PDR
Adu-Copy

RECEIVED

'99 DEC 23 A10:27

PUBLIC DOCUMENT ROOM

A Structured Approach for Review of Digital Plant Protection System Requirements Specifications*

Volume 2

June 15, 1999

Ray Berg — Sandia National Laboratories

Gary Johnson — Lawrence Livermore National Laboratory

Robert W. Brill -- Nuclear Regulatory Commission

*This work was supported by the United States Department of Energy under Contract DE-AC04-94AL85000. Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy.

Table of Contents

List of Figures iv

List of Tables v

Acronyms vii

1. Background 1

2. Goals, Purpose and Scope 3

3. Approach 4
   - 3.1 Overview 4
   - 3.2 Steps Comprising the Structured Approach 8
     - 3.2.1 Functional Requirements 8
     - 3.2.2 Integrity Requirements 9

4. Use of the Tables in Review 11

5. Implementation 12
   - 5.1 Identify PIE Characteristics and Protection System Functional Requirements 12
     - 5.1.1 Identify PIE Characteristics 13
     - 5.1.2 Identify Protection System Functional Requirements 14
   - 5.2 Identify Protection System Function Assignments 15
   - 5.3 Identify Component Functional Requirements 16
   - 5.4 Functional Requirements Reviews 19
     - 5.4.1 Specification Requirements Review 19
     - 5.4.2 Design Basis Requirements Review 20
   - 5.5 Identify Protection System Integrity Requirements 21
   - 5.6 Allocation of Integrity Hazards 25
   - 5.7 Compile Component Integrity Requirements 27
   - 5.8 Integrity Requirements Reviews 29
     - 5.8.1 Specification Requirements Review 29
     - 5.8.2 Design Basis Requirements Review 31

6. Conclusions 33

7. References 34
   - 7.1 Other Reading of Interest 35

Appendix A: Integrity Strategies 1

Appendix B: Examples of Table Developments from the Text 1

Appendix C: Example Library of Topics and Topic Taxonomy 1

Appendix D: Derivation of the Structured Approach 1

Appendix E: Identification of PIE Characteristics, Protection System Functional Requirements, and Protection System Functional Assignments 1

Glossary 1

List of Figures

FIGURE 1. STEPS 1–5 OF THE STRUCTURED APPROACH: REVIEWING THE FUNCTIONAL REQUIREMENTS FOR A CHOSEN COMPONENT OR SUBSYSTEM. 6
FIGURE 2. STEPS 6–9 OF THE STRUCTURED APPROACH: REVIEWING THE INTEGRITY REQUIREMENTS FOR A CHOSEN COMPONENT OR SUBSYSTEM. 7
FIGURE 3. STEPS 1 AND 2 OF THE STRUCTURED APPROACH. 12
FIGURE 4. STEP 3 OF THE STRUCTURED APPROACH. 15
FIGURE 5. STEP 4 OF THE STRUCTURED APPROACH. 17
FIGURE 6. STEP 5A OF THE STRUCTURED APPROACH. 19
FIGURE 7. STEP 5B OF THE STRUCTURED APPROACH. 20
FIGURE 8. STEP 6 OF THE STRUCTURED APPROACH. 22
FIGURE 9. STEP 7 OF THE STRUCTURED APPROACH. 26
FIGURE 10. STEP 8 OF THE STRUCTURED APPROACH. 28
FIGURE 11. STEP 9A OF THE STRUCTURED APPROACH. 30
FIGURE 12. STEP 9B OF THE STRUCTURED APPROACH. 31
FIGURE B1. VERTICAL RESPONSE SPECTRUM NUCLEAR ANNEX 50'. 14
FIGURE B2. HORIZONTAL RESPONSE SPECTRUM NUCLEAR ANNEX 50'. 15

List of Tables

TABLE 1. TEMPLATE FOR COLLECTION OF THE CHARACTERISTICS OF EACH PIE (LEVEL 1). 14
TABLE 2. TEMPLATE FOR COLLECTION OF EACH OF THE LIMITING PROTECTION SYSTEM FUNCTIONAL REQUIREMENTS (LEVEL 2). 15
TABLE 3. TEMPLATE FOR COLLECTION OF EACH OF THE PROTECTION SYSTEMS SUBSYSTEM AND FUNCTION ASSIGNMENTS (LEVEL 3). 16
TABLE 4. TEMPLATE FOR COLLECTION OF FUNCTIONAL REQUIREMENTS FOR EACH COMPONENT (LEVEL 4). 18
TABLE 5A. TEMPLATE FOR REVIEW OF SPECIFICATION FUNCTIONAL REQUIREMENTS (LEVEL 5A).20
TABLE 5B. TEMPLATE FOR REVIEW OF DESIGN BASIS FUNCTIONAL REQUIREMENTS (LEVEL 5B).21
TABLE 6A. TEMPLATE FOR COLLECTION OF THE CHARACTERISTICS OF INTEGRITY HAZARDS FOR EACH SYSTEM FAILURE (LEVEL 6A). 23
TABLE 6B. TEMPLATE FOR COLLECTION OF EACH NORMAL (AMBIENT) AND ACCIDENT ENVIRONMENTAL INTEGRITY HAZARDS (LEVEL 6B). 24
TABLE 6C. TEMPLATE FOR COLLECTION OF CHARACTERISTICS OF EACH PROCESS ENVIRONMENTAL INTEGRITY HAZARD (LEVEL 6C). 24
TABLE 6D. TEMPLATE FOR COLLECTION OF CHARACTERISTICS OF EACH INTEGRITY HAZARD FROM POWER SOURCES (LEVEL 6D). 25
TABLE 7. TEMPLATE FOR COLLECTION OF EACH OF THE PROTECTION SYSTEM'S INTEGRITY HAZARD ALLOCATIONS (LEVEL 7). 27
TABLE 8. TEMPLATE FOR COLLECTION OF CHARACTERISTICS OF EACH INTEGRITY MITIGATION AND DEFENSE REQUIREMENT (LEVEL 8). 29
TABLE 9A. TEMPLATE FOR REVIEW OF INTEGRITY REQUIREMENTS (LEVEL 9A). 31
TABLE 9B. TEMPLATE FOR REVIEW OF DESIGN BASIS INTEGRITY REQUIREMENTS (LEVEL 9B). 32
TABLE A1A. EXAMPLES OF DIGITAL PROTECTION SYSTEM INTEGRITY ACES. 1
TABLE A1B. EXAMPLES OF DIGITAL PROTECTION SYSTEM PROCESS DEVELOPMENT HAZARD SOURCES. 2
TABLE A2. PART OF A GENERAL INTEGRITY MITIGATION AND DEFENSE STRATEGY TAXONOMY. 2
TABLE A3. A DIVERSITY INTEGRITY MITIGATION AND DEFENSE STRATEGY TAXONOMY (FROM NUREG/CR-6303). 3
TABLE B1A. EXAMPLE OF DATA COLLECTION FOR PIE CHARACTERISTICS. 2
TABLE B1B. EXAMPLE OF DATA COLLECTION FOR PIE CHARACTERISTICS. 3
TABLE B2. EXAMPLE OF DATA COLLECTION OF LIMITING PROTECTION SYSTEM FUNCTIONAL REQUIREMENTS. 5
TABLE B3. EXAMPLE OF DATA COLLECTION FOR THE PROTECTION SYSTEM'S SUBSYSTEM AND FUNCTION ASSIGNMENTS. 6
TABLE B4. EXAMPLE OF DATA COLLECTION FOR THE PROTECTION SYSTEM MITIGATION AND DEFENSE FUNCTIONS. 8
TABLE B5A. EXAMPLE OF REVIEW OF SPECIFICATION FUNCTIONAL REQUIREMENTS. 11
TABLE B5B. EXAMPLE OF REVIEW OF DESIGN BASIS FUNCTIONAL REQUIREMENTS. 11
TABLE B6A. EXAMPLE OF DATA COLLECTION OF THE CHARACTERISTICS OF INTEGRITY HAZARDS FOR EACH SYSTEM FAILURE. 12
TABLE B6B. EXAMPLE OF DATA COLLECTION FOR NORMAL (AMBIENT) AND ACCIDENT ENVIRONMENTAL HAZARDS. 13
TABLE B6C. EXAMPLE OF DATA COLLECTION OF CHARACTERISTICS FOR PROCESS ENVIRONMENTAL INTEGRITY HAZARDS. 15
TABLE B6D. EXAMPLE OF DATA COLLECTION OF CHARACTERISTICS INTEGRITY HAZARDS FROM POWER SOURCES. 16
TABLE B7. EXAMPLE OF DATA COLLECTION OF THE PROTECTION SYSTEM'S INTEGRITY HAZARD ALLOCATIONS. 18
TABLE B8. EXAMPLE OF DATA COLLECTION OF CHARACTERISTICS OF INTEGRITY MITIGATION AND DEFENSE REQUIREMENTS. 21

TABLE B9A. EXAMPLE OF REVIEW OF SPECIFICATION INTEGRITY REQUIREMENTS. 32
TABLE B9B. EXAMPLE OF REVIEW OF DESIGN BASIS INTEGRITY REQUIREMENTS. 34
TABLE D1. GENERAL MEANS-ENDS ABSTRACTION HIERARCHY AND ITS COMPONENTS 1
TABLE D2. DOMAIN DEFINITIONS FOR THE RASMUSSEN'S MEANS-ENDS ABSTRACTION HIERARCHY APPLIED TO NUCLEAR POWER REACTORS. 3
TABLE D3. WHOLE PARTS DECOMPOSITIONS FOR THE DOMAIN DEFINITIONS OF TABLE D2. 4
TABLE D4. RASMUSSEN'S MEANS-ENDS ABSTRACTION HIERARCHY APPLIED TO NUCLEAR POWER REACTOR REGULATORY PROCESSES. 6
TABLE E1. ALLOCATION OF PROTECTIVE FUNCTIONS TO PIES AND TO SYSTEMS 5
TABLE E2. EXAMPLE OF A PIE CHARACTERISTIC 6
TABLE E3. LIMITING SYSTEM FUNCTIONAL CHARACTERISTICS 7

Acronyms

ACE	Abnormal Conditions and Events
ALWR	Advanced Light Water Reactor
ANS	American Nuclear Society
ANSI	American National Standards Institute
ATWS	anticipated transient without scram
BTP	Branch Technical Position
BWR	boiling water reactor
CFR	Code of Federal Regulations
CMF	common-mode failure
CSF	Critical Safety Function
DAC	design acceptance criteria
EFW	Emergency Feed Water
EMI	Electromagnetic Interference
EPRI	Electric Power Research Institute
ESD	electrostatic discharge
ESFAS	Engineered Safety Features Actuation System
FSAR	Final Safety Analysis Report
GDC	General Design Criteria
HEP	human error probability
I&C	Instrumentation and Control
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IPE	Individual plant examination
LBD	Licensing Basis Documents
LDBE	limiting design basis event
LER	licensee event report
LOOP	Loss of Offsite Power
MAHWD	means-ends abstraction hierarchy with whole-parts decomposition
MTBF	mean time between failures
MTTF	mean time to failure
NAS	National Academy of Sciences
NIST	National Institute of Standards and Technology
NRC	United States Nuclear Regulatory Commission
NRR	(NRC) Office of Nuclear Reactor Regulation
PDH	Process Development Hazard
PIE	Probable Initiating Event
PRA	probabilistic risk assessment
PWR	Pressurized Water Reactor
RES	(NRC) Office of Nuclear Regulatory Research
RFI	Radio Frequency Interference
RPS	Reactor Protection System
RTP	Rated Thermal Power
RTS	reactor trip system

SAR	Safety Analysis Report
SRP	Standard Review Plan
USQ	unreviewed safety question
V&V	verification and validation

A Structured Approach for Review of Digital Plant Protection System Requirements Specifications

1. Background

Instrumentation and control (I&C) systems provide monitoring, control, and protection functions in nuclear power plants. Until recently, most I&C systems have used analog devices. Analog I&C systems have served the nuclear industry well primarily because they are inherently more tractable with respect to their analysis and testing for safety, security, control and reliability. However, analog systems are becoming obsolete and their maintenance costs are increasing, so nuclear utilities are upgrading to digital systems [EPRI TR-106439, 1996 and NAS, 1997]. Digital systems offer several advantages over existing analog systems [NAS, 1997; NUREG-0800, 1997; and NUREG/CR-6323, 1995]. For example, digital systems are essentially free of the drifts associated with analog systems, so they maintain their calibration better. They have higher data handling and storage capabilities, so operating conditions can be more fully monitored and displayed. Digital systems provide improved system performance in terms of accuracy and computational capabilities such as fault tolerance and self-checking.

In the review of such systems NRC must address several new review considerations such as sampling effects, cycle times, discreteness of monitored parameters, and computer software quality. Studies indicate that the majority of all software errors are caused by incorrect or incomplete requirements [Leveson, 1995 and NUREG/CR-6323, 1995]. Frequently the cause of software requirements errors can be traced to incomplete or incorrect system requirements. Therefore, methods that help reviewers confirm that safety requirements are addressed in digital system requirements and software requirements can make an important contribution to improving the quality and consistency of reviews.

In the design and review of any complex safety-related system, it is vitally important to specify, clearly and accurately, the fundamental functions that the system is supposed to accomplish. These high-level requirements must be traceable from the system level, through subsystem layers, to the individual component that performs the function. If this is not done, serious undetected errors can creep into a system design, and the system may fail at a crucial moment.

Requirements errors are a major source of problems in designing and testing a system. Making sure that functional and integrity requirements are identified and tracked throughout a system is a difficult challenge, but one that must be faced if the system is to perform as intended. If errors are made in system requirements specifications, the entire basis for verification and validation of the system is compromised, and it is nearly impossible to ensure that the system is robust and reliable under all credible conditions.

The NRC's Standard Review Plan (SRP) for nuclear power plants points out the generally agreed-upon need to review requirements at various levels and to review acceptance criteria for

these reviews, but the question is, how is compliance with these acceptance criteria determined? This project describes a structured approach for extracting digital I&C safety requirements from plant licensing basis documents including technical specifications, the final safety analysis report (FSAR) and supporting safety and system analysis documentation. A structured approach can aid in confirming that these requirements have been adequately addressed in specifications for protection systems, subsystems, and components. By using the approach described below, reviewers can develop of matrix of tables that allow functional and integrity requirements to be traced from the plant requirements system to the I&C component level.

The advantage to this approach is that most of the information required to identify the functional and integrity requirements already exists as part of licensees' licensing basis documents (LBDs). These safety analyses exist as part of the licensing basis for existing plants, and are produced as part of the licensing process for new plants. Therefore, the structured approach is useful for reviewing both digital I&C retrofits to existing plants and digital I&C designs for new plants. This approach could also be used during the design phase to generate requirements, rather than trace them after the fact, but that is beyond the scope of this document.

2. Goals, Purpose and Scope

The goal of this document is to provide a method to aid NRC reviewers in confirming that the requirements specified by the licensee are consistent and complete, compared to the ones that are required by the LBDs. Using the structured approach described below, reviewers can identify the applicable safety-critical requirements by conducting a methodical review of plant licensing basis documentation. The requirements identified during the analyses will comprise a substantial part of the basis for evaluating digital I&C system requirements specifications during audits of licensees and applicants. Using the structured approach will help to confirm that the reactor system safety bases have been appropriately addressed in digital instrumentation and control system requirements.

The purpose of this document is to provide an overall description and examples of the application of this structured approach to protection system reviews.

While the structured approach is generally applicable to any I&C system important to safety, the scope of this document is limited to protection systems. Appendix B develops one example of the structured approach using the CE 80+ PWR system for illustrative purposes.

3. Approach

Volume 1 provides a general description of the structured approach and information that reviewers need to implement the methodology. This document (Volume 2) provides supporting information that will be used in a review, provides additional background information (e.g., definitions) that may aid in understanding the methodology described here, and describes the derivation and origins of the structured approach.

The structured approach produces a list of requirements that should be contained in the system requirements specification for each component reviewed. These expected requirements enable reviewer insights and judgments regarding the completeness and consistency of requirements documents, including questions to be asked and issues to be resolved. By comparing the requirements to the actual component specifications, NRC reviewers can spot weaknesses or inaccuracies in system design and specification.

To simplify the process of identifying requirements, the structured approach separately considers functional and integrity requirements. Figures 1 and 2 show a detailed breakdown of the steps comprising the structured approach.

The origin and development of the structured approach is discussed in Appendix D, titled "Derivation of the Structured Approach".

3.1 Overview

Expected requirements are derived from the safety and system analyses by completing two sets of linked tables. Following the nine steps of the process described below generates these tables. Each step uses specific information from the existing safety analyses and/or is derived from the previous steps. The information at each step, or level, is collected into one or more tables. One set of tables (generated in steps 1–5) defines the expected functional requirements, and compares them to system design bases and component requirements specifications. The second set of tables (generated in steps 6 through 9) defines the expected integrity requirements, and compares them to system design bases and component requirements specifications. There is some interaction between the first and second sets of tables, because the functional requirements must not cause an integrity hazard that cannot be addressed, and requirements introduced to address integrity hazards must be consistent with the final functional requirements. In some cases specific functional requirements may be modified to allow the use of desired integrity strategies. Data from a later step may therefore be used to reexamine results from an earlier step. Figures 1 and 2 illustrate how this methodology works together with the accident and system analyses to establish requirements traceability.

The number of tables required at each level may vary, depending on the extent of the review. For example, at level 1, a separate table is generated for each potential initiating event (PIE) under review. At levels 2 and 3, a table is generated for each protection system function under review. At levels 4 and 5, there is one table for each component selected for review. At level 6 there is one table for each component and one table for each function selected for review, and so

on. At each succeeding level, the reviewer extracts information from the previous table(s) and inputs additional data as required. This process may be simplified by using software that is designed to link table entries automatically, such as QuatroPro or Access, so large amounts of information do not have to be copied from table to table.

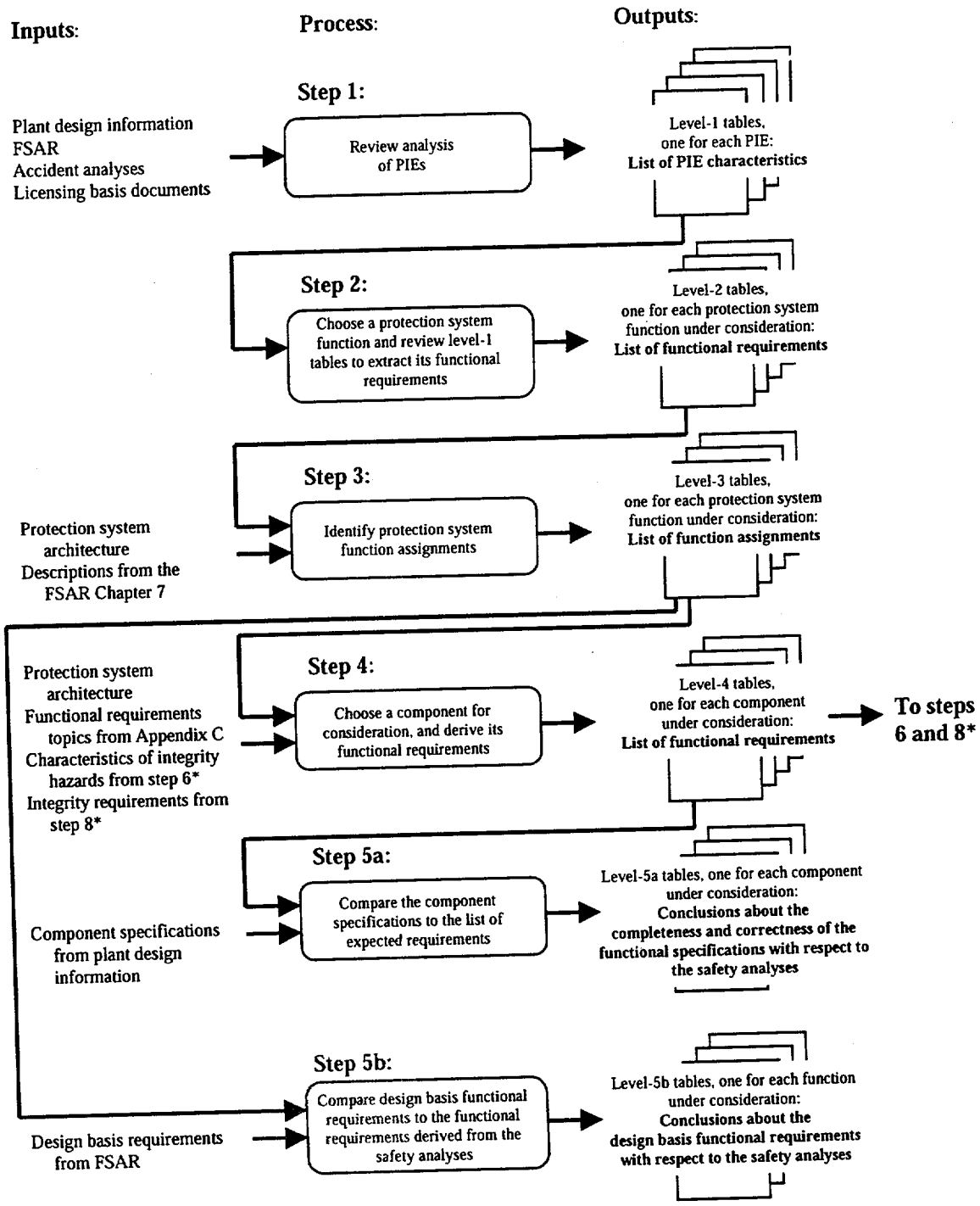
This structured approach provides a forward traceability from fundamental hazards to functional and integrity requirements for protection systems. Plant design assumptions and analyses, primarily those summarized in Chapter 15 of the Final Safety Analysis Reports (FSAR), identify the high-level functional requirements (both the functions to be performed and the performance required of those functions) necessary to ensure the integrity of the reactor coolant pressure boundary, to ensure the capability to shut down the reactor and maintain it in a safe shutdown condition, and to prevent or mitigate the consequences of accidents.

By constructing the first five levels of tables (outlined in Figure 1), the reviewer may extract fundamental requirements from the outputs and assumptions of the accident analyses and review the functional requirements for specific protection system components. Similarly, the reviewer may use existing descriptions and analyses of plant environments and systems and structures to extract integrity requirements and review design bases and component specifications, by following the steps to generate the level-6 through level-9 set of tables. (This process is outlined in Figure 2.) General Design Criteria 1, 2, 3, 4, 21, 22, 23, 24, and 29 of 10 CFR 50 specify the high-level integrity requirements that protection systems must meet.

As an aid in identifying requirements that are important for a particular component, a series of requirements specification "topics" define the information required for the component's requirements specifications. Appendix C of this report provides a catalog of example mitigation and defense requirements specification topics that are typically important for the sense, command, and execute features of protection systems. This catalog is intended to be updated as new insights are gained from requirements reviews and new components are developed or integrated into I&C systems. As the structured approach is applied, users will identify additional areas of consideration, and these will be added to the catalog. (These topics may also be relevant to components of these features, but development of a more complete set of topics for these components is not included in this report.) Each definition includes:

1. Name of topic,
2. Definition of topic,
3. Attributes that should be specified for the topic,
4. Source or reference of the origin of specific requirements for the topic, and
5. Behavioral or functional characteristics that describe how the topic can be used.

Reviewers may use the results of this analysis to confirm that relevant subjects have been appropriately considered in the system requirements specification under consideration. For a given review a reviewer may need to develop additional topics. These should be added to the topic catalog to aid future reviewers.



*The functional requirements and integrity characteristics interact such that the functional requirements must not create an integrity hazard that cannot be addressed. The functional and integrity requirements must not be mutually exclusive.

Figure 1. Steps 1–5 of the structured approach: reviewing the functional requirements for a chosen component or subsystem.

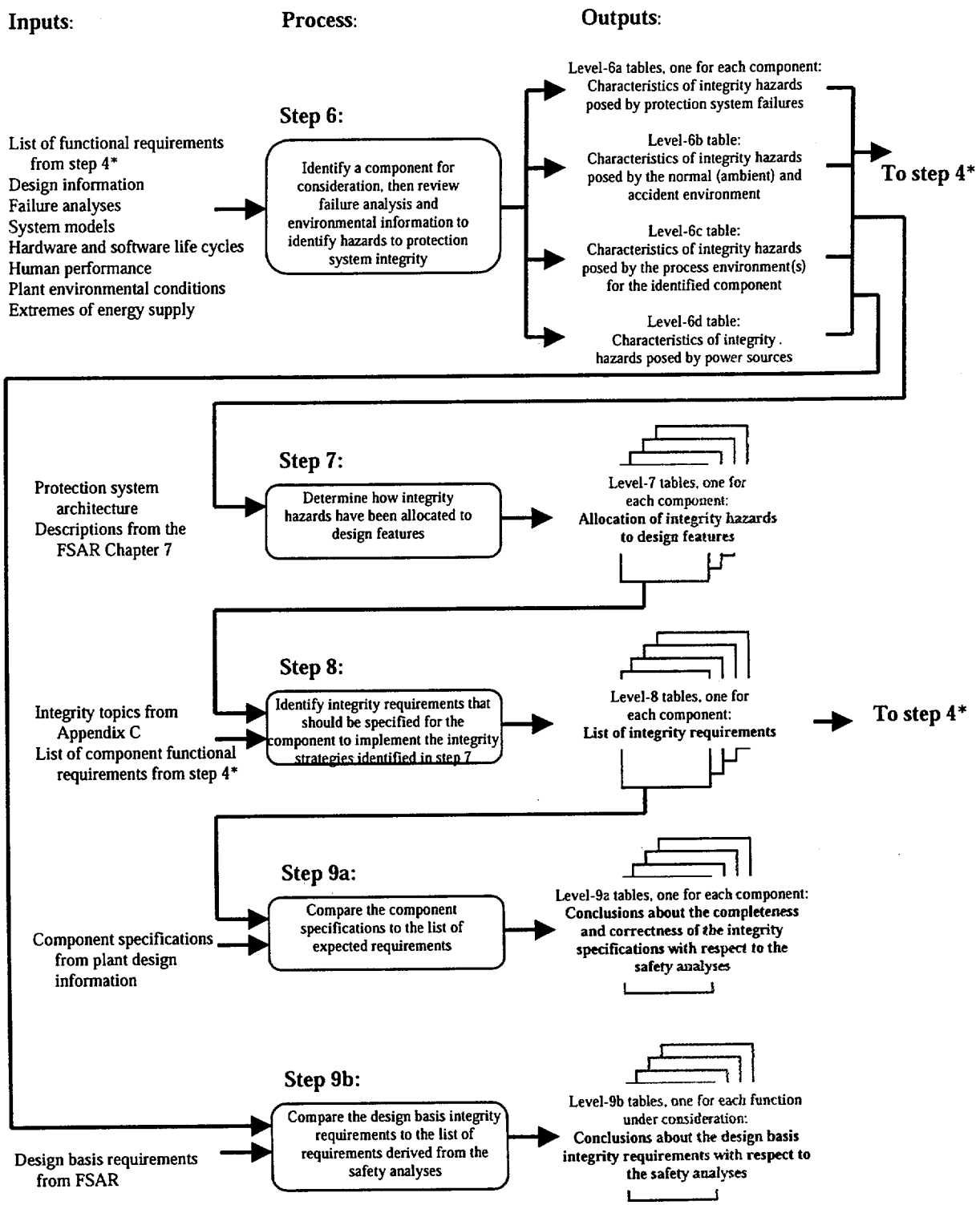


Figure 2. Steps 6–9 of the structured approach: reviewing the integrity requirements for a chosen component or subsystem.

3.2 Steps Comprising the Structured Approach

3.2.1 Functional Requirements

Step 1 of the structured approach begins with a review of accident analyses to identify protection system functional requirements (Section 5.1). This review extracts information about the protection system functions and performance assumed in the accident analysis, and the dynamic characteristics of plant parameters that establish requirements for the protection system's functions. Information is extracted for each PIE under consideration, and the result is a set of level-1 tables describing the limiting characteristics of each PIE. One table will be generated for each PIE under review.

Any given protection system function typically protects against more than one PIE, so a specific protection system function must be chosen for review, and the information collected in the level-1 tables must be summarized. Step 2 of the structured approach identifies the protection system requirements derived from the analyses of these PIEs. By analyzing the information collected in the level-1 tables, reviewers can extract the limiting cases that describe the protection system functional requirements for the specific protection system function (in the process creating the level-2 tables, one table for each protection system under review). For audit purposes, it is not necessary to review all PIEs in order to define completely the requirements for the protection system function under consideration.

Step 3 involves a review of the top-level protection system architecture to identify how the required functions, extracted from the above tables, are allocated to the protection system subsystems, e.g., reactor trip system and engineered safety feature actuation system (Section 5.2). The subsystem assignment information is then added to the level-2 table that describes the functional requirements for the protection system function under review, to produce a level-3 table. One level-3 table is generated for each protection system function under consideration, so there is a 1:1 correspondence with the level-2 tables.

In step 4, the functional requirements that were identified in steps 1 and 2, and knowledge about the protection system design, is used to develop expected requirements for any specific component that is being considered for review. The information in the level-3 table of functional requirements is used to create a new, level-4 table describing the functional requirements for particular protection system component(s) selected for review. These components may be implemented as hardware, software, or humans carrying out procedures. The functional requirements for any component are strongly dependent upon the component's role in the system architecture. Therefore, in carrying out this step it is important that the reviewer develop a good understanding of the system architecture and the component's role in that architecture in order to identify the functional requirements allocated to the component under consideration. The reviewer then uses the catalog of requirements topics to be provided in Appendix C to identify specific requirements that should be found in the specification for the component under consideration. The process for developing expected component requirements from requirements for the function under consideration is discussed in Section 5.3. Appendix B shows a derivation of a subset of expected requirements for a bistable trip processor in a typical digital protection system. This method can be used to derive expected requirements for any component (including hardware, software, or procedures) of the protection system. In all cases

the functional requirements identified by the analysis in steps 1–3 must be appropriately reflected in lower-level requirements. Any additional lower-level requirements introduced must also be consistent with the functional requirements.

Steps 5a and 5b are the actual component functional requirements reviews, after all of the pertinent information has been generated in steps 1 through 4 above. The list of expected requirements collected in the level-4 tables are evaluated against the actual specification for the component(s) under review (step 5a) to create a level-5a set of tables. If an expected functional requirement listed in the level-4 table is not addressed by the component specification, this is an indication that the specification is incomplete. Conversely, if all expected requirements are addressed by the specification, the review provides assurance that the functional requirements in the component specification are reasonably complete, although the process cannot guarantee completeness. In step 5b, the design basis requirements from the FSAR and the function assignments from the level-3 tables are similarly compared to the functional requirements derived from the safety analyses.

3.2.2 Integrity Requirements

Once the protection system design is known, hazards to the integrity of the protection system itself are identified by analyses of the systems and system failures that can threaten its integrity. The integrity hazards considered include both abnormal conditions and events (ACEs) (which include both plant excursions and natural-phenomena-related events) that must be handled on a real-time basis by the protection system, and process development hazards (PDHs) that must be anticipated in order to avoid introducing errors that could lead to hazards being incorporated in the final design. ACEs thus include hardware failures, software errors, human errors, and environmental hazards. The hazards posed by hardware, software, and human performance are identified so that specifications can be checked to confirm that they include design strategies and features that (1) minimize protection system failures, (2) ensure that the protection system design is robust, and (3) ensure that functional requirements are met when failures occur. These include, for example, requirements for quality, single-failure tolerance, diversity, testability, and independence. Environmental hazards are determined by the envelope of the environment within which the protection system must function under normal and abnormal conditions. This includes, for example, requirements for challenges to integrity derived from thermal (all sources), pressure, radiation, electromagnetic interference, power supply variations, seismic, and missile hazards.

Most integrity requirements are evaluated in a top-down fashion starting with PIEs analyzed in Chapter 15 of a Final Safety Analysis Report. This top-down approach enhances traceability and minimizes the potential for conflict. The most notable exceptions to a top-down approach are hazards to protection system integrity resulting from specific hardware and software design features, which, because they cannot be identified until the design is specified, must be handled iteratively.

In step 6 of the structured approach, the hazards to protection system integrity are determined by examining safety and system analyses. Information from this analysis is recorded in a set of level-6 tables that identify integrity hazards posed by hardware; software; system failures; normal, abnormal, and accident environments; process environments; and power supplies.

Step 7 involves a review of the top-level protection system architecture and FSAR to identify how the integrity hazard characteristics, extracted from the level-6 tables, are allocated to the protection system design features. This information is then added to the level-6 tables to produce level-7 tables. There is a 1:1 correspondence with the level-6 tables.

In step 8, the hazards to protection system integrity that were codified in the level-7 tables are used to develop level-8 tables that describe the integrity hazards that must be addressed by the particular protection system components selected for review. The reviewer's understanding of the system architecture and the component's role in that architecture is used to identify the hazards that must be addressed in the requirements for the component under consideration. The reviewer then uses the catalog of requirements topics provided in Appendix C to identify specific requirements topics that would address the identified integrity hazards. Section 5.6 describes this element of the structured approach. (Examples in the appendices show derivations of example integrity requirements topics.) All integrity requirements for a given design element must be appropriately reflected in lower-level requirements. In addition, any lower-level requirements introduced must be consistent with the integrity requirements. The structured approach provides a process for documenting the integrity requirements specified to address integrity hazards. It also facilitates checking to confirm that all integrity hazards have been appropriately addressed.

Steps 9a and 9b are the actual component integrity requirements reviews, after all of the pertinent information has been generated in steps 6 through 8 above. In step 9a, the list of expected requirements that were collected in the level-8 tables are evaluated against the actual specification for the component(s) under review. That information is collected into a level-9a set of tables. If an expected integrity requirement listed in a level-8 table is not addressed by the component specification, this is an indication that the specification is incomplete. Conversely, if all expected requirements are addressed by the specification, the review provides assurance that the integrity requirements in the component specification are reasonably complete, although the process cannot guarantee completeness. In step 9b, the design basis requirements from the FSAR and the characteristics of integrity hazards from the level-6 tables are similarly compared to the integrity requirements derived from the safety analyses.

The requirements identified in the level-5 tables and the level-9 tables (Sections 5.3 and 5.6) constitute the total requirements for the protection system component under consideration.

4. Use of the Tables in Review

The process described here may be used by NRC reviewers, field auditors, and inspectors in their reviews of digital protection systems. The data collection and development are guided by a set of interrelated tables, referred to in this document as levels 1-9 for clarity. The tables specify a form and format for collecting data from the FSAR and the supporting accident and system analyses.

By identifying areas of inconsistency, as well as incomplete or incorrect specifications, the tables can aid NRC reviewers in confirming that the requirements specified by the licensee are consistent and reasonably complete. However, the tables cannot guarantee completeness or correctness.

The templates in Section 5 for table levels 1 through 9, together with various libraries of data, can be used in the review of detailed design requirements to help confirm that high-level requirements have been propagated into the requirements for the specific systems, sub-systems, or components under review. The tables function as guides for collecting data in each step of the review process. A table is introduced to handle the data collection in each of the applicable steps of the process shown in Figures 1 and 2, and detailed in Section 5. By linking the tables, traceability of the requirements can be shown by following a direct path to the origin of each requirement of the protection system. Each requirement, whether functional or integrity, must result from such a trace through the tables. This process is best implemented in a form that allows for automatically linking tables rather than copying material from table to table (e.g., QuatroPro, Access).

The most likely use of the structured approach is to support a trace audit of requirements. In a trace audit, some subset of PIEs is examined to identify protection system functions for consideration. A subset of functional requirements is identified for these functions, and information about the protection system design is used to identify a specific component for consideration. System analysis information and the catalog of requirements topics provided in this report (Appendix C) can then be used to develop a list of expected requirements for the component under review. The system requirements specification for the component can then be evaluated against the expected requirements to confirm that the expected requirements extracted from the safety analyses are appropriately addressed. A trace audit such as this can find weaknesses in the licensee or applicant's system requirements specifications.

In practice, the starting point depends on the specific goals of the review. A review can be initiated over questions about handling of PIEs or questions about a protection function. In the latter cased, the activities in steps 1 to 3 might be repeated in order to assure that all PIEs associated with the chosen protection function have been identified. A more detailed example of how the Structured Approach might be used in such a review of PIEs and identification of functional and performance requirements is discussed in Appendix E.

5. Implementation

The structured approach described here involves nine general steps, as shown in Figures 1 and 2. The process is iterative, and may involve returning to earlier steps depending on the results. The steps are discussed in Sections 5.1 through 5.8. For clarity of discussion the descriptions below assume that a single function and single component are selected for consideration. References are given throughout to examples in Appendix B. The examples have been collected into an appendix for better readability.

5.1 Identify PIE Characteristics and Protection System Functional Requirements

The purpose of this analysis is to identify the potential initiating events (PIEs) and PIE characteristics that establish the functional and performance requirements for the protection system. The result serves as a knowledge base for evaluating digital protection systems designed to mitigate the PIEs. The inputs, processes, and outputs of these steps are shown in Figure 3.

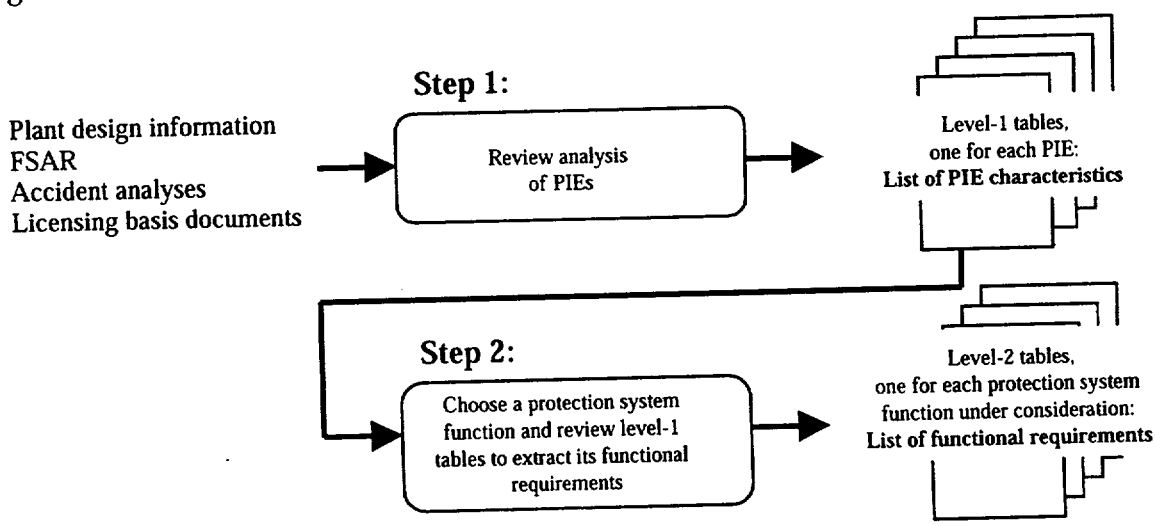


Figure 3. Steps 1 and 2 of the structured approach.

Inputs: The inputs to this section consist of the following information:

- Plant design information,
- FSAR,
- Accident analyses, and
- Supporting licensing basis documents.

Process: The process in this section is to review the analyses of PIEs to identify protection system functions and performance assumed in the accident analyses, as well as the plant parameter characteristics that must be accounted for in the protection system's

design. Next, the reviewer chooses a protection system function to examine. Normally any given protection system function is credited with responding to several PIEs. The performance requirements for any given function must, therefore, encompass the requirements associated with every PIE for which the function is responsible. The characteristics of all PIEs examined are then reviewed to determine the limiting cases that must be met in the design of the protection system function. The limiting cases are the most extreme values of the functions, performance, or parameter characteristics over all of the PIEs considered.

Outputs: The outputs from this section consist of the following information:

- One or more level-1 tables identifying the characteristics of PIEs under consideration in the review (those characteristics that may impose requirements on the protection system, and,
- One or more level-2 tables describing the required functions and performance of the protection system function(s) selected for consideration.

Discussion This process was exercised using Amendment 31 of the ABWR Standard Safety Analysis Report as the principle input. Since this project was intended to generate requirements for all protection system functions, it was necessary to have a complete list of protection system functions to make sure that we did not inadvertently overlook defining requirements for any function. Therefore, there was an interaction between this step and the identification of protection system functional assignments discussed in section 5.2. The results of that analysis were fed back into this step to ensure that each protection system function was considered. The example is discussed in Appendix E

5.1.1 Identify PIE Characteristics

Table 1 shows a template for collecting data on the characteristics of an individual PIE. The required information is typically available in Chapters 6 and 15 of the FSAR, LBDs, and other supporting detailed material. Examples of data collected for PIE characteristics are shown in Tables B1a and B1b.

Table 1. Template for collection of the characteristics of each PIE (Level 1).

Entry	Explanation
PIE name	Name of the event analysis being considered
Initial conditions	Values of all pertinent parameters prior to the PIE occurrence
Protective function	The protection function assumed by the accident analysis
Related CSFs	The critical safety functions related to the function
Parameter	The trip parameters assumed for the function
Parameter characteristics	For the particular PIE being considered
Time delay	The protection system time delay assumed in the accident analysis
Variable range	The maximum and minimum values of the parameters calculated by the analysis
Associated parameters	List of any other related parameters
Maximum rate of change	Maximum slope of the measured parameters
Analytical limit	The safety function actuation value assumed in the analysis
Frequency spectrum	Frequency spectra with important information about the parameter's behavior

5.1.2 Identify Protection System Functional Requirements

The reviewer may select one or more PIEs for consideration during a review. The reviewer completes a level-1 table for each PIE to be considered. If more than one PIE is considered, the requirements specific to the protection system function under review must be summarized into a set of limiting requirements specific to that function. Table 2 shows a template for reducing the data from the level-1 tables to describe the limiting requirements for a specific function. The differences from the level-1 tables are identified in each entry's explanation. An example of how the limiting requirements are derived is given in Table B2 and the discussion accompanying it.

Table 2. Template for collection of each of the limiting protection system functional requirements (Level 2).

Entry	Explanation
Protective function	The protection system function under consideration
PIE name	The name of the event and conditions that pose the bounding conditions (Note: this might be different for different characteristics)
Initial conditions	Values of all pertinent parameters prior to the PIE occurrence
Related CSFs	The critical safety functions related to the function
Parameter	The trip parameters assumed for the function
Parameter characteristics	Over all PIEs considered
Response time	The minimum protection system time delay assumed in the accident analysis
Parameter range	Maximum and minimum values of the parameters over the extremes of normal and accident conditions
Maximum rate of change	Maximum slope of the measured parameters
Analytical limit	The limiting safety function actuation value assumed in the analysis
Frequency spectrum	The composite of the frequency spectra
Associated parameters	List of any other related parameters

5.2 Identify Protection System Function Assignments

The purpose of this analysis is to identify the digital protection elements (i.e., naming and describing their protection functions) that handle each PIE cataloged in the previous section. The inputs, processes, and outputs of this steps are shown in Figure 4, and described in detail below.

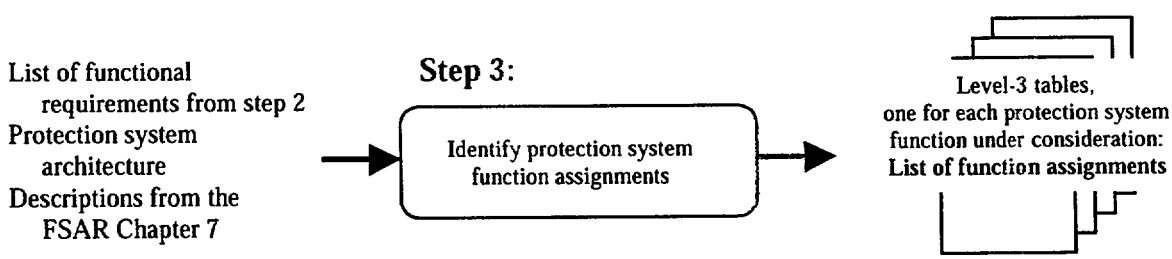


Figure 4. Step 3 of the structured approach.

Inputs: The inputs to this identification process include:

- The level-2 tables of functional requirements from step 2 (Section 5.1), and
- The protection system architecture or hierarchy (i.e., identification of protection systems subsystems and elements, and how they are interconnected) and,

- Descriptions from the FSAR Chapter 7.

Process: The process in this section is to examine the protection function allocations to ensure that the protection system function under consideration is handled by at least one of the defined protection systems. Definitions of the protection subsystems could be based on the traditional protection systems discussed in Section 7 or on novel concepts. Traditional protection subsystems include:

- The reactor protection system (RPS), and
- The engineered safety features actuation system (ESFAS).

Outputs: The outputs of this process include the following:

- Identification of the subsystem(s) assigned responsibility for the protection system function under consideration. This information is appended to the level-2 table of functional requirements to produce a level-3 table.

Table 3 shows a template for data collection on the protection subsystems and their responsibilities for protection functions. The data in Table 3 are derived from protection system architectural descriptions contained in FSAR Chapter 7 or supporting design documents, and Table 2 for the function(s) under consideration. The information in the shaded area of the table is carried over from Table 2. An example of the identification of functional assignments is shown in Table B3.

Table 3. Template for collection of each of the protection systems subsystem and function assignments (Level 3).

Entry	Explanation
System or subsystem	Name of the system or subsystem responsible for the protective function being considered
Protective function	Functional requirements from Table 2, Section 5.1, appended based on the key field "Protective Function" (may include several limiting PIEs and their respective limiting characteristics.)

5.3 Identify Component Functional Requirements

The purpose of this analysis is to identify protection system mitigation and defense requirements that should addressed in the specifications of digital components. These specifications are not typically in the FSAR, but in the plant design documentation for a given protection system component. For the purposes of this discussion a component can be any protection system design element (e.g., system, subsystem, module, or part) which has a separable function and for which requirements can be sensibly developed. A component might be composed of hardware, software, or procedures, or an integrated combination of these three. Specifications must describe requirements for all topics important to the component's mitigation and defense function.

The bases for the analysis are functional requirements identified previously, and the protection system architecture, as defined in the previous section. The inputs, processes, and outputs of this step are shown in Figure 5, and are described in detail below.

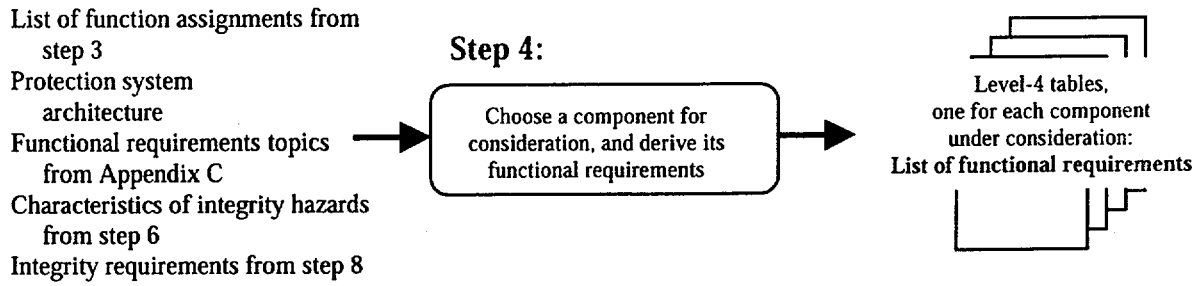


Figure 5. Step 4 of the structured approach.

Inputs: The inputs to this analysis are:

- The level-3 tables of protection system function assignments and their requirements from step 3 (Section 5.2),
- The protection system and subsystem architectures, and an understanding of the component's role within the system, and
- Functional requirements topics from Appendix C.

After integrity requirements are identified, the following are inputs to later iterations of the functional requirements:

- The characteristics of integrity hazards from step 6 (Section 5.5), and
- Integrity requirements from step 8 (Section 5.7).

Process: The process in this section is to review the protection system functional requirements to identify the areas that must be addressed in the system requirements specification for the chosen component. Topics that must be contained in the component specification are identified using the catalog given in Appendix C.

Because the functional and integrity requirements of the protection system interact (i.e., the functional requirements must not cause an integrity hazard that cannot be addressed), the characteristics of integrity hazards from step 6 and the integrity requirements from step 8 need to be considered after these requirements are developed. Note that steps 1–5 and 6–9 cover two series of relatively independent reviews, so the processes for reviewing the functional and integrity requirements can be undertaken concurrently.

Outputs: The outputs from this process are:

- Expected functional requirements for the component under consideration, in the form of a level-4 table.

Table 4 shows a template for data collection on the component expected functional requirements. The outputs of the analysis are functional requirements that must be addressed in the specifications for the component under consideration. Appendix C provides examples of the development of these topics and templates for functional requirements specifications for typical component sense, command, and execute features. Note that for a given component, several topics may work together to address a given hazard characteristic.

The data for Table 4 are derived from:

- The protection system functional requirements developed in Sections 5.1 and 5.2,
- The protection system architectural descriptions and component descriptions contained in FSAR Chapter 7 or supporting design documents from plant documentation, mitigation and defense topics from Appendix C of this report, and
- Integrity hazard characteristics and requirements from Tables 6a to 6d and Table 8.

The information in the shaded area is carried over from other tables. Appendix C contains an (incomplete) taxonomy of system requirements specification topics. For a given review, the reviewer may need to develop additional topics beyond those provided in the Appendix. An example of data identifying protection system mitigation and defense functions of an ESFAS is shown in Table B4.

Table 4. Template for collection of Functional Requirements for Each Component (Level 4).

Entry	Explanation
System or subsystem	Name of the system or subsystem under consideration
Component	Name of the component under consideration
Protective function	**Protection system functional requirements from Table 3, Section 5.2, appended based on the key field "Protective function" (may include several limiting PIEs and their respective limiting characteristics.)**
Parameter characteristic	
Functional requirement	
Topic	Name of the functional requirement topic that must be included to address the source hazard characteristic(s)
Definition	Description of the topic's meaning, or definition of the topic
Attributes	Attributes of the topic that must be specified in order to address the topic
Topic characteristics	Description of how the topic should be used in the system requirements specification characteristics of the topic
Expected functional requirements	The specific requirement for this topic

5.4 Functional Requirements Reviews

5.4.1 Specification Requirements Review

This section describes a method for collecting and organizing information for the review recommended by SRP Appendices 7.1-B (item 2) and 7.1-C (item 5), which recommend that NRC's review of protection systems confirm that functional requirements have been appropriately allocated to the various system components. Appendix 7.1-C further recommends that the review confirm that the system design fulfills the system design basis requirements. Branch Technical Position 14 recommends that software requirements specifications should be reviewed for consistency with, and traceability to, system requirements.

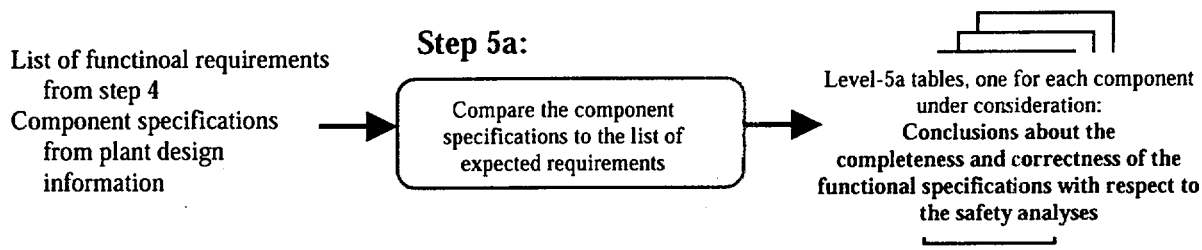


Figure 6. Step 5a of the structured approach.

Inputs: The inputs to this analysis are:

- The level-4 table identifying the functional requirements for the component under consideration from step 4 (Section 5.3), and
- Component specifications from plant design information.

Process: The list of expected functional requirements (level-4 tables) are evaluated against the specifications for the components under consideration (see Figure 1).

Specific requirements for each component are evaluated by correlating the protection system functional requirements with the characteristics of the related subsystems and components to identify the requirements applicable to the component being considered. The component's specification is then compared against the topics and related specific requirements to verify that all functional requirements derived from PIEs and assigned to the component under consideration are appropriately reflected in the system requirements specifications. If conflicts or omissions are found, questions are posed to the licensee or applicant. Another iteration through the process may be required to resolve review findings.

Outputs: The outputs from this process are:

- Conclusions about the completeness and correctness of the system requirements specifications, with respect to the safety analyses, in the form of a level-5a table.

Table 5a shows a template for comparison of component specifications to expected functional requirements. This enables development of conclusions about the completeness and correctness of the functional specification with respect to the requirements derived from the safety analyses. An example of data used for review of a specification functional requirement is shown in Table B5a

Table 5a. Template for review of specification functional requirements (Level 5a).

Entry	Explanation
Component	Name of the component under consideration
Expected component requirement	Functional requirement from Table 4
Source of expected component requirement	Table 4 row number
Actual component specification requirement	Corresponding component requirement from the component specification

5.4.2 Design Basis Requirements Review

This section describes a method for implementing the review recommended by Appendices 7.1-B (item 1) and 7.1-C (item 4) of the SRP. These recommend that review of protection systems include consideration of design basis: completeness with respect to the functions necessary to fulfill the system's safety intent, consistency with plant safety analyses, and traceability to the safety analysis.

The inputs, processes, and outputs of this step are shown in Figure 7, and are described in detail below.

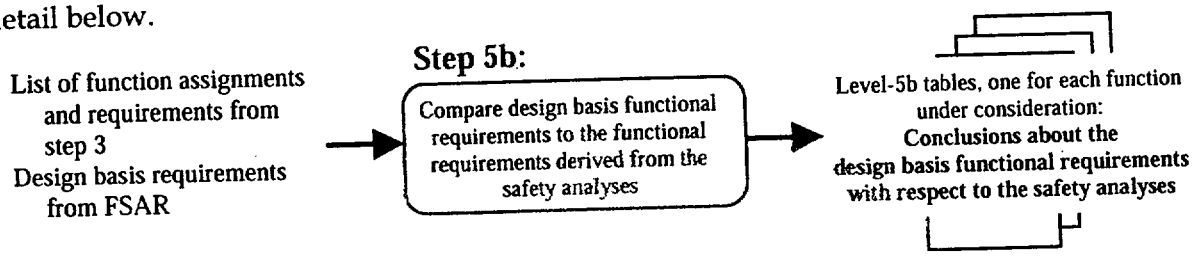


Figure 7. Step 5b of the structured approach.

Inputs: The inputs to this analysis are:

- The level-3 tables identifying the function assignments for the protection system under consideration from step 3 (Section 5.2), and
- Design basis requirements from the FSAR

Process: The list of function requirements and their assignments for the protection system under consideration (level-3 tables) are evaluated against the design basis requirements for each function under consideration (see Figure 1).

Specific requirements for each function are evaluated by comparing the design basis functional requirements from the FSAR to the functional requirements derived from the safety analyses. If conflicts or omissions are found, questions are posed to the licensee or applicant. Another iteration through the process may be required to resolve review findings.

Outputs: The outputs from this process are:

- Conclusions about the design basis functional requirements with respect to the safety analyses, in the form of a level-5b table.

Table 5b shows a template for conducting a review of expected design basis functional requirements for a given system or subsystem against the actual design basis functional requirements from the FSAR. Table B5b shows an example of the data developed for design basis functional requirements.

Table 5b. Template for review of design basis functional requirements (Level 5b).

Entry	Explanation
System or subsystem	Name of the system or subsystem responsible for the protective function being considered
Expected protection function requirement	Functional requirement of the Protective function from Table 3
Actual design basis requirement	Corresponding design basis functional requirement from the FSAR

5.5 Identify Protection System Integrity Requirements

The purpose of this analysis is to identify, analyze, and characterize hazards that threaten the integrity of the digital protection system being examined. This serves as a knowledge base for reviewing mitigation and defense strategies (e.g., functional diversity, redundancy, or environmental qualification) to protect the digital protection system itself against integrity hazards. The information utilized in this analysis is derived from the FSAR and supporting documentation, submittal information, and the licensee's records. The inputs, processes, and outputs of this step are shown in Figure 8, and are described in detail below.

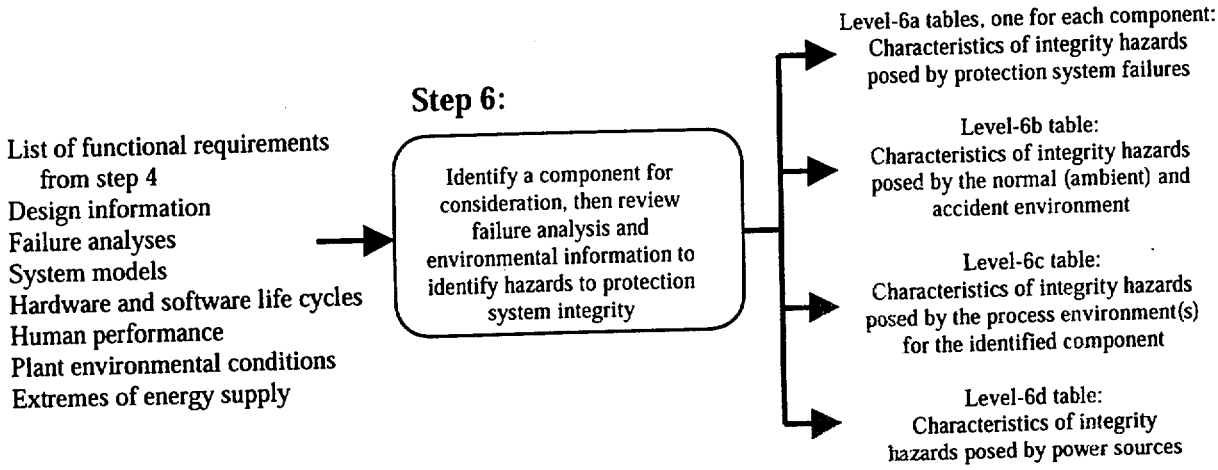


Figure 8. Step 6 of the structured approach.

Inputs: The inputs to this analysis consist of the following information:

- List of functional requirements from step 4 (Section 5.3),
- Design information,
- Failure analyses,
- System models,
- Hardware and software life cycles (e.g., requirements and design),
- Human performance (e.g., interaction with the human-machine interface),
- Plant environmental conditions (e.g., natural occurrences such as earthquakes, accident by-products such as radiation, and installed conditions), and
- Extremes of energy supply (e.g., power supply and power quality).

Process: The process in this section is to examine the analyses of the protection system designs, environments, and development processes to identify the characteristics of hazards that could threaten the integrity of the protection systems. Tables A1a and A1b in Appendix show high-level taxonomies of integrity hazards. The characteristics of environmental and energy source ACEs (of natural or mechanical origin) depend upon systems other than the protection system. The characteristics of these hazards are derived from analyses of these "external" systems whose normal operation or failure could create environments that pose an integrity hazard to the protection system.

The characteristics of hardware, software, human performance, and development process hazards depend upon the design of the protection system. The characteristics of these hazards are derived from analyses of the failures that can occur "internal" to the protection system and its development.

Outputs: The output from this section consists of the following information:

- A set of level-6 tables identifying the hazards to the integrity of the protection system and the characteristics of these hazards.

Tables 6a through 6d show templates for the collection of integrity hazards and their characteristics. Each table considers a different type of hazard. Examples of data collected for each of these tables are shown in Tables B6a through B6d

The data for Table 6a are derived from licensee or applicant failure and reliability analyses such as failure mode and effects analyses, reliability block diagrams, system fault trees, and human error analyses, or manufacturer-supplied testing and performance data. Examples of data collected for characteristics of the various integrity hazards are shown in Tables B6a through B6d.

Table 6a. Template for collection of the characteristics of integrity hazards for each system failure (Level 6a).

Entry	Explanation
System or subsystem	
Component	
Protective function	
Location	Plant location for which environment is specified (The location may describe an area or a specific point, for example, a specific mounting location and elevation may need to be described to specify the level of vibration seen by equipment mounted on process piping or equipment.)
Functional requirements	Information from Table 4 (Section 5.3)
Hardware and software events (failures)	
Failure mode	State of the failed system, subsystem, module, part
Failure type	Random or systematic
Failure effect	Result of the failure
Failure likelihood	Qualitative or quantitative probability of failure
Human errors	
Error	Description of the human error
Error type	Commission, omission, sequence, timing
Error effect	Result of the error
Error likelihood	Qualitative or quantitative probability of the error

The data for Tables 6b and 6c are derived from FSAR Chapter 3 and applicant or licensee's seismic and environmental qualification program descriptions, and from process descriptions in FSAR Chapters 4, 5, 6, 9, and 10.

Table 6b. Template for collection of each normal (ambient) and accident environmental integrity hazards (Level 6b).

Entry	Explanation
System or subsystem	
Component	
Protective function	
Location	Plant location for which environment is specified (The location may describe an area or a specific point, for example, a specific mounting location and elevation may need to be described to specify the level of vibration seen by equipment mounted on process piping or equipment.)

Normal (ambient) environments	Both normal and abnormal ambient environments need to be addressed
Tmax and Tmin	Temperature range
Pressure	Pressure range
Humidity	Range of Relative Humidity
Radiation	Radiation exposure type, spectrum, and dose
Fluid, chemical, or gas	Chemical exposure, composition, concentration, purging considerations
EMI and RFI	Electromagnetic and radio frequency interference
Vibration (non-seismic)	Horizontal and vertical vibration spectra
Accident environments	Natural or other phenomena
Temperature	Accident temperature time history
Pressure	Accident pressure time history
Humidity	Accident humidity environment
Fluid, chemical, or gas	Chemical and fluid exposure composition and concentration
Radiation	Type and dose rate, normally for both gamma and beta radiation
Flood	Flooding events by either accident or natural phenomena
Vibration (seismic)	Horizontal and vertical vibration spectra
Mechanical	Type and character of threats from, for example, missiles, pipe-whip, differential seismic motion, seismic II and I hazards
Fire	Smoke, heat and fire suppression chemicals

Table 6c. Template for collection of characteristics of each process environmental integrity hazard (Level 6c).

Entry	Explanation
System or subsystem	
Component	
Protective function	
Location	Plant location for which environment is specified (The location may describe an area or a specific point, for example, a specific mounting location and elevation may need to be described to specify the level of vibration seen by equipment mounted on process piping or equipment.)

Normal process environments	
Tmax and Tmin	Temperature range
Fluid, chemical, or gas	Chemical and fluid exposure, composition, and concentration, and purging considerations
Radiation	Type, spectrum, and dose
Pressure	Pressure range

The data for Table 6d are derived from power system descriptions in FSAR Chapter 8.

Table 6d. Template for collection of characteristics of each integrity hazard from power sources (Level 6d).

Entry	Explanation
System or subsystem	
Component	
Protective function	
Location	Plant location for which environment is specified (The location may describe an area or a specific point, for example, a specific mounting location and elevation may need to be described to specify the level of vibration seen by equipment mounted on process piping or equipment.)

Entry	Explanation
Power source	The power system or source for which the environment is specified (e.g., 125 VDC 1E system or battery backed inverter AC)
Electrical power source	
Vmax and Vmin	Voltage range
Frequency	frequency range or spectrum
Transients	Magnitude and duration
EMI	Conducted or radiated electromagnetic and radio frequency interference
Total harmonic distortion	Total harmonic distortion (with all loads connected and disconnected)
Air power sources	
Pmax and Pmin	Maximum and minimum pressure
Purity	Particulate, oil, and water content

5.6 Allocation of Integrity Hazards

The purpose of this analysis is to determine how integrity hazards have been allocated to the design features, using the characteristics of integrity hazards cataloged in the previous section. The inputs, processes, and outputs of this step are shown in Figure 9, and described in detail below.

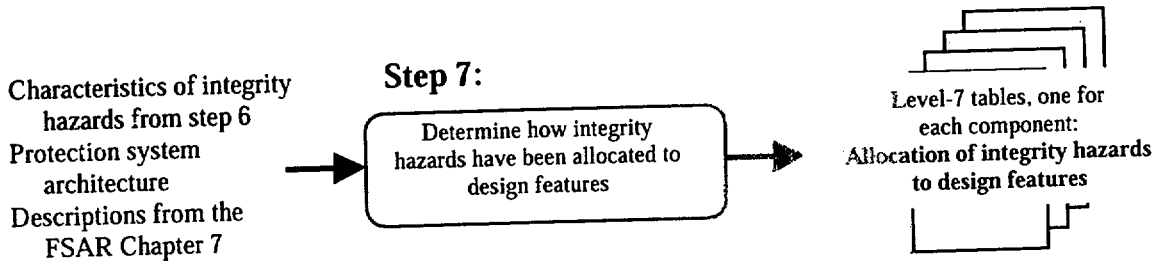


Figure 9. Step 7 of the structured approach.

Inputs: The inputs to this identification process include:

- The level-6 tables of integrity hazard characteristics from step 6 (Section5.5),
- The protection system architecture or hierarchy (i.e., identification of protection system's subsystems and elements, and how they are interconnected), and
- Descriptions of protection system integrity features from the FSAR Chapter 7.

Process: The process in this section is to examine the integrity hazard allocations to ensure that each hazard under consideration is handled by at least one integrity strategy implemented in the protection system design. In many cases a combination of strategies will be employed to address a given integrity hazard. For example, the hazard of random failures of system components is addressed by a combination of quality design, periodic testing, and redundancy.

Outputs: The outputs of this process include the following:

- Identification of the protection system integrity strategy that is assigned responsibility for the integrity hazards under consideration. This information is appended to the level-6 tables of integrity hazard characteristics to produce level-7 tables.

Table 7 shows a template for data collection on the protection subsystems and their responsibilities for protection functions. The data in Table 7 are derived from protection system architectural descriptions contained in FSAR Chapter 7 or supporting design documents, and Table 6a–6d for the function(s) under consideration. The information in the shaded area of the table is carried over from Table 6.

To assist in the review of integrity requirements, Appendix A, Tables A2 and A3, illustrate part of the development of a (non-exhaustive) integrity strategy taxonomy to handle integrity hazards. The strategies employed should provide reasonable assurance that the digital protection system will maintain its functional performance despite hazards to its integrity. Table B7 shows an example of data describing a protection system's integrity hazard allocation.

Table 7. Template for collection of each of the protection system's integrity hazard allocations (Level 7).

Entry	Explanation
System or subsystem	
Component	
Protective function	
Location	Plant location for which environment is specified (The location may describe an area or a specific point, for example, a specific mounting location and elevation may need to be described to specify the level of vibration seen by equipment mounted on process piping or equipment.)

Integrity hazards—protection system failures	Integrity hazard characteristics from Table 6a, Section 5.4	Integrity strategy for each hazard being considered
Integrity hazards—human errors	Integrity hazard characteristics from Table 6a, Section 5.4	Integrity strategy for each hazard being considered
Integrity hazards— normal and accident environment	Integrity hazard characteristics from Table 6b, Section 5.4	Integrity strategy for each hazard being considered
Integrity hazards—process environment	Integrity hazard characteristics from Table 6c, Section 5.4	Integrity strategy for each hazard being considered
Integrity hazards—power sources	Integrity hazard characteristics from Table 6d, Section 5.4	Integrity strategy for each hazard being considered

5.7 Compile Component Integrity Requirements

The purpose of this analysis is to identify expected integrity requirements that should be considered in system requirements specifications, in order to provide reasonable assurance that the digital protection system will maintain its functional performance despite hazards to its integrity. Specifications must describe requirements for all topics important to ensuring component integrity in the presence of expected integrity hazards. As an aid in identifying integrity topics that are important for a particular component, Appendix C contains a catalog of sample integrity requirements specification topics that are typically important to sense, command, and execute features of protection systems. Each topic includes the same information for topics described in Section 3.1. The inputs, processes, and outputs of this step are shown in Figure 10, and are described in detail below.

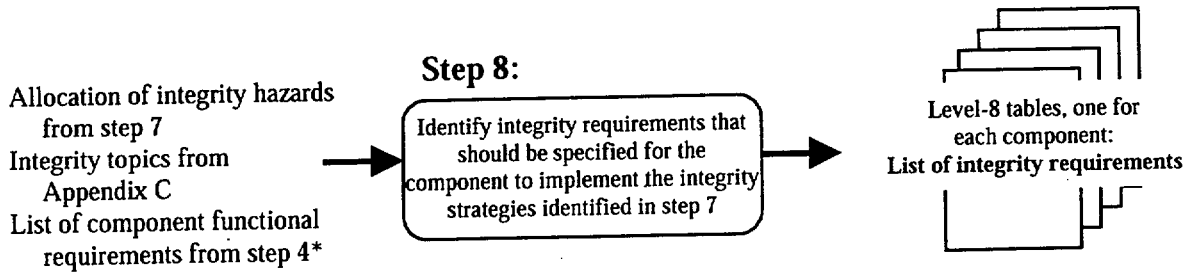


Figure 10. Step 8 of the structured approach.

Inputs: The inputs to this analysis are:

- The level-7 tables identifying the characteristics and allocation of integrity hazards to integrity strategies, as determined by the analysis in step 7 (Section5.6),
- Integrity topics identified in Appendix C, and
- The list of component functional requirements from step 4 (Section 5.3).

Process: The process in this section is to identify integrity requirements that should be specified for the component to implement the integrity strategies identified in step 7. This process identifies integrity requirements that address the hazards against which the component must protect. Topics that must be contained in the subsystem and component specification are then identified using the catalog of topics given in Appendix C.

Candidate integrity requirements for the component are then identified for each topic by examining the hazard characteristics, and considering the characteristics of interacting systems and components. This list of topics and related specific requirements can then be used to verify that all integrity requirements derived from the integrity hazards and assigned to the component under consideration are reflected in the system requirements specifications. Several integrity topics might be identified against the requirements to address a given integrity strategy.

Because the functional and integrity requirements of the protection system interact (i.e., the functional requirements must not cause an integrity hazard that cannot be addressed), the functional requirements from step 4 should be taken into account when performing this review.

Outputs: The outputs from this process are:

- A level-8 table identifying integrity requirements for the component under consideration.

Table 8 illustrates a template for data collection on integrity requirements. The information for Table 8 is derived from the characteristics and allocation of the integrity hazards from the level-7 tables in Section 5.6, and integrity topics and strategies from Appendix C of this report. The outputs of the analysis are a compilation of expected integrity requirements that might be

specified for the component or subsystem under consideration. Table B8 shows an example of integrity mitigation and defense requirements data.

The non-shaded sections of the table represent the main elements of integrity requirements. These elements are derived from integrity mitigation and defense topics discussed in Appendix C of this report. Note that for a given component, several topics may work together to address a given hazard characteristic.

Table 8. Template for collection of characteristics of each integrity mitigation and defense requirements (Level 8).

Entry	Explanation
System or subsystem	
Component	
Protective function	
Functional requirements	Information taken from Table 4 (Section 5.3)
Protection system failures data	See Tables 6a and 7 for expansion and Appendix B for examples
Human errors data	See Tables 6a and 7 for expansion and Appendix B for examples
Normal and accident environment data	See Tables 6b and 7 for expansion and Appendix B for examples
Process environment data	See Tables 6c and 7 for expansion and Appendix B for examples
Power sources data	See Tables 6d and 7 for expansion and Appendix B for examples
Topic (Integrity strategy from Table 7)	Name of the system requirements specification identified to mitigate the hazard
Definition	Description of hazard mitigation strategy
Attributes	Attributes that must be defined to allow implementation of the strategy
Topic characteristics	Characteristics that describe how the topic is used and how it relates to other topics or components
Expected functional requirement	The specific requirement for this topic

5.8 Integrity Requirements Reviews

5.8.1 Specification Requirements Review

This section describes a method for implementing the review recommended by Appendices 7.1-B (item 2) and 7.1-C (item 20) of the SRP. These recommend that NRC's review of protection systems confirm that the applicant/licensee has justified the degree of redundancy, diversity, testability, and quality provided in the safety system design. Chapter 18 of the SRP recommends that the NRC review confirm that critical or risk-significant human actions have been examined to consider ways of reducing or eliminating sources of human error. SRP Appendices 7.1-B (item 5) and 7.1-C (item 9) recommend that NRC verify that the applicant/licensee confirmed that safety system equipment is designed to meet the functional performance requirements over the range of environmental and electromagnetic interference conditions.

The inputs, processes, and outputs of this step are shown in Figure 11, and are described in detail below.

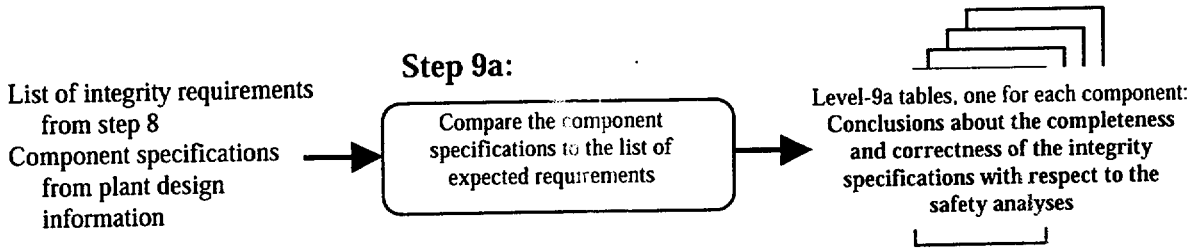


Figure 11. Step 9a of the structured approach.

Inputs: The inputs to this analysis are:

- The level-8 table identifying the integrity requirements for the component under consideration from step 8 (Section 5.7), and
- Component specifications from plant design information.

Process: The completed set of expected integrity requirements specifications (level-8 table) are evaluated against the specification for the components under specification (see Figure 2).

Specific requirements for each component are evaluated by correlating the protection system integrity requirements with the characteristics of the related subsystems and components to identify the requirements applicable to the component being considered. The component's specification is then compared against the topics and related specific requirements to verify that all integrity requirements derived from PIEs and assigned to the component under consideration are appropriately reflected in the system requirements specifications. If conflicts or omissions are found, questions are posed to the licensee or applicant. Another iteration through the process may be required to resolve review findings.

Outputs: The outputs from this process are:

- Conclusions about the completeness and correctness of the system requirements specifications with respect to the safety analyses, in the form of a level-9a table.

Table 9a shows a template for conducting a review of expected component specification integrity requirements against the actual component specifications. Table B9a is an example of the data used to review the specification integrity requirements.

Table 9a. Template for review of integrity requirements (Level 9a).

Entry	Explanation
System or subsystem	Name of the system or subsystem responsible for the protective function being considered
Component	Name of the component under consideration
Expected functional requirement	Functional requirement from Table 8
Source	Table 8 row entry
Actual specification requirement	Corresponding integrity requirement from the component specification

5.8.2 Design Basis Requirements Review

This section describes a method for collecting and organizing information for the review recommended by SRP Appendix 7.1-C (item 8), which recommends that the licensee's assessment of protection system reliability consider the effects of possible hardware and software failures. Chapter 18 of the SRP recommends that the licensee identify critical human actions. In addition, Appendices 7.1-B (item 1) and 7.1-C (item 4) of the SRP recommend that the NRC's review of protection system design bases consider the range of transient and steady-state conditions identified for the environment during normal, abnormal, and accident conditions.

The inputs, processes, and outputs of this step are shown in Figure 12, and are described in detail below.

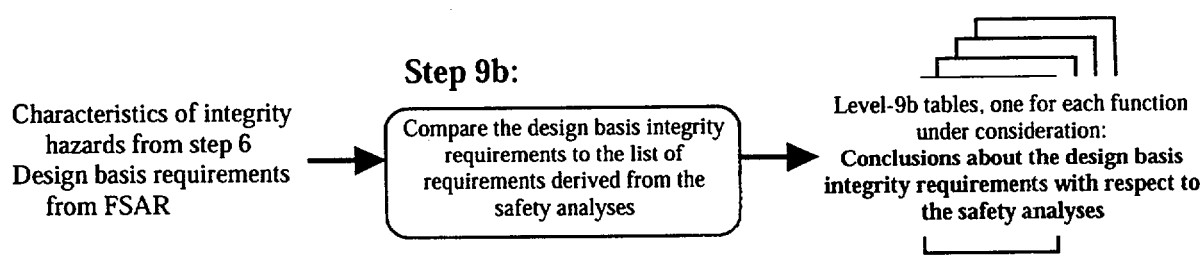


Figure 12. Step 9b of the structured approach.

Inputs: The inputs to this analysis are:

- The level-6 tables identifying the characteristics of integrity hazards for the function under consideration from step 6 (Section 5.5), and
- Design basis requirements from the FSAR.

Process: The completed set of characteristics of integrity hazards (level-6 tables) is evaluated against the design basis requirements for each function under consideration (see Figure 2).

Specific requirements for each function are evaluated by comparing the design basis integrity requirements from the FSAR to the integrity requirements derived from the safety analyses. If conflicts or omissions are found, questions are posed to the licensee or applicant. Another iteration through the process may be required to resolve review findings.

Outputs: The outputs from this process are:

- Conclusions about the design basis integrity requirements with respect to the safety analyses, in the form of a level-9b table.

Table 9b shows a template for conducting a review of expected design basis integrity requirements for a given system or subsystem against the actual design basis integrity requirements from the FSAR. Table B9b shows an example of data for review of design basis integrity requirements.

Table 9b. Template for review of design basis integrity requirements (Level 9b).

Entry	Explanation
System or subsystem	Name of the system or subsystem responsible for the protective function being considered
Component	Name of the component being considered
Expected design basis requirement	Integrity requirement from Tables 6a to 6d
Source	Table 6 row entry
Actual design basis requirement	Corresponding design basis integrity requirement from the FSAR

6. Conclusions

This document outlines an eight-step process for identifying, organizing, and tracing nuclear plant protection system requirements. The process is designed to aid in collecting information for NRC reviews of nuclear reactor protection systems. Using this process, the reviewer can develop and use a set of linked tables to track external and internal hazards to the protection system down to the requirements that must deal with those hazards. The tables provide a clear methodology for showing traceability of requirements from their sources.

7. References

[10 CFR 50.36, 1995] "Technical Specifications," Title 10 CFR Part 50.36, 1995.

[10 CFR 50, Appendix A, 1995] "General Design Criterial for Nuclear Power Plants," Title 10 CFR Part 50, Appendix A, 1995.

[10 CFR 50, Appendix B, 1995] "Quality Assurance Criteria for Nuclear Power Plants and Fuel Processing Plants," Title 10 CFR Part 50, Appendix B, 1995.

[10 CFR 50.62, 1995] "Requirements for Reduction of Risks from Anticipated Transients Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants," Title 10 CFR Part 50.62, 1995.

[Beltracchi, 1991] Beltracchi, L., "Conceptual Design of a Computer-Driven Display for Monitoring Reactor Coolant Mass," IEEE Transactions on Nuclear Science, Vol. 38, No. 3, June 1991.

[BTP HICB-11, 1997] "Guidance on Application and Qualification of Isolation Devices," BTP HICB-11, 1997.

[BTP HICB-14, 1997] "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems," BTP HICB-14, 1997.

[BTP HICB-17, 1997] "Guidance on Self-Test and Surveillance Test Provisions," BTP HICB-17, 1997.

[BTP HICB-19, 1997] "Guidance on Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems," BTP HICB-19, 1997.

[BTP HICB-21, 1997] "Guidance on Digital Computer Real-Time Performance," BTP HICB-21, 1997.

[EPRI-1, 1980] "Advanced Light Water Reactor Utility Requirements Document: ALWR Passive Plant," EPRI, August 1990.

[EPRI-2, 1980] "Advanced Light Water Reactor Utility Requirements Document: ALWR Evolutionary Plant," EPRI, August 1990.

[EPRI TR-106439, 1996] "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment in Nuclear Safety Applications," EPRI TR-106439, October 1993.

[Leveson, 1995] Leveson, N.G., "Safeware: System Safety and Computers," New York, Addison Wesley, 1995.

[NAS, 1997] "Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues," National Academy Press, Washington DC, 1997.

[NUREG-0800, 1997] "Standard Review Plan," NUREG-0800, Rev. 4, June 1997.

[NUREG/CR-6303, 1994] Preckshot, G. G., "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," NUREG/CR-6303, December 1994, also known as UCRL-ID-119239, Lawrence Livermore National Laboratory.

[NUREG/CR-6323, 1995] Seth, S., et al., "High Integrity Software for Nuclear Power Plants: Candidate Guidelines, Technical Basis, and Research Needs," NUREG/CR-6323, June 1995.

[Rasmussen, 1986] Rasmussen, J., " Information Processing and Human-Machine Interaction: An Approach to Cognitive Engineering," New York: North Holland, 1986.

[Vicente and Bisantz, 1994] Vicente, K. J. and Bisantz, A.M., "Making the Abstraction Hierarchy Concrete," Int. J. Human-Computer Studies, 1994.

7.1 Other Reading of Interest

[ANS/ANSI 4.5, 1980] "American National Standard Criteria for Accident Monitoring Functions in Light-Water-Cooled Reactors," ANS/ANSI-4.5, 1980.

[ANS/ANSI 58.8, 1994] "American National Standard Time Response Design Criteria for Safety-Related Opertaor Actions," ANS/ANSI-58.8, 1994.

[ANSI/IEEE Std 279, 1971] "Criteria for Protection Systems for Nuclear Power Generating Stations," ANSI/IEEE Std 279, 1971.

[ANSI/IEEE Std 1002, 1987] "IEEE Standard Taxonomy for Software Engineering, " ANSI/IEEE Std 1002, 1987.

[ANSI/ISA-67.04, 1994] "Setpoints for Nuclear Safety-Related Instrumentation Used in Nuclear Power Plants," ANSI/ISA-67.04, 1994.

[ASME Std. NQA-1, 1994] "Quality Assurance Requirements for Nuclear Facilities Application," ASME Std. NQA-1, 1994.

[ASME Std. NQA-2a, 1990] "Quality Assurance Requirements of Computer Software for Nuclear Facility Applications," ASME Std. NQA-2a Part 2.7, 1990

[Brilliant, et. al., 1990] Brilliant, S., J. C. Knight, and N. G. Leveson, "Analysis of faults in an N-version software experiment," IEEE Transactions of Software Engineering, Vol. 16, No. 2, 1990

[Draft NUREG-1602, 1997] "Guidelines for Use of PRA in Risk-Informed Applications," Draft NUREG-1602, February 1997.

[Draft Reg. Guide DG-1045, 1997] "Setpoints for Safety-Related Instrumentation," Draft Reg. Guide DG-1045, 1997.

[EPRI-1, 1980] "Advances Light Water Reactor Utility Requirements Document: ALWR Passive Plant," EPRI, August 1990.

[EPRI-2, 1980] "Advances Light Water Reactor Utility Requirements Document: ALWR Evolutionary Plant," EPRI, August 1990.

[EPRI TR-102348, 1993] "Guideline on Licensing Digital Upgrades," EPRI TR-102348, December 1993.

[Gopher et al., 1994] Gopher, D., Weil, M., and Bareket, T., "Transfer of Skills from a Computer Game Trainer to Flight," Human Factors, Vol. 36, No. 3, 1994.

[Heimdahl and Leveson, 1996] Heimdahl, M. P. E. and Leveson, N. G., "Completeness and Consistency in Hierarchical State-Based Requirements," IEEE Transactions on Software Engineering, Vol. 22, No. 6, 1996.

[IEEE Std. 610.12, 1990] "IEEE Std Glossary of Software Engineering Terminology," IEEE Std. 610.12, 1990.

[IEEE Std 603, 1991] "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," IEEE Std 603, 1991.

[IEEE Std. 7-4.3.2, 1993] "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," IEEE Std. 7-4.3.2, 1993.

[IEEE Std. 830, 1993] "IEEE Recommended Practice for Software Requirements Specifications," IEEE Std. 830, 1993.

[ISO/IEC 12207, 1995] "Standard for Information Technology -Software Life Cycle Processes," ISO/IEC 12207, 1995.

[Knight and Leveson, 1986] Knight, J. C. and Leveson, N. G., "An experimental Evaluation of the Assumption of Independence in Multi-version Programming," IEEE Transactions on Software, Vol. 12, No. 1, 1986.

[Lawrence and Gallagher, 1997] Lawrence, J. D. and J. M., Gallagher, " Performing Software Safety Hazard Analysis," Reliability Engineering and Systems Safety, Vol. 55, No. 3, 1997

[Leemis, 1995] Leemis, L. M., "Reliability: Probabilistic Models and Statistical Methods," Upper Saddle River, N.J., Prentice-Hall, 1995.

[Leveson et. al., 1994] Leveson, N. G., Heimdahl, M. P. E., Hildreth, H., and Reese, J. D., "Requirements Specification for Process-Control Systems," IEEE Transactions on Software Engineering, Vol. 20, No. 9, 1994.

[NIST, 1994] Wallace, D. and Ippolito, L., " A Framework for the Development and Assurance of High Integrity Software," NIST 500-223, December 1994.

[NUREG-0578] "TMI-2 Lessons Learned Task Force Status Report and Short Term Recommendations," NUREG-0578, July 1979.

[NUREG/CR-2623, 1982] Price, H. E., et al., " Allocation of Functions in Man-Machine Systems: A perspective and Literature Review," NUREG/CR-2623, 1982.

[NUREG/CR-6042, 1994] Haskin, F. E. and Camp, A. C., "Perspective on Reactor Safety," NUREG/CR-6042, March 1994.

[Oppenheim, 1997] Oppenheim, A. V., "Signals and Systems," Prentice Hall, New Jersey, 1997.

[Reg. Guide 1.152, 1996] "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," Reg. Guide 1.152, 1996.

[Reg. Guide 1.168, 1997] "Software Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Reg. Guide 1.168, 1997.

[Reg. Guide 1.169, 1997] "Software Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Reg. Guide 1.169, 1997.

[Reg. Guide 1.170, 1997] "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Reg. Guide 1.170, 1997.

[Reg. Guide 1.171, 1997] "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Reg. Guide 1.171, 1997.

[Reg. Guide 1.172, 1997] "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Reg. Guide 1.172, 1997.

[Reg. Guide 1.173, 1997] "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, " Reg. Guide 1.173, 1997.

[Reg. Guide 1.70, 1978] "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants," Reg. Guide 1.70, November 1978.

[Reg. Guide 1.97, 1980] "Instrumentation for Light Water Cooled Power Plants to Access Plant and Environs Conditions During and Following an Accident," Reg. Guide 1.97, 1980.

[SECY-93-087, 1993] "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor Designs," SECY-93-087, 1993.

Appendix A: Integrity Strategies

This appendix illustrates an Integrity Strategy Process that could be used to help identify integrity hazards and mitigation/defense methods. The tables shown first list top level integrity hazard sources for both ACEs and Process Development (see Tables A1a and A1b). Second, they illustrate a general integrity Mitigation and Defense Strategy Taxonomy (Table A2) which can be used to help guide the selection of techniques for dealing with integrity hazards. One part of the Mitigation and Defense Taxonomy (a diversity taxonomy, see Table A3) is expanded to show a more detailed listing of methods and techniques that can be used when diversity is a desired strategy.

Table A1a. Examples of digital protection system integrity ACEs.

Hardware	Software	Human Performance	Environment	Energy Sources
Common-mode failure Single-point failure Inadequate bandwidth Inadequate data storage capacity drift A to D or D to A conversion errors Propagation of failures between software safety channels and between software safety and non-safety channels Unauthorized alterations	Common-mode failure Single-point failure Unauthorized entries or alterations Propagation of failures between hardware safety channels and between hardware safety and non-safety channels	Common-mode failure Errors of omission Errors of commission Errors of timing Errors of sequence	Seismic Flood Tornado Radiation EMI and RFI ESD Lightning Temperature Pressure Moisture Humidity Steam Chemicals Smoke Radiation	Loss of power supply Fluctuation of power supply Conducted EMI and RFI Total harmonic distortion (THD)

Table A1b. Examples of digital protection system process development hazard sources.

Hardware	Software	Human Performance	Environment	Energy Sources
Requirements Design Coding Implementation Integration Testing Installation Operation Maintenance Unauthorized entries or alterations	Requirements Design Implementation Integration Testing Installation Operation Maintenance Unauthorized entries or alterations	Errors of commission Errors of omission Deficiencies in education and training Inadequate knowledge and skills	-	-

Table A2. Part of a general integrity mitigation and defense strategy taxonomy.

Generic	Software	Hardware	Human Performance	Other
Redundancy	Life cycle management	Life cycle management	Cognitive behavior	Independence
Diversity	Tools	Tools	Training	Incompatibility
Defense in depth	Metrics	Metrics	Simulation	Inoperability
Fail safe	Firewalls	Security	Security	Isolation
Fault management				

Table A3. A diversity integrity mitigation and defense strategy taxonomy (from NUREG/CR-6303).

Diversity Type	Definitions	Examples
Design	Different technology	Analog vs. Digital
	Different approach within a technology	AC coupled vs. DC coupled
	Different architecture	Arrangement or interconnection of components
Equipment	Different manufacturers of fundamentally different designs	
	Same manufacturer of fundamentally different designs	
	Different manufacturer of same design	
	Different versions of same designs	
	Different CPU architecture	Intel 80X86 vs. Motorola 68XXX
	Different CPU chip versions	Intel 80386 vs. Intel 80486
	Different printed circuit board designs	
	Different bus structure	VME vs. Multibus II
Functional	Different underlying mechanism	Gravity convection vs. Pumped flow Rod insertion vs. Boron poisoning
	Different purpose, function, control logic, or actuation means	Normal rod control vs. Reactor trip rod insertion
	Different response time scale	Secondary system activation for persistent accident condition
Human	Different design organization	Different companies
	Different engineering management team within the same company	
	Different designers, engineers or programmers	
	Different testers, installers, or certification personnel	
Signal	Different reactor or process parameters sensed by different physical effects	Pressure vs. Neutron flux
	Different reactor or process parameters sensed by the same physical effect	Pressure vs water level Flow sensed by different pressure sensors
	Same reactor or process parameter sensed by different redundant sets of similar sensors	Set of four redundant water level sensors plus four redundant water level sensors
Software	Different algorithms, logic and program architecture	
	Different timing or order of execution	
	Different operating system	
	Different computer language	

Appendix B: Examples of Table Developments from the Text

This appendix provides example tables illustrating the use of the structured approach. Much of the material in these tables is drawn from Chapter 15 of FSAR for CE System 80+. The specific FSAR sections, figures (F), and tables (T) that were the source of data are indicated in square brackets.

The examples given show how the use of the structured approach to identify areas where protection system requirements are incomplete or inconsistent. These items are identified in the notes column of each task, and are summarized at the end of each section of this appendix.

These tables are illustrative only and not intended to be complete. They have not been verified for correctness, and do not directly relate to the NRC staff's actual review of the System 80+ design certification application. The example tables follow the table numbering used in the discussions in Section 5. The following tables are provided:

Table B1a. Example of data collection for PIE characteristics.

Table B1b. Example of data collection for PIE characteristics.

Table B2. Example of data collection of limiting protection system functional requirements.

Table B3. Example of data collection for the protection system's subsystem and function assignments.

Table B4. Example of data collection for the protection system mitigation and defense functions.

Table B5a. Example of review of specification functional requirements.

Table B5b. Example of review of design basis functional requirements.

Table B6a. Example of data collection of the characteristics of integrity hazards for each system failure.

Table B6b. Example of data collection for normal (ambient) and accident environmental hazards.

Table B6c. Example of data collection of characteristics for process environmental integrity hazards.

Table B6d. Example of data collection of characteristics integrity hazards from power sources.

Table B7. Example of data collection of the protection system's integrity hazard allocations.

Table B8. Example of data collection of characteristics of integrity mitigation and defense requirements.

Table B9a. Example of review of specification integrity requirements.

Table B9b. Example of review of design basis integrity requirements.

B.1 Identify PIE Characteristics

Tables B1a and B1b illustrate the use of the structured approach as described in Section 5.1 to identify potential initiating events (PIEs) and PIE characteristics that establish the functional and performance requirements for the protection system. This example considers two PIEs and a single protective function: emergency feedwater (EFW) actuation on low steam generator water level. The information collected in this case could be used in a "trace audit." Because only a sample of events is considered, the PIE characteristics that are determined may not establish the bounding requirements for the protective function. Those PIE characteristics, however, do establish a subset of requirements against which the design basis for EFW actuation can be tested.

Table B1a. Example of data collection for PIE characteristics.

Entry	Data	Notes
PIE name	Loss of condenser vacuum [15.2.3]	
Initial conditions	Core power: 0–102 % rated full power (RTP) Axial shape index: -0/3 to + 0.3 Reactor vessel inlet coolant flow: 95–116% Full Flow Pressurizer water level: 26–60 % of tap span Coolant inlet temperature < 90 % RTP: 543–561°F 90–100% RTP: 550–561°F Pressurizer pressure: 2175–2325 psia Steam generator water level: 40.7% of wide range tap span, or 95.0% of narrow range tap span [Table 15.0-3] Steam bypass control system: in manual Reactor power cutback: in manual Alternate protection system: failed [15.2.3.1]	31 feet appears to be used [F15.2.3-8]. Presumably this equates to 40.7% of wide range level.
Protective function	Emergency feedwater actuation [T15.2.3-1]	
Related CSFs	Heat removal	
Parameter	Wide range steam generator water level [T15.2.3-1]	
Parameter characteristics		
Delay time	600 ms [T15.0.2]	
Variable range	17 ft–37 ft [F15.2.3-8]	

Entry	Data	Notes
Associated parameters	Pressurizer pressure—provides reactor trip when high setpoint exceeded [T15.2.3-1]	
Maximum rate of change	+0.55 ft/sec, -3 ft/sec [F15.2.3-8]	
Analytical limit	19.9% Wide Range Span [T15.2.3-1]. Note: This appears to conflict with Table 15.0-2, which states that the analytical limit is 40.7% of wide range span.	This conflicts with Table 15.0-2, which states that the analytical limit is 40.7% of wide range span. The 19.9% value is assumed here because it is consistent with Table 7.3-5, which states that the ***nominal setpoint*** is 23.4%.
Frequency spectrum	0 Hz to 0.14 Hz	Based upon analysis of FSAR Figure 15.2.3-8. Note, the figure probably has insufficient resolution to determine true spectrum of interest. Actual frequency content should be confirmed with applicant.

Table B1b. Example of data collection for PIE characteristics.

Entry	Data	Notes
PIE name	Single reactor coolant pump rotor seizure with loss of offsite power (LOOP) [15.3.3]	
Initial conditions	Core power: 0–102 % Rated full power (RTP) Axial shape index: -0/3 to + 0.3 Reactor vessel inlet coolant flow: 95–116% full flow Pressurizer water level: 26–60 % of tap span Coolant inlet temperature < 90 % RTP: 543–561°F 90–100% RTP: 550–561°F Pressurizer pressure: 2175–2325 psia Steam generator water level: 40.7% of wide range tap span, or 95.0% of narrow range tap span [Table 15.0-3] Pressurizer pressure control: fails on LOOP Pressurizer level control: fails on LOOP Reactor regulating system: fails on LOOP Steam bypass control system: fails on LOOP Feedwater control system: fails on LOOP ADS valve sticks open at 1800 sec Reactor power cutback: in manual Alternate protection system: failed [15.3.3.1]	195,000 lbm liquid appears to be used [F15.3.3-12]. Presumably this equates to 40.7% of wide range level.

Entry	Data	Notes
Protective function	Emergency feedwater actuation [T15.3.3-1]	
Related CSFs	heat removal	
Parameter	Wide range steam generator water level [T15.3.3-1]	
Parameter characteristics		
Time delay	600 ms [T15.0.2]	
Variable range	135,000 lbm liquid to 225,000 lbm liquid [F15.3.3-12] Equivalent to: 19.9 ft to 37.0 ft	To be useful the level range information must be expressed in consistent units for all analyses. The FSAR apparently does not provide a correlation between level in lbm liquid, ft, and % wide range. A correlation is inferred here (as discussed below) but the correct correlation should be obtained from the applicant before using this data in a specification review.
Associated parameters	Reactor coolant flow—provides reactor trip when low setpoint is exceeded [T15.2.3-1]	
Maximum rate of change	+250 lbm liquid/sec to -83 lbm liquid/sec [F15.3.3-12] Equivalent to: +0.05 ft/sec to -0.02 ft/sec	Assumes correlation of lbm to feet as discussed below.
Analytical limit	19.9 % of wide range span [T15.3.3-1]	This conflicts with Table 15.0-2, which states that the analytical limit is 40.7% of wide range span. The 19.9% value is assumed here because it is consistent with Table 7.3-5, which states that the ***nominal setpoint*** is 23.4%.
Frequency spectrum	0 Hz to 0.1 Hz	Based upon analysis of Figure 15.3.3-12.

B.2 Identify Protection System Functional Requirements

Correlation of Level Measurements

Table 15.0-2 gives water level conditions at t=0 as 40.7 % of wide range.

Tables 15.2.3-1 and 15.3.3-1 give the assumed trip point as 19.9% of wide range at the trip time, and give the time of trip.

Using this information, the water level in ft. and in lbm at these points can be approximated from Figures 15.2.3-8 and 15.3.3-12. This information can be used to establish an approximate correlation as follows:

Level		
% Wide Range	**Ft.**	**lbm liquid**
40.7	31.3	195000.0
19.9	19.9	135000.0
Therefore:		
A 1% change =	0.5	2884.6
The 0% reference =	9.0	77596.2

Note that these correlations are vastly over-simplistic and that the actual correlations will depend upon temperature and pressure conditions within the steam generator. Nevertheless, these rough correlations are sufficient for a rough analysis of requirements and certainly sufficient to illustrate this example.

Based upon the above correlations the level and level rate of change values in lbm extracted from Figure 15.3.3-12 roughly correspond to values in feet as follows.

135,000 lbm ≈	19.9 % WR ≈	19.9 ft
225,000 lbm ≈	51.1 % WR ≈	37.0 ft
250 lbm/sec ≈	0.09 % WR/sec ≈	0.05 ft/sec
-83 lbm/sec ≈	-0.03 % WR/sec ≈	-0.02 ft/sec

Table B2 reduces the information from Tables B1a and B1b to limiting requirements for the emergency feedwater actuation on low steam generator water level. Note that the requirements are limiting only for the two PIEs considered. More limiting requirements might be identified if a complete set of PIEs were examined.

Table B2. Example of data collection of limiting protection system functional requirements.

Entry	Functional Requirement	Notes
Protective function	Emergency feedwater actuation on low steam generator water level	
PIE name	Loss of condenser vacuum [15.2.3] Single reactor coolant pump rotor seizure with loss of offsite power (LOOP) [15.3.3]	
Initial conditions	40.7% wide range of wide range level [T15.0-2] 195,000 lbm liquid [F15.3.3-12] 31 ft [F15-2.3.8]	Presumably the values of 40.7% WR, 195,000 lbm liquid, and 31 ft are all equivalent, but this cannot be confirmed without additional information.
Related CSFs	Heat removal	
Parameter	Wide range steam generator water level	
Parameter characteristics		
Response time	600 ms [T15.0.2]	Accident analysis assumption.
Parameter range	17.0 to 37.0 ft	Correlation between level in % WR, ft, and lbm liquid needs to be confirmed with applicant. Loss of condenser vacuum sets lower bound. RCP seizure sets upper bound.

Entry	Functional Requirement	Notes
Maximum rate of change	+0.55 ft/sec, -3 ft/sec [F15.2.3-8]	Correlation between level in % WR, ft, and lbm liquid needs to be confirmed with applicant. Loss of condenser vacuum sets bounds.
Analytical limit	19.9% of wide range span	This conflicts with Table 15.0-2, which states that the analytical limit is 40.7% of wide range span. The 19.9% value is assumed here because it is consistent with Table 7.3-5, which states that the ***nominal setpoint*** is 23.4%. Nevertheless, design should accommodate any setpoint between just above 0% and just below 100% of indication.
Frequency spectrum	0 Hz to 0.14 Hz	Based upon analysis of loss of vacuum event. The analysis probably has insufficient resolution to determine true spectrum of interest. Actual frequency content should be confirmed with applicant.
Associated parameters	Pressurizer pressure Reactor coolant flow	The analyses assume reactor trip on these parameters prior to emergency feedwater initiation.

The structured approach, when used to identify a subset of limiting requirements, suggested the following areas for further investigation by the reviewer in discussions with the applicant:

1. What is the actual analytical limit for emergency feedwater actuation on low wide range steam generator water level?

2. How do the wide range water level units of percent full scale map to level in feet and water content in lbs liquid mass that are used in the analyses of Chapter 15?

1. What are the maximum and minimum frequencies of importance in the wide range level signal?

B.3 Identify Protection System Function Assignments

Table B3 illustrates the use of the structured approach, as described in Section 5.2, to identify the digital protection subsystems that handle all the PIEs cataloged in Section B.1 above.

Table B3. Example of data collection for the protection system's subsystem and function assignments.

Entry	Functional Requirement	Notes
System or subsystem	Engineered safety features actuation, and alternate protection system [F7.3-1c]	
Protective function	Emergency feedwater actuation on low steam generator water level.	Figure 7.3-1c is one of many possible citations for the function.

The review found that the selected function has been assigned to both a primary and a diverse protection system. No points for further investigation were identified by this phase of the

structured approach. The remainder of this appendix considers requirements only for the engineered safety features actuation system (ESFAS).

B.4 Identify Component Functional Requirements

Table B4 illustrates the use of the structured approach for collecting expected requirements. The bistable trip processor was selected to illustrate the use of the structured approach because information on this component is readily available in the System 80+ FSAR. Given information on the bistable trip processor software design, the structured approach could be applied to components of the bistable trip processor or any other device in the protection system. Such components might include, for example, the bistable trip processor software or a specific software module that is part of the bistable trip processor software. To apply the structured approach to such lower-level components, design information is necessary to determine how the functional and integrity requirements have been allocated to the component under review. Such information would be available upon request from the licensee or applicant. For this illustration, however, we have limited ourselves to readily available, non-proprietary information.

Table B4. Example of data collection for the protection system mitigation and defense functions.

System or subsystem	Engineered safety features actuation	
Component	Bistable trip processor	
Protective function	Emergency feedwater actuation on low steam generator water level	Note: These data only pertain to the EFW actuation function. EFW actuation on low steam generator water level is only one of many functions that will be performed by the bistable trip processor. The complete set of requirements for this component would be defined by examining all functions. However, examining requirements for a single function such as EFW actuation on low steam generator level is an example of how this method could be applied as part of a trace audit. The specific requirements field of this table identifies acceptance criteria against which the requirements in a detailed specification or design requirements document for the bistable trip processor could be judged. In an actual application of the structured approach, the specific requirements field might be used to record the actual requirements found by the reviewer for comparison against the functional requirements identified by the previous steps.

	Parameter characteristics	Functional requirement	Topic	Definition	Attributes	Topic characteristics	Expected specification requirements	Notes
1	Initial conditions	40.7% wide range of wide range level [T15.0-2] 195,000 lbm liquid [F15.3.3-12] 31 ft [F15-2.3.8]						Presumably the values of 40.7% WR, 195,000 lbm liquid, and 31 ft are all equivalent, but this cannot be confirmed without additional information.
2	Time delay	600 ms [T15.0.2]	Response time	The time required after an abrupt change has occurred in the measured quantity to a new constant value until the output has come to rest at its new value (IEEE Std. 559-1985).	Maximum step size and associated time delay. In some applications minimum time delay may also need to be considered.	The bistable processor response time, when taken together with all other system time delays (including sampling delays) must be less than the overall response time assumed in the accident analysis.	≤ 600 ms minus all other delays in the protective function for a negative step of 100% to less than 19.9% of wide range.	Accident analysis assumption. For this application the output has only two values (function name, trip) and (function name, not tripped).
3	Variable range	17.0 to 37.0 ft	Span	The algebraic difference between the upper and lower values of a calibrated range (ISA S67.04-1994).	Total span	The bistable processor range establishes the bounds of conditions that can be accommodated.	Wide Range level span must encompass the range 17 to 37 feet. For the processor the span should be specified to accommodate 0% to 100% of the input range.	Correlation between level in % WR, ft, and lbm liquid needs to be confirmed with applicant. Loss of condenser vacuum sets lower bound. RCP seizure sets upper bound.

	Parameter characteristics	Functional requirement	Topic	Definition	Attributes	Topic characteristics	Expected specification requirements	Notes
4	Maximum rate of change	+0.55 ft/sec, -3 ft/sec [F15.2.3-8]	Not applicable					The maximum rate of change will be addressed by the frequency spectrum requirement below, and will be used in conjunction with the sampling interval in the setpoint analysis. Correlation between level in % WR, ft, and lbm liquid needs to be confirmed with applicant. Loss of condenser vacuum sets bounds.
5	Analytical limit	19.9% of wide range span	Uncer-tainty	The amount to which an instrument channel's output is in doubt (or the allowance made therefore) due to possible errors, either random or systematic, that have not been corrected for (ISA S67.04-1994).	Value Probability Confidence interval	The bistable uncertainty, combined with command and execute uncertainty, establish a trip setpoint which must fall between the analytical limit and the operating band. Uncertainty will typically be composed of a number of terms such as error, drift, and repeatability.	Uncertainty must be within the allowance made in the setpoint analysis. For protection system functions NRC typically expects point estimates of uncertainties to have a 95% probability with 95% confidence level.	If the bistable trip processor is a completely digital component the uncertainty requirement may be so small as to be negligible. This conflicts with Table 15.0-2, which states that the analytical limit is 40.7% of wide range span. The 19.9% value is assumed here because it is consistent with Table 7.3-5, which states that the ***nominal setpoint*** is 23.4%. Nevertheless, design should accommodate any setpoint between just above 0% and just below 100% of indication.
6			Resolution	The least value of a measured quantity (or change in quantity) which can be distinguished (ANSI C37.1-1987).	Change in parameter value that can be detected.	The resolution must be accounted for in establishing trip setpoints.	The resolution provided must be consistent with the allowance made in the setpoint analysis.	Resolution requirements will impact the allowable data representation in the bistable processor computer.
7			Sampling interval	The time between samples in a sampling control system (IEEE Instrumentation and Measurement Society).	Time	The sample rate together with the maximum parameter rate of change establish the minimum ìrippleî that can be detected. The margin between the analytical limit and the setpoint must account for undetectable ripple.	Sample interval must be within the allowance made in the setpoint analysis.	Note that the sample interval must also be selected with consideration to the frequency spectrum of the sensed signal. Very likely the sensor will not be a sampled system.

	Parameter characteristics	Functional requirement	Topic	Definition	Attributes	Topic characteristics	Expected specification requirements	Notes
8	Frequency spectrum	0 Hz to 0.14 Hz Note, the figure provided in the FSAR probably has insufficient resolution to determine true spectrum of interest. Actual frequency content should be confirmed with applicant.	Sampling interval	The time between samples in a sampling control system (IEEE Instrumentation and Measurement Society).	Time	The sample rate determines the fidelity of the input signal capture.	Sample interval must be less than 3.5 sec to capture all of the frequency information represented in the FSAR analysis.	If the frequency spectrum derived from the FSAR is correct, the signal frequency content will not be the basis for sample rate selection. Sample rate will be controlled by noise, filtering, response time, and setpoint considerations. Sample rates set for these purposes should be rapid enough to prevent aliasing of the process signal.
9	Associated parameters	Pressurizer pressure Reactor coolant flow						The analyses assume reactor trip on these parameters prior to emergency feedwater initiation.

B.5 Functional Requirements Reviews

Tables B5a and B5b provide a template for review of bistable trip processor functional requirements. Where bistable trip processor requirements can be determined from examination of the FSAR they have been entered into the "actual specification requirement" column to illustrate the use of the structured approach. In actual use this column would be completed by examining actual trip processor specifications. In that case any blank in the actual specification requirement table would be an open item for discussion with the licensee or applicant.

Table B5a. Example of review of specification functional requirements.

Component	Bistable trip processor		
Expected specification requirement	**Source (Table B4 row number)**	**Actual specification requirement**	**Notes**
Time delay ≤ 600 ms minus all other delays in the protective function for a negative step of 100% to less than 19.9% of wide range.	2		
Range 0% to 100% of the input range.	3		Correlation between level in % WR, ft, and lbm liquid needs to be confirmed with applicant. Loss of condenser vacuum sets lower bound. RCP seizure sets upper bound.
Uncertainty must be within the allowance made in the setpoint analysis.	5		If the bistable trip processor is a completely digital component the uncertainty requirement may be so small as to be negligible.
The resolution provided must be consistent with the allowance made in the setpoint analysis.	6		Resolution requirements will impact the allowable data representation in the bistable processor computer.
Sample interval must be within the allowance made in the setpoint analysis, but in no case less than 3.15 sec.	2, 4, 7, 8		Note that the sample interval must also be selected with consideration to the frequency spectrum of the sensed signal. Very likely the sensor will not be a sampled system.

Table B5b. Example of review of design basis functional requirements.

System or subsystem	Engineered safety features actuation, and alternate protection system [F7.3-1c]	
Expected design basis requirement	**Actual design basis requirement from FSAR**	**Notes**
Emergency feedwater actuation on low steam generator water level	Emergency feedwater actuation on low steam generator water level	

B.6 Identify Protection System Integrity Requirements

Tables B6a through B6d illustrate the use of the structured approach, as described in Section 5.5, to identify, analyze, and characterize hazards that threaten the integrity of the digital protection system.

Table B6a. Example of data collection of the characteristics of integrity hazards for each system failure.

System or subsystem	Engineered safety features actuation	
Component	Bistable trip processor	
Protective function	Emergency feedwater actuation on low steam generator water level	
Location	Vital instrumentation and equipment room, nuclear annex, elevation +50 ft.	The bistable trip processor could be located in one of four vital instrumentation and equipment rooms: A, B, C, or D. The information in this table identifies the bounding conditions for all four rooms.

Hardware and software events (failures)1

Failure mode	Failure type	Failure effect	Failure likelihood	Notes
Loss of power	Random	Bistable trip outputs generated to logic processors in the same channel and to redundant channel logic processors via remote channel I/O drops. Pre-trip and trip signals generated in channel.	Not stated	
Failure of data communications links	Random (hardware)	Bistable trip outputs generated to logic processors in the same channel and to redundant channel logic processors via remote channel I/O drops. Pre-trip and trip signals generated in channel.	Not stated	
Failure of data communications links	Systematic (software)	Bistable trip outputs generated to logic processors in the same channel and to redundant channel logic processors via remote channel I/O drops. Pre-trip and trip signals generated in channel.	Not stated	It is presumed that recoverable corruptions in data transmission are not failures.
CPU failures that stop execution	Random (hardware)	Bistable processors will not respond to valid trip conditions.	Not stated	Failures that do not stop execution need to be considered.
CPU failures that stop execution	Systematic (software)	Bistable processors will not respond to valid trip conditions.	Not stated	Failures that do not stop execution need to be considered.

Human errors

Error	Error type	Error effect	Error likelihood

*Failure analysis information collected from FSAR Table 7.2-5 (Item 20).

Error	Error type	Error effect	Error likelihood
Non-conservative setpoint entered	Random	Bistable processors will not respond to valid trip conditions	Not stated
Non-conservative setpoint entered	Systematic	Bistable processors will not respond to valid trip conditions	Not stated
Bistable trip processor placed in bypass	Random	Reduces redundancy	Not stated
Bistable trip processor placed in trip	Random	Half-trip	Not stated

Table B6b. Example of data collection for normal (ambient) and accident environmental hazards.

System or subsystem	Engineered safety features actuation	
Component	Bistable trip processor	
Protective function	Emergency feedwater actuation on low steam generator water level	
Location	Vital instrumentation and equipment room, nuclear annex, elevation +50 ft.	The bistable trip processor could be located in one of four vital instrumentation and equipment rooms: A, B, C, or D. The information in this table identifies the bounding conditions for all four rooms.

Environment	Data	Notes
Normal (ambient) environments		The example ambient environments given are examples only. They are not derived from the System 80+ FSAR.
Tmax and Tmin	67 to 73 °F	Temperature is given for the room. The bistable trip processor will actually experience the internal cabinet temperature, which will be higher.
Pressure	Slightly positive to slightly negative	
Humidity	10 to 60%	
Radiation	< 2.5 mRad/hour γ [T12.3-1, T12.3-2] <1000 Rad γ, total integrated dose	
Fluid, chemical, or gas	None	
EMI and RFI	Not stated	
Vibration (non-seismic)	Not available – normal vibration is probably negligible	
Accident environments		
Temperature	Same as normal environment	
Pressure	Same as normal environment	
Humidity	Same as normal environment	
Fluid, chemical, or gas	Same as normal environment	

Environment	Data	Notes
Radiation	< 2.5 mRad/hour γ [T12.3-1, T12.3-4]	The post-accident radiation environment is highest in Rooms C and D because they are closer to the containment.
Flood	None	
Vibration (seismic)	Horizontal and vertical vibration spectrum—see Figures B1 and B2.	Spectra given are floor spectra. These will apply to the cabinet in which the bistable trip processor is located. If the processor is separately seismically qualified, then cabinet magnification must be considered.
Mechanical	None	
Fire	Combustion products Heat Water	

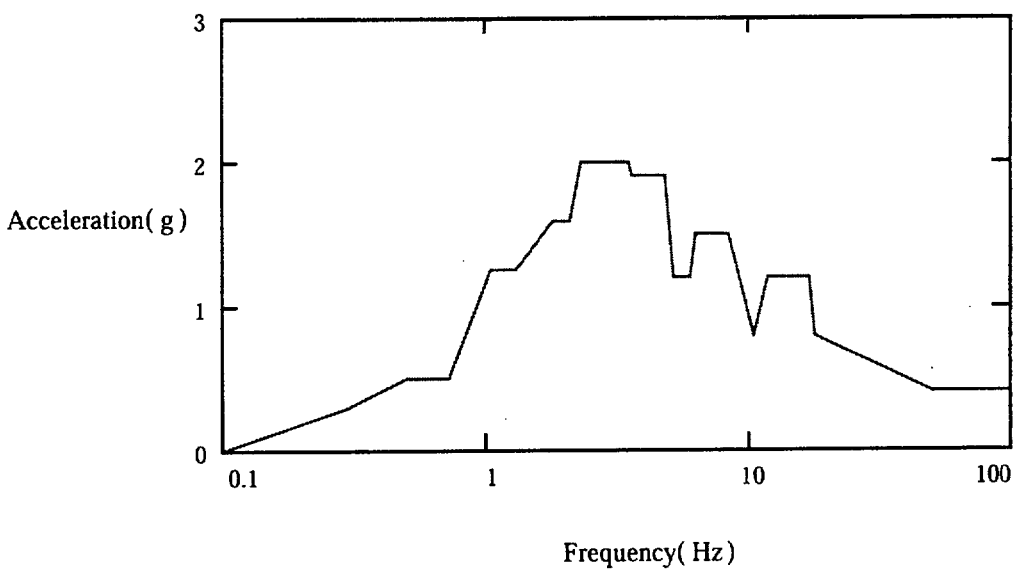


Figure B1. Vertical Response Spectrum Nuclear Annex 50'.

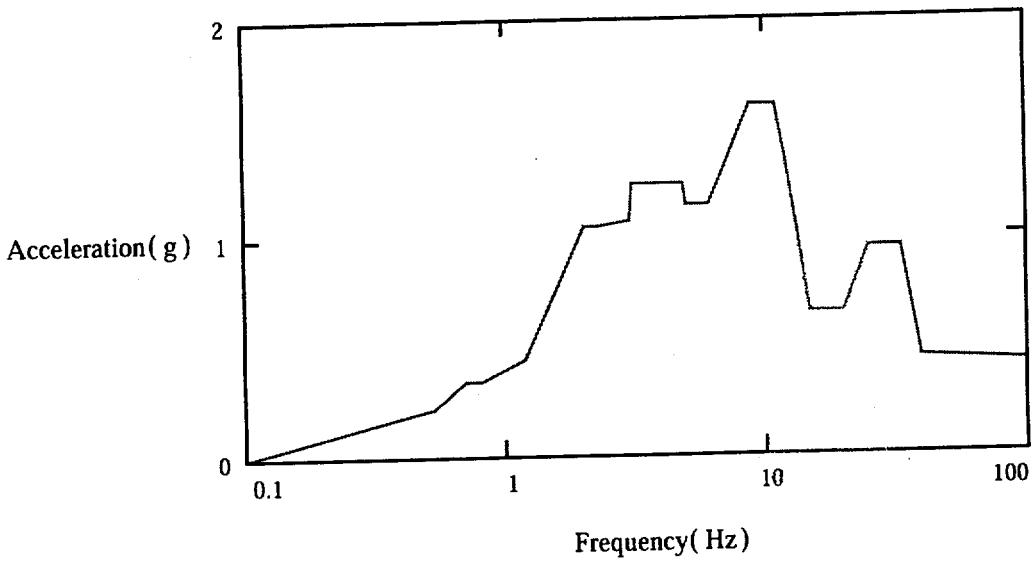


Figure B2. Horizontal Response Spectrum Nuclear Annex 50'.

Table B6c. Example of data collection of characteristics for process environmental integrity hazards.

System or subsystem	Engineered safety features actuation	
Component	Bistable trip processor	
Protective function	Emergency feedwater actuation on low steam generator water level	
Location	Vital instrumentation and equipment room, nuclear annex, elevation +50 ft.	The bistable trip processor could be located in one of four vital instrumentation and equipment rooms: A, B, C, or D. The information in this table identifies the bounding conditions for all four rooms.

Normal process environments		The bistable trip processor is not exposed to a process environment.
Tmax and Tmin	Not applicable	
Fluid, chemical, or gas	Not applicable	
Radiation	Not applicable	
Pressure	Not applicable	

Table B6d. Example of data collection of characteristics integrity hazards from power sources.

System or subsystem	Engineered safety features actuation	
Component	Bistable trip processor	
Protective function	Emergency feedwater actuation on low steam generator water level	
Location	Vital instrumentation and equipment room, nuclear annex, elevation +50 ft.	The bistable trip processor could be located in one of four vital instrumentation and equipment rooms: A, B, C, or D. The information in this table identifies the bounding conditions for all four rooms.

Entry	Data	Notes
Power source	120 V vital AC	It is not known if the bistable trip processor is powered by the AC source or by a lower-voltage supply that is powered from this source. If the latter is the case, data specific to the local power source will be needed from the applicant. The 120 VAC source could be from distribution center SA*D401, SB*D401, SC*D401, or SD*D401.
Electrical power source		
Vmax and Vmin	117.6 to 122.4 VAC	
Frequency	60 ± 0.5 Hz	
Transients	Not stated	
EMI	Not stated	
Total harmonic distortion	Not stated	Total harmonic distortion of supplied AC should be stated.
Air power sources		
Pmax and Pmin	Not applicable	
Purity	Not applicable	

The structured approach, when used to identify a subset of integrity requirements, suggested the following points for further investigation by the reviewer in discussions with the applicant:

1. Failure modes beyond those considered in the failure modes and effects analysis seem possible for the bistable trip processor. Are the failure modes stated for the bistable trip processors complete?
2. What abnormal environmental requirements should be specified for the bistable trip processor?
3. What EMI and RFI requirements should be specified for the bistable trip processor?
4. Should normal and abnormal vibration environments be specified?

5. What power source transients and total harmonic distortion need to be considered in specifying power quality?
6. What human-error integrity hazards should be considered in the design of the bistable trip processor, and what associated procedures and training should be implemented?
7. What are the ranges of normal environmental conditions for the bistable trip processor inside the protection system cabinets?

B.7 Allocation of Integrity Hazards

Table B7 illustrates the use of the structured approach, as described in Section 5.6, to determine what integrity strategies are to be incorporated into the design to mitigate the integrity hazards cataloged in Tables B6a through B6d.

Table B7. Example of data collection of the protection system's integrity hazard allocations.

System or subsystem	Engineered safety features actuation	
Component	Bistable trip processor	
Protective function	Emergency feedwater actuation on low steam generator water level	
Location	Vital instrumentation and equipment room, nuclear annex, elevation +50 ft.	The bistable trip processor could be located in one of four vital instrumentation and equipment rooms: A, B, C, or D. The information in this table identifies the bounding conditions for all four rooms.

Protection system failures

Failure mode	Failure type	Failure effect	Failure likelihood	Integrity strategy topic	Notes
Loss of power	Random	Bistable trip outputs generated to logic processors in the same channel and to redundant channel logic processors via remote channel I/O drops. Pre-trip and trip signals generated in channel.	Not stated	Redundancy	
Failure of data communications links	Random (hardware)	Bistable trip outputs generated to logic processors in the same channel and to redundant channel logic processors via remote channel I/O drops. Pre-trip and trip signals generated in channel.	Not stated	Redundancy Self-testing Periodic tests	
Failure of data communications links	Systematic (software)	Bistable trip outputs generated to logic processors in the same channel and to redundant channel logic processors via remote channel I/O drops. Pre-trip and trip signals generated in channel.	Not stated	Defense-in-depth and diversity Software engineering process	It is presumed that recoverable corruptions in data transmission are not failures.
CPU failures that stop execution	Random (hardware)	Bistable processors will not respond to valid trip conditions.	Not stated	Redundancy Self-testing Periodic tests	Failures that do not stop execution need to be considered.
CPU failures that stop execution	Systematic (software)	Bistable processors will not respond to valid trip conditions.	Not stated	Defense-in-depth and diversity Software engineering process	Failures that do not stop execution need to be considered.

Human errors

Error	Error type	Error effect	Error likelihood	Integrity strategy topic	Notes
Non-conservative setpoint entered	Random	Bistable processors will not respond to valid trip conditions	Not stated	Redundancy Self-testing Periodic tests	
Non-conservative setpoint entered	Systematic	Bistable processors will not respond to valid trip conditions	Not stated	Defense-in-depth and diversity	
Bistable trip processor placed in bypass	Random	Reduces redundancy	Not stated	Status indication Error-tolerant design Access control	
Bistable trip processor placed in trip	Random	Half-trip	Not stated	Status indication Access control	

Normal, accident, and process environments

Environment	Data	Integrity strategy topic	Notes
Normal (ambient) environments			The example ambient environments given are examples only. They are not derived from the System 80+ FSAR.
Tmax and Tmin	67 to 73 °F	Environmental qualification	Temperature is given for the room. The bistable trip processor will actually experience the internal cabinet temperature, which will be higher.
Pressure	Slightly positive to slightly negative	Environmental qualification	
Humidity	10 to 60%	Environmental qualification	
Radiation	< 2.5 mRad/hour γ [T12.3-1, T12.3-2] <1000 Rad γ, total integrated dose	Environmental qualification	
Fluid, chemical, or gas	None	Not applicable	
EMI and RFI	Not stated	Qualification testing Grounding Shielding	
Vibration (non-seismic)	Not available—normal vibration is probably negligible		

Environment	Data	Integrity strategy topic	Notes
Accident environments			
Temperature	Same as normal environment	Environmental qualification	
Pressure	Same as normal environment	Environmental qualification	
Humidity	Same as normal environment	Environmental qualification	
Fluid, chemical, or gas	None	Not applicable	
Radiation	< 2.5 mRad/hour γ [T12.3-1, T12.3-4]		The post-accident radiation environment is highest in Rooms C and D because they are closer to the containment.
Flood	None		
Vibration (seismic)	Horizontal and vertical vibration spectrum—see Figures B1 and B2.	Qualification	Spectra given are floor spectra. These will apply to the cabinet in which the bistable trip processor is located. If the processor is separately seismically qualified, then cabinet magnification must be considered.
Mechanical	None	Not applicable	
Fire	Combustion products Heat Water	Fire isolation Fire suppression Protection from fire suppression	
Normal process environments			
Tmax and Tmin	Not applicable	Not applicable	
Fluid, chemical, or gas	Not applicable	Not applicable	
Radiation	Not applicable	Not applicable	
Pressure	Not applicable	Not applicable	

Power sources

Entry	Data	Integrity strategy topic	Notes
Power source	120 V vital AC		It is not known if the bistable trip processor is powered by the AC source or by a lower-voltage supply that is powered from this source. If the latter is the case, data specific to the local power source will be needed from the applicant. The 120 VAC source could be from distribution center SA*D401, SB*D401, SC*D401, or SD*D401.

Electrical power source			
Vmax and Vmin	117.6 to 122.4 VAC	Design qualification	
Frequency	60 ± 0.5 Hz	Design qualification	
Transients	Not stated		
EMI	Not stated	Grounding, shielding, qualification	
Total harmonic distortion	Not stated	Design qualification	Total harmonic distortion of supplied AC should be stated.
Air power sources			
Pmax and Pmin	Not applicable	Not applicable	
Purity	Not applicable	Not applicable	

B.8 Compile Component Integrity Requirements

Table B8 illustrates the use of the structured approach, as described in Section 5.7, to develop topics that should be considered when confirming that protection system hardware, software, and human-performance integrity requirements have been appropriately addressed in specifications or procedures. This example considers some of the topics that should be addressed in the specification for a bistable trip processor that implements the ESFAS emergency feedwater actuation on low steam generator water level. The topics identified are illustrative rather than exhaustive. For a trace audit, however, the structured approach identifies a subset of topics against which the licensee or applicant's specifications may be tested.

Table B8. Example of data collection of characteristics of integrity mitigation and defense requirements.

System or subsystem	Engineered safety features actuation
Component	Bistable trip processor
Protective function	Emergency feedwater actuation on low steam generator water level
Functional requirements	Information taken from Table 4

Protection system failures

	Failure mode	Failure type	Failure effect	Failure likeli-hood	Topic	Definition	Attributes	Topic characteristics	Expected specification requirement	Notes
1	Loss of power	Random	Bistable trip outputs generated to logic processors in the same channel and to redundant channel logic processors via remote channel I/O drops. Pre-trip and trip signals generated in channel.	Not stated	Redundancy	Duplication of elements in a system or installation for the purpose of enhancing the reliability or continuity of operation of the system or installation (IEEE 446-1987).	Level of redundancy to be provided.	Establishes the need for backup sense channels and appropriate combinatorial logic functions.	Redundancy of power supply to redundant bistable trip processors. Independence of power supplies to redundant bistable trip processors.	
2	Failure of data communi-cations links	Random (hardware)	Bistable trip outputs generated to logic processors in the same channel and to redundant channel logic processors via remote channel I/O drops. Pre-trip and trip signals generated in channel.	Not stated	Redundancy	Duplication of elements in a system or installation for the purpose of enhancing the reliability or continuity of operation of the system or installation (IEEE 446-1987).	Level of redundancy to be provided.	Establishes the need for backup sense channels and appropriate combinatorial logic functions.	Redundancy of data communications links to redundant bistable trip processors. Independence of data communications links to redundant bistable trip processors.	
3					Self-testing	Testing by a device (or system) to check its own circuitry and operation.	Type of testing, test interval.	Establishes the need for test functions and potentially separate test hardware.	Self-test capability of data communications systems. Self test frequency of data communications systems.	Need to determine automatic test interval requirements.

	Failure mode	Failure type	Failure effect	Failure likeli-hood	Topic	Definition	Attributes	Topic characteristics	Expected specification requirement	Notes
4					Periodic tests	Tests performed at scheduled intervals to detect failures and verify operability.	Type of testing, test interval.	Establishes the need for test functions and potentially separate test hardware.	Periodic-test capability of data communications systems. Periodic test frequency of data communications systems.	
5	Failure of data communi-cations links*	Systematic (software)	Bistable trip outputs generated to logic processors in the same channel and to redundant channel logic processors via remote channel I/O drops. Pre-trip and trip signals generated in channel.	Not stated	Defense-in-depth and diversity	Provision of diverse systems to compensate for common-mode failure.	Diverse functions to be provided, type of diversity to be provided.	Establishes the need for diverse functions, systems, or equipment.	Diverse backup for emergency feedwater actuation.	CPUs that stop execution should be anticipated.
6					Software engineering process	Activities established to minimize errors in design or implementation of software.	Plans, and procedures that define the process. Design outputs to be produced by the process.	Establishes process to ensure software developed performs the required safety functions.	Software engineering life cycle for data communications software. Detailed description of software engineering life cycle activities for data communications software. Identification of software engineering life cycle design outputs for software engineering life cycle.	
7	CPU failures that stop execution	Random (hardware)	Bistable processors will not respond to valid trip conditions.	Not stated	Redundancy	Duplication of elements in a system or installation to enhance the reliability or continuity of operation of the system or installation (IEEE 446-1987).	Level of redundancy to be provided.	Establishes the need for backup sense channels and appropriate combinatorial logic functions.	Redundancy of bistable trip processors. Independence of redundant bistable trip processors.	

* In this case failure involves failure to deliver the required information within the timing constraints. Failure to properly transmit or receive an individual transmission packet is not a failure of the data links if this failure is appropriately handled by error detection and correction provisions.

	Failure mode	Failure type	Failure effect	Failure likeli-hood	Topic	Definition	Attributes	Topic characteristics	Expected specification requirement	Notes
8					Self-testing	Testing by a device (or system) to check its own circuitry and operation.	Type of testing, test interval.	Establishes the need for test functions and potentially separate test hardware.	Self-test capabilities for bistable trip processor. Self-test frequency for bistable trip processors.	Need to determine automatic test interval requirements.
9					Periodic tests	Tests performed at scheduled intervals to detect failures and verify operability.	Type of testing, test interval.	Establishes the need for test functions and potentially separate test hardware.	Manual test capability or bistable trip processors. Manual test frequency for bistable trip processors.	
10	CPU failures that stop execution	Systematic (software)	Bistable processors will not respond to valid trip conditions.	Not stated	Defense-in-depth and diversity	Provision of diverse systems to compensate for common-mode failure.	Diverse functions to be provided, type of diversity to be provided.	Establishes the need for diverse functions, systems, or equipment.	Diverse backup for emergency feedwater actuation.	CPU failures that stop execution should be anticipated.

Human errors

	Error	Error type	Error effect	Error likeli-hood	Topic	Definition	Attributes	Topic characteristics	Expected specification requirement	Notes
11	Non-conservative setpoint entered	Random	Bistable processors will not respond to valid trip conditions.	Not stated	Redundancy	Duplication of elements in a system or installation to enhance the reliability or continuity of operation of the system or installation (IEEE 446-1987).	Level of redundancy to be provided.	Establish need for backup sense channels and appropriate combinatorial logic functions.	Redundancy of bistable trip processors. Independence of redundant bistable trip processors.	
12					Self-testing	Testing by a device (or system) to check its own circuitry and operation.	Type of testing, test interval.	Establishes the need for test functions and potentially separate test hardware.	Self-test capability for checking bistable trip processor set points.	Need to determine automatic test interval requirements.
13					Periodic tests	Tests performed at scheduled intervals to detect failures and verify operability.	Type of testing, test interval.	Establishes the need for test functions and potentially separate test hardware.	Manual test capability for checking bistable trip processor set points.	

	Error	Error type	Error effect	Error likeli-hood	Topic	Definition	Attributes	Topic characteristics	Expected specification requirement	Notes
14	Non-conservative setpoint entered	Systematic	Bistable processors will not respond to valid trip conditions.	Not stated	Defense-in-depth and diversity	Provision of diverse systems to compensate for common-mode failure.	Diverse functions to be provided, type of diversity to be provided.	Establishes the need for diverse functions, systems, or equipment.	Diverse backup for emergency feedwater actuation.	
15					Verification	The process of evaluating a system or component to determine whether the products of a given development phase satisfy the conditions imposed at the start of that phase (IEEE 610.12).	Type of verification, independence of verifiers.	Establishes the need for independent verification activities.	Setpoint control process.	
16	Bistable trip processor placed in bypass	Random	Reduces redundancy	Not stated	Status indication	Provision of indications to alert operators to abnormal configurations.	Type of indication.	Establishes requirements for operator awareness.	Indication of bistable trip processor bypass. Type of bypass indication for bistable trip processor bypass.	
17					Error-tolerant design	Provision of design features to prevent adverse consequences of operator errors.	Error detection, error correction.	Establishes requirements for tolerance of human errors.	Interlocks to prevent bypassing multiple bistable trip processors.	
18					Access control	Provisions to prevent unauthorized access to protection system equipment or software.	Physical access control, software access control, electronic access control.	Establishes requirements for preventing unauthorized access.	Access control for bistable trip processor bypass capability.	Can bypass be initiated through any electronic communi-cation links?
19	Bistable trip processor placed in trip	Random	Half-trip	Not stated	Status indication	Provision of indications to alert operators to abnormal configurations.	Type of indication.	Establishes requirements for operator awareness	Indication of bistable trip processor trip	
20					Access control	Provisions to prevent unauthorized access to protection system equipment or software.	Physical access control, software access control, electronic access control.	Establishes requirements for preventing unauthorized access.	Access control for bistable trip processor trip capability. Type of trip indication for bistable trip processor trip.	Can trip be initiated through any electronic communi-cation links?

Normal, accident, and process environments

	Environment	Environmental conditions	Topic	Definition	Attributes	Topic characteristics	Expected specification requirement	Notes
	Ambient environments							
21	Tmax and Tmin	67 to 73 °F	Environmental qualification	Programs to demonstrate the ability of equipment to operate under the extremes of environmental conditions.	Type of qualification, qualification environment, qualification configuration, preventative maintenance.	Describes the activities necessary to demonstrate and to maintain ability to operate in the specified environment.	Ambient Tmax and Tmin 67 to 73 °F Analysis or testing of environmental capability.	Temperature is given for the room. The bistable trip processor will actually experience the internal cabinet temperature, which will be higher.
22	Pressure	Slightly positive to slightly negative	"	"	"	"	Ambient pressure slightly positive to slightly negative. Analysis or testing of environmental capability.	
23	Humidity	10 to 60%	"	"	"	"	Ambient humidity 10 to 60%. Analysis or testing of environmental capability.	
24	Radiation	< 2.5 mRad/hour γ [T12.3-1, T12.3-2] <1000 Rad γ, total integrated dose	"	"	"	"	Ambient radiation dose < 2.5 mRad/hour γ, <1000 Rad γ, total integrated dose. Analysis or testing of environmental capability.	Electronic materials are not susceptible to radiation doses or dose rates in the specified range.
25	Chemical	None					Not applicable	
26	EMI and RFI	Not stated	Environmental qualification	Programs to demonstrate the ability of equipment to operate under the extremes of environmental conditions.	Type of qualification, qualification environment, qualification configuration, preventative maintenance.	Describes the activities necessary to demonstrate and to maintain ability to operate in the specified environment.	Specification of ambient EMI and RFI. Analysis or testing of environmental capability.	

	Environment	Environmental conditions	Topic	Definition	Attributes	Topic characteristics	Expected specification requirement	Notes
27	Vibration (non-seismic)	Not available. Normal vibration is probably negligible.	"	"	"	"	Specification of ambient vibration spectrum. Analysis or testing of environmental capability.	
	Accident environments							
28	Temperature	Same as normal environment	Environmental qualification	Programs to demonstrate the ability of equipment to operate under the extremes of environmental conditions.	Type of qualification, qualification environment, qualification configuration, preventative maintenance.	Describes the activities necessary to demonstrate and to maintain ability to operate in the specified environment.	Specification of accident temperature. Analysis or testing of environmental capability.	
29	Pressure	Same as normal environment	"	"	"	"	Specification of accident pressure. Analysis or testing of environmental capability.	
30	Humidity	Same as normal environment	"	"	"	"	Specification of accident humidity. Analysis or testing of environmental capability.	
31	Fluid or chemical	Same as normal environment	"	"	"	"	Specification of accident fluids and chemicals. Analysis or testing of environmental capability.	
32	Radiation	< 2.5 mRad/hour γ [T12.3-1, T12.3-4] Total integrated dose < 10 Rad	"	"	"	"	Accident radiation dose < 2.5 mRad/hour γ. Total integrated dose < 10 Rad. Analysis or testing of environmental capability.	Electronic materials are not susceptible to radiation doses or dose rates in the specified range. The post-accident radiation environment is highest in Rooms C and D because they are closer to the containment.
33	Flood	None					Not applicable	

	Environment	Environmental conditions	Topic	Definition	Attributes	Topic characteristics	Expected specification requirement	Notes
34	Vibration (seismic)	Horizontal and vertical vibration spectrum.	Qualification	Programs to demonstrate the ability of equipment to operate under the extremes of seismic conditions.	Type of qualification, qualification environment, qualification configuration, preventative maintenance.	Describes the activities necessary to demonstrate and to maintain ability to operate in the specified environment.	Seismic vibration spectrum – see Figures B1 and B2. Analysis or testing of environmental capability.	Spectra given are floor spectra. These will apply to the cabinet in which the bistable trip processor is located. If processor is separately seismically qualified, then cabinet magnification must be considered.
35	Mechanical	None					Not applicable	
36	Fire	Combustion products Heat Water	Fire isolation	Features to prevent redundant channels from being affected by a common fire.	Type of isolation provisions.	Describes the methods and techniques to prevent the effects of a fire from affecting redundant channels.	Bistable processors to be located in separate fire areas. Bistable trip processor rooms to have a smoke removal system.	
37			Fire suppression	Features to minimize fire effects in the affected fire area.	Type of provisions.	Describes how fires are prevented or mitigated.	Fire loading in bistable trip processor rooms minimized by minimizing the amount of cable, using fire-retardant cable, and controlling transient fire loads. Fire suppression sprinklers in bypass trip processor rooms .	
38			Protection from fire suppression	Features to prevent fire suppression activities from affecting equipment.	Type of provisions.	Describes how component is protected from fire-suppression effects.	Bistable trip processor to be located in equipment cabinet. Bistable trip processor cabinets to have water shields. Bistable trip processor cabinets to be located on a raised base.	
	Normal process environments							Primarily applies to sense elements
39	Tmax and Tmin	Not applicable						Primarily applies to sense elements
40	Fluid or Chemical	Not applicable						Primarily applies to sense elements
41	Radiation	Not applicable						Primarily applies to sense elements
42	Pressure	Not applicable						Primarily applies to sense elements

Power sources

	Environment	Environmental conditions	Topic	Definition	Attributes	Topic characteristics	Expected specification requirement	Notes
	Electrical power source							
43	Vmax and Vmin	117.6 to 122.4 VAC	Design qualification	Programs to demonstrate the ability of equipment to operate under the extremes of conditions.	Type of qualification, qualification environment, qualification configuration, preventative maintenance.	Describes the activities necessary to demonstrate and to maintain ability to operate in the specified power environment.	Power source Vmax and Vmin 117.6 to 122.4 VAC. Analysis or testing of environmental capability.	It is not known if the bistable trip processor is powered by the AC source or by a lower-voltage supply that is powered from this source. If the latter is the case, data specific to the local power source will be needed from the applicant. The 120 VAC source could be from distribution center SA*D401, SB*D401, SC*D401, or SD*D401.
44	Frequency	60 ± 0.5 Hz	"	"	"	"	Power source frequency 60 ± 0.5 Hz. Analysis or testing of environmental capability.	

	Environment	Environmental conditions	Topic	Definition	Attributes	Topic characteristics	Expected specification requirement	Notes
45	Transients	None					Specification of power source transients. Analysis or testing of environmental capability.	
46	EMI	Not stated	Grounding	Provisions to bypass EMI signals to ground.	Description of design or construction measures.	Type of grounding	Specification of power source grounding requirements. Analysis or testing of environmental capability.	EMI prevention and mitigation measures should be specified.
47			Shielding	Provisions to shield from EMI signals.	Description of design or construction measures.	Type of shielding		"
48			Qualification	Programs to demonstrate the ability of equipment to operate under the EMI conditions and to demonstrate the EMI emissions are within the assumptions.	Type of qualification, qualification environment, qualification configuration, preventative maintenance.	Describes the activities necessary to demonstrate and to maintain ability to operate in the specified environment.	Specification of power source qualification requirements.	EMI qualification testing should be described.
49	Total harmonic distortion	Not stated	Qualification	Programs to demonstrate the ability of equipment to operate under the EMI conditions and to demonstrate the EMI emissions are within the assumptions.	Type of qualification, qualification environment, qualification configuration, preventative maintenance.	Type of qualification, qualification environment, qualification configuration, preventative maintenance.	Specification of power source total harmonic distortion. Analysis or testing of environmental capability.	
	Air power sources							
50	Pmax and Pmin	Not applicable						
51	Purity	Not applicable						

B.9 Integrity Requirements Reviews

Tables B9a and B9b provide a template for review of bistable trip processor integrity requirements and system design basis requirements that are necessary to implement integrity strategies that protect against failures involving the bistable trip processor. Where bistable trip processor requirements can be determined from examination of the FSAR they have been entered into the "actual specification requirement" column to illustrate the use of the structured approach. In actual use this column would be completed by

examining actual trip processor specifications. In that case any blank in the actual specification requirement table would be an open item for discussion with the licensee or applicant.

Table B9a. Example of review of specification integrity requirements.

System or subsystem	Engineered safety features actuation
Component	Bistable trip processor

Expected specification requirement	Source (Table B8 row number)	Actual specification requirement	Notes
Self-test capabilities for bistable trip processor.	8	Protection system functions are to be monitored by a separate test processor. Test processor monitors selected data communication links. [7.2.1.1.9]	
Self-test frequency for bistable trip processors.	8		
Manual test capability or bistable trip processors.	9	Manual testing that confirms appropriate performance when an input test signal varies above and below the trip setpoint. [7.2.1.1.9.2].	
Manual test frequency for bistable trip processors.	9	Test interval is quarterly [tech specs].	
Self-test capability for checking bistable trip processor set points.	12	Protection system functions are to be monitored by a separate test processor. Test processor monitors setpoints [7.2.1.1.9].	
Manual test capability for checking bistable trip processor set points.	13	Manual testing that confirms appropriate performance when a input test signal varies above and below the trip setpoint [7.2.1.1.9.2].	
Indication of bistable trip processor bypass.	16		
Type of bypass indication for bistable trip processor bypass.	16		
Interlocks to prevent bypassing multiple bistable trip processors.	17	All bistable trip processors are informed of each bypass. When any processor is placed into bypass it checks the bypass status of the redundant processors. If a bistable trip processor is placed into the bypass mode when any of the redundant processors are already in bypass, the affected processor goes to trip.	
Access control for bistable trip processor bypass capability.	18	Maintenance bypass switches are behind locked cabinet doors. Access keys are controlled by shift supervisor.	If bypass can be initiated through any electronic communication links the requirements need to address both physical and electronic access control.
Indication of bistable trip processor trip	19	Bypass and inoperable status indication is required to notify operators when bistable processor is placed in trip	

Expected specification requirement	Source (Table B8 row number)	Actual specification requirement	Notes
Access control for bistable trip processor trip capability.	20	Manual channel trip switches are behind locked cabinet doors. Access keys are controlled by shift supervisor.	If trip can be initiated through any electronic communication links the requirements need to address both physical and electronic access control.
Type of trip indication for bistable trip processor trip.	20		
Ambient Tmax and Tmin 67 to 73 °F	21		Temperature is given for the room. The bistable trip processor will actually experience the internal cabinet temperature, which will be higher.
Ambient pressure slightly positive to slightly negative.	22		
Ambient humidity 10 to 60%.	23		
Ambient radiation dose < 2.5 mRad/hour γ, <1000 Rad γ, total integrated dose.	24		Electronic materials are not susceptible to radiation doses or dose rates in the specified range.
Specification of ambient EMI and RFI.	26		Requirements not stated in FSAR, need to be requested from applicant.
Specification of ambient vibration spectrum.	27		"
Specification of accident temperature.	28		"
Specification of accident pressure.	29		"
Specification of accident humidity.	30		"
Specification of accident fluids and chemicals.	31		"
Accident radiation dose < 2.5 mRad/hour γ. Total integrated dose < 10 Rad.	32		Electronic materials are not susceptible to radiation doses or dose rates in the specified range. The post-accident radiation environment is highest in Rooms C and D because they are closer to the containment.
Seismic vibration spectrum — see Figures B1 and B2.	34	Seismic qualification testing required in accordance with IEEE-344.	Spectra given are floor spectra. These will apply to the cabinet in which the bistable trip processor is located. If processor is separately seismically qualified, then cabinet magnification must be considered.
Power source Vmax and Vmin 117.6 to 122.4 VAC.	43		It is not known if the bistable trip processor is powered by the AC source or by a lower-voltage supply that is powered from this source. If the latter is the case, data specific to the local power source will be needed from the applicant. The 120 VAC source could be from distribution center SA*D401, SB*D401, SC*D401, or SD*D401.

Expected specification requirement	Source (Table B8 row number)	Actual specification requirement	Notes
Power source frequency 60 ± 0.5 Hz.	44		
Specification of power source transients.	45		
Specification of grounding requirements.	46		
Specification of shielding requirements.	47		
Specification of power source qualification requirements.	48		
Specification of power supply total harmonic distortion	49		
Analysis or testing of environmental capability.	21, 22, 23, 24, 26, 27, 28, 29, 30, 31, 32, 34, 43, 44, 49		

Table B9b. Example of review of design basis integrity requirements.

System or subsystem	Engineered safety features actuation
Component	Bistable trip processor

Expected specification requirement	Source (Table B8 row number)	Actual specification requirement	Notes
Redundancy of powers supply to redundant bistable trip processors.	1	System is to be quad-redundant using 2 out of 4 logic. Independent power supply is required for each channel.	
Independence of power supplies to redundant bistable trip processors.	1	System is to be quad-redundant using 2 out of 4 logic. Independent power supply is required for each channel.	
Redundancy of data communications links to redundant bistable trip processors.	2		
Independence of data communications links to redundant bistable trip processors.	2		
Self-test capability of data communications systems.	3	Protection system functions are to be monitored by a separate test processor. Test processor monitors selected data communication links. [7.2.1.1.9]	
Self test frequency of data communications systems.	3		

Expected specification requirement	Source (Table B8 row number)	Actual specification requirement	Notes
Periodic-test capability of data communications systems.	4	Manual testing that confirms appropriate performance when a input test signal varies above and below the trip setpoint. [7.2.1.1.9.2]	
Periodic test frequency of data communications systems.	4	Test interval is quarterly [tech specs]	
Diverse backup for emergency feedwater actuation.	5, 10, 14	Alternate protection system initiation of emergency feedwater [7.7.1.1.11]. Diverse hardware and software used in process component control system [7.7.1.1.11.1].	
Software engineering life cycle for data communications software.	6		
Detailed description of software engineering life cycle activities for data communications software.	6		
Identification of software engineering life cycle design outputs for software engineering life cycle.	6		
Redundancy of bistable trip processors	7, 11	System is to be quad-redundant using 2 out of 4 logic.	
Independence of bistable trip processors	7, 11		
Setpoint control process.	15		
Bistable processors to be located in separate fire areas.	36	Redundant bistable processors are located in separate fire areas.	
Bistable trip processor rooms to have a smoke removal system.	36	Each redundant area is required to have a smoke removal system.	
Fire loading in bistable trip processor rooms minimized by minimizing the amount of cable, using fire-retardant cable, and controlling transient fire loads.	37	Fire loading is minimized by minimizing the amount of cable, using fire-retardant cable, and controlling transient fire loads.	
Fire suppression sprinklers in bypass trip processor rooms .	37	Fire suppression sprinklers required in each redundant area.	
Bistable trip processor to be located in equipment cabinet.	38	Bistable is located in equipment cabinet.	
Bistable trip processor cabinets to have water shields.	38	Equipment cabinet is required to have water shields.	
Bistable trip processor cabinets to be located on a raised base.	38	Equipment cabinet is located on a raised base.	

Appendix C: Example Library of Topics and Topic Taxonomy

Abbreviations:

I&C	Overall I&C System	SW	Software
PPS	Plant Protection System		
		CMF	Common Mode Failure
HW	Hardware	FA	Fault Avoidance
HW-S	Hardware Sense Element	SF	Single Failure
HW-C	Hardware Command Element	FT	Fault Tolerance
HW-E	Hardware Execute Element		
HW-Com	Hardware Communication	ACE	Abnormal Condition or Event
HW-Disp	Hardware Display	PS	Power Supply
		Seis	Seismic
HF	Human Factors	Chem	Chemical

Outline of Topics:

- Functional
  - Overall I&C System
  - Hardware
    - Sense
    - Command
    - Execute
    - Communication
    - Display
  - Software
  - Human Factors
- Integrity
  - Fault Tolerance
  - Fault Avoidance
  - Other

Format for Requirements Data

Guidance on the use of topics

Topic Name	Definition	Attributes	Characteristics	Comments
Dictionary	Define the meaning of the requirement topic. If the topic is defined in existing national or international standards this definition should be used.	Describe the attributes that must be specified for the topic and how they should be specified. Often the attribute is some numerical value must be specified. For example, for maximum normal temperature the attribute is that temperature, typically in degrees C. Other times the attribute is some qualitative description. For the topic of diversity, for example, the types of diversity to be provided should be specified.	Describe how the specific requirements for the topic are derived and how the topic relates to other topics. For example, the topic or response time is related to sample rate and frequency content. The response time can never be faster than the sample rate or1/(max frequency).In fact both of these things should be much shorter (0.1X) the response time.	This area is for any remarks that don't fit the above areas. The groups to which the requirement topic belongs are also listed here for cross-reference. The requirements topic group is use to group topics so that they can be more easily retrieved. A topic may belong to more than one group. A complete cross-reference listing of all groups including this topic is also included.

Functional Requirements

Overall I&C System

Topic Name	Definition	Attributes	Characteristics	Comments
Critical Safety Function	The critical safety functions that must be accomplished by the overall I&C system and the plant protection system	These are pre-defined by NRC as: Reactivity Control, Heat Removal, Primary Cooling System Integrity, Containment, and Radiation Release Monitoring	The critical safety functions are determined from review of the functions assumed by the accident analysis as described in Chapters15 and 6 of the FSAR.	I&C
Response Time	The time required after an abrupt change has occurred in the input quantity to a new constant value until the output of the component has come to rest at its new value (IEEE Std. 559-1985).	The allowable time delay associated with the specific function should be specified		I&C, HW-S, HW-C, HW-E, HW-Disp
System Functions	The names of the specific functions assigned to each system	For each system a list of the system functions should be provided.	I&C system functions may be determined from review of FSAR Chapter7.	I&C
Systems	The names of the systems required to comprise the overall I&C system	Names of the systems	The required systems are determined by review of FSAR Chapter 7. 10 CFR 50 requires provision of a protection system to trip the reactor and initiate operation of engineered safety features	I&C

Functional Requirements
System: Plant Protection System

Topic Name	Definition	Attributes	Characteristics	Comments
Analytical Limit	Parameter value at which the protective function is required to occur	For each protection system parameter the value of parameter assumed in the safety analysis and the process dependent effects that confound the measurement of the parameter should be specified.	The analytical limit is stated in the FSAR accident analysis. The plant set point analysis should also identify the analytical limit and process dependent effects. Each trip set point is related to an analytical limit but the set point accounts for measurement uncertainties and time delays.	PPS
Critical Safety Function	The critical safety functions that must be accomplished by the overall I&C system and the plant protection system	These are pre-defined by NRC as: Reactivity Control, Heat Removal, Primary Cooling System Integrity, Containment, and Radiation Release Monitoring	The critical safety functions are determined from review of the functions assumed by the accident analysis as described in Chapters15 and 6 of the FSAR.	PPS
Direct Parameters	The name of directly measured parameters used by the protection system	The name of each parameter to be directly measured and the associated protection system function(s) should be specified	The measured parameters and their role in performing protection system functions can be determined from review of FSAR Chapter7. These functions should be consistent with the functions assumed by the safety analysis of Chapters 15 and 6.	PPS, HW-C, HW-S

Topic Name	Definition	Attributes	Characteristics	Comments
Frequency Range	The range of frequencies over which the system or component must operate	The maximum and minimum frequency which contain necessary information about each parameter and signal should be specified	The required frequency range is determined by spectral analysis of parameter time histories for normal operations and accident conditions. The required frequency range should include95% of the power for the measured signal. The required frequency range will affect sample rate requirements.	Minimum frequency content may not be important in many cases. PPS, HW-C, HW-S, HW-Com, HW-Disp
Functional bypass permissive conditions	The plant conditions under which it will possible to disable a protective function.	The conditions under which each protection system function may, or must, be disabled should be specified.	The required bypass conditions will be derived from consideration of normal plant operations.	Typically only a few functions will need bypasses. For some plant designs bypasses may not be needed. PPS, HW-S, HW-C, HW-E
Parameter location	The specific location at which a parameter must be measured.	The location where the parameter is measured should be specified.	If the location at which a specific measurement is made is important, this should be indicated in the FSAR safety analysis.	This requirement is of particular importance where there is some spatial dependency in the measurement (flux monitoring for example) PPS, HW-S
Response Time	The time required after an abrupt change has occurred in the input quantity to a new constant value until the output of the component has come to rest at its new value (IEEE Std. 559-1985).	The allowable time delay associated with the specific function should be specified		PPS, HW-S, HW-C, HW-E, HW-Disp

Topic Name	Definition	Attributes	Characteristics	Comments
Signal rate of change	The magnitude of change per unit time that a system or component must accommodate for a specified signal.	The maximum and minimum rate of change of each parameter and signal should be specified.	The specified parameter rate of change should encompass (with margin) the fastest and slowest rate of change associated with normal operations and calculated by the accident analyses of Chapters 15 and 6. Signal rate of change should encompass the rate of change for analog or digital values that equate to the span of the related parameter.	Minimum rate of change may not be important in many cases PPS, HW-S, HW-C, HW-Com, HW-Disp
Signal Span	The algebraic difference between the upper and lower values of a calibrated range (ISA S67.04-1994) required to be measured by the system or component..	For each parameter (process signal), and electrical signal specify the maximum and minimum value which the system must be able to deal with	Parameter spans should encompass (with margin) the normal operating point and the maximum and minimum values of the parameter calculated by the accident analyses of Chapters 15 and 6.Signal spans should encompass the range of analog or digital values that equate to the span of the related parameter.	PPS, HW-S, HW-C, HW-Com, HW-Disp, SW

Topic Name	Definition	Attributes	Characteristics	Comments
Specific functions	Description of the specific functions that a given I&C system must perform	List of functions. For each function the required inputs, and outputs must be specified together with a description of the relationship (transfer function) between the inputs and outputs. The specification should also describe the relationship of each function to the fundamental critical safety functions	The specific protection system functions required can be identified from review of FSAR Chapter 7.These functions should be consistent with the functions assumed in the accident analysis of Chapters 15 and6.	PPS

Functional Requirements

Hardware

Sense Element

Topic Name	Definition	Attributes	Characteristics	Comments
Analytical Limit	Parameter value at which the protective function is required to occur	For each protection system parameter the value of parameter assumed in the safety analysis and the process dependent effects that confound the measurement of the parameter should be specified.	The analytical limit is stated in the FSAR accident analysis. The plant set point analysis should also identify the analytical limit and process dependent effects. Each trip set point is related to an analytical limit but the set point accounts for measurement uncertainties and time delays.	HW-S, HW-C
Communications protocol	The set of rules required of a functional unit to achieve communications with other elements of the system(IEEE-729).	The protocol model should be completely specified. This may be in the form of a protocol specification or a reference to a standard protocol.	The protocol requirements will be a design decision. The specified protocol should be deterministic and for digital communications include effective forms of error detection and correction.	Most directly applicable to digital communications, however there are implicit protocols underlying analog data communications. (e.g.,0 ma = failure, 4 ma = 0% of range, 20 ma = 100% of range) HW-S, HW-C, HW-E, HW-Com, HW-Disp

Topic Name	Definition	Attributes	Characteristics	Comments
Direct Parameters	The name of directly measured parameters used by the protection system	The name of each parameter to be directly measured and the associated protection system function(s) should be specified	The measured parameters and their role in performing protection system functions can be determined from review of FSAR Chapter7. These functions should be consistent with the functions assumed by the safety analysis of Chapters 15 and 6.	HW-S, HW-C, PPS
Electrical connections	The physical characteristics the electrical connections to a component must have in order to function in a system.	The types of physical connections to be used for inputs and outputs should be specified	The electrical connection requirements will be a characteristic of the overall system design.	Electrical connections might include fiber optic. In many cases the specifics of the electrical connection may not be important to safety. HW-S, HW-C, HW-E, HW-Com, HW-Disp
Electrical interface requirements	The electrical characteristics of connections to a component must meet in order to function in the system	The voltage, and current, of inputs and outputs should be specified. For some components the impedance must also be specified.	The electrical interface requirements will be a characteristic of the overall system design.	This category also includes optical connections. HW-S, HW-C, HW-E, HW-Com, HW-Disp

Topic Name	Definition	Attributes	Characteristics	Comments
Frequency Range	The range of frequencies over which the system or component must operate	The maximum and minimum frequency which contain necessary information about each parameter and signal should be specified	The required frequency range is determined by spectral analysis of parameter time histories for normal operations and accident conditions. The required frequency range should include95% of the power for the measured signal. The required frequency range will affect sample rate requirements.	Minimum frequency content may not be important in many cases. HW-S, HW-C, HW-Com, HW-Disp, PPS
Functional bypass permissive conditions	The plant conditions under which it will possible to disable a protective function.	The conditions under which each protection system function may, or must, be disabled should be specified.	The required bypass conditions will be derived from consideration of normal plant operations.	Typically only a few functions will need bypasses. For some plant designs bypasses may not be needed. HW-S, HW-C, HW-E, PPS
Measurement errors	The specified limit on the amount to which an instrument output is in doubt	Reference Accuracy, Environmental errors, (or the Uncertainty, Precision, Drift, allowance made therefore) due to possible errors, either random or systematic, that have not been corrected for (ISAS67.04-1994).	The allowable measurement errors will be assumptions of the plant set point analysis.	See ISA S67.04 for definition of attributes. Measurement errors may include signal processing errors. HW-S, HW-C, HW-Com, HW-Disp
Mounting	The method by which a component is to be attached to plant systems, structures, or other components.	The type of and orientation of the mounting should be specified.	The mounting requirements will depend upon the mechanical environmental hazards seen be the component.	HW-S, HW-C, HW-E, HW-Com, HW-Disp

Topic Name	Definition	Attributes	Characteristics	Comments
Parameter location	The specific location at which a parameter must be measured.	The location where the parameter is measured should be specified.	If the location at which a specific measurement is made is important, this should be indicated in the FSAR safety analysis.	This requirement is of particular importance where there is some spatial dependency in the measurement (flux monitoring for example) HW-S, PPS
Process connection	The required type of connection of an instrument to the measured process.	The physical characteristics of the sensor connection to the process being measured should be specified.	The mounting requirements will depend upon the mechanical environmental hazards seen be the component.	HW-S, HW-E
Response Time	The time required after an abrupt change has occurred in the input quantity to a new constant value until the output of the component has come to rest at its new value (IEEE Std. 559-1985).	The allowable time delay associated with the specific function should be specified		HW-S, HW-C, HW-E, HW-Disp, I&C, PPS
Sense element	The specific measurement technology to be used in measuring a parameter.	What parameter is to be sensed and the technology for sensing should be specified.	The type of element to be used will be determined from the characteristics (both functional characteristics and hazard characteristics) of the process to be measured.	For example level sensor technologies include delta-P, ultrasonic, floats, microwave, heated thermocouple. HW-S

Topic Name	Definition	Attributes	Characteristics	Comments
Signal rate of change	The magnitude of change per unit time that a system or component must accommodate for a specified signal.	The maximum and minimum rate of change of each parameter and signal should be specified.	The specified parameter rate of change should encompass (with margin) the fastest and slowest rate of change associated with normal operations and calculated by the accident analyses of Chapters 15 and 6. Signal rate of change should encompass the rate of change for analog or digital values that equate to the span of the related parameter.	Minimum rate of change may not be important in many cases HW-S, HW-C, HW-Com, HW-Disp, PPS, SW
Signal Span	The algebraic difference between the upper and lower values of a calibrated range (ISA S67.04-1994) required to be measured by the system or component..	For each parameter (process signal), and electrical signal specify the maximum and minimum value which the system must be able to deal with	Parameter spans should encompass (with margin) the normal operating point and the maximum and minimum values of the parameter calculated by the accident analyses of Chapters 15 and 6.Signal spans should encompass the range of analog or digital values that equate to the span of the related parameter.	HW-S, HW-C, HW-Com, HW-Disp, PPS, SW

Functional Requirements
Hardware
Command Element

Topic Name	Definition	Attributes	Characteristics	Comments
Analytical Limit	Parameter value at which the protective function is required to occur	For each protection system parameter the value of parameter assumed in the safety analysis and the process dependent effects that confound the measurement of the parameter should be specified.	The analytical limit is stated in the FSAR accident analysis. The plant set point analysis should also identify the analytical limit and process dependent effects. Each trip set point is related to an analytical limit but the set point accounts for measurement uncertainties and time delays.	HW-S, HW-C
Command functions	The specific functions that a command element is required to perform.	Each specific input and output as well as the command function transfer function(s) that maps inputs to outputs should be specified	The command functions are derived from the high-level system functions for which the command element is responsible. Command functions might include signal conditioning as well as decision functions (set points) of the command elements.	Note signal processing for display elements is considered to be a function of a command element. HW-C, SW

Topic Name	Definition	Attributes	Characteristics	Comments
Communications protocol	The set of rules required of a functional unit to achieve communications with other elements of the system(IEEE-729).	The protocol model should be completely specified. This may be in the form of a protocol specification or a reference to a standard protocol.	The protocol requirements will be a design decision. The specified protocol should be deterministic and for digital communications include effective forms of error detection and correction.	Most directly applicable to digital communications, however there are implicit protocols underlying analog data communications. (e.g.,0 ma = failure, 4 ma = 0% of range, 20 ma = 100% of range) HW-S, HW-C, HW-E, HW-Com, HW-Disp
Direct Parameters	The name of directly measured parameters used by the protection system	The name of each parameter to be directly measured and the associated protection system function(s) should be specified	The measured parameters and their role in performing protection system functions can be determined from review of FSAR Chapter7. These functions should be consistent with the functions assumed by the safety analysis of Chapters 15 and 6.	HW-S, HW-C, PPS
Electrical connections	The physical characteristics the electrical connections to a component must have in order to function in a system.	The types of physical connections to be used for inputs and outputs should be specified	The electrical connection requirements will be a characteristic of the overall system design.	Electrical connections might include fiber optic. In many cases the specifics of the electrical connection may not be important to safety. HW-S, HW-C, HW-E, HW-Com, HW-Disp
Electrical interface requirements	The electrical characteristics of connections to a component must meet in order to function in the system	The voltage, and current, of inputs and outputs should be specified. For some components the impedance must also be specified.	The electrical interface requirements will be a characteristic of the overall system design.	This category also includes optical connections. HW-S, HW-C, HW-E, HW-Com, HW-Disp

Topic Name	Definition	Attributes	Characteristics	Comments
Frequency Range	The range of frequencies over which the system or component must operate	The maximum and minimum frequency which contain necessary information about each parameter and signal should be specified	The required frequency range is determined by spectral analysis of parameter time histories for normal operations and accident conditions. The required frequency range should include95% of the power for the measured signal. The required frequency range will affect sample rate requirements.	Minimum frequency content may not be important in many cases. HW-S, HW-C, HW-Com, HW-Disp, PPS
Functional bypass permissive conditions	The plant conditions under which it will possible to disable a protective function.	The conditions under which each protection system function may, or must, be disabled should be specified.	The required bypass conditions will be derived from consideration of normal plant operations.	Typically only a few functions will need bypasses. For some plant designs bypasses may not be needed. HW-S, HW-C, HW-E, PPS
Measurement errors	The specified limit on the amount to which an instrument output is in doubt	Reference Accuracy, Environmental errors, (or the Uncertainty, Precision, Drift, allowance made therefore) due to possible errors, either random or systematic, that have not been corrected for (ISAS67.04-1994).	The allowable measurement errors will be assumptions of the plant set point analysis.	See ISA S67.04 for definition of attributes. Measurement errors may include signal processing errors. HW-S, HW-C, HW-Com, HW-Disp
Mounting	The method by which a component is to be attached to plant systems, structures, or other components.	The type of and orientation of the mounting should be specified.	The mounting requirements will depend upon the mechanical environmental hazards seen be the component.	HW-S, HW-C, HW-E, HW-Com, HW-Disp

Topic Name	Definition	Attributes	Characteristics	Comments
Response Time	The time required after an abrupt change has occurred in the input quantity to a new constant value until the output of the component has come to rest at its new value (IEEE Std. 559-1985).	The allowable time delay associated with the specific function should be specified		HW-S, HW-C, HW-E, HW-Disp, I&C, PPS
Signal rate of change	The magnitude of change per unit time that a system or component must accommodate for a specified signal.	The maximum and minimum rate of change of each parameter and signal should be specified.	The specified parameter rate of change should encompass (with margin) the fastest and slowest rate of change associated with normal operations and calculated by the accident analyses of Chapters 15 and 6. Signal rate of change should encompass the rate of change for analog or digital values that equate to the span of the related parameter.	Minimum rate of change may not be important in many cases HW-S, HW-C, HW-Com, HW-Disp, PPS, SW
Signal Span	The algebraic difference between the upper and lower values of a calibrated range (ISA S67.04-1994) required to be measured by the system or component..	For each parameter (process signal), and electrical signal specify the maximum and minimum value which the system must be able to deal with	Parameter spans should encompass (with margin) the normal operating point and the maximum and minimum values of the parameter calculated by the accident analyses of Chapters 15 and 6.Signal spans should encompass the range of analog or digital values that equate to the span of the related parameter.	HW-S, HW-C, HW-Com, HW-Disp, PPS, SW

Topic Name	Definition	Attributes	Characteristics	Comments
Synthesized parameters	Identification of virtual parameters to be used by the protection system.	Each synthesized parameter must be identified and described. The parameter description should include identification of directly measured parameters used and the transfer function that maps the directly measured parameters to the synthesized parameter.	The synthesized parameters and their role in performing protection system functions can be determined from review of FSAR Chapter 7.These functions should be consistent with the functions assumed by the safety analysis of Chapters 15 and 6.	Virtual parameters are synthesized from combinations of directly measured HW-C, SW

Functional Requirements

Hardware

Execute Element

Topic Name	Definition	Attributes	Characteristics	Comments
Communications protocol	The set of rules required of a functional unit to achieve communications with other elements of the system(IEEE-729).	The protocol model should be completely specified. This may be in the form of a protocol specification or a reference to a standard protocol.	The protocol requirements will be a design decision. The specified protocol should be deterministic and for digital communications include effective forms of error detection and correction.	Most directly applicable to digital communications, however there are implicit protocols underlying analog data communications. (e.g.,0 ma = failure, 4 ma = 0% of range, 20 ma = 100% of range) HW-S, HW-C, HW-E, HW-Com, HW-Disp
Electrical connections	The physical characteristics the electrical connections to a component must have in order to function in a system.	The types of physical connections to be used for inputs and outputs should be specified	The electrical connection requirements will be a characteristic of the overall system design.	Electrical connections might include fiber optic. In many cases the specifics of the electrical connection may not be important to safety. HW-S, HW-C, HW-E, HW-Com, HW-Disp
Electrical interface requirements	The electrical characteristics of connections to a component must meet in order to function in the system	The voltage, and current, of inputs and outputs should be specified. For some components the impedance must also be specified.	The electrical interface requirements will be a characteristic of the overall system design.	This category also includes optical connections. HW-S, HW-C, HW-E, HW-Com, HW-Disp

Topic Name	Definition	Attributes	Characteristics	Comments
Execute function	The specific output functions that a execute element is required to actuate.	The specific outputs(expressed either as electrical signal outputs, data outputs, or as actuation functions) and the conditions under which these signals are to be generated should be specified		HW-E, SW-C
Functional bypass permissive conditions	The plant conditions under which it will possible to disable a protective function.	The conditions under which each protection system function may, or must, be disabled should be specified.	The required bypass conditions will be derived from consideration of normal plant operations.	Typically only a few functions will need bypasses. For some plant designs bypasses may not be needed. HW-S, HW-C, HW-E, PPS
Mounting	The method by which a component is to be attached to plant systems, structures, or other components.	The type of and orientation of the mounting should be specified.	The mounting requirements will depend upon the mechanical environmental hazards seen be the component.	HW-S, HW-C, HW-E, HW-Com, HW-Disp
Process connection	The required type of connection of an instrument to the measured process.	The physical characteristics of the sensor connection to the process being measured should be specified.	The mounting requirements will depend upon the mechanical environmental hazards seen be the component.	HW-S, HW-E
Response Time	The time required after an abrupt change has occurred in the input quantity to a new constant value until the output of the component has come to rest at its new value (IEEE Std. 559-1985).	The allowable time delay associated with the specific function should be specified		HW-S, HW-C, HW-E, HW-Disp, I&C, PPS

Functional Requirements

Hardware

Communications Element

Topic Name	Definition	Attributes	Characteristics	Comments
Communications media	The material that is required to conduct information between system components.	The type of media and its required physical (size), electrical (impedance ,leakage resistance) or optical (transmissitivity) characteristics should be specified.	The media requirements are largely a design decision. The media requirements and the connection requirements of the connected components must be consistent.	Typically the communications media are copper wire or fiberopitic. HW-Com.
Communications protocol	The set of rules required of a functional unit to achieve communications with other elements of the system(IEEE-729).	The protocol model should be completely specified. This may be in the form of a protocol specification or a reference to a standard protocol.	The protocol requirements will be a design decision. The specified protocol should be deterministic and for digital communications include effective forms of error detection and correction.	HW-DE. Most directly applicable to digital communications, however there are implicit protocols underlying analog data communications. (e.g.,0 ma = failure, 4 ma = 0% of range, 20 ma = 100% of range) HW-S, HW-C, HW-E, HW-Com, HW-Disp
Communications speed	The rate at which data paths are required to carry data. [ANSI/IEEE C37.1]	The maximum required data rate and the conditions under which the rate is measured (e.g. with or without error correction) must be specified.	The specified communication speed must be consistent with other time domain requirements such as delay time, frequency response, and sampling interval.	Digital communications only. HW-Com, SW

Topic Name	Definition	Attributes	Characteristics	Comments
Electrical connections	The physical characteristics the electrical connections to a component must have in order to function in a system.	The types of physical connections to be used for inputs and outputs should be specified	The electrical connection requirements will be a characteristic of the overall system design.	Electrical connections might include fiber optic. In many cases the specifics of the electrical connection may not be important to safety. HW-S, HW-C, HW-E, HW-Com, HW-Disp
Electrical interface requirements	The electrical characteristics of connections to a component must meet in order to function in the system	The voltage, and current, of inputs and outputs should be specified. For some components the impedance must also be specified.	The electrical interface requirements will be a characteristic of the overall system design.	This category also includes optical connections. HW-S, HW-C, HW-E, HW-Com, HW-Disp
Frequency Range	The range of frequencies over which the system or component must operate	The maximum and minimum frequency which contain necessary information about each parameter and signal should be specified	The required frequency range is determined by spectral analysis of parameter time histories for normal operations and accident conditions. The required frequency range should include95% of the power for the measured signal. The required frequency range will affect sample rate requirements.	Minimum frequency content may not be important in many cases. HW-S, HW-C, HW-Com, HW-Disp, PPS

Topic Name	Definition	Attributes	Characteristics	Comments
Measurement errors	The specified limit on the amount to which an instrument output is in doubt	Reference Accuracy, Environmental errors, (or the Uncertainty, Precision, Drift, allowance made therefore) due to possible errors, either random or systematic, that have not been corrected for (ISAS67.04-1994).	The allowable measurement errors will be assumptions of the plant set point analysis.	See ISA S67.04 for definition of attributes. Measurement errors may include signal processing errors. HW-S, HW-C, HW-Com, HW-Disp
Mounting	The method by which a component is to be attached to plant systems, structures, or other components.	The type of and orientation of the mounting should be specified.	The mounting requirements will depend upon the mechanical environmental hazards seen be the component.	HW-S, HW-C, HW-E, HW-Com, HW-Disp
Signal rate of change	The magnitude of change per unit time that a system or component must accommodate for a specified signal.	The maximum and minimum rate of change of each parameter and signal should be specified.	The specified parameter rate of change should encompass (with margin) the fastest and slowest rate of change associated with normal operations and calculated by the accident analyses of Chapters 15 and 6. Signal rate of change should encompass the rate of change for analog or digital values that equate to the span of the related parameter.	Minimum rate of change may not be important in many cases HW-S, HW-C, HW-Com, HW-Disp, PPS, SW

Topic Name	Definition	Attributes	Characteristics	Comments
Signal Span	The algebraic difference between the upper and lower values of a calibrated range (ISA S67.04-1994) required to be measured by the system or component..	For each parameter (process signal), and electrical signal specify the maximum and minimum value which the system must be able to deal with	Parameter spans should encompass (with margin) the normal operating point and the maximum and minimum values of the parameter calculated by the accident analyses of Chapters 15 and 6.Signal spans should encompass the range of analog or digital values that equate to the span of the related parameter.	HW-S, HW-C, HW-Com, HW-Disp, PPS, SW

Functional Requirements

Hardware

Display Element

Topic Name	Definition	Attributes	Characteristics	Comments
Communications protocol	The set of rules required of a functional unit to achieve communications with other elements of the system(IEEE-729).	The protocol model should be completely specified. This may be in the form of a protocol specification or a reference to a standard protocol.	The protocol requirements will be a design decision. The specified protocol should be deterministic and for digital communications include effective forms of error detection and correction.	Most directly applicable to digital communications, however there are implicit protocols underlying analog data communications. (e.g.,0 ma = failure, 4 ma = 0% of range, 20 ma = 100% of range) HW-S, HW-C, HW-E, HW-Com, HW-Disp
Display - Human factors considerations	The human factors conventions to be met by a display.	The display type, location, resolution, size, and labeling should be specified.	NUREG-0700 contains guidance on the specific characteristics that should be specified.	HW-Disp, HF
Displayed parameters	The parameters which are required to be displayed.	The specific parameters (either direct or synthesized) to be displayed should be specified.	Required displayed parameters will be identified by the human factors analysis -in particular the task analysis.	HW-Disp
Electrical connections	The physical characteristics the electrical connections to a component must have in order to function in a system.	The types of physical connections to be used for inputs and outputs should be specified	The electrical connection requirements will be a characteristic of the overall system design.	Electrical connections might include fiber optic. In many cases the specifics of the electrical connection may not be important to safety. HW-S, HW-C, HW-E, HW-Com, HW-Disp

Topic Name	Definition	Attributes	Characteristics	Comments
Electrical interface requirements	The electrical characteristics of connections to a component must meet in order to function in the system	The voltage, and current, of inputs and outputs should be specified. For some components the impedance must also be specified.	The electrical interface requirements will be a characteristic of the overall system design.	This category also includes optical connections. HW-S, HW-C, HW-E, HW-Com, HW-Disp
Frequency Range	The range of frequencies over which the system or component must operate	The maximum and minimum frequency which contain necessary information about each parameter and signal should be specified	The required frequency range is determined by spectral analysis of parameter time histories for normal operations and accident conditions. The required frequency range should include95% of the power for the measured signal. The required frequency range will affect sample rate requirements.	Minimum frequency content may not be important in many cases. HW-S, HW-C, HW-Com, HW-Disp, PPS
Measurement errors	The specified limit on the amount to which an instrument output is in doubt	Reference Accuracy, Environmental errors, (or the Uncertainty, Precision, Drift, allowance made therefore) due to possible errors, either random or systematic, that have not been corrected for (ISAS67.04-1994).	The allowable measurement errors will be assumptions of the plant set point analysis.	See ISA S67.04 for definition of attributes. Measurement errors may include signal processing errors. HW-S, HW-C, HW-Com, HW-Disp
Mounting	The method by which a component is to be attached to plant systems, structures, or other components.	The type of and orientation of the mounting should be specified.	The mounting requirements will depend upon the mechanical environmental hazards seen be the component.	HW-S, HW-C, HW-E, HW-Com, HW-Disp

Topic Name	Definition	Attributes	Characteristics	Comments
Response Time	The time required after an abrupt change has occurred in the input quantity to a new constant value until the output of the component has come to rest at its new value (IEEE Std. 559-1985).	The allowable time delay associated with the specific function should be specified		HW-S, HW-C, HW-E, HW-Disp, I&C, PPS
Signal rate of change	The magnitude of change per unit time that a system or component must accommodate for a specified signal.	The maximum and minimum rate of change of each parameter and signal should be specified.	The specified parameter rate of change should encompass (with margin) the fastest and slowest rate of change associated with normal operations and calculated by the accident analyses of Chapters 15 and 6. Signal rate of change should encompass the rate of change for analog or digital values that equate to the span of the related parameter.	Minimum rate of change may not be important in many cases HW-S, HW-C, HW-Com, HW-Disp, PPS, SW
Signal Span	The algebraic difference between the upper and lower values of a calibrated range (ISA S67.04-1994) required to be measured by the system or component..	For each parameter (process signal), and electrical signal specify the maximum and minimum value which the system must be able to deal with	Parameter spans should encompass (with margin) the normal operating point and the maximum and minimum values of the parameter calculated by the accident analyses of Chapters 15 and 6.Signal spans should encompass the range of analog or digital values that equate to the span of the related parameter.	HW-S, HW-C, HW-Com, HW-Disp, PPS, SW

Functional Requirements
Software

Topic Name	Definition	Attributes	Characteristics	Comments
Command functions	The specific functions that a command element is required to perform.	Each specific input and output as well as the command function transfer function(s) that maps inputs to outputs should be specified	The command functions are derived from the high-level system functions for which the command element is responsible. Command functions might include signal conditioning as well as decision functions (set points) of the command elements.	Note signal processing for display elements is considered to be a function of a command element. HW-C, SW-C
Communications speed	The rate at which data paths are required to carry data. [ANSI/IEEE C37.1]	The maximum required data rate and the conditions under which the rate is measured (e.g. with or without error correction) must be specified.	The specified communication speed must be consistent with other time domain requirements such as delay time, frequency response, and sampling interval.	Digital communications only. HW-Com, SW-Com
Execute function	The specific output functions that a execute element is required to actuate.	The specific outputs(expressed either as electrical signal outputs, data outputs, or as actuation functions) and the conditions under which these signals are to be generated should be specified		HW-E, SW-E
Fault Tolerant Algorithms	Requirements to invoke alternative processing of information when faults are detected.	The types of faults, the means for detecting faults, and the specific algorithm response to the faults should be specified.	The redundancy management topic covers fault tolerance managed by specific hardware devices. This topic relates to schemes embedded in software processes.	SF-FT

Topic Name	Definition	Attributes	Characteristics	Comments
Signal rate of change	The magnitude of change per unit time that a system or component must accommodate for a specified signal.	The maximum and minimum rate of change of each parameter and signal should be specified.	The specified parameter rate of change should encompass (with margin) the fastest and slowest rate of change associated with normal operations and calculated by the accident analyses of Chapters 15 and 6. Signal rate of change should encompass the rate of change for analog or digital values that equate to the span of the related parameter.	Minimum rate of change may not be important in many cases HW-S, HW-C, HW-Com, HW-Disp, PPS, SW
Signal Span	The algebraic difference between the upper and lower values of a calibrated range (ISA S67.04-1994) required to be measured by the system or component..	For each parameter (process signal), and electrical signal specify the maximum and minimum value which the system must be able to deal with	Parameter spans should encompass (with margin) the normal operating point and the maximum and minimum values of the parameter calculated by the accident analyses of Chapters 15 and 6.Signal spans should encompass the range of analog or digital values that equate to the span of the related parameter.	HW-S, HW-C, HW-Com, HW-Disp, PPS, SW

Topic Name	Definition	Attributes	Characteristics	Comments
Synthesized parameters	Identification of virtual parameters to be used by the protection system.	Each synthesized parameter must be identified and described. The parameter description should include identification of directly measured parameters used and the transfer function that maps the directly measured parameters to the synthesized parameter.	The synthesized parameters and their role in performing protection system functions can be determined from review of FSAR Chapter 7.These functions should be consistent with the functions assumed by the safety analysis of Chapters 15 and 6.	Virtual parameters are synthesized from combinations of directly measured HW-C, SW

Functional Requirements
Human Factors

Topic Name	Definition	Attributes	Characteristics	Comments
Design for maintainability	Requirements specified to allow for ease of maintenance.	The human factors criteria to allow for maintenance should be specified.	Ease of maintenance may conflict with other requirements for the ability to withstand harsh environments or for control of access. Appropriate balance must be provided among these conflicting needs.	HF, CMF-FA, SF-FA
Display - Human factors considerations	The human factors conventions to be met by a display.	The display type, location, resolution, size, and labeling should be specified.	NUREG-0700 contains guidance on the specific characteristics that should be specified.	HF, HW-D
Failure Detection	The methods required to allow operators to be aware that failures have occurred.	The types of failures to be detected, the detection methods, the methods for indicating failures, and the criteria for deciding a failure has occurred should be specified	Failure detection requirements may interact with requirements for error checking or testability.	Tech spec surveillance tests are one example of failure detection that must be specified HV, SF-FT,
Human Factors for Operation	Requirements on the design of the user interface	The human factors design criteria should be specified. See NUREG-0700.	Human factors requirements may conflict with requirements for physical and electrical independence. An appropriate balance should be achieved.	HF, CMF-FA, SF-FA

Topic Name	Definition	Attributes	Characteristics	Comments
Maintenance tools	Requirements for special tools to be provided to support monitoring or maintenance of systems or components.	The tools to be provided to ease maintenance (reduce the probability of error during maintenance) should be specified.	The tool requirements should be consistent with the maintenance procedures and the engineered maintenance provisions.	HF
Procedures	Requirements specifying the procedures to be provided	The required operating and maintenance procedures should be specified.	Procedure requirements should be consistent with human factors and maintainability requirements and with the requirements for design features necessary to support procedure implementation.	HF, CMF-FA, SF-FA
Quality process	Requirements on the processes controlling operations or maintenance intended to ensure the system remains in a safe state.	Administrative controls over access, maintenance, modification, periodic maintenance, periodic testing requirements, and configuration management.	The procedure requirements should be consistent with the requirements for design features needed to allow implementation of the procedures.	HF
User qualification	Requirements imposed on user (operator, or maintainer) characteristics to ensure safe operation.	Required skills, knowledge, abilities for users. Required initial training for users. Required periodic training.	User qualification requirements should be consistent with the background and training typical for the user class.	HF, CMF-FA, SF-FA

Integrity Requirements

Fault Tolerance

Topic Name	Definition	Attributes	Characteristics	Comments
Automatic error checking and correction	Required provisions to detect or correct errors in inputs, outputs, or processes.	The type(s) of error checking to be performed, the criteria for determining if an error exists, and the actions to be taken when errors are detected should be specified.	Error checking may sometimes be part of a fault tolerant processing scheme.	Typical error checking schemes include watch dog timers, parity checks, inter-channel comparison, range checking. CMF-FT, SF-FT
Bypass of equipment protections	The requirements specifying the conditions under which equipment protections (i.e., integrity strategies) must be disabled in preference of ensuring continued functionality even for a short period	The protective functions to be bypassed and the conditions under which they maybe bypassed should be specified.	These requirements may conflict with many of the specified integrity strategies. An appropriate balance should be achieved.	SF-FT
Design for predominate failure modes	The requirements specifying the preferred condition to which components fail.	The preferred failure modes and the system actions in the presence of the expected failures should be specified	Redundancy and failure detection should be effective for the preferred failure mode and all other credible failure modes.	CMF-FT, SF-FT
Diversity	Requirements for the provision of diverse functions to compensate for failure, particularly common mode failure	The I&C system functions which must be diverse from each other and the types of diversity to be provided should be specified. NUREG/CR-6303 contains and example list of diversity techniques.		ACE, CMF-FT, SF-FA, ACEs-HW

Topic Name	Definition	Attributes	Characteristics	Comments
Electrical Independence	The provisions made to prevent multiple systems or components from being subject to damage from the same electrical transient on power or signal connections.	Identification of the systems and components (including cabling) that must be electrically independent, the points at isolation is provided, and the type (e.g., optical coupling) and the characteristics of the electrical transients that must be specified	Electrical independence is one of three types of independence that must typically be provided between redundant functions. The others being physical and communications independence.	ACE, CMF-FT, SF-FT, ACEs-HW
Failure Detection	The methods required to allow operators to be aware that failures have occurred.	The types of failures to be detected, the detection methods, the methods for indicating failures, and the criteria for deciding a failure has occurred should be specified	Failure detection requirements may interact with requirements for error checking or testability.	Tech spec surveillance tests are one example of failure detection that must be specified CMF-FT, SF-FT
Fault Tolerant Algorithms	Requirements to invoke alternative processing of information when faults are detected.	The types of faults, the means for detecting faults, and the specific algorithm response to the faults should be specified.	The redundancy management topic covers fault tolerance managed by specific hardware devices. This topic relates to schemes embedded in software processes.	CMF-FT, SF-FT
Physical Independence	The provisions made to prevent multiple systems or components from being subject to damage from the same event.	Identification of the systems and components (including cabling) that must be physically independent and the type (e.g., distance, barriers) and amount of physical separation between to be provided.	Physical independence is one of three types of independence that must typically be provided between redundant functions. The others being electrical and communications independence.	ACE, CMF-FT, SF-FT, ACE-HW

Topic Name	Definition	Attributes	Characteristics	Comments
Redundancy	Requirements for providing multiple (typically identical) components, channels, trains, or systems so that the overall system will tolerate failures.	The functions for which redundancy is required, and the redundancy management scheme(e.g., n/m-voting, fail-over, high select, low select, median select).	When redundancy is specified, independence requirements should also be specified.	The diversity topic covers requirements for redundant, but different systems. Diversity could also be considered as a different independence topic to be associated with the redundancy topic. ACE, SF-FT
Reliability testing and analysis	Requirements on the testing and analyses to be conduced to demonstrate reliability requirements are met	The type of reliability analysis or testing to be conducted and the acceptance criteria should be specified.	The type of analysis or testing should be appropriate for the technology being considered and the acceptance criteria should be within the capability of the analysis or testing technique. Analyses maybe quantitative or qualitative.	CMF-FA, SF-FA, CMF-FT, SF-FT
Unique signals	Requirements for specific signal forms that reduce the likelihood that a specific signal could be generated accidentally.	The signal(s) to be transmitted as a unique signal should be identified and the reasons for requiring uniqueness for the signal should be specified. The degree of uniqueness required should be specified.	Unique signals may be a means for providing noise immunity or fault tolerance under certain specific conditions.	CMF-FA, SF-FA, CMF-FT, SF-FT

Integrity Requirements

Fault Avoidance

Topic Name	Definition	Attributes	Characteristics	Comments
Access Control	The provisions required to prevent unauthorized operation or modification of systems	Measures for control of physical access, measures for control of electronic access to modify data or software via communications systems, and measures of control of electronic access to modify data or software via maintenance provisions should be specified	Access control requirements interact with the physical design of the facility and with maintenance and operating	CMF-FA,SF-FA
Communications Independence	The provisions made to prevent multiple systems or components from being subject to failure from because of failure in communications interfaces or due to shared	Identification of the systems and components (including cabling) that must have communications independence, the points at isolation is provided, and the type (e.g., one-way communications, data validation) and the protocol characteristics that must be provided to prevent propagation of failures via data communication paths.	Communications independence is one of three types of independence that must typically be provided between redundant functions. The others being physical and electrical independence.	SF-FA, CMF-FT, SF-FT, ACEs-HW

Topic Name	Definition	Attributes	Characteristics	Comments
Component Quality	Requirements on specific types of components to be used to enhance reliability or durability	The quality characteristics to be controlled and the processes for controlling quality should be specified.	Component quality requirements interact heavily with process quality requirements. In the limit the component quality requirements may envelop all of the requirement topics. More practically in this context the topic should consider the specific limitations on component selection imposed to assure quality(e.g., use of tantalum vs. Paper electrolytic capacitors or ceramic packaged vs. plastic packaged semiconductors.)	Certain pre-defined quality characteristics and control processes(e.g., MIL-SPEC, NEMA, EIA) might be cited. CMF-FA, SF-FA.
Derating	The margin to be provided between component's maximum operating limits and the nominal operating limits.	The components to be detrated, the type of, and amount of derating to be provided should be specified.	Typically derating will only be specified in requirements for new component designs. However, the amount of derating provided in existing component designs might be considered as part of a component selection process.	To specify derating the technology and the effects of derating on the type of technology must be understood. Note:MIL-HDBK-217 is a source of information about the effect of derating on reliability. CMF-FA, SF-FA.

Topic Name	Definition	Attributes	Characteristics	Comments
Design for maintainability	Requirements specified to allow for ease of maintenance.	The human factors criteria to allow for maintenance should be specified.	Ease of maintenance may conflict with other requirements for the ability to withstand harsh environments or for control of access. Appropriate balance must be provided among these conflicting needs.	CMF-FA, SF-FA
Diversity	Requirements for the provision of diverse functions to compensate for failure, particularly common mode failure	The I&C system functions which must be diverse from each other and the types of diversity to be provided should be specified. NUREG/CR-6303 contains and example list of diversity techniques.		ACE, CMF-FT, SF-FA, ACEs-HW
Environmental Qualification	Requirements on testing and analyses to be performed to confirm that equipment will not fail when exposed to design basis environmental hazards.	The qualification methods for each environment should be specified.	The qualification methods should be appropriate for the environmental hazards specified.	CMF-FA, SF-FA, Seis
Environmental Stress Screening	Requirements on environmental testing to be conducted at or beyond design conditions to screen out infant mortality in components before delivery or installation.	The environmental stress screening conditions and time should be specified.	To specify ESS the technology and the effects of ESS on the type of technology must be understood. Note: ESS has proven a particularly effective strategy for reducing infant mortality.	CMF-FA, SF-FA

Topic Name	Definition	Attributes	Characteristics	Comments
FormalMethods	Requirements on the use of design methods that allow the design to be proven using mathematical methods	The method to specify the requirements and to derive the implementation from the requirements and the method for proving the implementation should be specified.	Formal methods might be applied only to specify and prove certain specific aspects of the design (e.g., logic, timing). Some methods such logic diagrams may achieve the goals of formal methods although they are not generally recognized as formal methods by the research community.	CMF-FA, SF-FA
Functional Qualification (validation)	The testing required to demonstrate that the system or component performs the required functions.	The functional performance to be demonstrated and the method to demonstrate this performance should be specified.	Functional qualification is on aspect of validating product quality.	CMF-FA, SF-FA
Hazard Analysis	The analyses to be performed to determine if a system or component is sufficiently tolerant of failures and external hazards.	The specific set of hazards that the system must operate through should specified and acceptance criteria for the process by which theses hazards are identified should be described.	Hazard analysis may be part of a process quality requirement. Typically, this topic is more germane to systems than to individual components.	CMF-FA, SF-FA, CMF-FT, SF-FT
Human Factors for Operation	Requirements on the design of the user interface	The human factors design criteria should be specified. See NUREG-0700.	Human factors requirements may conflict with requirements for physical and electrical independence. An appropriate balance should be achieved.	CMF-FA, SF-FA

Topic Name	Definition	Attributes	Characteristics	Comments
Inherently safe design	Requirements for design provisions to prevent the system from being inadvertently placed into an unsafe state	The safety principle(s) (e.g., the operator should not be able to enter invalid set points) and the I&C characteristics that implement the safety principle(s) (e.g., range checking on set point inputs) should be specified.	Requirements for inherently safe design may conflict with functional requirements. An appropriate balance should be achieved.	CMF-FA, SF-FA
Maintenance tools	Requirements for special tools to be provided to support monitoring or maintenance of systems or components.	The tools to be provided to ease maintenance (reduce the probability of error during maintenance) should be specified.	The tool requirements should be consistent with the maintenance procedures and the engineered maintenance provisions.	CMF-FA, SF, FA
Noise immunity	The requirements for protection against electromagnetic interference.	Shielding requirements, grounding requirements should be specified.	The noise immunity requirements should be supported by requirements for environmental qualification testing to demonstrate the effectiveness of shielding and grounding.	CMF-FA, SF-FA
Procedures	Requirements specifying the procedures to be provided	The required operating and maintenance procedures should be specified.	Procedure requirements should be consistent with human factors and maintainability requirements and with the requirements for design features necessary to support procedure implementation.	CMF-FA, SF-FA

Topic Name	Definition	Attributes	Characteristics	Comments
Process Quality	The requirements on the process for designing and fabricating systems and components to assure the requirements are met.	Criteria for the design process, V&V requirements, configuration management process, and design analysis (e.g., reliability, safety) should be specified.	Specifications should contain both process quality and product quality requirements. For off the shelf components process quality may be the subject of a commercial dedication review rather than a requirement in the specification, however, specifications should still include a requirement to certify that the component delivered was developed according to the evaluated process.	CMF-FA, SF-FA
Quality process	Requirements on the processes controlling operations or maintenance intended to ensure the system remains in a safe state.	Administrative controls over access, maintenance, modification, periodic maintenance, periodic testing requirements, and configuration management.	The procedure requirements should be consistent with the requirements for design features needed to allow implementation of the procedures.	CMF-FA, SF, FA
Reliability testing and analysis	Requirements on the testing and analyses to be conduced to demonstrate reliability requirements are met	The type of reliability analysis or testing to be conducted and the acceptance criteria should be specified.	The type of analysis or testing should be appropriate for the technology being considered and the acceptance criteria should be within the capability of the analysis or testing technique. Analyses maybe quantitative or qualitative.	CMF-FA, SF-FA, CMF-FT, SF-FT

Topic Name	Definition	Attributes	Characteristics	Comments
System Derating	Requirements that specify operating the system away from the extremes of its	Safety margins to be used in the design and operation should be specified. (e.g., additional margin between set points and analytical limits)	Margins should be greater when the uncertainties in necessary system characteristics are greater.	CMF-FA, SF-FA
Unique signals	Requirements for specific signal forms that reduce the likelihood that a specific signal could be generated accidentally.	The signal(s) to be transmitted as a unique signal should be identified and the reasons for requiring uniqueness for the signal should be specified. The degree of uniqueness required should be specified.	Unique signals may be a means for providing noise immunity or fault tolerance under certain specific conditions.	CMF-FA, SF-FA, CMF-FT, SF-FT
Use of proven technology	Requirements for previous successful use for the components, technologies, or design concepts used in the system.	The areas where use of proven technology is required and the criteria for accepting that technology has been adequately proven should be specified.	Generally the use of technology proven in other applications should be specified and requirements for novel technologies or leaps in performance should not be required.	CMF-FA, SF-FA
User qualification	Requirements imposed on user (operator, or maintainer) characteristics to ensure safe operation.	Required skills, knowledge, abilities for users. Required initial training for users. Required periodic training.	User qualification requirements should be consistent with the background and training typical for the user class.	CMF-FA, SF-FA

Integrity Requirements

Other

Topic Name	Definition	Attributes	Characteristics	Comments
Diversity	Requirements for the provision of diverse functions to compensate for failure, particularly common mode failure	The I&C system functions which must be diverse from each other and the types of diversity to be provided should be specified. NUREG/CR-6303 contains and example list of diversity techniques.		ACE, CMF-FT, SF-FA, ACEs-HW
Electrical energy source	Requirements on the extremes of power supply conditions that must be tolerated.	Over-voltage, Under-voltage, Over-frequency, Under-frequency, Harmonic distortion, loss of phase (single phasing)	These requirements specify the extremes through which components must operate. Requirements for electrical isolation devices specify conditions under which the exposed equipment must fail, but failures must be prevented from propagating between system elements.	PS
Electrical Independence	The provisions made to prevent multiple systems or components from being subject to damage from the same electrical transient on power or signal connections.	Identification of the systems and components (including cabling) that must be electrically independent, the points at isolation is provided, and the type (e.g., optical coupling) and the characteristics of the electrical transients that must be specified	Electrical independence is one of three types of independence that must typically be provided between redundant functions. The others being physical and communications independence.	ACE, CMF-FT, SF-FT, ACEs-HW

Topic Name	Definition	Attributes	Characteristics	Comments
Energy source	Requirements on the allowable, or expected, interruptions of power to the system or component.	Degree of continuity required e.g., normal without back-up, normal with switchover to backup, uninterruptible	Typically protection system equipment will require supply from uninterruptable sources.	PS
Energy source noise	Requirements on the electrical noise that must be tolerated on the power supply inputs	Magnitude and frequency of conducted electromagnetic interference and harmonic distortion	Noise immunity requirements should support meeting energy source noiserequirements.	PS
Environmental Qualification	Requirements on testing and analyses to be performed to confirm that equipment will not fail when exposed to design basis environmental hazards.	The qualification methods for each environment should be specified.	The qualification methods should be appropriate for the environmental hazards specified.	CMF-FA, SF-FA, Seis
Fire Isolation	Requirements on provisions to prevent exposure to fire	The system components that must be protected and the type of protection to be provided should be specified.	Fire isolation requirements should not interfere with provisions for environmental control.	Chem
Fire protection	Requirements for systems and components to be able to withstand operation of fire suppression systems.	The equipment that may be exposed to fire suppression and the nature of the fire suppressant, the exposure duration, and the flood levels expected should be specified.	Fire protection requirements should not defeat environmental control provisions.	Chem

Topic Name	Definition	Attributes	Characteristics	Comments
Physical Independence	The provisions made to prevent multiple systems or components from being subject to damage from the same event.	Identification of the systems and components (including cabling) that must be physically independent and the type (e.g., distance, barriers) and amount of physical separation between to be provided.	Physical independence is one of three types of independence that must typically be provided between redundant functions. The others being electrical and communications independence.	ACE, CMF-FT, SF-FT, ACE-HW
Redundancy	Requirements for providing multiple (typically identical) components, channels, trains, or systems so that the overall system will tolerate failures.	The functions for which redundancy is required, and the redundancy management scheme(e.g., n/m-voting, fail-over, high select, low select, median select).	When redundancy is specified, independence requirements should also be specified.	The diversity topic covers requirements for redundant, but different systems. Diversity could also be considered as a different independence topic to be associated with the redundancy topic. ACE, SF-FT

Appendix D: Derivation of the Structured Approach

Rasmussen's Means-Ends Abstraction Hierarchy with Whole-Parts Decomposition.

In order to develop the total system requirements specification framework, a two-step methodology based on Rasmussen's "*means-ends abstraction hierarchy with whole-parts decomposition*" (MAHWD) was adapted [Rasmussen, 1986; Beltracchi, 1991; Vicente and Bisantz, 1994]. Rasmussen's MAHWD uses two multilevel mechanisms termed "means-ends abstraction hierarchy" and "whole-parts decomposition."

Rasmussen's MAHWD is a systematic, modular, top-down approach which partitions and decomposes high-level system, process, or analysis characteristics (e.g., response time characteristics associated with particular hazards) into lower-level, detailed characteristics and specifications (e.g., software requirements specifications). Thus, it provides a means for documenting the bases for these requirements and specifications in such a way that they are traceable and can more easily be reviewed, verified, and validated. Such an approach when combined with engineering judgement, expert peer reviews, and verification and validation activities, is well suited for the structured approach development since it (1) should help to ensure that a reasonably consistent and complete set of digital protection system requirements is established for software, hardware and human performance characteristics, (2) should provide evidence that a disciplined analysis or development process was used for incorporating digital protection systems into nuclear power plants, and (3) should help to increase the confidence that digital protection systems can achieve their safety objective.

The *means-ends abstraction hierarchy* consists of a five-level, top-down decomposition mechanism with each of the hierarchy levels describing a system or process in terms of a unique attribute(s) (see Table D1). In this hierarchy, the higher levels of the abstraction represent a system or process in terms of purpose or function, whereas the lower levels represent the system in terms of more detailed characteristics or specifications. This forms the first component of Rasmussen's MAHWD.

Table D1. General Means-Ends Abstraction Hierarchy and Its Components

System Decomposition	Whole System	Subsystems	Components	Elements
Functional Purpose	Purpose or goal			
Abstract Function:		First principles		
Generalized Function			General functions	
Physical Function				Characteristics analysis
Physical Form				Detailed characteristics

The five levels of the hierarchy and their definitions are:

(1) the *functional purpose* (the highest level) describes the purpose or goal of the system or process;

(2) the *abstract function* (the second level) describes the intended causal structure of the system or process in terms of first principles;

(3) the *generalized function* (the third level) describes the general functions of the system in terms of key variables;

(4) the *physical function* (the fourth level) describes the deterministic and probabilistic analyses necessary to determine the status/characteristics of components in the system; and

(5) the *physical form* (the lowest level) describes detailed characteristics (i.e., appearance, specifications, magnitudes, probabilities, set points, time responses, etc.) of the system.

Whole-parts decomposition (decomposition) is the process of partitioning of a system or process ("the whole") into a complete set of "parts" based on some logical or convenient characteristic of the system or process. This partitioning creates manageable parts that can more easily be handled. Whole-parts decomposition forms the second component of MAHWD. It is first utilized at the generalized function.

Translation to Engineering Processes for Nuclear Reactors

Rasmussen's process was originally developed for the purpose of specifying human machine interfaces. It can be refined for the task of specifying engineering requirements in nuclear reactor safety systems by adapting the process to the nuclear reactor safety system model. In this study, a means-ends *requirements* hierarchy with whole-parts decomposition is used to develop each of the top level safety goals, plant safety and safety system integrity, because the hazards and the mechanisms of mitigation and defense are different for each. Thus, the result of this process is four distinct but coupled domains:

Plant Safety Domain of Hazards
Plant Safety Domain of Mitigation and Defense
Integrity of Plant Safety Domain of Hazards
Integrity of Plant Safety Domain of Mitigation and Defense

Here, the higher levels of abstraction will represent the system in terms of purpose or functions, whereas lower levels represent the system in terms of more detailed specifications or characteristics.

These domains fit together to allow a complete definition of each reactor safety system. Figure D1 shows how they are used to define a Reactor Trip System. Each of the domains has its own definitions for the levels of the abstraction hierarchy, as summarized in Table D2.

The Whole-Parts Decomposition is the multilevel partitioning which involves the resolution of a system or process into a set of parts that are specific to the system and processes being analyzed. The flow for using the four domains defined above to develop a requirements specification for a Reactor Trip System (RTS) will illustrate the process.

These components of the whole parts decomposition correspond to components in each of the domains described in Table D2 for the system being described. They are illustrated in Table D3.

Table D2. Domain Definitions for the Rasmussen's Means-Ends Abstraction Hierarchy Applied to Nuclear Power Reactors.

System Decomposition	Plant Safety Domain of Hazards	Plant Safety Domain of Mitigation and Defense	Integrity of Plant Safety Systems Domain of Hazards	Integrity of Plant Safety Systems Domain of Mitigation and Defense
Functional Purpose	Evaluate and analyze hazards to define a requirements database for plant safety, a database of hazards	Define safety system requirements	Evaluate and analyze the hazards to a safety system's integrity	Define safety system integrity requirements
Abstract Function:	Analyze events that may lead to an unacceptable release of radiation; use of energy conservation laws as part of the analysis paradigm	Properties of requirements: unambiguous, complete, correct, etc.	Analyze events that may lead to the loss of integrity of the safety system	Properties of requirements: unambiguous, complete, correct, etc.
Generalized Function	Define plant events that challenge critical safety functions	Define performance requirements for safety systems' instrumentation and controls	Define the abnormal conditions and events that challenge safety system integrity: system hazards, environmental hazards, software hazards, hazards due to humans	Define functional performance requirements, safety principles for hardware, software and human activity
Physical Function	Conduct probabilistic and deterministic safety analyses	Design safety algorithms and allocate to hardware, software and humans	Perform probabilistic and deterministic hazards analyses, including analyses of human error	Design performance requirements: allocate functions to hardware, software and humans
Physical Form	Database of hazards containing limiting design basis events	Validate requirements specifications	Database of hazards for safety systems	Validate requirements specifications for hardware, software and human activity

Table D3. Whole Parts Decompositions for the Domain Definitions of Table D2.

Plant Safety Domain of Hazards	Plant Safety Domain of Mitigation and Defense	Integrity of Plant Safety Systems Domain of Hazards	Integrity of Plant Safety Systems Domain of Mitigation and Defense
Reactivity Control	Event A	Hardware Failures	Event A
Radioactivity Effluent Control	Event B	Environmental Hazards	Event B
Primary Containment Integrity	Event C	Human Errors, Design, Development, Operation, Maintenance	Event C
Core Cooling		Energy Source Failures	
Reactor Coolant Pressure Boundary Integrity	(performance designs for dealing with each set of limiting PIEs)		(integrity designs for dealing with each set of Integrity Hazards)

The Control Volume

The concept of a Control Volume (CV) is used in physical analysis to define a space that contains the "system" under analysis, and through which all physical phenomena are controlled, or at least known. The CV defines the (known) boundary conditions for the problem and the "space" in which all relevant equations or relationships are known. The CV will generally be drawn so that it includes all processes of interest in the system or sub-system. Within the CV a physical decomposition of the system is tied to the progression down the abstraction hierarchy, like those shown in the Tables.

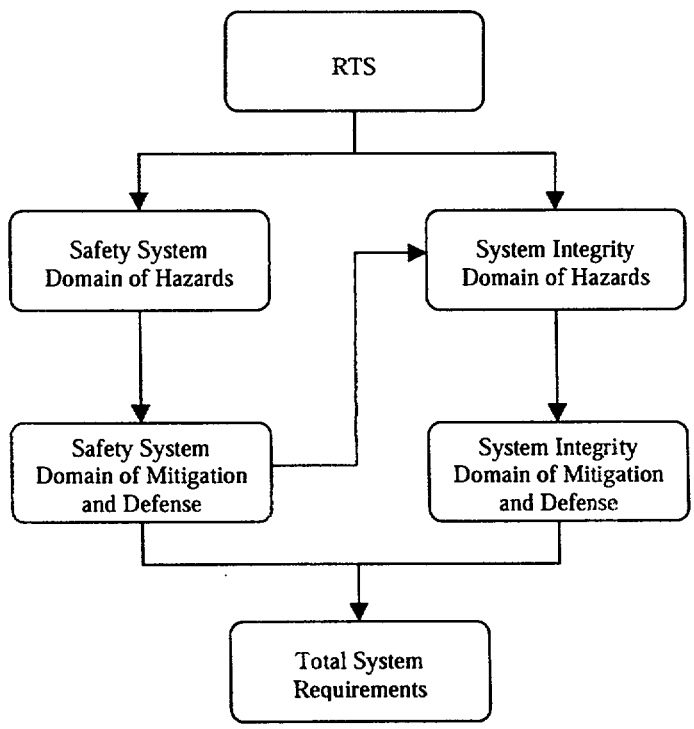


Figure D1. A complete means-ends requirements hierarchy for RTS.

The Model

The equations and relationships of the model on which the analysis is based are used in the Abstract Function of the Plant Safety Domain of Hazards. In order for hazards to be manifest, and for mitigation and defense system requirements to be derived

for them, the hazards must be described by the model defined in the Abstract Function. Alternatively, if a system hazard appears in Design Basis Accidents, LERs or other identified hazard and accident source list, but is not described in the derived hazard database, it must be assumed that an omission or error has occurred in the model or model development.

Translation to NRC Review Processes

In general, in the review of reactor safety systems, the original physics and simulation code used in reactor development is not referenced. Rather, the starting point is the information catalogued in the FSAR and plant design information. This is reflected in a change in the activities at the Generalized Function level of the Means-Ends Hierarchy and the Whole Parts Decomposition. The change is based on the differences in activities between the design process and the regulation process. Here, each requirement imposed by the safety system, whether functional or integrity, must be traceable to an implementation in the system.

This translation is from a nuclear reactor design/definition metaphor to a regulatory one, used by regulators in their assurance process. The differences start to show up at the Generalized Function level, where the function changes from one of "defining" activities to one of "review and identify" activities. The corresponding functions at lower levels change accordingly, as shown in Table D4. It is the functions in the lower three rows of Table D4 that constitute the tables described in the Implementation Section of the report (Section 5).

Table D4. Rasmussen's Means-Ends Abstraction Hierarchy Applied to Nuclear Power Reactor Regulatory Processes.

System Decomposition	Plant Safety Domain of Hazards	Plant Safety Domain of Mitigation and Defense	Integrity of Plant Safety Systems Domain of Hazards	Integrity of Plant Safety Systems Domain of Mitigation and Defense
Functional Purpose	Evaluate and analyze hazards to define a requirements database for plant safety, a database of hazards	Define safety system requirements	Evaluate and analyze the hazards to a safety system's integrity	Define safety system integrity requirements
Abstract Function:	Analyze events that may lead to an unacceptable release of radiation; use of energy conservation laws as part of the analysis paradigm	Properties of requirements: unambiguous, complete, correct, etc.	Analyze events that may lead to the loss of integrity of the safety system	Properties of requirements: unambiguous, complete, correct, etc.
Generalized Function	Review accident analyses to identify PIEs	Identify Safety System Mitigation and Defense Requirements based on their PIE characteristics	Identify the abnormal conditions and events that challenge safety system integrity: system hazards, environmental hazards, software hazards, hazards due to humans	Identify Safety System Integrity Mitigation and Defense Requirements based on their cataloged characteristics
Physical Function	Identify PIE limiting characteristics	Identify component functional requirements	Review the safety system architecture and FSAR to identify the integrity hazard characteristics	Identify the integrity strategy that has been chosen to protect against a chosen integrity hazard
Physical Form	Catalog limiting PIE characteristics	Compare the component specifications to the list of expected requirements	Catalog the integrity hazards to the safety system	Compare the integrity specifications to the requirements derived from the safety analyses

Appendix E: Identification of PIE Characteristics, Protection System Functional Requirements, and Protection System Functional Assignments

1. Implementation of Steps 1 and 2

The analysis was conducted using Amendment 31 of the ABWR Standard Safety Analysis Report as the principle input to the process described in section 5.1, "Identify PIE Characteristics and Protection System Functional Requirements." Since this project was intended to generate requirements for all protection system functions, it was necessary to have a complete list of protection system functions to make sure that we did not inadvertently overlook defining requirements for any function. Therefore, there was an interaction between this step and the identification of protection system functional assignments discussed in section 5.2, "Identify Protection System Functional Assignments." The results of that analysis were fed back into this step to ensure that each protection system function was considered.

The primary FSAR review inputs for identifying requirements applicable to each function are listed below. These inputs are listed roughly in the order of the amount of material used from each section.

Chapter 15,"Accident and Analysis,"
Chapter 16.3.3, "Technical Specifications — Instrumentation,"
Chapter 16.B.3.3, "Technical Specifications Bases —Instrumentation,"
Chapter 7.1, "Instrumentation and Control Systems — Introduction,"
Chapter 7.2, "Instrumentation and Control Systems — Reactor Protection System,"
Chapter 7.3, "Instrumentation and Control Systems — Engineered Safety Features Systems,"
Chapter 6.2, "Engineered Safety Features — Containment Systems,"
Chapter 6.3, "Engineered Safety Features — Emergency Core Cooling Systems,"
Chapter 6.5, "Engineered Safety Features — Fission Products Removal and Control Systems," and
Chapter 5.4, "Reactor Coolant System and Connected Systems — Component and Subsystem Design."
The level-1 tables from this analysis are provided in Appendix A. The level-2 tables are provided in Appendix B.

2. Evaluation of Usability and Completeness, Steps 1 and 2.

The structured approach was able to document the review of PIEs into the level-1 tables. However, the accident analysis does not always unambiguously identify the protective functions assumed. Since in step 2 we needed to map the bounding requirements for each protection system function, it was important that we unambiguously identify each function in our analysis. This required that the reviewer have a good understanding of the protection system functions and functional assignments to understand specifically what functions were

credited as protection for each PIE. To overcome this problem it may be necessary to go back to Step 1 after identifying the requisite protection system functional assignments.

It was difficult to locate information for a number of PIE characteristics. An example of this problem is the time delay allowance for Automatic Depressurization on Low Reactor Vessel Water Level. The safety analysis for this function is discussed in Chapter 6, not Chapter 15 of the FSAR. It proved necessary for reviewer to have a good understanding of the organization of the FSAR and particularly the organization of the chapter 15 material to effectively analyze the PIEs. As a result, less experienced reviewers should spend a few days becoming generally familiar with the FSAR chapters identified above.

It was not possible to locate information for certain PIE characteristics. An example of this problem is the time delay allowance for Main Steam Line Isolation on High Steam Line Flow. Table 15.0-1 gives the allowed time delay as 0 seconds which is unachievable. The actual allowable time delay is unknown, but must be greater than 0. In an actual review the reviewer might chose to review a different PIE for which all information is available, or to request the information from the licensee or applicant.

It was difficult to extract precise information for certain PIE characteristics. An example of this problem is extraction of signal frequency response information. Three issues needed to be overcome. First, the figures in the FSAR are very small; therefore it would difficult to identify fluctuations in the analytical results that would demand very high frequency response by the I&C system. Second, the frequency information in the analytical results has an upper cutoff due to the size of time-step selected when running the analytical codes. Essentially, the thermo-hydraulic analyst has made a decision about frequencies above which the dynamics of the signal are not important, but the structured approach will not give the reviewer any insights about the correctness of this decision. Finally, the transient results in the FSAR are given in a time domain representation. However, the analysis needs frequency domain information. Correctly performing this transformation would require a rather tedious mathematical analysis (or at least a tedious description of the parameter time histories to provide an input for computer analysis) by the reviewer. For this effort we developed a simplified rule of thumb: the maximum frequency content would be taken as 10 times the time interval over which the steepest ramp in the analysis outputs occurs. This was arrived at by assuming that the steepest ramp is the rise of a sawtooth wave, and then picking the cutoff frequency such that $% of the signal power is contained in frequencies below the cutoff. This is a conservative estimate because by assuming a sawtooth wave we maximize the analyzed bandwidth. This, or some similar rule of thumb must be developed for review purposes.

The information in the safety analysis is sometimes not specific to the requirements for the instrumentation and control system. An example of this problem is the response time for reactor trip on Main Steam Line Isolation Valve Closure. The allowed time delay for rod insertion can be deduced as 3.71 seconds from examining Table 15.0-1 together with Table 15.0-6. The allocation of this time delay between the rod drop time, scram discharge system time, and instrumentation delay time cannot be determined, however.

The structured approach was adequate to document the bounding PIE characteristics applicable to each protection system function in the level-2 tables. Many of the protection

system functions, however, are not explicitly discussed in the safety analysis. Therefore, we could not extract functional requirements for these protection system functions.

3. Implementation of Step 3

The analysis was conducted using Amendment 31 of the ABWR Standard Safety Analysis Report as the principle input to the process described in section 5.2, "Identify Protection System Function Assignments." The primary FSAR review inputs, listed roughly in the order of the amount of material used from each section, were:

- Chapter 16.B.3.3, "Technical Specifications Bases — Instrumentation,"
- Chapter 16.3.3, "Technical Specifications — Instrumentation,"
- Chapter 7.1, "Instrumentation and Control Systems — Introduction,"
- Chapter 7.2, "Instrumentation and Control Systems — Reactor Protection System," and
- Chapter 7.3, "Instrumentation and Control Systems — Engineered Safety Features Systems."

These sources of information were used to develop a table of systems, functions, and related PIEs to help in the identification of functions credited in the Accident Analyses. As a discussion of each function was encountered in the accident analysis, this fact was noted and the completed table was used to check that PIE information had been gathered for each unique combination of PIE and associated protection function. The result is shown in Table E1. This information was encoded in the level-1 and level-2 tables in the appendices using system, sub-system identification numbers. Therefore, there is no need to produce separate level-3 tables for this example. These tables are provided in Appendix A.3.

4. Evaluation of Usability and Completeness, Step 3

It is evident from Table E1 that the Chapter 15 accident analysis does not provide insight into the requirements for a large number of protective functions. There appear to be two reasons why these are not explicitly discussed. First, the function is not needed as a primary protection against any event and is provided primarily for functional diversity; second, the function is assumed to actuate in concert with other functions that are discussed. Containment isolation, for example, is assumed to initiate at the same time as several other functions such as low pressure flood. In these cases the associated function dictates most of the parameter characteristics for the functions that are not explicitly discussed. Certain characteristics, most notably the allowed time delay, must be inferred by the analyst. Generally, the requirements can be presumed to be relatively non-demanding. For the containment isolation example it can be reasonably presumed that the time delay of any practical I&C system would be much longer than the allowed delay time.

Reviewers may choose to give review emphasis to the functions credited in the safety analysis, in which case the lack of information on the back-up functions is unimportant. Otherwise, reviewers will need to consult more detailed licensee documents for information on the required characteristics for these functions. The implicitly assumed functions should have most of the same required characteristics as the driving functions that are discussed in the accident analyses. The structured approach needs to inform users about how to handle these two

situations. For the implicitly credited functions, the structured approach should caution reviewers to account for the few characteristics that will be unique to these functions.

Table E1. Allocation of Protective Functions to PIEs and to Systems

		SSLC														
			ESFAS													
		RPS											Other ESF			
	Systems	RPS	ECCS				Isolation									
	Subsystems	N/A	LPFL	RCIC	HPCF	ADS	MSIV	Contain	RCIC	CUW	SCSI	Diesel	SGTS	RCW/RSW	CAMS	SPC
1a	Startup Range Neutron Monitor - Neutron Flux - High	N														
1b	Startup Range Neutron Monitor - Neutron Flux - Short period	A														
2a	APRM - High Setdown	A														
2b	APRM - Simulated Thermal Power High	A														
	Recirculation Flow (part of APRM STP)	N														
2e	Rapid Core Flow Decease	A														
2f	Oscilation Power Range Monitor	N														
2g	APRM ATWS ADS Permissive (low APRM & Leve<1.5)					N										
3	Reactor Vessel Steam Dome Pressure - High	N	N							N	N					
4	Reactor Vessel Steam Dome Pressure - Low		A													
5	Reactor Vessel Water Level - High, Level 8			N (shut)	N (shut)											
6	Reactor Vessel Water Level - Level 3	A						N			N		N			
7	Reactor Vessel Water Level - Level 2			A				N		N						
8	Reactor Vessel Water Level - Level 1.5				A		N					N				
9	Reactor Vessel Water Level - Level 1		A			A		N				N		N	N	
10	Main Steam Isolation Valve - Closure	A										A	N	N	N	
11	Drywell Pressure - High	N	N	N	N	N		N								
12	CRD Water Header Charging Pressure - Low	N														
13	Turbine Stop Valve - Closure	A														
14	Turbne Control Valve Fast Closure, Trip Oil Pressure - Low	A														
15	Main Steam Tunnel Radiation - High	N					N									
16	Supression Pool Temperature - High	A														A
17	Condensate Storage Tank Level - Low			N	N											
18	Supression Pool Water Level - High			N	N											
19	Main Steam Line Pressure - Low						A									
20	Main Steam Line Flow - High						A									
21	Condenser Vaccum - Low						A									
22	Main Steam Tunnel Temperature - High						N			N						
23	Main Turbine Area Temperature - High						N									
24	Reactor Building / Fuel Handling Area, Exhaust Air Radiation - High							N					N			
25	RCIC Steam Line Flow - High								N							
26	RCIC Steam Supply Line Pressure - Low								N							
27	RCIC Equipment Area Temperature - High								N							
28	RHR Area Temperature - High										N					
29	CUW Dufferential Flow - High									N						
30	CUW Area Temperature - High								N	N						
	RHR Pump Discharge Pressure High				N											
	HPCF Pump Discharge Pressure - High				N											

A Function Considered in Accident Analysis

ESFAS Engineered Safety Features Actuation System

RCW Reactor Building Cooling Water

ADS Automatic Depressurization System
CAMS Containment Atmosphere Cleanup System
Contain Containment Isolation
CUW Reactor Water Cleanup System
ECCS Emergency Core Cooling System
HPCF High Pressure Core Flooder
LPFL Low Pressure Flooder
MSIV Main Steam Isolation Valve
N Function not Considered in Accident Analysis
RCIC Reactor Core Isolation Cooling
RPS Reactor Protection System
RSW Reactor Service Water
SCSI Shutdown Cooling System Isolation
SGTS Standby Gas Treatment System
SPC Suppression Pool Cooling
SSLC Safety System Logic Control

Table E2. Example of a PIE Characteristic

Entry	Data	Notes
PIE Name	Pressure Regulator Fails Open	Ref: 15.1.3
Initial Condition	Standard	Ref: 15.0.1
Protective Function	18 Reactor Vessel Water Level - Level 2	Ref: Chap16 - B3.3.1.1- Function 7
Time Delay	14.2 sec	Ref: T15.1-7
Variable Range	MAX Variable Range: 1.9 m	Ref: Figure 15.1-5. Value extracted from the figure 15.1-5
Variable Range	MIN Variable Range: -2 m	Ref: Figure 15.1-5. Minimum value was estimated keeping the gradient of the two portions in the graph and extrapolating. Considered WR sensed level
MAX Rate Change	0.5 m/sec	Ref: Figure 15.1-5
Analytical Limit	-0.75 m	Ref: T 15.0-1, item 32, m above bottom of separator
Frequency Spectrum	MAX Freq Spectrum: 10 Hz	Ref: Figure 15.1-5
	MIN Freq Spectrum: 0 Hz (assumed)	Ref: Figure 15.1-5

Table E3. Limiting System Functional Characteristics

Entry	Data	Notes
System Name	Engineered Safety Feature Actuation	
Subsystem Name	RCIC Initiation	
Protective Function	18 Reactor Vessel Water Level - Level 2	Chap16 - B3.3.1.1- Function 7
Response Time	7.4 sec	Ref Table 15.2-9, RCIC is initiated approximately 7.4 secs after four RIP are tripped. This time includes the actual delay time for RCIC
MIN Variable	-2 m	Figure 15.2-12, Figure 15.2-5
MAX Variable	1.9 m	Ref: Figure 15.1-5
Bounding Rate	2	Ref: Figure 15.2-11
Bounding Analytical Limit	-1	Ref Table 15.0-1 item 32, Reference point: above bottom of separator skirt
MIN Freq	0 Hz (assumed)	Ref: Figure 15.1-5
MAX Freq	7 Hz	Ref: Figure 15.2-12

Glossary

Abnormal conditions or events (ACEs). As defined in this report represent hazards (usually physical faults) that occur during activities in the operation phase of hardware (e.g., single-point failure), software (e.g., common-mode failure) or human performance life cycles (e.g., errors of omission), and those that normally emerge from environmental causes (e.g., EMI/RFI) and energy sources (e.g., external power grid failure) [IEEE Std. 7-4.3.2, 1993 and Lawrence and Gallegher, 1997].

Abstract variable. As defined in this report, represents general[2] variables (e.g., mass flow rates) derived from the mathematical equations for the conservation laws.

Accident. An undesired or unplanned event that results in a specified level of loss [Leveson, 1995].

Analytical limits. Bounds placed on important plant process variables associated with plant safety hazards to ensure that a safety limit is not exceeded [ANSI/ISA-S67.04-Part 1, 1994 and Draft Reg. Guide DG-1045, 1997]

Analog (technology). A device that represe`nts data by a continuously variable quantity [NAS, 1997].

Anticipated transients without scram (ATWS). 10 CFR 50.62 dictates that (1) each PWR manufactured by Combustion Engineering and Babcock and Wilcox have a diverse scram system independent of the existing reactor trip system and (2) each BWR have an alternative rod injection system (ARI) that is diverse and independent of the existing reactor trip system [Section 7, NUREG-0800, 1997].

Accuracy. The degree of freedom error of sensor and operator input, the degree of exactness exhibited by an approximation or measurement, and the degree of freedom from error of actuator output [Appendix 7-C, NUREG-0800, 1997].

Common-cause failure. Multiple component failures having the same cause [NAS, 1997].

Common-mode failure. The failure of multiple components in the same way. Both common-cause and common-mode failures arise when the assumption of independence of the failures of the components is violated. Common-mode failures are a concern when the failures occur concurrently or at least sequentially in a time frame before the minimum number of components required for system integrity recover [NAS, 1997].

---

[2] General is used to indicate that the variables do not have a specific reactor component name attached to their description.

Computer. Used broadly in this document to refer to any device that includes digital hardware (e.g., microprocessors), software, and interfaces [IEEE Std. 7-4.3.2, 1993].

Complete. A requirement is complete if, and only if, it includes all the necessary requirements [IEEE Std. 830, 1993].

Configuration management. A discipline applying technical and administrative direction and surveillance to: identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status, and verify compliance with specified requirements [IEEE Std. 610.12, 1990].

Consistent. A requirement is consistent if, and only if, no subset of individual requirements described in it conflict [IEEE Std. 830, 1993].

Correct. A requirement is correct if, and only if, every requirement stated therein is one that the hardware, software, and/or human will meet [IEEE Std. 830, 1993].

Data communication systems. Systems that transmit signals between systems and between components of systems. Data communication systems may include analog and digital multiplexes as well as non-multiplexed transmission. Where such systems are included in a design, they support one or more of the I&C systems [Appendix 7-C, NUREG-0800, 1997].

Design acceptance criteria. A set of prescribed limits, parameter, procedures, and attributes upon which the NRC relies in making a final safety determination to support design certification when detailed design information is not available [Appendix 7-C, NUREG-0800, 1997].

Defense-in-depth. The conservative design approach that uses multiple, layered systems to provide alternative means of accomplishing different functions related to common goals. This approach provides added protection against natural phenomena and plant operational transients and accidents [NAS, 1997].

Degree of stability. Stability can be expressed in terms of the number of expected changes to any requirement based on experience or knowledge of forthcoming events that affect the organization, functions, and people supported by the software system [IEEE Std. 830, 1993].

Design basis. Information on plant functional components and their response to a set of postulated failure scenarios [NAS, 1997].

Design faults. Faults committed during the original design or during subsequent modifications, which cause the system that is actually implemented to be different from that which was intended. Design faults can be contrasted with physical faults [NAS, 1997].

Digital safety systems. Those digital systems relied upon to remain functioning during and following design basis events to ensure (a) the integrity of the reactor coolant pressure boundary, (b) the capability to shut down the reactor and maintain it in a safe shutdown

condition, or (c) the capability to prevent or mitigate the consequences of accidents that could result in potential off-site exposures comparable to those described in the 10 CFR 100 guidelines [IEEE Std. 603, 1991].

Digital (technology). A technology that represents data by a combination of discrete digits, such as 0's and 1's [NAS, 1997].

Diversity. The use of two or more mutually exclusive means of performing the same function. There are several kinds of diversity:

- **Design diversity.** The use of two or more components with a different internal design to accomplish the same function [NAS, 1997].
- **Functional diversity.** The use of two or more components to achieve different component functions, although the functions may be related in terms of higher-level functions and requirements [NAS, 1997].
- **Nameplate diversity.** The use of components from different manufacturers to accomplish the same function [NAS, 1997]
- **Cognitive diversity.** The use of different personnel to perform different tasks [NUREG/CR-6303, 1994]

Electromagnetic interference (EMI). Electromagnetic disturbances which manifest themselves in performance degradation, malfunction, or electrical failure [EPRI TR-102348, 1993].

Energy sources. As defined in this report, represents sources of energy such as power and cooling supply used to support the proper functioning of a system.

Engineered safety features actuation system. A system that actuates engineered safety features (ESF) components to prevent or mitigate damage to the reactor core, the reactor coolant pressure boundary, and ensure containment integrity [Section 7, NUREG-0800, 1997].

Errors of commission. Incorrect performance of a task or action

Errors of omission. Failure to perform a task or action.

Environmental qualification. A set of testing and certification procedures to ensure the operation of nuclear components in anticipated environmental conditions [NAS, 1997].

Final safety analysis report (SAR). The formal documentation of the basis for licensing a nuclear power plant.

Five critical safety functions. The five functions that must be maintained for safety generally accepted by the nuclear power industry [Reg. Guide 1.97, 1980]. They include:

- **reactivity control.** Control of undesired changes in the neutron population,
- **core cooling.** Control of undesirable decreases or losses of energy transfer from the reactor core,
- **radioactivity effluent control.** Control of undesirable increases in radioactive effluent at planned plant release points,

- **reactor coolant pressure boundary integrity**. Control of undesirable pressure loss at the reactor's coolant pressure boundary, and
- **primary containment integrity**. Control of losses of containment vessel integrity.

Formal methods. Methods that include the use of requirement specification languages or special mathematical representations to reduce ambiguity; They can make incomplete and inconsistent requirements easier to recognize [Leveson, 1994; Leveson, 1996; Section 7.1 and Appendix 7-A, NUREG-0800, 1997].

Functional requirement. A requirement that specifies what function(s) a system or system component must perform. [Appendix 7-C, NUREG-0800, 1997].

Fundamental physics quantities. As defined in this report represent neutrons, mass, and energy.

Handshake. A four-step process of linked acknowledgments between a sender and a receiver used to transmit data or signals reliably. A handshake involves a signal that (1) initiates the transaction (from the initiating member of a pair), (2) accepts the transaction (from the passive member), (3) terminates the transaction (from the initiator), and (4) acknowledges the termination and readiness for another transaction (from the passive member) [Appendix 7-C, NUREG-0800, 1997].

Hazard. A state or set of conditions of a system that, together with other conditions in the environment of the system, will inevitably lead to an accident [Leveson, 1995].

Hardware. Physical equipment used to process, store, or transmit computer programs or data [IEEE Std. 610.12, 1990].

Hardware life cycle. Includes [ANSI/IEEE Std. 1002, 1987]:

- **Requirements**
- **Design**
- **Integration**
- **Testing**
- **Installation**
- **Operation**
- **Maintenance**
- **Retirement**

Human error probability (HEP). The probability that a human will mak an error when performing a task, or will fail to perform the task or some of its elements.

Implementation (as a software life-cycle process planning characteristic). Those characteristics of planning documents that describe the work necessary to achieve the purpose of the planning documents. The implementation characteristics of software life-cycle plans discussed in BTP HICB-14 are: measurement, procedures, record keeping, and schedule [Appendix 7-C, NUREG-0800, 1997].

Independence (non-interacting or non-interfering components). A set of components has "statistical independence" when the joint probability of a compound event among the set of components equals the product of the probabilities of the individual events that make up the compound event [NAS, 1997].

Instrumentation and control (I&C). Systems that provide plant monitoring, control, and protection functions in nuclear power plants [NAS, 1997].

Integrity design strategies (IDSs). As defined in this report represent functional implementation such as redundancy to used to mitigate ACEs such as single-point failures, functional diversity to mitigate common-mode failures, or shielding to reduce the effects of EMI/RFI.

Integrity hazard. An undesirable event that causes loss of function of the system that responds to a system hazard [IEEE Std. 7-4.3.2, 1993].

Integrity process development assurance strategy (IPDAS). As defined in this report represents quality-based procedural capabilities [NIST, 1994] such as:

(1) quality assurance, project management, verification and validation (includes tests), configuration management, test and maintenance training and procedures, and best-practice engineering practices used to plan, monitor, manage, direct, and document the design and development processes for software and hardware,

(2) training, operating procedures, and performance monitoring used to teach and direct operators,

(3) environmental qualification, and

(4) energy sources procedures used to reduce the incidence of errors.

IPDAS also include administrative controls to prevent unauthorized changes from being introduced through a human-machine interface. Note that this is similar to the situation that is faced now with existing equipment and the associated administrative controls and IEEE Std. 603 provides guidance on access control and human interfaces. Administrative controls should specifically address software access in addition to typical equipment access provisions.

Integrity process development hazards (IPDHs). As defined in this report represents errors that usually occur during all phases of the life cycle of the digital safety system (e.g., requirements specification errors and software testing errors) [NIST, 1994].

Integrity requirements. Constraints that specify quantities such functional diversity in software or electromagnetic interference (EMI) / radio frequency interference (RFI) compatibility of hardware that ensures the functional performance of a digital safety system despite hazards to its integrity [IEEE 7-4.3.2, 1993].

Interface. A shared boundary across which information is passed [IEEE Std. 610.12, 1990]

Inventories. As defined in this report represents the storage of fundamental physics quantities in a control volume.

Limiting[3] plant safety hazards. The limiting cases of initiating events[4] (e.g., a control rod ejection that produces the fastest response time that threaten the five critical safety functions that must be maintained in order to ensure plant safety [Reg. Guide 1.97, 1980].

Limiting Nyquist signal frequency response. As defined in this report represents the highest signal response frequency for an important plant process variable as a result of a plant safety hazard.

Limiting response time. As defined in this report represents the shortest or fastest response time for an important plant process variable to reach an analytical limit as a result of a plant safety hazard.

Limiting variable range. As defined in this report represents the highest or the lowest value of an important plant process variable (i.e., extreme values) associated with a plant safety hazard.

Man-machine interface. All interfaces between the digital system and plant personnel, including operators, maintenance technicians, and engineering personnel [EPRI TR-102348, 1993].

Means-ends abstraction hierarchy. Consists of a five-level, top-down decomposition mechanism with each of the hierarchy level describing a system or process in terms of a unique attribute(s) [Vicente and Bisantz, 1994]. The five levels of the hierarchy are:

(1) the *functional purpose* (the highest level of abstraction), which describes the purpose or goal of a system or a process;

(2) the *abstract function* (the second level of abstraction), which describes the causal structure of the system or process in terms of first principles or laws that govern the behavior of the system or process;

(3) the *generalized function* (the third level of abstraction), which describes generic functions associated with the functional purpose or goals of the system or process;

(4) the *physical function* (the fourth level of abstraction), which describes the deterministic and probabilistic analyses necessary to characterize the functions in the generalized function of the hierarchy; and

---

[3] Limiting implies bounding or worst cases of the plant safety hazards which must be designed for to ensure that all plant safety hazards can be mitigated.

[4] Hazards and initiating events are used interchangeably in the structured approach.

(5) the *physical form* (constituting the output of abstraction), which catalogs in a database the detailed characteristics or specifications (e.g., requirements specifications, probabilities, set points, and response times) of the functions in the generalized function.

Memory sharing. The use of common memory storage for different functions that use a common historical database [NAS, 1997].

Modifiable. A requirement is modifiable if, and only if, its structure and style are such that any changes to the requirements can be made easily, completely, and consistently while retaining the structure and style [IEEE Std. 830, 1993].

Multiplexing. Transmission of data signals across shared pathways. A multiplexer is a digital switch that connects data from one of many sources to its output [NAS, 1997].

Multitasking. "Simultaneous" execution of several tasks (processes) on a single computer. The operating system controls the switching between the different tasks [NAS, 1997].

Performance requirements. As defined in this report represents constraints that specify quantities such as response time, speed, accuracy, or memory usage with which digital safety systems or their components must perform their digital safety system functions [IEEE Std. 610.12, 1990; IEEE Std. 603, 1991; IEEE Std. 7-4.3.2, 1993].

Plant process variables. Variables such as mass flow rate or neutron flux used to characterize a reactor's behavior [Reg. Guide 1.70, 1978 and ANS/ANSI-4.5, 1980].

Plant safety hazards. Initiating events that threaten the five critical safety functions that must maintain in order to assure plant safety [Reg. Guide 1.97, 1980].

Physical faults. Faults that occur during operation and are caused by internal or external physical phenomena (wear-out electromagnetic perturbations, temperature, vibration, etc.). Physical faults are sometimes called random faults, and can be contrasted with design faults [NAS, 1997].

Probabilistic risk assessment (PRA). An analysis method used to (a) assess the relative frequency and consequences of postulated events and, (b) search for design weaknesses, and identify and assess the frequency and associated risk of improbable events which are beyond the plant design basis [NAS, 1997].

Radio-frequency interference (RFI). A form of electromagnetic disturbance restricted to about 10 kHz to 50 kHz [EPRI R TR-102348, 1993].

Reactor protection system (RPS). A set of plant components that initiate rapid and complete response actions in response to plant transients and accidents to bring the reactor to a safe condition [NUREG-0800, 1997]

Reactor trip system (RTS). A system that shuts the reactor down in order to protect against gross damage to the fuel cladding or loss of primary system integrity which could lead to release of radioactive material to the containment [Section 7, NUREG-0800-1997].

Real-time processing. A mode of operation in which a computation is performed during the actual time that an external process occurs [IEEE Std. 610.12, 1990].

Ranked for importance and/or stability. A requirement is ranked for importance and/or stability if each requirement in it has an identifier to indicate either the importance or stability of that particular requirement. Typically, all of the requirements that relate to a software product are not equally important. Some requirements may be essential, especially for life-critical applications, while others may be desirable. Each item in the Requirements should be identified to make these differences clear and explicit [IEEE Std 830, 1993].

Redundancy. The use of identical or diverse items to provide alternative means of performing a required function in the event of failure of an individual item [NAS, 1997].

Reliability. The probability that a component will perform its intended function satisfactorily for a prescribed time and under stipulated environmental conditions [Leveson, 1995].
Safety limits. Bounds placed on important plant process variables associated with plant safety hazards and necessary to protect the integrity of the physical barriers (i.e., fuel, the reactor vessel and the primary containment) that guard against uncontrolled release of radioactivity [10 CFR 50.36, 1995].

Safety (and nonsafety) systems. Those systems relied upon to remain functioning during and following design basis events to ensure (a) the integrity of the reactor coolant pressure boundary, (b) the capability to shut down the reactor and maintain it in a safe shutdown condition, or the capability to prevent or mitigate the consequences of accidents that could result in potential off-site exposures comparable to those described in the 10 CFR 100 guidelines [IEEE Std. 603-1991].

Security. The ability to prevent unauthorized, undesired, and unsafe intrusions [Appendix 7-C, NUREG-0800, 1997].

Self-test. A test or series of tests, performed by a device upon itself. Self-test includes on-line continuous self-diagnostics, equipment-initiated self-diagnostics, and operator-initiated self-diagnostics [Appendix 7-C, NUREG-0800, 1997].

Separation. Physical or functional independence of systems [NAS, 1997].

Software. Computer programs, procedures, and possibly documentation and data pertaining to the operation of a computer system [ANSI/IEEE Std. 610.12, 1990].

Software Life cycle. Includes [ANSI/IEEE Std. 1002, 1987]:

- **Requirements**
- **Design**
- **Coding**

- **Integration**
- **Testing**
- **Installation**
- **Operation**
- **Maintenance**
- **Retirement**

Software quality assurance. Development processes and standards that attempt to produce software with certain specified qualities [NAS, 1997].

Software specification. A description of a piece of software which is a basis for its design and implementation.

Sinks. As defined in this report represent the transfer of fundamental physics quantities out of a control volume or the destruction of fundamental physics quantities in a control volume.

Sources. As defined in this report represent the transfer of fundamental physics quantities into a control volume or involve the production of fundamental physics quantities in a control volume.

Standard Review Plan (SRP). A set of guidance documents used by NRC reviewers to determine what is needed from the licensee to assess the adequacy of a proposed design and what represents a satisfactory method of complying with the licensing requirements. Regulatory acceptance criteria, branch technical positions, regulatory guides, and industry standards provide additional, more detailed guidance.

System. An integrated composite that consists of one or more of the processes, hardware, software, facilities and people, that provides a capability to satisfy a stated need or objective [ISO/IEC 12207, 1995].

System integrity. A system's ability to satisfy a stated need or objective in an environment of hazards [Leveson, 1995].

Traceable. A requirement is traceable if the origin of each of its requirements is clear and if it facilitates the referencing of each requirement in future development or enhanced documentation [IEEE Std. 830, 1993].

Unambiguous. A requirement is unambiguous if, and only if, every requirement stated therein has only one interpretation. As a minimum, this requires that each characteristic of the final product be described using a single unique term. The requirements should be unambiguous both to those who create it and to those who use it [IEEE Std. 830, 1993].

Verification and validation. The process of determining whether a product at each stage of the system design process fulfills the requirements imposed by the previous design stage (verification) and the test and evaluation of the integrated system design to ensure compliance with the functional, performance, and interface requirements as specified in the system functional requirements (validation) [IEEE 7-4.3.2, 1993; IEEE Std. 610.12, 1990].

Verifiable. A requirement is verifiable if, and only if, every requirement stated therein is verifiable. A requirement is verifiable if, and only if, there exists some finite cost-effective process by which a person or machine can check that the software product meets the requirement [IEEE Std. 830, 1993].

Whole-parts decomposition. As defined in this report represents the partitioning of a system or process ("the whole") into a complete set of constituents or well-defined and understood "parts" based on some logical or convenient characteristic of the system or process. This partitioning creates manageable parts that can more easily be handled.