NUREG/CR-6680
UCRL-ID-139344

# Review Templates for Computer-Based Reactor Protection Systems

Lawrence Livermore National Laboratory

**U.S. Nuclear Regulatory Commission**
**Office of Nuclear Regulatory Research**
**Washington, DC 20555-0001**

## AVAILABILITY OF REFERENCE MATERIALS IN NRC PUBLICATIONS

### NRC Reference Material

As of November 1999, you may electronically access NUREG-series publications and other NRC records at NRC's Public Electronic Reading Room at www.nrc.gov/NRC/ADAMS/index.html.
Publicly released records include, to name a few, NUREG-series publications; *Federal Register* notices; applicant, licensee, and vendor documents and correspondence; NRC correspondence and internal memoranda; bulletins and information notices; inspection and investigative reports; licensee event reports; and Commission papers and their attachments.

NRC publications in the NUREG series, NRC regulations, and *Title 10, Energy,* in the Code of *Federal Regulations* may also be purchased from one of these two sources.

1. The Superintendent of Documents
   U.S. Government Printing Office
   P. O. Box 37082
   Washington, DC 20402–9328
   www.access.gpo.gov/su_docs
   202–512–1800
2. The National Technical Information Service
   Springfield, VA 22161–0002
   www.ntis.gov
   1–800–533–6847 or, locally, 703–805–6000

A single copy of each NRC draft report for comment is available free, to the extent of supply, upon written request as follows:
Address: Office of the Chief Information Officer,
Reproduction and Distribution
Services Section
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
E-mail: DISTRIBUTION@nrc.gov
Facsimile: 301–415–2289

Some publications in the NUREG series that are posted at NRC's Web site address www.nrc.gov/NRC/NUREGS/indexnum.html are updated periodically and may differ from the last printed version. Although references to material found on a Web site bear the date the material was accessed, the material available on the date cited may subsequently be removed from the site.

### Non-NRC Reference Material

Documents available from public and special technical libraries include all open literature items, such as books, journal articles, and transactions, *Federal Register* notices, Federal and State legislation, and congressional reports. Such documents as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings may be purchased from their sponsoring organization.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at—
The NRC Technical Library
Two White Flint North
11545 Rockville Pike
Rockville, MD 20852–2738

These standards are available in the library for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from—
American National Standards Institute
11 West 42nd Street
New York, NY 10036–8002
www.ansi.crg
212–642–4900

The NUREG series comprises (1) technical and administrative reports and books prepared by the staff (NUREG–XXXX) or agency contractors (NUREG/CR–XXXX), (2) proceedings of conferences (NUREG/CP–XXXX), (3) reports resulting from international agreements (NUREG/IA–XXXX), (4) brochures (NUREG/BR–XXXX), and (5) compilations of legal decisions and orders of the Commission and Atomic and Safety Licensing Boards and of Directors' decisions under Section 2.206 of NRC's regulations (NUREG–0750).

**DISCLAIMER:** This report was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any employee, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus, product, or process disclosed in this publication, or represents that its use by such third party would not infringe privately owned rights.

NUREG/CR-6680
UCRL-ID-139344

# Review Templates for Computer-Based Reactor Protection Systems

Manuscript Completed: July 2000
Date Published: August 2000

Prepared by
G. Johnson, LLNL and University of California at Berkeley
D. Schrader, LLNL
R. Yamamoto, University of California at Berkeley

Lawrence Livermore National Laboratory
7000 East Avenue
Livermore, CA 94550

University of California
Berkeley, CA 94720

R. Brill, NRC Project Manager

**Prepared for**
**Division of Engineering Technology**
**Office of Nuclear Regulatory Research**
**U.S. Nuclear Regulatory Commission**
**Washington, DC 20555-0001**
**NRC Job Code W6677**

## Disclaimer

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

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

# ABSTRACT

This report provides review templates to help ensure the completeness and traceability of protection system requirements specifications. The templates identify safety important characteristics of reactor protection systems and the hardware and software components that comprise typical computer-based protection systems. The templates include checklists that are used to verify that important safety characteristics are specified in the requirements documents for protection system components, and that the specified characteristics are consistent with the plant safety analysis.

# CONTENTS

# TABLES

# FIGURES

# EXECUTIVE SUMMARY

Instrumentation and control systems provide monitoring, control, and protection functions in nuclear power plants. Most existing nuclear power plant instrumentation and control systems were designed using analog devices. Digital systems offer several advantages over existing analog systems. For example, digital systems are essentially free of the drifts associated with analog systems, have higher data handling and storage capabilities, and provide improved system performance in terms of accuracy and computational capabilities. However, systems engineering methods have not been developed to ensure that nuclear power plant protection system and software requirements are complete, consistent, and correct. Frequently, the cause of software requirements errors can be traced to incomplete or incorrect system requirements.

This report provides review templates to help ensure the completeness and traceability of protection system requirements specifications. The templates identify safety important characteristics of reactor protection systems and the hardware and software components that comprise typical computer-based protection systems. The templates include checklists that are used to verify that important safety characteristics are specified in the requirements documents for protection system components, and that the specified characteristics are consistent with the plant safety analysis.

These templates provide one tool to support specification reviews. They should be used in conjunction with other requirements review methods. Since the templates provide a static view, methods applicable to review of dynamic behavior are recommended for use in conjunction with the templates. The construction of sequence diagrams, state diagrams, or use case diagrams are example of techniques applicable to the review of dynamic characteristics.

This report describes the processes used to identify typical protection system components and to develop the templates. It also discusses the use of the templates to review specifications, and provides guidance on developing new templates. A complete set of templates in the form of Quattro Pro workbooks is provided on CD-ROM included with this report.

# ACKNOWLEDGMENT

The authors wish to thank and acknowledge the efforts of Mr. Bob Brill from the Nuclear Regulatory Commission who guided the project, reviewed this work and provided insights and comments. The authors also wish to thank Mr. Ray Berg of Sandia National Laboratory who laid the groundwork for much of this project and who gave structure to requirement topic categories

# REVIEW TEMPLATES FOR COMPUTER-BASED REACTOR PROTECTION SYSTEMS

## 1. INTRODUCTION

### 1.1 Background

Instrumentation and control systems provide monitoring, control, and protection functions in nuclear power plants. Most existing nuclear power plant instrumentation and control systems were designed using analog devices. However, parts for these analog systems are becoming unavailable due to obsolescence and their maintenance costs are increasing, so nuclear utilities are upgrading to digital systems. Digital systems offer several advantages over existing analog systems. For example, digital systems are essentially free of the drifts associated with analog systems, have higher data handling and storage capabilities, and provide improved system performance in terms of accuracy and computational capabilities. As would be expected, new technologies bring new challenges that must be considered, such as sampling rate considerations, cycle times, discreteness of monitored parameters, greater susceptibility to environmental effects, and guaranteeing high computer software quality.

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. This is of particular concern for computer-based systems because application of the technology to reactor safety systems is relatively new. Widely accepted proven design solutions have not yet emerged, and software requirements must be more carefully specified since software implementations are not bounded by physical laws.

### 1.2 Problem

Systems engineering methods have not been developed to ensure that nuclear power plant protection system and software requirements are complete, consistent, and correct. Studies indicate that the majority of all software errors are caused by incorrect or incomplete system requirements.

### 1.3 NRC Need

Section 7 of the Standard Review Plan (SRP) for nuclear power plants states the need to review requirements at various levels. However, acceptance criteria for these reviews are very high-level, requiring mainly completeness and consistency, with little specific guidance on how to determine if these characteristics have been achieved. Yet, in reviewing such systems NRC must address several new considerations such as sampling effects, cycle times, discreteness of monitored parameters, and computer software quality.

### 1.4 Overview of Project

This report presents a review tool developed to assist in the evaluation of requirements documents for reactor protection systems (RPSs), RPS devices, and RPS software. This tool provides a form for evaluating the forward tracability of protection system requirements to confirm that these requirements consistent with the commitments and assumptions of the plant safety analysis. These safety analysis assumptions and commitments, along with certain decisions made in the design process do necessarily directly translate into hardware and software requirements. Instead they impose constraints which must be addressed by the requirements in lower level documents. The review tool described in this document identifies typical protection system components. For each component type, the tool identifies the typical safety-related characteristics, and source of safety constraints that each characteristic must meet. It is intended that reviewers will use the tools to identify and record safety constraints on component requirements as a basis for reviewing component requirement specifications. Specification requirements are then compared against the safety constraints to confirm that safety analysis commitments and assumptions have been appropriately addressed in the requirements specifications.

The tool consists of a set of review templates for typical types of protection system components. The templates are composed of a checklist of characteristics that should be addressed in RPS specifications, definitions of these characteristics, and references to where a reviewer may find that safety constraints that must be addressed in specifying these characteristics. Templates are provided for the overall protection system specification, as well as specifications of hardware and software components that are included in typical modern protection system designs. These templates provide one tool to support specification reviews. They should be used in conjunction with other requirements review methods. Since the templates provide a static view, methods applicable to review of dynamic behavior are recommended for use in conjunction with the templates. The construction of sequence diagrams, state diagrams, or use case diagrams are example of techniques applicable to the review of dynamic characteristics.

To develop the templates, current computer-based protection systems were examined in order to create a class diagram that identifies typical protection system components. A class diagram shows the protection system structure in terms of classes of components, including how the classes relate to each other. The class diagram for this project was based upon the protection system architectures for the Advanced Boiling Water Reactor [GE 1993], System 80+ [CE 1994], and Siemens Teleperm XS [Erin 1998].

Each class of components was described in terms of the component attributes and behaviors important to safety. *Attributes* describe the static characteristics of a component (e.g., the power supply characteristics needed by a physical device), while *behaviors* describe the dynamic performance (e.g., the fluid pressure to current transformation performed by a pressure sensor). The catalog (or requirements topics) developed in the previous work [Berg 1999] and included in this report as Appendix C was used to help identify the typical attributes and behaviors of protection system components. Two system-level standards — IEEE Std. 603 [IEEE 1991] and IEEE Std. 7-4.3.2 [IEEE 1993] — were reviewed to confirm that the safety attributes covered in these standards were addressed. The protection system design information from the three systems identified above was also reviewed to confirm that safety-important component behaviors were identified. A set of review templates was developed, one set for each component.

Each review template is a QuatroPro workbook containing three spreadsheets. One spreadsheet identifies and defines the safety characteristics important for the subject component

A second spreadsheet in each template identifies the likely source of safety constraints on the requirements for the subject component. Safety analysis assumptions, regulatory requirements, environmental conditions, and interfacing systems place constraints upon the attributes and behaviors of each specific protection system component. These constraints are different depending upon the role of the component in plant safety. A reviewer can use these spreadsheets to understand the attributes and behaviors that should be addressed by requirements specifications, and to find the constraints imposed by the safety analysis assumptions, the safety analysis commitments, and the safety analysis results.

A third spreadsheet is provided for the reviewer's use in documenting his or her evaluation. It provides a place to record the safety constraints applicable to the component, document where the constraint was found, list the corresponding specification requirement, and cite the location of the requirement. A reviewer should normally find that all attributes and behaviors have been addressed in the component's requirements document, and that each requirement is consistent with the corresponding safety constraint. A contrary finding is a matter for further investigation.

Tables 1, 2, and 3 (grouped at the end of Section 1) provide an example of a review template. The shaded rows of these spreadsheets provide header information or identify logical groupings of requirements topics. They are not separate characteristics that need to be addressed separate from the assessment of the individual characteristics identified in the group. Section 3 of this report describes the spreadsheets in more detail. Note that the example in figure 1 does not include all of the expected behaviors for protection systems. The complete forms of these tables are provided in Appendix A.

## 1.5 Relationship to Previous Work

This project was initiated in response to work done by Leo Beltracchi of the Nuclear Regulatory commission to apply a means–ends-hierarchy approach to the specification of nuclear power plan instrumentation and control safety systems [Beltracchi 1996]. Previously, Rasmussen [1987] had proposed developing system requirements by beginning with an abstract definition of system purpose and then, through a series of steps, decomposing the abstract purpose into progressively more concrete and explicit terms until a complete and unambiguous specification is obtained. This "structured approach" was intended to ensure completeness of requirements specifications and provide visible traceability between detailed specifications and high-level functional requirements.

Sandia National Laboratory (SNL) developed an initial version of the structured approach incorporating the ideas of Beltracchi and Rasmussen [Staple 1997]. In parallel with this effort Lawrence Livermore National Laboratory (LLNL) examined existing system engineering approaches and standards to develop issues to be considered in reviewing the Sandia approach [Scott 1997]. After the initial SNL and LLNL efforts were completed, the NRC refocused the effort toward developing a review method that could be used by NRC staff. SNL and LLNL collaborated in recasting the structured approach to this effect [Berg 1998]. LLNL, in collaboration with the University of California at Berkeley (UCB), performed a trial application of this method to the Advanced Boiling Water Reactor (ABWR) protection systems [Johnson 1999].

The trial application revealed that using the structured approach lead to a thorough review of the design issues for the plant protection systems, and highlighted areas for further investigation that may not have been identified in a more casual review. It was also found, however, that implementing the structured approach is very resource-intensive because the approach's attempt to establish "forward traceability" requires an exhaustive search of documentation for fundamental requirements in order to develop a basis for specification review. A "reverse traceability" review would be equally effective at finding incorrect requirements, but less effective at detecting incomplete requirements. Consequently, LLNL proposed that a more practical tool would be to develop a set of review templates using concepts from the structured approach. The templates would identify the critical requirement topics that the reviewer expects specifications to cover. The structured approach process (for extracting protection system functional requirements based upon accident analysis assumptions and results) would be used in a simplified form to perform trace audits of functional requirements. Integrity requirement checklists could be developed based upon the guidance of IEEE Std. 603, IEEE Std. 7-4.3.2, and their supporting standards. Generic checklists could be developed for typical protection system architectures and design elements. Such checklists would address most systems because using the IEEE standards is essentially mandated by 10 CFR 50.55a(h), and considerable commonality exists between the system architectures from the various vendors. The templates would assist reviewers in confirming that system and component specifications are consistent with the requirements of 10 CFR 50.55a(h) (IEEE Std. 603 as supplemented by IEEE Std. 7-4.3.2). These templates would be used to conduct reviews in accordance with SRP Section 7.1-C.

LLNL's proposals for modifying the structured approach were accepted and the modifications discussed above were incorporated [Brill 1999]. This report describes the how the templates were developed, and provides the templates for the review of typical protection system components.

## 1.6 Terminology

Several terms are used with specific meanings in this report.

Protection systems: Those I&C systems which initiate safety actions to mitigate the consequences of design basis accidents. The protection systems include the reactor trip system (RTS) and the engineered safety features actuation system (ESFAS). [NUREG-0800]

Component: A physical part of a system that performs some function. It may be implemented either in hardware or software. This term is not intended to refer by itself to any specific level of system decomposition. It may refer to a part as big as the entire system itself, or to a part as small as an executable software module with identity and a well-defined interface. (This extends the definition of (software) component in OMG 1997]

Class: A description of a set of components or systems that share the same characteristics. [OMG 1997] A class may be directly instantiated as a specific system or component. A class may also describe abstract objects that will never physically exist as components but are useful for organizing characteristics that are common to a group of classes.

Characteristic: A feature or property of a system, component, or class. Characteristics may be either static properties, attributes, dynamic properties, or behaviors. This report is concerned with safety-important characteristics — those features or properties that a component or system must have to reliably perform its safety function.

Attribute: A static characteristic of a component, system, or class.

Behavior: A dynamic characteristic of a component, system, or class.

Constraint: A semantic restriction or condition. [OMG 1997] Within the context of the review templates constraints define restrictions on the characteristics of a component that must be met in order for the component to reliably perform its safety function. The basic goal of the review templates is to provide a tool to help a reviewer confirm that specifications address all safety important characteristics, and address them in a way that the safety constraints are met.

## Table 1. Example Definitions of Expected Attributes and Behaviors

System Requirements Specification

| Attributes | Definition |
|---|---|
| *Safety Classification* | *The system safety classification (e.g., safety, important to safety)* |
| Failure Avoidance | |
| Functional Qualification | The testing and analyses required to demonstrate the system performs the required functions |
| Control of Access | The provisions for preventing unauthorized access to equipment or controls. |
| Restrictions on sharing between units | The limitations of using system functions or equipment to perform functions in more than one unit. |
| Human Factors | The requirements imposed upon the human machine interface. Typically a reference to NUREG-0700. |
| Reliability Goals | The qualitative or quantitative goals for probability of the system performing protective actions on demand. |
| Reliability Analysis Requirements | The testing and analyses required to demonstrate reliability goals are met. |
| Failure Tolerance | |
| Redundancy | Requirements for providing multiple components, channels, trains, or systems |
| Diversity | Requirements for the provision of diverse functions to compensate for failure, particularly common mode failure |
| Failure Mode | The state to which functions should preferentially fail |
| Failure Isolation | |
| Electrical Independence | The provisions made to prevent propagation of failures between redundant functions along electrical connections |
| Physical Independence | The provisions made to prevent failure of redundant functions because of common equipment locations |
| Control Protection Isolation | The provisions made to prevent failures from both causing accidents and disabling the protective system response |
| Behaviors | |
| Protective Actions () | The initiation of a signal for the purpose of accomplishing a safety function. |
| Function Name | The identification of the function under review. |
| Inputs | |
| Parameter | The parameters or set of parameters to be measured |
| Measurement Location | The location at which each parameter is to be measured |
| Span | The difference between the maximum and minimum values to be measured. |
| Rate of Change | The magnitude of change per unit time that the system must accommodate for a specified signal |
| Frequency Content | The signal bandwidth that must be maintained in the measurement |
| *Spatial Dependency* | *Number & locations of measurements needed (most often used for core flux or temperature measurements)* |
| Manual Controls | Manual inputs to the functions |
| Process | |
| Actuation Algorithm | The relationship between input and the trip/no-trip conditions. Typically a constant with hysteresis. Sometimes a function of other parameters. |
| Initialization / Reset Mode | The condition that the function assumes upon startup or energization - both initially and after reset. |
| Outputs | |
| Outputs | The output signals or commands to be provided by the system |
| Completion of Protective Action | The point at which the function is considered to be complete and may be reset. |
| Displays | The information about the function to be displayed to operators |
| Performance | |
| Uncertainty | The allowable about by which the channel output is in doubt. Typically includes accuracy, environment effects, drift, etc. |
| Response Time | The time required after an abrupt change input until the output comes to rest a its new value |
| Update Rate | The time required to obtain a collection of data |
| Operational Bypass Functions () | Inhibition of the capability to accomplish a safety function that could otherwise occur in response to a particular set of generating conditions. |
| Function Name | The identification of the function under review. |
| Inputs | |
| Permissive Parameter | The parameters or set of parameters to be measured |
| Measurement Location | The location at which each parameter is to be measured |
| Span | The difference between the maximum and minimum values to be measured. |
| Rate of Change | The magnitude of change per unit time that the system must accommodate for a specified signal |
| Frequency Content | The signal bandwidth that must be maintained in the measurement |
| Spatial Dependency | Number & locations of measurements needed (most often used for core flux or temperature measurements) |
| Manual Controls | Manual inputs to the functions. Typically the controls to manually trip or actuate safety functions. |
| Process | |
| Bypass Algorithm | The relationship between input and the trip/no-trip conditions. Typically a constant with hysteresis. Sometimes a function of other parameters. |
| Initialization / Reset Mode | *The condition that the function assumes upon startup or energization - both initially and after reset.* |
| Outputs | |

## Table 2. Example Constraints on Attributes and Behaviors

System Requirements Specification

| Attributes | Typical Source of Constraints | Typical Location of Constraints | Comments |
|---|---|---|---|
| Safety Classification | 10 CFR 50, IEEE 603 Sec 5.12 | SAR Ch. 7.1 | Protection systems and auxiliary features must be safety |
| Failure Avoidance | | | |
| Functional Qualification | 10 CFR 50 Appendix B, Sec III | SAR Ch. 7.1, 7.2, 7.3 | |
| Control of Access | IEEE 603 Sec. 5.9 | SAR Ch. 7.1, 7.2, 7.3 | |
| Restrictions on sharing between units | IEEE 603 Sec. 5.13 | SAR Ch. 7.1, 7.2, 7.3 | |
| Human Factors | IEEE 603 Sec 5.14 | SAR Ch. 18 | |
| Reliability Goals | GDC 21, GDC 29, IEEE 603 Sec. 5.5 | SAR Ch. 7.1, 7.2, 7.3, 19 | May be quantitative or qualitative |
| Reliability Analysis Requirements | IEEE 603, Sec. 5.15 | SAR Ch. 7.2, 7.3 | |
| Failure Tolerance | | | |
| Redundancy | IEEE 603 Sections 5.1 | SAR Ch. 7.1, 7.2, 7.3 | |
| Diversity | DID&D Analysis, IEEE 603 Sec. 5.16 | SAR Ch. 7.1, 7.2, 7.3, 7.8 | DID&D analysis should conform with SECY 93-087 |
| Failure Mode | GDC 23 | SAR Ch. 7.1, 7.2, 7.3 | |
| Failure Isolation | | | |
| Electrical Independence | IEEE 603, Sections 5.6 | SAR Ch. 7.1, 7.2, 7.3 | |
| Physical Independence | IEEE 603, Sections 5.6 | SAR Ch. 7.1, 7.2, 7.3 | |
| Control Protection Isolation | GDC 24, IEEE 603, Sections 6.3 | SAR Ch. 7.1, 7.2, 7.3 | |
| Behaviors | | | |
| Protective Actions () -- Each function described in the SAR should be specified. Typically the function may be supported by a process control and measurement diagram or a logic diagram. | | | |
| Function Name | Accident analysis assumptions | SAR Ch. 7.2, 7.3, 15 | |
| Inputs - For manual functions only the manual controls item is germane | | | |
| Parameter | Accident analysis assumptions, IEEE 603 Sec 6.4 | SAR Ch. 15 | Parameters shall be direct measures where feasible and practical |
| Measurement Location | Accident analysis assumptions | SAR Ch. 7.2, 7.3, 15 | Unnecessary if parameter measurement is insensitive to location |
| Span | Accident analysis results (bounds of accident and normal values) | SAR Ch. 15 | |
| Rate of Change | Accident analysis results (measured from transient curves) | SAR Ch. 15 | |
| Frequency Content | Accident analysis results (calculated from transient curves) | SAR Ch. 15 | |
| Spatial Dependency | Accident analysis assumptions | SAR Ch. 7.2, 7.3, 15 | Typically important only for neutron monitoring. |
| Manual Controls | IEEE 603 Section 6.2 | SAR Ch. 7.1, 7.2, 7.3 | |
| Process | | | |
| Trip Algorithm | Accident analysis assumptions | SAR Chapter 15 | Typically bistable decision |
| Initialization / Reset Mode | SRP | SAR Ch. 7.1, 7.2, 7.3 | |
| Outputs | | | |
| Outputs | Accident analysis assumptions | SAR Ch. 7.1, 7.2, 7.3, 15 | |
| Completion of Protective Action | IEEE 603, Section 5.2 | SAR Ch. 7.1, 7.2, 7.3 | |
| Displays | | SAR Ch. 7.1, 7.2, 7.3, 18 | |
| Performance | | | |
| Uncertainty | Accident analysis assumptions | SAR Chapter 15 | |
| Response Time | Accident analysis assumptions | SAR Chapter 15 | |
| Update Rate | Accident analysis results (calculated from transient curves) | SAR Ch. 15 | Update rate must be fast enough to be consistent with these. |
| Operational Bypass Functions () -- For each function the following constraints should be considered | | | |
| Function Name | Identifier Only | SAR Ch. 7.1, 7.2, 7.3 | |
| Inputs | | | |
| Permissive Parameter | Accident analysis assumptions | SAR Ch. 15 | Bypasses will typically be implemented using a sensor channel |
| Measurement Location | Accident analysis assumptions | SAR Ch. 7.2, 7.3, 15 | that is also used for a trip function. In these cases, the input |

## Table 3. Example Review Checklist

System Requirements Specification

| Attributes | Safety Constraint | Source | Actual Requirement | Source | Constraints Met? | Comments |
|---|---|---|---|---|---|---|
| *Safety Classification* | | | | | | |
| Failure Avoidance | | | | | | |
| Functional Qualification | | | | | | |
| Control of Access | | | | | | |
| Restrictions on sharing between units | | | | | | |
| Human Factors | | | | | | |
| Reliability Goals | | | | | | |
| Reliability Analysis Requirements | | | | | | |
| Failure Tolerance | | | | | | |
| Redundancy | | | | | | |
| Diversity | | | | | | |
| Failure Mode | | | | | | |
| Failure Isolation | | | | | | |
| Electrical Independence | | | | | | |
| Physical Independence | | | | | | |
| Control Protection Isolation | | | | | | |
| Behaviors | | | | | | |
| Protective Actions ( ) -- For each function the following constraints should be considered | | | | | | |
| Function Name | | | | | | |
| Inputs | | | | | | |
| Parameter | | | | | | |
| Measurement Location | | | | | | |
| Span | | | | | | |
| Rate of Change | | | | | | |
| Frequency Content | | | | | | |
| Spatial Dependency | | | | | | |
| Manual Controls | | | | | | |
| Process | | | | | | |
| Actuation Algorithm | | | | | | |
| Initialization / Reset Mode | | | | | | |
| Outputs | | | | | | |
| Outputs | | | | | | |
| Completion of Protective Action | | | | | | |
| Displays | | | | | | |
| Performance | | | | | | |
| Uncertainty | | | | | | |
| Response Time | | | | | | |
| Update Rate | | | | | | |
| Operational Bypass Functions ( ) -- For each function the following constraints should be considered | | | | | | |
| Function Name | | | | | | |
| Inputs | | | | | | |
| Permissive Parameter | | | | | | |
| Measurement Location | | | | | | |
| Span | | | | | | |
| Rate of Change | | | | | | |
| Frequency Content | | | | | | |
| Spatial Dependency | | | | | | |
| Manual Controls | | | | | | |
| Process | | | | | | |
| Bypass Algorithm | | | | | | |
| Initialization / Reset Mode | | | | | | |
| Outputs | | | | | | |

# 2. PROTECTION SYSTEM MODEL

To develop the templates, actual computer-based protection systems were used to create a class diagram that identified typical protection system components. This class diagram described the generic structure of typical protection systems. Class diagrams show the structure of a system in terms of the classes of components that comprise the system, and illustrate how these classes relate to each other. They are useful for studying the types of components that may be encountered in the review of protection system requirements, and also help to describe the sets of requirements that may be common to many components. The structure of the class diagram is described in more detail below.

## 2.1 Class Diagrams

Each part of the protection system can be modeled as a member of a class of objects that have similar characteristics. Characteristics are divided into two types: attributes, which describe static characteristics, and behaviors, which describe the dynamic characteristics. This is shown graphically in a three-section box (Figure 1). The top section contains the name of the class of components, the middle section lists the static attributes of those components (e.g., environmental qualification requirements), and the third section lists the behaviors (functions) of the components. Sometimes just the top section of the box is used to represent a class.

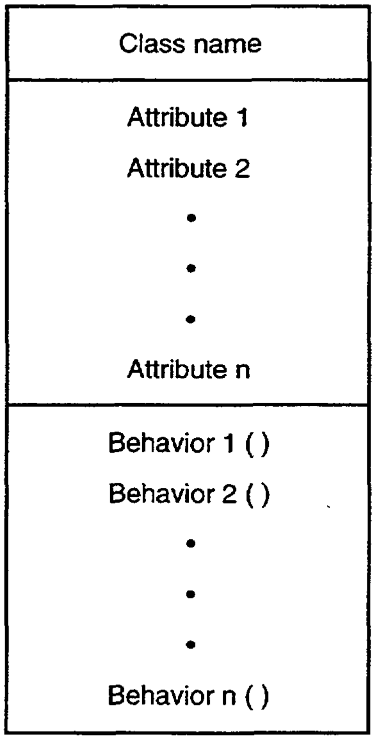


**Figure 1. Representation of a Class**

Two other features of class diagrams, generalization and aggregation, were used in the development of the class diagrams and to organize the templates described in this report.

If a class is a special form of another class, the relationship between these two classes is called a generalization. The term inheritance is also sometimes used. In a generalization relationship the more specialized class retains the characteristics defined for the more general class, although it may specialize them. The specialized class may also have additional characteristics. Viewed from a different perspective, the more specialized class inherits the characteristics of the more general class. Graphically, generalization is shown by an arrow from the specialized class to the general class, showing that the lower class is a member of the higher class. (Note that a filled arrowhead is used in this report although an open arrowhead is the more common notation.)

Aggregation occurs when one class is physically or conceptually composed of another class of components. Aggregation is shown by a line between the two classes. A diamond is located at the end connecting to the larger class. The connecting lines may be annotated to note how many of each type of component are at each end of the relationship. Where the number is unknown, the range of possibilities are indicated by "m...n" where m is the minimum and n is the maximum. An asterisk indicates that any number is allowed.

These concepts are illustrated in the following discussion. A more detailed discussion may be found in many available textbooks on object oriented design. This report uses (with minor changes) the notation of the Universal Modeling Language (UML) [OMG 1999].

## 2.2 Protection System Class Diagram

The protection system is itself a class, because it has behaviors and attributes that apply to itself as a system but not to the individual components that are included in the system. Examples are system-level functions and integrity attributes, such as redundancy, which apply only at the system level. Figure 2 illustrates the class "Protection Systems." The list of characteristics is intended as an illustrative example; only some sample characteristics are listed.

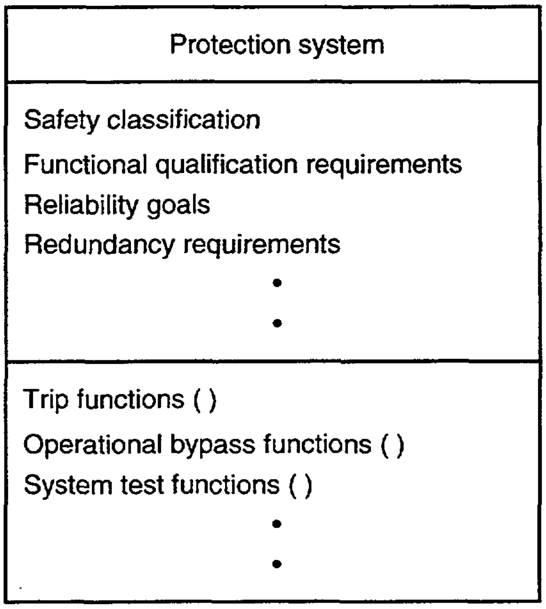


Figure 2. The Class "Protection System"

The protection system of a specific plant or specific generic design is an instance of this class. The plant-specific instance would have the characteristics of the protection system class, but the specific instantiation of these characteristics may vary from plan to plant.

The protection system is itself composed of physical devices that implement the protection system functions. There are a number of characteristics that are common to all physical devices in a protection system. For example, they will all have the same quality requirements, as defined by 10 CFR 50 Appendix B. Generally, the same static safety-related attributes need to be considered for all physical devices. The specialization of these devices is that they will have different behaviors. They will all also have some set of input and output characteristics. A group of characteristics in the class diagram notation is enclosed in guillemets (« »). Figure 3 illustrates this relationship.

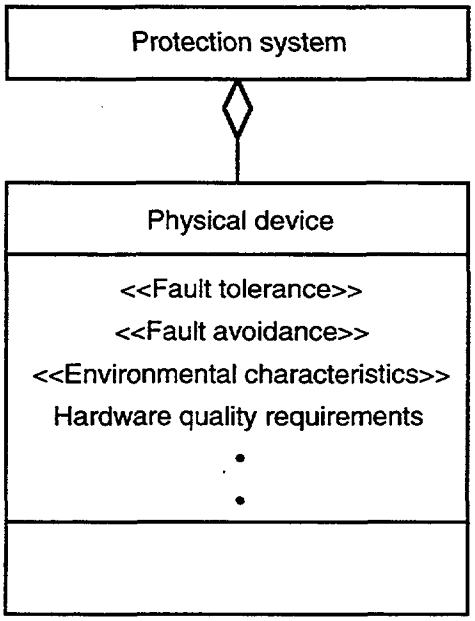


**Figure 3. The Protection System as an Aggregation of Physical Devices**

The GE Advanced Boiling Water Reactor, the CE System 80+ reactor, and the Seimens Teleperm XS generic designs were reviewed to identify the physical devices that are typically used in modern protection systems.[1]

The analysis resulted in identifying the common protection system devices shown in Table 4. All three designs use a common set of components. This is not too surprising, as the modern designs implement the same basic functions using similar technology, they must comply with the same design standards, and they evolved from similar traditional designs. The physical make-up of all protection systems can thus be modeled as shown in Figure 4, which shows the specific classes of components that are part of the general class "physical devices."

[1] The Westinghouse Eagle 21 design was not considered because Westinghouse is in the process of replacing this design with the Ovation system, which is expected to be similar to the other three considered.

**Table 4. Common Protection System Devices**

| Common name | Siemens | GE | CE |
|---|---|---|---|
| Analog sensor | Analog sensor | Analog sensor | Analog sensor<br>Transmitter |
| Switch | Switch<br>Digital sensor | Switch<br>Digital sensor | Switch<br>Digital sensor |
| Digital trip module | Function computer | Digital trip module | PPS bistable trip processors & core protection calculators (CPC) |
| Output logic unit | Actuation computer | Trip logic unit | Coincidence processors |
| Multiplexers | Acquisition computer | Multiplexers | CEA multiplexer |
| Nuclear instrumentation — Processor | Nuclear instrumentation — Specific modules | Nuclear instrumentation — Specific modules | Nuclear instrumentation — Specific modules |
| Trip actuators | Actuation computer | ACT trip actuators | Initiation circuit |
| Service monitor server | Service monitor server | None | None |

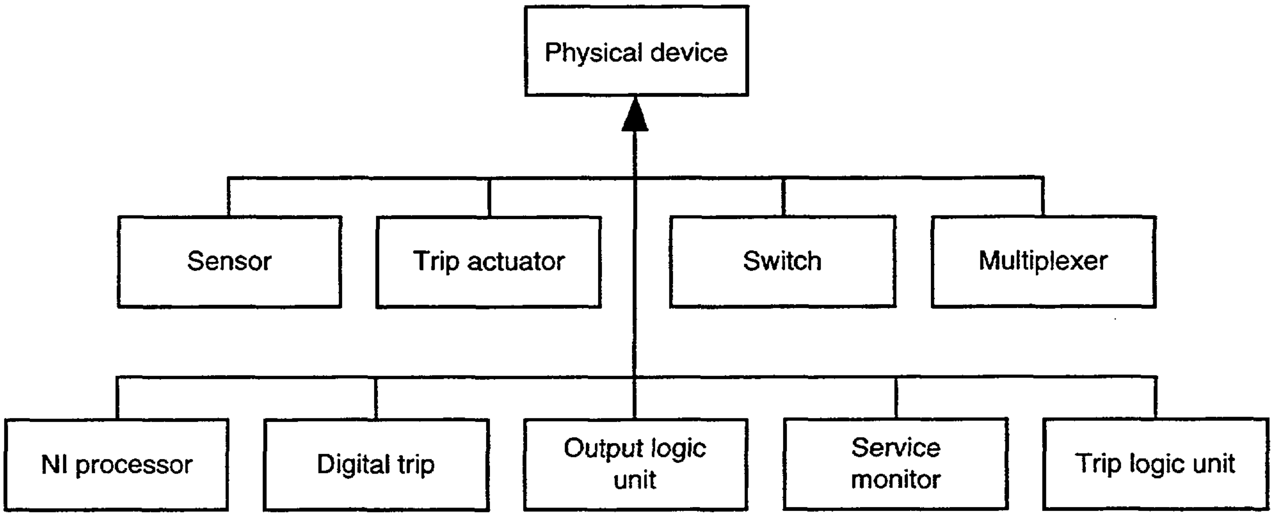


**Figure 4. The Classes of Protection System Components**

The Siemens design was examined to identify the common software components. Siemens was chosen because it is the only one of the three designs considered for which NRC has received detailed software design information. This analysis identified the common set of software components listed in Table 5. The software components have certain common characteristics, which can be generalized into the class "software." Figure 5 then shows the classes of protection system software components. Again, static attributes are treated at the superclass (software) level and behaviors are addressed at the individual level.

Associated with the protection system and with each physical device will be a set of procedures that describe the human interactions with the device. Figure 6 shows how all of the elements come together to form the class model for a physical device. To simplify the illustration, only a couple of software modules are shown. Figure 7 shows how all of the elements come together to form the overall class model for a protection system.

**Table 5. Common Protection System Software Components**

| Common Name | Siemens Teleperm XS | GE | CE |
|---|---|---|---|
| Input | Input | Not identified | I/O handling |
| Output | Output | Not identified | I/O handling |
| Processing | Processing | Not identified | Applications software |
| Diagnostics & self-monitoring | Diagnostics & self-monitoring | Not identified | Equipment self-test & automatic test |
| Operator display | Operator display | Not identified | Status reporting |
| Communications | Communications | Not identified | Communications handling |
| Initialization | Initialization | Not identified | Not identified |
| Operating system | Operating system | Not identified | Operating system |
| Debugging | Debugging | Not identified | Operating system |
| Exception handling | Exception handling | Not identified | Operating system |
| Interrupt handling | Interrupt handling | Not identified | Operating system |

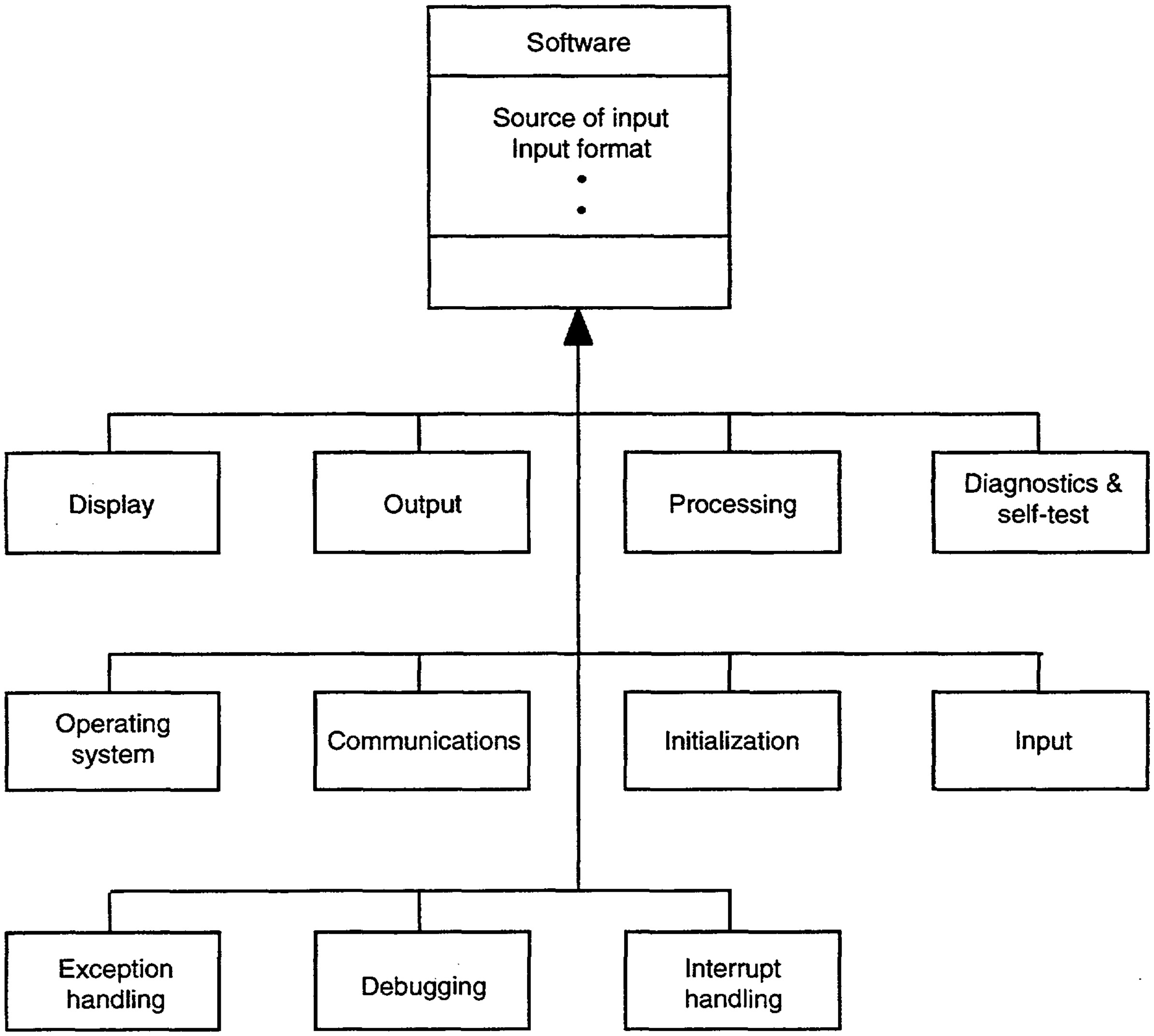


**Figure 5. Protection System Software Classes**

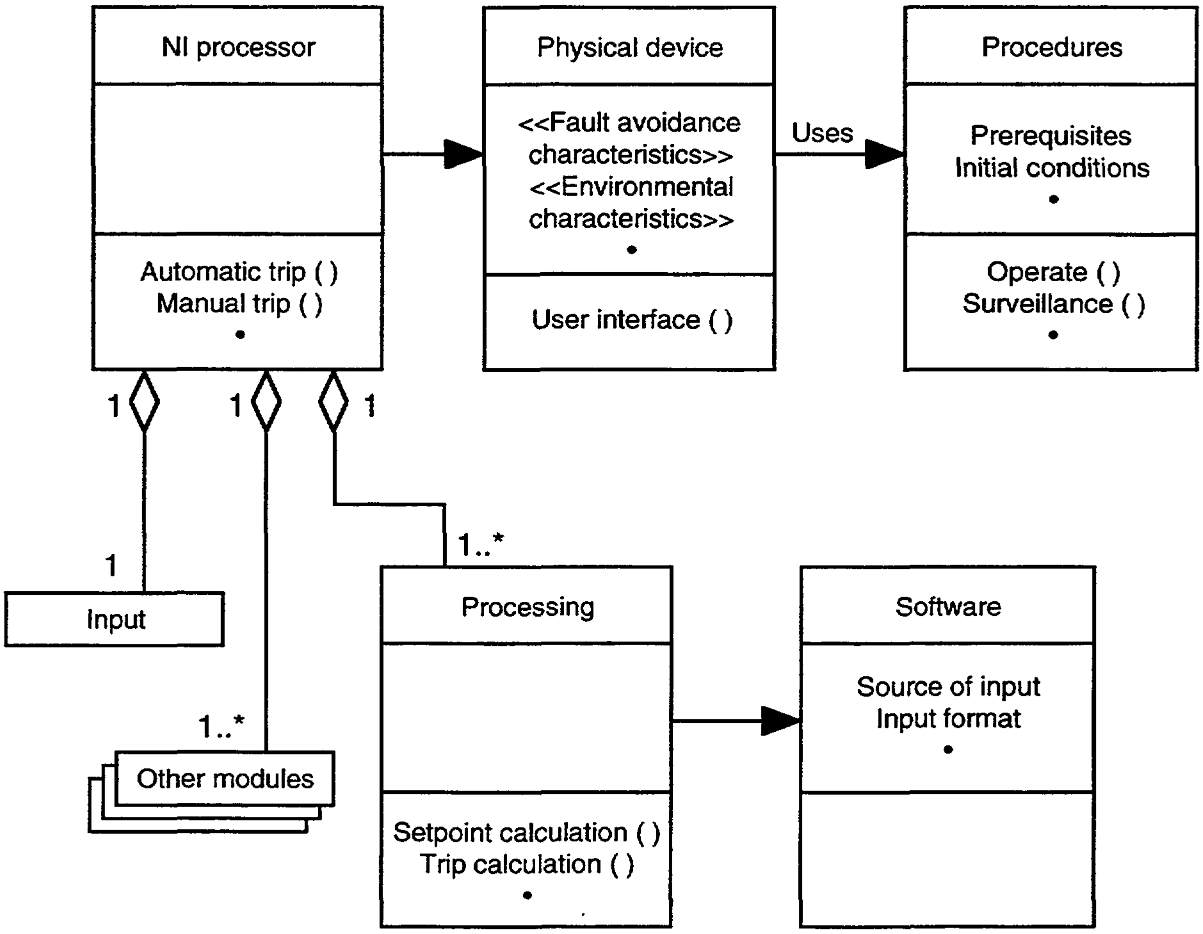


**Figure 6. Class Model of a Nuclear Instrumentation Processor**

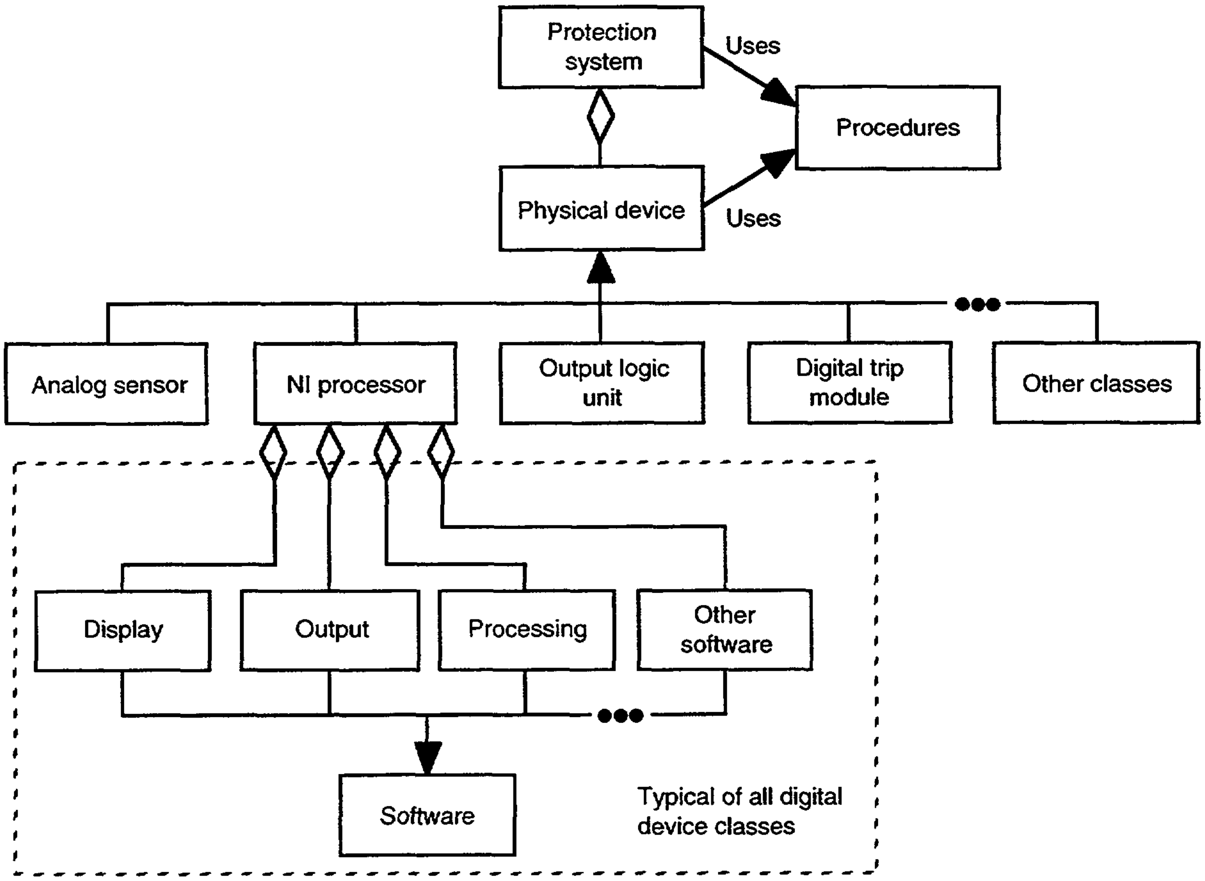


Figure 7. Overall Protection System Class Model

# 3. REVIEW TEMPLATES

Once the construction and analysis of the class diagram was complete, review templates were developed to describe the safety-important characteristics of protection system components that may be considered in the review process. The class model described in Section 2.2 defines the review templates that are needed. Essentially, one template is needed to describe the characteristics of the protection system as a system, separate from the requirements of the individual parts. Two templates are needed to describe the characteristics that are common to all physical devices and the characteristics that are common to all software. Twenty-one templates are needed to address the characteristics that are unique to the individual hardware and software components. Templates were not developed for procedures because a number of NRC procedure guides and review tools already exist.

## 3.1 Structure of the Review Template Set

Two of the templates are generalizations of components. One template is for physical devices; the other is for software. These two do not, by themselves, map to any specific instance of a component in the review process. Instead, they are used in conjunction with the more specific templates. The basis for reviewing any specific physical device in a protection system will be both the general physical device template and the specific component template. Similarly, the basis for reviewing any software component will be both the general software template and the specific template that applies to the software component. The separation of the templates into general and specific elements simplifies maintenance — when changes that affect multiple components are needed, only the general templates need to be revised. This avoids the problem of synchronizing changes to many templates when common characteristics are revised.

## 3.2 Structure of Individual Review Templates

The review templates are designed to help a reviewer confirm that protection system requirements address all of the safety-important characteristics, and that the requirements meet the safety constraints imposed by the safety analysis. Each review template has three spreadsheets. The left hand of each spreadsheet lists the characteristics that were identified as safety significant for the component to which the template applies. The listing of characteristics is the same on all three spreadsheets within a template.

The characteristics identified are grouped into static attributes and dynamic behaviors and further grouped into the categories shown in Table 6. These categories are based upon the taxonomy of requirements topics presented in Appendix C. The category names are not themselves intended to identify specific characteristics for which requirements must be specified. Instead, they name general concepts that may need to be addressed by specifying one or more specific characteristics. In the spreadsheets, the rows containing category names are shaded to indicate that requirements are not expected to be defined for the category as a whole, but only for the individual characteristics within each category. Indentation is used in the spreadsheet and in Table 6 to indicate nesting of categories and to identify the specific characteristics within each category.

**Table 6 Hierarchy of Requirements Topic Categories Considered**

- Attributes
  - Integrity
    - Safety Classification
    - Fault Avoidance
      - Environmental Requirements
      - Normal Environment
      - Abnormal Environment
      - Accident Environment
      - Natural Phenomena Environment
      - Electromagnetic Environment
      - Electrical Power
    - Failure Detection
    - Failure Tolerance
    - Failure Isolation
  - Interfaces

- Behaviors
  - Inputs
  - Process
  - Outputs
  - Performance

The three spreadsheets in each template are described below. Readers may find it useful to refer to Figures 1, 2, and 3 while reading this description.

* Definitions. This spreadsheet contains two columns: a) Characteristics that name the safety-important characteristics, and b) Definitions that gives a short definition of the characteristic. References to the source of the definition may also be included.

* Constraint Source. This spread sheet contains four columns: a) Characteristics as discussed above, b) Typical Source of Constraints, which direct the user to the documents, or analyses that typically describe the fundamental assumptions, analytical results, or regulatory requirements that affect the requirements for the characteristic under consideration, c) Typical Location of Constraints, which identifies where specific licensee or applicant commitments relevant to the characteristic under consideration a likely to be found, and d) Comments, which provides additional information which may be useful in finding or interpreting constraints.

* Review Checklist, which the reviewer uses to record the safety constraint on each characteristic, the actual requirement associated with each characteristic, and to record whether the requirement found in the component specification satisfies the safety constraints. This spreadsheet contains seven columns: a) Characteristics as discussed above, b) Safety Constraint, where the reviewer may record the specific commitments or assumptions that impose safety related constraints on the component characteristic under consideration, c) Constraint Source, where the reviewer may record where the constraint was found, d) Actual Requirement, where the reviewer may record the corresponding requirement found in the component specification, e) Requirement Source, where the reviewer may record where the specification requirement was found, f) Constraints Met?, where the reviewer may

record his or her judgement about whether or not the specification requirements have satisfied the corresponding safety constraints, and g) Comments, where the reviewer may record any other useful information.

## 3.3 Development of the Review Templates

The list of characteristics was developed from a review of the catalog of requirement specification topics (Appendix C). The guidance of IEEE Stds. 603 and 7-4.3.2, and IEC Std. 61069 were also considered in developing both the characteristics and the descriptions of the attributes to be considered.

The various types of behaviors for the physical devices were identified by considering the uses of these devices. The behaviors could be directly identified for relatively simple devices, such as sensors. For more complex devices, such as a Trip Logic Unit, it was helpful to develop use case diagrams based upon component descriptions. Use case descriptions allow visualization of how a component interacts with the outside world. Use case diagrams show two types of entities: external users of the component, represented as stick figures, and basic component functions, represented as ovals. Sometimes it is useful to describe sub-functions that are utilized by other system functions. Communication between external entities and uses cases is shown by a solid line. Use cases that extend the functionality of other use cases may also be shown. The extension relationship is shown by a dashed line with the arrow pointing to the use case that provides additional functionality. Use case diagrams are a modeling technique in the Universal Modeling Language. Appendix D provides the complete set of Use case diagrams for the components considered.

Figure 8 shows and example of the use case diagrams, that a Trip Logic Unit. The external users were identified by reviewing the ABWR Plant Protection System interconnection diagram. The basic functions of Trip, Bypass, Operational Bypass, and Maintain were identified by reviewing the SAR description of the component. Analysis of these functions revealed that defining additional supporting functions of Receive Digital Input, Receive Binary Input, Access Control, Digital Output, and Display would simplify analysis. Defining these supporting functions allows these common functions to be considered just once. The alternative would be to consider them each four times, once as a part of each of the basic functions.

For a given TLU design one or more types of each behavior may need to be present. In the ABWR design for example, there are two types of digital outputs: one to the multiplexer system, one to other RPS devices. The detailed characteristics of these behaviors may be different. For the purpose of the review template, it is not necessary to identify these separately — the reviewer may use the digital output art of the template to review either type.

References to the source of safety constraints on the characteristics of protection system components were developed based upon experience gained in applying the structured approach to the protection system requirements for the ABWR [Johnson 1999]. Typically, safety constraints can be found in one of the following sources:

The accident analysis provided in Chapters 15 and 6 of the Safety Analysis Report (SAR). These parts of the safety analysis typically impose constraints on safety-system behaviors.

The environmental constraints described in Chapters 3.10 and 3.11 of the SAR. These requirements are based upon analyses predicting the environmental conditions that will be present in the plant under various conditions.

The protection system design commitments made in SAR Chapters 7.1, 7.2, and 7.3. These chapters constrain how the integrity requirements of IEEE Std. 603 and the guidance of IEEE Std. 7-4.3.2 are to be met.

Descriptions of interfacing systems. These descriptions may be contained in the SAR chapters dealing with the systems that interface with the protection system, or in more detailed licensee documentation about these systems. The interfacing systems typically impose constraint on the protection system connections and upon protection system behaviors. Systems that typically have important interfaces with the protection system include the following:

- Reactor (SAR Chapter 4)
- Reactor coolant system (SAR Chapter 5)
- Engineered safety features (SAR Chapter 6)
- Other instrumentation and control systems (SAR Chapter 7)
- Electric power systems (SAR Chapter 8)
- Main steam supply system (SAR Chapter 10.3)
- Feedwater systems (SAR Chapter 10.4)

* The accident analysis provided in Chapters 15 and 6 of the Safety Analysis Report (SAR). These parts of the safety analysis typically impose constraints on safety-system behaviors.

The environmental constraints described in Chapters 3.10 and 3.11 of the SAR. These requirements are based upon analyses predicting the environmental conditions that will be present in the plant under various conditions.

The protection system design commitments made in SAR Chapters 7.1, 7.2, and 7.3. These chapters constrain how the integrity requirements of IEEE Std. 603 and the guidance of IEEE Std. 7-4.3.2 are to be met.

Descriptions of interfacing systems. These descriptions may be contained in the SAR chapters dealing with the systems that interface with the protection system, or in more detailed licensee documentation about these systems. The interfacing systems typically impose constraint on the protection system connections and upon protection system behaviors. Systems that typically have important interfaces with the protection system include the following:

- Reactor (SAR Chapter 4)
- Reactor coolant system (SAR Chapter 5)
- Engineered safety features (SAR Chapter 6)
- Other instrumentation and control systems (SAR Chapter 7)
- Electric power systems (SAR Chapter 8)
- Main steam supply system (SAR Chapter 10.3)
- Feedwater systems (SAR Chapter 10.4)

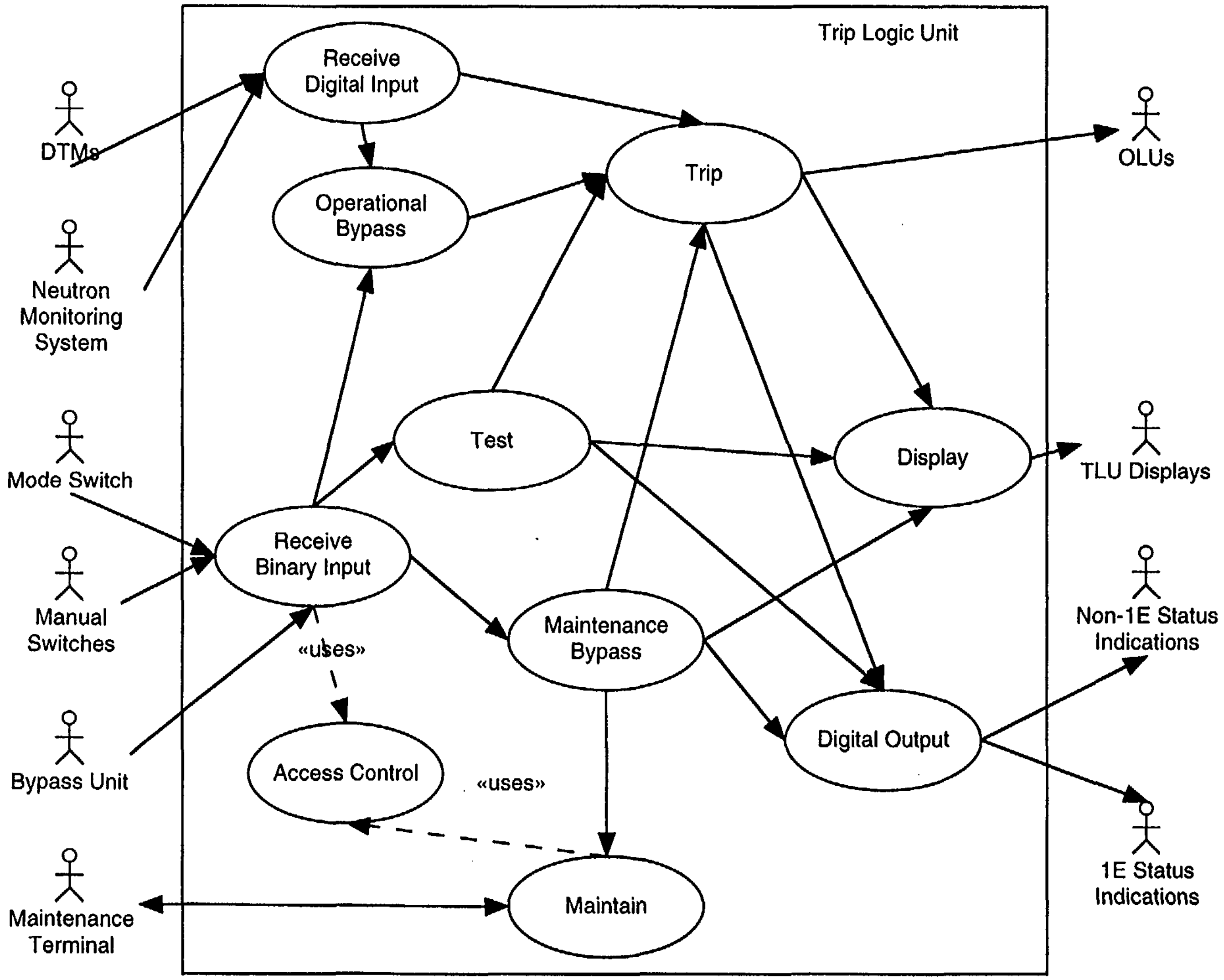


Figure 8. Trip Logic Unit Use Case Model

## 3.4 Index of Review Templates

One example of review templates, the system-level template, is provided as a hardcopy in Appendix A. A complete set of templates is provided as a CD-ROM of Quattro Pro workbooks included with this report. The index to these is provided in Table 7.

**Table 7. Index to Template Files**

| Protection System | Template File Name |
|---|---|
| System Requirements | System.wb3 |
| Physical Devices | |
| Physical Device Generalization | Device.wb3 |
| Sensor | Sensor.wb3 |
| Switch (covers both operator and process actuated switches) | Switch.wb3 |
| Digital Trip Module | DTM.wb3 |
| Trip Logic Unit | TLU.wb3 |
| Trip Actuator | Actuator.wb3 |
| Output Logic Unit | OLU.wb3 |
| Multiplexer | Mux.wb3 |
| Nuclear Instrumentation — Processor | NI.wb3 |
| Service Monitor Server | SMS.wb3 |
| Software Components | |
| Software Generalization | Software.wb3 |
| Input | Input.wb3 |
| Output | Output.wb3 |
| Processing | Process.wb3 |
| Diagnostics & Self-Monitoring | Diag.wb3 |
| Operator Display | Display.wb3 |
| Communications | Com.wb3 |
| Initialization | Init.wb3 |
| Operating System | OS.wb3 |
| Debugging | Debug.wb3 |
| Exception Handling | Exception.wb3 |
| Interrupt Handling | Interrupt.wb3 |
| Master Templates | |
| All Physical Device Attributes and Behaviors | DeviceMaster.wb3 |
| All Software Attributes and Behaviors | SoftwareMaster.wb3 |

# 4. USE OF THE REVIEW TEMPLATES

The following describes a typical sequence of use for the review and provides an example for the use of the templates.

A. Decide the scope of the requirements review. The scope may be to review the requirements for a single component, or a set of components. For the example, reviewing trip logic unit requirements was selected.

B. Select the characteristics to be reviewed. A review may attempt to examine all of the characteristics, or only a subset. The latter would more likely be the case if many components must be examined. A reviewer may decide to look at requirements related to a subset of characteristics over a large number of components. For the example review, all static attributes are selected, but only one behavior was selected for review.

C. Select the review checklists to be used. For the example, the checklists needed are the Physical Device Generalization, the Trip Logic Unit, the Software Generalization, the Input, the Output, the Processing, and the Communications checklists.

D. For each characteristic, examine the safety analysis documentation to determine the safety constraints, and record these constraints and the reference to their locations on the checklist.

E. Where constraints cannot be found, contact the licensee or applicant to discuss the apparent open items so that all safety constraints can be identified.

F. Review the specification(s) for the component under consideration and record the relevant requirements found for each characteristic.

G. For characteristics for which relevant requirements cannot be located, contact the licensee or applicant to attempt to resolve the apparent open item.

H. For each characteristic, record the judgement about whether or not the characteristic and associated safety constraint have been adequately addressed by the specifications.

I. Document any remaining open items for resolution by the licensee or applicant.

If the specification covers all of the safety-important characteristics identified by the template, and the requirements meet the constraints imposed by the safety analysis, the reviewer can conclude that the specification is complete and traceable to the safety analysis. If not, the individual characteristics where this finding cannot be made are areas for further investigation. The reviewer should eventually be able to conclude that all characteristics have been addressed within the established constraints, or that there is a reasonable rationale for each discrepancy. Such a review gives assurance that the safety-important characteristics of a component have been addressed.

The requirements review checklist is most effective for evaluating the static attributes of components. It is more difficult to evaluate the completeness of the specification of component behaviors using a static checklist. The review of behaviors described here could, however, be supplemented by other techniques such as the development of sequence diagrams or state transition diagrams. These techniques are well-documented (see Douglass 1998 for one example). A reviewer might, for example, develop a sequence diagram representing the behavior of a system function or component as described in the SAR, and then develop another sequence diagram based upon the specification description. If a complete sequence diagram can be completed using the specification requirements, and if that diagram is consistent with the one developed from the SAR discussion, then it is very likely that the behavior has been adequately described in a way that complies with the applicable safety constraints.

Appendix B provides an example of a completed set of review checklists illustrating the application to review of trip logic unit requirement specifications for a hypothetical ABWR. The constraints recorded in these checklists are safety constraints derived from the non-proprietary sections of the ABWR Safety Analysis Report [GE 1993]. The actual requirements listed are hypothetical examples of what might be found in review of requirement specifications. Certain open items are left to illustrate the use of the Review Checklists.

The templates could also be used in the process of upgrading existing analog systems to digital systems. Several of the physical device templates correspond to functions performed by the physical devices in existing analog systems. The templates could be used to record the known constraints on the characteristics of the existing system and components. Where characteristics are unknown or are not applicable to the system, the developer would need to investigate the safety analysis assumptions, results, and commitments to document the constraints that should be placed upon the new system. Where software-based components are involved, the templates can be used to help identify the characteristics that should be considered for inclusion in specifications, and the constraints that must be imposed on the design to ensure the safe implementation of the new system.

# 5. PROCESS FOR CREATING NEW TEMPLATES

Reviewers may encounter components that are not adequately covered by existing templates. These components must necessarily be physical devices or software, so the templates for the generalized components will apply. A new device-specific template can be constructed by reviewing the full list of characteristics considered in this study and selecting those that are relevant to the new component to form a new specific review template. (The complete set of characteristics are included as files DeviceMaster.wb3 for physical devices and SoftwareMaster.wb3 for software on the template CD-ROM.) Only characteristics that are not already included in the related generalized checklist (physical device or software) should be included. The types of characteristics identified in Section 3.2 should be considered to determine if additional characteristics, not in the master template, should be included. The catalog of requirements topics included in Appendix C may be a source of ideas regarding possible additional characteristics.

For the most part, the static attributes in the existing templates are expected to be adequate to cover any new components. If it appears that a new template is needed to cover additional static attributes, it may be the case that the safety-important attributes are missing from the existing templates. Consideration should be given to modifying the existing templates, particularly the generalization templates, to include the missing attributes rather than creating a new template.

New templates will most likely be required because some new class of components is identified which has different behaviors than the classes that have already been considered. In this case, a new template should be prepared. Use case modeling is a useful technique for identifying behaviors. This technique is commonly taught in college-level computer science programs, and is well documented in a number of textbooks (see, for example, Douglass 1988). The first step in developing use cases is to identify the external actors. This can typically be done by examining system block diagrams. Each class that connects to the component of interest is an actor or is subsumed in an actor. The use cases are defined by understanding the functional transformations that occur between actors that provide inputs and actors that receive outputs. In some cases, it is useful to break out common functions into separate use cases that perform intermediate transformations or that are used by other functions. Once all of the functions are defined, the safety-related characteristics of each function should be defined and included in the template. The definition of behaviors for each identified function should consider the input, output, process, and performance characteristics of the new behavior.

# 6. CONCLUSION

The review templates included with this report provide a tool to help the NRC staff evaluate the completeness and traceability of protection system requirement specifications. The templates assist reviewers to identify safety important characteristics of reactor protection systems and their hardware and software components. Reviewers use the checklists to verify that important safety characteristics credited in safety analyses are addressed in the requirements documents.

Application of the templates at the system level and to physical devices will assist in confirming compliance with the review guidance of SRP Appendix 7.1-C. The application of the templates to software requirements specifications in particular support the review of the functional and software development process characteristics of software requirements specifications as described in Branch Technical Position 14 (BTP-14) of the SRP. The templates can be used to confirm that software accuracy, functionality, reliability, safety, security, and timing requirements are consistent with assumptions and commitments made in the safety analysis and in higher level design documents. In doing this, the templates also support confirmation of completeness, consistency, correctness, and traceability of the specifications. Users of the templates should be thoroughly familiar with the guidance of both BTP-14 and Appendix 7.1-C.

It is anticipated that use of the tools described in this report will help the NRC staff to perform high quality reviews that assess licensee and applicants requirement specifications and the engineering activities that produce them. Use of the templates will also lend transparency to the review process. High quality, transparent reviews will allow outside observers to develop confidence in NRC staff activities and in the plants that are licensed as a result. Use of these templates should help improve the consistency and efficiency of reviews during the requirements phase of protection system development, thus reducing unnecessary regulatory burden on licensees and applicants.

These templates are only one tool that the NRC may use in the review of requirement specification activities. Since the templates provide a static view, methods applicable to review of dynamic behavior are recommended for use in conjunction with the templates. In particular, the construction of sequence diagrams and state diagrams are more applicable tools for reviewing dynamic characteristics. These may also be useful tools in identifying the timing constraints to be entered in the templates as the basis for reviewing timing specifications for individual hardware and software modules.

The templates provided with this report cover the types of components commonly encountered in modern plant protection systems. It is expected that as the templates are used, reviewers will identify additional characteristics that should be considered and may find that certain characteristics should be deleted. Reviewers of specific designs may also encounter additional types of components not covered by the templates. It is hoped that the templates will be updated and improved as experience is gained through their use. Reviewers may use the techniques described in this report to develop new templates and to modify existing templates.

# 7. REFERENCES

Berg, R., and Johnson, G., "A Structured Approach for Review of Digital Plant Protection System Requirements Specifications," Sandia National Laboratory, June 8, 1998.

Berg, R., and Johnson G., "A Structured Approach for Review of Digital Plant Protection System Requirements Specifications, Volume 2: Overview," Sandia National Laboratory, June 1999.

Beltracchi, L., "Notes on a Means-Ends Requirements Hierarchy," Nuclear Regulatory Commission, 1996.

Brill, R., Berg, R., and Johnson, G., "A Structured Approach for Review of Digital Plant Protection System Requirements Specifications, Volume 1: Overview," Lawrence Livermore National Laboratory, August 1999.

Combustion Engineering, Inc., "System 80+ Standard Design, CESSAR, Design Certification," Amendment W, June 1994.

Douglass, B., "Real-Time UML, Developing Efficient Objects for Embedded Systems," Addison-Wesley, 1988.

Erin, L., Winkler, M., and Graf, A., "Topical Report for the Generic Approval of TELEPERM XS Equipment at the United States Nuclear Regulatory Commission, EMF-2110 (NP), Siemens Power Corporation, September 1998

GE Nuclear Energy, "ABWR Standard Safety Analysis Report," Amendment 31, General Electric Corporation, 32A6100, July 1993.

IEC Std. 61069, "International Standard, Industrial-Process Measurement and Control — Evaluation of System Properties for the Purpose of System Assessment," International Electrotechnical Commission, (Six September 1991 through April 1998).

IEEE Std. 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Institute of Electrical and Electronic Engineers, 1991.

IEEE Std. 7-4.3.2. "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations," Institute of Electrical and Electronic Engineers, 1993.

Johnson, G., and Yamamoto, R., "A Structured Approach for Review of Digital Plant Protection System Requirements Specifications, Volume 3: Trial Application to Advanced Boiling Water Reactor Protection System Specifications," Lawrence Livermore National Laboratory, August 1999.

NUREG-0800, "Standard Review Plan for Review of Safety Analysis Reports for Nuclear Power Plants," Chapter 7, Revision 4, Nuclear Regulatory Commission, June 1997.

Scott, J., "Potential Review Considerations for the Requirements Specification Framework," Lawrence Livermore National Laboratory, CS&R 97-05-11, May 21, 1997.

Object Modeling Group, "UML Semantics, Version 1.1," September 1997.

## Appendix A

Object Modeling Group, “Universal Modeling Language Version 1.3,” June 1999.

# APPENDIX A
# SAMPLE REQUIREMENTS TEMPLATES

Appendix A

This appendix contains one example of a requirements template, the template for plant protection system requirements. A complete set of templates may be found on the accompanying CD-ROM.

System Requirements Specification

| Attributes | Safety Constraint | Source | Actual Requirement | Source | Constraints Met? | Comments |
|---|---|---|---|---|---|---|
| Safety Classification | | | | | | |
| Failure Avoidance | | | | | | |
| Functional Qualification | | | | | | |
| Control of Access | | | | | | |
| Restrictions on sharing between units | | | | | | |
| Human Factors | | | | | | |
| Reliability Goals | | | | | | |
| Reliability Analysis Requirements | | | | | | |
| Failure Tolerance | | | | | | |
| Redundancy | | | | | | |
| Diversity | | | | | | |
| Failure Mode | | | | | | |
| Failure Isolation | | | | | | |
| Electrical Independence | | | | | | |
| Physical Independence | | | | | | |
| Control Protection Isolation | | | | | | |
| Behaviors | | | | | | |
| Protective Actions ( ) -- For each function the following constraints should be considered | | | | | | |
| Function Name | | | | | | |
| Inputs | | | | | | |
| Parameter | | | | | | |
| Measurement Location | | | | | | |
| Span | | | | | | |
| Rate of Change | | | | | | |
| Frequency Content | | | | | | |
| Spatial Dependency | | | | | | |
| Manual Controls | | | | | | |
| Process | | | | | | |
| Actuation Algorithm | | | | | | |
| Initialization / Reset Mode | | | | | | |
| Outputs | | | | | | |
| Outputs | | | | | | |
| Completion of Protective Action | | | | | | |
| Displays | | | | | | |
| Performance | | | | | | |
| Ucertanity | | | | | | |
| Resolution | | | | | | |
| Response Time | | | | | | |
| Update Rate | | | | | | |
| Operational Bypass Functions ( ) -- For each function the following constraints should be considered | | | | | | |
| Function Name | | | | | | |
| Inputs | | | | | | |
| Permissive Parameter | | | | | | |
| Measurement Location | | | | | | |
| Span | | | | | | |
| Rate of Change | | | | | | |
| Frequency Content | | | | | | |
| Spatial Dependency | | | | | | |
| Manual Controls | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Process | | | | | | |
| Bypass Algorithm | | | | | | |
| Initialization / Reset Mode | | | | | | |
| Outputs | | | | | | |
| Bypass Outputs | | | | | | |
| Displays | | | | | | |
| Performance | | | | | | |
| Uncertanity | | | | | | |
| Resolution | | | | | | |
| Response Time | | | | | | |
| Update Rate | | | | | | |
| Functional Test ( ) -- For each function the following constraints should be considered | | | | | | |
| Function Name | | | | | | |
| Inputs | | | | | | |
| Manual Controls | | | | | | |
| Process | | | | | | |
| Test Process | | | | | | |
| Initialization / Reset Mode | | | | | | |
| Outputs | | | | | | |
| Action on Test Failure | | | | | | |
| Displays | | | | | | |
| Maintenance Bypass Functions -- For each bypass function the following constraints should be considered | | | | | | |
| Function Name | | | | | | |
| Inputs | | | | | | |
| Manual Controls | | | | | | |
| Process | | | | | | |
| Bypass algorithms | | | | | | |
| Outputs | | | | | | |
| Displays | | | | | | |
| Bypass and Inoperable Status Indication Functions -- For each function the following constraints should be considered | | | | | | |
| Inputs | | | | | | |
| Bypass Inputs | | | | | | |
| Inoperable Status Inputs | | | | | | |
| Manual Controls | | | | | | |
| Process | | | | | | |
| Bypass indication algorithms | | | | | | |
| Outputs | | | | | | |
| Displays | | | | | | |

System Requirements Specification

| Attributes | Definition |
|---|---|
| Safety Classification | The system safety classification (e.g., safety, important to safety) |
| Failure Avoidance | |
| Functional Qualification | The testing and analyses required to demonstrate the system performs the required functions |
| Control of Access | The provisions for preventing unautorized access to equipment or controls. |
| Restrictions on sharing between units | The limitations of using system functions or equipment to perform functions in more than one unit. |
| Human Factors | The requirements imposed upon the human machine interface. Typically a reference to NUREG-0700. |
| Reliability Goals | The qualitative or quantitative goals for probability of the system performing protective actions on demand. |
| Reliability Analysis Requirements | The testing and analyses required to demonstrate reliability goals are met. |
| Failure Tolerance | |
| Redundancy | Requirements for providing multiple components, channels, trains, or systems |
| Diversity | Requirements for the provision of diverse functions to compensate for failure, particularly common mode failure |
| Failure Mode | The state to which functions should preferentially fail |
| Failure Isolation | |
| Electrical Independence | The provisions made to prevent propagation of failures between redundant functions along electrical connections |
| Physical Independence | The provisions made to prevent failure of redundant functions because of common equipment locations |
| Control Protection Isolation | The provisions made to prevent failures from both causing accidents and disabling the protective system response |
| Behaviors | |
| Protective Actions () | The initiation of a signal for the purpose of accomplishing a safety function. |
| Function Name | The identification of the function under review. |
| Inputs | |
| Parameter | The parameters or set of parameters to be measured |
| Measurement Location | The location at which each parameter is to be measured |
| Span | The difference between the maximum and minimum values to be measured. |
| Rate of Change | The magnitude of change per unit time that the system must accommodate for a specified signal |
| Frequency Content | The signal bandwidth that must be maintained in the measurement |
| Spatial Dependency | Number & locations of measurements needed (most often used for core flux or temperature measurements) |
| Manual Controls | Manual inputs to the functions |
| Process | |
| Actuation Algorithm | The relationship between input and the trip/no-trip conditions. Typically a constant with hysterisis. Sometimes a function of other parameters. |
| Initialization / Reset Mode | The condition that the function assumes upon startup or energization - both initially and after reset. |
| Outputs | |
| Outputs | The output signals or commands to be provided by the system |
| Completion of Protective Action | The point at which the function is considered to be complete and may be reset. |
| Displays | The information about the function to be displayed to operators |
| Performance | |
| Uncertanity | The allowable abount by which the channel output is in doubt. Typically includes accuracy, environment effects, drift, etc. |
| Response Time | The time required after an abrupt change input until the output comes to rest a its new value |
| Update Rate | The time required to obtain a collection of data |
| Operational Bypass Functions () | Inhibition of the capability to accomplish a safety function that could otherwise occur in response to a particular set of generating conditions. |
| Function Name | The identification of the function under review. |
| Inputs | |
| Permissive Parameter | The parameters or set of parameters to be measured |
| Measurement Location | The location at which each parameter is to be measured |
| Span | The difference between the maximum and minimum values to be measured. |
| Rate of Change | The magnitude of change per unit time that the system must accommodate for a specified signal |
| Frequency Content | The signal bandwidth that must be maintained in the measurement |
| Spatial Dependency | Number & locations of measurements needed (most often used for core flux or temperature measurements) |
| Manual Controls | Manual inputs to the functions. Typically the controls to manually trip or actuate safety functions. |
| Process | |
| Bypass Algorithm | The relationship between input and the trip/no-trip conditions. Typically a constant with hysterisis. Sometimes a function of other parameters. |
| Initialization / Reset Mode | The condition that the function assumes upon startup or energization - both initially and after reset. |
| Outputs | |
| Bypass Outputs | The output signals or commands to be provided by the system |
| Completion of Protective Action | The point at which the function is considered to be complete and may be reset. |
| Displays | The information about the function to be displayed to operators |

| | |
|---|---|
| Performance | |
| Uncertanity | The allowable abount by which the channel output is in doubt. Typically includes accuracy, environment effects, drift, etc. |
| Response Time | The time required after an abrupt change input until the output comes to rest a its new value |
| Update Rate | The time required to obtain a collection of data |
| Functional Test () -- For each function the following constraints should be considered | |
| Function Name | The identification of the function under review. |
| *Inputs* | |
| Manual Controls | Manual inputs to the functions. Typically the controls to initiate bypass. |
| Process | |
| Test Process | The description of the tests to be performed including pass / fail criteria. |
| Initialization / Reset Mode | The condition that the function assumes upon startup or energization - both initially and after reset. |
| *Outputs* | |
| Action on Test Failure | The automatic actions, e.g. trip or bypass (if any) taken upon test failure. |
| Displays | The displays of test results or test status. |
| Maintenance Bypass Functions -- For each byp | Functions to allow removal of the capability of a channel to perform a potective action duee to a requirement for replacement, repair, test, or calibration. |
| Function Name | The identification of the function under review. |
| *Inputs* | |
| Manual Controls | Manual inputs to the functions. Typically the controls to initiate and remove bypass. |
| Process | |
| Bypass algorithms | The relationship between input and the bypass/unbypass conditions. Typically a function of the manual bypass control and the status of redundant channels. |
| Outputs | |
| Displays | *The display of bypass status at the bypass actuation location.* |
| Bypass and Inoperable Status Indication Functions -- For each function the following constraints should be considered | |
| Inputs | |
| Bypass Inputs | The bypass status inputs to the bypass and inoperable status indication (BISI) display. |
| Inoperable Status Inputs | The inoperable status inputs to the bypass and inoperable status indication (BISI) display. |
| Manual Controls | *Manual inputs to the BISI system. Typically switches to manually input status information.* |
| Process | |
| Bypass indication algorithms | The function that describes the relationship between input conditions and the display. Typically a simple function such as "if bypass then display bypass." |
| Outputs | |
| Displays | The system level display of bypass and inoperable status in the control room operating area. |

System Requirements Specification

| Attributes | Typical Source of Constraints | Typical Location of Constraints | Comments |
|---|---|---|---|
| Safety Classification | 10 CFR 50, IEEE 603 Sec 5.12 | SAR Ch. 7.1 | Protection systems and auxiliary features must be safety |
| Failure Avoidance | | | |
| Functional Qualification | 10 CFR 50 Appendix B, Sec III | SAR Ch. 7.1, 7.2, 7.3 | |
| Control of Access | IEEE 603 Sec. 5.9 | SAR Ch. 7.1, 7.2, 7.3 | |
| Restrictions on sharing between units | IEEE 603 Sec. 5.13 | SAR Ch. 7.1, 7.2, 7.3 | |
| Human Factors | IEEE 603 Sec 5.14 | SAR Ch. 18 | |
| Reliability Goals | GDC 21, GDC 29, IEEE 603 Sec. 5.5 | SAR Ch. 7.1, 7.2, 7.3, 19 | May be quantitative or qualitative |
| Reliability Analysis Requirements | IEEE 603, Sec. 5.15 | SAR Ch. 7.2, 7.3 | |
| Failure Tolerance | | | |
| Redundancy | IEEE 603 Sections 5.1 | SAR Ch. 7.1, 7.2, 7.3 | |
| Diversity | DID&D Analysis, IEEE 603 Sec. 5.16 | SAR Ch. 7.1, 7.2, 7.3, 7.8 | DID&D analysis should conform with SECY 93-087 |
| Failure Mode | GDC 23 | SAR Ch. 7.1, 7.2, 7.3 | |
| Failure Isolation | | | |
| Electrical Independence | IEEE 603, Sections 5.6 | SAR Ch. 7.1, 7.2, 7.3 | |
| Physical Independence | IEEE 603, Sections 5.6 | SAR Ch. 7.1, 7.2, 7.3 | |
| Control Protection Isolation | GDC 24, IEEE 603, Sections 6.3 | SAR Ch. 7.1, 7.2, 7.3 | |
| Behaviors | | | |
| Protective Actions () -- Each function described in the SAR should be specified. Typically the function may be supported by a process control and measurement diagram or a logic diagram. | | | |
| Function Name | Accident analysis assumptions | SAR Ch. 7.2, 7.3, 15 | |
| Inputs - For manual functions only the manual controls item is germane | | | |
| Parameter | Accident analysis assumptions, IEEE 603 Sec 6.4 | SAR Ch. 15 | Parameters shall be direct measures where feasible and practical |
| Measurement Location | Accident analysis assumptions | SAR Ch. 7.2, 7.3, 15 | Unnecessary if parameter measurement is insensitive to location |
| Span | Accident analysis results (bounds of accident and normal values) | SAR Ch. 15 | |
| Rate of Change | Accident analysis results (measured from transient curves) | SAR Ch. 15 | |
| Frequency Content | Accident analysis results (calculated from transient curves) | SAR Ch. 15 | |
| Spatial Dependency | Accident analysis assumptions | SAR Ch. 7.2, 7.3, 15 | Typically important only for neutron monitoring. |
| Manual Controls | IEEE 603 Section 6.2 | SAR Ch. 7.1, 7.2, 7.3 | |
| Process | | | |
| Trip Algorithm | Accident analysis assumptions | SAR Chapter 15 | Typically bistable decision |
| Initialization / Reset Mode | SRP | SAR Ch. 7.1, 7.2, 7.3 | |
| Outputs | | | |
| Outputs | Accident analysis assumptions | SAR Ch. 7.1, 7.2, 7.3, 15 | |
| Completion of Protective Action | IEEE 603, Section 5.2 | SAR Ch. 7.1, 7.2, 7.3 | |
| Displays | | SAR Ch. 7.1, 7.2, 7.3, 18 | |
| Performance | | | |
| Uncertainty | Accident analysis assumptions | SAR Chapter 15 | |
| Response Time | Accident analysis assumptions | SAR Chapter 15 | |
| Update Rate | Accident analysis results (calculated from transient curves) | SAR Ch. 15 | Update rate must be fast enough to be consistent with these. |
| Operational Bypass Functions () -- For each function the following constraints should be considered | | | |
| Function Name | Identifier Only | SAR Ch. 7.1, 7.2, 7.3 | |
| Inputs | | | |
| Permissive Parameter | Accident analysis assumptions | SAR Ch. 15 | Bypasses will typically be implemented using a sensor channel that is also used for a trip function. In these cases, the input characteristics will be the same as for the trip function. |

System Requirements Specification

| Attributes | Typical Source of Constraints | Typical Location of Constraints | Comments |
|---|---|---|---|
| Measurement Location | Accident analysis assumptions | SAR Ch. 7.2, 7.3, 15 | |
| Span | Accident analysis results (bounds of accident and normal values) | SAR Ch. 15 | |
| Rate of Change | Accident analysis results (measured from transient curves) | SAR Ch. 15 | |
| Frequency Content | Accident analysis results (calculated from transient curves) | SAR Ch. 15 | |
| Spatial Dependency | Accident analysis assumptions | SAR Ch. 7.2, 7.3, 15 | Typically important only for neutron monitoring. |
| Manual Controls | IEEE 603 Section | SAR Ch. 7.1, 7.2, 7.3 | |
| Process | | | |
| Bypass Algorithm | Accident analysis assumptions, IEEE 603 Sec. 6.6, 7.4 | SAR Chapter 15, 7.1, 7.2, 7.3 | |
| Initialization / Reset Mode | SRP | SAR Ch. 7.1, 7.2, 7.3 | |
| Outputs | | | |
| Bypass Outputs | IEEE 603 Sec | SAR Ch. 7.1, 7.2, 7.3 | |
| Displays | IEEE 603 Sec. 5.8 | SAR Ch. 7.1, 7.2, 7.3 | |
| Performance | | | |
| Uncertainty | Accident analysis assumptions | SAR Chapter 15 | Bypasses will typically be implemented using a sensor channel that is also used for a trip function. In these cases, the trip will normally establish the performance characteristics. |
| Resolution | Accident analysis assumptions | SAR Chapter 15 | |
| Response Time | Accident analysis assumptions | SAR Chapter 15 | |
| Update Rate | Accident analysis results (calculated from transient curves) | SAR Ch. 15 | |
| Functional Test () -- For each function the following constraints should be considered | | | |
| Function Name | Identifier Only | SAR Ch. 7.1, 7.2, 7.3 | |
| Inputs | | | |
| Manual Controls | Design Decision | SAR Ch. 7.1, 7.2, 7.3 | |
| Process | | | |
| Test Process | *GDC 21, IEEE 503 Sec 5.7, 6.5* | SAR Ch. 7.1, 7.2, 7.3 | |
| Initialization / Reset Mode | SRP 7.1-C, Section 10 | SAR Ch. 7.1, 7.2, 7.3 | |
| Outputs | | | |
| Action on Test Failure | SRP 7.1-C, Section 10 | SAR Ch. 7.1, 7.2, 7.3 | |
| Displays | IEEE 603 Sec 5.10 | SAR Ch. 7.1, 7.2, 7.3 | |
| Maintenance Bypass Functions -- For each bypass function the following constraints should be considered | | | |
| Function Name | Identifier Only | SAR Ch. 7.1, 7.2, 7.3 | |
| Inputs | | | |
| Manual Controls | Design Decision | SAR Ch. 7.1, 7.2, 7.3 | |
| Process | | | |
| Bypass algorithms | GDC 21, IEEE 603 Sec 6.7 | SAR Ch. 7.1, 7.2, 7.3 | |
| Outputs | | | |
| Displays | IEEE 603 Sec. 5.8 | SAR Ch. 7.1, 7.2, 7.3 | |
| Bypass and Inoperable Status Indication Functions -- For each function the following constraints should be considered | | | |
| Inputs | | | |
| Bypass Inputs | IEEE 603 Sec. 5.8.3 (b) | SAR Ch. 7.1, 7.2, 7.3 | |
| Inoperable Status Inputs | IEEE 603 Sec. 5.8.3 (b) | SAR Ch. 7.1, 7.2, 7.3 | |
| Manual Controls | IEEE 603 Section 5.8.3 (c) | SAR Ch. 7.1, 7.2, 7.3 | |
| Process | | | |
| Bypass indication algorithms | IEEE 603 Sec. 5.8 | SAR Ch. 7.1, 7.2, 7.3 | |
| Outputs | | | |
| Displays | IEEE 603 Sec. 5.8 | SAR Ch. 7.1, 7.2, 7.3 | |

# APPENDIX B
# EXAMPLE USE OF TEMPLATES TO REVIEW ABWR TRIP LOGIC UNIT REQUIREMENTS

This appendix provides an example of a completed set of review checklists illustrating the application to review of trip logic unit requirement specifications for a hypothetical BWR. The constraints recorded in these checklists are safety constraints derived from the non-proprietary sections of the ABWR Safety Analysis Report [GE 1993]. The actual requirements listed are hypothetical examples of what might be found in review of requirement specifications. Certain open items are left to illustrate the use of the Review Checklists. These open items are indicated by shading in the "Contraints Met?" column.

Physical Device Requirements - Trip Logic Unit

| Attributes | Safety Constraint | Source | Actual Requirement | Source | Constraints Met? | Comments |
|---|---|---|---|---|---|---|
| Safety Classification | | | Safety-related | TLU Specification 4.1.4.1 | Yes | |
| Failure Avoidance | | | | | | |
| Functional Qualification | | | | | Yes | |
| Hardware Quality Assurance | | | Compliance with NQA-1 | TLU Specification Sec 4.1.1.1 | Yes | |
| Human Factors | | | Compliance with NUREG-0700 | TLU Specification Sec 4.1.1.1 | Yes | |
| Reliability Goals | | | | | | No requirements stated at module level. |
| Reliability Analysis Requirements | | | | | | No requirements stated at module level. |
| Maintainability | Standardized, interchangeable modules. Effect of removing a card for service to be minimized. MTTD+MTTR < 12 hr. Routine service and calibration possible on-line without disturbing system. | System specification Sec 4.3.1, 4.3.2 | | | N/A | Dealt with at rack level. |
| Environmental Requirements | | | | | | |
| Location | Main control Room | | | | | |
| Normal | | | | | | |
| Life | | | | | N/A | |
| Chemical | None | SAR T3I-5 | | | N/A | |
| Vibration | None | SAR T3I-5 | | | N/A | |
| Temperature | | | | | | |
| Max | 40 ℃ | SAR T3I-5 | 50 ℃ | TLU Specification Sec 4.2.1.4 | Yes | |
| Min | 5 °C | SAR T3I-5 | 5 °C | TLU Specification Sec 4.2.1.4 | Yes | |
| Humidity | | | | | | |
| Max | 90% | SAR T3I-5 | 95% | TLU Specification Sec 4.2.1.5 | Yes | |
| Radiation | | | | | | |
| γ Total Dose | 300 Rad | SAR F12.3-46, F12.3-47 | | | Yes | No requirement stated, but requirement is well below known damage thresholds for electronics. Conservatively assumes 60 yr life |
| γ Dose Rate | | SAR F12.3-46, F12.3-47 | | | N/A | |
| β Total Dose | 0 | SAR F12.3-46, F12.3-47 | | | N/A | |
| β Dose Rate | 0 | SAR F12.3-46, F12.3-47 | | | N/A | |
| n Total Dose | 0 | SAR F12.3-46, F12.3-47 | | | N/A | |

Appendix B

Physical Device Requirements - Trip Logic Unit

| | | | | | | |
|---|---|---|---|---|---|---|
| n Dose Rate | 0 | SAR F12.3-46, F12.3-47 | | | N/A | |
| Abnormal | | | | | | |
| Chemical | Abnormal inc. in Normal | | | | N/A | |
| Flood | Abnormal inc. in Normal | | | | N/A | |
| Vibration | Abnormal inc. in Normal | | | | N/A | |
| Temperature | | | | | | |
| Max | Abnormal inc. in Normal | | | | N/A | |
| Min | Abnormal inc. in Normal | | | | N/A | |
| Humidity | | | | | | |
| Max | Abnormal inc. in Normal | | | | N/A | |
| Radiation | | | | | | |
| γ Total Dose | Abnormal inc. in Normal | | | | N/A | |
| γ Dose Rate | Abnormal inc. in Normal | | | | N/A | |
| β Total Dose | Abnormal inc. in Normal | | | | N/A | |
| β Dose Rate | Abnormal inc. in Normal | | | | N/A | |
| n Total Dose | Abnormal inc. in Normal | | | | N/A | |
| n Dose Rate | Abnormal inc. in Normal | | | | N/A | |
| Accident | | | | | | |
| Qualification Requirements | | | Environmental Qualification per Reg Guide 1.89 | Hardware Qualification Requirements Report, Environmental Qualification Program Manual, A-1184 | Yes | The Hardware Qualification Requirements Report references the Environmental Qualification Program Manual for test and analysis requirements, and drawing A-1184 for environmental conditions. |
| Duration | 8760 hrs | SAR T3I-15 | | | N/A | Seismic - Aging interaction not expected. No harsh environment qualified life is required. |
| Chemical | None | SAR T3I-15 | | | N/A | |
| Flood | Yes - Fire suppression system | T9.5-5 | Mounting above flood level. | SAR 7.2 | Yes | |
| Mechanical | None | SAR T3I-15 | | | N/A | |
| Jet Impingement | None | SAR T3I-15 | | | N/A | |
| Vibration | None | SAR T3I-15 | | | N/A | |
| Temperature | | | | | | |
| Max | 50 °C | SAR T3I-15 | 50 ℃ | TLU Specification Sec 4.2.1.4 | Yes | |
| Min | 5 °C | SAR T3I-15 | 5 °C | TLU Specification Sec 4.2.1.4 | Yes | |
| Pressure | | | | | | |
| Max | 0 kg/sqcm g | SAR T3I-15 | | | N/A | |
| Min | 0 kg/sqcm g | SAR T3I-15 | | | N/A | |
| Humidity | | | | | | |
| Max | 90% | SAR T3I-15 | 95% | TLU Specification Sec 4.2.1.6 | Yes | |
| Radiation | | | | | | |

**Physical Device Requirements - Trip Logic Unit**

| | | | | | | |
|---|---|---|---|---|---|---|
| γ Total Dose | 2190 Rad | SAR F12.3 | | | Yes | No requirement stated, but requirement is well below known damage thresholds for electronics. Requirement conservatively assumes dose rate at highest level for full duration. |
| γ Dose Rate | | SAR F12.3 | | | N/A | |
| b Total Dose | 0 | SAR F12.3 | | | N/A | |
| β Dose Rate | 0 | SAR F12.3 | | | N/A | |
| n Total Dose | 0 | SAR F12.3 | | | N/A | |
| n Dose Rate | 0 | SAR F12.3 | | | N/A | |
| Natural Phenomena | | | | | | |
| Type Test Requirements | | | Seismic design and qualification per IEEE 344 | Hardware Qualification Requirements Report, Seismic Qualification Program Manual, C-1063 | Yes | The Hardware Qualification Requirements Report references the Seismic Qualification Program Manual for test and analysis requirements, and drawing C-1063 for environmental conditions. |
| Flood | None | | | | N/A | |
| Seismic | | | | | | |
| Qualification Requirements | Qualification per Reg. Guide 1.100 | SAR Sec 3.10 | Seismic design and qualification per IEEE 344 | Hardware Qualification Requirements Report, Seismic Qualification Program Manual, C-1063 | Yes | The Hardware Qualification Requirements Report references the Seismic Qualification Program Manual for test and analysis requirements, and drawing C-1063 for environmental conditions. |
| Acceleration | Spectra given in Reference | SAR F3G.5-14, F3G.5-12 | Qualification to C-1063, sheet | Hardware Qualification Requirements Report, Seismic Qualification Program Manual, C-1063 | Yes | Figures are in SAR amendment 16. Final issue does not contain response spectra. |
| Tornado | | | | | | |
| Max Pressure | N/A | | | | N/A | Equipment protected in control room |
| Rate of Change | N/A | | | | N/A | Equipment protected in control room |
| Mechanical | N/A | | | | N/A | Equipment protected in control room |
| Electromagnetic Interference (EMI) | | | | | | |
| Type Test Requirements | | | | | | EMI Qualification Requirements not stated. |
| Radiated EMI Withstand | | | | | | EMI Qualification Requirements not stated. |
| Conducted EMI Withstand | | | | | | EMI Qualification Requirements not stated. |
| Electrostatic Discharge | | | | | | EMI Qualification Requirements not stated. |
| Radiated EMI Emission | | | | | | EMI Qualification Requirements not stated. |
| Conducted EMI Emission | | | | | | EMI Qualification Requirements not stated. |
| Grounding and Shielding Practice | | | Protection against electrical noise, use of fiber optic cables, elimination of ground loops, signal isolation. | TLU Specification Sec 2.3.5 | Yes | |
| Electrical Power | | | | | | |
| Safety Classification | | | Class 1E Vital Power | TLU Specification Sec 2.3.5, 2.2.4.1 | Yes. | |

## Physical Device Requirements - Trip Logic Unit

| | | | | | | |
|---|---|---|---|---|---|---|
| Max Voltage | 132 V | SAR Sec 8.3.1.1.4.1 | +/- 50V | | | Power supply requirements may be for panel vs. TLU itself. |
| Min Voltage | 108 V | SAR Sec 8.3.1.1.4.1 | +/- 48V | | | |
| Frequency | 58 - 62 Hz | SAR Sec 8.3.1.1.4.1 | DC | | Yes | |
| Harmonic Distortion | | | N/A | | Yes | |
| Interruption Tolerance | | | Uninterruptable power | TLU Specification Sec 2.2.4.1, 2.2.2.2 | Yes | |
| Failure Tolerance | | | | | | |
| Diversity | | | | | | Confirm diversity consistent with defense-in-depth and diversity analysis. |
| Failure Mode | | | Trip actuation on loss of power | TLU Specification Sec 3.3.9 | Yes | |
| Behaviors - Behaviors are defined for specific physical devices | | | | | | |

Trip Logic Unit

| Attributes | Safety Constraint | Source | Actual Requirement | Source | Constraints Met? | Comments |
|---|---|---|---|---|---|---|
| See physical device template for attributes | | | | | | |
| Behaviors - Behaviors are defined for specific physical devices | | | | | | |
| Receive Digital Inputs () -- For each input function the following constraints should be considered | | | | | | |
| Function Name | Channel trip status from DTM | SAR F7.2-2, Hardware Generic Requirements Sec 1.3.7.a | Logic per logic diagram. | Drawing E-1834 Sheet 22 | Yes | Only one of several digital inputs reviewed. |
| Inputs | | | | | | |
| Input Description | Fiberoptic data link. | Hardware Generic Requirements Sec 1.3.7.a | 100 MB/sec FDDI | System Communication Specification | Yes | |
| Process | | | | | | |
| Communications Protocol | | | 100 MB/sec FDDI | System Communication Specification | Yes | |
| Data Validation | | | | | | |
| Performance | | | | | | |
| Precision | | | | | N/A | |
| Update Rate | | | 5 msec | System Communication Specification | Yes | |
| Receive Binary Inputs () -- For each input function the following constraints should be considered | | | | | | |
| Function Name | Mode switch position | SAR F7.2-2 | Logic per logic diagram. | Drawing E-1834 Sheet 19 | Yes | |
| Inputs | | | | | | |
| Input Description | Switch contact | MSIV Isolation Function Requirement Specification | Logic per logic diagram. | Drawing E-1834 Sheet 19 | Yes | |
| Process | | | | | | |
| Data Validation | | | | | N/A | |
| Performance | | | | | | |
| Precision | | | | | N/A | |
| Update Rate | | | 5 msec | TLU Specification Sec 3.6.7 | Yes. | |
| Division Trip () - For each trip function the following constraints should be considered | | | | | | |
| Function Name | MSIV Isolation Trip | System Requirement Specification Sec 4.4.4 | Logic per logic diagram. | Drawing E-1834 Sheet 22 | Yes | |
| Process | | | | | | |
| Trip Algorithm | Trip if either inboard or outboard MSIV not open on two steam lines and the same function is tripped in at least one other TLU, and the function is not bypassed. | System Requirement Specification Sec 4.4.4.1, SAR F7.2-4, MSIV Isolation Function Requirement Specification Sec 6.2 | Logic per logic diagram. | Drawing E-1834 Sheet 20 | Yes | |
| Performance | | | | | | |

Trip Logic Unit

| | | | | | | |
|---|---|---|---|---|---|---|
| Response Time | .01 sec - communications, DTM, OLU, Load Driver, and Input ( ) delay times. | System Requirement Specification Sec 4.1.4.13.1.2, 4.14.13.1.3, SAR F7.2-2 | 5 msec | TLU Specification Sec 3.6.7 | | Need to confirm relationship to other delay times. |
| Update Rate | | | 5 msec | TLU Specification Sec 3.6.7 | | Need to confirm relationship to other delay times. |
| Division Operational Bypass ( ) - For each operational bypass function the following constraints should be considered | | | | | | |
| Function Name | MSL Pressure Bypass | System Requirement Specification Sec 4.4.4.1.1.c, 4.4.4.3, 4.4.4.4 | Logic per logic diagram. | Drawing E-1834 Sheet 19 | Yes | |
| Process | | | | | | |
| Bypass Algorithm | Bypass when Mode switch in Shutdown, refuel, or startup and reactor pressure is low (< approximately 42.2 kg/sqcm). Automatically remove bypass when permissive conditions not met. | System Requirement Specification Sec 4.4.4.1.1.c, 4.4.4.3, 4.4.4.4, 4.4.4.1.b, 4.1.4.6.2 | Logic per logic diagram. | Drawing E-1834 Sheet 19 | Yes | |
| Performance | | | | | | |
| Response Time | | | | | N/A | Response time of many seconds is acceptable. |
| Update Rate | | | | | N/A | Update interval of many seconds is acceptable. |
| Digital Output ( ) -- For each output function the following constraints should be considered | | | | | | |
| Function Name | Trip signal to OLU. | SAR F7.2-2, Hardware Generic Requirements Sec 3.3 | Logic per logic diagram. | Drawing E-1834 Sheet 23 | Yes | |
| Process | | | | | | |
| Communications Protocol | | | | | | |
| Initialization / Reset Mode | Must be known | Hardware Generic Requirements Sec 4.6.3.5 | Reference to generic requirements. | TLU Specification Sec 2.3.5 | | Confirm actual initialization is required to be in safe mode. |
| Outputs | | | | | | |
| Output Description | <2V = trip, >2V=not trip. | OLU Specification Sec 3.3 | <2V = trip, >2V=not trip. | TLU Specification Sec 4.5.3 | Yes | |
| Communications Protocol | | | | | N/A | binary |
| Performance | | | | | | |
| Precision | | | | | N/A | |
| Response Time | | | | | Yes | Taken as part of function response time. |
| Update Rate | 5 msec | Hardware Generic Requirements 4.2.7.4 | 5 msec | TLU Specification Sec 3.6.7 | Yes | |
| Display ( ) -- For each display function the following constraints should be considered | | | | | | |
| Function Name | Bypass Display | System Requirement Specification Sec 3.4.2 | Logic per logic diagram. | Drawing E-1834 Sheet 19 | Yes | |
| Process | | | | | | |

Trip Logic Unit

| | | | | | | |
|---|---|---|---|---|---|---|
| Display Algorithm | Yellow if bypassed, green if not-bypassed. | System Requirement Specification Sec 3.4.2 | Yellow if bypassed, green if not-bypassed. | TLU Specification Sec 5.2.7 | Yes | |
| Initialization / Reset Mode | Must be known | Hardware Generic Requirements Sec 4.6.3.5 | Both lit until initialization completed. | TLU Specification Sec 5.2.7 | Yes | |
| Outputs | | | | | | |
| Display Outputs | Lights | Hardware Generic Requirements Sec 4.6.3.5 | LEDs | TLU Specification Sec 5.2.7 | Yes | |
| Performance | | | | | | |
| Uncertainty | | | | | N/A | |
| Response Time | | | | | N/A | Response time of many seconds is acceptable. |
| Update Rate | | | | | N/A | Update interval of many seconds is acceptable. |
| Test () -- For each test function the following constraints should be considered | | | | | | |
| Function Name | Self Test | Hardware Generic Requirements Sec 4.4.7 | Self Test | TLU Specification Sec 6.4.5 | Yes | |
| Inputs | | | | | | |
| Manual Controls | None | Hardware Generic Requirements Sec 4.4.7 | | N/A | Yes | |
| Process | | | | | | |
| Test Process | Verify integrity of each card or module, program flow, RAM and ROM condition, and coincidence logic. Logging of intermittent failures. Testing not to interfere with safety functions, actuate trip functions, or change logic signals. | Hardware Generic Requirements Sec 4.4.7.1 | Verify integrity of each card or module, program flow, RAM and ROM condition, and coincidence logic. Logging of intermittent failures. Testing not to interfere with safety functions, actuate trip functions, or change logic signals. | TLU Specification Sec 6.4.5 | Yes | |
| Initialization / Reset Mode | Must be known | Hardware Generic Requirements Sec 4.6.3.5 | Tests are executed as part of initialization sequence. | TLU Specification Sec 6.4.5 | Yes | |
| Outputs | | | | | | |
| Trip Outputs | None | Hardware Generic Requirements Sec 4.4.7.1 | | | N/A | |
| Local Displays | Fault indication via Display () | Hardware Generic Requirements Sec 4.4.7.1 | LED status displays. | TLU Specification Sec 6.4.5 | Yes | |
| Remote Outputs | Non-intermittent failures output to annunciator and plant computer via Digital Output () | Hardware Generic Requirements Sec 4.4.7.1 | Failure indication via non-essential MUX to plant computer and annunciator. | TLU Specification Sec 6.4.8 | Yes | |
| Performance | | | | | | |
| Uncertainty | | | | | N/A | |
| Response Time | Not to affect trip response time. | Hardware Generic Requirements Sec 4.4.7.1 | Trip signals other than those created by the test are to override test. | TLU Specification Sec 6.4.3 | Yes | Response time of many seconds is acceptable. |
| Update Rate | | | | | Yes | Update interval of many seconds is acceptable. |
| Maintenance Bypass () -- For each bypass function the following constraints should be considered | | | | | | |

# Appendix B

## Trip Logic Unit

| | | | | | | |
|---|---|---|---|---|---|---|
| Function Name | Bypass of detector inputs | System Requirement Specification Sec 4.1.4.6.1, 4.4.4.4.a | Logic per logic diagram. | Drawing E-1834 Sheet 19 | Yes | |
| Inputs | | | | | | |
| Input Description | Bypass Switch Position | System Requirement Specification Sec 4.1.4.6.1 | Logic per logic diagram. | Drawing E-1834 Sheet 19 | Yes | |
| Process | | | | | | |
| Bypass algorithms | Bypass reduces trip logic to 2 out of 3. Interlocks to prevent bypass of more than one division at a time. | System Requirement Specification Sec 4.1.4.6.1.2, 4.4.4.4.a, MSIV Isolation Function Requirement Specification Sec 5.4 | Logic per logic diagram. | Drawing E-1834 Sheet 19 | Yes | |
| Initialization / Reset Mode | Must be known | Hardware Generic Requirements Sec 4.6.3.5 | Initialization in un-bypassed condition. | TLU Specification Sec 2.3.5 | Yes | |
| Outputs | | | | | | |
| Trip Outputs | Bypass status to other TLUs, annunciators, and plant control boards via Digital Output ( ) | System Requirement Specification Sec 4.1.4.6.1.1, 4.4.4.4.a, SAR F7.2-2 | Logic per logic diagram. | Drawing E-1834 Sheet 22 | Yes | |
| Local Displays | Bypass indication via Display ( ) | Hardware Generic Requirements Sec 4.4.7.1 | LED status displays. | TLU Specification Sec 4.4.5 | Yes | |
| Remote Outputs | Bypass status to annunciator and plant computer via Digital Output ( ) | Hardware Generic Requirements Sec 4.4.7.1 | Bypass indication via non-essential MUX to plant computer and annunciator. | TLU Specification Sec 6.4.8 | Yes | |
| Maintain () | | | | | | |
| Function Name | Display intermittent failures | Hardware Generic Requirements Sec 4.4.7.1 | Logging and display of all failures. | TLU Specification Sec 5.3.1 | Yes | |
| Inputs | | | | | | |
| Input Description | Log of intermittent self-test failures from Test ( ) | Hardware Generic Requirements Sec 4.4.7.1 | Logging and display of all failures. | TLU Specification Sec 5.3.1 | Yes | |
| Communications Protocol | | | | | N/A | |
| Process | | | | | | |
| Maintenance Process | Display of failure log | Hardware Generic Requirements Sec 3.4.3.5 | Failure log can be called up on alpha numeric display or down loaded to maintenance terminal. | TLU Specification Sec 5.3.1 | Yes | |
| Initialization / Reset Mode | Must be known | Hardware Generic Requirements Sec 4.6.3.5 | | | | Initialization and reset should not delete failure history. |
| Outputs | | | | | | |

Trip Logic Unit

| | | | | | | |
|---|---|---|---|---|---|---|
| Output Description | Failure log on diagnostic display. | System Requirement Specification Sec 4.1.4.6.1.1, 4.1.4.7, 4.4.4.2 | Failure log can be called up on alpha numeric display or down loaded to maintenance terminal. | TLU Specification Sec 5.3.1 | Yes | |
| Communications Protocol | Per standard maintenance interface. | Hardware Generic Requirements Sec 8.1.4.2 | Reference to standard requirement | TLU Specification Sec 7.5.3 | Yes | |
| Access Control () | | | | | | |
| Function Name | Security for modification of trip logic. | System Requirement Specification Sec 4.1.4.6.1.1 | Password protection of maintenance functions. | TLU Specification Sec 5.8.1 | Yes | |
| Inputs | | | | | | |
| Input Description | | | Key lock switch and password on keypad. | TLU Specification Sec 5.8.2 | Yes | |
| Process | | | | | | |
| Validate Access | | | | | | Needs to be specified |
| Change Access Criteria | | | | | | Needs to be specified |
| Initialization / Reset Mode | Must be known | Hardware Generic Requirements Sec 4.6.3.5 | | | | Needs to be specified. Should be protected during initialization and should initialize in protected mode. |
| Outputs | | | | | | |
| Output Description | Per standard maintenance interface. | Hardware Generic Requirements Sec 8.1.4.2 | Reference to standard requirement | TLU Specification Sec 7.5.3 | Yes | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Failure Detection | | | | | | |
| Failure Annunciation | Provides error flags to module "Error" | Software Architecture Doc Sec. 4.7.2 | Returns error flags on detectable errors. | Software Requirements Specification Sec. 3.5.8 | Yes | |
| Software Portability Provisions | No requirements | Software Architecture Doc | | | N/A | Intended for single platform |
| Failure Tolerance | | | | | | |
| Redundancy | No requirement | | | | N/A | |
| Diversity | Not written in C | DiD&D study | To be written in a safety subset of ADA | Software Requirements Specification Sec. 2.7.4 | Yes | |
| Dominant Failure Mode(s) | Failures should cause trip | TLU Specification Sec 3.2.5 | Status to be set to trip at the beginning of each cycle and reset to non-trip only on successful execution of this module. | Software Requirements Specification Sec. 3.6.4 | Yes | |
| Logical Database | | | | | | |
| Types of information | Function name (string), channel name (integer), channel trip status (binary), time (integer), bypass status (binary), Division trip status (binary) | Software Architecture Doc Sec. 4.2.1 | Function name (string), channel trip status (binary), time (integer), bypass status (binary) | Software Requirements Specification Sec. 3.5.12 | Yes | |
| Frequency of use | Each cycle | Software Architecture Doc Sec. 4.2.1 | Each cycle | Software Requirements Specification Sec. 3.5.12 | Yes | |
| Accessing capabilities | Read only | Software Architecture Doc Sec. 4.2.1 | Read only | Software Requirements Specification Sec. 3.5.12 | Yes | |
| Data entities and their relationships | Division trip status derived from the other parameters. | Software Architecture Doc Sec. 4.7.3 | Specific division trip algorithm provided | Software Requirements Specification Sec. 3.1.4 | Yes | |
| Database Integrity constraints | Shall be defined | Software Architecture Doc Sec. 2.3.4 | Function name - single valid value; channel name - integer 1, 2, 3, or 4; channel trip status - 0=trip 1=no trip, time 00:00:00.000 to 23:59:59.999; bypass status - 0=nobypass, 1=bypass; Division trip - 0=trip, 1=no trip | Software Requirements Specification Sec. 3.6.3 | Yes | |
| Data retention requirements | None | | | | N/A | |

Processing Behaviors

| Attributes | Safety Constraint | Source | Actual Requirement | Source | Constraints Met? | Comments |
|---|---|---|---|---|---|---|
| See software attributes template for attributes | | | | | | |
| Behaviors--Behaviors are defined for software in specific physical devices | | | | | | |
| Process | | | | | | |
| Operating Modes | Trip, Not tripped | | | | | |
| Functional Transformation | Trip if either inboard or outboard MSIV not open on two steam lines and the same function is tripped in at least one other TLU, and the function is not bypassed. | System Requirement Specification Sec 4.4.4.1, SAR F7.2-4, MSIV Isolation Function Requirement Specification Sec 6.2 | Trip on 2/4 MISV channels tripped in any 2 non-tripped division and any other TLU tripped on the same function. Each MISV channel trips on 1/2 MSIV open = false. Also trip if placed into bypass when any other TLU is already in bypass. | Software Requirements Specification Sec. 4.1.3 | Yes | |
| Initialization / Reset Mode | Must be known | Hardware Generic Requirements Sec 4.6.3.5 | Module is to be reset to trip on initialization and at the end of each processing cycle. | Software Requirements Specification Sec. 3.2.5 | Yes | |
| Validity checks on inputs & actions | None | | | N/A | Yes | |
| Exact sequence of operations | Initialization, check bypass status, check trip status, reset | Software Architecture Doc Sec. 4.5.1 | See sequence diagram | Software Requirements Specification Sec. 4.1.3 | Yes | |
| Abnormal events--errors & recovery | Overflow, underflows, termination | Software Architecture Doc Sec. 2.4.3 | Return error on overflow, or underflow. Memory is reset to trip at the end of each processing cycle. Most errors will not allow incorrect reset to no-trip. | Software Requirements Specification Sec. 4.1.3 | Yes | |

# APPENDIX C
# CATALOG OF REQUIREMENTS TOPICS

Appendix C

This appendix reproduces Appendix C of Berg 1999. It provides a listing of requirements topics that were considered in identifying characteristics for inclusion in the review templates and provides a source of topics that might be considered in future modifications of the templates or in the development of new templates.

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.<br>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.<br>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.<br>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)<br>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<br>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)<br>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.<br>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.<br>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.<br>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.<br>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.<br>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)<br>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, and heated thermocouple.<br>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<br>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.<br>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)<br>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.<br>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.<br>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.<br>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.<br>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.<br>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<br>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<br>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)<br>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.<br>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.<br>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.<br>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 fiber optic.<br>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)<br>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.<br>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.<br>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.<br>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.<br>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.<br>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<br>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)<br>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.<br>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.<br>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.<br>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.<br>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<br>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.<br>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.<br>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<br>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<br>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<br>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 watchdog timers, parity checks, inter-channel comparison, range checking.<br>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<br>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.<br>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.<br>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 derated, 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.<br>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 |
|---|---|---|---|---|
| Formal Methods | 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 |

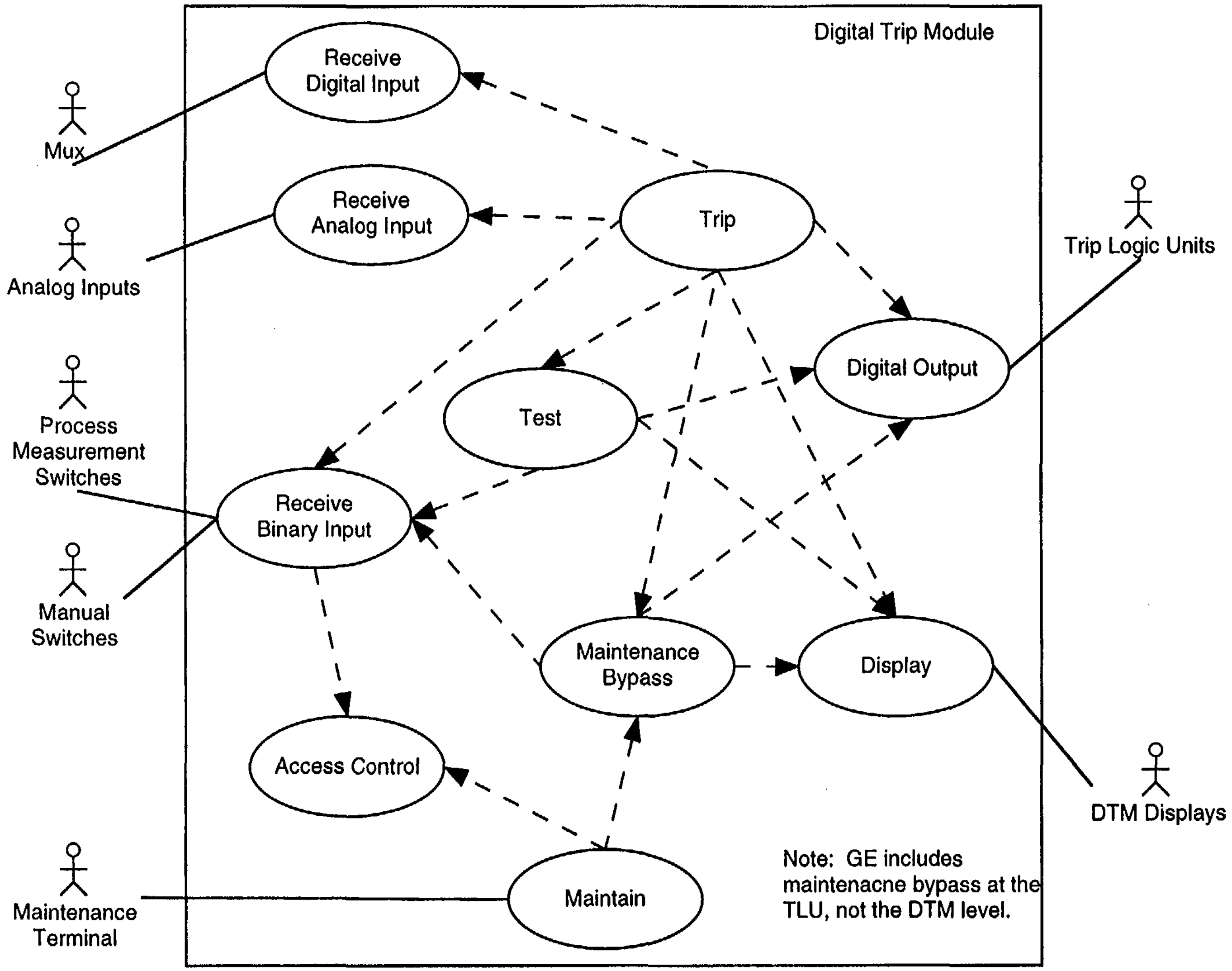
| Topic Name | Definition | Attributes | Characteristics | Comments |
|---|---|---|---|---|
| Energy source | Requirements on the allowable, or expected, interruptions of power to the system or component. | Degree of continuity required e.g., normal without back-up, normal with switchover to backup, 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 noise requirements. | 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.<br>ACE, SF-FT |

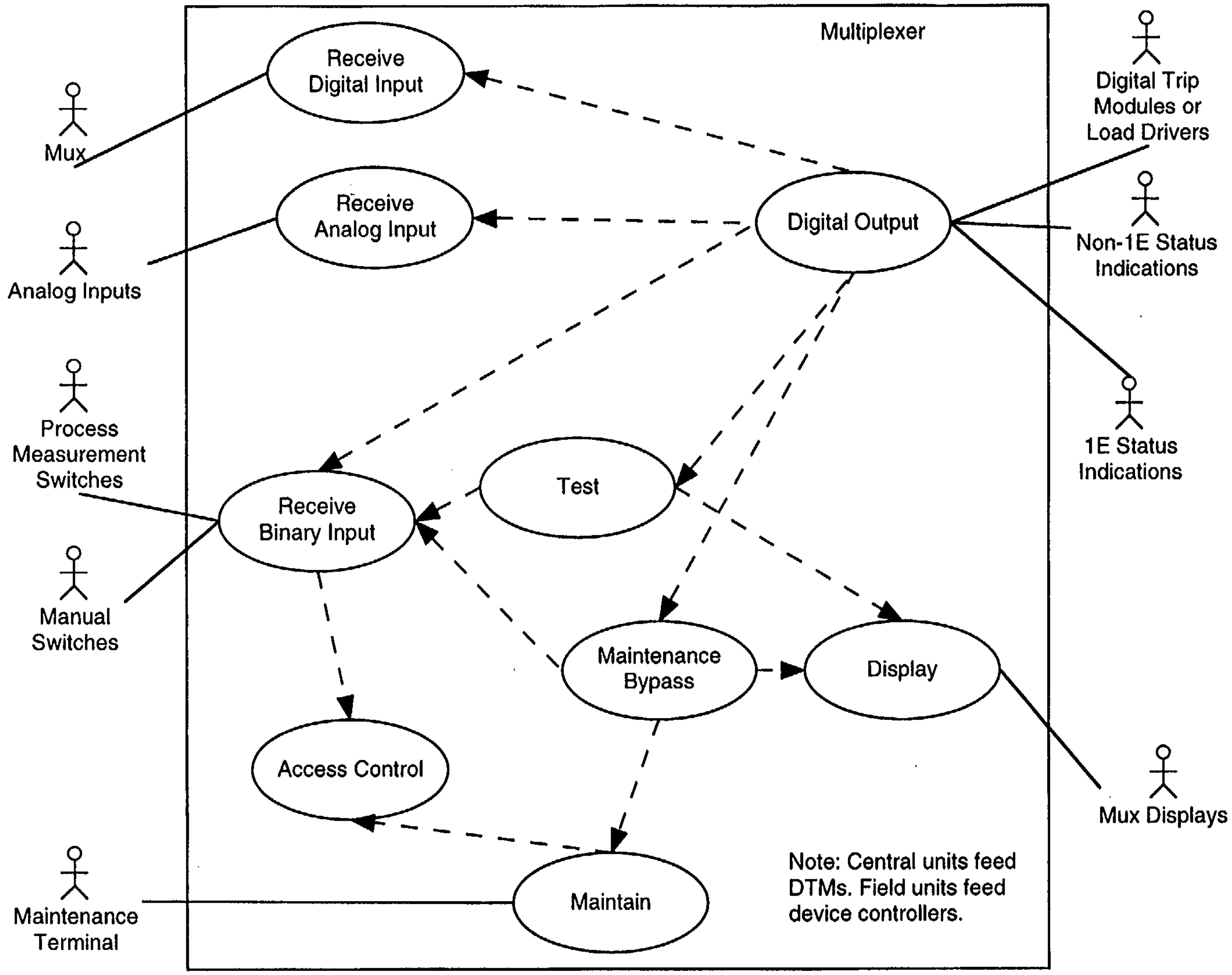
# APPENDIX D
# USE CASE DIAGRAMS

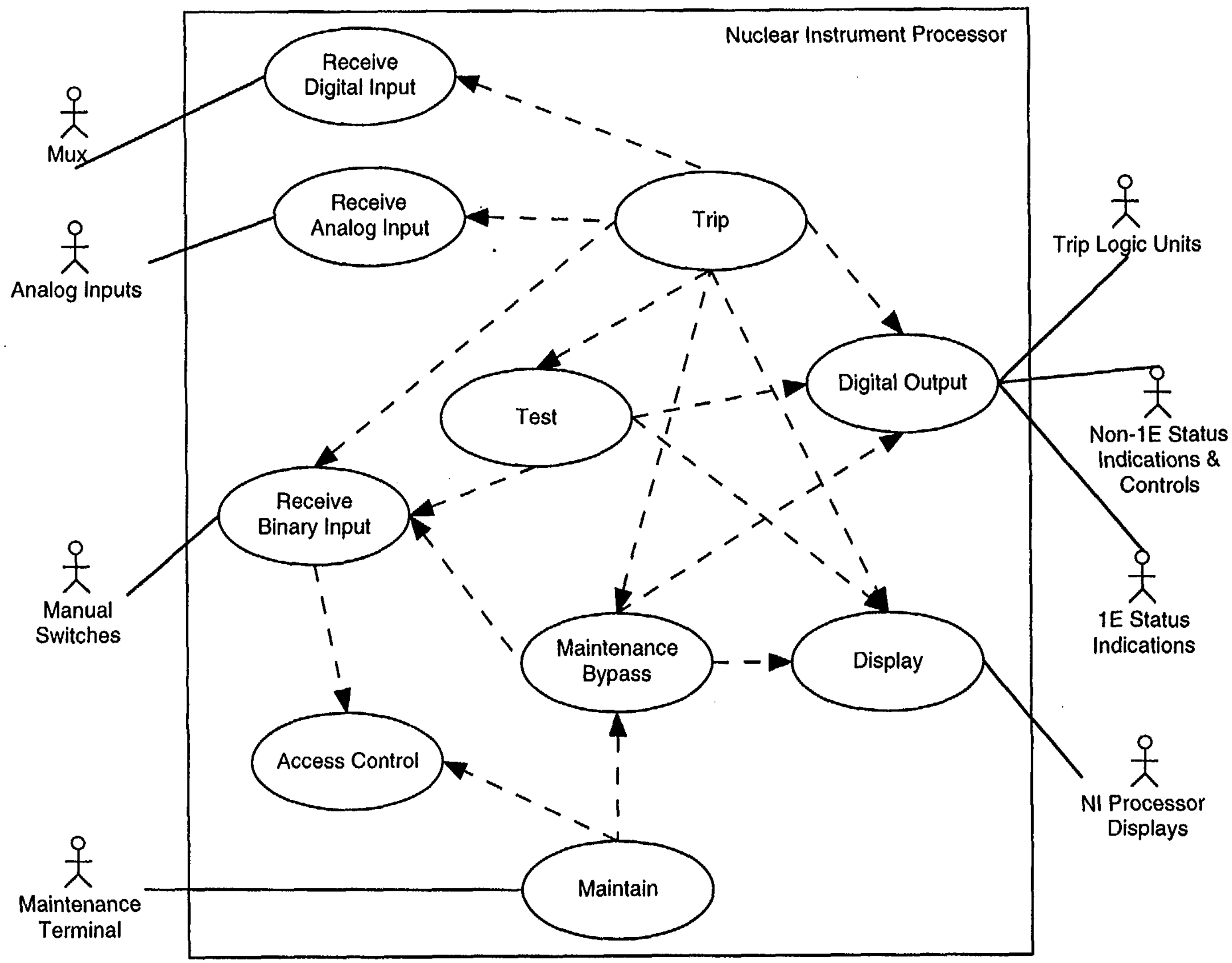
Appendix D

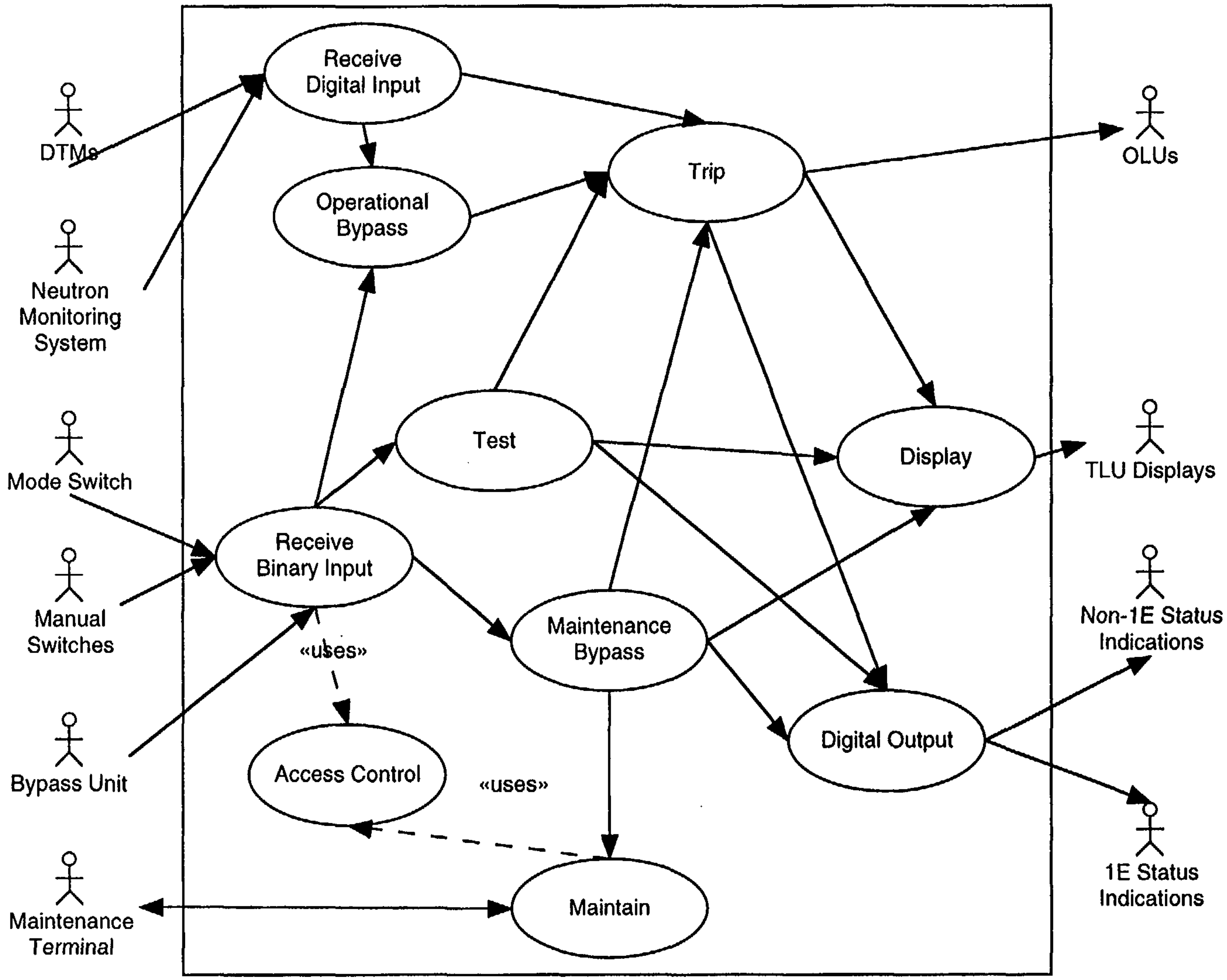
This appendix contains use case diagrams that were developed to examine the behavior of complex protection system components. Each use case in the diagram became a behavior included for which characteristics are defined in the review templates.

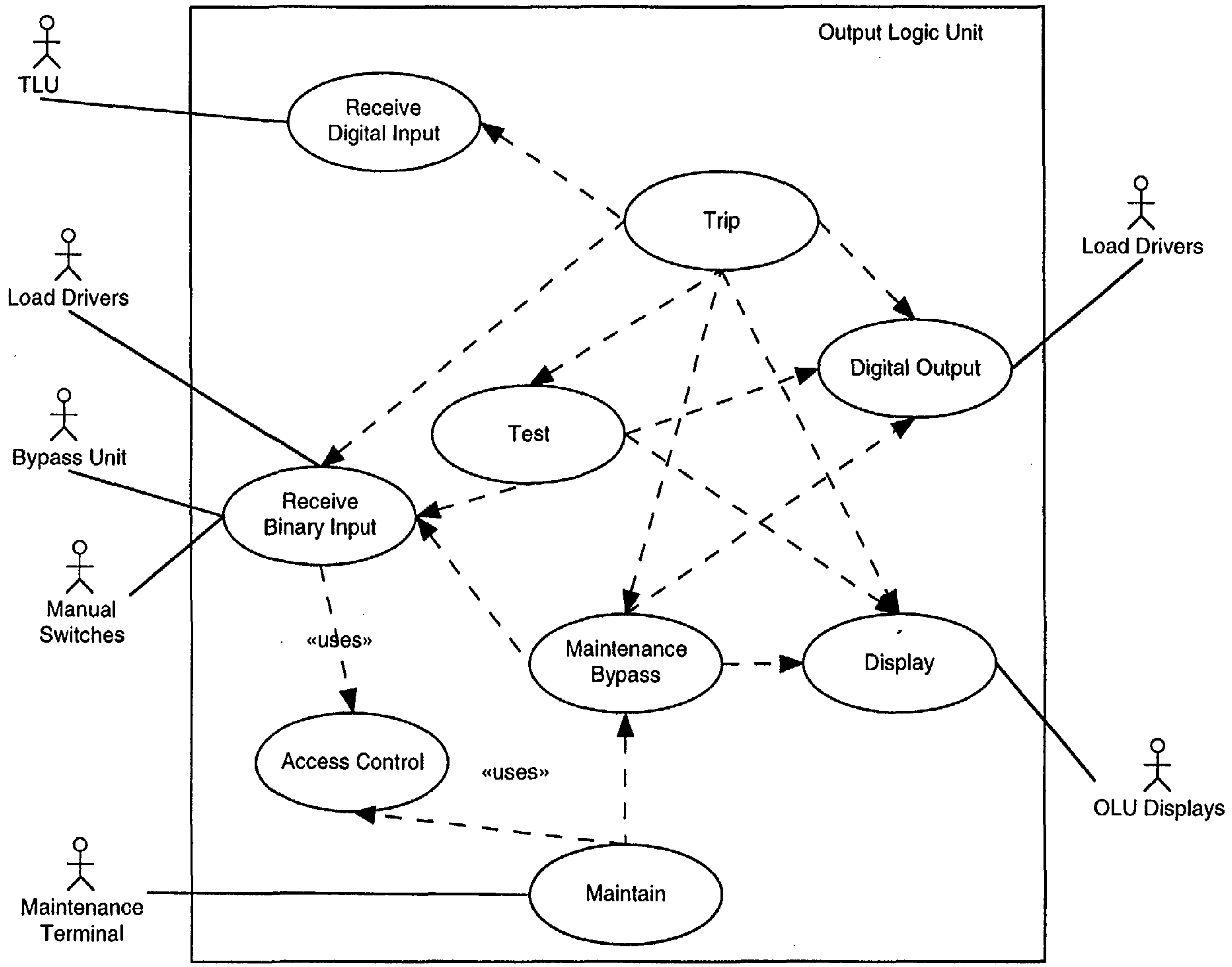


Note: GE includes maintenacne bypass at the TLU, not the DTM level.


Multiplexer
Mux
Analog Inputs
Process Measurement Switches
Manual Switches
Maintenance Terminal
Receive Digital Input
Receive Analog Input
Digital Output
Test
Receive Binary Input
Maintenance Bypass
Display
Access Control
Maintain
Digital Trip Modules or Load Drivers
Non-1E Status Indications
1E Status Indications
Mux Displays
Note: Central units feed DTMs. Field units feed device controllers.


Nuclear Instrument Processor
Receive Digital Input
Mux
Receive Analog Input
Analog Inputs
Trip
Trip Logic Units
Digital Output
Test
Non-1E Status Indications & Controls
Receive Binary Input
Manual Switches
1E Status Indications
Maintenance Bypass
Display
Access Control
NI Processor Displays
Maintain
Maintenance Terminal


DTMs
Neutron Monitoring System
Mode Switch
Manual Switches
Bypass Unit
Maintenance Terminal
Receive Digital Input
Operational Bypass
Trip
Test
Display
Receive Binary Input
«uses»
Maintenance Bypass
Access Control
«uses»
Digital Output
Maintain
OLUs
TLU Displays
Non-1E Status Indications
1E Status Indications


Output Logic Unit
TLU
Receive Digital Input
Trip
Load Drivers
Digital Output
Load Drivers
Test
Bypass Unit
Receive Binary Input
Manual Switches
«uses»
Maintenance Bypass
Display
Access Control
«uses»
OLU Displays
Maintenance Terminal
Maintain

NRC FORM 335
(2-89)
NRCM 1102,
3201, 3202

U.S. NUCLEAR REGULATORY COMMISSION

# BIBLIOGRAPHIC DATA SHEET

*(See instructions on the reverse)*

1. REPORT NUMBER
**(Assigned by NRC, Add Vol., Supp., Rev., and Addendum Numbers, if any.)**

NUREG/CR-6680
UCRL-ID-139344

2. TITLE AND SUBTITLE

Review Templates for Computer-Based Reactor Protection Systems

3. DATE REPORT PUBLISHED

| MONTH | YEAR |
|---|---|
| August | 2000 |

4. FIN OR GRANT NUMBER

W6677

5. AUTHOR(S)

G. Johnson, LLNL and University of California at Berkeley
D. Schrader, LLNL
R. Yamamoto, University of California at Berkeley

6. TYPE OF REPORT

Technical

7. PERIOD COVERED *(Inclusive Dates)*

Dec. 1998-Aug. 2000

8. PERFORMING ORGANIZATION - NAME AND ADDRESS *(If NRC, provide Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address; if contractor, provide name and mailing address.)*

Lawrence Livermore National Laboratory
7000 East Avenue
Livermore, CA 94550

University of California
Berkeley, CA 94720

9. SPONSORING ORGANIZATION - NAME AND ADDRESS *(If NRC, type "Same as above"; if contractor, provide NRC Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address.)*

Division of Engineering Technology
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

10. SUPPLEMENTARY NOTES

R. Brill, NRC Project Manager

11. ABSTRACT *(200 words or less)*

This report provides review templates to help ensure the completeness and traceability of protection system requirements specifications. The templates identify safety important characteristics of reactor protection systems and the hardware and software components that comprise typical computer-based protection systems. The templates include checklists that are used to verify that important safety characteristics are specified in the requirements documents for protection system components, and that the specified characteristics are consistent with the plant safety analysis.

12. KEY WORDS/DESCRIPTORS *(List words or phrases that will assist researchers in locating the report.)*

Software Requirements Specification Guidelines
I&C Protection systems, I&C systems, I&C Component Class,
I&C Characteristic, I&C Attribute, I&C Behavior

13. AVAILABILITY STATEMENT

unlimited

14. SECURITY CLASSIFICATION

*(This Page)*
unclassified

*(This Report)*
unclassified

15. NUMBER OF PAGES

16. PRICE

Printed
on recycled
paper

Federal Recycling Program

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

1975 25 2000
years