



UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
WASHINGTON, D. C. 20555

NRC PUBLIC DOCUMENT ROOM

AUG 27 1979

Generic Task No. A-17

MEMORANDUM FOR: S. H. Hanauer, Director, Unresolved Safety Issues Program

FROM: J. Angelo, Task Manager, Task A-17, Systems Interaction in Nuclear Power Plants

SUBJECT: SUMMARY OF MEETING WITH SANDIA LABORATORIES ON AUGUST 8-9, 1979 TO DISCUSS TASK A-17

On August 8-9, 1979 members of the NRC staff met with representatives of Sandia Laboratories in Albuquerque, NM to discuss the series of fault trees which depict the reactor coolant pressure boundary safety function which is one of three safety functions being investigated in Generic Task A-17. Persons who attended the meeting are listed in Enclosure 1 to this summary report. The significant items discussed at the meeting are summarized in the following paragraphs of this report.

1. Operator Actions

While we did not specifically include operator actions as basic events in the fault trees, nevertheless there are a number of events that are more likely to be the result of operator actions than automatic controls. The situation may be further compounded by the fact that the valve may be initially in the faulted position at the start of the occurrence, or may be initially in the success position. There are also a large number of manual valves that are placed in the locked-open or locked-closed position. There are also a number of manual by-pass valves around automatic valves that are normally in the closed position. Sandia Laboratories can manipulate the computer code for evaluating fault trees to discriminate these kinds of events by inputting either unity or zero at that particular logic gate. Sandia Laboratories intends to revise the fault trees as necessary so that these situations are treated as uniformly as possible.

2. Reactor Coolant System Overpressurization

The fault tree for reactor coolant system overpressurization does not presently include the loss of heat removal events that can potentially cause overpressurization. The reason for this is that the loss of heat sink is treated in the decay heat removal function as an event that can lead to the top event of the fault trees by itself, regardless of the overpressurization. Sandia Laboratories explained that this cause of

905 208

790926 0238

AUG 27 1979

overpressurization can be added to the fault trees but would not achieve any meaningful differences in the analysis of the events. Subsequent to this meeting, the NRC staff members had further discussion with the conclusion that the overpressurization caused by insufficient heat removal should be depicted in the fault tree. We have informed Sandia Laboratories of this conclusion subsequent to this meeting, and we are prepared to discuss this matter at a future meeting with Sandia Laboratories.

### 3. Event Trees

During the course of this task performance, the question has been raised regarding the relative merits of using event trees to supplement the fault trees. Sandia Laboratories has constructed event trees for the RCPB function and has verified that failure paths in the event trees have a corresponding branch in the fault trees. We have found it advantageous to use the event trees as a means of following the fault trees with greater ease of understanding. Sandia Laboratories will include event trees in their next interim report which is scheduled for completion in September 1979.

### 4. Loss of Reactor Coolant Pressure Boundary

We decided early in this program to exclude loss-of-coolant accidents and mitigating systems for these accidents. We did, however, include systems interactions that could potentially lead to loss-of-coolant accidents, for example, by overpressurization of the reactor coolant system and overpressurization of systems connected to the reactor coolant system. We made a definition that the loss of reactor coolant boundary occurs when the potential loss of coolant exceeds the capacity of the normal makeup or charging system. On reconsideration of this definition we agree with Sandia Laboratories that events which have the potential of creating a non-normal leakage or flow path for the reactor coolant should be developed in the reactor coolant pressure boundary fault trees, whereas events that occur in normal leakage or flow paths are best depicted in the decay heat removal fault trees under a sub-function identified as "loss of coolant inventory." The principal reason for this arrangement of fault tree branches is that it is difficult to distinguish when a particular fault (such as a failed check valve, for example) may lead to a loss of reactor coolant which exceeds normal charging capacity.

### 5. Evaluation and Analysis of Fault Trees

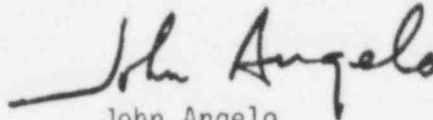
Work is currently in progress on the evaluation and analysis of the reactor coolant pressure boundary fault trees using the Set Equation Transformation System (SETS) computer code. Sandia expects to complete this analysis by early September 1979 at which time we plan to meet with Sandia Laboratories to discuss the analysis results and methods.

905 209

AUG 27 1979

6. Specific Comments on the Fault Trees

In addition to the more generalized discussions summarized in the paragraphs above, we discussed some specific comments on the fault trees and left Sandia Laboratories with a list of these comments for their further consideration. These comments are shown in Enclosure 2 to this summary report.



John Angelo  
Task Manager  
Generic Task A-17

Enclosures:

1. Attendance List
2. Comments on Fault Trees

cc: J. Hickman/W. Cramond  
Division 4412  
Sandia Laboratories  
P. O. Box 5800  
Albuquerque, NM 87185

905 210

7. On page 4 (far left), under "Boric Acid Transfer Pump 1 Output Diverted", one input to the OR gate is entitled "Bat A Return Line AOV 1 Fails Open". It appears that a normally closed manual valve is installed in this line. Therefore, the fault tree should be modified to account for the required failure of this manual valve.
8. On page 4, the subtree, "Failure of Both Normal and Aux Pressurizer Sprays," appears incomplete. The failure of normal spray capability through mechanical failure or loss of the reactor coolant pumping power has not been addressed.
9. On page 5 (far left), under "Centrifugal Charging Pump Trains or Letdown Fails", the input for insufficient letdown is in error. The input should concern insufficient letdown for the centrifugal charging pumps, not the positive displacement pump.

POOR ORIGINAL

905 211

dump is delivering high flow, the failure of the excess letdown line is not necessary. Therefore, the OR gate shown in the subtree should have only two inputs, "Charging pump Output Flow Control Valve Fails Open" and "Normal Letdown Path Fails Closed".

5. The conditional gates shown for the Overpressure Cases appear to have the wrong pressure value in some instances. Where applicable, the valves should be changed to correspond to the correct PORV and safety valve settings, and Safety Injection pump design pressure.
6. On page 5, under the subtree, "Excess Letdown Path Fails Closed," two inputs, "Seal Flow Return Line Filter Manual Bypass Valve Not Opened" and "Seal Water Heat Exchanger Bypass Valve Not Opened," involve human error. Since the scope of the study excludes human error, these inputs should be restated to assume a mechanical failure. The exclusion of human error can be accomplished by one of the two following methods:
  - (1) the operator is assumed to perform every possible correct action on time and following the correct sequence in an attempt to achieve a safe plant condition, or
  - (2) the operator is assumed to perform absolutely no action whatsoever and the plant reacts independently.

I believe that the latter method is more realistic. In either case, the fault trees should be conceived and structured consistent with the method which is selected.

POOR ORIGINAL

905 212

Comments on the Fault Tree for the Reactor Coolant Pressure Boundary (RCPB) Safety Function (Figure 5.3-7, dated July 2, 1979)

POOR ORIGINAL

1. The RHR system is normally operating to provide for decay heat removal in the cold shutdown mode. Therefore, if pressure rises to 600 psig, the RHR system will be automatically isolated. If not, failure of RHR piping or opening of a relief valve would cause a RCPB failure. This system has not been addressed in the fault tree.

2. The fault tree utilizes a conditional gate to address the probability of a RCPB failure given a certain pressure. This pressure is unrealistic in some cases since the pressure will be limited by much lower piping design pressures. For example, in Overpressure Case 1, it is possible for the pressure to be limited by the normal letdown design pressure of 600 psig or the excess letdown design pressure of 150 psig. In either instance, the pressure would never reach the conditional gate value of 2000 psig.

This same situation is also, present in Overpressure Cases 3, 5, 6, 12, and 13.

3. The fault tree indicates that Primary Water Supply is available under all conditions. In previous versions of the DHR, RS, and Loss of RCPB fault trees, primary water was assumed unavailable for a loss of off-site power condition. The fault trees should be mutually consistent.

4. On page 3, under the subtree, "Insufficient Letdown Compensate for CCPS", three inputs are shown necessary to achieve an insufficient letdown situation at charging minimum flow. Actually, if normal letdown is inoperable and a charging

Valve Not Opened" and "Seal Water Heat Exchanges Bypass Valve Not Opened," involve human error. These should be restructured to assume a mechanical failure.

6. On page 4 (right), the subtrees, "Excess Letdown Path Fails Closed" and "Normal Letdown Path Fails Closed other than Flow Control Orifices," contain situations where letdown flow is blocked by low design pressure components. This would prevent the reactor pressure from reaching the pressure value assumed in the overpressure cases.

**POOR ORIGINAL**

7. On page 6 (left), the subtree "Alternate Coolant Source Available" utilizes an "AND" gate for the three inputs depicting possible water sources. Actually, the RWST or Primary Water Supply would be capable of providing sufficient supply. Therefore, the "AND" gate is not adequate and should be restructured.

In addition, three of the faults in the subtree involve human error and should be restructured to assume a mechanical failure.

Comments on the Fault Tree for Reactor Coolant Pressure Boundary (RCPB) Safety Function (Figure 5.3-2 dated 6/30/79)

1. The fault tree does not address the overpressure situation where a loss of feed-water causes an overpressurization of the RCS. This is a very common transient and, therefore, should be incorporated into the fault tree.
2. In Overpressure Cases 7 and 8, the reactor control system would respond and insert control rods to maintain a constant average reactor temperature. The transient would be stable when the heat output from the core was lowered such that the total heat output including the contribution from the RCP was nearly correct for that power level.

**POOR ORIGINAL**

Therefore, these two cases are not viable methods for RCS overpressurization.

3. On page 3 (far left), the subtree "Insufficient CVCS Letdown with Pump FCV at Min Flow" contains unnecessary inputs. If both the normal and excess letdown paths are closed, the other two inputs (FCV at minimum and contraction insufficient) are not necessary.
4. On page 4 (far left), under "Boric Acid Transfer Pump 1 Output Diverted," one input to the OR gate is entitled "Bat A Return Line AOV 1 Fails Open." It appears that a normally closed manual valve is installed in this line. Therefore, the fault tree should be modified to account for the required failure of this manual valve.
5. On page 4 (center), two basic events, "Seal Flow Return Line Filter Manual Bypass



7. Figure 5.3-5 WFT-CVCS-I

Under "Valve Failures on the Normal or Alternate CVCS Charging Lines," another input to the OR gate entitled "Valve Failures on the Auxiliary Spray Line" should be added. This would include the possible failure of the check valve and air operated valve in the auxiliary spray line.

8. Figure 5.3-5 WFT-CVCS-I

Under "Valve Failures on the Alternate CVCS Charging Line", an input to the AND gate is entitled "AOV in Alternate Charging Line Fails Open with Loss of Air". The possibility exists for the valve to functionally fail to the open position regardless of the status of the control air system. Therefore, the qualifier, "with Loss of Air", should be deleted.

9. Figure 5.3-5 WFT-CVCS-I

POOR ORIGINAL

The regenerative heat exchanger has not been included in this fault tree. The fact that the regenerative heat exchanger cross-connects both the charging and letdown lines makes it a prime source for a failure that could result in unacceptable core damage.

10. Figure 5.3-5 WFT-CVCS-I

Under "RCS Pressure Boundary Failure due to CVCS Normal Letdown Line", the inputs, "Letdown High Pressure Isolation Valves Fail Open" and "Letdown Relief Valve Fails to Open with Overpressure", are unnecessary. The blockage of flow downstream of the letdown orifice valves would result in an operating reactor pressure of 2235 psig being applied to the relief valve which has a setpoint of 600 psig. This situation would result in a loss of reactor coolant pressure boundary.

11. Figure 5.3-5 WFT-CVCS-I

Under "RCS Pressure Boundary Failure due to CVCS Excess Letdown Line," I have the following comments:

- a. To provide a flow path from the reactor coolant system such that a RCPB failure will result, the three excess letdown air operated valves must fail open. The failure of these valves should not be an input to an OR gate.
- b. The input, "Return Flow from Reactor Coolant Pump Seals", should be deleted. A fault tree should contain only failures, not events. In addition, return flow from the seals is normal and does not represent a failure.
- c. A more direct method of excess letdown line failure is the pathway resulting from the three air operated valves failing open and the three-way air operated valve failing such that flow is directed to the RCDT.

ENCLOSURE 2

Comments on the Fault Trees for Reactor Coolant  
Pressure Boundary (RCPB) Safety Function (dated 6/30/79)

1. Figure 5.3 GFT-RCPB-POHS

Under "RCS Pressure Boundary Failure due to Safety and Relief Valves", the fault, "Failure to Close Power Operated Relief Valve Isolation MOV", involves human error. This fault should be restated to specify a mechanical failure, since the scope of the study excludes the consideration of human error.

2. Figure 5.3-1 WFT-LOOPS-C-POHS

The fault tree indicates that a seal failure of any one reactor coolant pump will result in a RCPB failure. It should be noted that this RCPB failure will result in unacceptable core damage only if the charging system is unable to maintain reactor coolant inventory.

3. Figure 5.3-3 WFT-LPS-I-POHS

**POOR ORIGINAL**

The potential failure of the SI system if subjected to reactor operating pressure should be more completely addressed. The SI train relief valve setting is significantly lower than the normal operating reactor pressure. The operability or failure of this relief valve should be incorporated into the fault tree or the reasons for its absence should be explained separately.

4. Figure 5.3-3 WFT-LPS-I-POHS

The branch entitled "RCPB Fails thru the RHRS Return Path" is unclear. The normal plant design for PWRs utilizes a single line from one reactor coolant leg to the RHR system with two isolation valves in series.

The design which is most typical for operating power plants should be modeled to allow more widely applicable conclusions from the study.

5. Figure 5.3-5 WFT-CVCS-I

Under "High Pressure Flow from RCS Via Pump Seals to CVCS Pumps", the fault tree indicates that a seal failure must occur for reactor coolant to flow back into the charging line. The seal water is injected such that part of the flow travels up through the seals and the remainder flows down through the labyrinth thermal barrier and into the reactor coolant system. Therefore, a seal failure is not necessary to allow backflow into the charging lines.

6. Figure 5.3-5 WFT-CVCS-I

Under "CVCS Charging Pumps Fail to Prevent Reverse Flow", the fault tree contains an input entitled "Charging Pump Fails to Prevent Flow in the Reverse Direction". In actuality, the charging pump must be secured such that it is no longer providing charging flow.

ENCLOSURE 1

ATTENDANCE LIST

MEETING WITH SANDIA LABORATORIES

ON

AUGUST 8-9, 1979

GENERIC TASK NO. A-17

USNRC

D. C. Fischer  
T. G. Scarbrough  
J. Angelo  
J. M. Griesmeyer  
John A. Zwolinski

Sandia Laboratories

G. J. Kolb  
G. J. Boyd  
J. W. Hickman  
S. H. McAhren  
W. R. Cramond

POOR ORIGINAL