



---

---

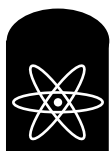
# **Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems**

---

---

**Prepared by  
G. G. Preckshot**

**Prepared for  
U.S. Nuclear Regulatory Commission**



**FESSP**

**Fission Energy and Systems Safety Program**

**Lawrence Livermore National Laboratory**

### **Disclaimer**

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

This work was supported by the United States Nuclear Regulatory commission under a Memorandum of Understanding with the United States Department of Energy, and performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract W-7405-Eng-48.

---

---

# **Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems**

---

---

**Manuscript date: December, 1994**

**Prepared by  
G. G. Preckshot  
Lawrence Livermore National Laboratory  
7000 East Avenue  
Livermore, CA 94550**

**Prepared for  
U.S. Nuclear Regulatory Commission**



## **ABSTRACT**

The purpose of this NUREG is to describe a method for analyzing computer-based nuclear reactor protection systems that discovers design vulnerabilities to common-mode failure. The potential for common-mode failure has become an important issue as the software content of protection systems has increased. This potential was not present in earlier analog protection systems because it could usually be assumed that common-mode failure, if it did occur, was due to slow processes such as corrosion or premature wear-out. This assumption is no longer true for systems containing software. It is the purpose of the analysis method described here to determine points of a design for which credible common-mode failures are uncompensated either by diversity or defense-in-depth.



# CONTENTS

1. Introduction .....	1
1.1. Purpose of this NUREG .....	1
1.2. When to Perform This Analysis .....	1
1.3. History .....	1
1.4. Goals, January 1994 .....	1
1.5. Philosophy Behind the Analysis .....	2
1.6. Overview of Contents .....	2
2. Definitions .....	2
2.1. Defense-in-Depth .....	2
2.2. Echelons of Defense .....	2
2.2.1. Control System .....	2
2.2.2. Reactor Trip or Scram System .....	2
2.2.3. ESF Actuation System .....	2
2.2.4. Monitoring and Indicator System .....	3
2.3. Channel .....	3
2.4. Instrumentation System .....	3
2.5. Block .....	3
2.6. Diversity .....	3
2.6.1. Human Diversity .....	3
2.6.2. Design Diversity .....	3
2.6.3. Software Diversity .....	4
2.6.4. Functional Diversity .....	4
2.6.5. Signal Diversity .....	4
2.6.6. Equipment Diversity .....	4
2.7. Common-Mode (or -Cause) Failure .....	4
2.8. Anticipated Operational Occurrences .....	4
2.9. Accidents .....	5
3. Analysis GUIDELINES .....	5
3.1. Guideline 1—Choosing Blocks .....	5
3.2. Guideline 2—Determining Diversity .....	6
3.2.1. Design Diversity .....	7
3.2.2. Equipment Diversity .....	7
3.2.3. Functional Diversity .....	7
3.2.4. Human Diversity .....	7
3.2.5. Signal Diversity .....	7
3.2.6. Software Diversity .....	8
3.2.7. Combining Diversity Attributes .....	8
3.3. Guideline 3—System Failure Types .....	8
3.3.1. Type 1 Failures .....	8
3.3.2. Type 2 Failures .....	8
3.3.3. Type 3 Failures .....	9
3.4. Guideline 4—Echelon Requirement .....	9
3.5. Guideline 5—Method of Evaluation .....	9
3.6. Guideline 6—Postulated Common-Mode Failure of Blocks .....	9
3.7. Guideline 7—Use of Identical Hardware and Software Modules .....	10
3.8. Guideline 8—Effect of Other Blocks .....	10
3.9. Guideline 9—Output Signals .....	10
3.10. Guideline 10—Diversity for Anticipated Operational Occurrences .....	10
3.11. Guideline 11—Diversity for Accidents .....	10

3.12. Guideline 12—Diversity Among Echelons of Defense .....	10
3.13. Guideline 13—Plant Monitoring .....	11
3.14. Guideline 14—Manual Operator Action .....	11
4. Data Required to Do the Analysis .....	12
4.1. System Diagram and Logic Diagrams .....	12
4.2. Chapter 15 Events .....	12
4.3. Alternate Trips .....	12
4.4. Required Mitigation .....	12
5. What Should be in an Analysis? .....	12
6. Assumptions to be Stated .....	14
6.1. Worst-Case Assumptions .....	14
6.2. Assumptions Based on System Structure .....	14
6.2.1. Diversity of Blocks .....	15
6.3. Assumptions for Echelon .....	15
6.4. Evaluation Criteria .....	16
7. Description of the Design .....	16
7.1. Design Basis .....	16
7.1.1. General or Regulatory Bases .....	16
7.1.2. Additional Agreed Bases .....	17
7.1.3. Applicant's Statements .....	17
7.2. Design Architecture .....	17
7.3. Intentional Design Diversity .....	17
8. Findings .....	18
8.1. General Vulnerabilities .....	18
8.2. Specific Vulnerabilities .....	18
8.3. Evaluation of Diversity .....	18
8.4. Shared Signals .....	18
8.5. Special Findings .....	18
9. Aids to Presentation or Analysis .....	18
9.1. Analysis Charts .....	18
9.2. System Block Diagram .....	18
9.3. Vulnerability Summary Charts .....	19
References .....	27
Appendix—Block Examples .....	29

## FIGURES

Figure 1. Pressurized Water Reactor Analysis Chart .....	20
Figure 2. Boiling Water Reactor Analysis Chart .....	21
Figure 3. Use of Analysis Charts .....	22
Figure 4. Sample Pressurized Water Reactor Vulnerability Summary Chart .....	23
Figure 5. Sample Boiling Water Reactor Vulnerability Summary Chart .....	24
Figure 6. Summary Chart for Analysis of Type 3 Failures .....	25
Figure A-1. Sample BWR System Block Diagram .....	30
Figure A-2. Sample PWR System Block Diagram .....	34



## **ACKNOWLEDGMENTS**

Some work from NUREG-0493, dated March 1979, has been included verbatim or slightly modified without specific acknowledgment. Some work from references (Palomar et al. 1993a, Palomar et al. 1993b, Preckshot 1993a) has been included without specific acknowledgment. The author thanks and acknowledges previous workers in this area. One person in particular, Joseph P. Joyce of the Nuclear Regulatory Commission Staff, was both involved in the original NUREG-0493 work, and has been directly involved and has guided the work described herein. Mr. Joyce provided continuity and foresight that might otherwise be lacking. The author also thanks and acknowledges the efforts of other Nuclear Regulatory Commission staff members who reviewed this work and provided their insights and comments. These gentlemen are Mr. John Gallagher and Mr. Matthew Chiramal. The presentation of this document is due in considerable part to the efforts of Ms. Karen McWilliams.



# METHOD FOR PERFORMING DIVERSITY AND DEFENSE-IN-DEPTH ANALYSES OF REACTOR PROTECTION SYSTEMS

## 1. INTRODUCTION

### 1.1. Purpose of this NUREG

The purpose of this NUREG is to describe a method for analyzing computer-based nuclear reactor protection systems that discovers and identifies design vulnerabilities to common-mode failure. The potential for common-mode failure has become an important issue as the software content of protection systems has increased. This potential was not present in earlier analog protection systems because it could usually be assumed that common-mode failure, if it did occur, was due to slow processes such as corrosion or premature wear-out. This assumption is no longer true for systems containing software. It is the purpose of the analysis method described here to postulate common-mode failures and to determine what portions of a design are uncompensated either by diversity or defense-in-depth.

In a series of documents, staff concerns regarding digital computers in advanced reactor systems were set forth in SECY 91-292, and an initial statement of a four-point diversity and defense-in-depth requirement was made in SECY 93-087. In a staff requirements memorandum (SRM) dated July 21, 1993, the full Commission approved the modified four-point requirement stated below.

1. The applicant shall assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common-mode failures have been adequately addressed.
2. In performing the assessment, the vendor or applicant shall analyze each postulated common-mode failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using best-estimate (using realistic assumptions) methods. The vendor or applicant shall demonstrate adequate diversity within the design for each of these events.
3. If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common mode failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.

4. A set of displays and controls located in the main control room shall be provided for manual system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system identified in items 1 and 3 above.

With regard to the first three points, NRC staff considers that software design errors are a credible source of common-mode failures. Diverse digital or non-digital systems are acceptable means of compensating for such failures, as is manual action if sufficient time and information are available to operators.

### 1.2. When to Perform This Analysis

Diversity and defense-in-depth analyses should be performed when a credible potential exists for common-mode failure. This is presently the case for computer-based safety systems and would be the case for new-technology safety systems whose reliability properties are imperfectly known. The analysis technique can be used to demonstrate adequate diversity and defense-in-depth, or used as a constructive design technique to add diverse protection schemes or equipment to counteract common-mode failure vulnerabilities.

### 1.3. History

NUREG-0493, "A Defense-in-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System," published March 1979, was an assessment of a single reactor protection system that addressed common-mode failure concerns and introduced a method of analysis. Although the application was specific, the 1979 work established sufficiently general principles that it was adapted to analyze the GE ABWR in 1991, the Westinghouse AP-600 in 1993, and the GE SBWR in 1993 by an independent NRC contractor. ABB Combustion Engineering used the principles themselves in 1992 to analyze their System 80+ protection system.

### 1.4. Goals, January 1994

Experience applying NUREG-0493 to four other vendor's protection systems has led to a clearer picture of how to do the analysis. In parallel, NRC staff has clarified its technical position and obtained Commission approval of the four-point diversity and defense-in-depth requirement.

## Section 2. Definitions

NUREG-0493 is rewritten here to capture that experience, to explain the techniques for performing the analysis, to remove those details specific to the RESAR-414, and to reflect the technical position of the staff and the Commission.

### 1.5. Philosophy Behind the Analysis

Analyses performed using the methods of this NUREG are not intended to require the inclusion or exclusion of specific failures in a reactor protection system design basis, but are intended to determine points of vulnerability in a design to common-mode failures, should they occur. For this reason, the choice of credible failures should err on the liberal side of interpretation, and the decision of whether or not to compensate for discovered vulnerabilities should be made after this analysis is complete. Accordingly, many of the examples presented herein show apparent vulnerabilities, which were either later determined to be due to insufficient or inaccurate design information, or were compensated by design modifications.

Modern computer-based systems have become sufficiently complex that details can soon overwhelm the analyst. Dividing the system into blocks is intended to reduce design detail to the abstraction level consistent with the goals of the analysis. Consequently, the failures postulated herein subsume many kinds of similar, individual failures and must be considered group failures whose inner workings need not be defined precisely. This is typical of the effects of software failures in which many individual failures are capable of producing the same or similar outputs. Attempting to postulate all possible individual software errors is impossible on any relevant human time scale and is unnecessary.

### 1.6. Overview of Contents

The balance of this document includes definitions, analysis guidelines, six sections on applying the guidelines and generating a documented analysis, and an appendix demonstrating two different reactor protection systems redrawn as connected blocks. The application sections deal with data required, suggested report contents, statement of analysis assumptions, design descriptions at appropriate levels of detail, analysis findings, and graphical aids. Three published analyses in the style recommended by this document are noted in the references for those wishing to see complete examples.

## 2. DEFINITIONS

### 2.1. Defense-in-Depth

Defense-in-depth is a principle of long standing for the design, construction and operation of nuclear reactors, and may be thought of as requiring a concentric arrangement of protective barriers or means, all of which must be breached before a hazardous material or dangerous energy can adversely affect human beings or the environment. The

classic three physical barriers to radiation release in a reactor—cladding, reactor pressure vessel, and containment—are an example of defense-in-depth.

### 2.2. Echelons of Defense

“Echelons of defense” are specific applications of the principle of defense-in-depth to the arrangement of instrumentation and control systems attached to a nuclear reactor for the purpose of operating the reactor or shutting it down and cooling it. Specifically, the echelons are the *control system*, the *reactor trip or scram system*, the *Engineered Safety Features actuation system* (ESFAS), and the *monitoring and indicator system*. The echelons may be considered to be concentrically arranged in that when the control system fails, the reactor trip system shuts down reactivity; when both the control system and the reactor trip system fail, the ESFAS continues to support the physical barriers to radiological release by cooling the fuel, thus allowing time for other measures to be taken by reactor operators to reduce reactivity. All four echelons depend upon sensors to determine when to perform their functions, and a serious safety concern is to ensure that no more than one echelon is disabled by a common sensor failure or its direct consequences.

#### 2.2.1. Control System

The *control echelon* is that non-Class 1E manual or automatic equipment which routinely prevents reactor excursions toward unsafe regimes of operation and is generally used to operate the reactor in the safe power production operating region. Indicators, annunciators, and alarms may be included in the *control echelon*. Reactor control systems typically contain some equipment to satisfy the ATWS rule (10 CFR 50.62) or the requirement for a remote shutdown panel. Examples of such equipment include high-quality non-Class 1E equipment for which credit may be taken solely for compensating rare common-mode failures of Class 1E reactor protection equipment (see point 3 of the diversity and defense-in-depth requirement, presented above).

#### 2.2.2. Reactor Trip or Scram System

The *reactor trip echelon* is that safety equipment designed to reduce reactivity rapidly in response to an uncontrolled excursion. It consists of instrumentation for detecting potential or actual excursions, means for rapidly and completely inserting the reactor control rods, and may also include certain chemical neutron moderation systems (e.g., boron injection).

#### 2.2.3. ESF Actuation System

The *ESFAS echelon* is that safety equipment which removes heat or otherwise assists in maintaining the integrity of the three physical barriers to radioactive release (cladding, vessel, and containment). This echelon detects the need for and performs such functions as emergency cooling, pressure relief or depressurization, isolation, and

control of various support systems (e.g., emergency generators) or devices (valves, motors, pumps) required for ESF equipment to operate.

### 2.2.4. Monitoring and Indicator System

The *monitoring and indication echelon* is the slowest and also the most flexible echelon of defense. Like the other three echelons, operators are dependent upon accurate sensor information to perform their tasks, but, given information, time, and means, can perform previously unspecified logical computations to react to unexpected events. The *monitoring and indication echelon* includes both Class 1E and non-Class 1E manual controls, monitors, and indicators required to operate equipment nominally assigned to the other three echelons.

## 2.3. Channel

A channel is defined as a set of interconnected hardware and software components that processes an identifiable sensor signal to produce a single protective action signal in a single division when required by a generating station condition. A channel includes the sensor, data acquisition, signal conditioning, data transmission, bypasses, and logic up to voters or actuating device inputs. The objective of the channel definition is to define subsets of a reactor protection system that can be unambiguously tested or analyzed from input to output.

## 2.4. Instrumentation System

A plant instrumentation system is that equipment which senses various plant parameters and transmits appropriate signals to control systems, to the reactor trip system, to the engineered safety features actuation system, and to the monitoring and indicator system for use in determining the actions these systems or reactor operators will take. Independence is required between control systems, safety-related monitoring and display systems, the safety systems, and between redundant divisions of the safety systems.

## 2.5. Block

Generally, a system is described as an arrangement of components or black boxes interconnected by communication, electrical connections, pipes, or physical effects. This kind of description, often called a “system architecture,” may be too complex or may not be partitioned conveniently for diversity and defense-in-depth analysis. A more convenient description may be obtained by restricting the portion of the system under consideration to instrumentation and control equipment and partitioning the restricted portion into “blocks.” A “block” is the smallest portion of the system under analysis for which it can be credibly assumed that internal failures, including the effects of software errors, will not propagate to other equipment. The objective of choosing blocks is to reduce the need for detailed examination of internal failure

mechanisms while examining system behavior under reasonable assumptions of failure containment.

Examples of typical software-containing blocks are computers, local area networks or multiplexers, or programmable logic controllers (PLCs). A block can be solely hardware, but there are no solely software blocks; software-containing blocks suffer the distinction that both hardware or software faults (and sometimes both acting together) can cause block failure. Consequently, it is difficult to separate the effects of software from the machine that executes that software. For example, a software defect in one small routine can cause an entire computer to fail by corruption of other data or software. Guideline 1 and Guidelines 6 through 9 (Section 3) provide additional direction on block choice and failure propagation limits.

## 2.6. Diversity

Diversity is a principle in instrumentation systems of sensing different parameters, using different technologies, using different logic or algorithms, or using different actuation means to provide several ways of detecting and responding to a significant event. Diversity is complementary to the principle of defense-in-depth and increases the chances that defenses at a particular level or depth will be actuated when needed. Defenses at different levels of depth may also be diverse from each other. There are six important types of diversity to consider: human diversity, design diversity, software diversity, functional diversity, signal diversity, and equipment diversity. An extended discussion of diversity is given in Guideline 2 (Section 3.2).

### 2.6.1. Human Diversity

The effect of human beings on the design, development, installation, operation, and maintenance of safety systems is known to be extremely variable, and has been a factor in several serious accidents. Used in a positive way, human diversity can be a plus for system safety. For instance, using different maintenance personnel to calibrate separate, redundant divisions of safety instrumentation may provide some assurance that the same, systematic error is not made in all divisions. Using separate designers to design functionally diverse safety systems may reduce the possibility of similar design errors.

### 2.6.2. Design Diversity

Design diversity is the use of different approaches, including both software and hardware, to solve the same or similar problem. Software diversity is a special case of design diversity and is mentioned separately because of its potential importance and its potential defects. The rationale for design diversity is that different designs will have different failure modes and will not be susceptible to the same common influences. A factor that weakens this argument is that different designs may nonetheless use similar elements or approaches.

## Section 2. Definitions

### 2.6.3. Software Diversity

Software diversity is the use of different programs designed and implemented by different development groups with different key personnel to accomplish the same safety goals—for example, using two separately designed programs to compute when a reactor should be tripped. It has been suggested that sufficient diversity can be obtained by implementing the same specification through intentionally diverse designs (possibly by the same programming team); however, the bulk of significant reported experience concerns independent software teams (Kelly et al. 1991). The great hope of software diversity is that different programmers will make different mistakes. Unfortunately, some (very sparse) data suggest that different programmers designing to the same requirements too often make similar mistakes (Knight and Leveson 1986).

### 2.6.4. Functional Diversity

Two systems are functionally diverse if they perform different physical functions though they may have overlapping safety effects. For example, cooling systems normally intended to function when containment is isolated are functionally different from other liquid control systems intended to inject coolant or borated water for other reasons. However, the other liquid control systems may have a useful cooling effect, while the isolation cooling systems may have useful coolant makeup side effects. Functional diversity is often useful when determining if sufficient mitigation means have been employed in a postulated accident; a combination of alternative systems in the face of primary system failure may be enough to mitigate the effects of an accident.

A type of functional diversity, called “aspect” diversity, was applied to systems using relays, specifically to distinguish “de-energize to trip” arrangements from “energize to trip” arrangements. Subsequent experience (Hanauer 1990) has shown that this is less effective—even in relay systems—than originally supposed. In digital systems, aspect diversity can be implemented by a trivial interposition of one logical negation instruction, which renders claims of aspect diversity even more suspect. Some advantage may be claimed by the use of “watchdog” timers or watchdog processors, but experience has shown that

these, too, are difficult to implement reliably (Mahmood and McCluskey 1988).

### 2.6.5. Signal Diversity

Signal diversity is the use of different sensed parameters to initiate protective action, in which any of the parameters may independently indicate an abnormal condition, even if the other parameters fail to be sensed correctly. For example, in a BWR, neutron flux increase due to void reduction is a diverse parameter to reactor pressure excursion for events that cause a reactor pressure pulse.

### 2.6.6. Equipment Diversity

Equipment diversity is the use of different equipment to perform similar safety functions, in which “different” means sufficiently unlike as to significantly decrease vulnerability to common failure. The fact that equipment is made by different manufacturers does not guarantee diversity; many computer designs use the same semiconductor chips, and in the most extreme cases, two suppliers may acquire, re-label, and sell the same printed circuit boards from a single manufacturer. The use of diverse computer equipment may have an effect on software diversity; using a different computer architecture forces the use of diverse compilers, linkers, and other support software.

## 2.7. Common-Mode (or -Cause) Failure

Common-mode failures (CMFs) are causally related failures of redundant or separate equipment. For example, (1) A CMF of identical subsystems across redundant divisions defeats the purpose of redundancy, or (2) A CMF of different subsystems or echelons of defense defeats the use of defense-in-depth. CMF embraces all causal relations, including severe environments, design errors, calibration and maintenance errors, and consequential failures. Common-mode failure is further elaborated in Guideline 3, and discussed in detail with respect to rules for postulating it in Guideline 6.

## 2.8. Anticipated Operational Occurrences

For the purposes of the analysis described in this document, a basis set of anticipated operational occurrences should be identified by the following criteria.

“‘Anticipated operational occurrences’ mean those conditions of normal operation which are expected to occur one or more times during the life of the nuclear power unit and include but are not limited to loss of the turbine generator set, isolation of the main condenser and loss of offsite power” (10 CFR 50, Appendix A, Definitions and Explanations). Such occurrences are further categorized as to frequency:<sup>1</sup>

- Incidents of moderate frequency—these are incidents, any one of which may occur during a calendar year for a particular plant.
- Infrequent incidents—these are incidents, any one of which may occur during the lifetime of a particular plant.

## 2.9. Accidents

Accidents are defined as those conditions of abnormal operation that result in limiting faults:<sup>2</sup>

These are occurrences that are not expected to occur but are postulated because their consequences would include the potential for the release of significant amounts of radioactive material.

Limiting faults are further defined as those accidents whose effects circumscribe or bound the effects of similar faults of lesser magnitude. For the purposes of the analysis described in this document, a basis set of limiting faults, identical to those considered in the Standard Safety Analysis Report, Chapter 15, should be identified.

## 3. ANALYSIS GUIDELINES

Specific guidelines are presented in the sequel for performing diversity and defense-in-depth analyses. This introductory section describes a road map of how to put these guidelines together to make a complete analysis.

A block diagram of the system to be analyzed should first be constructed using the Block Guideline (1). Candidate blocks should then be examined under the Diversity Guideline (2) to decide which blocks are identical for analysis purposes, and which will be considered diverse, as required by Guideline 7.

With the system block diagram and other information as suggested in Section 4, the analysis should be conducted as required by the general analysis guidelines (4–14), keeping in mind that the ultimate goal of the analysis is to detect

vulnerabilities to the three system failure types described in the System Failure Guideline (3).

For anticipated operational occurrences as described in Guideline 10 (in combination with primary protection system failure), the goal of defense-in-depth analysis using best-estimate (realistic assumptions) methodology is to show that no more than a small fraction (10%) of the 10 CFR 100 dose limit is exceeded, and that the integrity of the primary coolant pressure boundary is not violated.

For design basis accidents as described in Guideline 11 (in combination with primary protection system failure), the goal of defense-in-depth analysis using best-estimate methodology is to show that any credible failure does not result in exceeding the 10 CFR 100 dose limits, violation of the integrity of the primary coolant pressure boundary, or violation of the integrity of the containment. The resulting analysis should be documented as described in Section 5, with details amplified and illustrated similarly to Figures 1–6, Sections 6 through 9, and the Appendix.

### 3.1. Guideline 1—Choosing Blocks

Since an objective of this analysis method is to view the subject design at a level of abstraction that reduces the level of detail, the main criterion for selecting blocks (previously defined in Section 2.5) is that the actual mechanism of failure inside a block should not be significant to other blocks. Therefore, a block is a physical subset of equipment and software for which it can be credibly assumed that internal failures, including the effects of software errors, will not propagate to other equipment or software. Examples of typical blocks are computers, local area networks or multiplexers, or PLCs.

Failure propagation modes can be divided into two classes: physical (e.g., electrical) and logical (e.g., by corrupted data or corrupted interactions caused by software design faults). In general, physical containment of faults is well understood and consists of (but is not limited to) physical separation, electrical isolation, electrical shielding, and separation of power supplies. For instance, it would be reasonable to assume that a computer consisting of printed circuit cards mounted on an electrically connected backplane bus and supplied by a single power supply could not be divided into more than one block. Propagation of logical faults (caused, for example, by software design errors), however, is not so well understood. In general, logical faults can propagate by the transmission of data<sup>3</sup> for which the recipient is unprepared,<sup>4</sup> or by failure to transmit data for which a recipient is waiting. Almost always, processors on printed circuit cards that are mounted on the

1 Standard Format, Section 15, “Accident Analysis,” USNRC Reg. Guide 1.70.

2 Ibid.

3 More generally, data includes any electrical signal or digital representation of such a signal.

4 In this context, “unprepared” means either not ready in time, as in early or out of sequence, or not able to handle the datum value or format correctly, as in a program fault caused by inability to handle corrupted data by taking reasonable default action.

### Section 3. Guidelines

same backplane bus are able to interfere with one another logically through shared memory or bus transactions unless such interactions are made physically impossible by hardware design. It is sometimes asserted that two software modules A and B, running in the same computer, are independent by virtue of protection provided by an operating system that controls the access privileges of A and B, or some other non-physical method of separation. This assertion is difficult to defend if it depends upon the reliability of the operating system software that enforces the separation. Computer systems that are physically separate and electrically isolated may still interfere with one another logically through the medium of local area network connections or communication links. The decision about where to draw block boundaries may hinge upon design commitments made by the applicant about certain equipment interconnections and logical dependencies.

Criteria for determining physical failure containment are:

- Physical separation
- Electrical isolation
- Power supply separation
- Electrical shielding

Criteria for determining containment of logical failures are:

- Given two software modules A and B, if it is physically impossible for a software fault in A to cause module B to fail, then there is sufficient fault isolation between A and B.
- There is no interaction through shared memories.
- There is only unidirectional communication (no handshaking) with other systems.
- The software continues to work regardless of local area network faults (i.e., the software is impervious to errors transmitted by, or occurring in, networks to which the processor running the software is connected).
- All input data from other systems are qualified before use.<sup>5</sup>

### 3.2. Guideline 2—Determining Diversity

During the late 1970s, the following conclusions were reached through work on improving reactor instrumentation system reliability (NUREG-0493):

1. Random independent component or subsystem failures are adequately mitigated by redundancy and should not be an important part of concerns over control/safety interdependence.

---

<sup>5</sup> Format and value are checked to be sure that subsequent software will not fail if the data are used.

2. Given adequate redundancy, the remaining concern is some sort of non-random, multiple failure or common-mode failure.
3. Physical and electrical independence is the beginning, not the end, of common-mode failure concerns. Related and almost-coincident failures of supposedly separate systems can occur because of functional interactions, shared signals, common design errors, common environmental effects, and human actions.

For those common-mode effects that can be identified, the usual engineering approach of designing, qualifying, installing, and operating instrumentation systems with great attention to physical, electrical, and functional independence is adequate. However, not all common-mode failures can be predicted, especially those of low—but still significant—probability. For these failures, judicious use of diversity is the current state of the art. In the 1979 study of the Westinghouse RESAR-414 integrated protection system, the NRC staff took an approach to diversity the staff termed “approach using a specified degree of system separation,” by which the staff meant that the (then) three functional echelons of defense (*control*, *trip*, and *ESFAS*) were to be sufficiently separated and diverse so that postulated CMF events did not lead to unacceptable consequences. One of the goals of the staff was to avoid detailed hypotheses and analyses of individual common-mode failures because the number of such analyses required would result in an impossibly large workload. This is still a guiding principle for judging diversity.

Diversity cannot be considered in the absence of independence; diverse protection system elements that are not independent are assumed to fail simultaneously through interdependencies. Thus, diversity is not a substitute for, nor should it be proposed instead of the independence required by regulation and by standard. Rather, diversity should be seen as a necessary accessory to independence for increasing system robustness in the face of unidentified common-mode failures.

For purposes of this guideline and convenience in assessment, diversity will be assumed to be separable into six attributes, listed in alphabetical order:

- Design diversity
- Equipment diversity
- Functional diversity
- Human diversity
- Signal diversity
- Software diversity

To determine the degree of diversity between two blocks, subsystems, or items of equipment, each block, subsystem, or item should be assessed with respect to the diversity



attributes. A set of recommended criteria is listed below for each attribute. A documented basis for claimed diversity attributes should be assembled, with arguments or supporting data.

After assessing individual diversity attributes between two blocks, subsystems, or items of equipment, the combined assessment should be used to present an argument that the one is either diverse or not diverse from the other. Following the suggested criteria for judging diversity attributes, an example is given for computer-based systems of combining such results to reach a diversity conclusion.

### 3.2.1. Design Diversity

Factors increasing diversity between two designs meeting the same requirements—excluding the effects of human diversity—are listed here in decreasing order of effect:

- Different technologies (e.g., analog versus digital)
- Different approaches within a technology (e.g., transformer-coupled AC instrumentation versus DC-coupled instrumentation)
- Different architecture (i.e., arrangement and connection of components)

### 3.2.2. Equipment Diversity

Factors increasing equipment diversity between two groups or items of equipment are listed here in decreasing order of effect:

- Different manufacturers of fundamentally different designs
- Same manufacturer of fundamentally different designs
- Different manufacturers making the same design
- Different versions of the same design

In computer equipment, there are additional details which help in judging the degree of diversity:

- Different CPU architecture (e.g., Intel 80X86 architecture versus Motorola 68000)
- Different CPU chip versions (e.g., Intel 80386 versus Intel 80486)
- Different printed circuit board designs<sup>6</sup>
- Different bus structure (e.g., VME versus Multibus II)

---

<sup>6</sup> Besides the processor board (or boards), a computer will probably contain memory boards, peripheral control boards, and special-purpose boards designed by the applicant or other custom design house.

It is worth mentioning that different CPU architecture is a very powerful sort of diversity, since this forces different compilers, linkers, and other auxiliary programs to be used. This also illustrates the deep connection between some diversity attributes; six attributes are presented for convenience of assessment, but this does not mean that they are independent of each other.

### 3.2.3. Functional Diversity

Factors increasing functional diversity between two independent subsystems are listed here in decreasing order of effect:

- Different underlying mechanism (e.g., gravity convection versus pumped flow, rod insertion versus boron poisoning).
- Different purpose, function (e.g., normal rod control versus reactor trip rod insertion), control logic, or actuation means.
- Different response time scale (e.g., a secondary system may react if accident conditions persist for a time).

### 3.2.4. Human Diversity

Factors increasing the human diversity of a design in decreasing order of effect are:

- Different design organization (i.e., company).
- Different engineering management team within the same company.
- Different designers, engineers, or programmers.<sup>7</sup>
- Different testers, installers, or certification personnel.

Management has the most significant effect on diversity because management controls the resources applied and the corporate culture under which designers, engineers, or programmers work. Poor resource allocation and a lack of “quality” commitment can vitiate the effectiveness of using different personnel. The relative importance of the human diversity attribute is the most difficult to assess of all the diversity attributes. It should be noted in this regard that diversity and quality are different issues; using a separate organization that has little experience with nuclear power plant protection systems may guarantee diversity, but it also may guarantee many fundamental errors that a more experienced, but possibly less diverse, organization would avoid.

### 3.2.5. Signal Diversity

Factors increasing signal diversity between two signal sources are listed here in decreasing order of effect:

---

<sup>7</sup> Designers, engineers, or programmers are sometimes shared by different management teams.

### Section 3. Guidelines

- Different reactor or process parameters sensed by different physical effects (e.g., pressure or neutron flux).
- Different reactor or process parameters sensed by the same physical effect (e.g., pressure versus water level or flow sensed by differential pressure sensors).
- The same reactor or process parameter sensed by a different redundant set of similar sensors (e.g., a set of four redundant water level sensors backed up by an additional set of four redundant water level sensors driving a diverse design of protective equipment).

#### 3.2.6. Software Diversity

Factors increasing diversity between software designs meeting the same requirements, excluding the effects of human diversity, are listed here in decreasing order of effect:

- Different algorithms, logic, and program architecture
- Different timing, order of execution
- Different operating system
- Different computer language

Another way of expressing these points is that software must differ significantly in parameters, dynamics, and logic to be considered diverse, but only if the “operating system” is sufficiently simple that it can be considered a small set of demand-driven subroutines. More complex operating systems introduce significant difficulties in analysis and may limit the independence that can be achieved, regardless of the quality of the safety software that uses the operating system. In other words, two different safety-critical subsystems that use the same operating system may be subject to CMF through the operating system even if no CMF exists in the safety software. The reason that computer language, for example *C*, *Ada*, or *Pascal*, is not listed among the more effective criteria, is that modern languages are converging, offer a common set of features, and can often be intermixed at the subroutine level. Computer language, therefore, has little effect on algorithms, logic, architecture, timing, or operating system services.

#### 3.2.7. Combining Diversity Attributes

Once an assessment of diversity attributes is made, the results can be combined to make an overall decision or to declare, for instance, that sufficient signal diversity exists. Which diversity attributes assume the greatest importance depends upon the situation. Since this document concerns diversity and defense-in-depth of computer-based reactor protection systems (including ESFAS), the immediate discussion will be limited to determining diversity of various architectures in that context.

For example, the clearest distinction between two candidate subsystems would be design diversity; a non-digital subsystem would easily be considered a diverse alternative to a digital subsystem. Between two digital systems (limited design diversity), different computer equipment (equipment diversity) made by different manufacturers (human diversity) would be considered diverse provided there was some functional and signal diversity or some software diversity. Some caution is indicated even where there is apparent computer equipment diversity, since program portability is now fairly common and the same software may run on two different computer types. In the likely instance of the same developer (limited human diversity) and similar equipment (limited equipment diversity), then software diversity coupled with either functional diversity or signal diversity would probably be necessary to declare that two subsystems were diverse.

In any case, the basis for claiming that a particular combination of diversity attributes constitutes sufficient diversity should be documented.

### 3.3. Guideline 3—System Failure Types

Guidelines 5 and 6 describe the method for postulating common-mode failures of blocks of the protective system. The system-level effects of these postulated CMFs are described here as three instrumentation system failure types, in order to clarify what the analyst should look for. Note that these failures are not the same as those considered in SAR Chapter 15 analyses.

#### 3.3.1. Type 1 Failures

Failures of type 1 happen when a plant transient is induced by the instrumentation system for which reactor trip or ESF function is needed, but may not occur, because of an interaction between echelons of defense. Type 1 failures typically begin with a challenge presented by the control system to the reactor trip system or to the ESFAS due to failure of a common sensor or signal source. Defense against such failures depends upon means of accomplishing safety functions that are diverse to the shared signals or equipment (i.e. not impaired by the postulated common-mode failure). Defense-in-depth analysis of type 1 failures is required by general analysis Guideline 12.

#### 3.3.2. Type 2 Failures

Failures of type 2 do not directly cause plant transients but are undetected until environmental effects or physical equipment failure cause a plant transient or design basis accident to which protective equipment may not respond. Failure to respond is due to postulated common-mode failure of redundant protection system divisions or portions thereof. Type 2 failures can have serious consequences only if the event needing safety action occurs while the protection system is in the failed state and before the failure is repaired. Defense against type 2 failures depends upon some combination of diverse *control system*, *reactor trip system*, ATWS mitigation equipment, *ESFAS*, and

*monitoring and indication* functions that are sufficient to mitigate the postulated incident. Defense-in-depth analysis of type 2 failures is required by general analysis Guidelines 10 and 11.

### 3.3.3. Type 3 Failures

Type 3 failures occur because, for some reason the primary sensors expected to respond to a design-basis event instead produce anomalous readings. For instance, accident conditions may have modified instrument response or an unanticipated event sequence may have modified the parameter values seen by the instrumentation (Hanauer and Walker 1968). Since type 3 failures are unpredictable by definition, a strategy dictated by experience is to ensure sufficient signal diversity that alternate means of detecting significant events exist. At a minimum, there should be sufficient signal diversity to ensure that for each anticipated operational occurrence in the design basis in conjunction with postulated CMFs, the plant shall be brought to a stable hot standby condition. For each accident in the design basis in conjunction with postulated CMFs, the plant response calculated using best-estimate (using realistic assumptions) analyses should not result in exceedance of the 10 CFR 100 dose limits, violation of the integrity of the primary coolant pressure boundary, or violation of the integrity of the containment. Defense-in-depth analysis that supports signal diversity required for type 3 failures is required by general analysis Guidelines 10 and 11.

## 3.4. Guideline 4—Echelon Requirement

The instrumentation system should provide four echelons of defense-in-depth: *control*, *reactor trip*, *engineered safety features* (ESF) actuation, and *monitoring and indicator system*.

The ***control echelon*** is that non-safety equipment which routinely prevents reactor excursions toward unsafe regimes of operation and is used for normal operation of the reactor.

The ***reactor trip echelon*** is that safety equipment designed to reduce reactivity rapidly in response to an uncontrolled excursion.

The ***ESFAS echelon*** is that safety equipment that removes heat or otherwise assists in maintaining the integrity of the three physical barriers to radioactive release (cladding, vessel, and containment).

The ***monitoring and indication echelon*** is that set of sensors, safety parameter displays, and independent manual controls required for intelligent human response to events.

In other words, echelons are defined by their function, while the instrumentation that initiates those functions resides in what are nominally called the control system, the scram or reactor trip system, the engineered safety features actuation system (ESFAS), the safety parameter display system, or the manual controls.

The ***monitoring and instrumentation echelon*** allows operators to compensate for control system excursions, or, in some cases, for failure of one of the two automatic safety echelons. The usual definition of Class 1E equipment (equipment essential to safety) still applies.

In general, the normal operational hierarchy for transients and accidents is that the second echelon (*reactor trip*) functions when the first (*control*) fails, and the third (*ESFAS*) and fourth (*monitoring and indication*) echelons support the first two. In the analysis method presented in this document, this order is sometimes reversed when non-Class 1E echelons are allowed to compensate for rare common-mode failures in Class 1E echelons (see Section 1.1, requirement 3).

## 3.5. Guideline 5—Method of Evaluation

The protection system is usually subdivided into redundant divisions, with each division consisting of interconnected blocks as described in Sections 2.1, 3.1, and 9.2. Each block should be considered a “black box,” so that any failure required to be postulated within the block fails all output signals. Block output signals must be assumed to fail in a manner that is credible but that produces the most detrimental consequences when analyzed in accordance with Guideline 9. In blocks containing software, it is credible that outputs shall assume values irrespective of inputs because the only logic connecting inputs to outputs is software, and the effects of software failures on outputs are unpredictable.

## 3.6. Guideline 6—Postulated Common-Mode Failure of Blocks

Analysis of defense-in-depth should be performed by postulating concurrent failures of the same block or identical blocks (as defined in Guideline 7) in all redundant divisions. Since several channels may pass through the same block or identical blocks, such common-mode failures have the potential to cause multiple channel failures in a single division, with the same failure replicated across all (four) protection system divisions. The output signals of the blocks thus postulated to fail should do so in accordance with Guideline 5. In other words, signals entering failed blocks assume the most adverse credible values on output, essentially losing their protective function at that point. Subject to Guidelines 7, 8, and 9, concurrent failure of each set of identical blocks in all divisions should be postulated in turn (until the list of diverse blocks has been exhausted), and the result of the failure should be documented as a finding of the analysis.

## 3.7. Guideline 7—Use of Identical Hardware and Software Modules

Blocks are to be considered identical for the purposes of the postulated common-mode failures required in Guideline 6 when the likelihood of a CMF affecting them simultaneously is not acceptably low. This means that the

### Section 3. Guidelines

probabilities of block failure are not independent and the probability of system failure cannot be calculated by simply multiplying block failure probabilities. Guideline 2 should be used to provide the basis for judging diversity of blocks.

#### 3.8. Guideline 8—Effect of Other Blocks

During any postulated common-mode failure, signals from failed blocks are propagated to downstream blocks, which react to the possibly erroneous signals. Subject to Guidelines 7 and 9, the other blocks are assumed to function correctly in exact response to all correct or incorrect inputs they receive.

#### 3.9. Guideline 9—Output Signals

Output signals are assumed to function one-way; that is, failures cannot propagate backwards into an output of a previous block. In cases where a block has more than one output signal, no output signal should be significantly influenced by any credible change or failure of equipment to which any other output signal is connected. This guideline includes any signal transmission paths involving multiplexed memory, local area networks, serial communication links, or multiplexers. If compliance with this guideline cannot be demonstrated, block definitions are incorrect and involved blocks should be redefined so that blocks mutually affected through output interconnections are coalesced into one block.

#### 3.10. Guideline 10—Diversity for Anticipated Operational Occurrences

For each anticipated operational occurrence in the design basis<sup>8</sup> which occurs in conjunction with each postulated CMF, the calculated plant response should not exceed a small fraction (10%) of the 10 CFR 100 dose limit or violate the integrity of the primary coolant pressure boundary. This guideline covers instrumentation system CMFs of types 2 and 3 (Guideline 3) for anticipated operational occurrences. A part of the analysis described herein should either (1) demonstrate that sufficient diversity exists to achieve these goals, or (2) identify the vulnerabilities discovered and the corrective actions taken, or (3) identify the vulnerabilities discovered and provide a documented basis that justifies actions not taken.

#### 3.11. Guideline 11—Diversity for Accidents

For each limiting fault in the design basis<sup>9</sup> which occurs in conjunction with each postulated CMF, the combined action of all echelons of defense should ensure that equipment provided by the design and required to mitigate the effects of the accident is promptly initiated, supported by necessary auxiliary equipment, and operated for the

necessary period of time. This guideline covers instrumentation system CMFs of types 2 and 3 (Guideline 3) for accidents. The plant response calculated using best-estimate (using realistic assumptions) analyses should not exceed the 10 CFR 100 dose limits, violate the integrity of the primary coolant pressure boundary, or violate the integrity of the containment. A part of the analysis described herein should either (1) demonstrate that sufficient diversity exists to achieve these goals, or (2) identify the vulnerabilities discovered and the corrective actions taken, or (3) identify the vulnerabilities discovered and provide a documented basis that justifies actions not taken.

#### 3.12. Guideline 12—Diversity Among Echelons of Defense

The control system, which includes most instrumentation and control equipment not part of the protection system, is not required to be Class 1E. The plant design basis includes postulated failures, some involving the control system, for which the reactor trip and the ESF actuation systems must provide ample protection. Yet the control system, even though not Class 1E equipment, plays three important roles in defense-in-depth. First, most disturbances are controlled without the need for action by the protection system. Second, failures in the control system may challenge the protection system. Third, during an incident in which one of the protection system echelons (*reactor trip* or *ESFAS*) is incapacitated by a CMF, the control system may mitigate the disturbance. From the first two roles, it is evident that the control system largely determines the frequency of challenges to the protection system, which by fault-tolerant design is expected to function reliably in response. Only in the third role is the control system actively involved as a diverse echelon of defense, in the rare instance that the protection system fails to function due to CMF. To prevent the protection system from failing in the second role and to preserve the control system's ability to act in the third role, it is important that transients or control system failures (type 1 failures described by Guideline 3) needing protection system action should not also induce protection system failures, or, in short, that the control system and the protection system should not be disabled by the same single failure. This concern is stated by GDC 24 of 10 CFR 50 Appendix A (separation of protection and control systems), the IEEE 279 requirement for no interaction between protection and control due to single random failures, and also by the IEEE 379 inclusion of identifiable cascaded failures within the definition of single failures.

Diversity between echelons is therefore necessary and is a concern of this analysis. The instrumentation and control system should be examined for potential interactions between the four echelons of defense, the *control system*, the *reactor trip system*, the *ESFAS*, and the *monitoring and indicator system*, with the intention of determining that the *functions* of at least two out of the four echelons of defense

<sup>8</sup> Usually these are elucidated in Section 15, "Accident Analysis," USNRC Reg. Guide 1.70.

<sup>9</sup> Ibid.

are unimpaired by interconnections.<sup>10</sup> In some cases, semi-independent subsystems such as ATWS mitigation equipment, may initiate functions of several echelons. In such cases, any additional interactions that may simultaneously disable one or more echelons of defense and may also disable the diverse semi-independent subsystem should be investigated. For example, when elements are shared between ATWS mitigation equipment and either the *reactor trip system* or the *ESFAS*, the analyst should ensure that the same failure that incapacitates the primary echelon of defense does not also disable the ATWS mitigation equipment, or that the consequences are acceptable. In the following, potential interactions between the nominal echelons are considered.

#### *Control/Reactor Trip Interaction*

When a CMF of a common element or signal source shared between the *control system* and the *reactor trip system* is postulated according to Guidelines 5 through 9, and (1) this CMF results in a plant response that requires reactor trip and (2) the CMF also impairs the trip function, then diverse means, which are not subject to or failed by the postulated CMF, should be provided to ensure that the plant response calculated using best-estimate (using realistic assumptions) analyses should not exceed a small fraction (10%) of the 10 CFR 100 dose limit or violate the integrity of the primary coolant pressure boundary. The diverse means may include manual action if the conditions of Guideline 14 are met.

#### *Control/ESFAS Interaction*

When a CMF of a common element or signal source shared between the *control system* and the *ESFAS* is postulated according to Guidelines 5 through 9, and (1) this CMF results in a plant response that requires ESF and (2) the CMF also impairs the ESF function, then diverse means, which are not subject to or failed by the postulated CMF, should be provided to effect the ESF function and to ensure that the plant response calculated using best-estimate (using realistic assumptions) analyses should not exceed a small fraction (10%) of the 10 CFR 100 dose limit or violate the integrity of the primary coolant pressure boundary. The diverse means may include manual action if the conditions of Guideline 14 are met.

#### *Reactor Trip/ESFAS Interaction*

Interconnections between reactor trip and ESFAS (for interlocks providing for (1) reactor trip if certain ESFs are initiated, (2) ESF initiation when a reactor trip occurs, or (3) operating bypass functions) are permitted provided it can be demonstrated that functions required by the ATWS rule (10 CFR 50.62) are not impaired under the constraints of Guidelines 8 and 9.

### 3.13. Guideline 13—Plant Monitoring

Signals may be transmitted from the *reactor trip* and the *ESFAS* to the control system or other display systems for plant monitoring purposes provided that all guidelines are met (with special attention to Guidelines 8 and 9) and the independence required by regulations and standards is maintained (GDC 24–10 CFR 50 Appendix A, IEEE 279, IEEE 603, IEEE 379, and IEEE 384). In addition, the Commission has approved the following requirements for alarm systems in ALWRs:

[...] alarm systems for ALWRs should meet the applicable EPRI requirements for redundancy, independence, and separation. In addition, alarms that are provided for manually controlled actions for which no automatic control is provided and that are required for the safety systems to accomplish their safety functions, shall meet the applicable requirements for Class 1E equipment and circuits (SECY-93-087 as approved). For example, type A variables in Regulatory Guide 1.97, Revision 3.

Connections and software used for plant monitoring and for surveillance of the *reactor trip* and *ESF* actuation systems should not significantly reduce the reliability of or increase the complexity of these systems. No failure of monitoring or display systems should influence the functioning of the reactor trip system or the ESFAS. A part of the analysis described herein should address the possibility that failure of the plant monitoring system may induce operators to attempt to operate the plant outside safety limits or in violation of the limiting conditions of operation. The analysis should demonstrate that such operator-induced transients will be compensated by protection system function, or a basis should be documented for claiming that the identified operator-induced transients are either not credible or result in no damage.

### 3.14. Guideline 14—Manual Operator Action

The fourth point of the Commission's diversity position (Section 1.1, item 4) requires that independent and diverse displays and manual controls be available so that operators can initiate a system-level actuation of critical safety functions. To verify this, the analysis should identify the critical safety functions, identify variables necessary for operator decisions using Regulatory Guide 1.97 for guidance, and demonstrate that the required sensor channels, displays, and manual controls are diverse and independent from the other three echelons (*control*, *reactor trip*, and *ESFAS*). In addition, manual operator action is permissible as a diverse means of response to postulated CMFs if the following criteria are met:

<sup>10</sup> Credit can be taken for operator action under restricted circumstances. See Guideline 14 in Section 3.14.

## Section 4. Data Required

- The postulated CMF and its effects do not impair any related aspect of the manual action, including information displayed that is necessary for operator action.
- Sufficient information is available to the operator.
- Sufficient time is available for operator analysis, decision, and action.
- Sufficient information and time is available for the operator to detect, analyze, and correct reasonably probable errors of operator function.

## **4. DATA REQUIRED TO DO THE ANALYSIS**

Besides the general guidelines and other background information, a diversity and defense-in-depth analysis requires certain specific information, some of which is unique to this analysis process. This section describes the main analysis data inputs.

### **4.1. System Diagram and Logic Diagrams**

A system diagram showing one division (of multiple redundant divisions) of the protective system to be analyzed is required. Additional detailed logic diagrams or textual descriptions may be necessary so that system response to various events can be determined by the analyst. The system diagram is equivalent to a single-line electrical diagram in that it is an abstraction that presents the system architecture at a level of detail appropriate to “block” failure analysis. Two examples are shown in the Appendix. A number of applicant design drawings and text descriptions often must be consolidated and re-drawn on one drawing as an arrangement of interconnected blocks, where the blocks are those chosen as described in Sections 2.5 and 3.1 of this document.

### **4.2. Chapter 15 Events**

In most instances, the SAR Chapter 15 events form the basis set of anticipated operational occurrences and accidents which will be used to challenge the protective system design. The applicant usually presents simulation curves of reactor parameters during the Chapter 15 incidents which at least determine the primary trip variables, but often exclude secondary trips due to postulated prompt protection system action. This is appropriate, considering the goals of Chapter 15 analyses. Chapter 15 analyses are also performed under conservative, rather than best-estimate, assumptions.

### **4.3. Alternate Trips**

Because the purpose of diversity and defense-in-depth analysis is to determine whether sufficient diversity or defense-in-depth exists to compensate for primary trip (or

ESF initiation) failure, it is necessary to know which secondary trip or initiation signals will activate defenses, if any, if primary signals or signal paths fail. Sometimes this is possible if trip point values are known and simulation curves of an incident or a closely similar incident show that alternative reactor parameters exceed trip values. When such information exists, a secondary trip will occur under conservative assumptions, although it is sometimes not clear whether, for less severe event sequences, a secondary trip point will be reached. In cases in which secondary trips cannot be clearly determined, it may be necessary to perform simulations that assume the primary trip variable fails. A set of best-estimate (using realistic assumptions) secondary trip sequences for events lacking a clear secondary trip should be deduced or obtained. An alternative to secondary trip data is best-estimate analyses that demonstrate for each such event that all possible sequences lead to safe conclusions.

### **4.4. Required Mitigation**

Success or failure of protective system action, whether by primary or alternate trip variables, is determined solely by the actuation of, or failure to actuate, appropriate mitigation measures. For this, the analyst needs to know the mitigation measures required for satisfactory response to the design basis incidents. For example, uncomplicated generator load rejection, an incident of moderate frequency, usually requires no more than reactor trip (if that), and normal condenser cooling operation is sufficient to protect fuel cladding. On the other hand, emergency cooling is required for a large loss of coolant accident inside containment.

## **5. WHAT SHOULD BE IN AN ANALYSIS?**

The report of a diversity and defense-in-depth analysis should explain why and how the analysis was done in sufficient detail that a competent reviewer can identify the underlying bases and assumptions and follow the reasoning to the report’s conclusions. Normally an analysis will be presented as a report body, which describes significant features and results, to which is attached one or more appendices which contain the detailed work. The following suggested format, presented in brief outline in this section, is a structure that accomplishes these purposes.

**1. Introduction**

An introduction identifies the design being evaluated and those doing the evaluation.

**2. Purpose**

Purpose describes the certification or approval for which the evaluation is being performed, or other reasons, if applicable.

**3. Background**

Background cites relevant regulatory or applicant history and places this particular analysis in historical context.

**4. New or Unusual Design Features**

New or unusual features of the analyzed design which may affect the analysis process or outcomes should be noted.

**5. Scope**

The scope of the current analysis is important to both analyst and reviewer to ensure appropriate coverage. What is not in the scope is just as important as what is in the scope.

*5.1. What is in Scope*

The subsystems and equipment being analyzed should be identified. The types of failure being postulated should be stated. The basis set of anticipated operational occurrences and accidents to be used should be stated or referenced.

*5.2. What is not in Scope*

Subsystems and equipment being excluded should be identified and reasons for the exclusion should be stated. Certain failures that are incredible or do not fit the definition of common-mode failure as used in the analysis should be described and reasons given for their exclusion.

**6. Description of Analysis Methods**

The analysis methods and their derivation from various authorities and guidelines should be described in detail. It is particularly important to discuss deviations from standard methods or assumptions made to clarify missing, incomplete, or inconsistent information

provided by design descriptions (which usually accompany a Standard Safety Analysis Report).

**7. Authorities and Guidelines**

Guidelines for performing the diversity and defense-in-depth analysis are given in Section 3, and should be referred to in this section of the analysis document. However, these guidelines do not supplant or supersede the general design criteria of 10 CFR 50, Appendix A, or other standards or design bases required by regulation or practice. Such criteria or standards as are applicable to the design should also be stated here. Criteria and standards are covered at greater length in Section 7.1 of this document.

**8. Types of Failures**

The types of failures to be considered in the analysis should be noted here. See Section 3.3 of this document for further detail.

**9. Sources of Design Information**

The sources from which design information was taken should be cited.

**10. Assumptions**

Rarely is a design so perfect that there are no uncertainties in its description. Practically, there will be uncertainties of material effect, and these should be described and resolved by stated assumptions that can be reviewed and corrected later, if necessary, by others. In the three analyses performed by independent contractors in 1992 and 1993, the assumptions section has proved to be a significant section. Assumptions are more fully covered in Section 6 of this document.

**11. Description of the Design**

Even if a diversity and defense-in-depth analysis is being performed by an applicant rather than an independent contractor, constructing an accurate design description may be an educational experience. This section, the assumptions section (described above), and a system diagram (Section 4.1 of this document) combine to provide an accurate description of the design to be analyzed. This section should be a high-level text description that, combined with the system diagram, lays out the system architecture and the details of the

design that are material to the analysis. Design description is elaborated in Section 7 of this document.

## 12. Findings

This section contains the analysis findings organized as described previously. Certain graphical aids to presenting results are suggested in Section 9 of this document.

## 13. References

Standards, regulations, and publications (such as this one) used during the preparation of the analysis should be cited in this section.

## 14. Appendices

The appendices contain the actual analysis worksheets and narratives. Section 9 describes an analysis worksheet that may be useful for systematic documentation of analysis details.

### *Autodiagnostic Software*

Autodiagnostic software is assumed to detect only malfunctions anticipated by software designers, but not unintended errors made by software designers.

### *Latency of Failures*

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

## 6.2. Assumptions Based on System Structure

System structure is the crux of defense-in-depth and diversity analysis. The assumptions in this section should describe what portions of the design have potential for common-mode failures and how and why block delineations were made. The example below, from a BWR analysis, describes the assumptions made regarding the blocks at risk of CMF:

## 6. ASSUMPTIONS TO BE STATED

The assumptions made by the analyst are crucial to understanding the decisions made during analysis. This section provides examples of subjects that should be covered, although there will be differences in detail depending upon the design being analyzed. Statement of the analysis assumptions is important because it permits easier and faster resolution of misunderstandings, should they arise.

### 6.1. Worst-Case Assumptions

The worst-case assumptions describe the particular application of Guideline 5 to the subject design. In the following example, the handling of an applicant's stated design features is described. In this instance the features discussed are "energize to trip," "de-energize to trip," "deadman timers," and "autodiagnostic software." The assumption on failure latency is the worst-case assumption applied to surveillance effectiveness.

#### *Failure Consequences*

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. Deadman timers are assumed to continue to be reset as if the subsystem were functioning normally.

#### *BWR CMF Blocks*

The RPS consists of the assembly shown in the System Diagram. Of the objects shown in that diagram, only Digital Trip Modules (DTMs), Trip Logic Units (TLUs), and the Essential Multiplexor System (EMS) contain software.

CMF blocks in a PWR were:

#### *PWR CMF Blocks*

The IEEE-796 standard bus is used as the interconnect between the logic cards which make up the various subsystems of the protection system. Communication between subsystems is carried on by other means. Therefore the blocks used in this analysis consist of the subsystems, where each subsystem uses a single IEEE-796 bus for interconnection of the logic cards of the subsystem. NUREG-0493 'Measured Variable Blocks' and 'Derived Variable Blocks' cannot usefully be identified in this design.



This choice is made because a subsystem so defined appears to be the smallest block into which the (reactor) protection system can be subdivided with credible restrictions on block-to-block fault propagation. Hardware or software failure of any printed circuit board in an IEEE-796 chassis is assumed to fail the entire chassis. It is assumed that some failures are not detected by the watchdog timer.

### 6.2.1. Diversity of Blocks

Guideline 7 requires that “identical” blocks in a design be determined. Guideline 2 provides criteria for determining diversity (or similarity) among subsystems, and this section should describe the precise application of Guideline 2 to the instant design so that it is clear which blocks are considered identical. Here, the application of Guidelines 2 and 7 is stated for a BWR design, followed by substantially the same example for a PWR:

#### *Guideline 2 Applied to a BWR*

The standard for independence between two subsystems as defined above is that they must differ significantly in parameters, dynamics, and logic. If two such subsystems perform similar functions but have differing inputs (different parameters being sensed) combined by different logic, it is assumed that the two subsystems do not have a common failure mode. This assumption is reasonable since it is implicit that the programs being run will differ in timing and logic because of the differing inputs and processing code. By this standard, DTMs with differing inputs will differ from each other, and TLUs with differing inputs will be independent of each other.

In contrast, subsystems with the same functions, hardware, and similar inputs (as exist in functionally identical subsystems in separate protection system divisions) are assumed to have common failure modes due to potential replicated software errors. These subsystems are substantially the same in parameters, dynamics, and logic. Such failures need not occur at identical times, but merely close

enough that surveillance is insufficient to detect the failures in time for effective repair. (This assumption implies common-mode failures in DTMs of similar inputs, TLUs of similar inputs, and the EMS.)

#### *Guideline 2 Applied to a PWR*

The standard for independence between two subsystems as defined (in Guideline 2) is that they must differ significantly in parameters, dynamics, and logic. If two such subsystems perform similar functions but have differing inputs (different parameters being sensed) combined by different logic, it is assumed that the two subsystems do not have a common failure mode. This assumption is reasonable since it is implicit that the programs being run will differ in timing and logic because of the differing inputs and processing code.

In contrast, IEEE-796 subsystems with the same functions, hardware, and similar inputs (as exist in functionally identical subsystems in separate protection system divisions) are assumed to have common failure modes due to potential replicated software errors. These subsystems are substantially the same in parameters, dynamics, and logic. Such failures need not occur at identical times, but merely close enough that surveillance is evaded. (This assumption implies common-mode failures in the RT groups, ESF groups, Engineered Safety Features Actuation Subsystems (ESFAS), PLCs, Trip Enable, or Global Trip subsystems of each division; failure of the ESFAS would disable automatic initiation of ESF equipment, while still allowing manual initiations; a PLC failure would disable automatic and manual initiation of all ESF equipment; failure of the Trip Enable Subsystem would incapacitate automatic partial reactor trips from the Reactor Trip Subsystems, but Global Trips and manual trips would still be available; a common mode failure of the Global Trip subsystems prevents any automatic reactor trip, while still allowing manual trip.)

## 6.3. Assumptions for Echelon Defense-in-Depth

The equivalent of the four nominal echelons, *control*, *trip*, *ESFAS*, and *monitoring and indicator* must be identified in a design. Defense-in-depth assumptions describe the arrangement of echelons of defense

## Section 7. Design Description

(which equipment is part of which echelon), necessary mitigations or effectiveness of certain mitigation equipment, and any other assumptions necessary to clarify which combinations of equipment must function during the events studied. In some instances, this may require identifying and categorizing equipment such as that designed to satisfy the ATWS rule, but which crosses nominal echelon boundaries in its effects.

### 6.4. Evaluation Criteria

The criteria for success are stated in Guidelines 10 through 12 for event responses and in Guideline 13 for plant monitoring. Any deviation or additional criteria should be stated here. By default, the applicant's list (if such a list exists) of necessary and sufficient mitigation actions for various events is considered sufficient protection system response to fulfill Guidelines 10 through 12. These actions, or the list reference, would normally be detailed in the previous section on echelons of defense.

## 7. DESCRIPTION OF THE DESIGN

The design being analyzed should be described with emphasis on factors that are important to diversity and defense in depth. This is not merely a repetition of the applicant's SAR submission, which may be detailed, but is a critical selection from what may be voluminous material of that part that forms the basis for analytic decision making. A design description consists of three parts: the design basis which any successful design must satisfy, a description of the design architecture (probably supported by a number of drawings), and a description of intentional diversity in the design.

### 7.1. Design Basis

Design bases are the rules under which a design is executed and they specify general qualities that the resulting design will satisfy. In cases where it may not be clear from details how to decide a particular analytic question, the design basis may provide guidance sufficient to make the decision. Certain design qualities are mandated by regulation and these are listed below under "General or Regulatory Bases." An applicant may also have agreed or may have volunteered to use certain standards or techniques.

#### 7.1.1. General or Regulatory Bases

Design basis requirements pertinent to defense-in-depth and diversity for the light water reactor designs 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... (S)ome 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... (T)he 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:*

4.17, Manual Initiation. The protection system shall include means for manual initiation.

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

4.6, Channel Independence. Channels that provide signals for the same protective functions shall be independent and physically separated.

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, and is endorsed by Regulatory Guide 1.153 as an alternative.

### 7.1.2. Additional Agreed Bases

The applicant may have agreed to use additional standards or conform to regulations or design techniques that are not directly required by the sources mentioned above. These bases should be identified.

### 7.1.3. Applicant's Statements

The applicant may have made statements in SAR text that certain standards would be used or that certain design techniques would be used or would be avoided. For example, an applicant may voluntarily commit to avoiding the use of interrupts and multitasking operating systems. Commitments that have or could have a material effect on the outcome of the analysis should be identified.

## 7.2. Design Architecture

The points of the applicant's design that are salient to defense-in-depth and to the separation of the design into independent, diverse subsystems should be described. A system block diagram, such as that demonstrated in the Appendix, is extremely helpful here. The echelons of defense should be identified, and any division into redundant, independent divisions should be described. Relations between the echelons, and between the echelons and subsystems such as diverse ATWS mitigation equipment or the remote shutdown panel, should be detailed with attention to aspects important to the analysis. In parts of the design that use redundancy, the voting scheme should be described, particularly where it may have asymmetries that could be single-failure vulnerabilities. It should also be noted where the applicant's design commitments are being used to decide significant design issues rather than using applicant-supplied design details.

### 7.3. Intentional Design Diversity

Any specific diversity or design features intended by the applicant to improve protection system performance in the face of CMF should be acknowledged.

## 8. FINDINGS

Findings should be presented in a sensible organization that could be used directly by license applicants to reduce discovered vulnerabilities in their reactor protection systems. Previous analyses have used an organization similar to the following.

### 8.1. General Vulnerabilities

These are vulnerabilities that appear in a majority of cases studied under Guidelines 10 and 11. Reducing these would probably be considered a higher priority than reducing isolated, specific vulnerabilities.

### 8.2. Specific Vulnerabilities

Vulnerabilities found under Guidelines 10 and 11 that occur only during one or a few SAR Chapter 15 events are reported here. These might be considered lower priority than general vulnerabilities, depending upon the event consequences.

### 8.3. Evaluation of Diversity

This section contains an evaluation of how many events are potentially detected only by one sensor. Since reactor trip and various ESF functions are initiated by different logical combinations of sensor signals, this findings section discusses diversity for all mitigation functions.

### 8.4. Shared Signals

This section reports the results of the analysis required by Guideline 12.

### 8.5. Special Findings

Any other findings that a responsible reviewer may have noted during perusal of the design should be reported here.

## 9. AIDS TO PRESENTATION OR ANALYSIS

Graphical aids can be used to enhance the intelligibility of a report and their use is encouraged. Previous workers have found two kinds of charts and a drawing to be particularly useful both in doing the analysis and in presenting the results. Analysis charts aid the analyst by presenting analytic decisions in a matrix format that permits failure-by-failure determination of system response. Vulnerability summary charts show analysis results consolidated in matrix form by design basis event versus signals and blocks. The system block diagram presents the system architecture with only the interconnections of interest to the analyst being displayed.

Examples of graphical aids are given in the following sections, some of which have been taken from diversity and

defense-in-depth studies prior to the conclusion of the regulatory review process. Since this is done for explanatory reasons only, no conclusions should be drawn regarding the eventual resolution of apparent vulnerabilities in the subject reactor protection systems.

### 9.1. Analysis Charts

Two analysis charts are shown in Figures 1 and 2, one for a pressurized water reactor and one for a boiling water reactor. These charts differ in detail, but their common purpose is to record failed signals or blocks ("CMF groups") systematically and to indicate the results of each failure. One analysis chart is prepared for each Chapter 15 event studied. The top portion of the chart consists of lines labeled with reactor parameters and columns labeled with sensors or blocks. The failure of a sensor or a block will prevent a reactor parameter signal from passing through the sensor or the block, and this is indicated by placing a zero in the appropriate intersection of row and column in the upper half of the chart. If the column is followed to the lower half of the chart, the mitigation means required for this event and for the CMF represented in this column are marked either with a zero (meaning no diverse initiation) or the number of the reactor parameter that does cause initiation. The chart is marked for each sensor, block, parameter, and mitigation means relevant to the event and then examined for zeros in the lower half. The lower-half zeros represent a failure to initiate mitigation for the columnar CMF in conjunction with the Chapter 15 event, and if insufficient mitigation is initiated, a vulnerability has been found. Insufficient mitigation exists if the sum of mitigation means with non-zero initiators in a column is less than the applicant's required mitigation for the Chapter 15 event, reduced by the effects of portions of the control system that are postulated to continue operation. A demonstration of the use of analysis charts is contained in Figure 3.

The analysis chart provides a stepwise method of considering common-mode failures and their effects. However, it may be difficult for others to interpret the analyst's work solely from the chart, so it should be accompanied with a short narrative describing the reasoning behind the chart marking.

### 9.2. System Block Diagram

Two system block diagrams are contained in the Appendix, along with a discussion of how blocks were selected and what level of detail is appropriate. Since an applicant has several purposes for preparing diagrams of a proposed protection system, it is unlikely that there will be an applicant system drawing containing the necessary detail for CMF analysis but not overburdened with extraneous matter. Arrangement into blocks also aids the analyst's perceptions and presents the significant interconnections graphically. Guidelines 6 through 9 require that input and output connections be determined for each CMF taken in conjunction with SAR Chapter 15 events, and it is tedious

and inefficient to have to search through several drawings each time. Also, the system block diagram makes the analyst's view of the system clear to readers of the analysis results, so that analyst misperceptions can be corrected by knowledgeable reviewers. In spite of the effort involved, making an accurate system block diagram is recommended.

### **9.3. Vulnerability Summary Charts**

There are potentially about 20 or 30 events to analyze, which result in an equal number of analysis charts. Vulnerabilities documented on the analysis charts can be transferred to a Vulnerability Summary chart, of which two examples are shown in Figures 4 and 5, for a PWR and a BWR respectively. These examples are from analyses in progress, before resolution of vulnerabilities has occurred, a process beyond the scope of this discussion. Showing these examples after the resolution process has been completed would be uninformative.

It is also possible to summarize vulnerabilities discovered during analysis of type 3 failures discovered under Guideline 12. A summary chart for such a purpose is shown in Figure 6. This chart, too, is presented prior to the vulnerability resolution process.

## Section 9. Aids to Presentation

Event Number Title	CMF Groups	Reactor Trip Subsystem 1	Reactor Trip Subsystem 2	ESF Subsystem 1	ESF Subsystem 2	Global Trip Subsystem	Trip Enable Subsystem	A1 & A2 ESFAS	Protection Logic Cabinet	Soft Control Workstation	NISPAC 1 Subsystem	NISPAC 2 Subsystem	Table Number
													LEGEND: Blank - not involved or affected 0 - not available due to CMF 1 to 23 - initiating parameter
Reactor Parameter													
1 High Startup Neutron Flux													
2 Overtemperature		0				0							Indicates that failure of the global trip subsystem inhibits protective action caused by these parameters
3 Overpower		0				0							
4 Low Coolant Flow													
5 Low RCP Speed													
6 High Pressurizer L													
7 High RCP Bearing						0							
8 High Inter. Neutron Flux													Comment lines
9 High Power Neutron Flux													
10 High + Flux Rate													
11 Low Pressurizer Pressure													
12 High Pressurizer Pressure													
13 Low SG Level													
14 High SG Level													Plant parameters with ID numbers
15 Low Steam Line Pressure													
16 Neg. Rate SL Pressure													
17 High Hot Leg Temp.													
18 Low Cold Leg Temp.													
19 Low Startup FW Flow													
20 High Cont. Pressure													
21 Low CMT Level													Failure ID numbers
22 Low Tavq													
23 Low Pressurizer Level													
Mitigation		1	2	3	4	5	6	7	8	9	10	11	
Automatic Reactor Trip		14/9				0							A zero in the lower section means that indicated mitigation (reactor trip) fails if failure 5 (global trip) occurs
Safeguards Actuation Signal													
1st Stage ADS Valve Signal													
IRWST injection													
Main Feedwater Line Isolation													Even if RT Group 1 fails, the reactor will trip on diverse parameters 14 or 9
RCP Trip													
CMT Injection													
Auto. Depressurization System													
Turbine Trip													
Steam Line Isolation													Mitigation systems
SG Blowdown Isolation													
Containment Cooling													
Startup Feedwater Isolation													
Passive Residual Heat Removal													
Accumulator Injection													
CVCS Isolation													
Block Steam Dump													
Letdown Line Isolation													

A single common-mode failure and its consequences are represented by a column of the chart. The sensor channel or block that 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 of 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.

**Figure 1. Pressurized Water Reactor Analysis Chart**

GE SBWR		CMF Groups														Table Number
Event Number Title	Reactor Parameter		DTM	TLU	EMS	APRM	(N) RPV Nar. Rng. Water Level	(W) RPV Wd. Rng. Water Level	RPV Dome Pressure	MSLIV Position Switches	MSL Flow Sensors	Condenser Vac. Sensors	Turbine Inlet Pressure	LEGEND: Blank—not involved or affected 0—not available due to CMF 1 to 23—initiating parameter		
1	Low RPV Water Level															
2	High RPV Water Level															
3	High RPV Pressure															
4	Low RPV Pressure															
5	High Drywell Pressure															
6	MSIVs Close															
7	High Suppr. Pool Temp															
8	Low Suppr. Pool Level		0													
9	High Neutron Flux															
10	Short Reactor Period															
11	Low GDCS Pool Level															
12	High Basemat Temp		0													
13	Turbine Stop Valve Close															
14	Turb. Inlet Pressure Low															
15	Main Condenser Vacuum															
16	High SL Flow															
17	High SL Radiation															
18	High Contmnt Radiation															
19	High Area Radiation															
20	High Area Temp															
21	Low CRD Pressure															
22	Manual DPV Actuation															
23	Manual GDCS Actuation															
Mitigation																
Automatic Reactor Trip																
Close MSIVs																
Reactor Blowdown, SRVs																
Reactor Blowdown, DPVs																
GDCS Initiation																
GDCS Deluge Valves																
Operate ICS Valves																
LD & IS Valves Operate																
SLCS																

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.

Figure 2. Boiling Water Reactor Analysis Chart

Event Number 15.2.4 Title: Inadvertent Closure of All MSLIVs		Table Number 15.2-8										
Reactor Parameter		DTM	TLU	EMS	APRM	(N) RPV Nar. Rng. Water Level	(W) RPV Wd. Rng. Water Level	RPV Dome Pressure	MSLIV Position Switches	MSL Flow Sensors	Condenser Vac. Sensors	Turbine Inlet Pressure
		LEGEND: Blank—not involved or affected 0—not available due to CMF 1 to 21—initiating parameter										
1	Low RPV Water Level	0	0	0								
2	High RPV Water Level											
3	High RPV Pressure	0	0	0				0				
4	Low RPV Pressure											
5	High Drywell Pressure											
6	MSLIVs Close	0	0	0					0			
7	High Suppr. Pool Temp											
8	Low Suppr. Pool Level											
9	High Neutron Flux		0		0							
10	Short Reactor Period											
11	Low GDCS Pool Level											
12	High Basemat Temp											
13	Turbine Stop Valve Close											
14	Turb. Inlet Pressure Low											
15	Main Condenser Vacuum											
16	High SL Flow											
17	High SL Radiation											
18	High Contmnt Radiation											
19	High Area Radiation											
20	High Area Temp											
21	Low CRD Pressure											
<b>Mitigation</b>												
Automatic Reactor Trip		9*	3*	6	6			6	9			* = ARI
Close MSLIVs												
Reactor Blowdown, SRVs												
Reactor Blowdown, DPVs												
GDCS Initiation												
GDCS Deluge Valves												
Operate ICS Valves		1*	1*	6	6			6	3			* = diverse actuation (L2)
LD & IS Valves Operate												
SLCS												

Figure 3. Use of Analysis Charts



CMF Vulnerability Summary	CMF Groups	CMF Vulnerability Summary										
		Reactor Trip Subsystem 1	Reactor Trip Subsystem 2	ESF Subsystem 1	ESF Subsystem 2	Global Trip Subsystem	Trip Enable Subsystem	A1 & A2 ESFAS	Protection Logic Cabinet	Soft Control Workstation	NISPAC 1 Subsystem	NISPAC 2 Subsystem
Chapter 15 Event												
15.1.2 - FW Sys. Malfunction that Results in an Inc. in FW Flow				E	E	T		E	E	E		
15.1.4 - Inadvertent Opening of a SG Relief or Safety Valve					E	T		E	E	E		
15.1.5 Steam System Piping Failure					E	T		E	E	E		
15.1.6 - Inadvertent Operation of the PRHR System				E	E	T		E	E	E		
15.2.2 through 15.2.5 - Turbine Trips						T						
15.2.6 - Loss of AC Power to the Plant Auxiliaries				E		T		E	E	E		
15.2.7 - Loss of Normal Feedwater Flow						T		E	E	E		
15.2.8 - Feedwater System Pipe Break				E	E	T		E	E	E		
15.3.1 - Partial Loss of Forced Reactor Coolant Flow						T						
15.3.2 - Complete Loss of Forced Reactor Coolant Flow						T						
15.3.3 RCP Shaft Seizure (Locked Rotor)						T						
15.3.4 RCP Shaft Break						T						
15.4.1 - Unc. RCCA Bank Wd. from a Subc. or LP. Startup		T				T						T
15.4.2 - Unc. RCCA Bank Withdrawal at Power						T						
15.4.3 RCCA Misalignment						T						
15.4.4 - Startup of an Inactive RCP at Inc. Temp.		T				T						T
15.4.6 - CVCS Malfunction that Res. in Dec. in Boron Conc.				E				E	E	E	E	E
15.4.8 - Spectrum of RCCA Ejection Accidents		T				T		E	E	E		T
15.5.2 - CVCS Malfunction that Inc. Reactor Coolant Inventory				E	E	T		E	E	E		
15.6.1 - Inad. Opening of a Przr SRV or Inad. Op. of the ADS				E		T		E	E	E		
15.6.3 SG Tube Rupture				E	E	T		E	E	E		
15.6.5 LOCA				E	E	T		E	E	E		

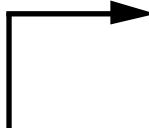
**Legend:**  
blank - not involved  
T - Trip vulnerability  
E - ESFAS vulnerability

Figure 4. Sample Pressurized Water Reactor Vulnerability Summary Chart

Section 9. Aids to Presentation

CMF Vulnerability Summary	CMF Groups												Vulnerability Summary
		DTM	TLU	EMS	APRM	(N) RPV Nar. Rng. Water Level	(W) RPV Wd. Rng. Water Level	RPV Dome Pressure	MSLIV Position Switches	MSL Flow Sensors	Condenser Vac. Sensors	Turbine Inlet Pressure	
Chapter 15 Event													
15.1.2—Feedwater Controller Failure—Maximum Demand													
15.1.3—Pressure Regulator Failure—Open													
15.1.4—Inadvertent Opening of an RPV Relief or Safety Valve													
15.1.6—Inadvertent RWCU/SDC Operation													
15.2.1—Pressure Regulator Failure—Closed													
15.2.2—Generator Load Rejection													
15.2.3—Turbine Trip													
15.2.4—Inadvertent MSLIV Closure													
15.2.5—Loss of Condenser Vacuum													
15.2.6—Loss of AC Power to the Plant Auxiliaries													
15.2.7—Loss of Normal Feedwater Flow													
15.5.1—Inadvertent Startup of an Isolation Condenser													
15.6.2—Small Break of Instrument Line													
15.6.4—Steam Pipe Break Outside Containment			E										
15.6.5—LOCA Inside Containment			E										
15.6.6—Feedwater Line Break Outside Containment													

Figure 5. Sample Boiling Water Reactor Vulnerability Summary Chart

ESF Subsystem 		Reactor Parameter																													
		1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	"S" Signal	Cont. ISO	ADS	Main FW ISO	Main FW Pump Trip	RCP Trip	CMT ISO	Turbine Trip	MSIV ISO	SU FW ISO	PRHR	CVCS ISO	Blk Stm Dump	CMT Injection	
Low Pressurizer Pressure																															
Low Comp. Steam Line Pressure																															
Low-1 Tavg																															
Low-2 Tavg																															
Low-2 Pressurizer Level																															
Low SG WR Level																															
High Hot Leg Temp. Thot																															
High Neg. Rate SL Pressure																															
High Pressurizer Level																															
Low Cold Leg Temp. Tcold																															
High-1 Cont. Pressure																															
Low-1 CMT Level																															
High-2 Comp. SG NR Level																															
High RCP Bearing Temp.																															
Low SG NR Level																															
Low Startup Feedwater Flow																															
"S" Signal																															
CMT Injection																															
ADS 1st Stage																															
Manual FW ISO																															
Reactor Trip																															

Note: An X with a number must be coincident with the same numbered X to actuate the system (e.g., both X1's must be asserted to initiate ADS).

Figure 6. Summary Chart for Analysis of Type 3 Failures

This page intentionally left blank.

## REFERENCES

- Branch Technical Position, "Digital Instrumentation and Control Systems in Advanced Plants," HICB, 1993.
- Hanauer, S. H., and Walker, C. S., *Design Principles of Reactor Protection Systems*, ORNL-NSIC-51, Oak Ridge National Laboratory, September 1968.
- Hanauer, Stephen H., "A Review of Diversity in Trip Units," *Letter Report*, EG&G Idaho, Inc., February 1990.
- Kelly, John P. J., McVittie, Thomas I., Yamamoto, Wayne I., "Implementing Design Diversity to Achieve Fault Tolerance," *IEEE Software*, July 1991, pp. 61–71.
- Knight, J. C., and Leveson, N. G., "An Experimental Evaluation of the Assumption of Independence in Multi-Version Programming," *IEEE Transactions on Software Engineering*, Vol. SE-12, No. 1, January 1986, pp. 96–109.
- Mahmood, Aamer, and McCluskey, E. J., "Concurrent Error Detection Using Watchdog Processors—A Survey," *IEEE Trans. on Comm.*, Vol. 37, No. 2, February 1988, pp. 160–174.
- NUREG-0493, *A Defense-in-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System*, United States Nuclear Regulatory Commission, March, 1979.
- NUREG-800, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants*, United States Nuclear Regulatory Commission.
- NRC Regulatory Guide 1.70, Revision 2, *Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants*, September 1975.
- Palomar, J. V., Preckshot, G. G., and Wyman, R. H., *A Defense-in-Depth and Diversity Assessment of the General Electric ABWR Protection System*, Lawrence Livermore National Laboratory, UCRL-ID-114000, April 30, 1993a.
- Palomar, J. V., Preckshot, G. G., and Wyman, R. H., *A Defense-in-Depth and Diversity Assessment of the Westinghouse AP-600 Protection System*, Lawrence Livermore National Laboratory, Draft Report, September 1, 1993b.
- Preckshot, G. G., *A Defense-in-Depth and Diversity Assessment of the General Electric SBWR Protection System*, Lawrence Livermore National Laboratory, Draft Report, July 30, 1993a.
- Preckshot, G. G., *Reviewing Real-Time Performance of Nuclear Reactor Safety Systems*, NUREG/CR-6083, 1993b.
- Preckshot, G. G., "Assessment of IEEE Standard 796-1983 'IEEE Microprocessor System Bus'," *Technical Letter Report*, Lawrence Livermore National Laboratory, January 15, 1993c.
- Regulatory Guide 1.97, "Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident," NRC, Rev. 3, May 1983.
- Regulatory Guide 1.153, "Criteria for Power, Instrumentation, and Control Portions of Safety Systems," NRC.
- SECY-91-292, "Digital Computer Systems for Advanced Light Water Reactors," NRC, September 16, 1991.
- SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," NRC, April 2, 1993.
- Staff Requirements Memorandum, "SECY-93-087, Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," July 21, 1993.

## References

This page intentionally left blank.

## APPENDIX—BLOCK EXAMPLES

Choosing blocks in a design is sufficiently important that this appendix provides two system block diagrams and discusses the reasons why choices were made in these cases. The first block diagram was prepared for an analysis of a BWR protection system that included intentionally diverse (non-digital) logic elements as alternate trip pathways to digital elements. To emphasize this, the digital elements are drawn in the upper-left quadrant of the (2-page) system block diagram, while the intentionally diverse elements occupy the lower-left quadrant. The reasoning in the report was stated as follows:

### *Choice of blocks*

The RPS consists of the assembly shown in (the following) System Diagram. Of the objects shown in that diagram, only DTMs, TLUs, and the EMS contain software.

### *Blocks that are independent*

The standard for independence between two subsystems as defined above is that they must differ significantly in parameters, dynamics, and logic. If two such subsystems perform similar functions but have differing inputs (different parameters being sensed) combined by different logic, it is assumed that the two subsystems do not have a common failure mode. This assumption is reasonable since it is implicit that the programs being run will differ in timing and logic because of the differing inputs and processing code. By this standard, DTMs with differing inputs will differ from each other, and TLUs with differing inputs will be independent of each other.

### *Blocks that are identical*

In contrast, subsystems with the same functions, hardware, and similar inputs (as exist in

functionally identical subsystems in separate protection system divisions) are assumed to have common failure modes due to potential replicated software errors. These subsystems are substantially the same in parameters, dynamics, and logic. Such failures need not occur at identical times, but merely close enough that surveillance is insufficient to detect the failures in time for effective repair. (This assumption implies common-mode failures in DTMs of similar inputs, TLUs of similar inputs, and the EMS.)

### *Effect of the operating system*

The operating system, which is common to all subsystems in this design, will not be included as a source of common-mode software failures. It is assumed that the operating system as described by (the vendor) is simple enough that failures are related to service demands and that service demands are distributed differently enough in subsystems defined as dissimilar (above) to exclude the operating system as a separate cause of common-mode failure. Consequently, any common-mode operating system failures are subsumed by (the previous paragraph). This assumption is not valid if (the vendor) uses a complex, multitasking operating system or uses more than a simple clock-updating timer interrupt.

The system block diagram shows the detail of which signals go to which blocks and through the EMS, which is considered a potential site of common-mode failures. Internal logic is not shown because it is irrelevant for the purposes of the analysis.

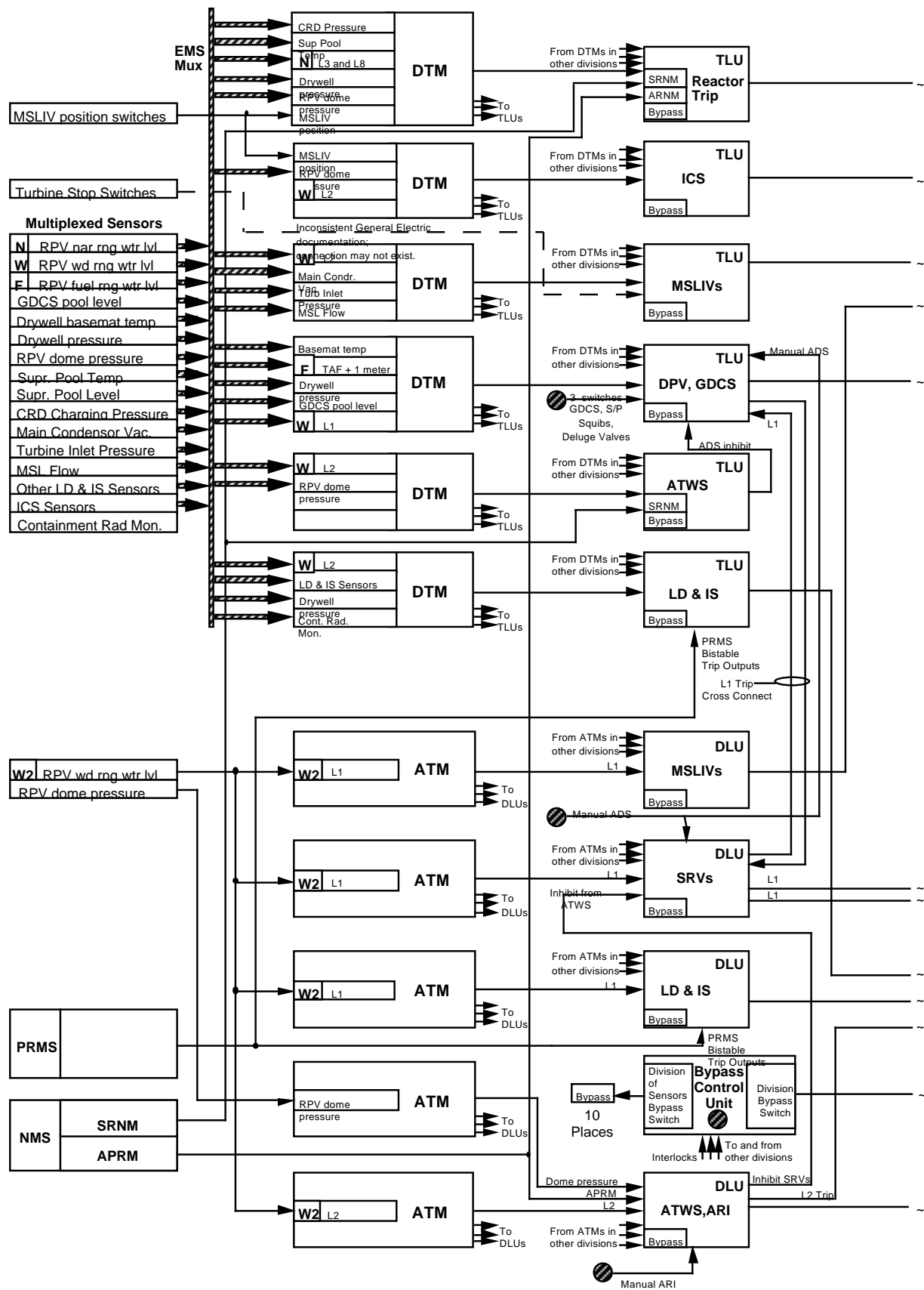


Figure A-1. Sample BWR System Block Diagram



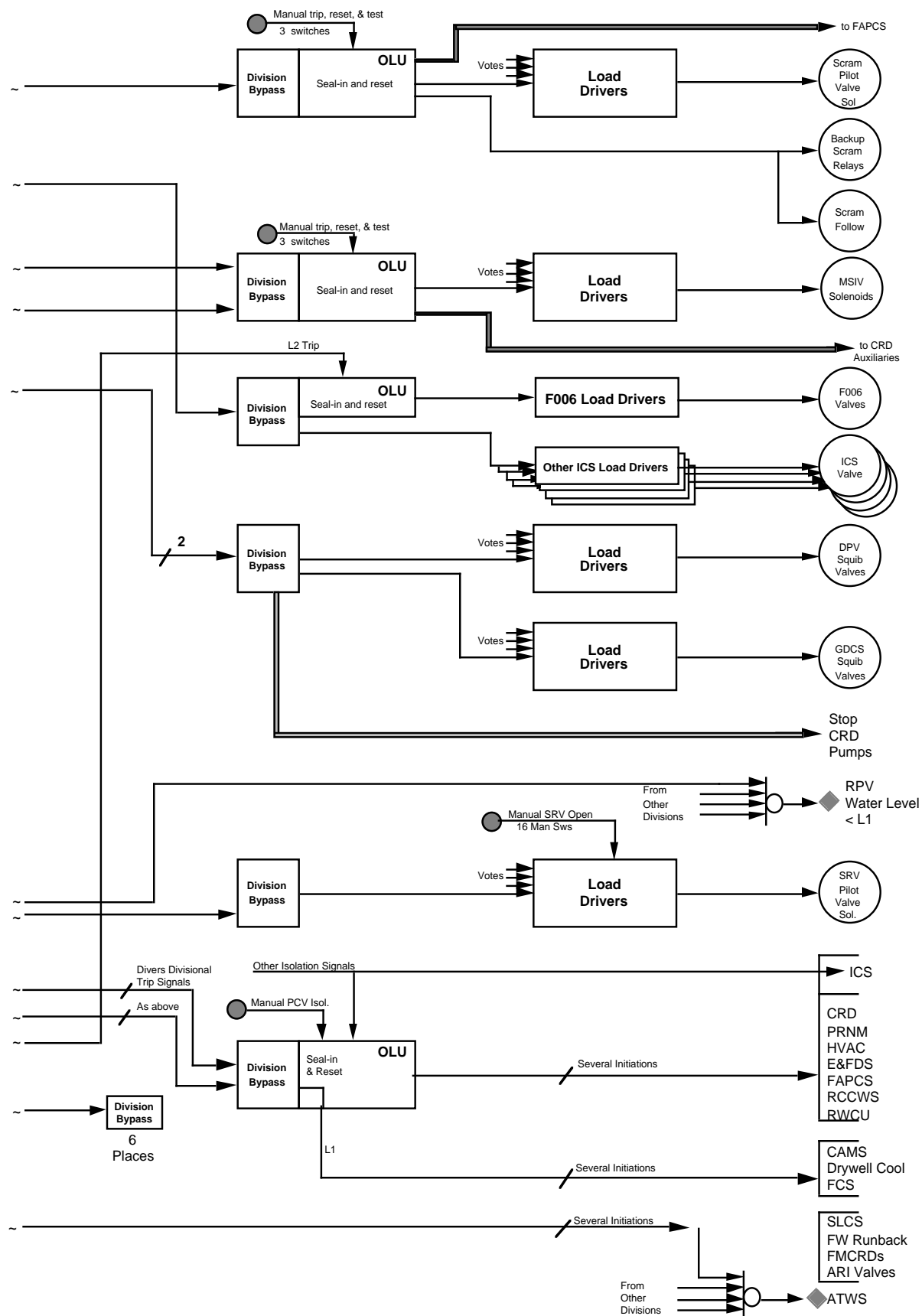


Figure A-1. Sample BWR System Block Diagram (continued)

This page intentionally left blank.

The second block diagram was prepared for an analysis of a PWR protection system that was constructed by interconnecting a number of superficially similar IEEE 796 bus computer systems. These computer systems appear to be similar because they consisted of standard printed circuit card modules plugged into IEEE 796 backplanes. The computer systems, however, differed significantly in function performed, detailed configuration, and purpose within the architecture. The reasoning that was used in the report for the choice of identical or diverse blocks was stated as follows:

#### *Choice of blocks*

The IEEE-796 standard bus is used as the interconnect between the logic cards which make up the various subsystems of the protection system. Communication between subsystems is carried on by other means. Therefore the blocks used in this analysis consist of the subsystems, where each subsystem uses a single IEEE-796 bus for interconnection of the logic cards of the subsystem. NUREG-0493 "Measured Variable Blocks" and "Derived Variable Blocks" cannot usefully be identified in this design.

This choice is made because a subsystem so defined appears to be the smallest block into which the (reactor) protection system can be subdivided with credible restrictions on block-to-block fault propagation. Hardware or software failure of any printed circuit board in an IEEE-796 chassis is assumed to fail the entire chassis. It is assumed that some failures are not detected by the watchdog timer. For additional information on the reliability of the IEEE-796 standard bus, see Preckshot 1993c. In the balance of this document, unless otherwise stated, "subsystem" is used in the (vendor's) sense to identify an IEEE-796 bus system.

#### *Blocks that are independent*

The standard for independence between two subsystems as defined above is that they must differ significantly in parameters, dynamics, and logic. If two such subsystems perform similar functions but have differing inputs (different parameters being sensed) combined by different logic, it is assumed that the two subsystems do not have a common failure mode. This assumption is reasonable since it is

implicit that the programs being run will differ in timing and logic because of the differing inputs and processing code.

#### *Blocks that are identical*

In contrast, IEEE-796 subsystems with the same functions, hardware, and similar inputs (as exist in functionally identical subsystems in separate protection system divisions) are assumed to have common failure modes due to potential replicated software errors. These subsystems are substantially the same in parameters, dynamics, and logic. Such failures need not occur at identical times, but merely close enough that surveillance is evaded. (This assumption implies common-mode failures in the RT groups, ESF groups, Engineered Safety Features Actuation Subsystems (ESFAS), PLCs, Trip Enable, or Global Trip subsystems of each division; failure of the ESFAS would disable automatic initiation of ESF equipment, while still allowing manual initiations; a PLC failure would disable automatic and manual initiation of all ESF equipment; failure of the Trip Enable Subsystem would incapacitate automatic partial reactor trips from the Reactor Trip Subsystems, but Global Trips and manual trips would still be available; a common mode failure of the Global Trip subsystems prevents any automatic reactor trip, while still allowing manual trip.)

#### *Effect of the operating system*

The operating system, which is common to all IEEE-796 subsystems in this design, will not be included as a source of common-mode software failures. It is assumed that the operating system as described by (the vendor) is simple enough<sup>11</sup> that failures are related to service demands and that service demands are distributed differently enough in subsystems defined as dissimilar in section 3.6.3.2 to exclude the operating system as a separate cause of common-mode failure. Consequently, any common-mode operating system failures are subsumed by section 3.6.3.3. This assumption is not valid if (the vendor) uses a complex, multitasking operating system or uses more than a simple clock-updating timer interrupt.

<sup>11</sup> See Preckshot 1993b for a discussion of complexity.

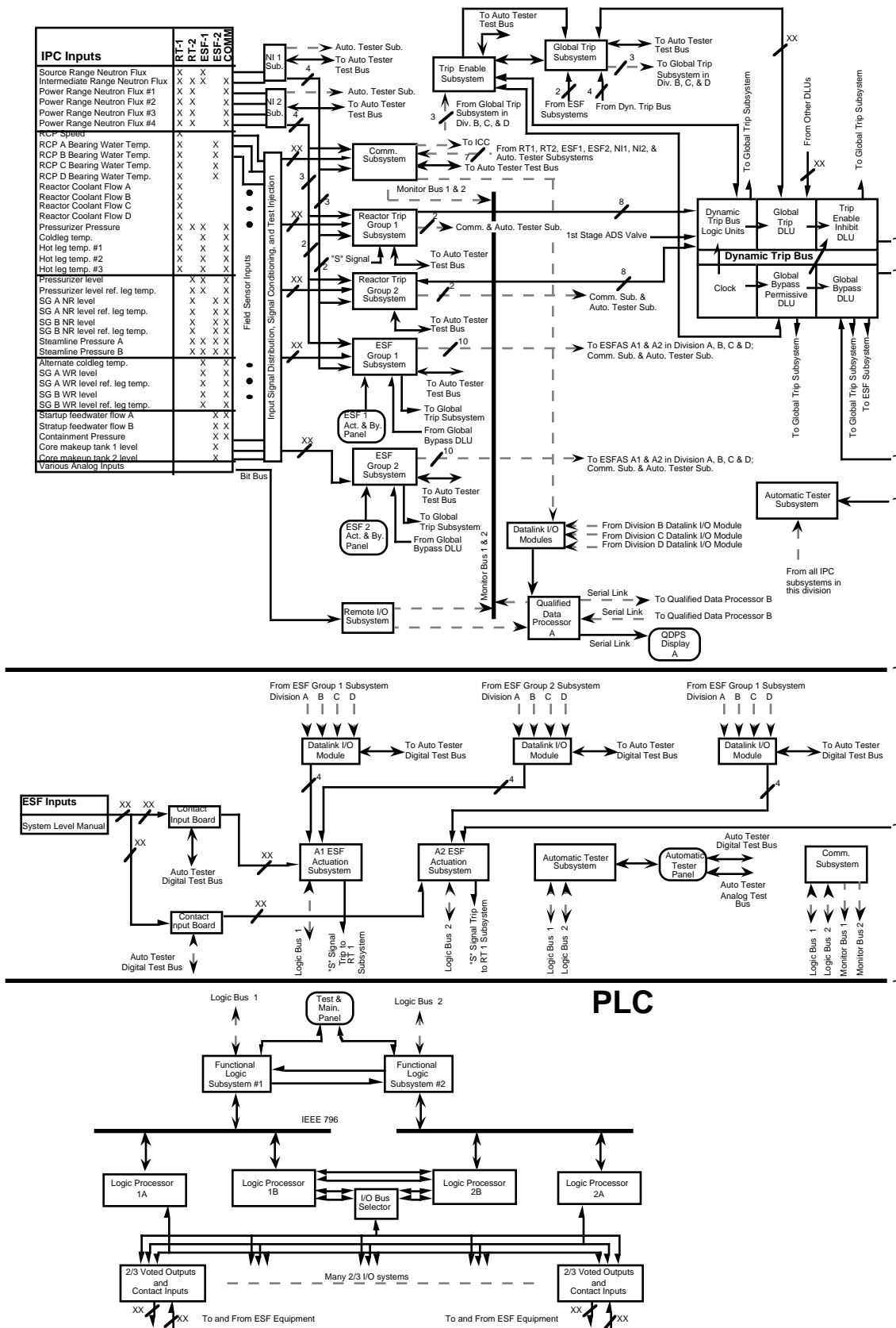


Figure A-2. Sample PWR System Block Diagram

# IPC

