A Defense-in-Depth and Diversity Assessment of the GE ABWR Protection System

J. Palomar
G. Preckshot
R. Wyman

December 17, 1991
Version 2

Lawrence Livermore National Laboratory
Nuclear Systems Safety Program

DRAFT

Table of Contents

Table of Figures

A Defense-in-Depth and Diversity Assessment of the GE ABWR Protection System

1. Introduction

1.1 Sponsor

This assessment was conducted by Lawrence Livermore National Laboratory personnel at the direction of the NRC as part of Task 8 under FIN L-1867. The work was in support of the NRC's evaluation of the ALWR technologies. The work started on October 15, 1991, and a first draft of the report was submitted to the NRC on December 4, 1991.

1.2 Purpose

General Electric Corporation has submitted design information for the Advanced Boiling Water Reactor (ABWR) to the Nuclear Regulatory Commission for certification under 10CFR Part 52, Subpart B. The purpose of this report is to identify potential vulnerabilities with regard to defense-in-depth provided in the proposed ABWR protection system design which is part of that submittal (SAR Chapter 7). This analysis provides a detailed assessment of diversity and defense-in-depth for this design.

1.3 Executive Summary

This assessment is similar to that performed in NUREG-0493. The primary concern of the assessment is the possibility of a causal failure of more than one echelon of defense. This would result from some form of interdependence among echelons.

The three echelons of defense identified for the GE ABWR are control, scram and the engineered safety features actuation system. The objective of the assessment is to determine if postulated common-mode failures could result in impairment of more than one echelon thus compromising defense-in-depth.

The GE protection system was broken into blocks which are compatible with the architecture of the system and which allow an analysis to be performed according to the principles of the NUREG. Charts were developed which aid the analysis of common-mode-failures during design basis events. A number of assumptions were made to allow the analysis to proceed where data on the design was missing or inadequate. The charts and the assumptions made are fully documented in the report.

A number of vulnerabilities were identified. The design has both diversity and defense-in-depth in many cases but the consequences of certain postulated common-mode-failures in the digital units were found to result in inadequate defense-in-depth with respect to NUREG-0493 guidelines.

1.4 Background

Defense-in-depth is a principal of long standing for the design, construction and operation of nuclear reactors. For reactor I&C systems this has taken the form of three echelons: Control System, Reactor Protection System (RPS) and Engineered Safety Features Actuation System (ESFAS).

Two of these systems, RPS and ESFAS, are Class 1-E safety systems and are designated as the Protection System. The control system is not class 1-E. Because the control system is a non-safety system, no credit is allowed in a safety analysis for control system action and, in fact, the control system is assumed to challenge the protection systems by spurious or incorrect actions.

Diversity comes in several forms. Signal diversity is the availability of several different signals to initiate a protective action. For example, either high pressure or high reactivity, both of which occur for some events analyzed in this report, can initiate a scram of the reactor. Equipment diversity is the provision of several different methods for providing the same safety function. For example, for cooling the core of the ABWR, there is the Reactor Core Isolation Cooling (RCIC) system which uses a steam turbine driven pump to force water into the core in the event of a feedwater system failure, and there is the High Pressure Core Flooder (HPCF) which provides the same function with two electrically driven pumps. And finally there is diversity in defense-in-depth which provides different systems in each echelon to accomplish the same

function. For example, ATWS, which is part of the ABWR control system, will scram the reactor under certain circumstances, providing a redundant method of scram outside the RPS.

Analog systems employing defense-in-depth and diversity have comparatively long histories in reactor systems. The introduction of digital systems into protection systems adds a new level of complexity to these systems and introduces a potential for new common-mode failures which must be considered whenever a new protection system is proposed. In particular, the use of common software in the divisions of the safety system and in the control system provides a mechanism by which all protection divisions may fail simultaneously and cause the echelons of defense to be compromised. On the other hand, there are strong economic reasons using common software wherever possible, and this is encouraged by the notion that it is easier to verify and validate one software system and replicate it many times than to verify and validate many different systems. Thus diversity and defense-in-depth may be reduced in systems using digital elements.

One of the first formal assessments by the NRC of defense-in-depth for innovative technology was documented in NUREG-0493, "A Defense-In-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System," March, 1979. The method established in this NUREG is the basis for the assessment presented in this report.

1.5 Comparison of ABWR to GESSAR II

A review of GESSAR II protection system design and the ABWR SAR leads to the conclusion that the functional requirements for the ABWR protection system are substantially similar to those for GESSAR II. Further, it is also concluded that the reactor protection and engineered safety features actuation strategies are not fundamentally different for the two designs.

The significant difference with respect to defense-in-depth considerations is in the implementation of the functional requirements. The GESSAR II protection, control, and information systems are comprised of analog instrumentation; the proposed ABWR protection, control, and information systems are comprised of digital instrumentation. This section presents a brief summary of

differences in design implementation of the proposed ABWR instrumentation as compared to GESSAR II instrumentation previously reviewed.

Input sensor interfaces for the protection, control and information systems in the GESSAR II design are hardwired; in the ABWR design many of the inputs are multiplexed via fiber optic networks. Essential and non-essential multiplexer networks were identified by GE for protection, control, and information functions.

Outputs from the protection and control systems in the GESSAR II design are hardwired; in the ABWR design many of these outputs are multiplexed via the same fiber optic networks as used for inputs.

Protection logic is accomplished by hardwired logic in the GESSAR II design; protection logic is accomplished by software running on microprocessors in the ABWR design.

Control and information functions are accomplished by analog circuits and hardwired logic in the GESSAR II design; control functions are accomplished by software running on microprocessors and digital data networks in the ABWR design.

The potential for new common mode failure vulnerabilities that might result from this design evolution arises from the following differences in the ABWR design relative to GESSAR II:

1) Substantial reduction in the number of nuclear boiler system instruments accomplished by broad sharing of instruments for different systems and functions.

2) The use of identical software elements in the digital systems for protection functions in different divisions.

3) The use of identical software elements in the digital systems for both protection and control functions.

4) The use of hardware having more potential for vulnerability to electromagnetic interference (EMI) or surge.

5) The use of electronic hardware having increased thermal densities, therefore more sensitive to loss of HVAC (for example during a station blackout event).

Design and qualification measures must be identified to address these vulnerabilities. For example, the foregoing assumptions regarding identical software modules were made in the absence of any identifiable design requirements to the contrary, particularly in light of the applicant's standardization objectives.

2. The Scope of the Analysis

2.1 Those Items in the Scope of this Report

The protection system has two main units: The reactor protection system (RPS) and the engineered safety features actuation system (ESFAS). The function of RPS is to initiate the scram of the reactor automatically for all design basis events. This system is analyzed in detail.

The ESFAS has a number of subsystems, some of which are examined in detail. Those examined in detail are the emergency core cooling system (ECCS), the automatic depressurization system (ADS) and the leak detection and isolation system (LD&IS). Those systems which are given a more cursory examination (see Appendix B) are the wetwell/drywell sprays, suppression pool cooling, standby gas treatment, emergency diesels, reactor building cooling water, high pressure gas supply, manual bypass and the essential HVAC system and its auxiliaries.

The anticipated-transient-without-scram (ATWS) system is also considered in this analysis for events where it is needed to back up the RPS. ATWS has two parts. The first is the alternate rod insertion function (ARI) and the second is the standby liquid control system (SLCS). The initiation of ARI is analyzed whenever it is needed to scram the reactor but the SLCS design does not have sufficient detail for an analysis.

Three types of failures defined by section 2.4.2 of NUREG-0493 are in the scope of this study. They are described as follows:

> Type 1: "Some failures have the capability to induce plant transients for which scram and/or ESF function is needed. Defense-in-depth analysis requires that any credible failure of this type should not significantly impair the safety function." In a typical failure of this type, the sensor, channel, or block which fails (causing the transient) may also be required to mitigate the effects of the failure.
>
> Type 2: "Alternatively, failures that do not indirectly cause plant transients requiring safety action could still impair the safety function. Such failures would persist in general until they were discovered and repaired. Such failures would have serious consequences only if an event needing safety action were to occur while the system was in the failed state, after the failure had occurred, and before the failure was discovered."
>
> Type 3: "...For each anticipated operational occurrence in the design basis occurring in conjunction with a CMF, sufficient signal diversity should be provided in the design so that the plant can be brought to a stable hot standby condition...."

The analysis of Appendix A regards failures of types 2 and 3 for the anticipated transients and faults of General Electric SAR Chapter 15. For each event described by Chapter 15, except where a more severe event encompasses the effects of a similar but less severe event, a common-mode failure analysis was performed for sensor, channel and block failure as described by NUREG-0493 Guideline 7 and partly by Guideline 8. General Electric categorizes the events of Chapter 15 into three frequency classes:

I. incidents of moderate frequency
II. infrequent events
III. limiting faults

Classes I and II fall within the NUREG-0493 section 1.2.11 definition of "Anticipated Operational Occurrences" and class III matches the section 1.2.12 definition of "Accidents".

The analysis of Appendix D regards failures of type 1 for signals shared between the three echelons of defense. For each such shared signal a common-mode failure is assumed that will force the reactor into an unsafe transient, if that is possible. This analysis is mandated by NUREG-0493 Guideline 8.

For the purposes of this report, the Definitions of section 1.2 of NUREG-0493 and the Block Concept of section 2.5 are used in their entirety with modifications as noted to accommodate the differences in architecture between RESAR-414 and the GE ABWR.

2.2 Those Items Not in the Scope of this Report

There are common-mode failures of identical sensors which could be postulated. These failures may not be limited to a particular model but may, because of common technology, occur in a large number of devices sold by a manufacture. for measuring parameters in different ranges and in some instances different parameters. For example, pressure transducers can be used for sensing pressure and also sensing liquid level by sensing differential pressures. The focus of this assessment is on applications of innovative technology and therefore this class of failure is not included in this analysis.

Power supply failures (zero voltage) are not included in this analysis. The scram solenoids for the reactor cause a scram if power is removed and this analysis does not go beyond that. Further, complex or insidious failures of the various power supplies of the system (high ripple, high voltage, intermediate voltage, surges) are not included in this analysis since in all cases there is not enough information about the hardware to be employed to be able to predict the effects of these failures.

3. Methods

3.1 NUREG-0493 Guidelines

The Guidelines of NUREG-0493 section 3.3 are applied to this study as described below.

3.1.1 Guideline 1 - General Requirement

"The instrumentation system should provide three echelons of defense in depth: control, scram, and ESF."

The General Electric design provides the required three echelons.

3.1.2 Guideline 2 - Method of Evaluation

"The instrumentation system should be subdivided into redundant channels, and each channel should be analyzed as consisting of blocks ... The output signals must be assumed to fail in a manner that is credible but that produces the most detrimental consequences..."

The General Electric design consists of redundant divisions of sensors and logic. The analysis in this study considers blocks as described in section 3.6.3.2, subject to architectural limitations described in sections 3.6.2.3 and 3.6.3.1. Output signals are assumed to fail with the most detrimental consequences as described in section 3.6.1, Worst-Case Assumptions.

3.1.3 Guideline 3 - Postulated Common-Mode Failure of Blocks

"Analysis of defense in depth should be performed by postulating concurrent failures of the same block or blocks in all redundant channels."

The method of analysis of defense-in-depth conforming to Guideline 3 is described in section 3.3 and analyses of various events are presented in detail in Appendix A.

3.1.4 Guideline 4 - Use of Identical Hardware and Software Modules.

Treatment of identical modules in this study according to Guideline 4 is described and motivated in sections 3.6.1.2, 3.6.2.2, and 3.6.5.4. Sections 3.6.5.6 and 3.6.5.7 list assumptions that certain modules in the General Electric design are not identical.

3.1.5 Guideline 5 - Effect of Other Blocks

During any postulated common-mode failure, signals from failed blocks are propagated to downstream blocks which react correctly to the possibly erroneous signals.

3.1.6 Guideline 6 - Output Signals

Output signals are assumed to function one-way; that is, failures cannot propagate backwards into an output.

3.1.7 Guideline 7 - Diversity for Anticipated Operational Occurrences (Failure type 3, NUREG-0493)

General Electric, in their SAR Chapter 15, did not simulate reactor and protection system response for situations in which the preferred initiator signal failed. This study uses GE simulation curves and trip set points to determine diverse initiators, if any (see sections 3.3, third paragraph, and 3.6.2.1). Core cooling combinations described by General Electric (see section 3.6.6.4) are assumed to prevent a non-coolable geometry of the core and violation of the integrity of the primary coolant pressure boundary. Approved cooling combinations and containment isolation are assumed to prevent violation of the integrity of the containment.

3.1.8 Guideline 8 - Diversity Among Echelons of Defense

Common-mode failures postulated in accordance with Guidelines 3 through 6 are considered in the studies in both Appendix A and D, with special attention being paid in Appendix D to signals shared between echelons and to failures caused by the same sensor needed to initiate mitigation.

3.1.8.1 Control/Scram

Failure type 1 (NUREG-0493), same sensor causing a transient as required to detect the transient, is considered for control system/scram system interactions in Appendix D. Failure types 2 and 3 are studied in Appendix A.

3.1.8.2 Control/ESF

Failure type 1 (NUREG-0493), same sensor causing a transient as required to detect the transient, is considered for control system/ESF system interactions in Appendix D. Failure types 2 and 3 are studied in Appendix A.

3.1.8.3 Scram/ESF

Interconnections between scram and ESF "...(for interlocks providing for scram initiation if certain ESF are initiated, or ESF initiation when a scram occurs, or operating bypass functions)..." (NUREG-0493, par. 3.3.8.3) were considered, but none appear to exist. There are, however, signals shared between the scram and ESF system, and these are considered in Appendix A and explicitly in Appendix D.

3.1.9 Guideline 9 - Plant Monitoring

The General Electric design transmits signals from the scram and ESF actuation systems to the control system for plant monitoring purposes. Connections and software used to monitor the scram and ESF actuation systems are considered in section 5.5. The possibility that incorrect values returned by the plant monitoring system may cause operators to make adjustments that place the plant in an unsafe condition or cause it to operate outside regulatory limiting conditions is considered in sections 5.2.2 and 5.5.

3.2 Type 1 Failure Analysis

The analysis of Appendix D considers failures of type 1 for signals shared between echelons, as shown by Figure 3. Using Guideline 8 (section 3.1.8), each of the eleven shared signals is examined to determine credible common-mode failures and these failures are postulated to study the reactions of the involved echelons acting together. In the words of section 2.1, sixth paragraph, NUREG-0493, ".... it is important that transients or control system failures needing protection system action for safety not also induce protection system failure." While the emphasis is on transients induced by the postulated failures, effects of type 2 failures are also considered in case there may be inter-echelon dependencies not discovered in the method described in section 3.3, following.

3.3 Types 2 and 3 Failure Analysis

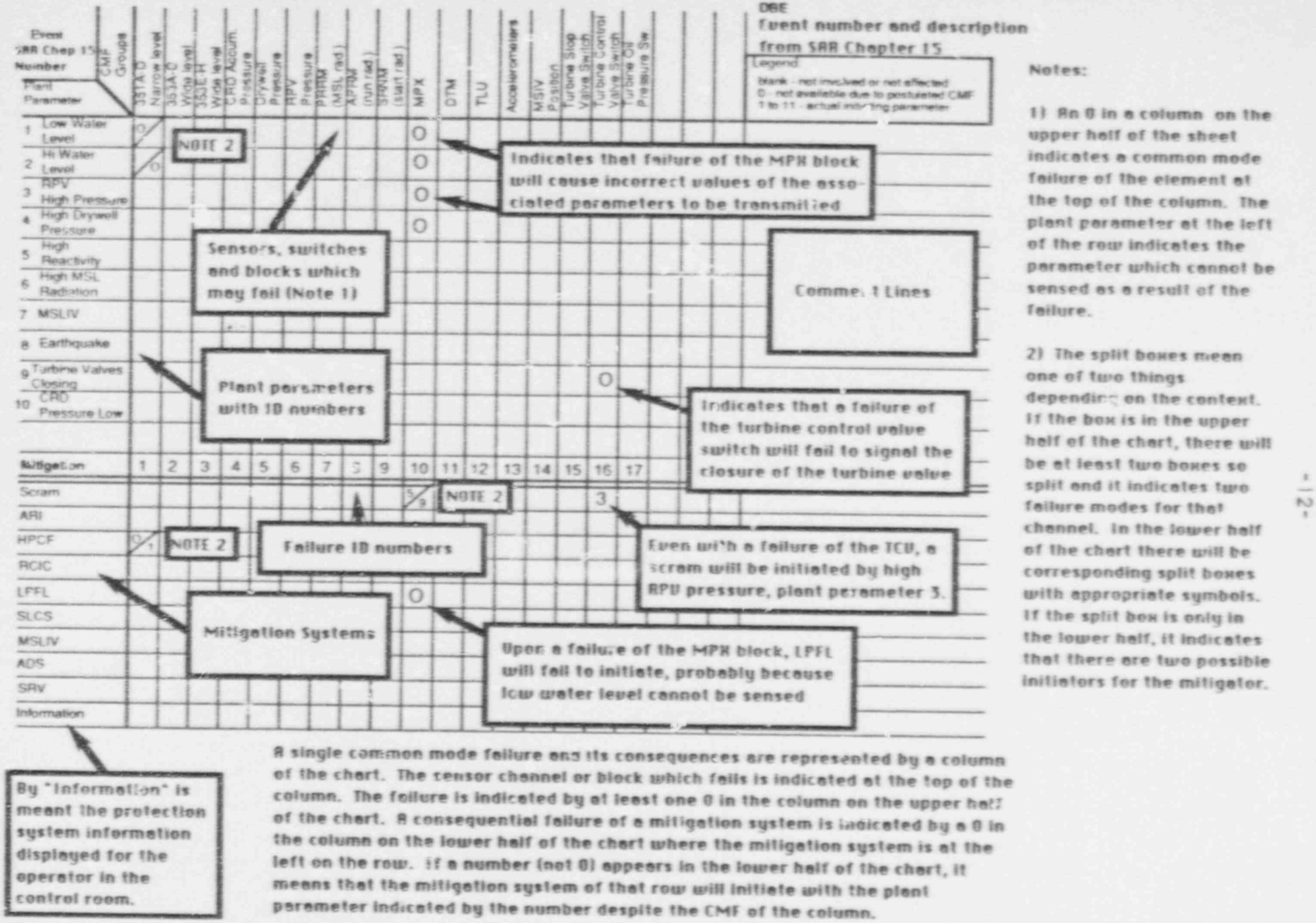
In accordance with Guideline 7 (section 3.1.7) and the definitions of failure type 3, common-mode failures were postulated and analyzed for each of the events of Chapter 15 of the SAR which required the invocation of the protection systems. By including limiting faults of Chapter 15, failures of type 2 were also analyzed for design-basis accidents for the ABWR. To facilitate this analysis, a chart was developed to systematicaliy record failed signals or blocks and to indicate the results of each failure. This chart, together with explanations and illustrations, is shown in Figure 1, Analysis Chart.

For each event of Chapter 15 which challenged the protection system, a set of assumptions was made about the way the protection system would fail and also about facts which were unclear or unknown. These assumptions were divided into general assumptions (section 3.6 of this report) and assumptions specific to the event being analyzed.

The starting place for the analysis of each event was the associated sequence table and the curves which appear in Chapter 15. (The tables were, in fact, derived from the curves which are the output of computer simulation runs made by GE for the event.) The General Electric analysis of Chapter 15 always assumed correct functioning of the protection system. Where postulated common-mode failures rendered primary protective action initiators ineffective, it was necessary to combine assumptions, results of the simulations, knowledge of reactor physics and thermal-hydraulic characteristics to determine secondary initiators if any existed. Sensor channels were failed one at a time across all divisions simultaneously to determine if there was enough diversity and defense-in-depth to mitigate the effects of the event. General Electric logic diagrams (IBDs), system architecture (see Figure 4), and various amendments to the SAR (see References) were used to determine the probable reaction of the protection system to the challenge presented. After the analysis of individual channels was complete, system blocks were failed and the effect of these block failures analyzed in the same way.

3.4 The Trip Tables

To assist in the analysis methods described in sections 3.2 and 3.3, a set of tables was made up, one for each mitigation system of the



A single common mode failure and its consequences are represented by a column of the chart. The sensor channel or block which fails is indicated at the top of the column. The failure is indicated by at least one 0 in the column on the upper half of the chart. A consequential failure of a mitigation system is indicated by a 0 in the column on the lower half of the chart where the mitigation system is at the left on the row. If a number (not 0) appears in the lower half of the chart, it means that the mitigation system of that row will initiate with the plant parameter indicated by the number despite the CMF of the column.

Notes:

1) An 0 in a column on the upper half of the sheet indicates a common mode failure of the element at the top of the column. The plant parameter at the left of the row indicates the parameter which cannot be sensed as a result of the failure.

2) The split boxes mean one of two things depending on the context. If the box is in the upper half of the chart, there will be at least two boxes so split and it indicates two failure modes for that channel. In the lower half of the chart there will be corresponding split boxes with appropriate symbols. If the split box is only in the lower half, it indicates that there are two possible initiators for the mitigator.

Figure 1
Analysis Chart

protection system. These tables show all of the inputs to a particular sub-function of a trip action and the effect of the trip once the necessary inputs are present, although the detailed logic is not shown. These tables are used to consolidate information which may appear on a number of pages of the SAR so as to remind the reviewer of the signals important to each protective function. These tables appear in Appendix C.

3.5 Summarizing Findings

After the analyses of sections 3.2 and 3.3 were complete (Appendices D and A, respectively), the vulnerabilities revealed were summarized in section 5 of this study.

3.6 General Assumptions

The assumptions of this section apply to all of the analyses performed. They are categorized by their relationship to various GE documents or by their applicability.

3.6.1 Worst-Case Assumptions

3.6.1.1 Failures are assumed to occur in the most limiting fashion possible consistent with hardware or software construction. For example, a module which energizes to trip is assumed to take no action, or a module which de-energizes to trip is assumed to fail so that it continues to block trip (NUREG-0493 Guideline 2).

3.6.1.2 Software which is essentially identical except for constant or address parameters is assumed to fail identically. Identical software/hardware modules in separate divisions are assumed to fail simultaneously (NUREG-0493 Guideline 4).

3.6.1.3 Failures are assumed to be latent and undetectable until stressed by event or accident, at which time the failure becomes manifest.

3.6.2 Assumptions based on GE texts

3.6.2.1 Reactor physics and thermal-hydraulic analyses, as described by GE's Table 15.0-2 [Ref. 1] and the simulation curves in Chapter 15 are assumed to be correct. Initial conditions and trip points described in Table 15.0-1 are used in conjunction with Table 15.0-2 and Chapter 15 simulation curves to determine secondary and tertiary trips, if needed.

3.6.2.2 Common software modules will be used for similar functions where they occur [Ref. 4]. This means that similar modules in each protection system division are assumed to have essentially identical software.

3.6.2.3 Sensor signals are intermingled once they enter the multiplexer system and are identified only by software [Ref. 4]. Signals entering at points other than the multiplexer are assumed to be identified only by software also. See the discussion of signal channels below.

3.6.2.4 "Autodiagnostic software and hardware watchdog timers" [Ref. 4] are assumed to detect only malfunctions anticipated by software designers, but not unintended errors made by software designers.

3.6.3 Assumptions based on GE software structure

For the purposes of this study a signal channel is defined as a sensor, signal conditioning circuitry, A to D converter if required, and all of the software which is needed to maintain the identity and integrity of the sensor signal through to where the signal is used in the process[1]. Further, as long as a derived signal is derived from only one sensor signal, the software which maintains the identity of this derived signal shall be considered as part of the original signal channel. If a derived signal is dependant on more than one sensor signal then this derived signal will have a unique identity and there will be defined a derived signal channel which has all of the characteristics of a signal channel except for the sensor and its attendant signal processor and converter.

---

[1]This meets the definition of a channel as it appears in IEEE 279.

3.6.3.1 A failure in a signal channel can be caused by a number of events - calibration error, an error introduced when a software change is made, an existing error in the software which causes a channel to become corrupted, etc. Based on General Electric's statements regarding common software modules [Ref. 4], it is highly likely that software changes in all four divisions will be made as if only one change were being made. Thus it is conceivable that a common-mode failure of a channel can be introduced and be undetected for some time. Therefore, one type of common-mode failure assumed in this study is a channel failure occurring over all divisions of the protection system.

3.6.3.2 Another type of common-mode failure assumed in this study is the simultaneous failure of all like modules (blocks) in all divisions. Failure is assumed undetectable by downstream modules. NUREG-0493 "Measured Variable Blocks" (MVB) correspond to sensors, signal conditioning, analog-to-digital converters, remote multiplexing units (RMUs), transmission media, and control-room multiplexing units (CMUs) in the General Electric design. NUREG-0493 "Derived Variable Blocks" (DVB) correspond to digital trip modules (DTMs) in the General Electric design. NUREG-0493 "Command Blocks" (CB) correspond to trip logic modules (TLUs) in the General Electric design. "Actuation Blocks" (AB) correspond to output logic units (OLUs), load drivers, or CMUs, transmission media, and RMUs in the General Electric design. The correspondences stated are imprecise because of the intermingling which occurs in the General Electric multiplexing scheme and because the TLU has some of the characteristics of a DVB. For this reason, NUREG-0493 common-mode block failure is assumed to occur in the multiplexer (MPX)[2], the DTMs, and the TLUs.

3.6.4 Assumptions contrary to GE assumptions

This study differs on several assumptions made in Amendment 18, Appendix 19N to the General Electric PRA for ABWR, submitted to the NRC on October 11, 1991.

3.6.4.1 Manufacturing error is considered a credible cause of common-mode failure. Errata sheets and buglists for delivered hardware are common occurrences for more complicated integrated circuits (such as microprocessors) and the

[2]The MPX consists of RMU, transmission media, and CMU, considered as a unit.

possibility of undetected design or manufacturing process error cannot be ruled out. Furthermore, corrections[3] to printed circuit boards (PCBs) which use integrated circuits are common in the industry. Both integrated circuit and printed circuit manufacturing errors may not be obvious until an appropriate set of inputs, instruction sequences, and environmental conditions challenge the equipment.

3.6.4.2 Loss of data communication is only one of many failures which can occur in data communications systems. Many faults are undetectable downstream. One such fault is the transmission of plausible but incorrect data which is the fault assumed in this study.

3.6.4.3 Failure of a "de-energize-to-trip" mode is possible anywhere software is involved.

3.6.4.4 Software self-test and watchdog timers can detect only those errors anticipated by system designers. It is assumed in this study that all common-mode failures which occur were not anticipated by designers, otherwise they would have been fixed. Therefore, it is assumed that failures of upstream blocks cannot be detected by downstream blocks.

3.6.5 Assumptions based on GE's logic diagrams

It is impossible to tell from GE's logic diagrams (IBDs and P & IDs) where some logic functions are implemented. Therefore, some of the following assumptions are made with regard to the module location of signal and trip logic shown in General Electric IBDs in Chapter 7 of the SAR.

Some of the assumptions below, in particular 3.6.5.6, 3.6.5.7 and 3.6.5.9, assert diversity which is speculative. If this diversity does not exist in the final product, the analysis will change in the direction of more vulnerability.

3.6.5.1 Logic functions such as limit switches and torque limit switches associated with motor-operated valves or actuators are assumed to be hardwired to the associated motor control center because of location and industry practice.

---

[3]In the form of cut traces or wires soldered to the surface of the PCB.

3.6.5.2 Logic functions involving the positions of valves, switches, or interlocks other than the valve directly being controlled are assumed to require the multiplexer and the TLU because of distance, wiring economy, and lack of indication by General Electric that this logic is implemented by directly wiring to the motor control center of interest.

3.6.5.3 "Manual" control switches are assumed to require the multiplexer and the TLU to be effective because General Electric drawings indicate that this is the case (see General Electric drawing 103E1805, sheets 1 - 5).

3.6.5.4 The Non-Essential Multiplexer (NEMS) and the Essential Multiplexer (EMS) are identical with the exception of the sensors connected. Both use essentially identical software [Ref. 4]. A common-mode failure in multiplexer software renders the NEMS and the EMS inoperative or transmitting erroneous but plausible information.

3.6.5.5 The Alternate Rod Insertion (ARI) is initiated by signals passing through the NEMS and by one signal (low water level) passing through the EMS [Ref. 5]. In the absence of other information, it is assumed that the Standby Liquid Control System (SLCS) is initiated by the same signals as the ARI.

3.6.5.6 The DTM and the control system are sufficiently diverse that a failure in the DTM preventing scram does not imply a failure of ARI.

3.6.5.7 The MPX and the DTM have diverse software so that a failure in one does not imply a failure in the other.

3.6.5.8 The TLU is the only unit that sends information to the control system for display to the operators. Only status and trip information is sent.

3.6.5.9 The eight wide range water level transmitters, B21-LT353A through H, are used as two presumably diverse groups, A - D and E - H. It is assumed that these two sensor groups are treated separately in software so that a common-mode channel failure of one group does not affect the other group.

3.6.5.10 The ECCS initiation preference is:

1) RCIC (water level 2, channel group B21-LT353(A-D)),
2) HPCF (water level 1.5, channel group B21-LT353(E-H)),
3) LPFL (water level 1, channel groups B21-LT353(A-D),(E-H)).

3.6.6 Assumptions for echelon Defense-in-Depth (DID)

3.6.6.1 In all normal fuel configurations, the reactor control rods have at least the cold shutdown margin control of reactivity even with all recirculation pumps running at maximum flow.

3.6.6.2 The fuel rods will experience damage if uncovered or if significant boiling occurs at fuel rod surfaces. Cladding damage is an unacceptable consequence.

3.6.6.3 The echelons of defense are the control system, the reactor protection system (RPS), and the engineered safety features (ESF). See Figure 2. The only signals common to the echelons are shown in Figure 3. Mitigating functions for ATWS events are to be implemented by GE as part of the control system.

3.6.6.4 The mitigation combinations described in Amendment 14, Table 19.3-2 "Success Criteria to Prevent Initial Core Damage for Transients and LOCA Events with RPS Scram", General Electric SAR, are assumed to be correct. Because no data are given for events without scram, it is assumed in this study that no combination of control system (excluding scram by ARI and FMCRD) and ESF actions can compensate for failure to scram from full power and that unacceptable consequences will occur if this happens.

3.6.6.5 Manual actuation of scram or ESF mitigation features is considered to be a backup defense if the conditions of NUREG-0493 for manual actuation are met:

1) The postulated CMF does not impair manual control from the control room.

2) Sufficient information is available to the operator.

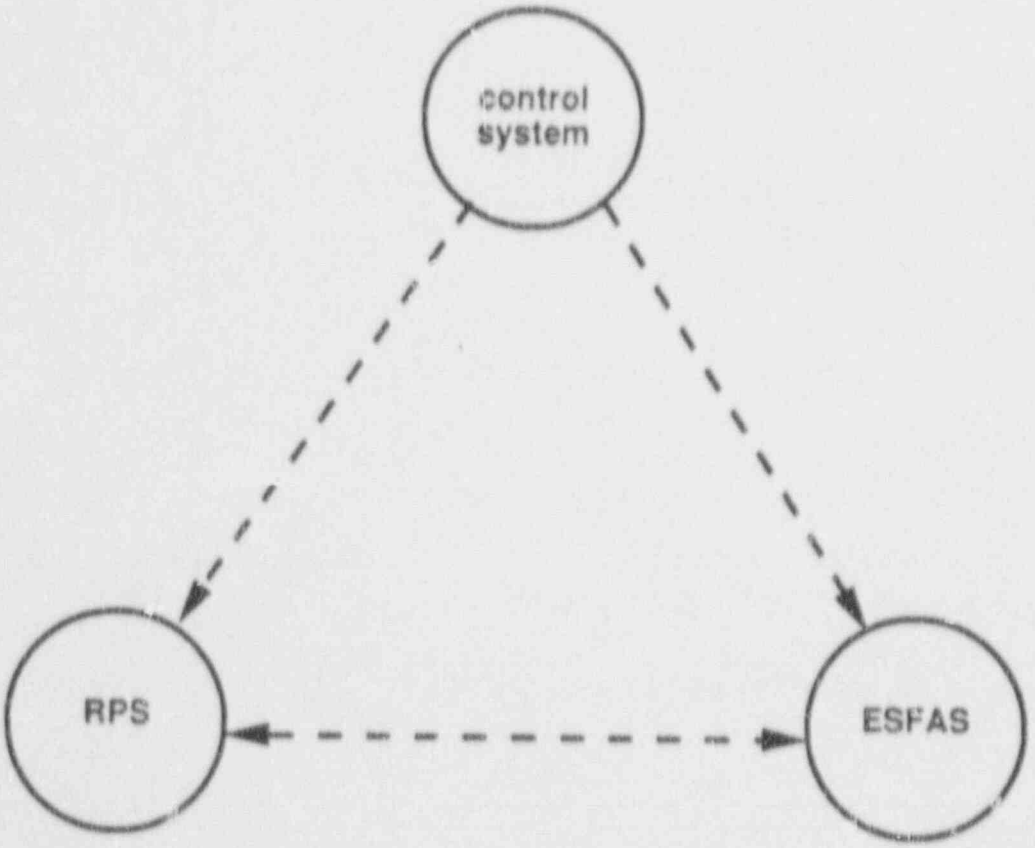


Figure 2 Echelon diagram showing possible interactions (dotted).

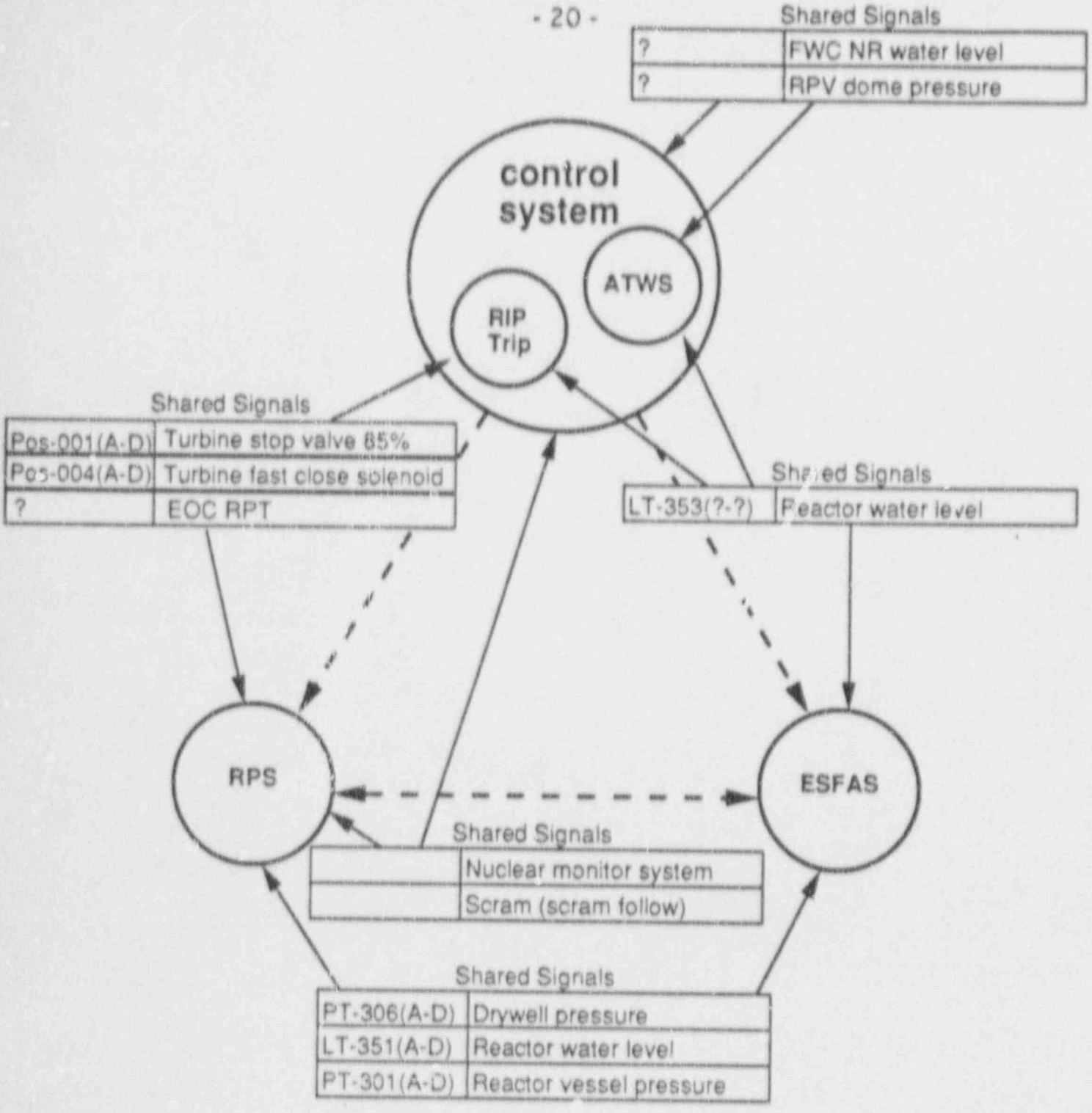


Figure 3 Echelon diagram showing possible interactions (dotted) and shared signals.

3) Sufficient time is available for operator analysis, decision, and action.

4) Sufficient information and time are available for the operator to detect, analyze, and correct reasonably probable errors of operator function.

For the purposes of this study, operator backup actions are assumed to require at least five minutes to be considered effective defense-in-depth backup.

3.7 Evaluation Criteria

The only criteria for success is whether or not the protection system performs adequately with the failure. Thus, if the RPS, ARI or SLCS shuts down the reaction if required by the postulated failure, that part of the protection system is deemed to have operated successfully. If the ECCS functions adequately to prevent damage to the core with the postulated failure, that part of the system is deemed to have worked successfully.

3.3 Some Disclaimers

The reader of this report needs to understand some issues so that there are no misunderstandings of what the report contains. Further, there are some parts which take some skill in interpretation and those items need to be indicated to the reader.

3.8.1 The words "failure", "common-mode failure" and "CMF" are used interchangably. The context should make clear when "failure" means a CMF.

3.8.2 The words "sensor", "channel" and "sensor channel" are used interchangably and context should make clear when this interchangability is implied.

3.8.3 The CMF analysis charts do not stand alone and they vary from chart to chart in column and line headings. The assumptions and conclusions are a necessary part of an analysis and an understanding of the GE ABWR is required.

3.8.4 This analysis does not claim to have found all common-mode failure vulnerabilities which may be in the design.

The primary purpose was to identify sensitivity to adverse interactions among the three defense echelons.

4. Description of the Design

4.1 Design Basis

4.1.1 Regulations and Standards Requirements

Design basis requirements pertinent to defense-in-depth and diversity that have been identified by GE in the SAR for the ABWR design include the regulations and standards summarized in this section.

10 CFR 50 Appendix A, "General Design Criteria" states in part in the introduction that:

> "The development of these General Design Criteria is not yet complete.... some of the specific design requirements for structures, systems, and components important to safety have not as yet been suitably defined. Their omission does not relieve any applicant from considering these matters in the design of a specific facility and satisfying the necessary safety requirements. These matters include:
>
> "...(2) Consideration of redundancy and diversity requirements for fluid systems important to safety...the minimum acceptable redundancy and diversity of subsystems and components within a subsystem, and the required interconnection and independence of the subsystems have not yet been developed or defined. (see Criteria 34, 35, 38, 41, and 44).
>
> "...(4) Consideration of the possibility of systematic, nonrandom, concurrent failures of redundant elements in the design of protection systems and reactivity control systems. (See Criteria 22, 24, 26, and 29).
>
> "...There will be some water-cooled nuclear power plants for which the General Design Criteria are not sufficient and for which additional criteria must be identified and satisfied in the interest of public safety. In particular, it is expected that

additional or different criteria will be needed...for water-cooled nuclear power units of advanced design."

From the General Design Criteria of 10 CFR 50 Appendix A.

21) "Protection system reliability and testability", requires in part that "...no single failure results in loss of the protection system..."

22) "Protection system independence" requires in part that "Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function."

23) "Protection system failure modes" requires that: "The protection system shall be designed to fail in a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as disconnection of the system, loss of energy (e.g., electric power, instrument air) or postulated adverse environments (e.g., extreme heat or cold, fire, pressure, steam, water, and radiation) are experienced.

24) "Separation of protection and control systems" requires in part that: "Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired."

29) "Protection against anticipated operational occurrences" requires that: "The protection and reactivity control systems shall be designed to assure an extremely high probability of accomplishing their safety functions in the event of anticipated operational occurrences."

10 CFR 50.55a(h) requires that protection systems meet the requirements of IEEE Std 279. IEEE Std 279 includes the following requirements:

"4.2 Single Failure Criterion. Any single failure within the protection system shall not prevent proper protective action at the system level when required.

"4.7.4 Multiple Failures Resulting From a Credible Single Event. Where a credible single event can cause a control system action that results in a condition requiring protective action and can concurrently prevent the protective action from those protection system channels designated to provide principal protection against the condition, one of the following must be met.

"4.7.4.1 Alternate channels, not subject to failure resulting from the same single event, shall be provided to limit the consequences of this event to a value specified by the design bases. In the selection of alternate channels, consideration should be given to (1) channels that sense a set of variables different from the principal channels, (2) channels that use equipment different from that of the principal channels to sense the same variable, and (3) channels that sense a set of variables different from those of the principal protection channels using equipment different from that of the principal protection channels. Both the principal and alternate protection channels shall meet all the requirements of this document.

"4.7.4.2 Equipment, not subject to failure caused by the same credible single event, shall be provided to detect the event and limit the consequences to a value specified by the design bases. Such equipment shall meet all the requirements of this document."

IEEE Std 603-1980 includes criteria substantially similar to the foregoing IEEE Std 279 requirements.

4.1.2 Other Design Basis Requirements

GE has indicated to the NRC staff recently [Ref. 4] that standardization of hardware and software modules is a design objective.

4.2 Architecture

The Instrumentation and Control System for the GE ABWR consists of three echelons (Figure 2), the Reactor Protection System (RPS), the Engineered Safety Features Actuation System (ESFAS or ESF), and

the control system. A diverse method for scramming the reactor, anticipated-trip-without-scram (ATWS), is being implemented as part of the control system. For the most part, these echelons are separate. However, some signals are shared between echelons, and this is shown in Figure 3 with ATWS and RIP trip being made explicit.

The protection system for the GE ABWR is divided into four independent and redundant divisions. Voting takes place among the four divisions to decide on actions with two-out-of-four being enough for action. A division bypass function is available so that one division can be maintained while the other three vote in a two-out-of-three configuration. If one division is bypassed, no other division can be bypassed.

Each division has its own set of sensors, each of which has an A to D converter if required, which are connected through either a multiplexer or directly to the digital processing system. Following the multiplexer are two digital subsystems, a Digital Trip Module (DTM) which compares digital representations of analog signals against set points and delivers a decision (below, above) to the Trip Logic Unit (TLU) which performs combinatorial logic on various binary signals to determine a binary output. This binary signal then passes to a final two-out-of-four voter. Binary signals from DTMs are also passed across divisions to all of the TLUs to allow voting in the TLUs also. This is to avoid spurious cross channel trips. Thus for each signal which can cause a trip, a vote is taken among the signals to determine if there are at least two signals which assert a trip. Then the division asserts a trip. Finally, the divisions vote with two divisions sufficient to actuate a trip.

In the RPS, the four divisions are identical. Such is not the case in the ESFAS. Whereas two-out-of-four voting is maintained in ESFAS, there are a number of asymmetries which are not found in the RPS.

For the purposes of this analysis, the four divisions have been collapsed into one with the elements shown in Figure 4. The elements shown are essentially those of the system architecture. But they also serve as the blocks of a NUREG-0493 type analysis. Thus, in the analysis, in addition to the channel failures which make a particular sensor fail according to assumption 3.6.3.1, the blocks of the figure are failed according to assumption 3.6.3.2. Figure 5 shows the architecture with only the signals shared between

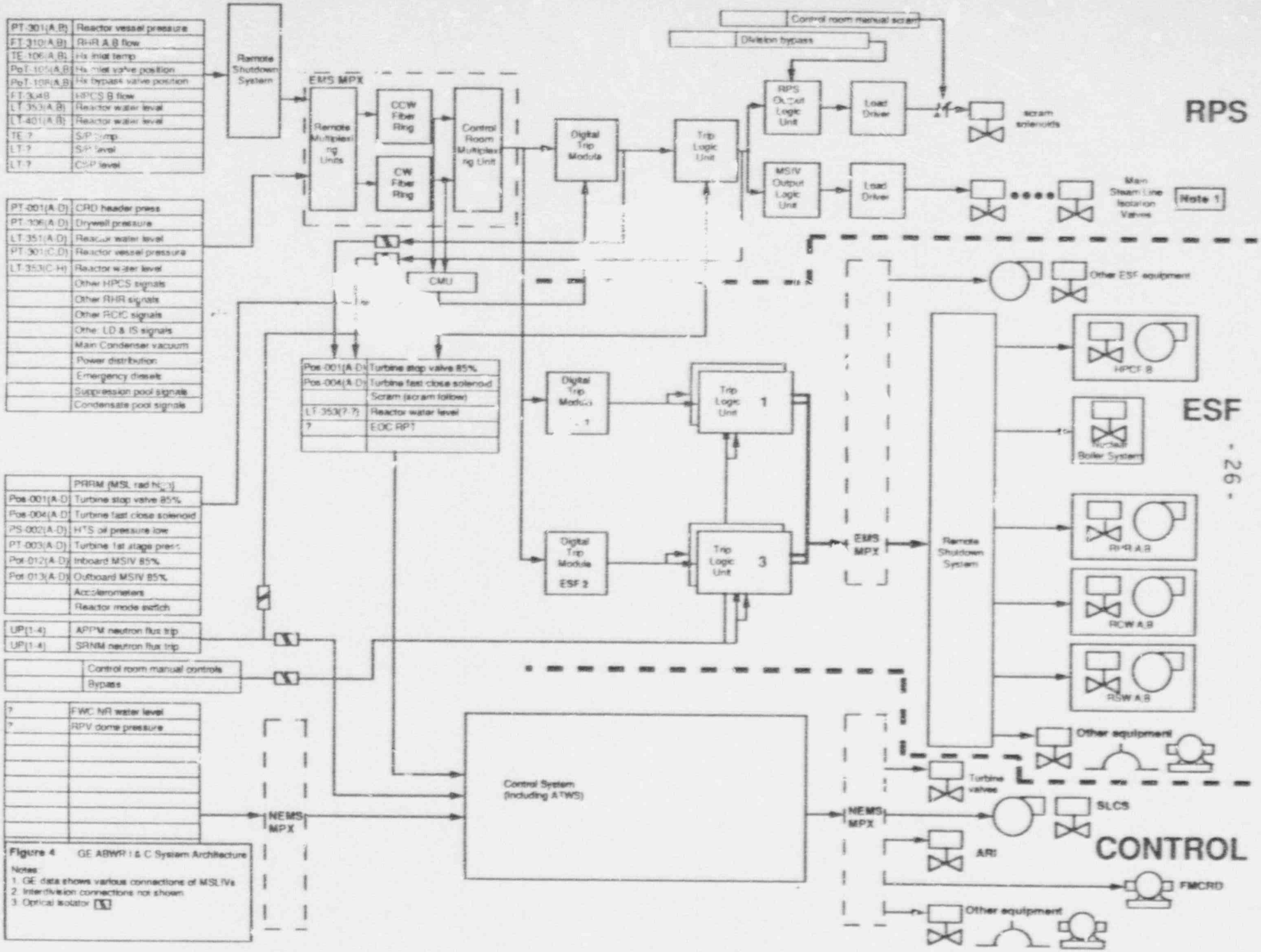


Figure 4 GE ABWR I & C System Architecture

Notes:
1. GE data shows various connections of MSIVs
2. Interdivision connections not shown
3. Optical isolator

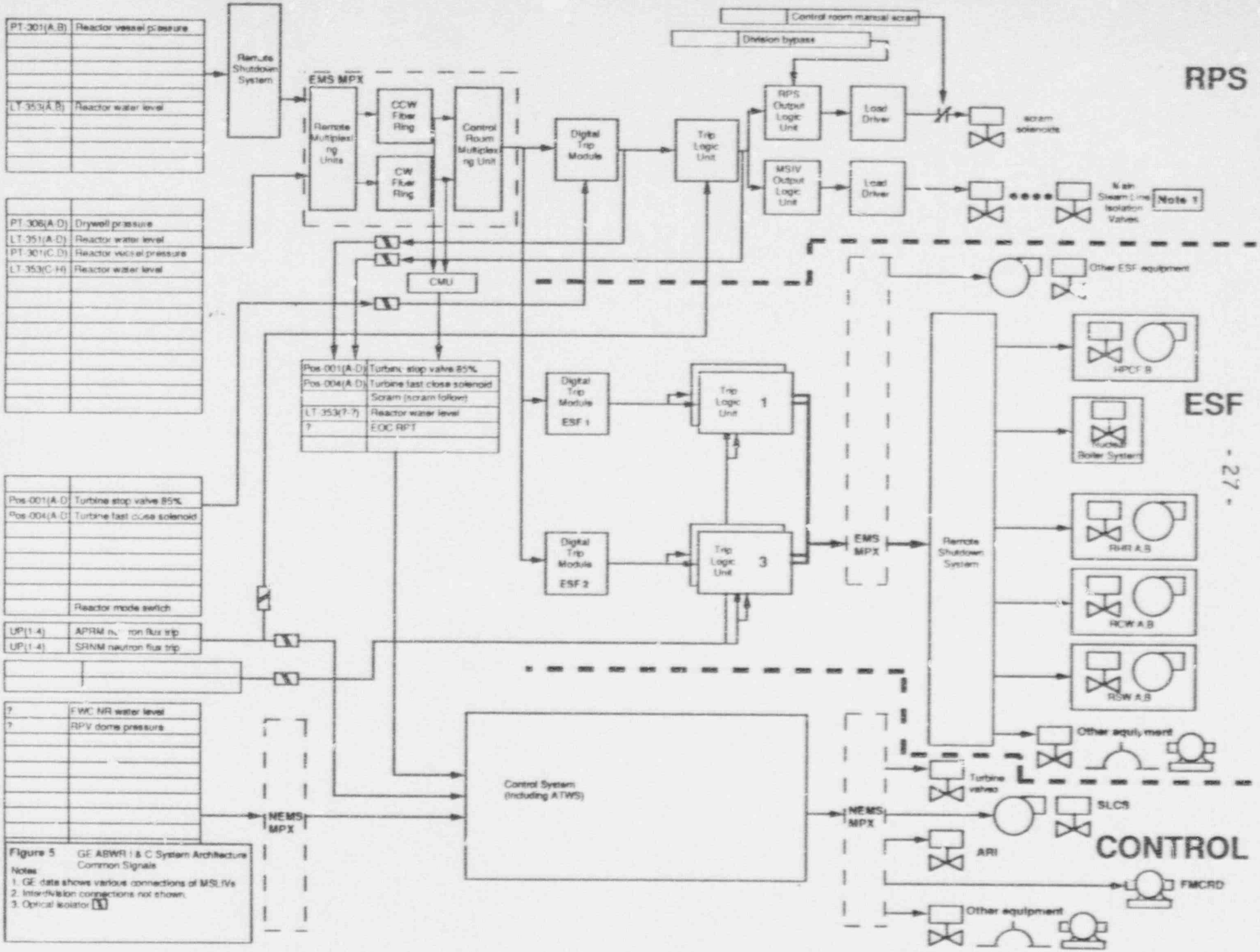


Figure 5 GE ABWR I & C System Architecture Common Signals

Notes
1. GE data shows various connections of MSLIVs
2. Interdivision connections not shown.
3. Optical isolator

echelons (compare with echelon diagram Figure 3). Signal flow is demonstrated in Figure 6 (the LT-353 signal that passes through the EMS) and in Figure 7 (turbine switches that enter the RPS DTM and are passed to the control system through an optical isolator).

The documentation for how the MSLIVs are controlled is reasonably clear but exactly where control is exercised is confused. On GE drawing 103E1805 sheets 1 - 5, the MSLIVs are shown as connected directly to the TLUs of the RPS. But those same drawings show the LDS as part of the ESFAS. On the IBDs for the LD&IS (LDS) are shown all of the logic for the actuation of the MSLIVs. Further, in Ref. 2, page 1 of the List of Equipment Interface with the Essential Mux Signals (sic), is shown the MSIVs from which it could be inferred that the MSIVs are actuated through the multiplexer. It has been assumed for this analysis that the control of the MSLIVs rests in the ESFAS but that the software which evaluates the various functions for operating the MSLIVs runs on the DTM and TLU which also evaluate RPS functions. Further, it is assumed that the actuation signals for the valves is hardwired from the RPS/MSIV TLUs to the valve load drivers. These assumptions blur the separation between RPS and ESFAS but do not affect the analysis.

4.3 Signal Diversity

The Trip Tables (Appendix C) show the diverse signals which are available to trip the various functions required by the protection system. Not all signals are operative for each event of Chapter 15. This does not imply that there are failures but only that certain signals do not cross necessary thresholds for every event.

5. Findings

Documentation of the analyses performed as described in sections 3.2 and 3.3 is in Appendices D and A, respectively. Figure 8 is a chart summarizing the results of the analysis of Appendix A. A short discussion of systems for which design is particularly sketchy appears in Appendix B. This section summarizes the vulnerabilities discovered during detailed analysis. These findings are valid only so far as the assumptions made are correct. If the assumptions are ignored or overlooked, meaning may be attached to the findings which is not real.

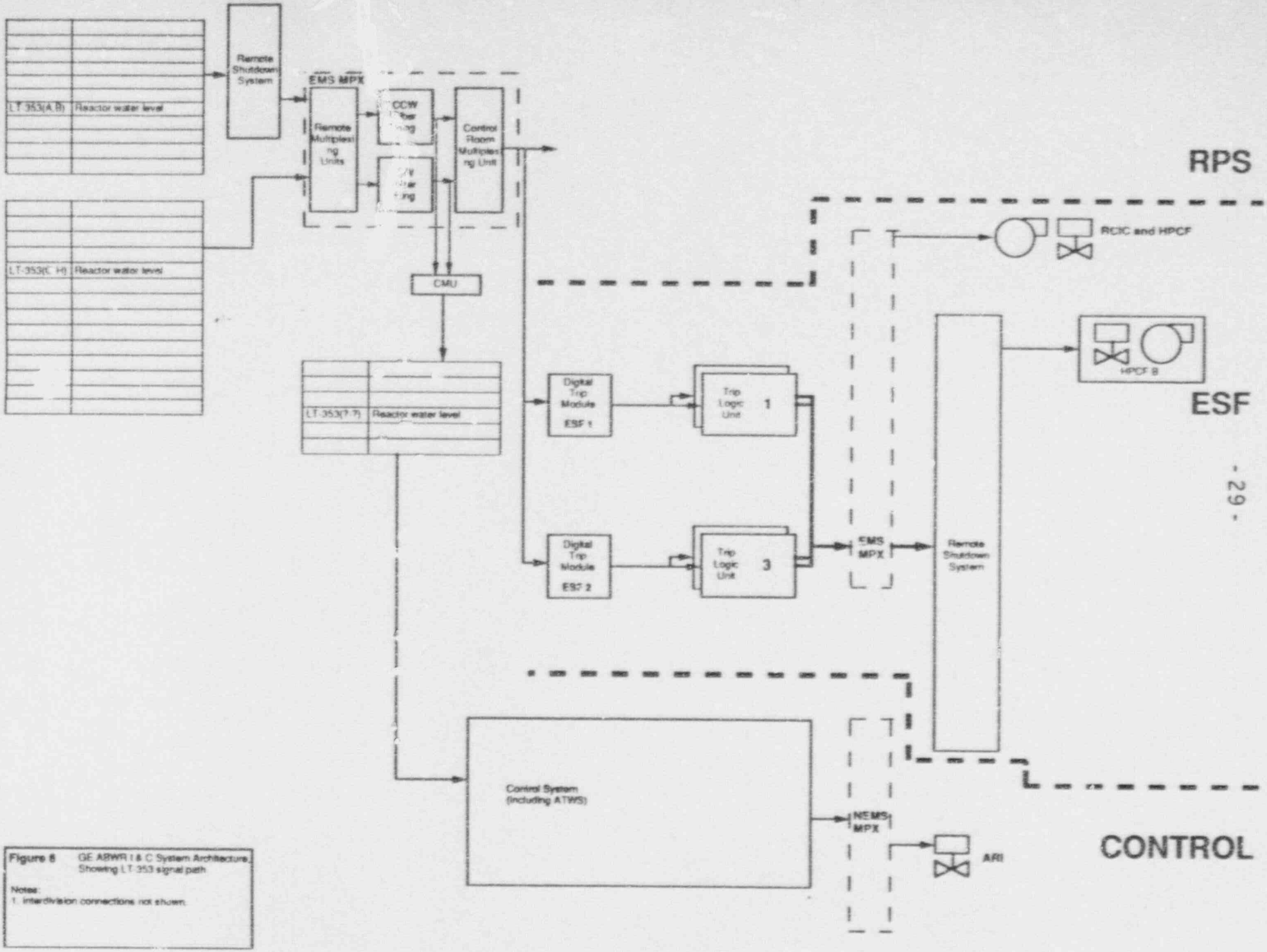


Figure 6 GE ABWR I & C System Architecture Showing LT-353 signal path

Notes:
1. Interdivision connections not shown.

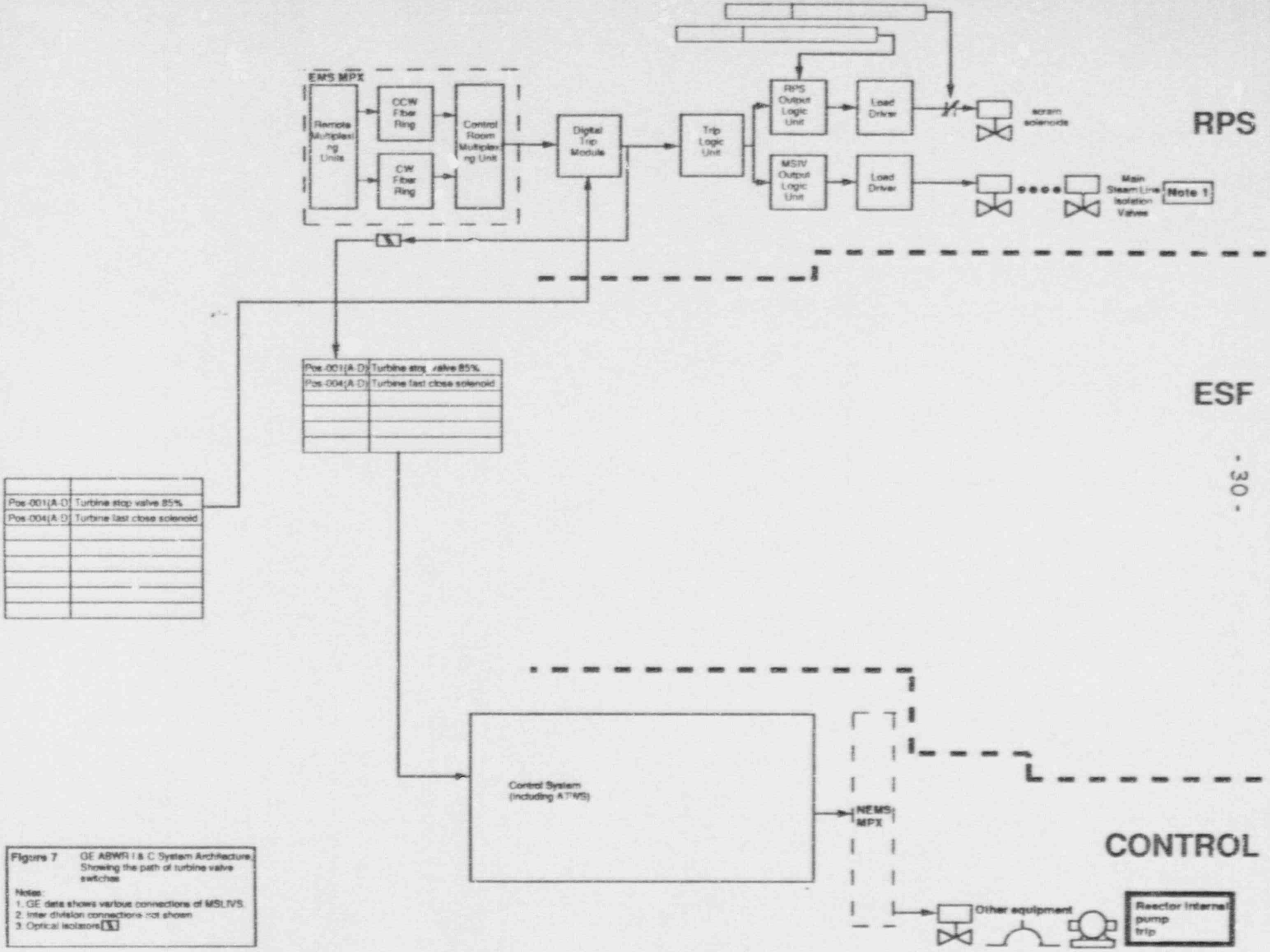


Figure 7 GE ABWR I & C System Architecture, Showing the path of turbine valve switches

Notes:
1. GE data shows various connections of MSLIVS.
2. Inter division connections not shown
3. Optical isolators [S]

CMF Vulnerability Summary Chapter 15 Event / CMF Groups	351A-D Narrow level	353A-D Wide level	353E-H Wide level	CRD Accum. Pressure	Drywell Pressure	RPV Pressure	PRRM (MSL rad.)	APRM (run rad.)	SRNM (start rad.)	MPX	DTM	TLU	MSIV Position	Turbine Stop Valve Switch	Turbine Fast Solenoid Valve	Turbine Oil Pressure Sw.	ADS Water Level Switch	ADS Drywell Press. Switch	MSIV Low Water Level Switch	Low Turbine Inlet Pressure
15.1.2 Runout 2 FWP	E									E	E	E								
15.1.3 Pressure Reg Fail	E									E	E	E								
15.1.6 Inadv. Cooling									S			S								
15.2.1 Pressure Reg Fail										E										
15.2.2 Load Rejection										E										
15.2.3 Turbine Trip										E										
15.2.4 Inadv. MSIV Clos	E									E	E	E								
15.2.5 Loss Cond. Vac.	E									E	E	E								
15.2.6 Loss Aux XFMR	E									E	E	E								
15.2.7 Loss Feedwater	E									E	E	E								
15.3.1 Trip all RIPs	E									E	E	E								
15.4.1 Inadv. Rod Rem.												S								
15.4.5 Runout RIPs																				
15.6.4 Outside LOCA	E									E I S	E I S	E I S								
15.6.5 Inside LOCA	E									E I S	E I S	E I S					E	E		
15.6.6 Feedwater LOCA	E									E I S	E I S	E I S								

Vulnerability Summary

Legend:
blank - not involved or not affected
S - Scram vulnerability
E - ESFAS vulnerability
I - Isolation vulnerability

Figure 8 Vulnerability summary of data in Appendix A

The design analyzed is primarily an architecture and does not contain all of the necessary detail for a complete design. Where detail is present, an analysis of the detail is presented. Where detail is inadequate, analysis of the architecture is presented. These findings reflect the state of the design.

5.1 Successful Operation

The analysis of Appendix A demonstrates that for many common-mode failures there is sufficient diversity and defense-in-depth in the protection systems to mitigate the effects of the failures. They will not be listed here because of the number. The reader is encouraged to examine the Appendix if he is interested in specific cases.

5.2 Areas of Concern

No signal in the design presented crosses all three echelons of defense. There are, however, several signals which cross two echelons. Further, one block - the TLU - links two echelons and one block - the multiplexer - links all echelons. This section presents findings regarding those signals and blocks where vulnerabilities were found. This is the separation issue of NUREG-0493, section 2.4.2. More appears in Appendix D.

5.2.1 B21-LT351A - D

This is a set of four narrow-range water level transmitters used for several functions. The functions of most interest are those of low-water-level scram and high-water-level shutoff of the RCIC and HPCF. For RCIC it shuts down the whole system including the turbine. For HPCF it closes the injection valve. Thus these transmitters cross the RPS and ESFAS echelons (Figure 9). If this transmitter or its associated signal channel should stick in the high-water-level state (>L8) the reactor would not scram on its normal low-water-level condition, RCIC would not initiate, and although the HPCF pumps would start, the HPCF injection valve would not open. This can all be seen from the IBDs included in Chapter 7. Once the water level gets low enough, the MSLIVs will close and a diverse reactor trip will be initiated when the MSLIVs are at 85% open.

5.2.2 APRM

The APRM produces a high flux scram for the RPS, provides information on which rod-block determinations are made by the control system, provides neutron flux level used for automatic load following by the rod control system, and provides neutron flux level information for use by operators. Thus it links the control, manual control and RPS echelons (Figure 9). A failure of the APRM could prevent a rod-block from occurring (this is not clear from the documentation) while simultaneously preventing a high-flux scram from occurring. Under-reporting neutron flux levels by the APRM has the potential for inducing high flux operation of the reactor either by automatic (Guideline 8) or manual control (Guideline 9) while preventing a high-flux scram. This is a vulnerability that should be examined carefully.

5.2.3 B21-LT353A - D

In the rather sketchy ATWS documentation [Ref. 5] it is stated that the SSLC provides water level information to the control system for initiating ARI on low-water-level. For this study it is assumed that the above sensor is the one used. This sensor is used to initiate RCIC in the ESFAS. This sensor therefore links both ESFAS and the control system. Thus a failure of this sensor will prevent RCIC from initiating and will inhibit ARI should it be needed. However, if this sensor fails a diverse reactor low-water scram would be initiated by B21-LT351A - D and a diverse initiation of HPCF would occur through B21-LT353E - H.

5.2.4 Multiplexer

The multiplexer in this system links all three echelons. It carries low-water-level data and rod-separation information to the control system to initiate ARI and rod-block. It carries a large number of signals to both ESFAS and RPS. (Some RPS signals are wired directly to either the DTM or TLU of the RPS.) This linkage could cause unacceptable failures by preventing scram when needed and simultaneously preventing ARI and the initiation of ECCS. (SLCS may be affected by this linkage, but there is no information on how SLCS is initiated automatically. It is stated in section 9.3.5.2 of the SAR that SLCS can be manually initiated.)

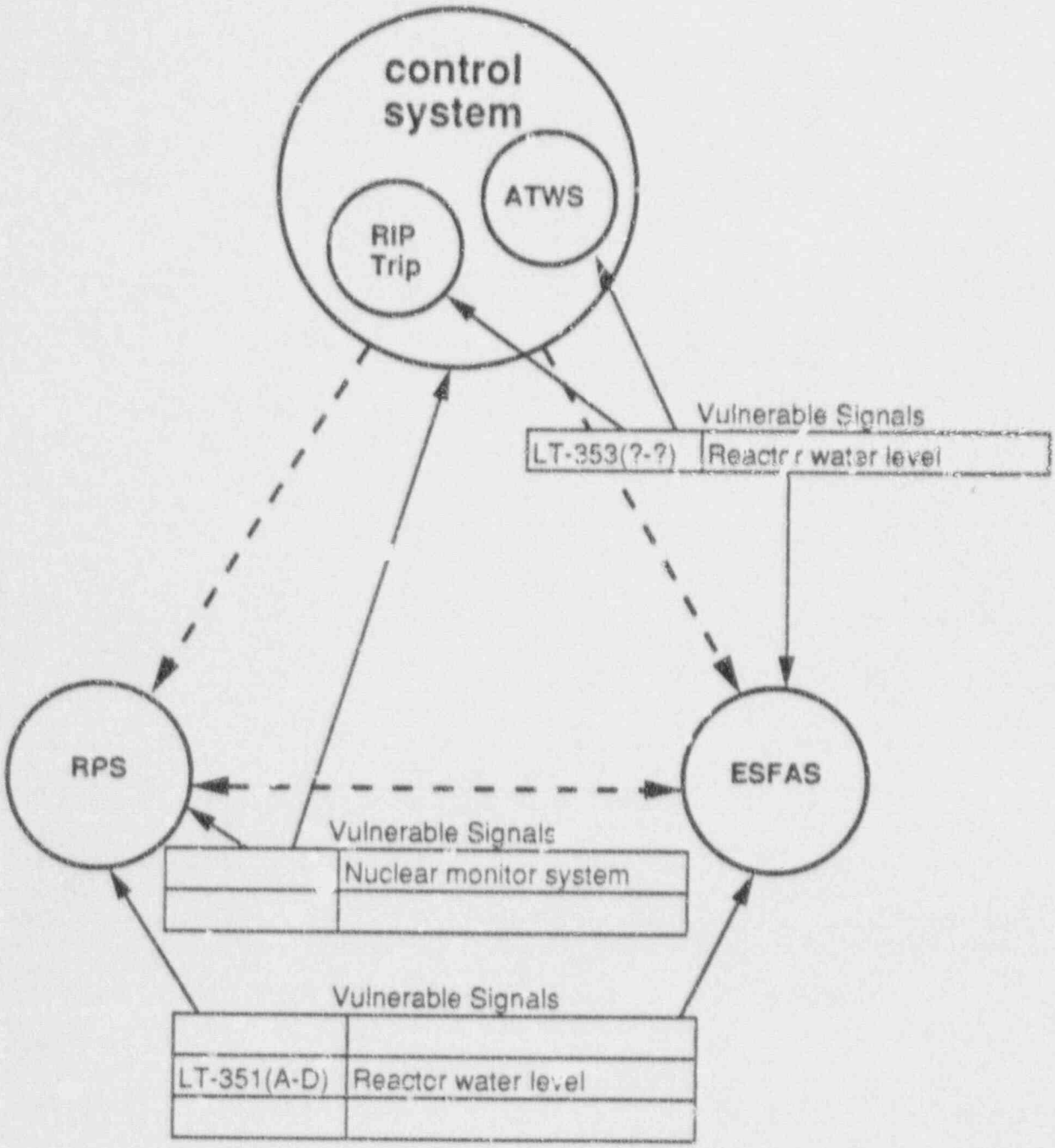


Figure 9 : Echelon diagram showing shared signals which are vulnerable to causing multiple failures either by induced transient (fault type 1) or by latent fault (fault type 2).

5.2.5 The TLU

On GE drawing 103E1805, sheets 1 - 5, it is indicated that manual control of the ECCS from the control room is exercised through the TLU and the multiplexer. A failure of the TLU will not only prevent automatic initiation of the ECCS but will also prevent manual initiation of that system. Further, if the multiplexer fails in such a way that initiation signals are inhibited, manual and automatic initiation of the ECCS is similarly prevented.

5.2.6 High water level

Although this assessment does not include detailed analysis of the control system, a potential problem was observed in the control system while searching the documentation and that problem is presented here.

In the control system, the same water level sensors which are used to control feedwater flow are also used to initiate high-water turbine trip. Thus a failure which could induce an off-normal condition also inhibits corrective action. The RPS does not trip on high water level but does scram on turbine stop valve closure, which in this case will not occur (Figure 10). Although high water level is not an immediate danger to the reactor, the potential exists for this condition to remain for extended periods of time. It may be appropriate to review the effects of lengthy uncontrolled reactor high water level.

5.2.7 Local Control

Valves, pumps, and other effectors may be inoperable from local motor control centers if control room electronics fail or multiplexers fail. Logic diagrams for various devices are unclear about where logic functions are implemented and whether such functions are interconnected through the multiplexers. Some of these functions can block operation of motor contactors according to General Electric IBDs. For example, the HPCF injector valve (Figure 7.3-1d HPCF IBD sheet 4) may be inoperable from the local motor control center. Likewise, the HPCF pump (Figure 7.3-1c) may be inoperable. Figure 7.3-3j mo-F031 shows a valve which looks like a correctly hardwired local motor control center (would work if remote electronics died), but this depends upon the assumption that

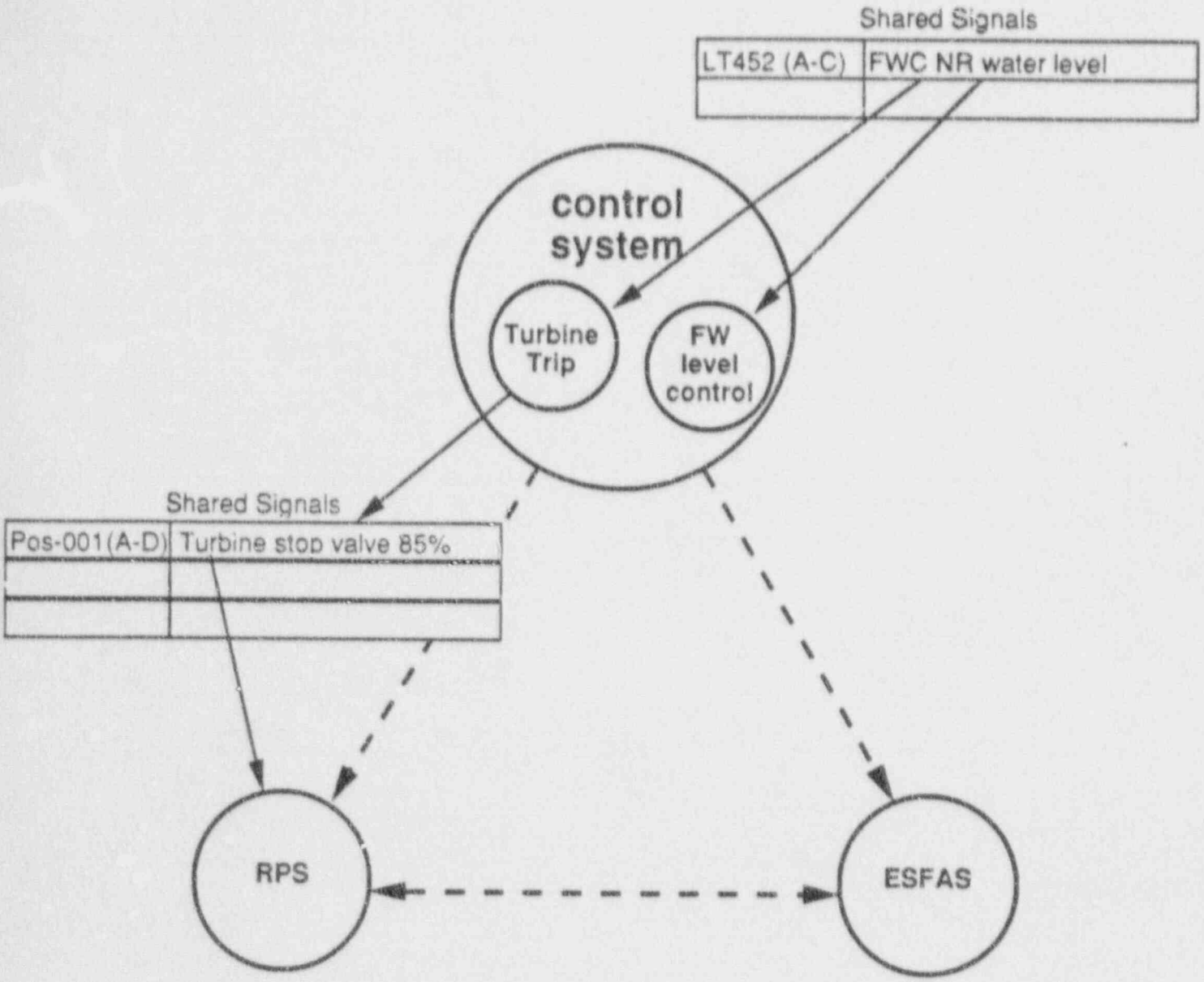


Figure 10 Echelon diagram showing shared water level signal (in control system) which may result in persistent high reactor water level. RPS will not scram because linkage is through turbine stop valve switches.

logic functions that look like motor control centers really are motor control centers.

5.3 Digital Systems Issues

The digital systems (multiplexer, DTM, TLU) are the main vulnerabilities of the protection system. Postulated common-mode failures in these modules prevent initiation of the ECCS, MSLIV closure and in some cases suppress necessary reactor scram initiation and ATWS mitigation. Further, the DTM and TLU that operate the RPS also operate the MSLIVs which are part of ESFAS. This provides a strong link between the RPS and ESFAS echelons which might prove detrimental to safe operation.

5.4 Initiation of LPFL as Backup to RCIC or HPCF

The LPFL pumps start if either low water level in the reactor is sensed or high drywell pressure is sensed. This seems to be as it should be. However, the LPFL cannot get water into the RPV unless the vessel is de-pressurized. This requires the initiation of ADS and that requires both high drywell pressure and low reactor water level. Thus LPFL is an effective backup to RCIC or HPCF only if a LOCA occurs within containment.

5.5 Plant Monitoring

The RPS and ESFAS are connected to the plant monitoring system by means for which there is no communication protocol specified or known. It therefore cannot be determined whether the plant monitor significantly impedes RPS and ESFAS or increases their complexity.

Failures of the digital units of the protection system (MPX, DTM, TLU) prevent the transmission of protection system status to the operators. The consequences of this are undetermined.

References

1) GE SAR, chapters 6, 7, 15.

2) Additional information transmitted to James Stewart (NRC) by R. W. Strong (GE) on October 22, 1991.

3) Answers to NRC concerns faxed by an unknown person (GE) to Jim Stewart and Chet Poslusny (NRC) on October 4, 1991.

4) Viewgraphs presented by M. A. Ross and B. H. Simon (GE) to the NRC on October 10, 1991.

5) ATWS supplemental information presumably authored by GE and faxed from Jim Stewart (NRC) to Robert H. Wyman (LLNL) on October 23, 1991.

6) NUREG-0493, A Defense-in-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System.

Acronym	Definition	Reference
ABWR	Advanced BWR	GE
ADS	Automatic Depressurization System	GE
APRM	Average Power Range neutron Monitor(NMS)	GE
ARI	Alternate Rod Insertion function	NRC
ATIP	Automated Traversing In-core Probe (neutron monitor)	GE
ATWS	Anticipated Transient Without Scram	NRC
BWR	Boiling Water Reactor	NRC
CAM	Containment Atmosphere Monitor system	GE
CPR	Critical Power Ratio	GE
CRD	Control Rod Drive	GE
CS	Control Systems non-1E	GE
DOD	Department of Defense	
DTM	Digital Trip Module	GE
ECCS	Emergency Core Cooling System	NRC
EDG	Emergency Diesel Generator support system	GE
EMS	Essential Multiplexing System	GE
ESFAS	Engineered Safety Feature Actuation System	NRC
FMEA	Failure Modes and Effects Analysis	IEEE
FPCS	Fuel Pool Cooling and cleanup System	GE
H/LP	High pressure/Low Pressure interlocks	GE
HECW	HVAC Emergency Cooling Water system	GE
HPCF	High Pressure Core Flooder	GE
HPIN	High Pressure Nitrogen Gas Supply	GE
HVAC	Essential HVAC system	GE
LDS	Leak Detection and isolation System	GE
LOCA	Loss of Coolant Accident	NRC
LPFL	Low Pressure FLooder	GE
LPRM	Local Power Range Monitor (Neutron monitor)	GE
MCPR	Minimum Critical Power Ratio	GE
MDT	Mean Down Time	Fisher, art
MRBM	Multi-channel Rod Block Monitor	GE
MSIV	Main Steam Isolation Valve	GE
MSLIV	Main Steam Line Isolation Valve	GE
MTBF	Mean Time Between Failures	Fisher, art.
MTDF	Mean Time to Diagnose Fault	Fisher, art
MTDL	Mean Time to Determine fault Location	Fisher, art.
MTRF	Mean Time to Replace Faulty component	Fisher, art
MTRO	Mean Time to Return to Operation	Fisher, art

Acronym	Definition	Reference
MTTF	Mean Time To Failure	GE
NMS	Neutron Monitoring System	GE
NBR	Nuclear (or Nucleate) Boiling Ratio	
NSSS	Nuclear Steam Supply System	NRC
OLU	Output Logic Unit	GE
PRM	Process Radiation Monitoring	GE
PWR	Pressurized Water Reactor	NRC
RCIC	Reactor Core Isolation Cooling system	GE
RCPB	Reactor Coolant Pressure Boundary	GE
RCW	Reactor building Cooling Water system	GE
RHR	Residual Heat Removal	NRC
RHR-SC	RHR Shutdown Cooling	GE
RHR-SP	RHR Suppression Pool cooling	GE
RHR-WD	RHR Wetwell Drywell spray	GE
RIP	Reactor Internal Pump	GE
RPS	Reactor protection System	NRC
RRS	Reactor Recirculation System	GE
RSS	Remote Shutdown System	GE
SER	Safety Evaluation Report	NRC
SACF	Single Active Component Failure	GE
SAR	Safety Analysis Report	NRC
SB&PCS	Steam Bypass and Pressure Control System	GE
SGTS	Standby Gas Treatment System	GE
SLCS	Standby Liquid Control System	GE
SLU	System Logic Unit (a form of TLU)	GE
SOE	Single Operator Failure	GE
SPTM	Suppression Pool Temperature Monitor	GE
STPT	Simulated Thermal Power Trip	GE
SRD	Safety Related Display	GE
SRNM	Start-up Range Neutron Monitor (NMS)	GE
SRP	Standard Review Plan	NRC
SRV	Safety Relief Valve	GE
SSAR	Safety System Analysis Report	NRC
SSLC	Safety System Logic and Control	GE
STS	Self Test System	GE
TLU	Trip Logic Unit	GE
UHS	Ultimate Heat Sink	GE
V&V	Validation and Verification	

Appendix A

A1. Analysis

This appendix contains the analysis done of common-mode failures (types 2 and 3) during Chapter 15 events as required by Guideline 7 of NUREG-0493. The assumptions of section 3.6 above are applied to each event and also some special assumptions are made for each event. Each analysis consists of the special assumptions, a chart like that of section 3.2 and a set of conclusions.

A2. Runout of Two Feedwater Pumps - Event 15.1.2.2.1.2

This sequence of events for this event shown in Table 15.1-5. This is a limiting fault.

A2.1 Special Assumptions:

1) Failure of the turbine stop valve switch channel ultimately leads to either a high pressure scram or an APRM scram. The former occurs at about 18 seconds and the latter at about the same time. This is approximately the same time as the scram would have occurred had the stop valve switches operated correctly. See Figure 15.1-3.

2) The high water level (L8) which initiates the turbine and feedwater pump trips is sensed by a transmitter which is part of the control system; this sensor is assumed to operate correctly. It must be noted that if this sensor channel in the control system has a CMF which causes it to fail for this event that the reactor could fill up. A scram could possibly be initiated by high flux, but sending water to the turbine seems to be a possibility.

3) Stop valve switch status enters the RPS at the DTM. See RAI response dated 10/4/91, number 9a, page 15.

A2.2 Conclusions

Failure 1 is actually two failures in one. If the transmitter sticks indicating permanent high water level the injection valve for HPCF will never open. If the transmitter sticks indicating permanent intermediate water level then the injection valve, once open, will never close and the reactor may overflow. (If the transmitter sticks at a permanent low level, there is a permanent scram initiated.)

The behavior of RCIC for failure 1 is straight forward. If the channel sticks below the high water level setpoint (L8) then the reactor may overflow. If the channel sticks at or above the high water level setpoint RCIC will not initiate.

Mitigation for failures 3, 6 and 8 involves normal operation of the protection systems. For failure 15, the primary scram initiator is not available but either of the two secondary initiators will provide scram.

DBE 15.1.2

Feedwater controller failure

Table 15.1-5

Legend:

blank - not involved or not affected
0 - not available due to postulated CMF
1 to 11 - actual initiating parameter

Event 15.1.2 / CMF Groups / Plant Parameter	351A-D Narrow level	353A-D Wide level	353E-H Wide level	CRD Accum. Pressure	Drywell Pressure	RPV Pressure	PRRM (MSL rad.)	APRM (run rad.)	SRNM (start rad.)	MPX	DTM	TLU	Accelerometers	MSIV Position	Turbine Stop Valve Switch	Turbine Control Valve Switch	Turbine Oil Pressure Sw.				
1 Low Water Level	0	O	O							O	O	O									ECCS initiator
2 Hi Water Level	0																				
3 RPV High Pressure						O				O	O	O									Secondary scram initiator
4 High Drywell Pressure																					
5 High Reactivity								O				O									Secondary scram initiator
6 High MSL Radiation																					
7 MSLIV																					
8 Earthquake																					
9 Turbine Valves Closing											O	O			O						Primary scram initiator
10 CRD Pressure Low																					
Mitigation	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17				
Scram	9	9	9			9		9		9	5	O			3/5						
ARI												3									
HPCF	0/1	1								O	O	O									Secondary core cooler
RCIC	0/1	O	1			1		1		O	O	O			1						Primary core cooler
LFFL	O	O								O	O	O									Unavailable because ADS will not initiate
SLCS																					
MSLIV																					
ADS	O	O								O	O	O									ADS requires high drywell pressure
SRV																					
Information										O	O	O									

Mitigation for failure 2 involves initiation of the HPCF.

For failures 10 and 11, scram is initiated by either the primary or one of the secondary initiators. However, no ECCS is available and the core may become exposed. Manual actuation of the ECCS from the control room is also inhibited. See GE drawings 103E1805 sheets 1 - 5.

Failure 12 requires ATWS to scram the reactor but again no ECCS is available either manually or automatically.

The primary reactor scram initiators are the switches on the turbine stop valves with high RPV pressure and high neutron flux providing diverse initiators. Much or all of this diversity is lost with CMFs in the digital systems (MPX, DTM, TLU).

Manual scram and ARI from the control system together with the RPS scrams described above provide defense-in-depth. Much of this depth is lost, however, with CMFs in the digital systems (MPX, DTM, TLU).

RCIC provides the first level of ECCS with HPCF providing diversity. LPFL is not available for this event (see below). But CMFs of the digital systems eliminate all diversity.

The only defense-in-depth for the ECCS is provided by the manual controls in the control room. But these are inoperative with CMFs of the MPX or TLU.

It should be noted that LPFL is never available because ADS will never initiate. ADS initiation requires high drywell pressure as well as low water level. See figure 7.3-2h. The design requirements for this (RHR starting on either low water level or high drywell pressure but ADS requiring both low level and high pressure) are not obvious and it is possible that there is an error in the logic.

A3. Failure of Turbine Bypass and Control Valves Open

This is event 15.1.3.1.2.2 and is the failure of all the turbine bypass valves and turbine control valves in the open state - Table 15.1-7. This is a limiting fault.

A3.1 Special Assumptions:

1) Failure of the turbine stop valve switch channel ultimately leads to a high pressure scram. The high pressure scram occurs at about 5 seconds after the start of the incident. This is approximately 2 seconds after the scram would have occurred had the stop valve switches operated correctly. See Figure 15.1-5.

2) The high water level (L8) which initiates the turbine and feedwater pump trips is sensed by a transmitter which is part of the control system; this sensor is assumed to operate correctly. If this sensor fails, then neither the turbine, feedwater pumps nor the reactor will trip. If the feedwater control system does not or cannot control the reactor level then sending water droplets to the turbine becomes a possibility.

3) Stop valve switch status enters the RPS at the DTM. See RAI response dated 10/4/91, number 9a, page 15.

A3.2 Conclusions

Failure 1 is actually two failures in one. If the transmitter sticks indicating permanent high water level the injection valve for HPCF will never open. If the transmitter sticks indicating permanent intermediate water level then the injection valve, once open, will never close and the reactor may overflow. (If the transmitter sticks at a permanent low level, there is a permanent scram initiated.)

The behavior of RCIC for failure 1 is straight forward. If the channel sticks below the high water level setpoint (L8) then the reactor may overflow. If the channel sticks at or above the high water level setpoint RCIC will not initiate.

Failures 3 and 6 do not change system operation from normal. Failure 15 causes the scram to be initiated by a secondary initiator but otherwise system operation is normal.

DBE 15.1.3

Failure of turbine bypass and control valves open

Legend:
blank - not involved or not affected
0 - not available due to postulated CMF
1 to 11 - actual initiating parameter

Event 15.1.3 / Plant Parameter	CMF Groups	351A-D Narrow level	353A-D Wide level	353E-H Wide level	CRD Accum. Pressure	Drywell Pressure	RPV Pressure	PRNM (MSL rad.)	APRM (run rad.)	SRNM (start rad.)	MPX	DTM	TLU	Accelerometers	MSIV Position	Turbine Stop Valve Switch	Turbine Control Valve Switch	Turbine Oil Pressure Sw				
1 Low Water Level		0	O	O							O	O	O									ECCS initiator
2 Hi Water Level		0																				
3 RPV High Pressure							O				O	O	O									Secondary scram initiator
4 High Drywell Pressure																						
5 High Reactivity																						
6 High MSL Radiation																						
7 MSLIV																						
8 Earthquake																						
9 Turbine Valves Closing												O	O			O						Primary scram initiator
10 CRD Pressure Low																						
Mitigation		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17				
Scram		9	9	9			9				9	O	O			3						
ARI												3	3									
HPCF		0	1								O	O	O									Secondary core cooler
RCIC		0 1	O	1			1				O	O	O			1						Primary core cooler
LPFL		O									O	O	O									Unavailable because ADS will not initiate
SLCS																						
MSLIV																						
ADS		O									O	O	O									ADS requires high drywell pressure
SRV																						
Information											O	O	O									

Failure 2 has a normal scram but the HPCF is initiated when RCIC fails to start.

For failure 10, the scram is normal but no ECCS is available to cool the core if needed. For failures 11 and 12, ARI is required to scram the reactor and again there is no ECCS. Further, for failures 10 and 12, manual initiation of the ECCS from the control room controls is prevented because both the MPX and the TLU are needed for initiation.

Closing of the turbine stop valve is the primary scram initiator with reactor high pressure providing a diverse initiator. This diversity vanishes for failures of the DTM or TLU.

Defense-in-depth for reactor scram is provided by the control system with manual controls and ARI.

RCIC and HPCF provide diverse methods for cooling the core. However, all diversity vanishes and nothing is left with failures in the digital systems. It should be noted that although LPFL will start automatically it is never effective because ADS will never initiate. ADS initiation requires high drywell pressure. See figure 7.3-2h.

Defense-in-depth for the ECCS is provided by manual initiation of the ECCS from the control room, provided there is time for operator action. Again, however, the depth vanishes for MPX and TLU CMFs since not only does the ECCS not automatically initiate but manual initiation from the control room is also prevented. See GE drawing 103E1805, sheets 1 - 5. If only the DTM fails manual initiation still works.

A4. Inadvertent Cooling of the Reactor

This is event 15.1.6 and is the cooling of the reactor by inadvertent operation of the RHR heat exchanger - Table 15.1-9. This event is a limiting fault.

A4.1 Special Assumptions:

1) The TLU is the only unit that sends information to the control system for display to the operators. Only status information is sent.

2) There is no backup scram for this incident since:

a. There is not enough pressure to scram on high pressure and such a pressure cannot be reasonably expected to occur.

b. Low water level is not part of this scenario.

c. No other possible scram initiators are part of this scenario.

DBE 15.1.6

Inadvertant RHR cooling

Table 15.1-9

Event 15.1.6 / Reactor Parameter	CMF Groups	351A-D Narrow level	353A-D Wide level	353E-H Wide level	CRD Accum. Pressure	Drywell Pressure	RPV Pressure	PRRM (MSL rad.)	APRM (run rad.)	SRNM (start rad.)	MPX	DTM	TLU	Accelerometers	MSIV Position	Turbine Stop Valve Switch	Turbine Control Valve Switch	Turbine Oil Pressure Sw				
1 Low Water Level																						
2 Hi Water Level																						
3 RPV High Pressure																						
4 High Drywell Pressure																						
5 High Reactivity										O			O									Scram initiator
6 High MSL Radiation																						
7 MSLIV																						
8 Earthquake																						
9 Turbine Valves Closing																						
10 CRD Pressure Low																						
Mitigation																						
Scram										O			O									
ARI																						
HPCF																						
RCIC																						
LPFL																						
SLCS																						
MSLIV																						
ADS																						
SRV																						
Information										O			O									

Legend:

blank - not involved or not affected
0 - not available due to postulated CMF
1 to 11 - actual initiating parameter

A4.2 Conclusions

It is not clear whether or not this is an unsafe common-mode failure. Certainly if the SRNM system does not cause a scram then the reactor will keep cooling and the neutron flux will keep increasing, making the core hotter and hotter. This is, however, either start-up or shut-down mode and the operators should be more alert than perhaps they would be when in full power steady state operation. Thus they should catch the problem prior to a disaster.

The defense-in-depth and diversity here is essentially zero with the operators providing all of the backup to the SRNM.

A5. Inadvertent Closure of One Turbine Control Valve

This is incident 15.2.1.1.2.1 and is the inadvertent closure of one main turbine control valve - Table 15.2-1. The incident is treated as a moderate frequency operational occurrence and classified as an anticipated operational transient.

A5.1 Assumptions:

1) Neutron flux increases rapidly because of void reduction caused by reactor pressure increase. From Figure 15.2-1, upper-righthand curve, failure to scram on neutron flux level should result in reactor dome pressure exceeding the scram trip point of 1105 psig (Table 15.0-1) at about 2.0 to 2.5 seconds into the incident. This causes an additic delay of 0.5 to 1.0 seconds over what would occur with neutron flux scram. The sequelae of this delay are unknown. Reactor water would decrease, but would not reach trip level before pressure trip (Figure 15.2-1, lower-lefthand curve).

2) MSLIVs do not close so that adequate steam is available to maintain operation of the feedwater pumps, which in turn maintain the water level in the RPV. (Low turbine inlet pressure will close the MSLIV, but the sensor for this parameter is upstream of the stop valve.)

3) Turbine fast solenoid valve switches will not actuate on inadvertent closure of a main turbine control value.

4) Reactor pressure indication enters the RPS through the EMS. APRM trip output enters the RPS through the TLU modules.

Incident 15.2.1

DBE 15.2.1
Inadvertent Closure Main Turbine Valve, Table 15.2-1

Reactor Parameter \ CMF Groups	351A-D Narrow level	353A-D Wide level	353E-H Wide level	CRD Accum. Pressure	Drywell Pressure	RPV Pressure	PRRM (MSL rad.)	APRM (run rad.)	SRNM (start rad.)	MPX	DTM	TLU	Accelerometers	MSIV Position	Turbine Stop Valve Switch	Turbine Fast Solenoid Valve	Turbine Oil Pressure Sw.			
1 Low Water Level										O										
2 Hi Water Level																				
3 RPV High Pressure										O	O	O								
4 High Drywell Pressure																				
5 High Reactivity								O				O								
6 High MSL Radiation																				
7 MSLIV																				
8 Earthquake																				
9 Turbine Valves Closing																				
10 CRD Pressure Low																				
Mitigation	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	CJ
Scram								3		5	5	O								
ARI												3								
HPCF										O										
RCIC										O										
LPFL										O										
SLCS																				
MSLIV																				
ADS										O										
SRV																				
info										O		O								

Legend:
blank - not involved or not affected
0 - not available due to pos. ated CMF
1 to 11 - actual initiating parameter

ECCS initiator

Secondary scram initiator

Primary scram initiator

DID Scram

A5.2 Conclusions

Common-mode failure of the primary scram initiator channel (column 8) will result in a backup scram due to high pressure. The control system will provide adequate core cooling (feedwater pump control) in all instances except for a failure of the multiplexer block, which disables the feedwater control system (column 10). This also disables all ESF mitigation and manual operation of ESF from the control room. DTM block failure results in a backup scram due to high pressure, but cooling is provided by the feedwater control system (column 11). Likewise, TLU failure disables RPS scram, but this is backed up by ARI and the feedwater control system (column 12). ESF is ineffective in both columns 11 and 12.

In failure 10, there is no diverse signal and no echelon of defense (including operator manual action) which can actuate the Engineered Safety Features. In all other failures, diversity and DiD provide both scram and core cooling when challenged.

A6. Pressure Regulator Downscale Failure

This accident, event number 15.2.1.1.2.2, is the failure of steam pressure regulator wherein all valves close attempting to go to zero pressure at the turbine inlet - Table 15.2-2. The accident is treated as a once-in-time (plant lifetime) postulated occurrence and classified as a limiting fault.

A6.1 Special Assumptions:

1) Neutron flux increases rapidly because of void reduction caused by reactor pressure increase. From Figure 15.2-2, upper-righthand curve, failure to scram on neutron flux level should result in reactor dome pressure exceeding the scram trip point of 1105 psig (Table 15.0-1) at less than 2.0 seconds into the incident. This causes an additional delay of less than 0.5 seconds over what would occur with neutron flux scram. The sequelae of this delay are unknown. Reactor water would decrease, but would not reach trip level before pressure trip (Figure 15.2-2, lower-lefthand curve).

2) MSLIVs do not close so that adequate steam is available to maintain operation of the feedwater pumps, which in turn maintain the water level in the RPV. (Low turbine inlet pressure will close the MSLIV, but the sensor for this parameter is upstream of the stop valve.)

3) Turbine valve switches will not actuate on pressure regulation failure.

4) Reactor pressure indication enters the RPS through the EMS. APRM trip output enters the RPS through the TLU modules.

Accident 15.2.1 / Reactor Parameter	CMF Groups	351A-D Narrow level	353A-D Wide level	353E-H Wide level	CRD Accum. Pressure	Drywell Pressure	RPV Pressure	PRRM (MSL rad.)	APRM (run rad.)	SRNM (start rad.)	MPX	DTM	TLU	Accelerometers	MSIV Position	Turbine Stop Valve Switch	Turbine Fast Solenoid Valve	Turbine Oil Pressure Sw.				
1 Low Water Level											O											
2 Hi Water Level																						
3 RPV High Pressure											O	O	O									
4 High Drywell Pressure																						
5 High Reactivity									O				O									
6 High MSL Radiation																						
7 MSLIV																						
8 Earthquake																						
9 Turbine Valves Closing																						
10 CRD Pressure Low																						
Mitigation	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20		
Scram								3		5	5	O										
ARI												3										
HPCF										O												
RCIC										O												
LPFL										O												
SLCS																						
MSLIV																						
ADS										O												
SRV																						
info										O		O										

CFE 15.2.1
Pressure regulator downscale failure, Table 15.2-2

Code:
Blank - not involved or not affected
0 - not available due to postulated CMF
1 to 1? - actual initiating parameter

ECCS initiator

Secondary scram initiator

Primary scram initiator

DID Scram

A6.2 Conclusions

Common-mode failure of the primary scram initiator channel (column 8) will result in a backup scram due to high pressure. The control system will provide adequate core cooling (feedwater pump control) in all instances except for a failure of the multiplexer block, which disables the feedwater control system (column 10). This also disables all ESF mitigation and manual operation of the ESF from the control room. DTM block failure results in a backup scram due to high pressure, but cooling is provided by the feedwater control system (column 11). Likewise, TLU failure disables RPS scram, but this is backed up by ARI and the feedwater control system (column 12). ESF is ineffective in both columns 11 and 12.

In failure 10, there is no diverse signal and no echelon of defense (including operator manual action) which can actuate the Engineered Safety Features. In all other failures, diversity and DID provide both scram and core cooling when challenged.

Because this event is an accident and because ATWS is not classified as a safety system, it may fail due to relaxed maintenance requirements or exposure to harsh accident conditions.

A7. Generator Load Rejection with Normal Bypass

This incident, number 15.2.2.2.1.2, is generator load rejection with normal bypass - Table 15.2-3. The incident is treated as a moderate frequency operational occurrence and classified as an anticipated operational transient.

A7.1 Special Assumptions:

1) The primary reactor trip indication is actuation of the turbine fast closure solenoid valves. From Figure 15.2-3, upper-lefthand curve, neutron flux increases rapidly because of void reduction caused by reactor pressure increase, reaching a peak of 137.1% NBR (Table 15.0-2) at about 0.7 seconds into the incident. Failure to scram on turbine fast closure solenoid valve operation should be followed almost immediately by a neutron flux scram at 127.5% NBR (Table 15.0-1). From Figure 15.2-3, upper-righthand curve, failure to scram on neutron flux level should result in reactor dome pressure exceeding the scram trip point of 1105 psig (Table 15.0-1) no later than about 1.0 seconds into the incident.

2) MSLIVs do not close so that adequate steam is available to maintain operation of the feedwater pumps, which in turn maintain the water level in the RPV. (Low turbine inlet pressure will close the MSLIV, but the sensor for this parameter is upstream of the stop valve.)

3) Reactor pressure indication enters the RPS through the EMS. APRM trip output enters the RPS through the TLU modules. Turbine valve status enters the RPS through the DTM modules.

Incident 15.2.2

DBE 15.2.2
Generator load rejection with normal bypass, Table 15.2-3

Reactor Parameter \ CMF Groups	351A-D Narrow level	353A-D Wide level	353-H Wide level	CRD Accum. Pressure	Drywell Pressure	RPV Pressure	PRRM (MSL rad.)	APRM (run rad.)	SRNM (start rad.)	MPX	OTM	TLU	Accelerometers	MSIV Position	Turbine Stop Valve Switch	Turbine Fast Solenoid Valve	Turbine Oil Pressure Sw
1 Low Water Level										O							
2 Hi Water Level																	
3 RPV High Pressure										O	O	O					
4 High Drywell Pressure																	
5 High Reactivity												O					
6 High MSL Radiation																	
7 MSLIV																	
8 Earthquake																	
9 Turbine Valves Closing											O	O				O	
10 CRD Pressure Low																	

Mitigation	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Scram										9	5	O				5		
ARI												3						
HPCF										O								
RCIC										O								
LPFL										O								
SLCS																		
MSLIV																		
ADS										O								
SRV																		
info										O		O						

Legend:
blank - not involved or not affected
0 - not available due to postulated CMF
1 to 11 - actual initiating parameter

ECCS initiator

Tertiary initiator

Secondary initiator

Primary initiator

DID Scram

A7.2 Conclusions

Common-mode failure of the primary scram initiator channel (column 16) will result in a backup scram due to high flux. The control system will provide adequate core cooling (feedwater pump control) in all instances except for a failure of the multiplexer block, which disables the feedwater control system (column 10). This also disables all ESF mitigation and manual operation of the ESF from the control room. DTM block failure results in a backup scram due to high flux, but cooling is provided by the feedwater control system (column 11). Likewise, TLU failure disables RPS scram, but this is backed up by ARI and the feedwater control system (column 12). ESF is ineffective in both columns 11 and 12.

In failure 10, there is no diverse signal and no echelon of defense (including operator manual action) which can actuate the Engineered Safety Features. In all other failures, diversity and DID provide both scram and core cooling when challenged.

A8. Generator Load Rejection with the Failure of All Bypass Valves

This accident, number 15.2.2.2.1.3, is generator load rejection with all bypass valves failing - Table 15.2-5. The accident is treated as a one-time (plant lifetime) postulated occurrence and classified as a limiting fault. This event is more stressing than generator load rejection with one bypass valve failure and the analysis for total bypass failure is considered to encompass the analysis for one bypass failure.

A8.1 Specific Assumptions

1) The primary reactor trip indication is actuation of the turbine fast closure solenoid valves. From Figure 15.2-5, upper-lefthand curve, neutron flux increases rapidly because of void reduction caused by reactor pressure increase, reaching a peak of 157.6% NBR (Table 15.0-2) at about 0.6 seconds into the incident. Failure to scram on turbine fast closure solenoid valve operation should be followed almost immediately by a neutron flux scram at 127.5% NBR (Table 15.0-1). From Figure 15.2-5, upper-righthand curve, failure to scram on neutron flux level should result in reactor dome pressure exceeding the scram trip point of 1105 psig (Table 15.0-1) no later than about 0.6 seconds into the incident.

2) MSLIVs do not close so that adequate steam is available to maintain operation of the feedwater pumps, which in turn maintain the water level in the RPV. (Low turbine inlet pressure will close the MSLIV, but the sensor for this parameter is upstream of the stop valve.)

3) Reactor pressure indication enters the RPS through the EMS. APRM trip output enters the RPS through the TLU modules. Turbine valve status enters the RPS through the DTM modules.

Accident 15.2.2

DBE 15.2.2
Generator load rejection with treal bypass failure, Table 15.2-5

Legend:
blank - not involved or not affected
0 - not available due to postulated CMF
1 to 11 - actual initiating parameter

Reactor Parameter \ CMF Groups	351A-D Narrow level	353A-D Wide level	353E-H Wide level	CRD Accum. Pressure	Drywell Pressure	RPV Pressure	PRRM (MSL rad.)	APRM (run rad.)	SRNM (start rad.)	MPX	DTM	TLU	Accelerometers	MSIV Position	Turbine Stop Valve Switch	Turbine Fast Solenoid Valve	Turbine Oil Pressure Sw				
1 Low Water Level										O											ECCS initiator
2 Hi Water Level																					
3 RPV High Pressure										C	O	O									Tertiary initiator
4 High Drywell Pressure																					
5 High Reactivity												O									Secondary initiator
6 High MSL Radiation																					
7 MSLIV																					
8 Earthquake																					
9 Turbine Valves Closing											O	O				O					Primary initiator
10 CRD Pressure Low																					

Mitigation	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	
Scram										9	5	O				5					
ARI												3									DID Scram
HPCF										O											
RCIC										O											
LPFL										O											
SLCS																					
MSLIV																					
ADS										O											
SRV																					
info										O		O									

A8.2 Conclusions

Common-mode failure of the primary scram initiator channel (column 16) will result in a backup scram due to high flux. The control system will provide adequate core cooling (feedwater pump control) in all instances except for a failure of the multiplexer block, which disables the feedwater control system (column 10). This also disables all ESF mitigation and manual operation of the ESF from the control room. DTM block failure results in a backup scram due to high flux, but cooling is provided by the feedwater control system (column 11). Likewise, TLU failure disables RPS scram, but this is backed up by ARI and the feedwater control system (column 12). ESF is ineffective in both columns 11 and 12.

In failure 10, there is no diverse signal and no echelon of defense (including operator manual action) which can actuate the Engineered Safety Features. In all other failures, diversity and DID provide both scram and core cooling when challenged.

Because this event is classified as a limiting fault and ATWS is not classified as a safety system, it may fail due to relaxed maintenance requirements or exposure to harsh accident conditions.

A9. Turbine Trip with Normal Bypass

This incident, number 15.2.3.2.1.1, is turbine trip with normal bypass - Table 15.2-6. The incident is treated as a moderate frequency operational occurrence and classified as an anticipated operational transient.

A9.1 Special Assumptions

1) The primary reactor trip indication is actuation of turbine stop valve 85% switches. From Figure 15.2-6, upper-lefthand curve, neutron flux begins to increase rapidly because of void reduction caused by reactor pressure increase, but the peak value reached in this simulation is 111.8% NBR (Table 15.0-2), due to simulated scram at 0.2 seconds (Figure 15.2-6 lower-righthand curve). If the turbine stop valve switches fail, this incident is most similar to accident 15.2.1, pressure regulator downscale failure. From accident 15.2.1, failure to scram on turbine stop valve 85% switches should be followed 1.2 seconds later (Figure 15.2-2, lower-righthand curve) by a neutron flux scram at 127.5% NBR (Table 15.0-1). From Figure 15.2-2, upper-righthand curve, failure to scram on neutron flux level should result in reactor dome pressure exceeding the scram trip point of 1107 psig (Table 15.0-1) after an additional delay of 0.8 seconds. The effects of these additional delays are unknown.

2) MSLIVs do not close so that adequate steam is available to maintain operation of the feedwater pumps, which in turn maintain the water level in the RPV. (Low turbine inlet pressure will close the MSLIV, but the sensor for this parameter is upstream of the stop valve.)

3) Reactor pressure indication enters the RPS through the EMS. APRM trip output enters the RPS through the TLU modules. Turbine valve status enters the RPS through the DTM modules.

Incident 15.2.3

DBE 15.2.3
Turbine trip with normal bypass, Table 15.2-6

Legend:
blank - not involved or not affected
0 - not available due to postulated CMF
1 to 11 - actual initiating parameter

Reactor Parameter \ CMF Groups	351A-D Narrow level	353A-D Wide level	353E-H Wide level	CRD Accum. Pressure	Drywell Pressure	RPV Pressure	PRAM (MSL rad.)	APRM (run rad.)	SRNM (start rad.)	MPX	DTM	TLU	Accelerometers	MSIV Position	Turbine Stop Valve Switch	Turbine Fast Solenoid Valve	Turbine Oil Pressure Sw				
1 Low Water Level										O											ECCS initiator
2 Hi Water Level																					
3 RPV High Pressure										O	O	O									Tertiary scram initiator
4 High Drywell Pressure																					
5 High Reactivity												O									Secondary scram initiator
6 High MSL Radiation																					
7 MSLIV																					
8 Earthquake																					
9 Turbine Valves Closing											O	O			O						Primary scram initiator
10 CRD Pressure Low																					
Mitigation	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	
Scram										9	5	O			5						
ARI												3									DID Scram
HPCF										O											
RCIC										O											
LPFL										O											
SLCS																					
MSLIV																					
ADS										O											
SRV																					
info										O		O									

A9.2 Conclusions

Common-mode failure of the primary scram initiator channel (column 15) will result in a backup scram due to high flux delayed approximately 1.2 seconds. Additional diversity is provided by reactor vessel high pressure but with further delay of 0.8 seconds. The control system will provide adequate core cooling (feedwater pump control) in all instances except for a failure of the multiplexer block, which disables the feedwater control system (column 10). This also disables all ESF mitigation and manual operation of the ESF from the control room. DTM block failure results in a backup scram due to high flux, but cooling is provided by the feedwater control system (column 11). Likewise, TLU failure disables RPS scram, but this is backed up by ARI and the feedwater control system (column 12). ESF is ineffective in both columns 11 and 12.

In failure 10, there is no diverse signal and no echelon of defense (including operator manual action) which can actuate the Engineered Safety Features. In all other failures, diversity and DID provide both scram and core cooling when challenged.

The effects of delays on fuel condition are not known.

A10. Turbine Trip with All Bypass Valves Failing

This accident, number 15.2.3.2.1.3, is a turbine trip with all bypass valves failing - Table 15.2-8. The accident is treated as a one-time (plant lifetime) postulated occurrence and classified as a limiting fault. This event is more stressing than turbine trip with one bypass valve failure and the analysis for total bypass failure is considered to encompass the analysis for one bypass failure.

A10.1 Special Assumptions

1) The primary reactor trip indication is actuation of the turbine stop valve 85% switches. From Figure 15.2-8, upper-lefthand curve, neutron flux increases rapidly because of void reduction caused by reactor pressure increase, reaching a peak of 137.5% NBR (Table 15.0-2) at about 0.8 seconds into the accident. Failure to scram on turbine stop valve 85% switches should be followed by a neutron flux scram at 127.5% NBR (Table 15.0-1) delayed by about 0.8 seconds. From Figure 15.2-8, upper-righthand curve, failure to scram on neutron flux level should result in reactor dome pressure exceeding the scram trip point of 1105 psig (Table 15.0-1) no later than about 1.0 seconds into the incident.

2) MSLIVs do not close so that adequate steam is available to maintain operation of the feedwater pumps, which in turn maintain the water level in the RPV. (Low turbine inlet pressure will close the MSLIV, but the sensor for this parameter is upstream of the stop valve.)

3) Reactor pressure indication enters the RPS through the EMS. APRM trip output enters the RPS through the TLU modules. Turbine valve status enters the RPS through the DTM modules.

DBE 15.2.3

Turbine trip with total bypass failure, Table 15.2-8

Legend:

blank - not involved or not affected
0 - not available due to postulated CMF
1 to 11 - actual initiating parameter

Accident 15.2.3 / CMF Groups / Reactor Parameter	351A-D Narrow level	353A-D Wide level	353E-H Wide level	CRD Accum. Pressure	Drywell Pressure	RPV Pressure	PRRM (MSL rad.)	APRM (run re	SRN (start rad.)	MPX	DTM	TLU	Accelerometers	MSIV Position	Turbine Stop Valve Switch	Turbine Fast Solenoid Valve	Turbine Oil Pressure Sw.				
1 Low Water Level										0											ECCS initiator
2 Hi Water Level																					
3 RPV High Pressure										0	0	0									Tertiary scram initiator
4 High Drywell Pressure																					
5 High Reactivity												0									Secondary scram initiator
6 High MSL Radiation																					
7 MSLIV																					
8 Earthquake																					
9 Turbine Valves Closing											0	0			0						Primary scram initiator
10 CRD Pressure Low																					
Mitigation	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	
Scram										9	5	0			5						
ARI												3									DID Scram
HPCF										0											
RCIC										0											
LPFL										0											
SLCS																					
MSLIV																					
ADS										0											
SRV																					
info										0		0									

A10.2 Conclusions

Common-mode failure of the primary scram initiator channel (column 15) will result in a backup scram due to high flux with a delay of approximately 0.8 seconds. Additional diversity is provided by reactor vessel high pressure. The control system will provide adequate core cooling (feedwater pump control) in all instances except for a failure of the multiplexer block, which disables the feedwater control system (column 10). This also disables all ESF mitigation and manual operation of the ESF from the control room. DTM block failure results in a backup scram due to high flux, but cooling is provided by the feedwater control system (column 11). Likewise, TLU failure disables RPS scram, but this is backed up by ARI and the feedwater control system (column 12). ESF is ineffective in both columns 11 and 12.

In failure 10, there is no diverse signal and no echelon of defense (including operator manual action) which can actuate the Engineered Safety Features. In all other failures, diversity and DID provide both scram and core cooling when challenged.

The accident is classified as a limiting fault. The ATWS is not classified as a safety system and may fail due to relaxed maintenance requirements or exposure to harsh accident conditions.

A11. Inadvertent Closure of All MSLIVs

This incident, number 15.2.4.1.2.1, is inadvertent closure of all Main Steam Line Isolation Valves - Table 15.2-9. The incident is treated as a moderate frequency operational occurrence and classified as an anticipated operational transient.

A11.1 Special Assumptions

1) The primary reactor trip indication is actuation of MSLIV 85% switches. From Figure 15.2-9, peak neutron flux level in this simulation is 105.7% NBR (Table 15.0-2), due to simulated scram at 0.4 seconds (Figure 15.2-9 lower-righthand curve). If the MSLIV switches fail, this incident is most similar to accident 15.2.1, pressure regulator downscale failure. From accident 15.2.1, failure to scram on MSLIV 85% switches should be followed 1.2 seconds later (Figure 15.2-2, lower-righthand curve) by a neutron flux scram at 127.5% NBR (Table 15.0-1). From Figure 15.2-3, upper-righthand curve, failure to scram on neutron flux level should result in reactor dome pressure exceeding the scram trip point of 1105 psig (Table 15.0-1) after an additional delay of 0.8 seconds. The effects of these additional delays are unknown.

2) RCIC is expected to be required because closure of MSLIV inhibits steam flow to feedwater pump turbines. Alternative mitigation is HPCF, followed by ADS blowdown and LPFL if HPCF fails.

3) Reactor pressure indication enters the RPS through the EMS. APRM trip output enters the RPS through the TLU modules. Turbine valve status enters the RPS through the DTM modules.

Incident 15.2.4

DBE 15.2.4
Inadvertent MSLIV closure,
Table 15.2-9

Legend:
blank - not involved or not affected
0 - not available due to postulated CMF
1 to 11 - actual initiating parameter

Reactor Parameter \ CMF Groups	351A-D Narrow level	353A-D Wide level	353E-H Wide level	CRD Accum. Pressure	Drywell Pressure	RPV Pressure	PRRM (MSL rad.)	APRM (run rad.)	SRNM (start rad.)	MPX	DTM	TLU	Accelerometers	MSIV Position	Turbine Stop Valve Switch	Turbine Fast Solenoid Valve	Turbine Oil Pressure Sw.				
1 Low Water Level	0	O	O							O	O	O									ECCS initiator
2 Hi Water Level	0																				Injection and turbine permissive
3 RPV High Pressure						O				O	O	O									Tertiary initiator
4 High Drywell Pressure																					
5 High Reactivity								O				O									Secondary initiator
6 High MSL Radiation																					
7 MSLIV											O	O		O							Primary initiator
8 Earthquake																					
9 Turbine Valves Closing																					
10 CRD Pressure Low																					
Mitigation	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	
Scram	7	7	7			7		7		7	5	O		5							
ARI												3									DID Scram
HPCF	0	1	O							O	O	O									Secondary core cooling
RCIC	0/1	O	1			1		1		O	O	O		1							Primary core cooling
LPFL	O									O	O	O									unavailable because no ADS
SLCS																					
MSLIV																					
ADS	O									O	O	O									ADS requires high drywell pressure
SRV																					
info										O	O	O									

A11.2 Conclusions

Common-mode failure of the primary scram initiator channel (column 14) will result in a backup scram due to high flux with a delay of approximately 0.8 seconds. Additional diversity is provided by reactor vessel high pressure. Reactor core cooling is necessary and is provided by RCIC except as noted below (feedwater pumps are unusable because feedwater pump turbine steam supply is interrupted by MSLIV closure). Multiplexer failure (column 10) results in scram but complete failure of ECCS. DTM block failure results in a backup scram due to high flux, but again with complete failure of ECCS (column 11). TLU failure disables RPS scram, but this is backed up by ARI (column 12). However, ECCS fails to operate.

Columns 1 through 3 demonstrate water level channel failures. For failure 2, diverse initiation of HPCF backs up RCIC. For failure 1 there are two possible modes of failure. If the transmitter sticks indicating permanent high water level the injection valve for HPCF will never open and RCIC turbines will not start. If the transmitter sticks indicating permanent intermediate or low water level then the injection valve, once open, will never close and the reactor may overflow. (If the transmitter sticks at a permanent low level, there is a permanent scram initiated.) LPFL will start but will be ineffective without blowdown by the ADS. ADS blowdown will not occur until both low water level and high drywell pressure have existed for a timeout period, and high drywell pressure will not occur in this accident.

Summarizing, reactor scram is initiated by diverse signals (failures 11 and 14) or by DID backup by ARI (failure 12). In failures 1, 10, 11, and 12, the control system is unable to provide DID core cooling and there is no diverse method for automatic operation of any of the ECCS features. Manual blowdown of ADS is possible in failure 1, allowing LPFL to substitute for ineffective HPCF and RCIC. Manual operation of RCIC or HPCF from the control room may be possible for failure 11, but is precluded in failures 10 and 12.

Because this event is classified as a limiting fault and ATWS is not classified as a safety system, it may fail due to relaxed maintenance requirements or exposure to harsh accident conditions.

A12. Loss of Condenser Vacuum

This incident, number 15.2.5, is loss of condenser vacuum - Table 15.2-14. The incident is treated as a moderate frequency operational occurrence and classified as an anticipated operational transient.

A12.1 Special Assumptions

1) The primary reactor trip indication is actuation of turbine stop valve 85% switches. From Figure 15.2-10, upper-lefthand curve, neutron flux begins to increase rapidly because of void reduction caused by reactor pressure increase, but the peak value reached in this simulation is 111.0% NBR (Table 15.0-2), due to simulated scram at 0.2 seconds (Figure 15.2-10 lower-righthand curve). If the turbine stop valve switches fail, this incident is most similar to accident 15.2.1, pressure regulator downscale failure. From accident 15.2.1, failure to scram on turbine stop valve 85% switches should be followed 1.2 seconds later (Figure 15.2-2, lower-righthand curve) by a neutron flux scram at 127.5% NBR (Table 15.0-1). From Figure 15.2-2, upper-righthand curve, failure to scram on neutron flux level should result in reactor dome pressure exceeding the scram trip point of 1105 psig (Table 15.0-1) after an additional delay of 0.8 seconds. The effects of these additional delays are unknown.

2) Reactor pressure indication enters the RPS through the EMS. APRM trip output enters the RPS through the TLU modules. Turbine valve status enters the RPS through the DTM modules.

Incident 15.2.5

DBE 15.2.5
Loss of condenser vacuum, Table 15.2-10

Legend:
blank - not involved or not affected
0 - not available due to postulated CMF
1 to 11 - actual initiating parameter

Reactor Parameter \ CMF Groups	351A-D Narrow level	353A-D Wide level	353E-H Wide level	CRD Accum. Pressure	Drywell Pressure	RPV Pressure	PRRM (MSL rad.)	APRM (run rad.)	SRNM (start rad.)	MPX	DTM	TLU	Accelerometers	MSIV Position	Turbine Stop Valve Switch	Turbine Fast Solenoid Valve	Turbine Oil Pressure Sw				
1 Low Water Level	0	0	0																		ECCS initiator
2 Hi Water Level	0																				Injection and turbine permissive
3 RPV High Pressure										0	0	0									Tertiary scram initiator
4 High Drywell Pressure																					
5 High Reactivity												0									Secondary scram initiator
6 High MSL Radiation																					
7 MSLIV																					
8 Earthquake																					
9 Turbine Valves Closing											0	0			0						am initiator
10 CRD Pressure Low																					
Mitigation	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	
Scram	9	9	9							9	5	0			5						
ARI												3									DID Scram
HPCF	0	1	0							0	0	0									Secondary core cooling
RCIC	0/1	0	1							0	0	0									Primary core cooling
LPFL	0									0	0	0									unavailable because no ADS
SLCS																					
MSLIV																					
ADS	0									0	0	0									ADS requires high drywell pressure
SRV																					
info										0	0	0									

A12.2 Conclusions

Common-mode failure of the primary scram initiator channel (column 15) will result in a backup scram due to high flux delayed approximately 1.2 seconds. Additional diversity is provided by reactor vessel high pressure but with further delay of 0.8 seconds. The control system will be ineffective in providing core cooling because the MSLIVs are expected to close at 5 seconds due to low condenser vacuum. DTM block failure results in a backup scram due to high flux. Likewise, TLU failure disables RPS scram, but this is backed up by ARI (column 12). ESF is ineffective in columns 10 through 12.

Columns 1 through 3 demonstrate water level channel failures. For failure 2, diverse initiation of HPCF backs up RCIC. For failure 1 there are two possible modes of failure. If the transmitter sticks indicating permanent high water level the injection valve for HPCF will never open and RCIC turbines will not start. If the transmitter sticks indicating permanent intermediate or low water level then the injection valve, once open, will never close and the reactor may overflow. (If the transmitter sticks at a permanent low level, there is a permanent scram initiated.) LPFL will start but will be ineffective without blowdown by the ADS. ADS blowdown will not occur until both low water level and high drywell pressure have existed for a timeout period, and high drywall pressure will not occur in this accident.

Summarizing, reactor scram is initiated by diverse signals (failures 11 and 15) or by DID backup by ARI (failure 12). In failures 1, 10, 11, and 12, the control system is unable to provide DID core cooling and there is no diverse method for automatic operation of any of the ECCS features. Manual blowdown of ADS is possible in failure 1, allowing LPFL to substitute for ineffective HPCF and RCIC. Manual operation of RCIC or HPCF from the control room may be possible for failure 11, but is precluded in failures 10 and 12.

The effects of delays on fuel condition are not known.

A13. Loss of Auxiliary Power Transformer

This incident, number 15.2.6.1.1.1, is loss of unit auxiliary power transformer - Table 15.2-16. The incident is treated as a moderate frequency operational occurrence and classified as an anticipated operational transient.

A13.1 Special Assumptions

1) The primary scram initiator is turbine fast closure solenoid valve operation. The event is similar to a load rejection. From Figure 15.2-11, upper-righthand curve, reactor pressure exceeds the trip setpoint of 1105 psig at about 2 seconds, providing a diverse trip to the turbine fast closure solenoid valve 85% switches. The General Electric simulation differs from a load rejection, however, in that neutron flux rises during the load rejection (upper-lefthand curve, Figure 15.2-3) whereas it does not for this incident (upper-lefthand curve, Figure 15.2-11). Since there does not appear to be any significant difference between this incident and a load rejection during the early stages, high flux will be assumed to be another diverse trip, if needed.

2) General Electric SAR Chapter 15, paragraph 15.2.6.2.2.1, in sequence action 2, assumes immediate trip of half of all electrical pumps as a result of loss of electrical power. It is assumed that this occurs because of load-shedding caused by the reactor control system rather than operation of the protection system. The pumps tripped include five RIPs, one condensate pump, and two condenser circulating water pumps.

3) Feedwater pump trips as described by sequence action 3, SAR Chapter 15, paragraph 15.2.6.2.2.1 are assumed to occur.

4) Turbine trip occurs at 8 seconds after loss of unit auxiliary power transformer.

6) MSLIV closure occurs at about 28 seconds after loss of unit auxiliary power transformer. The loss of feedwater pumps and the closure of MSLIVs make ECCS a necessity, since no other cooling means are available.

7) Reactor pressure indication enters the RPS through the EMS. APRM trip output enters the RPS through the TLU modules. Turbine valve status enters the RPS through the DTM modules.

A13.2 Conclusions

Common-mode failure of the primary scram initiator channel (column 16) will result in a backup scram due to high flux with a delay of approximately 0.8 seconds. Additional diversity is provided by reactor vessel high pressure. Reactor core cooling is necessary and is provided by RCIC except as noted below (feedwater pumps are unusable because feedwater pumps are tripped and turbine steam supply is interrupted by MSLIV closure). Multiplexer failure (column 10) results in scram but complete failure of ECCS. DTM block failure results in a backup scram due to high flux, but again with complete failure of ECCS (column 11). TLU failure disables RPS scram, but this is backed up by ARI (column 12). However, ECCS fails to operate.

Columns 1 through 3 demonstrate water level channel failures. For failure 2, diverse initiation of HPCF backs up RCIC. For failure 1 there are two possible modes of failure. If the transmitter sticks indicating permanent high water level the injection valve for HPCF will never open and RCIC turbines will not start. If the transmitter sticks indicating permanent intermediate or low water level then the injection valve, once open, will never close and the reactor may overflow. (If the transmitter sticks at a permanent low level, there is a permanent scram initiated.) LPFL will start but will be ineffective without blowdown by the ADS. ADS blowdown will not occur until both low water level and high drywell pressure have existed for a timeout period, and high drywell pressure will not occur in this accident.

DBE 15.2.6
Loss of unit auxiliary transformer, Table 15.2-11

Legend:
blank - not involved or not affected
0 - not available due to postulated CMF
1 to 11 - actual initiating parameter

Incident 15.2.6 / CMF Groups / Reactor Parameter	351A-D Narrow level	353A-D Wide level	353E-H Wide level	CRD Accum. Pressure	Drywell Pressure	RPV Pressure	PRRM (MSL rad.)	APRM (run rad.)	SRNM (start rad.)	MPx	CTM	TLU	Accelerometers	MSIV Position	Turbine Stop Valve Switch	Turbine Fast Solenoid Valve	Turbine Oil Pressure Sw				
1 Low Water Level	0	0	0							0	0	0									ECCS initiator
2 Hi Water Level	0																				Injection and turbine permissive
3 RPV High Pressure						0				0	0	0									Tertiary scram initiator
4 High Drywell Pressure																					
5 High Reactivity								0				0									Secondary scram initiator
6 High MSL Radiation																					
7 MSLIV																					
8 Earthquake																					
9 Turbine Valves Closing											0	0				0					Primary scram initiator
10 CRD Pressure Low																					
Mitigation	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	
Scram	9	9	9			9		9		9	5	0				5					
ARI												3									DID Scram
HPCF	0	1	0							0	0	0									Secondary core cooling
RCIC	0/1	0	1			1		1		0	0	0				1					Primary core cooling
LPFL	0									0	0	0									unavailable because no ADS
SLCS																					
MSLIV																					
ADS	0									0	0	0									ADS requires high drywell pressure
SRV																					
info										0	0	0									

Summarizing, reactor scram is initiated by diverse signals (failures 11 and 16) or by DID backup by ARI (failure 12). In failures 1, 10, 11, and 12, the control system is unable to provide DID core cooling and there is no diverse method for automatic operation of any of the ECCS features. Manual blowdown of ADS is possible in failure 1, allowing LPFL to substitute for ineffective HPCF and RCIC. Manual operation of RCIC or HPCF from the control room may be possible for failure 11, but is precluded in failures 10 and 12.

Loss of unit auxiliary transformer and one startup transformer is not dealt with separately because the main difference, besides greater dependence on diesel generators, is the additional trip of the last three reactor recirculating pumps, which tends to further reduce reactivity. The consequences of this additional failure appear to be less than those for failure of the unit auxiliary transformer alone.

A14. Loss of Feedwater Flow

This incident, 15.2.7, is loss of feedwater flow - Table 15.2-18. The incident is treated as a moderate frequency operational occurrence and classified as an anticipated operational transient.

A14.1 Special Assumptions

1) The primary reactor trip indication is water level 3 indicated by the LT351(A-D) narrow range water level transducer channel. Neutron flux and reactor vessel pressure do not react quickly during this incident. Ultimately, the MSLIVs will close because of level 1.5 water level switches or because of low turbine inlet pressure. Secondary reactor trip indication is therefore the MSLIV 85% switches. Time delay to secondary trip is unknown. ARI at level 2 may beat the MSLIV switches.

2) RCIC is expected to be required because feedwater pump turbines are not working. Alternative mitigation is HPCF. However, since there is no leak into the drywell, ADS will not blow down the reactor and LPFL is therefore not an alternative automatic cooling means.

3) Reactor water level indication enters the RPS through the EMS. APRM trip output enters the RPS through the TLU modules. Turbine valve status enters the RPS through the DTM modules.

DBE 15.2.7
Loss of feedwater flow,
Table 15.2-18

Legend:
blank - not involved or not affected
0 - not available due to postulated CMF
1 to 11 - actual initiating parameter

Incident 15.2.7 / CMF Groups / Reactor Parameter	351A-D Narrow level	353A-D Wide level	353E-H Wide level	CRD Accum. Pressure	Drywell Pressure	RPV Pressure	PRNM (MSL rad.)	APRM (run rad.)	SRNM (start rad.)	MPx	DTM	TLU	Accelerometers	MSIV Position	Turbine Stop Valve Switch	Turbine Fast Solenoid Valve	Turbine Oil Pressure Sw.				Remarks
1 Low Water Level	0	O	O							O	O	O									Primary scram and ECCS initiator
2 Hi Water Level	0																				Injection and turbine permissive
3 RPV High Pressure																					
4 High Drywell Pressure																					
5 High Reactivity																					
6 High MSL Radiation																					
7 MSLIV											O	O									Secondary scram initiator
8 Earthquake																					
9 Turbine Valves Closing																					
10 CRD Pressure Low																					
Mitigation	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	
Scram	7	1	1							7	O	O									
ARI	1										1	1									DID Scram
HPCF	0	1	O							O	O	O									Secondary core cooling
RCIC	0	O	1							O	O	O									Primary core cooling
LPFL	O									O	O	O									unavailable because no ADS
SLCS																					
MSLIV																					
ADS	O									O	O	O									ADS requires high drywell pressure
SRV																					
info										O	O	O									

A14.2 Conclusions

Common-mode failure of the primary scram initiator channel (column 1, low water level 3) as stuck-at level 8 will result in a backup scram due to MSLIV 85% switches or by alternate rod insertion (ARI) caused by diverse water level sensing. Reactor core cooling is necessary and is provided by RCIC except as noted below. (feedwater pumps are unusable because feedwater pumps are tripped and turbine steam supply is interrupted by MSLIV closure). Multiplexer failure (column 10) results in scram but complete failure of ECCS. DTM and TLU failures disable RPS scram, but this is backed up by ARI (columns 11 and 12). However, ECCS fails to operate.

Columns 1 through 3 demonstrate water level channel failures. For failure 2, diverse initiation of HPCF backs up RCIC. For failure 1 there are two possible modes of failure. If the transmitter sticks indicating permanent high water level the injection valve for HPCF will never open and RCIC turbines will not start. If the transmitter sticks indicating permanent intermediate or low water level then the injection valve, once open, will never close and the reactor may overflow. (If the transmitter sticks at a permanent low level, there is a permanent scram initiated.) LPFL will start but will be ineffective without blowdown by the ADS. ADS blowdown will not occur until both low water level and high drywell pressure have existed for a timeout period, and high drywell pressure will not occur in this accident.

Summarizing, reactor scram is initiated by diverse signals (failures 10 and 1) or by DID backup by ARI (failures 11 and 12). In failures 1, 10, 11, and 12, the control system is unable to provide DID core cooling and there is no diverse method for automatic operation of any of the ECCS features. Manual blowdown of ADS is possible in failure 1, allowing LPFL to substitute for ineffective HPCF and RCIC. Manual operation of RCIC or HPCF from the control room may be possible for failure 11, but is precluded in failures 10 and 12.

A15. Trip of All RIPs

This event, number 15.3.1.1.2.2, is the trip of all of the RIPs - Table 15.3-2. This is a limiting fault event.

A15.1 Special Assumptions

1) Failure of the turbine stop valve switch channel ultimately leads to a high pressure scram. The high pressure scram occurs at about 2 seconds after the start of the incident. This is approximately the same time as the scram would have occurred had the stop valve switches operated correctly. See Figure 15.3-2.

2) The high water level (L8) which initiates the turbine and feedwater pump trips is sensed by a transmitter which is part of the control system; this sensor is presumed to operate correctly.

3) Stop valve switch status enters the RPS at the DTM. See RAI response dated 10/4/91, number 9a, page 15.

4) An APRM trip (STPT) does not occur.

A15.2 Conclusions

Failure 1 is actually two failures in one. If the transmitter sticks indicating permanent high water level the injection valve for HPCF will never open. If the transmitter sticks indicating permanent intermediate water level then the injection valve, once open, will never close and the reactor may overflow. (If the transmitter sticks at a permanent low level, there is a permanent scram initiated.)

The behavior of RCIC for failure 1 is straight forward. If the channel sticks below the high water level setpoint (L8) then the reactor may overflow. If the channel sticks at or above the high water level setpoint RCIC will not initiate.

For failures 3 and 6 the system operates normally. For failure 15, an alternate scram initiator is used but otherwise the system behaves normally.

For failure 2, the RCIC fails to start but is backed up by the HPCF.

DBE 15.3.1
Trip of all RIPs.
Table 15.3-2

Legend:
blank - not involved or not affected
0 - not available due to postulated CMF
1 to 11 - actual initiating parameter

Event 15.3.1 / Plant Parameter	351A-D Narrow level	353A-D Wide level	353E-H Wide level	CRD Accum. Pressure	Drywell Pressure	RPV Pressure	PRNM (MSL rad.)	APRM (run rad.)	SRNM (start rad.)	MPX	DTM	TLU	Accelerometers	MSIV Position	Turbine Stop Valve Switch	Turbine Control Valve Switch	Turbine Oil Pressure Sw.				
1 Low Water Level	0	O	O							O	O	O									ECCS initiator
2 Hi Water Level	0																				
3 RPV High Pressure						O				O	O	O									Secondary scram initiator
4 High Drywell Pressure																					
5 High Reactivity																					
6 High MSL Radiation																					
7 MSLIV																					
8 Earthquake																					
9 Turbine Valves Closing											O	O			O						Primary scram initiator
10 CRD Pressure Low																					
Mitigation	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17				
Scram	9	9	9			9				9	O	O			3						
ARI											3	3									
HPCF	0	1								O	O	O									Secondary core cooler
RCIC	0/1	O	1			1				O	O	O			1						Primary core cooler
LPFL	O									O	O	O									Unavailable because ADS will not initiate
SLCS																					
MSLIV																					
ADS	O									O	O	O									ADS requires high drywell pressure
SRV																					
Information										O	O	O									

For failure 10 the scram is normal but there is no system for cooling of the core and the core may become exposed. For failures 11 and 12 ARI is invoked to scram the reactor and again there is no core cooling if needed. In failures 10 and 12 there is no manual initiation of the core cooling machinery from the control room because these controls require the correct functioning of both the MPX and the TLU. See GE drawings 103E1805 sheets 1 - 5.

Reactor scram initiation is provided by the turbine valves with RPV pressure providing a diverse trip. Power scram will probably not provide other diversity because the trip of the RIPs reduces core reactivity. This diversity vanishes with CMFs of the digital system (MPX, DTM, TLU).

Manual scram initiation and ARI from the control system provide defense-in-depth for scram.

RCIC and HPCF provide diverse methods for cooling the core. However, all of that diversity vanishes and nothing is left with any failures in the digital systems. It should be noted that although LPFL may initiate on low water level, it is never available because ADS will never initiate. ADS initiation requires high drywell pressure. See figure 7.3-2h.

Manual control provides defense-in-depth for the ECCS providing there is time for the operators to act and there are no failures in the TLU or MPX. With a failure in either one of those digital systems manual initiation of any part of ECCS from the control room is lost. See GE drawing 103E1805 sheets 1 - 5.

If the high water level sensor in the control system fails to trip the turbine, there may be undesirable consequences since there are no reactor trips available: first, there may be water droplets sent to the turbine if the feedwater control system does not or can not keep the water level properly controlled and second, there may be boiling at the fuel rods with consequent fuel rod damage.

A16. Inadvertent Control Rod Removal During Startup

This event, 15.4.1.2, is an inadvertent control rod removal during start-up. Refer to Table 15.4-2 and Figure 15.4-1. It is categorized as an infrequent incident.

A.16.1 Special Assumptions

1) Per GE ABWR SAR, the reactor is assumed to be in the critical condition before the incident, 0.001% rate power and 286°C.

2) The neutron monitor scram initiation preferences are:

Short Period Trip (SRNM)
15% power (APRM).

No other automatic scram initiators are available. For power percentages below 15% the fuel is not damaged

3) It is unclear whether or not fuel damage will occur above 15%. In addition no process evaluations were done on rod withdrawal error past 15% power. Thus, it is unclear if any process variable other than SRNM or APRM will initiate a scram.

4) The feedwater pumps maintain reactor water level above level 3. Thus, ARI and ECCS will not be challenged.

5) The SRNM signal does not go through the MPX or DTM and is directly transmitted to the TLU.

A16.2 Conclusions

Mitigations 8 and 9 involve normal operation of the protection systems. A short period reactivity increase detected by the SRNM is the primary scram initiator. If the SRNM is not available the setdown mode of the APRM detects a high average neutron flux (15% rated power). Mitigation 8 relies on the primary scram initiator, thus loss of the APRM has no affect in this incident. Mitigation 9 scrams on the secondary initiator otherwise operation is normal.

In mitigation 12, the loss of the TLU will inhibit a scram. There are no other automatic initiating signals. ARI and RPS cannot initiate. The ECCS is not challenged.

Accident 15.4.1.2

DBE 15.4.1.2 Rod withdrawal error - low power (start-up). Table 15.4-2 and Figure 15.4-1

Legend:
blank - not involved or not affected
0 - not available due to postulated CMF
1 to 11 - actual initiating parameter

Reactor Parameter \ CMF Groups	351A-D Narrow level	353A-D Wide level	353E-H Wide level	CRD Accum. Pressure	Drywell Pressure	RPV Pressure	PRRM (MSL rad.)	APRM (run rad.)	SRNM (start rad.)	MPX	DTM	TLU	Accelerometers	MSIV Position	Turbine Stop Valve Switch	Turbine Control Valve Switch	Turbine Oil Pressure Sw.				
1 Low Water Level																					
2 Hi Water Level																					
3 RPV High Pressure																					
4 High Drywell Pressure																					
5 High Reactivity								O				O									Secondary scram initiator
6 High MSL Radiation																					
7 MSLIV																					
8 Earthquake																					
9 Turbine Valves Closing																					
10 CRD Pressure Low																					
11 Short Period Reactivity									O			O									Primary scram initiator
Mitigation	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17				
Scram								11	5			O									
ARI																					
HPCF																					
RCIC																					
LPFL																					
SLCS																					
MSLIV																					
ADS																					
SRV																					
info												O									

The time the operators may have to respond to this event before fuel rod damage can not be determined from the current information in the GE ABWR SAR (Chapter 15.4, Table 15.4-2 and Figure 15.4-1). At start-up the operators should have a heightened awareness. They should be monitoring the process variables very carefully and paying particular attention to any deviations from normal start-up. If a deviation from normal start-up is observed the operators should immediately scram the reactor. It is unclear whether or not this is an unsafe common-mode failure scenario.

The SRNM and APRM provide diversity for mitigations 8 and 9, while mitigation 12 has no diversity. Diversity does not exist for all possible CMFs for this incident.

Defense-in-depth is provided through the control room manual scram system.

A17. Fast Runout of All RIPs

This event, number 15.4.5.1.2.2, is a fast runout of all RIPs. Refer to Table 15.4-5 and Figure 15.4-3. This event is categorized as a limiting fault.

A17.1 Special Assumptions

1) By interpretation of the first eight seconds of Figure 15.4-3 and Figure 4.4-1 the reactor variables will settle into a new steady-state without a scram. Although the new steady-state may be above 100% of rated power. In this case no other scram initiators other than APRM will be sensed.

2) The turbine may be operating at a low enough power such that the runout of the RIPs increases the reactor steam flow beyond the capability of the SB&PCS. The turbine control valve throttles to maintain constant pressure/flow and the SB&PCS diverts steam flow at full capacity. In this case, the turbine control valve would not allow an increase in steam flow and the SB & PCS could not handle any additional steam flow, therefore the reactor pressure will build and finally initiate a scram.

2) The feedwater pumps maintain reactor water level above level 3. Thus, ECCS will not be challenged.

3) The APRM signal does not go through the MPX or DTM and is directly transmitted to the TLU.

Accident 15.4.5

DBE 15.4.5

Fast runout of all RIPs - Table 15.4-5 and Figure 15.4-3

Legend:

blank - not involved or not affected
0 - not available due to postulated CMF
1 to 11 - actual initiating parameter

Reactor Parameter \ CMF Groups	351A-D Narrow level	353A-D Wide level	353E-H Wide level	CRD Accum. Pressure	Drywell Pressure	RPV Pressure	PRRM (MSL rad.)	APRM (run rad.)	SRNM (start rad.)	MPX	CTM	TLU	Accelerometers	MSIV Position	Turbine Stop Valve Switch	Turbine Control Valve Switch	Turbine Oil Pressure Sw.				
1 Low Water Level																					
2 Hi Water Level																					
3 RPV High Pressure						O															Possible secondary scram initiator
4 High Drywell Pressure																					
5 High Reactivity								O				O									Primary scram initiator
6 High MSL Radiation																					
7 MSLIV																					
8 Earthquake																					
9 Turbine Valves Closing																					
10 CRD Pressure Low																					

Mitigation	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17				
Scram						5		3/0				O									
ARI												3									
HPCF																					
RCIC																					
LPFL																					
SLCS																					
MSLIV																					
ADS																					
SRV																					
info												O									

A17.2 Conclusions

Mitigation 6 involves normal operation of the protection systems. The APRM initiates a scram.

Mitigation 8 considers two possible initial states, one leads to a scram while the other will not. The first initial state (8-3) is where the turbine and the reactor are operating at low power. Thus when the RIPs runout, a large amount of steam must be diverted by the SB&PCS. Since the SB&PCS can only divert a limited amount of steam the reactor vessel pressure will build, eventually initiating a scram. The second initial state (8-0) is where the turbine and the reactor are operating at high power (near 100%) and the SB&PCS system is diverting very little steam. In this case the SB&PCS can handle the increased steam flow due to RIP runout and the reactor system will simple go into another steady-state. With a CMF in the APRMs a scram is inhibited. This higher steady-state will be detectable by the operators at which time the operators may decide upon and implement a course of action.

Mitigation 12 considers the same two initial states as mitigation 8. The first initial state (12-3) leads to an ARI scram. The second initial state (12-0) leads to a new process steady-state in which mitigation depends on the operators.

The ECCS is not challenged.

Diversity exist for three of the five mitigations (6, 8-3, 12-3). The other two mitigations (8-0, 12-0) have no diversity. Diversity does not exist for all postulated CMFs.

Defense-in-depth is provided through the control room manual scram system.

A18. Steam Piping Break Outside Containment

This event, number 15.6.4, is a steam system piping break outside of containment - Table 15.6-4. This is a limiting fault.

A18.1 Special Assumptions

1) The closure of the MSLIVs is initiated from the ESFAS. The documentation for how the MSLIVs are controlled is reasonably clear [illegible] exactly where control is [illegible]ercised is confused. On GE drawing 103E1805 sheets 1 [illegible] MSLIVs are shown as connected directly to the TL[illegible]PS. But those same drawings show the LDS as par[illegible]s. On the IBDs for the LD&IS (LDS) are shown all of [illegible] actuation of the MSLIVs. Further, in Ref. 2, pa[illegible] of Equipment Interface with the Essential Mux [illegible] shown the MSIVs from which it could be inter[illegible] MSIVs are actuated through the multiplexer. It has been assumed for this analysis that the control of the MSLIVs rests in the ESFAS but that the software which evaluates the various functions for operating the MSLIVs runs on the DTM and TLU which also evaluate RPS functions. Further, it is assumed that the actuation signals for the valves is hardwired from the RPS/MSIV TLUs to the valve load drivers. These assumptions blurs the separation between RPS and ESFAS but do not effect the analysis.

2) All 16 flow sensor channels fail together.

3) Since the feedwater pump loses its steam supply with the closing of the MSLIVs (see paragraph 15.2.4.3.1), both RCIC and HPCF are needed to maintain the water level in the RPV. This may not be a necessity, but the scenario shows it.

4) The SB&PCS is oblivious to the break in the line (a really worst-case assumption) although it will not be able to do more than idle the turbine on the line. Thus no scram initiating signals will come from the turbine.

5) The low-turbine-inlet-pressure sensor channel is through the MPX. These sensors are different from the first-stage-turbine-pressure sensors which connect directly to the DTM. See the material faxed to Stewart and Poslusny (NRC) on 10/4/91 from an unknown party in GE responding to NRC concerns, item number 9.

Low pressure may not initiate the closing of the MSLIVs if the break is not too complete or is located far from the turbine inlet.

A18.2 Conclusions

Failure 1 is actually two failures in one. If the transmitter sticks indicating permanent high water level the injection valve for HPCF will never open. If the transmitter sticks indicating permanent intermediate water level then the injection valve, once open, will never close and the reactor may overflow. (If the transmitter sticks at a permanent low level, there is a permanent scram initiated.)

The behavior of RCIC for failure 1 is straight forward. If the channel sticks below the high water level setpoint (L8) then the reactor may overflow. If the channel sticks at or above the high water level setpoint RCIC will not initiate.

For failure 8, scram is most likely to occur because of high pressure because the MSLIVs have closed successfully. However, a power scram may occur because the high pressure will increase the reactivity of the core. ECCS operates normally.

For failures 2 and 3, the failure of the low water level transmitters causes either HPCF or RCIC to fail. It is not clear that both RCIC and HPCF are needed to keep the water level up in the RPV, but if both are needed and one fails LPFL cannot provide a backup since ADS is required and cannot initiate because the drywell pressure is normal. See figure 7.3-2h.

For failure 11 everything operates normally.

For CMFs 12, 13 and 14 nothing works. All of the sensor channels which could close the MSLIVs come through the MPX, DTM and TLU. As long as the MSLIVs stay open, neither high reactor pressure nor high reactivity can cause a reactor scram. Water level will probably be maintained in the reactor by the feedwater system since there is probably enough steam pressure to run the feedwater pumps. Even if

DBE 15.6.4
Steam System Piping Break
Outside Containment - table 15.6-4

Event 15.6.4

Plant Parameter	CMF Groups	351A-D Narrow level	353A-D Wide level	353E-H Wide level	Drywell Pressure	RPV Pressure	PRRM (MSL rad.)	APRM (run rad.)	MSIV Position	Steam Tunnel Temperature	Turbine Room Temperature	Steam Line Flow	MPX	DTM	TLU	Turbine Stop Valve Switch	Turbine Control Valve Switch	Turbine Oil Pressure Sw.			
1 Low Water Level		0	O	O									O	O	O						ECCS initiator
2 RPV High Pressure						O							O	O	O						Secondary scram initiator
3 High Water Level		0																			
4 High Reactivity								O							O						Secondary scram initiator
5 High MSL Radiation																					
6 MSLIV									O					O	O						Primary scram initiator
7 Steam Tunnel Temperature										O			O	O	O						Secondary MSIV initiator
8 Turbine Room Temperature											O		O	O	O						Secondary MSIV initiator
9 Steam Line Flow												O	O	O	O						Primary MSIV initiator
10 Turbine Valves Closing																					
11 Low Turbine Inlet Pressure													O	O	O						Tertiary MSIV initiator
Mitigation		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17			
Scram		6	6	6		6		6	2/4	6	6	6	O	O	O						
ARI													O	O	O						
HPCF		0/1	O	1		1		1	1	1	1	1	O	O	O						Secondary core cooler
RCIC		0/1	1	O		1		1	1	1	1	1	O	O	O						Primary core cooler
LPFL		O	O	O									O	O	O						Unavailable because ADS will not initiate
SLCS																					
MSLIV		9	9	9		9		9	9	9	9	7/8	O	O	O						
ADS		O	O	O									O	O	O						ADS is required for LPFL
SRV																					
Information													O	O	O						

Legend:
blank - not involved or not affected
0 - not available due to postulated CMF
1 to 11 - actual initiating parameter

the water level falls to a low level ARI will not be invoked. ARI is initiated by low water level signals from the SSLC [Ref. 5].

Closing of the MSLIVs limit switches is the primary reactor scram initiator with high RPV pressure and high neutron flux scrams providing diversity. However, all three are linked in that the two diverse backup scrams depend on the MSLIVs closing. Therefore failures in the digital systems prevent scram from occurring.

High steam line flow is the primary initiator for MSLIV closure with tunnel temperature and turbine room temperature providing diversity. Low turbine inlet pressure is a third diverse initiator but it may not always function. Since all of these signals are processed through the digital system, the MSLIVs will not close for a CMF there.

Manual controls provide defense-in-depth for both scram and closure of the MSLIVs. ARI also provides DID for scram but for this event ARI fails when the digital systems fail because the MSLIVs do not close. If they are manually closed then ARI may get invoked but if the operators are alert enough to close the MSLIVs manually, they will probably manually scram the reactor also.

RCIC and HPCF provide diverse means for cooling the core should that be required. The GE scenario indicates that both RCIC and HPCF are required to keep the core covered, which reduces the diversity somewhat but this does not seem to be a critical issue. As above, failure of any of the digital systems eliminates all ECCS. LPFL is not available although it will initiate. LPFL requires the operation of the ADS and ADS will not initiate because the drywell pressure remains normal. See figure 7.3-2h.

DID for initiation of the ECCS is provided by manual initiation from the control room, assuming there is time for operator action. However, with the CMF of either the MPX or the TLU this manual initiation capability is cut off.

A19. LOCA Inside Containment

This event, number 15.6.5, is a loss of coolant accident (LOCA) inside containment - Table 6.3-2. This is a limiting fault.

A19.1 Special Assumptions

1) Any break in the piping which causes this event will increase the drywell pressure sufficiently to trigger mitigating action. This is justified if the break is a main steam line or a feedwater line. (Feedwater temperature is 422F and the flow is over 4000 lb/sec. (Table 15.0-1). Therefore it should flash as it enters the drywell and the volume should be adequate to increase drywell pressure to the trip point (1.7 psig, figure 7.3-4c). For other (unidentified) breaks this assumption is not so clear.

2) A number of signals may initiate the closing of the MSLIVs - excessive steam flow , low turbine inlet pressure, or low reactor water level (figure 7.3-5, sheets 4 - 7). The first two are problematical since if a steam line breaks the position and extent of the break may prevent them from initiating the valve closing and a feedwater line break clearly will not increase the flow in the steam lines or reduce the turbine inlet pressure. Low water level appears to be the only MSLIV trip that can be counted on. However, after the reactor scrams on low water level, if the MSLIVs have not closed, for whatever reason, ultimately the MSLIVs will close on low turbine inlet pressure.

3) All signals that initiate MSLIV trips come through the EMS. There is some confusion on this because turbine first stage pressure which trips the reactor enters the system at the RPS DTM. But this signal is a bypass signal for start-up rather than a trip. These items are covered in more detail in assumption 1 for event 15.6.4.

DBE 15.6.5
Loss of Coolant Accident
Table 6.3-2

Legend:
blank - not involved or not affected
0 - not available due to postulated CMF
1 to 11 - actual initiating parameter

Event 15.6.5 / CMF Groups / Plant Parameter	351A-D Narrow level	353A-D Wide level	353E-H Wide level	CRD Accum. Pressure	Drywell Pressure - PT306	RPV Pressure	PRRM (MSL rad.)	APRM (run rad.)	SRNM (start rad.)	MPX	DTM	TLU	MSIV Position	Turbine Stop Valve Switch	Turbine Control Valve Switch	Turbine Oil Pressure Sw.	ADS Water Level Switch	ADS Drywell Press. Switch	MSIV Low Water Level Switch	Low Turbine Inlet Pressure	
1 Low Water Level	9	O	O							O	O	O					O		O		Primary scram and ECCS initiator
2 Hi Water Level	0																				
3 RPV High Pressure																					
4 High Drywell Pressure					O					O	O	O						O			Secondary scram initiator
5 High Reactivity																					
6 High MSL Radiation																					
7 MSLIV													O								Tertiary scram initiator
8 Turbine Valves Closing																					
9 CRD Pressure Low																					
10 Low Turbine Inlet Pressure										O	O	O								O	Tertiary scram initiator
Mitigation	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	
Scram	4/7	1	1		1					O	O	O	1				1	1	1	1	
ARI										O	1	1									
HPCF	9/1	4	1		1					O	O	O	1				1	1	1	1	All three of the ECCS systems, RCIC, HPCF, and LPFL must be available to mitigate the effects of this accident.
RCIC	9/1	1	4		1					O	O	O	1				1	1	1	1	
LPFL	1	1	1		1					O	O	O	1				O	O	1	1	
SLCS																					
MSLIV	1	1	1		1					O	O	O	1				1	1	10	1	
ADS	1	1	1		1					O	O	O	1				O	O	1	1	Required for LPFL
SRV																					
Information										O	O	O									

A19.2 Conclusions

For failure 1 scram will initiate on either of the two backup signals, high drywell pressure or MSLIV closure.

Failure 1 is actually two failures in one. If the transmitter sticks indicating permanent high water level the injection valve for HPCF will never open. If the transmitter sticks indicating permanent intermediate water level then the injection valve, once open, will never close and the reactor may overflow. (If the transmitter sticks at a permanent low level, there is a permanent scram initiated.)

The behavior of RCIC for failure 1 is straight forward. If the channel sticks below the high water level setpoint (L8) then the reactor may overflow. If the channel sticks at or above the high water level setpoint RCIC will not initiate.

For failures 2, 3, 5, 19 and 20 the system reacts in a reasonably normal fashion with scram occurring on time and all elements of the ECCS initiating as they should. It should be noted that the LPFL initiates on either the wide level A - D transmitters or the E - H transmitters. Drywell pressure is needed to initiate scram, HPCF and RCIC as the various low water level transmitters fail. The MSLIV's will close on low water level in the normal way except in 19 where low turbine inlet pressure is needed.

For failures 17 and 18 scram and initiation of the high pressure parts of ECCS occur normally (low water level) but although LPFL will initiate, it is unavailable because ADS requires both the low water level switch and the high drywell pressure to initiate. This jeopardizes the core integrity. The MSLIVs close normally on low water level.

For failure 10 none of the protection systems will initiate since all of the necessary signals are transmitted through the MPX. Manual initiation of the ECCS from the control room is prevented because these manual controls operate through the MPX. See GE drawings 103E1805 sheets 1 - 5. Manual scram of the reactor from the control room is available since these pushbuttons are hard wired to the scram solenoids. Again see GE drawings 103E1805 sheets 1 - 5. Core exposure and significant fuel damage probable.

For failure 11 and 12 ARI will scram the reactor but as in 10, above, none of the ECCS will initiate automatically. In failure 11 manual initiation of the ECCS can be accomplished from the control room but a failure of the TLU (failure 12) disconnects these controls as in 10. Core exposure and fuel damage is very likely.

For all failures except 10 through 12 the MSLIVs will close as required when the water level gets low enough or the turbine pressure gets low enough.

Low water level is the primary scram initiator with high drywell pressure and closure of the MSLIVs providing diversity.

ARI provides defense-in-depth for scram but for failures in the digital systems most of this depth vanishes. Manual scram is available at all times but there may not be encugh time for the operators act so this may not provide more depth to the defense.

RCIC, HPCF and LPFL provide diverse means for cooling the core. Failures in the digital systems, however, prevent any of these systems from initiating.

Manual initiation of the ECCS from the control room provides defense-in-depth but this is not operational for a CMF of the MPX or TLU.

A20. Feedwater Line Break Outside Containment

This event, number 15.6.6, is a break in a feedwater line outside containment - Table 15.6-15. This is a limiting fault.

A20.1 Special Assumptions

1) Both RCIC and HPCF will normally be available to mitigate this event and are adequate for the task. Table 15.6-15 states that RCIC is not available because the feedwater line is broken. This is not backed up by any other documentation and examination of other pertinent documentation leads to the impression that the statement is in error. If one or the other of these systems fail, it is assumed that LPFL will turn on as required.

2) Low water level will normally trip the MSLIVs (figure 7.3-5, sheets 4 - 7). However, after the reactor scrams on low water level, if the MSLIVs have not closed, for whatever reason, ultimately the MSLIVs will close on low turbine inlet pressure.

3) All signals that initiate MSLIV trips come through the EMS. There is some confusion on this because turbine first stage pressure which trips the reactor enters the system at the RPS DTM. But this signal is a bypass signal for start-up rather than a trip. Also, the MSL radiation trip enters the RPS at the DTM and is then passed to the ESFAS to initiate MSLIV trip. These items are covered in more detail in assumption 1 for event 15.6.4.

DBE 15.6.6

Feedwater line break outside containment - Table 15.6-15

Event 15.6.6 / Plant Parameter	CMF Groups	351A-D Narrow level	353A-D Wide level	353E-H Wide level	CRD accum. Pressure	Drywell Pressure	RPV Pressure	PRRM (MSL rad.)	APRM (run rad.)	SRNM (start rad.)	MPX	DTM	TLU	MSIV Position	Turbine Stop Valve Switch	Turbine Control Valve Switch	Turbine Oil Pressure Sw.	MSIV Low Water Level Switch	Low Turbine Inlet Pressure			
1 Low Water Level		0	O	O							O	O	O					O				Primary scram and ECCS initiator
2 Hi Water Level		0																				
3 RPV High Pressure																						
4 High Drywell Pressure																						
5 High Reactivity																						
6 High MSL Radiation																						
7 MSLIV														O								Secondary scram initiator
8 Turbine Valves Closing																						
9 CRD Pressure Low																						
10 Low Turbine Inlet Pressure											O	O	O						O			Tertiary scram initiator
Mitigation		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18			
Scram		7	1	1							O	O	O	1				1	1			
ARI											O	1	1									
HPCF		0/1	O	1							O	O	O	1				1	1			Both RCIC and HPCF may be required to maintain water level in the reactor
RCIC		0/1	1	O							O	O	O	1				1	1			
LPFL		O	O	O							O	O	O									ADS required for LPFL
SLCS																						
MSLIV		1	1	1							O	O	O	1				10	1			
ADS		O	O	O							O	O	O									ADS requires high drywell pressure
SRV																						
Information											O	O	O									

Legend:

blank - not involved or not affected
0 - not available due to postulated CMF
1 to 11 - actual initiating parameter

A20.2 Conclusions

For failure 1 scram is initiated by the MSLIVs closing.

Failure 1 is actually two failures in one. If the transmitter sticks indicating permanent high water level the injection valve for HPCF will never open. If the transmitter sticks indicating permanent intermediate water level then the injection valve, once open, will never close and the reactor may overflow. (If the transmitter sticks at a permanent low level, there is a permanent scram initiated.)

The behavior of RCIC for failure 1 is straight forward. If the channel sticks below the high water level setpoint (L8) then the reactor may overflow. If the channel sticks at or above the high water level setpoint RCIC will not initiate.

For failures 2 and 3, the reactor scrams normally but only one of the two ECCS systems is available. If this is inadequate to maintain the water level in the reactor during cooldown, the core may become exposed because LPFL is unavailable since ADS will not initiate because the drywell pressure is not elevated.

For failure 10 none of the protection systems will initiate since all of the necessary signals are transmitted through the MPX. Manual initiation of the ECCS from the control room is prevented because these manual controls operate through the MPX. See GE drawings 103E1805 sheets 1 - 5. Manual scram of the reactor from the control room is available since these pushbuttons are hard wired to the scram solenoids. Again see GE drawings 103E1805 sheets 1 - 5. Core exposure and significant fuel damage is guaranteed.

For failure 11 and 12 ARI will scram the reactor but as in 10, above, none of the ECCS will initiate automatically. In failure 11 manual initiation of the ECCS can be accomplished from the control room but a failure of the TLU (failure 12) disconnects these controls as in 10. Core exposure and fuel damage is very likely.

Failures 17 and 18 are not particularly significant since the only unusual occurrence is the belated trip of the MSLIVs from low pressure as a result of the reactor running out of steam.

Low water level is the primary scram initiator with closure of the MSLIVs providing diversity. Not all initiators are functional for all CMFs and with any failure in the digital systems both initiators fail.

Defense-in-depth is provided by ARI and, if there is enough time for the operators to act, manual scram. Failures in the digital systems impair this depth with a failure in the MPX eliminating ARI, leaving manual initiation as the only means of scramming the reactor.

RCIC and HPCF provide diverse means for cooling the reactor core but this diversity vanishes with any failure in the digital system. LPFL is never available for this event. LPFL requires the operation of the ADS and ADS will not initiate because the drywell pressure remains normal. See figure 7.3-2h.

Manual initiation of the ECCS from the control room provides defense-in-depth if there is enough time for the operators to act. These manual controls are cut off when either the MPX or the TLU fails.

Appendix B

B1. Various Support Systems

There are several systems contained within the protection system for which a detailed CMF analysis is impractical because of a lack of design information or unnecessary because their failure to activate automatically poses no serious risk to the reactor system. For those systems for which we have inadequate information, the number of assumptions required would be so great that the analysis would be essentially meaningless. Further, these systems are not typically required to meet the challenges of Chapter 15. These systems are:

1) RHR/Wetwell and Drywell Spray Cooling Modes

2) RHR/Suppression Pool Cooling Mode

3) Standby Gas Treatment System

4) Emergency Generator Support Systems

5) Reactor Building Cooling Water System

6) Essential HVAC System

7) HVAC Emergency Cooling Water System

8) High Pressure Nitrogen Gas Suppiy System

What can be said about these systems is that they all may suffer from the same problems that the ECCS suffers from if they are controlled through the MPX, DTM, TLU systems. That is, failures in these digital systems may well prevent any or all of these systems from starting when required. Further, manual control from the control room may be prevented if the MPX or TLU fails in a common-mode. See GE drawing 103E1805 sheet 1.

B2. CRD Header Pressure Scram and High Pressure Nitrogen Supply

The high pressure nitrogen supply system is required for scram but depends on the operators to make sure that the supply is adequate for the action required. We presume that low pressure is

annunciated to the operators but a large leak might get ahead of them. Further, the CRD pressure scram scrams only if there is a leak in the purge water flow system. There maybe a link between these systems (high pressure nitrogen and CRD pressure scram) but it is obscure and that makes the analysis weak.

It is questionable whether scramming with a detected leak in the CRD header is a good idea. If the header system is leaking at 1000 psi and it is suddenly pressurized to 2000 psi there might be a disaster.

B3. Seismic System

The accelerometers are shown entering the SSLC in Ref. 2. The signals are shown on Figure 19N.1-1. However, in Ref. 3, concern number 9, no mention is made of the place that seismic signals enter the system.

If the signals enter the SSLC at the DTM, a CMF of the DTM or the TLU will prevent scram for a seismic event. If they enter a little farther along at the TLU, then only a CMF of the TLU would prevent scram. Corruption of the channels is probably not an issue with these signals since there are three sets of accelerometers and a trip will occur if any one set functions correctly.

B4. Manual Bypass System

The manual bypass system allows the bypassing of sensors and divisions of the protection system. The purpose is to allow maintenance of the various parts of the system while still maintaining the protective function. The logic of section 7.2 shows that if one division is bypassed, the other divisions cannot be bypassed. However, since all of the logic is implemented by software, a potential common-mode failure is for the bypass of one division to cause the bypass of all divisions thus eliminating any protective actions if protection is required.

Appendix C

This appendix contains the Trip Tables which were used in this analysis. What the tables show are the inputs for the various functions of the protection system together with actions which are triggered by the functions.

Reactor Protection System
Trip Table

Input Sensors	Output Logic Trips: Coinc. NMS	Non-Coinc. NMS	CRD Pres. Low	RPV Pres. Hi	MSL Isolated	RPV Water Low	MSL Rad. Hi	Seismic Act.	Drywell Pres. Hi	Turb. Valves Clsd
APRM/ UP (1-4)	X	X	X							
Non-Coinc. Dis. Sw.		X								
Reactor Mode Sw.	X	X	X							
SRNM/ UP(1-4)	X	X	X							
CRD Press. Low										
CRD Press. Bypass Sw.										
RPV/ PT-301(A-D)				X						
In. MSIV 85%/ POT-012 (A-D)					X					
Out. MSIV [illegible]%/ POT-013 (A-D)					X					
MSIV Bypass A					X					
MSIV Bypass B					X					
MSIV Bypass C					X					
MSIV Bypass D					X					
Div. I Sensor Bypass			X	X		X	X	X	X	X
Div. II Sensor Bypass			X	X		X	X	X	X	X
Div. III Sensor Bypass			X	X		X	X	X	X	X
Div. IV Sensor Bypass			X	X		X	X	X	X	X
RPV NR Water/ LT-351 (A-D)						X				
MSL Radiation Hi/ RT [illegible]ni)							X			
Bottom Horiz. Accel./ ACS(bh)								X		
Bottom Vert. Accel./ ACS(bv)								X		
Top Horiz. Accel./ ACS(th)								X		
Drywell/ PT-306 (A-D)										
TSV/ POS-001 (A-D)									X	
TCV/ POS-004 (A-D)										X
HTS Low Oil/ PS-00[illegible] (A-D)										X
Turb 1st Stg/ PT-00[illegible] (A-D)										X
Reactor Action										
Scram	X	X	X	X	X	X	X	X	X	X
MSIV closure							X			

ECCS - HPCF

Trip Table

input sensors	Start pump	Stop pump	Injector valve mov-F004	Close mov-F004	Suppression Pool mov-F001	Condensate Pool mov-F009
Water level 1.5 LT-353 (E-H)	X		X			
Drywell high pressure PT-306 (A-D)	X		X			
Water level 8 LT-351 (A-D)		X		X		
Suppression pool suction valve fulll open switch	X	X				
Condensate pool suction valve full open switch	X	X				
Suppression pool level					X	X
Condensate pool level					X	X
Manual control	X	X	X	X	X	X
PB Reset		X				
Pump suction pressure switch	X	X				
Containment flood level bypass					X	X
Reactor action						
HPCF pumps tripped on - require reset to stop	X					
HPCF flow to rpv disabled		X		X		
Water intake from suppression pool					X	
Water intake from condensate pool						X

ECCS - RCIC

Trip Table

input sensors	Output Logic Trips	Pump discharge valve mov-F013	Condensate pool water mov-F010	Suppression pool water mov-F031	Steam supply mov-F045	Cooling water supply mov-F046	Sup. pool bypass close mov-F022	Sup. pool bypass close mov-F059	RCIC Turbine trip	Steam bypass mov-F092		
Drywell high pressure PT-306 (A-D)		X	X		X	X	X	X		X		
Reactor water level 2 LT-353(A-D)		X	X		X	X	X	X		X		
Reactor water level 8 LT-351(A-D)					X	X				X		
Suppression pool water level high LT-005(D,H)				X								
Low pump suction pressure PT-303									X			
Leak detect									X			
Condensate pool water level low LT-001(D,H)				X								
mov F031 position			X									
Reactor action												
RCIC trip		X	X		X	X						
RCIC cooling water flowing into reactor		X	X		X	X			X	X		
Bypass for testing							X	X				
Suction valve lineup			X	X								

ECCS - ADS/SRV

Trip Table

input sensors	Output Logic Trips: SRV F031A	SRV F031B	SRV F031C	SRV F031(D-F)	SRV F031(G-K)	SRV F031(L-P)	SRV F031(R-U)				
RPV pressure high PS-MT010(A-D) 71.4/76.6	X										
RPV pressure high PS-MT011(A-D) 72.1/77.3		X									
RPV pressure high PS-MT012(A-D) 72.8/78.0			X	X							
RPV pressure high PS-MT013(A-D) 73.5/78.7					X						
RPV pressure high PS-MT014(A-D) 74.2/79.4						X					
RPV pressure high PS-MT015(A-D) 74.9/780.1							X				
Manual key operated switch H11 SRV control	X	X	X	X	X	X	X				
Manual PBS H11 ADS oper.						X	X				
Manual PBS H11 ADS reset						X	X				
Reactor water level LS-MT004(A-D)						X	X				
Reactor water level LS-MT004(E-H)						X	X				
Drywell pressure PS MT019(A-D)						X	X				
RHR pump discharge pressure E11-PIS302(A-C)						X	X				
RHR pump discharge pressure E11-PIS303(A-C)						X	X				
HPCS pump discharge pressure E22-PIS306(B,C)						X	X				
HPCS pump discharge pressure E22-PIS307(B,C)						X	X				
Reactor action											
Blowdown						X	X				
Pressure relief	X	X	X	X	X	X	X				

ECCS - RHR/LPFL

Trip Table

Input sensors	Output Logic Trips: LOCA initiated	RHR pump started	Injection valve mov-F047(A-C)	MG set start
Drywell pressure PT-306(A-D)	X			
Reactor water level LT-353(A-D)	X			
Reactor water level LT-353(E-H)	X			
Reactor vessel pressure PT-301(A-D)			X	
RHR manual initiate PBS	X			
RHR PBS reset	X			
Diesel generator running, switch ?		X		
AC power available, switch ?		X		
RHR pump suction valve mov-F001(A-C) open, switch ?		X		
Shutdown suction iso valve mov-F002(A-C), switch ?		X		
LOCA Trip		X	X	X
Reactor action				
RHR LPFL tripped	X			
LPFL pumping water into core		X	X	

LD & IS

MSLIV Trip Table

input sensors \ Output Logic Trips	Close MSL Isolation Valves									
MSL tunnel area ambient temp TS-Z620(A-D)	X									
MSL turbine area ambient temp TS-Z621(A-D)	X									
Reactor water level B21-LS Z603(E-H)	X									
MSL turbine inlet pressure B21-PIS Z628(A-D)	X									
Main condenser vacuum B21-PS Z901(A-D)	X									
MSL (A) steam flow DPIS-Z616(A-D)	X									
MSL (B) steam flow DPIS-Z616(E-H)	X									
MSL (C) steam flow DPIS-Z616(J-M)	X									
MSL (D) steam flow DPIS-Z616(N-S)	X									
Channel A sensor bypass switch	X									
Channel B sensor bypass switch	X									
Channel C sensor bypass switch	X									
Channel D sensor bypass switch	X									
Division (1-4) TLU auto trip test switch	X									
Reactor mode switch	X									
Division (1-4) main condensor vacuum bypass switch	X									
RPS IBD Ref Doc 5 MSL Radiation high	X									
MSL (A-D) MSIV (IB/OB) Auto/Close switch	X									
MSL (A-D) MSIV (IB/OB) Test Close switch	X									
Reactor action										

LD & IS

RHR, RCIC, CUW, & Miscellaneous Isolation Trip Table

input sensors	Output Logic Trips	RHR Loop A Isolated	RHR Loop B Isolated	RHR Loop C Isolated	RCIC isolate, turbine trip	CUW Isolated	Dry well Fission Products Isolated	SPCU Isolated	DCW & HCW Drains Isolated	RCW,HNCW,PCV Valves isolated	SGTS Initiate & R/B HVAC isolate	FCS Isolation
MSL Tunnel Ambient Temp TS-Z620(A-D)						X						
Reactor water level LS-Z603-3(A-D)										X		
Reactor water level LS-Z603(A-D)							X					
Reactor water level LS-Z601(A-D)	X	X	X			X		X	X		X	X
Reactor pressure PIS-Z607(A-D)	X	X	X									
Drywell pressure PS-625(A-D)							X	X	X	X	X	X
R/A, HVAC,or F/H area radiation high (Ref Doc 6, D11)									X		X	
RHR area (A-C) temp high TS-Z608(A-D,E-H,J-M)	X	X	X									
PCV Div (1-3) isolation PB switch	X	X	X			X	X	X	X	X	X	X
PCV Div (1-3) reset PB switch	X	X	X			X	X	X	X	X	X	X
RCIC area temp high TS-Z605(A-D)					X							
RCIC steam line pressure low PS-Z607(A-D)					X							
Div (1-4) sensor bypass switch	X	X	X		X						X	
RCIC steam line flow high DPS Z606(A-D)					X							
RCIC PB isolation switch Div (1,2)					X							
RCIC PB isolation reset switch					X							
RCIC turbine exhaust pressure high (Ref. Doc 10 E51)					X							
CUW mass diff flow high DMFS-Z613(A-D)						X						
CUW Hx Reg ambient temp high TS-Z609(A-D)						X						
CUW Hx non-Reg ambient temp high TS-Z609(E-H)						X						
CUW valve room ambient temp high TS-Z609(J-M)						X						
Reactor action												

Appendix D

D1. Shared signal analyses

In addition to the analyses performed under section 3.3 and results presented in section 5 of this report, eleven signals which are shared between two or more echelons (see Figure 3 or Figure 5) are singled out for special attention in this section. The question asked is "can a sensor failure cause one echelon to challenge another and also inhibit the second echelon from mitigating the effects of the failure". For each shared signal this question is examined.

D1.1 Turbine valve 85% switches

These switches cause reactor scram upon load rejection or turbine trip. An optically isolated version of switch condition is passed to the control system where it is used to trip five reactor internal pumps, thereby reducing reactivity. The turbine valve switches do not serve as an input variable for a control process in the control system, so that there is no credible scenario in which failure of the turbine valve 85% switches will cause the control system to challenge either RPS or ESFAS Two types of failure are considered possible: failure to indicate turbine valve closure and false indication of turbine valve closure.

D1.1.1 Failure to indicate closure

Scenarios with turbine valve closure have been considered in the review of Chapter 15 events 15.2.2 (generator load rejection) and 15.2.3 (turbine trip). Failure of the turbine valve switches results in scram due to neutron flux or high reactor vessel pressure. Insertion of all control rods will stop the reaction (assumption 3.6.6.1) and there is diverse signal (reactor dome pressure) in the control system to cause internal pump trip.

D1.1.2 False indication of turbine valve closure

RPS will scram the reactor and five internal pumps will trip. Steam pressure will decrease and eventually, if no operator action occurs, low turbine inlet pressure or low condenser vacuum will cause the MSLIVs to close. RCIC will start on low water level to continue reactor cooldown. The net result is an unplanned shutdown.

D1.2 Nuclear monitor system

The nuclear monitor system (NMS) provides trip inputs to the RPS and other NMS outputs are used in the control system for rod block and reactivity control. Operators may use flux level as a power indication. The nuclear monitor system clearly has the potential to induce a reactivity transient caused by the control system which the RPS does not see. Two types of failure are considered: the neutron monitor system indicates significantly less flux than actually exists in the reactor and the monitor system indicates more neutron flux than actually exists in the reactor. Oscillatory failures are not considered, and failures during startup are not considered.

D1.2.1 NMS indicates low

If the reactor is running under automatic load following control or the operator adjusts reactivity to match an intended value, the reactor will operate at some percentage overpower. Making the worst possible assumption, the reactor will exceed the 127% NBR trip point without scramming. There is insufficient information available to analyze the expected consequences because no General Electric simulation encompasses this event. Some possible scenarios are:

1) The reactor may be inadvertently driven prompt critical.
2) High vessel pressure may initiate a scram.
3) Generator protective relays may cause a load rejection.
4) Turbine protective relays may cause a turbine trip.

D1.2.2 NMS indicates high

If the reactor is running under automatic load following control or the operator adjusts reactivity to match an intended value, the reactor will operate at some percentage underpower. Underpower operation will not challenge the safety of the reactor but there is a danger that operators will compensate by running at higher values of indicated neutron flux.

D1.3 Scram

The scram signal is generated by the RPS and is used by the control system to run the fine motion control rod drive all the way in during a scram. The scram signal is not an input variable to a control

process in the control system and there is no credible scenario by which a failure can cause the control system to initiate a challenging transient which the RPS has not already seen.

D1.4 EOC RPT

The End-Of-Cycle Recirculating Pump Trip signal is generated by the RPS and is used by the control system to trip four reactor recirculating pumps immediately. The EOC RPT signal is not an input variable to a control process in the control system and there is no credible scenario by which a failure can cause the control system to initiate a challenging transient which the RPS has not already seen.

D1.5 Drywell pressure

Drywell pressure transducer signal PT-306 (A-D) is shared between the RPS and the HPCF, RCIC, and LPFL of the ESFAS. In all cases it is used as a diverse trip or initiator signal, so that the only unsafe failure is failure to indicate high drywell pressure when it exists. False indication of high drywell pressure causes spurious trip, an annoying but safe failure. Failure of PT-306 was analyzed under Chapter 15 event 15.6.5, LOCA in containment. In this analysis, diverse signals (low water level, low turbine inlet pressure) lead to reactor scram and emergency cooling actuation if high drywell pressure fails to do so.

D1.6 Reactor water level

Narrow-range reactor water level transducer signal LT-351 (A-D) is shared between the RPS and the HPCF and RCIC of the ESFAS. The signal from this transducer is used to initiate scram (water level < L3), as a permissive for the HPCF injector valve (water level < L8), and as a permissive for RCIC steam turbines (water level < L8). A failure that reports water level > L8 will disable all three mitigation actions. Backup scram is available from ATWS (Alternate Rod Insertion), but LPFL will be ineffective as a backup for RCIC and HPCF (ADS does not operate) unless there is also high drywell pressure. Since this can occur with containment isolated, the reactor control system (feedwater control) is ineffective as a second echelon of defense. There is therefore insufficient diversity and defense-in-depth to initiate effective emergency core cooling in the face of common-mode failure of the LT-351 (A-D) water level transducer channels.

D1.7 Reactor vessel pressure

Reactor vessel pressure transducer signal PT-301 (A-D) is shared between the RPS and LPFL of the ESFAS. The signal from this transducer is used to initiate reactor scram (reactor pressure > 1104 psig) and as a permissive for the LPFL injector valve (reactor pressure < 457 psig). Failure of this signal channel indicating mid-range affects both RPS and LPFL. Diverse methods of initiating scram are available, depending upon the situation. ATWS provides direct high pressure scram backup since it depends upon pressure switches which are diverse to PT-301. Most instances which result in high reactor vessel pressure also result in high neutron flux, causing scram by an alternate route. Common-mode failure of PT-301 (A-D) does not, however, challenge ESFAS, since RCIC and HPCF are preferentially initiated on reactor water level, and HPCF provides diverse mitigation if LPFL is ineffective. There is therefore sufficient diversity and defense-in-depth to compensate for common-mode failure of the PT-301 (A-D) pressure transducer channels.

D1.8 Reactor water level

Wide-range reactor water level transducer signal LT-353 (?-?)[4] is shared between the HPCF or the RCIC of the ESFAS, and ATWS in the control system. This signal is used to initiate Alternate Rod Insertion (ARI) in ATWS and one of RCIC or HPCF. The only unsafe failure of this signal channel is failure to indicate low water level when it exists. In this case, reactor scram will have already been initiated by diverse water level sensors in the RPS, and one of either RCIC or HPCF will successfully initiate. There is therefore sufficient diversity and defense-in-depth to compensate for common-mode failure of the LT-353 (?-?) water level transducer channels.

D1.9 FWC NR water level

The Feed Water Control (FWC) system narrow-range water level transducer (unknown designation) is shared between ATWS and the FWC. This signal is used in ATWS for recirculating pump trip and is

---

[4]Which four of the eight LT-353 (A-H) transducers are shared is unclear from the General Electric SAR.

assumed to be used in FWC for water level maintenance. A failure of this channel in the FWC can result in a challenge to the reactor protection system either directly (causing low water level) or indirectly (by high water level). If the challenge is low water level (see the analysis of Chapter 15 event 15.2.7, loss of feed water flow), diverse water level sensors initiate scram and ESF operation. If the challenge is high water level, RPS and ESFAS do not react until subsequent control system actions initiate turbine trip and low water level is sensed through diverse sensors. See the analysis of Chapter 15 event 15.1.2, runout of two feedwater pumps.

D1.10 SB & PC dome pressure

The Steam Bypass and Pressure Control (SB & PC) dome pressure transducer (unknown designation) is shared between ATWS and the SB & PC. This signal is used to initiate Alternate Rod Insertion (ARI) in ATWS and is assumed to be used by SB & PC for steam pressure maintenance. A failure of this channel in the SB & PC can result in a challenge to the reactor protection system either directly (by causing high reactor vessel pressure) or indirectly (by causing loss of reactor vessel pressure). Both of these challenges have been dealt with in analyses of Chapter 15 events (event 15.2.1, pressure regulation failure high, and event 15.1.3, failure of all pressure regulation valves in the open state). In both cases, diverse signals initiate reactor scram and emergency core cooling. However, ATWS ARI is unavailable if needed unless reactor water level drops below L2.

the water level falls to a low level ARI will not be invoked. ARI is initiated by low water level signals from the SSLC [Ref. 5].

Closing of the MSLIVs limit switches is the primary reactor scram initiator with high RPV pressure and high neutron flux scrams providing diversity. However, all three are linked in that the two diverse backup scrams depend on the MSLIVs closing. Therefore failures in the digital systems prevent scram from occurring.

High steam line flow is the primary initiator for MSLIV closure with tunnel temperature and turbine room temperature providing diversity. Low turbine inlet pressure is a third diverse initiator but it may not always function. Since all of these signals are processed through the digital system, the MSLIVs will not close for a CMF there.

Manual controls provide defense-in-depth for both scram and closure of the MSLIVs. ARI also provides DID for scram but for this event ARI fails when the digital systems fail because the MSLIVs do not close. If they are manually closed then ARI may get invoked but if the operators are alert enough to close the MSLIVs manually, they will probably manually scram the reactor also.

RCIC and HPCF provide diverse means for cooling the core should that be required. The GE scenario indicates that both RCIC and HPCF are required to keep the core covered, which reduces the diversity somewhat but this does not seem to be a critical issue. As above, failure of any of the digital systems eliminates all ECCS. LPFL is not available although it will initiate. LPFL requires the operation of the ADS and ADS will not initiate because the drywell pressure remains normal. See figure 7.3-2h.

DID for initiation of the ECCS is provided by manual initiation from the control room, assuming there is time for operator action. However, with the CMF of either the MPX or the TLU this manual initiation capability is cut off.

A19. LOCA Inside Containment

This event, number 15.6.5, is a loss of coolant accident (LOCA) inside containment - Table 6.3-2. This is a limiting fault.

A19.1 Special Assumptions

1) Any break in the piping which causes this event will increase the drywell pressure sufficiently to trigger mitigating action. This is justified if the break is a main steam line or a feedwater line. (Feedwater temperature is 422F and the flow is over 4000 lb/sec. (Table 15.0-1). Therefore it should flash as it enters the drywell and the volume should be adequate to increase drywell pressure to the trip point (1.7 psig, figure 7.3-4c). For other (unidentified) breaks this assumption is not so clear.

2) A number of signals may initiate the closing of the MSLIVs - excessive steam flow , low turbine inlet pressure, or low reactor water level (figure 7.3-5, sheets 4 - 7). The first two are problematical since if a steam line breaks the position and extent of the break may prevent them from initiating the valve closing and a feedwater line break clearly will not increase the flow in the steam lines or reduce the turbine inlet pressure. Low water level appears to be the only MSLIV trip that can be counted on. However, after the reactor scrams on low water level, if the MSLIVs have not closed, for whatever reason, ultimately the MSLIVs will close on low turbine inlet pressure.

3) All signals that initiate MSLIV trips come through the EMS. There is some confusion on this because turbine first stage pressure which trips the reactor enters the system at the RPS DTM. But this signal is a bypass signal for start-up rather than a trip. These items are covered in more detail in assumption 1 for event 15.6.4.

DBE 15.6.5
Loss of Coolant Accident
Table 6.3-2

Legend:
blank - not involved or not affected
0 - not available due to postulated CMF
1 to 11 - actual initiating parameter

Event 15.6.5 / CMF Groups / Plant Parameter	351A-D Narrow level	353A-D Wide level	353E-H Wide level	CRD Accum. Pressure	Drywell Pressure - PT306	RPV Pressure	PRNM (MSL rad.)	APRM (run rad.)	SRNM (start rad.)	MPX	DTM	TLU	MSIV Position	Turbine Stop Valve Switch	Turbine Control Valve Switch	Turbine Oil Pressure Sw.	ADS Water Level Switch	ADS Drywell Press. Switch	MSIV Low Water Level Switch	Low Turbine Inlet Pressure	
1 Low Water Level	0	O	O							O	O	O					O		O		Primary scram and ECCS initiator
2 Hi Water Level	0																				
3 RPV High Pressure																					
4 High Drywell Pressure					O					O	O	O						O			Secondary scram initiator
5 High Reactivity																					
6 High MSL Radiation																					
7 MSLIV													O								Tertiary scram initiator
8 Turbine Valves Closing																					
9 CRD Pressure Low																					
10 Low Turbine Inlet Pressure										O	O	O								O	Tertiary scram initiator
Mitigation	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	
Scram	4/7	1	1		1					O	O	O	1					1	1	1	
ARI										O	1	1									
HPCF	0/1	4	1		1					O	O	O	1				1	1	1	1	All three of the ECCS systems, RCIC, HPCF, and LPFL must be available to mitigate the effects of this accident.
RCIC	0/1	1	4		1					O	O	O	1				1	1	1	1	
LPFL	1	1	1		1					O	O	O	1				O	O	1	1	
SLCS																					
MSLIV	1	1	1		1					O	O	O	1				1	1	10	1	
ADS	1	1	1		1					O	O	O	1				O	O	1	1	Required for LPFL
SRV																					
Information										O	O	O									