRC. In the past, overemphasis

Has little to do with damage modeling

may have been placed upon modeling and testing the rapid damage scenarios rather than slowly developing damage as occurred at TMI-2. This is being corrected as shown by the damage experiments listed in Table 4.

- PBF
etc
3. It is recommended that damage experiments for slow moving accidents such as gradual core uncovering be performed and that models be developed for medium and very long periods of uncovering time. Such models would have helped greatly in assessing TMI-2 conditions after the accident. Another important source of information will be the TMI-2 reactor core itself. It is hoped that serious efforts will be made to collect important damage information from that core.

2.6. Training Simulator Models

2.6.1 Background - The use of nuclear reactor simulators began in 1968 when General Electric put into operation a simulator at Morris, Illinois. The Morris simulator modeled the Dresden-2 and -3 plants, which at that time were not yet operating. The purpose of this simulator and all subsequent simulators was to provide a realistic facility for training reactor operators. The major advantage of a simulator over a real control room is that it can provide the operator with exposure to unusual events which might otherwise take an entire career to experience.

The models which are used in these simulators to represent the water flow, steam flow, core power, valve position, control rod position, etc., are much simpler than the models described earlier in this report. There are

STAFF DRAFT CONFIDENTIAL
NOT FOR DISTRIBUTION

two reasons for this: first there is less need for detailed information in a training simulator, and second, it must be simple in order to perform the calculations in real time.

The simulator's computer performs relatively straightforward calculations, such as a heat balance around the flow loop and in the reactor vessel. It calculates pressure drops in the piping from simple pressure drop-flow equations, and it calculates core power with a relatively simple point kinetics model, similar to ones used in the transient analysis models described in section 2.3.

Standard transients are run on the simulator model once it is assembled, and adjustments are made to make the control room indications to be the same as that expected on the real reactor, within the tolerance limits allowed.

Thus, while the design codes which have been described in earlier sections solve the basic differential equations for fluid mechanics, heat transfer, void fraction, neutronics, the reactor simulators use simpler relationships, such as $\Delta P = K \frac{1}{2} \rho V^2$ *. The output from these calculations is much simpler than those of the detailed design codes, which must calculate peaking factors, pressure forces on internal components, margin to critical heat flux, fuel cycle reactivity, and other parameters needed to properly design a plant, but which are not necessary to operate one.

* ΔP corresponds to pressure drop, K is a loss coefficient, ρ is the fluid density and V its velocity.

In spite of these simplifications, some training simulators are capable of analyzing relatively complex situations, with conditions degraded well beyond normally expected conditions. The most recent simulators have greatly increased computing capability, compared to earlier simulators, and generally do a better job of simulation. This new generation of simulators can simulate a wide variety of malfunctions, either singly, or in multiple combinations, including instrumentation malfunctions. There are limits, however, to how far these simulators can be stretched, due to the simplicity of the models. Additional sophistication would have to be added to the current training simulators before they could be used as engineering simulators for design or licensing applications or for failure mode and effect analysis.

2.6.2 Findings

1. The current generation training simulator models are very capable of modeling operational maneuvers such as startup, shutdown, turbine trip, and load demand changes. To varying degrees they are also capable of simulating multiple component failures and instrumentation and control malfunctions.
2. The current capability of simulation of the TMI-2 event is not very good. For example, the Lynchburg training simulator cannot take into account the location of steam void formation or simulate the breakdown of natural circulation when the plant is employing that mode of cooling. Even the most recent generation of simulators, which do a much better job of simulating the TMI accident have a problem of coarse modeling in the primary loop, which makes the

natural circulation calculations marginal.

- analog + digital*
3. The computer/simulator industry appears to have the capability of designing simulators which are much more sophisticated through the use of faster, larger computers and improved programming techniques. Going from "single instruction/single data" programming to "multiple instruction/multiple data" programming has improved Boeing airplane simulator's computing speed by about a factor of 100.
 4. The introduction of the Applied Dynamics International "Black Box" for table interpolation has permitted the use of data tables instead of polynomial to increase simulator computing speed.
 5. In aerospace applications, the models for aircraft simulation are relatively simple, with the flight motion and visual simulator requiring large computing capacity. The nuclear simulation models are generally more complex than aerospace simulation models, but have the advantage of not needing complex visual and cockpit motion simulation. Aerospace simulation appears to be more advanced than nuclear simulation because of the need for speed and capacity for cockpit simulation. However, the overall level of technology appears to be equivalent between the aerospace and nuclear industries.
 6. Simulators are often calibrated against analytical results which are

presented in licensing documents. These licensing calculations are usually very conservative, rather than being "best estimate", and therefore often introduce a bias into what is presented to the trainee as a normal event.

2.6.3 Recommendations

1. Training simulation models should be improved to allow calculation of degraded conditions beyond what is now possible. For example, the capability to calculate the generation and transport of steam in a PWR core and its transport through the recirculation system and natural circulation should be developed. There is no need to have simulators calculate conditions much beyond core uncover and heatup. Simulators should be capable of simulating stuck-open relief valves and small breaks up to the point of core uncover and heatup, including faithful simulation of natural circulation.
2. Operator response to degraded situations, (e.g. stuck-open relief valve, small breaks) on improved simulators should play a role in the NRC's safety requirements.
3. The latest high-speed computing technology developed for the aerospace simulators should be applied to the next generation of nuclear simulation models.
4. All training simulators should be calibrated to the best estimate

of how a reactor will respond to various inputs. All events in training simulators which are calibrated to conservative calculations should be adjusted to reflect best estimate conditions. All training simulators should be checked periodically against sample problems or test cases which are different from the cases which the simulator was calibrated to. These periodic checks by the Operators Institute and or the NRC would confirm that all simulators are simulating real situations rather than the less realistic licensing situations. They, also, would give a measure of the capability of such simulators to predict conditions beyond those for which they were designed.

5. Flow of information between designers, operators, and simulator designers could be increased to the benefit of all.

3.0 HARDWARE TYPE SIMULATORS3.1 Engineering Simulators3.1.1 Concept

This section is concerned with high fidelity simulators which could be used for design, and failure modes and effects evaluations. The performance accuracy required here would be equivalent to that obtained from the models discussed in sections 2.2 to 2.5, except that the computations need to be carried out in real time. All critical functions would be included, and man-machine interactions could be evaluated by incorporating not only the control room equipment, but all other components which are operated by plant personnel. A comparable simulator in scale and details exists at NASA AMES where it is employed to design and check out advance airplanes. This NASA flight propulsion simulation center is about a 50 million dollar facility with annual operating budget of 5 to 10 million dollars.

From a concept viewpoint, the proposed simulator would be similar to the advanced training simulator being built today. It will have a complete reproduction of the control room. In addition, it will have another separate room which will simulate all other components which can be operated by plant personnel outside the control room. It will employ a very fast and a large digital computer to carry out the desired calculations.

incl secondary side controls + power grid things

INITIAL
COPY

The models incorporated in the engineering simulator will include many of the features provided in the codes discussed in section 2. Referring back to Table 2, the model for a B&W plant would have the control systems and balance of plant features of POWER TRAIN, combined with the reactor descriptions of CADDIS and with the loss of coolant features of CRAFT and TRAP. With respect to the loss of coolant modes, one will not try to simulate the sonic waves so that large enough time intervals could be used to perform the calculations in real time. This would be limiting only for the very early part of the largest pipe breaks.

The engineering simulator need to be designed so that component and system modifications can be introduced. Also, flexibility needs to be provided to allow software, and model improvements as such improvements surface.

3.1.2 Applicability

The high fidelity engineering simulator would make it possible to do the following:

1. To systematically investigate the safety of nuclear plants. It can be used to evaluate the entire spectrum of transients and accidents under various conditions of equipment malfunctions, operator errors... etc. It could be used to carry out failure modes and effects studies.
2. To evaluate the adequacy of human engineering in control room.
This simulator should make it possible to judge the adequacy of

CONFIDENTIAL

information provided to operators and their capability to assimilate it.

3. To try out "what if" situations and how to cope with them.
4. To develop advanced plant designs both in terms of control and safety systems.
5. To evaluate alternate strategies of operation after an emergency condition develops in an operating plant.
6. To provide advanced analytical models to be incorporated in future training simulators.

This type of simulator will have to deal with each reactor type rather than a specific plant design. In that sense, primary application would be by:

1. Operations Institute Center to provide support to operating plants.
2. NRC to evaluate safety of plants.
3. Reactor suppliers to evaluate safety of designs and to improve them.

Because of high capital and operating costs, it does not make sense for the above three groups to each have such high fidelity simulators. Even

if an arrangement could be developed for all three possible users to use the same simulator, one is still faced with the need to build one BWR and at least two PWR simulators.

3.1.3 Feasibility

The feasibility of high fidelity engineering simulators was discussed with many organizations in this study and the general conclusion was that such a simulator was feasible but developmental. It was suggested that it was most important to define an achievable goal and not to have such a simulator try to do everything right away. Another key to the success of the simulator will be software development and enough judicious simplifications need to be made to achieve real time simulation. It was felt by many that it would be best to spend one or two years to define the scope of the simulator and to establish software feasibility. Even after this initial phase, it would be wise to design and build the engineering simulator in phases, i.e. improving and adding to the simulation in a stepwise manner.

3.1.4 Implementation Schedule

It is estimated that a high fidelity engineering simulator would be available 5 to 7 years after the start of the project. It will cost about 50 million dollars, and will require an annual operating budget of at least 5 million dollars. Initially, it would be wise to embark on a single simulator of this type rather than two or three.

STAFF DRAFT CONFIDENTIAL
NOT FOR DISTRIBUTION

3.1.5 Merits

The technical merits of such a high fidelity simulator are apparent. Its greatest drawback is schedule and costs. Benefits will not be obtained from it for at least 6 years, and one could argue that the other simulation improvements recommended in this study could produce nearly equivalent results and on a shorter schedule. Yet, if a mechanism could be found for all interested parties (both in the USA and overseas) to support such a program and spread the costs, it might be worthwhile to proceed with a prototype high fidelity simulator. There could be enough early indirect benefits from such a prototype to justify such a development.

3.2 CONTROL ROOM SAFETY INFORMATION ENHANCEMENT

3.2.1 Concept - One of the early conclusions of nearly everyone who investigated the operator's actions in the first few hours of the incident at Three Mile Island was that, while he had enough data at his disposal to be able to do the right thing, the information he needed was not presented to him in a form which was easily assimilated.

One of the lessons to be learned from the TMI-2 incident is that nuclear plants should be designed to provide information to the operator in an easily assimilated form in order for the operator to cope with accidents which have not been previously analyzed or experienced. In their report on incident at TMI*, the NRC stated:

"There will always be a residuum of possible but not postulated and analyzed situations. *To address this, and as an attempt to extend the defense-in-depth concept, we should study ways to make the operator a more effective recovery agent/accident mitigator. Such a study should look for ways to (a) prevent (inhibit) inappropriate actions and (b) promote productive intervention. An element of the study that could serve both purposes would be an investigation of methods that would furnish the operator with correct, current, digestible information regarding principal plant conditions (i.e., processes, systems and equipment). The means by which the operator would best use this information should also be considered, however, such means should not be so rigid as to preclude expedited and improvised actions for the operators for unanticipated phenomena."

*NUREG-0560, "Staff Report on the Generic Assessment of Feedwater Transients in PWRs Designed by B&W" May 1979

The same computer technology advancements which make improved simulation possible, also make it possible to process the existing information about the safety status of a nuclear power station. The addition of such an advanced computerized monitoring system would greatly improve the effectiveness of the operator. This computerized monitoring system could, for example, calculate and display the status of the reactor coolant inventory by keeping a continuous tally of all outflow and inflow to the reactor pressure vessel, and converting these flows to water level relative to the top of the core. It could also tell the operator whether the water level is rising or dropping, and how long before the core will become uncovered if the water level continues to drop at its current rate.

In addition to pressure, power and water level, this computerized monitoring system could tell the operator the status of crucial safety systems (e.g. RHR, HPI, safety relief valves, emergency power) upon operator request. The output information would be processed to summarize the high priority information to the operator, rather than telling him everything about the system.

The mass flow rate of all the above sources of inflow and outflow could be continuously monitored and displayed on a standard cathode ray tube (CRT) output screen in a form which is immediately useful to the operator, by integrating the outflow and inflow of mass to the reactor system. Then,

based upon temperature measurements and a simplified void distribution correlation, it could convert this into a volume and distribution of liquid in the vessel or primary system. The final step would be to relate the liquid volume to the distance from the top of the active fuel. This output could then be displayed on the CRT screen in the following manner:

- o Water level is 5 feet above the top of the top of the active fuel
- o Two-Phase water level is 10 feet above the top of the active fuel
- o Water level is dropping at a rate of 2 feet per minute
- o At the present rate, it will take 13 minutes before the top of core is uncovered.
- o Neutron Power is zero
- o Primary source of outflow is through the relief valves
- o Primary source of inflow is from the HPI system
- o Core flow is in forced circulation at 10 million pounds per hour 90% of rated core flow.

EXAMPLE ONLY

In addition to the primary output, there is also some secondary output which could be displayed upon the operator's request, such as:

- o Ranked Sources of Outflow from Primary System
- o Ranked Sources of Inflow to Primary System
- o Status of Safety and Recirc Pump Systems
- o Criticality and Power Status of Core
- o Status of Containment
- o Status of Isolation System
- o Status of Instrumentation

This improvement would be primarily for the benefit of the reactor operator in the control room of the power plant. However, there is also the possibility that this same information could be telemetered to central sites, such as Bethesda and Lynchburg, as a means of continuously communicating a plant's status. This telecommunication could be used during an emergency, such as the one at Three Mile Island, or as a means of continuously monitoring all plants' safety status. (See discussion in section 5.)

3.2.2 Feasibility

This improvement could be designed and manufactured using existing state-of-the-art technology of instrumentation, computers and display systems. It would not necessarily require any new instrumentation. It should require only the processing of existing signals, which are already transmitted to the control room. Thus, it should be possible to backfit this design to operating plants without requiring major construction, such as making new containment penetrations, or installing new instrumentation. For operating plants, it may not be possible to design such a system to the latest industry safety standards, but for plants in the design or early construction stage, this should be relatively simple. The cost of installation labor and materials should be in the range of \$500,00 to \$1,000,000 per plant, excluding engineering costs.

3.2.3 Implementation Schedule

Because this improvement involves instrumentation and computers which should require little or no modifications to the equipment or operating

plants, the schedule for implementation would be dependent on the time to engineer the system (signal processing and computer programming), time to procure the components and the time to install and check out the finished product. A reasonable schedule for implementation should, therefore, be about 18 to 24 months for the time of the decision to install the device.

For application as a telecommunication device, the time required to implement should be about the same, except for the time to reach agreement among the utility owners and vendors and the NRC on the standard form of the telemetered signal which would require another 6 to 12 months. ✓

3.2.4 Merit

This safety monitoring system has a great potential for improving reactor safety in two ways: providing information which improves operator response in an emergency, and improving communications between the reactor site and off-site locations such as the suppliers and NRC. Also, it could be implemented in a reasonable period of time. Therefore, it should be given a high priority for implementation at both operating plants and plants under construction.

3.3 IMPROVED REACTOR TRAINING SIMULATOR

3.3.1 Concept - One of the tasks of this study was to determine whether it is possible to build a simulator which goes a step beyond the current training simulators, to be used as an engineering or advanced training simulator, much as is done in the aerospace industry. This simulator could then be used in the design process to improve control room design, to perform failure sensitivity analyses and to optimize control system design. In the licensing area, the engineering simulator could be used to investigate operator response to degraded conditions, to answer industry and NRC questions regarding accident situations and to evaluate the adequacy of safety system design. In the training area, the advanced simulator would be used to expose plant operators to more complex and potentially confusing situations and to improve their ability to respond properly to unusual situations on the real reactor.

3.3.2 Applicability - An improved reactor simulator would have a role for the utility owner, for the NRC, and for the reactor vendor. The utility owner could use the simulator to expand and improve the quality of operator training. The NRC could use it for independent safety studies. The reactor vendor could use such a simulator to improve reactor design.

Potential NRC Staff Applications:

- o Perform independent safety studies, study implications of abnormal occurrences
- o Assist reactors in jeopardy during emergency situations
- o Improve understanding of reactor safety margins, allow improved prioritization of safety issues

Potential Utility Owner Applications:

- o Improve operator training
- o Check out procedures earlier in design stage
- o Review reactor design in early design stages for operability improvements
- o Support reactor operator during emergency situations

Potential Reactor Vendor Applications:

- o Check out design improvements
- o Adjust control system characteristics
- o Improve Man/Machine interface in Control Room

3.3.3 Feasibility

The state-of-the-art in simulation has reached a level in the aerospace and nuclear industries such that it appears to be entirely feasible to improve the models in nuclear reactor simulators sufficiently to allow a significant increase in the amount of degradation, or number of component failures simulated. (See Section 2.6 for more detail.) For example, reproductions of events which result in reaching saturated conditions in a PWR (such as small breaks or stuck open relief valves) are feasible using today's simulation and computer technology. The three areas which need to be improved in order to do a better job of simulation are: core thermal hydraulics, core kinetics and piping dynamics.

3.3.4 Implementation Schedule

Since the time required to design, build, shake-down and install an ordinary reactor simulator is two to two and a half years, it would take at least that long to complete a more sophisticated version. Since there

is some extra front-end engineering and software development necessary for an advanced version, it would probably take an additional twelve to eighteen months. Thus, it should be possible to have an operating advanced reactor simulator about three and one-half years after the decision is made to build one. It may even be possible to improve a simulator currently in operation and have an advanced simulator operating within two to three years.

3.3.5 Merit

The merit of whether to build an improved reactor simulator is slightly different for the three applications (utility, NRC, vendors). For application at the utility, the safety significance of a more flexible and more sophisticated computer is in its ability to provide a broader spectrum of problems with which to challenge the operator-trainee. An improved training simulator of this sort is very important and should be given a high priority. Next in rank, but still of high priority is the use of these improved simulators by the vendors, utilities, and NRC staff to perform independent safety assessments. Of lower priority from a safety standpoint, is the use of such simulators by reactor vendors to develop advanced future designs. The cost of a standard simulator today is about six or seven million dollars. It would cost another two to three million dollars for an improved simulator. Thus, the additional cost of an improved simulator is not exorbitantly greater than the standard design being purchased today.

3.4 Simulator for Each Site

3.4.1 Concept

One of the ideas which seemed to be brought up by many of the people who were interviewed was the concept of having a simulator located at each site which would be an exact duplicate of the actual plant control room, and would be available for nearly continuous training of the reactor operators.

3.4.2 Applicability

This concept clearly is tailored only to the utility owners of the nuclear power stations, since to have duplicates elsewhere for all plants would result in an excessive number of simulators. However, in addition to its use as an on-site training facility for nuclear plant operators, the presence of a nuclear simulator at each site could also have the following advantages:

1. The site located simulator could be used to investigate the implications of unusual events which occur at this plant or other plants to verify that safety margins are still as great as was considered before the particular new event. It also would be a good way of educating the site personnel as to the events which occur at other sites, and the lessons to be learned from each experience.
2. When an unusual event occurs at a site, causing shutdown of the plant for safety reasons, an on-site simulator could

very quickly reproduce the event, and check to see if any safety limits were approached and to train all site operators how to properly handle the incident. This ad hoc study could be used to allow faster restart of the plant following such an incident.

3. The site-located simulator could be used by supporting engineering personnel to acquire an improved understanding of plant performance.

There has been an increasing tendency for the utility to purchase a simulator at the time of the purchase of a reactor. This trend, would probably eventually result in most future plants having simulators, especially at multiple plant sites.

It is probably not necessary nor feasible, however, for the NRC to have the capability of simulating every nuclear plant exactly. If the NRC had a simulator for each class of plant, that should be sufficient for them to perform their independent safety margin studies.

3.4.3 Feasibility

The design and construction of such site simulators is being done right now, i.e. it is clearly feasible

3.4.4 Implementation Schedule

Such simulators would be operational about 3 years after the decision is made to proceed.

3.4.5 Merit

The concept of having a simulator at each site for improved reactor safety is one of moderately high priority, and one consistent with the oft-stated goals of improved operator training. Because of lack of standardization in control room and power plant designs, it may be especially useful to have a plant simulator when its configuration is very different from that of the training simulator.

4.1 Approach

The subject of safety margins is a very broad one and it is presumptuous to assume that it can be dealt with in enough detail in this study. The approach that was taken was to look at the basic safety philosophy employed in the United States in the designing of water cooled reactors and to determine whether the TMI-2 accident might suggest revisions to the basic safety philosophy. In section 4.2 it is shown that the basic philosophy is a sound one and that the issue is one of complying with the philosophy rather than revising it. Recommended actions to satisfy the writers' perception of that basic philosophy are given in section 4.2. In section 4.3, a few of the key principal design margins are discussed. Summary definitions and the history of such margins are given together with a judgement evaluation of their adequacy. Finally, in section 4.4 a brief comparison of the various PWR reactor types is included and their relative margins discussed. Sections 4.2 to 4.4 were developed at the request of the Commission Staff and it is most important to realize that within the time available the most striking characteristic of these sections is that they can only be cursory.

4.2 Basic Nuclear Reactor Safety Philosophy

4.2.1 Description of Philosophy

The basic safety philosophy adopted in the United States is one of defense in depth. Three barriers are provided to avoid or reduce the consequences of fission product release. The first barrier is the fuel itself with UO_2 retaining most of the fission products in the fuel matrix and the cladding providing a pressure boundary against any such release. The second barrier is the primary system. The primary system is built of the highest quality

SLI-7904

structural material and it is inspected repeatedly to avoid any leak or break of this pressurized boundary. The third barrier is the containment which is provided to avoid fission product release to the environment. A multitude of engineered safety systems are incorporated to enhance the integrity of the three barriers and to assist in their resistance to fission product escape. Just to mention a few engineered safety systems, light water reactors have control and reactor protection systems, emergency cooling systems, fission product removal and pressure suppression systems...etc. Superimposed upon this fundamental barrier philosophy is the safety requirement that limits the release of fission products from fuel rods as the probability of events producing such an occurrence is increased. More specifically, it is generally accepted that light water reactors should be designed so that:

1. There should be no fuel failures when the reactor is subjected to normal or anticipated transients. Such transients are considered to be quite frequent. For example, according to NUREG-0560, PWR feedwater transients have occurred at the rate of 2 to 3 per year per plant.
2. The number of fuel failures should be insignificantly small when the reactor is subjected to a normal or anticipated transient and a single equipment failure or a single operator error.
3. For accidents of low frequency and clearly of lesser frequency than under (2) above, failure of a limited number of fuel rods is allowed after one assumes another single failure. In this class of events are put such accidents as small breaks produced from structural failure of the primary or secondary boundary systems together with a loss of off-site power.

4. For accidents of very low frequency, damage of a significant number of fuel rods is permitted after postulating another single failure. The large rupture of a primary or secondary system pipe together with loss of off-site power is put in such a category. For such a rare event, the reactor core is still kept in a coolable geometry so that fission products escaping through the break can be retained in the containment.

In essence, the preceding four groundrules define a probability versus reactor core damage curve which has not been quantified numerically. The groundrules have not been translated into numbers to avoid being sidetracked into just a "numbers game". In this section, a very gross quantification of the basic safety philosophy is proposed in order to assess whether designs are meeting this perceived philosophy. For simplification purposes, we shall assign a probability of approximately unity, to a normal transient and a probability P to an equipment failure or operator error. We shall also assume that the occurrence of a small break has a probability P^2 while large LOCA breaks have a probability P^3 . The basic philosophy can, therefore, be quantified in a gross way as follows:

<u>Probability</u>	<u>Extent of Fuel damage</u>
≈ 1None
PNone
P^2Insignificant number of fuel rods
P^3	Limited number of fuel rods
P^4	Significant number of fuel rods but coolable geometry

single failure mode not discussed

This gross approach is similar to that employed in the Nuclear Reactor Safety Study except that in the Nuclear Reactor Safety Study each probability was quantified as well as possible and the consequences of releasing fission products to the environment were calculated. It is felt that by looking at consequences to the environment, one might put overemphasis on the events which lead to core meltdown, i.e., much more degraded events and less frequent events than covered here. While it is wise in design to consider such high consequence events, it might be advisable to define separate probability-damage levels for events for which the fission products are retained in the containment. Such events are more frequent and of overwhelming importance to the continued plant power generation and the owner's investment.

With the very rough quantification proposed herein one can proceed to evaluate the loss of coolant events depicted in Figures 11 and 12 and this is done in sections 4.2.2 and 4.2.3.

4.2.2 Evaluation of Loss of Coolant at Very High Pressure

Figure 22 is a modification of Figure 11 except that types of information that might be available to the operators are shown in boxes. Some of the options for activity by the operators are also given along side the boxes. Employing the same gross basis as in section 4.2.1, the occurrence of the loss of main feedwater has a probability near one; the failure of delivery of auxiliary feedwater raises the overall probability to P as shown on the left side. Operator inaction adds another P to give a total probability P^2 . Yet, after many open-close cycles of the relief valves the coolant inventory is decreasing, a steam water mixture is flowing through the reactor circulation

ABILITY TIME

INFORMATION TO OPERATOR

POSSIBLE OPERATOR ACTION

0

LOSS OF MAIN FEEDWATER

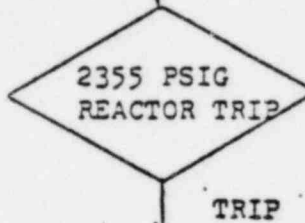
3 Sec



Loss of Feedwater
Increasing Pressure
Increasing Level

Reestablish Feed

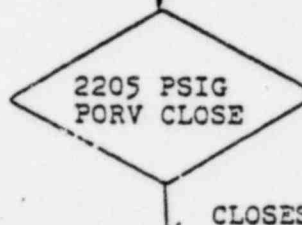
8 Sec



Loss of Feedwater
PORV open
High Pressure

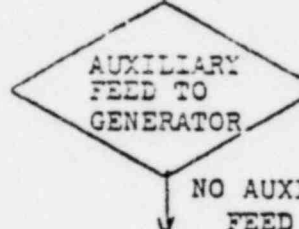
Reestablish Feed

12 Sec



Loss of Feedwater
Low Reactor Flux
Pressure Decreasing
Decreasing Level

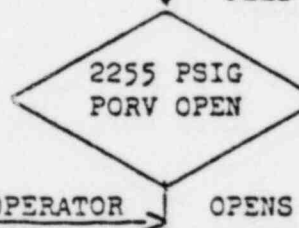
20-30 Sec



Loss of Feedwater
Low Reactor Flux
Decreasing Level

Reestablish Feed
Establish Auxiliary Feedwater

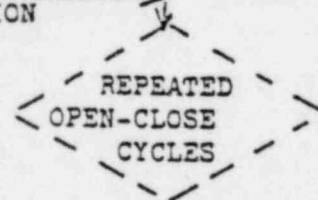
20-60 Sec



Loss of normal and auxiliary feed
Low Reactor Flux
High Pressurizer Level
Rising Coolant Temperature

2

20-40 Minutes



Reestablish Feed
Establish auxiliary feedwater
Depressurize and put HPI on

FIGURE 22 HIGH PRESSURE LOSS OF INVENTORY

pumps and they will cavitate or might be tripped by the operators when this occurs, the core damage might be comparable to TMI-2, i.e. the number of fuel rods failed will be significant but the reactor core geometry will be coolable. It is seen that for an approximate probability of P^2 the core damage could reach the level which was assigned the P^4 probability level in section 4.2.1. Now, one of the problems with probabilities is that they are subject to debate, which in many ways explains the reluctance of adopting them in the licensing process. There are those who will argue that the operator had time to take the same action several times or more than one action in the course of the event, especially if he is able to restore feedwater to the steam generator. In other words, some would say, the probability of operator inaction should be lowered. Indeed, the available time to operators is estimated to be between 40 and 60 minutes, and operator inaction could rate P^2 by itself. On the other hand, one could argue that the auxiliary feedwater system is subject to a single failure which cannot be corrected by the operator. Also, the operator is still getting a full pressurizer level signal to countermand the indication of high pressure and saturation temperature in the coolant and a considerable number of other signals to be concerned about. While debate about the exact probability value is expected, it is suspected that most will agree that it is above P^3 (i.e., closer to P^2) and the gross probability-damage level quantification of section 4.2.1 is not met.

4.2.3 Evaluation of Loss of Coolant at Medium Pressure

Figure 23 is a redo of Figure 12 with the same additions as provided in Figure 22. Only the early stages of the accident are dealt with because the evaluation which follows will focus on that part of the event. Assigning

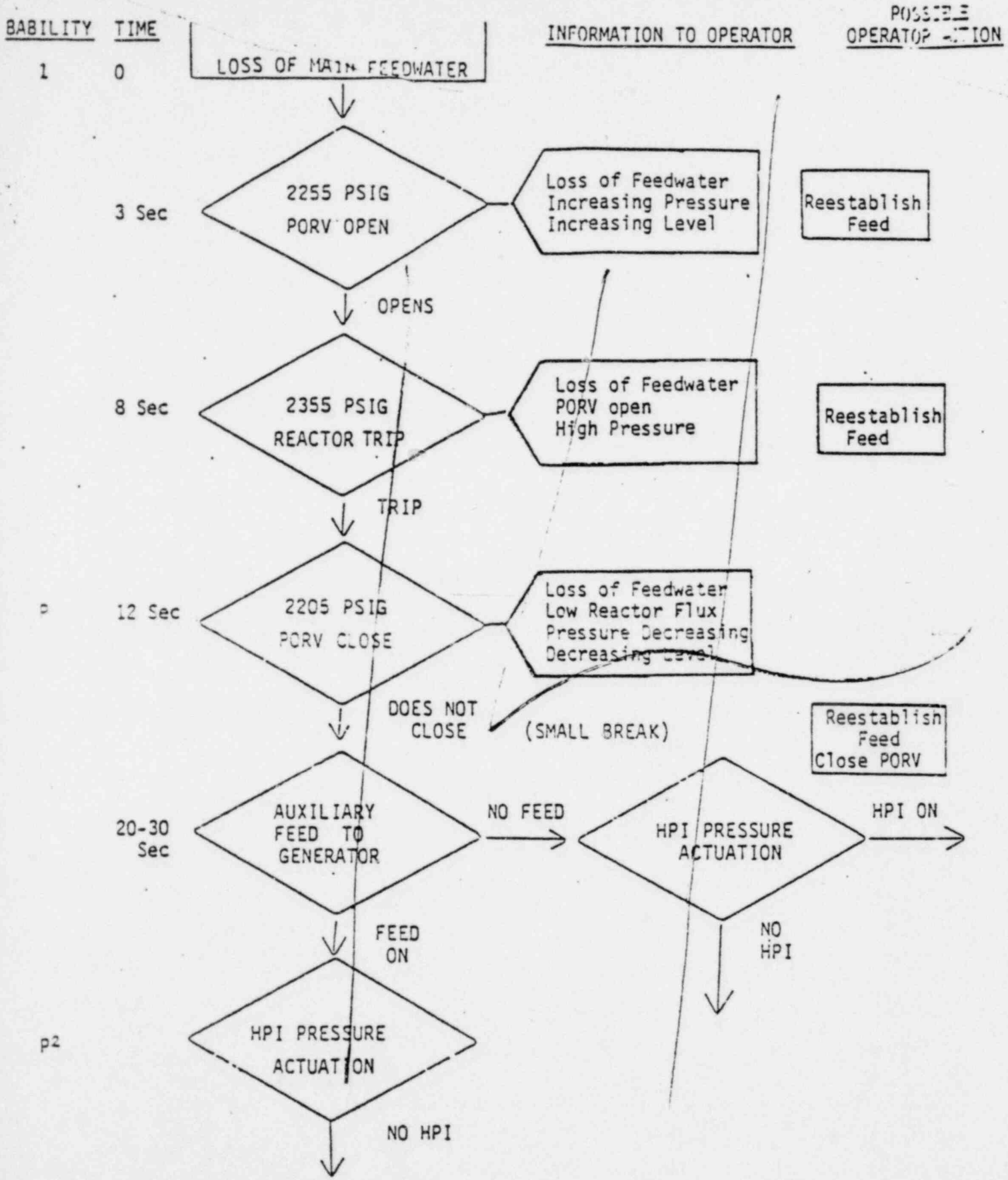


FIGURE 23-MEDIUM PRESSURE LOSS OF INVENTORY

a probability approximately unity to the loss of main feedwater and a probability P to the failure of PORV to close, a small "break" (i.e., stuck open PORV) is found to occur at the probability level P rather than the P^2 level presumed in section 4.2.1. Figure 23 can also be employed to evaluate the probability for a TMI-2 type accident. Assigning a probability of approximately unity to the loss of main feedwater, the failure of PORV to close gives an overall probability of P . Loss of auxiliary feedwater raises the probability factor to P^2 and interruption of HPI by the operator gives an overall probability factor of P^3 . Now again, one could argue that enough time was available to the operators that their incorrect actions should be assigned a probability of P^2 . On the other hand, one needs to give them credit for restoring auxiliary feedwater and an overall value between P^3 and P^4 may be more appropriate, which still falls below the value of P^4 suggested in section 4.2.1.*

4.2.4 Evaluation of Means to Improve Probability - Damage Estimates

There are many ways to improve the probability numbers developed in section 4.2.2 and 4.2.3 and the NRC has proposed many actions along that line. The new NRC requirements are oriented to

1. Reduce the probability of loss of main feedwater, thus reducing the probability of such events.
2. Increase the reliability of the auxiliary feedwater system, thus lowering its probability of failure to below P .

* Another scenario can be postulated from Figure 13. Failure of PORV has a probability P . The safety valve is allowed to open and close repeatedly without operator intervention for an overall probability of P^2 . With no auxiliary feed one gets an overall probability of P^3 . The primary system would be losing inventory at a pressure between 2450 and 2500 psig where HPI is not effective and where the operator may not have an easy way to depressurize it.

3. Retraining operators to not focus exclusively on pressurizer level but also watch pressure and coolant temperature before deactivating HPI. Also, operators were to receive training about the possibility of no natural circulation if the pumps are tripped at the wrong time. Finally, operators are expected to more readily use the block valve to isolate PORV valves which fail to close.

4. Anticipatory trips have been added and the pressure setting of the PORV valve has been raised above that of the reactor trip in the B&W units. This new system response is shown in Figure 24 and should reduce the probability of PORV opening and i.e. of its failure to reclose.*

All of the above actions are in the right direction and should help attain the probability -- damage values proposed in section 4.2.1. The NRC has also requested substantial new information for small breaks to ascertain that the previously submitted analyses are correct.

As one might expect, there are many other methods to reduce the risks and they are being considered for implementation over a longer period of time. Some suggestions have been developed based upon the methods of 4.2.1. It should be realized that the suggestions have not been looked at in detail or optimized in any sense.

*A concern about the settings of Figure 24 deserve mention here. If the PORV opens, its pressure setting is so close to the safety relief valve setting of 2500 psig that it might trigger both safety valves to open. If one of the safety valves fail to reclose, a break equivalent to one open safety valve could be generated at the probability level P versus the probability P^2 suggested in section 4.2.1. This deserves further checking to ascertain that the probability of PORV opening the two safety relief valves is remote.

If one returns to Figure 22, the most apparent way to lower the probability of the event is to make the auxiliary feedwater single failure proof. This would reduce the probability of losing feedwater to P^2 . Another way to reduce risks is to lower the probability of operator inaction. First, one could provide the operator with another signal to improve the chances of the operator taking action. It has been suggested, for example, that water level should be measured above the reactor core. Another alternative is to develop and provide a computerized primary coolant inventory system as discussed in Section 3.2. This system would give an integrated picture of water leaving and entering the primary system and it would also track the opening and closing of the PORV. The level or the core inventory system could also be connected to the emergency core cooling systems thus providing an alternate and diversified signal to such systems.

To truly lower the probability of the event to P^4 , it is necessary to use coolant temperature and pressure, or reactor core water level, or core inventory system to trigger the necessary action to terminate the transient. One would call for depressurization and in turn HPI actuation if there is no normal and auxiliary feedwater and if coolant temperature is close to saturation, or the core level, or the core inventory system reach a low prescribed setting.

In the case of Figure 23, one can improve the probability of operator action after the PORV does not close through additional instrumentation.

The temperature signals presently available do not make it easy to differentiate between a PORV opening and closing repeatedly,, a leaky PORV and a PORV staying open. Sensors that can detect flow combined with pressure measurements would discriminate between these two circumstances and would enhance the operator chances of using the block valve to close PORV. A similar suggestion was made in NUREG 0578. From the cursory study performed here, the preferred functional changes to be made in the future are shown below together with their effectiveness rating.

Highest: make auxiliary feedwater system not susceptible to single failure

High: develop and install a water inventory system or provide another means of detecting possibility of core recovery.

High: provide alternate and diversified signal besides pressure to initiate HPI and have it remain effective.

Medium: develop and install alternate means of detecting an open relief valve and its failure to close.

It is worthwhile to note that the highest rating is given to removal of the reactor heat by the steam generator. The importance of such heat removal was stressed by Michelsen and it has an even greater role for inventory losses such as postulated in Figure 22 where the pressure remains high enough to be above the shut off head of the HPI pump. A similar finding is noted in a September 18, 1975 letter from Combustion Engineering to TVA* which states that "for breaks equal to or smaller than 0.1 ft², Emergency Feed Water was found absolutely essential". Attached to the Lumpkin letter

* Letter from R. L. Lumpkin of Combustion Engineering to D. R. Patterson of TVA with the subject of SMALL BREAK LOCA.

is a graph which shows that substantial core uncovering would result at about 25 minutes after the break.

There are many other possibilities to the functional changes suggested here and they need to be evaluated systematically. Also, the ease with which such improvements can be made at their implementation time must be taken into account because this determines the number of plants that can be affected. Finally, in the long term, one might find it preferable to implement some of the design changes proposed here instead of the interim requirements imposed by the NRC. For example, while the anticipatory trips might make sense in the interim period of time, they can lead to spurious scrams. Also, they do not make it possible to recover from a turbine trip as was possible before, thus forcing additional plant shutdowns and restarts.

4.2.5 Findings and Recommendations

1. There appear to be sequences of events of higher probability than those postulated in safety analyses which produce the same damage. Such sequences of events have been identified in this study for the case of loss of primary water inventory at high and medium pressure. (See Figures 22 and 23 for examples.) Such accident scenarios tend to involve events which take place over longer periods of time and which require operator actions. It is recommended that all such sequence of events be reexamined and compared in terms of probability/end result with the accidents

analyzed for licensing purposes. The proposed reassessment needs to be expanded to other areas besides loss of coolant. While the gradual loss of coolant may be the most important of such initiating events, one needs to search for other slow moving events with operator errors and equipment failures which might produce significant fuel failures. For example, one should look at power increase with flow reduction, long term cooling of the reactor, ...etc.

2. Such evaluations can be done along the lines employed in Figure 22 where the event is defined versus time along with its probability. Also, information available to operator and his possible actions are considered with respect to available time. Such logic charts would help reveal areas of improvements and suggest necessary functional changes. Out of such studies would emerge malfunction charts to be employed by operators instead of the very tedious written procedures now available. This technique has been well developed by NASA. It consists of having operators generate functional control diagrams for all systems and sub-systems. Such diagrams show the instrumentation and the information available to the operator. The operators next employ their functional control diagram to produce malfunction charts which become the equivalent of operating procedures used in the nuclear industry. It is recommended that the NASA techniques be adopted in the nuclear industry.

a way to do it

3. A cursory examination of loss of inventory events (such as occurred at TMI-2) reveals that in the long term TMI-2 type accidents could be avoided by making auxiliary feedwater not susceptible to single failure; providing an alternate means of determining reactor core water inventory; utilizing the system to measure water inventory to initiate HPI and keep it effective; and, detecting relief valves which fail to close. A systematic study of such improvements should be carried out to confirm the merits of their implementation in the long term. In the mean time, the NRC recently developed requirements should help reduce the probability and consequences of TMI-2 type accidents.

4. It is recommended that the present licensing process, which defines specific sets of accidents to be analyzed, to complemented with quantitative safety goals to be satisfied and a rigorous safety evaluation method to show that they have been met. As illustrated in this study for loss of coolant accidents, a safety goal could be defined for the degree of fuel failure to be allowed versus probability. All initiating events, including malfunctions and operator actions could then be evaluated against this safety goal. In implementing such a method and safety goal, it is important that they not be defined so accurately that the safety evaluations primarily become a "numbers game".

4.3 Design Margins

4.3.1 Background

Because one effective way of achieving safety is to provide adequate design margins, considerable emphasis has been put in this area in light water reactors. One outstanding example is the development of ASME codes for nuclear components and of stress calculation models to assure that sufficient structural margins have been provided; not only for normal conditions, but for transients, and such emergency conditions as earthquakes and rare natural disasters. In this section, one cannot deal with all design margins (stress, reactivity, ... etc.) thus the focus will be placed only upon those design margins which are relevant to the TMI-2 accident. They are essentially the margins provided in:

1. peak fuel duty (kw/ft), or peak heat transfer rate from fuel to coolant. This margin determines the degree to which fuel rods may fail during transients and accidents from excessive stresses upon the cladding.
2. critical heat flux (CHF) or departure from nucleate boiling (DNB). These margins determine to what degree the fuel rods can avoid a sudden decrease in heat removal capability on the water side. As the heat transfer from fuel to water is increased, the fuel rod can reach the point where the fuel surface is completely blanketed with steam and the heat transfer rate from cladding to water decreases significantly; when this occurs, the cladding surface temperature rises well above its normal value.

3. peak clad temperature during a loss of coolant. This margin determines to what degree fuel rods during a LOCA might be subjected to failure from overheating and metal-water chemical reaction with the ensuing release of hydrogen.

The technical specifications for each nuclear plant provide maximum allowable values for peak fuel duty and peak clad temperature during a LOCA. They also specify a power or heat flux ratio to be maintained to avoid CHF or DNB.

The peak fuel duty not only specifies the peak heat flux from the fuel rod for a specified fuel geometry, but it also determines the maximum UO_2 fuel temperature. Peak fuel duty is important because it establishes the heat stored within the fuel at the start of an accident as well as the margin to CHF or DNB. Peak fuel duty has been found to be important to fuel life because it has an important role in determining the stress interaction between fuel pellets and zircaloy cladding. Higher fuel duty causes greater pellet clad interaction during transients and maneuvers; higher fuel duty also causes a greater number of fuel failures, which is kept as small as possible before fuel discharge.

The critical heat flux (CHF) or departure from nucleate boiling (DNB) produce cladding surface temperatures which are high enough to lead to cladding failure if sustained for a sufficient time at high power levels. Also, if the CHF/DNB condition can be delayed during the initial stages of an accident, the amount of heat which is stored in the fuel is reduced,

thereby reducing the amount of heat which needs to be coped with in subsequent stages of the accident. CHF and DNB conditions are determined in out-of-reactor heat transfer facilities where electrical heating is used to simulate nuclear power production. These tests are performed at prototypical conditions of water flow and pressure and with prototypical geometrical arrangements.

The peak allowable clad fuel temperature during a LOCA has been established through in-reactor and out-of-reactor tests which determine the start of cladding failure, geometry distortion and amount of zircaloy-water reaction. The peak allowable clad temperature is set with the objective of preserving a sufficient margin to a coolable geometry. In the Technical Specifications for each plant it is expressed in terms of a fuel maximum average power linear heat generation rate which would produce temperatures in excess of 2200°F if it were exceeded for the design basis accident.

4.3.2 Findings and Recommendations

1. Design margins have varied with time as knowledge about the related phenomena increased. Design margin trends in three key areas can be summarized as follows between the 1960s and 1970s:

Peak Fuel Duty Margins	Up
CHF or DNB Margins	Down
Peak Clad Temperature Margins	Up

2. In the case of peak fuel duty, the designs of the 1950s employed a peak value of about 10 kw/ft. This value increased up to about 18 kw/ft in the sixties as efforts were made to increase the power production per unit volume of reactor. In the seventies, the peak

fuel duty was lowered back to about 14 kw/ft. This was brought about by the new conservative Appendix K requirements for the LOCA. This reduction in peak fuel duty was also beneficial in reducing the number of fuel failures during normal operations.

3. In the case of CHF or DNB, both the curves defining CHF or DNB have been raised and the margins to CHF or DNB lowered. These changes have resulted for many reasons. In the sixties, CHF or DNB were defined from simplified, non-prototypical tests and additional margins were provided to account for uncertainties in extrapolating such information. By the end of the sixties, complete prototypical tests with non-uniform power distributions were carried out and the number of test points for such geometries became statistically significant, allowing the introduction of improved correlations. Also, probabilistic analysis was employed to take into account uncertainties in the test data and reactor power distributions. Present designs provide 95% probability with 95% confidence of not experiencing CHF or DNB. Considerable operating experience has been acquired to-date and it supports the latest bases.

4. The peak clad temperature during a LOCA was originally set at about 3400°F. It was lowered first to 2300°F, then with the issuance of Appendix K, this limit was reduced to 2200°F. In addition, conservative assumptions were introduced in the analyses so that the net impact of adding margin was, in fact, considerably improved. Many reports have been published to quantify ^{the} conservatism in the

analysis and to compare best estimate values of peak temperature versus the maximum allowable value of 2200^oF. The best estimates fall between about 1200 and 1500^oF.*

3
5. A systematic study of design margins of one reactor type versus another has never been made. Safety margins are evaluated against requirements in the licensing process and all reactors satisfy the requirements relatively equally. The only comprehensive comparative study performed to date is the probabilistic Nuclear Reactor Safety Study and the different plant results fall well within the uncertainties of the methods. Most recently, the NRC has carried out comparative studies for Anticipated Transients Without Scram (ATWS), and for Feed-water Loss Accidents in PWR reactors. Such studies are useful in defining weaknesses and potential improvements (see Section 4.4) and it might be advantageous to extend such comparisons to other areas.

6. The course of events at TMI-2 would not have been changed considerably or the consequences seriously reduced if the design margins at TMI-2 had been greater.

7. While there are strong capital and fuel cycle cost pressures to reduce margins, there are also strong pressures to provide sufficient margins to achieve reliable plant operation and to satisfy the Technical Specification safety limits.

8. No recommendations are made in this area.

*General Electric Report NEDM 21761, October 1977.

STAFF DRAFT CONFIDENTIAL
NOT FOR DISTRIBUTION

4.4 Equipment Margins

4.4.1 Discussion

One way of assessing safety margins is to compare the equipment of different manufacturer's designs for safety systems parameters such as flow rate, pump shutoff head, number of components, etc. Table 5 is a summary of these key parameters which was presented in NUREG-0560 "Staff Report on the Generic Assessment of Feedwater Transients in B&W PWRs" (May 1979). In this table, similar sized plants of the three PWR manufacturers are compared by listing key components which affect safety.


One of the key uniquenesses of B&W reactors is that B&W uses a Once Through Steam Generator (OTSG) which is a factor of 2 to 4 smaller than an equivalent U-tube steam generator. This is reflected in the table under the parameter identified with note . The B&W reactor has about 1/2 full power minute to boil the steam generator dry, while the other vendors have one to two full power minutes. The smaller steam generator (OTSG) can be a disadvantage for some transients because it has less ability to ride through sudden drops in power demand without lifting safety or relief valves (see Table 6, taken from NUREG-0560). On the whole, however, the smaller steam generator volume of the B&W plant does not seem to be a significant contributor to plant safety margins, since many of the limiting transients are longer in duration than one minute anyway (e.g. loss of feedwater combined with loss of auxiliary feedwater). The biggest effect of a small steam generator on safety margin is the greater propensity of the B&W plant to lift relief valves, which may then fail in the stuck open position,

Table 5 - COMPARISON OF KEY CHARACTERISTICS OF OPERATING B&W PLANTS
WITH C-E and W PLANTS FOR THE LOSS OF FEEDWATER TRANSIENT

Characteristic	B&W	W		C-E	
	TMI-2	IP-3	D.C. Cook	Palisades	Millstone 2
Thermal rating, MW+	2772	3025	3250	2530	2560
Trip from secondary	No	Yes	Yes	Yes	Yes
Rx press trip, psig*	2355	2385	2385	2240	2385
RCS volume, ft ³ x 10 ⁻³	11.5	11.3	12.6	10.9	10.8
Pressurizer vol./RCS vol.	0.13	0.15	0.14	0.14	0.14
2 PORV capacity, lb/hr MW	40.4	118.	194	121	119
Set point, psig*	2255	2335	2335	2385	2385
Oper. margin, psi	70	100	100	150	150
2 SV capacity, lb/hr Mwt	249	416	388	272	231
Low set point, psig	2450	2485	2485	2485	2485
1 Steam gen., minutes to inventory, boil-off @ FP	0.45	1.22	1.17	1.55	1.94
Aux. FW cap motor	2@ 2.0ea	2.@1.3ea	2@1.6ea	1@1.53	2@1.1
% of design rating turbine	1@3.8	1@2.6	1@3.2	1@1.53	1@2.2
4 High-press inject/dead head, psi	2820	1463	1560/2590	1214	1192
Charging cap gpm @ des. press.	2@300 ea	0	400/150	300	
gpm @ 1600 psig	2@450 ea	0	0/	0	
3 RCP vapor trap geom	Yes	No	No	No	No
Hot leg/S.G. vapor trap geom	Yes	No	No	No	
Pressurizer loop seal geom	Yes	No	No	No	
5 Internals vent valves	Yes	No	No	No	

*To be revised per IE Bulletin 79-05B

TABLE 6

SUSCEPTIBILITY TO PORV VALVE LIFT FOR B&W, C-E, AND W PWRs
AS A RESULT OF A LOSS OF FEEDWATER EVENT

Susceptibility to PORV Valve Lift*

NSSS <u>Supplier</u>	<u>Before Reactor Trip</u>		<u>After Reactor Trip</u>	
	<u>Aux. Feed</u>	<u>No Aux. Feed</u>	<u>Aux. Feed Immediately</u>	<u>Aux. Feed after 10. min.</u>
B&W	Very high	Very high	low	Very high
C-E	Very low	Very low	Very low	Low
<u>W</u>	Very low	Very low	Very low	Low

*These findings are subject to reconsideration following licensee actions in response to IE Bulletin 70-05A and shutdown of the B&W plants.

thereby generating an equivalent small pipe break and the potential for a situation similar to the one at Three Mile Island. Another impact of the B&W design is to about cut in half the time available to operators to take action; this could become important if the reactor is tripped early. On the other hand, in many cases the issue will be whether the operator took the right action rather than the amount of time he had to do it in.

The safety valve and relief valve capacity of the B&W plant (identified by $\diamond 2$ on Table 5) is a factor of 2 to 4 lower than the other two PWR suppliers. This capacity difference can result in increased pressures in the primary system when the steam generators are disabled, or in degraded situations such as Anticipated Transients Without Scram.

Table 7, from NUREG-0460, Volume 1, "Anticipated Transients Without Scram for Light Water Reactors" (Dec. 1978), demonstrates this sensitivity with the high pressures associated with the ATWS event for both Combustion Engineering and Babcock & Wilcox designs. The combined relief and safety valve capacity of these plants is much less than the Westinghouse plant.

The combined safety and relief valve capacity of the TMI design is $(280,000 + 280,000 + 110,000)$ 670,000 lb/hr from two safety valves and one relief valve. If the decay heat is all converted into steam (i.e., no heat transfer in the steam generator), the steam generation rate at various times is: 1,098,000 lb/hr at 10 seconds, 870,000 lb/hr at 40 seconds, and 726,000 lb/hr at 100 seconds. Since Table 5 shows that the TMI-2 steam generator has 0.45 full power minutes, or 27 full power seconds, it appears that the combined safety and relief valve capacity relies heavily on the steam generators to take up a good share of the

TABLE 7


Summary of PWR Analyses

<u>Vendor</u>	<u>ATWS Event</u>	<u>Peak Reactor Pressure, psia</u>
Westinghouse	Loss of load with one relief valve failed	3197 (system pressure)
Combustion Engr. 2560 Mwt	Loss of feedwater with one relief valve failed	4508 (pressurizer pressure)
3800Mwt	Loss of feedwater	4087 (pressurizer pressure)
Babcock & Wilcox 148 FA	Loss of feedwater with one relief valve failed	5004 (core outlet pressure)
177 FA 205 FA	"	4978 (" " " ")
3600Mwt	"	4555 (" " " ")
3800Mwt	"	4372 (" " " ")
Limit	—	3200

energy removal during the early period shortly after scram. If a safety or relief valve were to fail shut, the steam generation rate would be greatly in excess of the steam discharge rate, which will cause rapid system pressure increases. Assuming a constant latent heat of vaporization for simplicity, and the failure of one safety valve, and making the very severe assumption that the steam generators were not available to remove energy after 30 seconds, the reactor pressure at 40 seconds would be over 5000 psi, and at 100 seconds, over 4000 psi. These pressures are clearly well in excess of the rating of the system. Thus it appears that the margins associated with the system pressure and the number of relief valves may be low, and merits some further study to assess whether some action to add margin should be taken. Also, in a footnote at the end of section 4.2.3, it was pointed out that failure of the PORV to open together with loss of auxiliary feedwater could lead to loss of primary coolant inventory with HPI not being effective. This suggests the need at least of redundancy in PORV valves.

Another design aspect where margins appear to be different among the three suppliers is in the presence of vapor traps in the primary system, which can impede natural circulation. Table 5 shows that B&W has vapor traps in both the hot leg and the reactor coolant pumps (see note 3), whereas the other two vendors do not. This certainly can make the once through steam generator (OTSG) design somewhat less desirable from a natural circulation standpoint. However, it is not so much the presence of vapor at the top of the hot leg (see Figure 25 and 26) which is important, as the presence of non-condensibles and what they would do to impede natural circulation. Non-condensibles can collect at the top of the U-tubes in a

U-tube steam generator and impede natural circulation the same way as they would at the top of the hot leg in an OTSG. Furthermore, the OTSG actually has the potential for having better natural circulation qualities of the U-tube steam generator since the location of the "equivalent cold point" can be raised by raising the water level on the secondary side, while this has no effect on the "equivalent cold point" of the U-tube steam generator. (The "effective cold point" is the place in the steam generator where you would get the same natural circulation if you assumed all the heat were transferred at that point, as you get by distributing the heat transfer over the actual region where it occurs.) A U-tube steam generator layout looks much like the advanced OTSG design shown in Figure 26. The effective cold point is at about the same elevation as the control rod drive flanges (8 feet above the reactor vessel head parting line). Even in the early version of OTSG, the effective cold point can be raised to near the top of the OTSG (see Figure 25) which gives it better natural circulation properties than the U-tube steam generator. Of course, the advanced OTSG shown in Figure 26 can also raise the effective cold point to the top of the OTSG, and get even greater natural circulation driving heads than the earlier version because of their elevated location. Both the U-tube steam generator and the elevated OTSG have the safety advantage of having more liquid above the core to drain down in an emergency.

Another important measure of equipment-related safety margins is in the shutoff head and flow rate of ECCS pumps (see note ). Some designs have a pump shutoff head capable of pumping into the system at high pressure (TMI-2 and D. C. Cook), while others must rely on another system (Power Operated Relief Valve (PORV) or steam generator) to bring the pressure down to have HPI function (Indian Point-3, Palisades, Millstone-2). Clearly, the

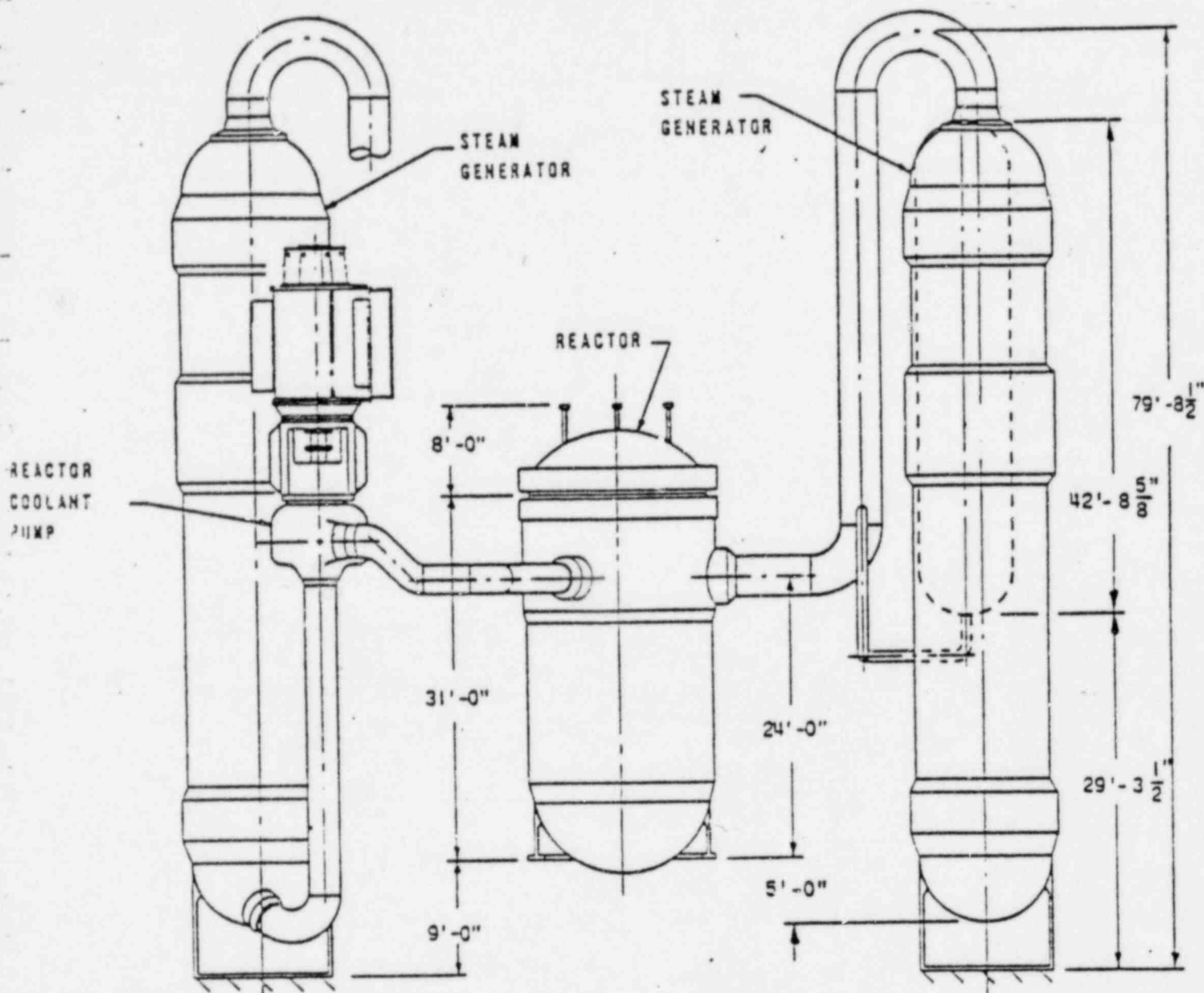


Figure 25. - Reactor Coolant System Arrangement - Elevation, from Three Mile Island, Unit 2, FSAR.

SLI-7904

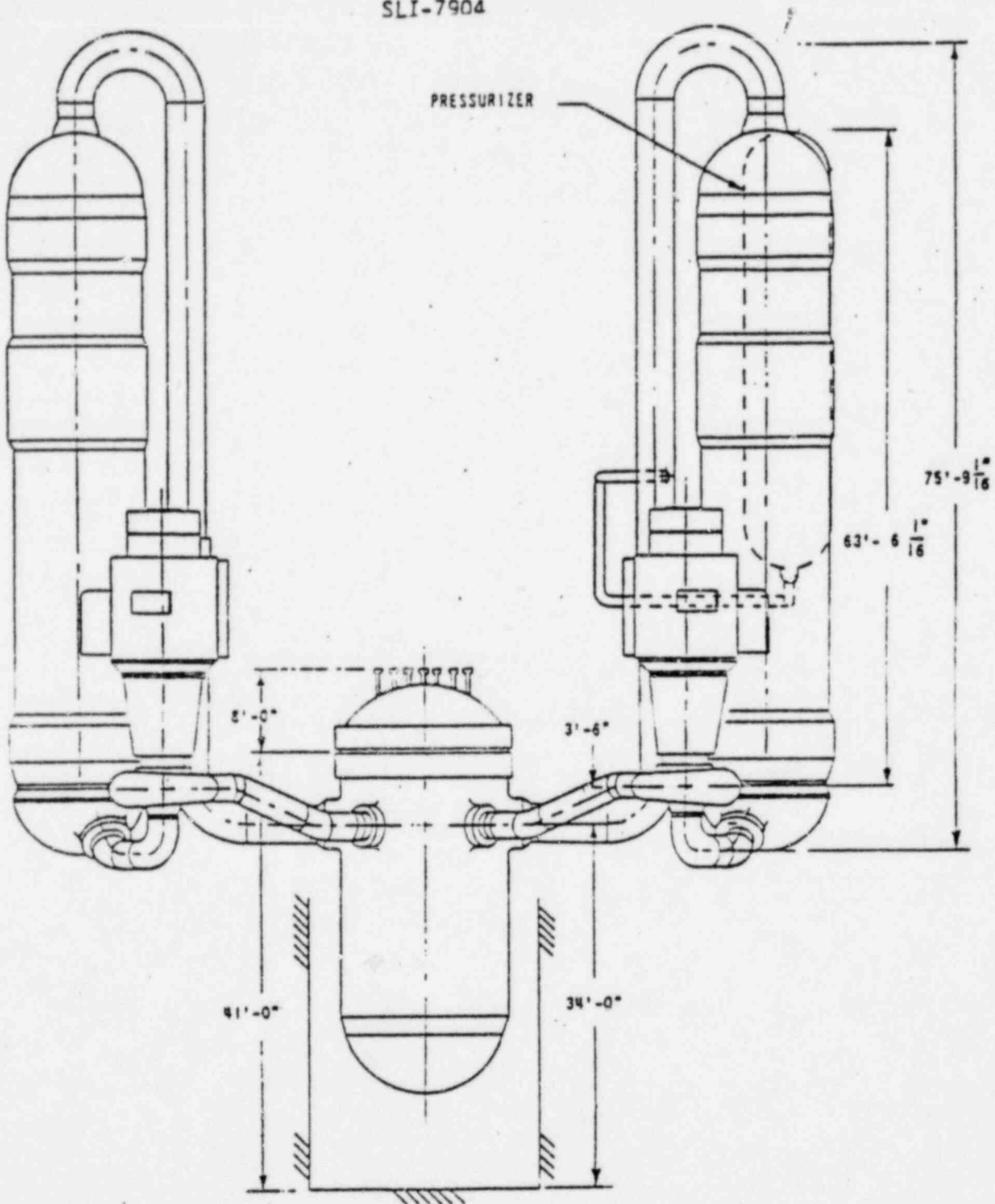


Figure 26 - Reactor Coolant System Arrangement - Elevation, from Davis-Besse, Unit 1, FSAR.

plants having the higher HPI shutoff head have the greatest design margin, since in the situation in which the steam generators are not functioning, it only takes the additional failure of the PORV to disable all means of removing decay heat from the primary system. This situation should be studied to assess its importance and the proper steps taken, should a remedy be required.

The B&W plant has internal vent valves (see note 5 on Table 5) which provide an extra degree of safety margin for the loss of coolant accident, or for other unanticipated accidents for which pressure differences in the reactor vessel could cause a degradation of core heat transfer. Such vent valves would not permit gas to accumulate in top of reactor.

4.4.2 Conclusions

As the preceding discussion illustrates, the amount of margin differs in detail from one design to another, but overall, the margins appear to be about equivalent. This is especially true when considering the licensing basis, since the plants are all designed to meet the same safety criteria. The Three Mile Island accident placed the focus on some Babcock & Wilcox design shortcomings (less steam generator thermal capacity, fewer relief valves, loop seal on pressurizer surge line, control room information which is potentially confusing, poor natural circulation with low water level on the secondary side of the steam generator). On the other hand, the B&W plant has some positive aspects (high shutoff head HPI, vent valves, good natural circulation properties when water level is high, internal vent valves, less steam release from a secondary steam break). On the whole, the safety margins of the PWR designs appear to be roughly equivalent, but also appear to have the capability for improvements with some modest changes.

4.4.3 Recommendations

With respect to equipment margins, if it is deemed necessary to improve them, the following should be considered:

1. Eliminate loop seals on pressurizer surge lines.
2. Double the PORV capacity, if possible, on those plants with small capacity. *(even if it makes the TMI-2 accident happen faster?)*
3. Install a vent at the high point of the primary system. - *not discussed*
4. Use only the raised steam generator configuration in future designs.
5. Incorporate other means of improving natural circulation characteristics, such as automatically raising OTSG secondary side steam generator water level during shutdowns.
6. Raise the HPI shutoff head to the level of the safety valve setting for future designs.
7. Improve the control room information to simplify the operator's decision making.

5.0 COMMUNICATION LINK TO REMOTE CENTERS

5.1 Concept - This concept is to establish a formal communications link between each reactor and a central location such as NRC headquarters in Bethesda. This communication link would be continuous and would, therefore, be in place and operating in case of a crisis, such as the one at Three Mile Island. The primary role of the communication link during a crisis would be to transmit technical data to the center from the stricken nuclear power station, and to communicate advice from the center.

Since the type of data needed at a remote center is the same type of data which would be processed and ready for display on the safety information interpretation system described in paragraph 3.2 of this report, it would be a logical extension of this system's role to also telemeter the same safety diagnostic information to the remote center, where it could be displayed in the same manner as at the reactor site. This information could easily be transmitted over a normal telephone line, with a second dedicated line available for voice communication.

5.2 Applicability - This concept is primarily directed at the interface between the utility at the power station and the NRC. However, the same telecommunication link, if it were standardized could be used to transmit

the data during a crisis to the reactor vendor's headquarters, national laboratories and other participants in the recovery from an emergency.

5.3 Feasibility - The transmission of the previously prepared information from the reactor site to a central location is no more difficult than transmitting to another location on the power plant site. All that is needed is a telephone line and compatible equipment at the receiving location. This kind of information communication has been done routinely by the telephone companies for many years.

5.4 Implementation Schedule - The primary determinant of the schedule for implementing this communication link is the engineering of the terminal at the reactor site for processing the information prior to transmission. If the data interpretation system which was described in paragraph 3.2 were used as the sending unit, it would require about 18 months to design and manufacture the equipment, and no additional time for the telecommunication. Obviously, a dedicated telephone line for voice communication with the site from a central location would not affect schedule either, and could be implemented immediately.

5.5 Merit - The difficulty of communicating with the reactor site at Three Mile Island demonstrated the importance of having a good communication system. If the information system described here were implemented, it would make it possible for outside experts to assist reactor sites in the time of need, and

should result in an improvement in safety. For this reason, this system and a dedicated telephone line for voice communication should have a high priority, especially if the data interpretation system exists, since the cost of communicating the information to the central location is very low.

6.0 APPLICATION OF AEROSPACE TECHNIQUES TO NUCLEAR SAFETY

6.1 Concept - Part of the mission of this study was to review simulator technology to assess whether there are opportunities to improve nuclear simulation through the use of aerospace techniques. A by-product of the review of aerospace technology was the discovery of techniques other than simulation which should be considered for application to nuclear power. There are three aspects of aerospace technology which appear to have a potential application to the nuclear power industry:

1. The use of computerization to simplify and enhance control room design and even control room procedures.
2. The use of logic diagrams in place of written procedures for response to equipment failure or malfunction.
3. The use of flight recorders to record key data and conversations at the time of an accident.

Control room computerization is a trend already begun by the nuclear industry with their advanced control room designs, such as General Electric's Nuclenet, and others. However, the degree of computerization in these advanced control rooms is still well below the level possible with miniaturized computers, and visual techniques developed by the aerospace industry. For example, if the emergency procedures were stored in a computerized memory, with display on a CRT screen instead of a long row of books, access to them would be simplified during an emergency. In addition, keeping these procedures up to date could be done electronically, so that the procedures are easier to keep current. The technical specifications for a plant could be computerized so that when a tech spec limit is being approached or violated, the information would be flashed on a CRT screen.

The aerospace industry uses logic diagrams instead of written text for emergency procedures related to equipment malfunction. Logic diagrams can condense the number of pages written such that six or seven pages of written material can be replaced with one logic diagram. This approach also eliminates the need for skipping back and forth in the text, depending on the nature of the specific failure. The Houston Space Center uses this technique for their Malfunction Procedure Documents, and has found that operator acceptance of this form of procedure documentation is very high.

Flight recorders in airplane cockpits have been used for many years as a tool for reconstructing airplane accidents after the fact in order to diagnose their cause. An analogous system is used by all nuclear reactor suppliers during pre-op and startup testing to record data. These systems (B&W's Reactimeter, General Electric's Star Track) typically record continuously, and save the previous twenty seconds or so, when triggered by a "start" signal, and then continuously record pre-selected variables, once the device is triggered. These systems are available for permanent installation at the utilities' option, but are usually removed shortly after the plant goes into commercial operation. Fortunately, the Babcock and Wilcox Reactimeter was still operating at the Three Mile Island-2 site, and provided a great deal of information as to the true nature of the accident.

6.2 Applicability - The three concepts discussed above are all applicable to the electric utility owner for use in the control room of a nuclear power plant.

6.3 Feasibility - The use of computers to simplify and enhance control room information for better operator understanding is a concept which can be implemented with existing state-of-the-art hardware. It would require only engineering to make it applicable to nuclear control room design, with no significant cost increase over standard control room designs.

The use of logic diagrams for emergency procedures is feasible to implement right away, once the decision is made to do it. Before it is done, a detailed study should be performed to decide which procedures should use logic diagrams and which ones should remain unchanged.

The use of accident monitoring systems in a nuclear control room, to automatically record plant data in the event of an accident is feasible. It would require the electric utility to pay to keep the recorder which is normally on site for pre-op and startup tests. The cost of these devices is in the range of \$300,000 to \$500,000.

6.4 Implementation Schedule - The schedule for implementation of computerized control rooms is very long. For practical reasons, it probably would not be applied in greater degree than current advanced control rooms, to any plants already sold. It would thus be applied to plants as yet unsold, which means it would be ten to fifteen years before these control rooms would be used at an operating plant. However, it is possible for the concept to be applied to small portions of the control room in two to three years, as discussed in paragraph 3.2.

The schedule for implementation of logic diagrams for emergency procedures is only limited by manpower. It is feasible to apply these right away, and develop the first procedures in a matter of a few months.

The schedule for implementation of accident monitoring (such as the B&W Reactimeter) is also very short. It can be immediate at those plants which are in the startup phase and, therefore, already have them on site. For those plants which are operating without them, a one year delivery schedule is probably a reasonable schedule to expect.

6.5 Merit - All three of these concepts from aerospace application would probably have a beneficial effect on nuclear plant safety. With time, computerized control rooms are probably going to become the standard of industry since the industry is already moving in that direction. This tendency should be encouraged and accelerated by the industry and NRC. Accident monitoring systems (such as the B&W Reactimeter) are a very desirable accident diagnostic tool, and could be used to gather other data which would be gathered during normally expected upset conditions, as well as collecting data during a once-in-a-lifetime emergency. Therefore, this type of system should be given high priority for implementation at all reactor sites: planned, under construction, and operating.

APPENDIX ILIST OF MEETINGS BY S. LEVY INCORPORATED PERSONNEL

1. July 2, 1979 S. Levy, E. D. Fuller and J. Hench met with A. Cook, NASA Ames to review the Ames flight simulator.
2. July 5, 1979 S. Levy, J. E. Hench and E. D. Fuller met with I. Stuart, J. Cox, J. Miller, R. Davison, J. Duncan of General Electric at the GE office in San Jose to discuss General Electric nuclear simulation.
3. July 10, 1979 S. Levy, J. E. Hench and E. D. Fuller met with GE engineers to discuss transient analysis and loss of coolant models. GE attendees: G. Scatena, A. Rao, G. Sozzi, J. Dolence, A. Burgess, K. Holland, B. Shiralkar, E. Wood, R. Linford, J. Duncan, G. Eckert, D. Wilkins.
4. July 13, 1979 S. Levy and E. D. Fuller met with P. Oubre' and others of Sacramento Municipal Utility District at the Rancho Seco reactor site to discuss the operator's view of nuclear simulators.
5. July 16, 1979 S. Levy and E. D. Fuller met with EAI in the S. Levy offices to discuss current simulator capabilities. EAI attendees: R. W. Maslo and R. A. Meermous.
6. July 17, 1979 S. Levy, J. E. Hench, R. English and L. Jaffe met with Gus Wanner and Ron Poe of Singer-Link at the Singer-Link facility in Silver Springs, Md. to discuss current simulator capabilities.