Instrumentation and Control Diversity and Defense-in-Depth Technical Report

July 2012
Revision 0
Nonproprietary

NuScale Power, LLC
1100 NE Circle Blvd Suite 350
Corvallis, Oregon 97330
www.nuscalepower.com

This page intentionally blank

PROPRIETARY INFORMATION NOTICE

This document does not contain proprietary information.

COPYRIGHT NOTICE

CONTENTS

TABLES

FIGURES

1.0 Introduction

This NuScale Power, LLC (NuScale) Instrumentation and Control Defense-in-Depth and Diversity Preliminary technical report describes the approach to defense-in-depth and diversity for the instrumentation and control (I&C) systems for the NuScale nuclear power module.

The purpose of this technical report is to describe the reactor protection system (RPS), which consists of the reactor trip system (RTS) and the engineered safety features actuation system (ESFAS). This report provides an overview of the RPS architecture, a discussion of the key attributes of the RPS, and an overview of how NuScale incorporates the four echelons of defense and the six attributes of diversity into the RPS design. In a future revision, this report will discuss in greater detail how the NuScale design incorporates the four echelons of defense and six attributes of diversity within the overall I&C architecture. It will also include an evaluation of the design against the guidelines of NUREG/CR-6303.

The NuScale design includes features and processes that minimize the potential for common-cause failures (CCF) in the RPS. This report discusses the measures taken to ensure that vulnerabilities to CCF have been adequately addressed, as well as how the NuScale design uses a diverse means to mitigate a CCF when a safety function could be disabled.

Echelons of defense are defined in NUREG/CR-6303 (Reference 5.2.1) as "specific applications of the principle of defense-in-depth to the arrangement of instrumentation and control systems attached to a nuclear reactor for the purpose of operating the reactor or shutting it down and cooling it. Specifically, the echelons are the control system, the reactor trip or scram system, the Engineered Safety Features Actuation System (ESFAS), and the monitoring and indicator system."

I&C diversity is a principle of measuring different variables, using different technology, logic or algorithms, or actuation means to provide diverse ways of responding to postulated plant conditions. Six attributes of diversity are discussed in NUREG/CR-6303: human diversity, design diversity, software diversity, functional diversity, signal diversity, and equipment diversity. This report discusses the methods NuScale is using to incorporate the six attributes of diversity into its RPS design.

1.1 Abbreviations and Definitions

Table 1-1. Abbreviations

Term	Definition
AOO	anticipated operational occurrences
ATWS	anticipated transient without scram
BOP	balance of plant
CCF	common-cause failure
ESF	engineered safety features
ESFAS	engineered safety features actuation system
I&C	instrumentation and controls
NCIS	non-safety control and instrumentation system
NSSS	nuclear steam supply system

Term	Definition
MWS	maintenance workstation
RCIS	rod control and information system
RCS	reactor coolant system
RPS	reactor protection system
RTS	reactor trip system
SCIS	safety control and instrumentation system

Table 1-2. Definitions

Term	Definition
accident	Any unintended event, including operating errors, equipment failures, or other mishaps, the consequences or potential consequences of which are not negligible from the point of view of protection or safety requirements of its application.
anticipated operational occurrences (AOO)	A condition of normal operation that is expected to occur one or more times during the life of the plant.
channel	A set of interconnected hardware and software components that processes an identifiable sensor signal to produce a single protective action signal in a single division when required by a generating station condition. A channel includes the sensor, data acquisition, signal conditioning, data transmission, bypasses, and logic up to voters or actuating device inputs. The objective of the channel definition is to define subsets of a reactor protection system that can be unambiguously tested or analyzed from input to output.
common cause failure (CCF)	A failure caused by software errors or software-developed logic that could defeat the redundancy achieved by hardware architecture.
control system	A set of devices and equipment in place to ensure stability, accuracy, and smooth transition of a process or activity.
design diversity	One of the six attributes of diversity important to the design of instrumentation systems. Design diversity is the use of different approaches, including software and hardware, to solve the same or a similar problem. Software diversity is a special case of design diversity and is mentioned separately because of its potential importance and its potential defects. The rationale for design diversity is that different designs have different failure modes and are not be susceptible to the same common influences.
deterministic	Behaves in a predictable manner.
diversity	The principle in instrumentation systems of sensing different parameters, using different technologies, logic or algorithms, or means of actuation to provide several ways of detecting and responding to a significant event. Diversity is complementary to the principle of defense-in-depth and increases the chances that defenses at a particular level or depth will be actuated when needed. There are six attributes of diversity: human diversity, design diversity, software diversity, functional diversity, signal diversity, and equipment diversity.
division	The designation applied to a given system or set of components that enables the establishment and maintenance of physical, electrical, and functional independence from other redundant sets of components.

Term	Definition
echelons of defense	Specific applications of the principle of defense-in-depth to the arrangement of instrumentation and control systems attached to a nuclear reactor for the purpose of operating the reactor or shutting it down and cooling it. Specifically, the echelons are the control system, the reactor trip or scram system, the ESFAS, and the monitoring and indicator system.
engineered safety features actuation system (ESFAS)	A system that is specifically engineered for mitigating the effects of an accident.
equipment diversity	One of the six attributes of diversity important to the design of instrumentation systems. Equipment diversity is the use of different equipment to perform similar safety functions. In this case, "different" means sufficiently unlike as to significantly decrease vulnerability to common failure.
functional diversity	One of the six attributes of diversity important to the design of instrumentation systems. Two systems are functionally diverse if they perform different physical functions though they may have overlapping safety effects.
human diversity	One of the six attributes of diversity important to the design of instrumentation systems. Relates to addressing human-induced faults throughout the system development life-cycle (e.g., mistakes, misinterpretations, errors, configuration failures) and is characterized by dissimilarity in the execution of life-cycle processes.
module	Any assembly of interconnected components that constitutes an identifiable device, instrument, or piece of equipment. A module can be disconnected, removed as a unit, and replaced with a spare. It has definable performance characteristics that permit it to be tested as a unit.
monitoring and indicator system	The slowest and also the most flexible echelon of defense. The monitoring and indicator system echelon includes both Class 1E and non-Class 1E manual controls, monitors, and indicators required to operate equipment nominally assigned to the other three echelons.
protective action	The initiation of a signal within the sense and command features or the operation of equipment within the execute features to accomplish a safety function.
protective function	The measurement of one or more variables associated with a particular generating station condition, the signal processing, and the initiation and completion of the protective action at values established in the design bases.
reactor protection system (RPS)	A subset of the SCIS that initiates safety actions to mitigate the consequences of design basis events. The reactor protection system includes the RTS and the ESFAS.
reactor trip system (RTS)	The RTS echelon consists of safety equipment designed to reduce reactivity rapidly in response to an uncontrolled event. The RTS is part of the RPS, which includes all equipment (including hardware, software, and firmware) from sensors to actuation devices (power sources, sensors, signal conditioners, initiation circuits, logic, bypasses, interlocks, racks, panels, control boards, interconnections, and actuation devices) required to initiate reactor shutdown. The RTS is designed to automatically initiate the reactivity control system (control rods) to ensure that specified acceptable fuel design limits are not exceeded.
safety function	One of the processes or conditions essential to maintain plant parameters within acceptable limits established for a design basis event. A safety function is achieved by the RTS or the ESF completing all required protective actions or the auxiliary supporting features completing all required protective actions, or both.

Term	Definition
sensor	The portion of a channel that responds to changes in a plant variable or condition and converts the measured process variable into an electric, optic, or pneumatic signal.
separation group	A physical grouping of process channels with the same Class-1E electrical channel designation (I, II, III, or IV). Each of the four redundant separation groups is provided with separate and independent power feeds and process instrumentation transmitters. Each of the four redundant separation groups is physically and electrically independent of the other groups.
signal diversity	One of the six attributes of diversity important to the design of instrumentation systems. Signal diversity is the use of different parameters to initiate protective action, in which any of the parameters may independently indicate an abnormal condition, even if the other parameters fail to be detected correctly.
single failure	A random failure that results in the loss of the capability of a component to perform its intended safety function. Consequential failures resulting from a single random occurrence are considered to be part of the single failure.
software diversity	One of the six attributes of diversity important to the design of instrumentation systems. Software diversity is the use of different software programs designed and implemented by different software development groups with different key personnel to accomplish the same safety goals, for example, using two separately designed programs to determine when a reactor should be tripped.
state machine	A collection of digital logic circuits that can be in one of a finite number of states. The machine is in only one state at a time, called the current state. The state machine changes from one state to another when initiated by a triggering event or set of conditions. This change is called a state transition or transition.

2.0 Instrumentation and Control Architecture and the Echelons of Defense

The primary purpose of the instrumentation and control (I&C) systems is to provide automatic initiating signals, automatic and manual control signals, and monitoring displays to mitigate the consequences of fault conditions. The I&C systems provide protection against unsafe reactor operation during steady state and transient power operation.

During normal operation, the NuScale power plant instrumentation measures various parameters and transmits the signals to the control systems. During abnormal operation and accident conditions, the instrumentation transmits signals to the reactor trip system (RTS) and engineered safety features actuation system (ESFAS) based on predetermined set points.

2.1 Overview

The NuScale I&C architecture consists of the following systems (see Figure 2-1):

- non-safety control and instrumentation system (NCIS)
- safety control and instrumentation system (SCIS)
- monitoring and indicator system

The NCIS provides control and monitoring of the following systems:

1. non-safety nuclear steam supply system (NSSS), such as secondary steam bypass to condensers, pressurizer heaters and spray, and feedwater control
2. balance of plant (BOP) systems, such as turbine control and atmospheric relief valves
3. rod control and information system (RCIS)

A function of the NCIS is to constrain operational transients, to prevent unit trip, and re-establish steady state unit operation.

The RTS is part of the SCIS. The RTS consists of four independent separation groups with independent measurement channels to monitor plant parameters that can generate a reactor trip. Each measurement channel trips when the parameter exceeds a predetermined set point. The RTS coincident logic is designed so that no single failure can prevent a reactor trip when required, and no failure in a single measurement channel can generate an unnecessary reactor trip.

The ESFAS is part of the SCIS. The ESFAS consists of four independent measurement channels that monitor plant parameters that activate the operation of the engineered safety features (ESF) systems. Each measurement channel trips when the parameter exceeds a predetermined set point. The ESFAS coincident logic is designed so that no single failure can prevent a safeguards actuation when required, and no single failure in a single measurement channel can generate an unnecessary safeguards actuation.

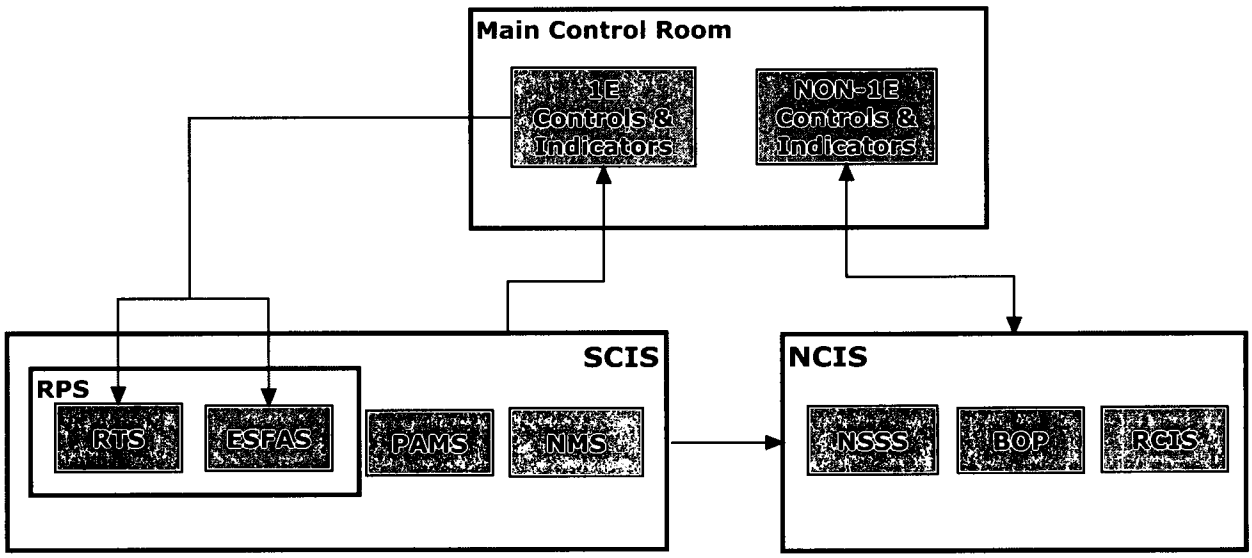

Figure 2-1. Instrumentation and control architecture overview

2.2 Echelons of Defense

The four echelons of defense (see Figure 2-2) are defined in NUREG/CR-6303 (Reference 5.2.1). The following subsections define each echelon of defense and describe the NuScale I&C system or systems that achieve each of the echelons.

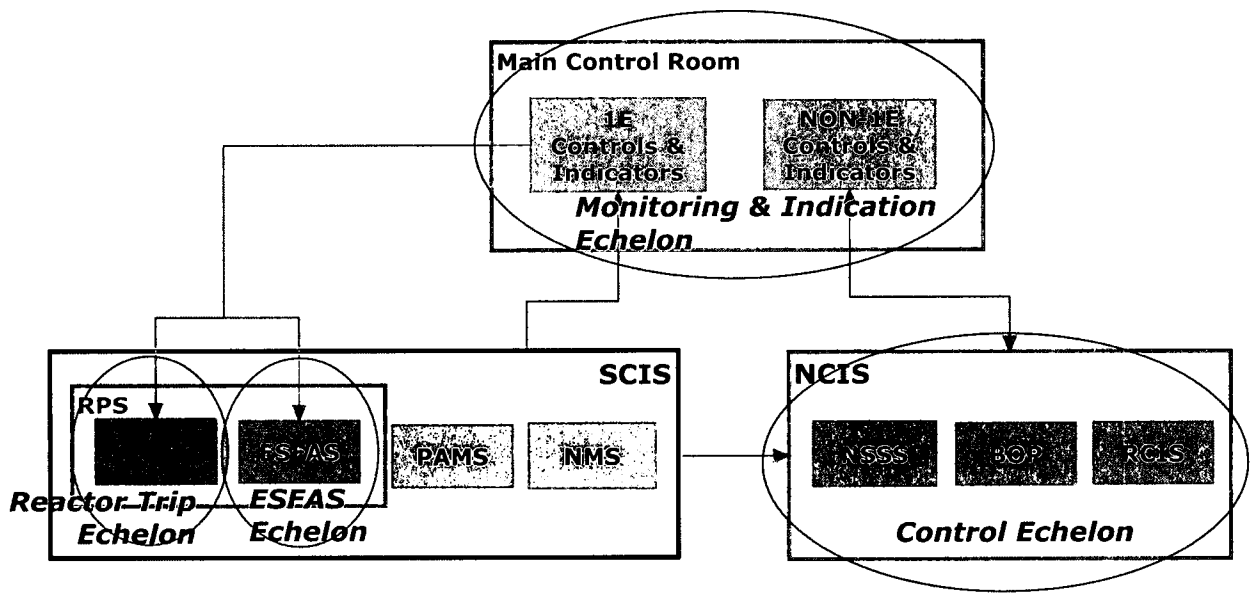

Figure 2-2. Overall instrumentation and control architecture and the echelons of defense

2.2.1 Control System

"The control echelon is that non-Class 1E manual or automatic equipment which routinely prevents reactor excursions toward unsafe regimes of operation and is generally used to operate the reactor in the safe power production operating region. Indicators, annunciators, and alarms may be included in the control echelon. Reactor control systems typically contain some equipment to satisfy the ATWS rule (10 CFR 50.62) or the requirement for a remote shutdown panel. Examples of such equipment include high-quality non-Class 1E equipment for which credit may be taken solely for compensating rare common-cause failures of Class 1E reactor protection equipment." (NUREG/CR-6303, paragraph 2.2.1)

The reactor control functions performed by the control system echelon are included in the NCIS. The NCIS includes functions to maintain the plant within operating limits to avoid the need for reactor trip or ESF actuation.

2.2.2 Reactor Trip System

"The reactor trip echelon is that safety equipment designed to reduce reactivity rapidly in response to an uncontrolled excursion. It consists of instrumentation for detecting potential or actual excursions, means for rapidly and completely inserting the reactor control rods, and may also include certain chemical neutron moderation systems (e.g., boron injection)." (NUREG/CR-6303, paragraph 2.2.2)

The automatic reactor trip functions performed by the reactor trip echelon are included in the SCIS.

2.2.3 Engineered Safety Features Actuation System

"The ESFAS echelon is that safety equipment which removes heat or otherwise assists in maintaining the integrity of the three physical barriers to radioactive release (cladding, vessel, and containment). This echelon detects the need for and performs such functions as emergency cooling, pressure relief or depressurization, isolation, and control of various support systems (e.g., emergency generators) or devices (valves, motors, pumps) required for ESF equipment to operate." (NUREG/CR-6303, paragraph 2.2.3)

The automatic ESF actuation functions performed by the ESFAS echelon are included in the SCIS.

2.2.4 Monitoring and Indicator System

"The monitoring and indication echelon is the slowest and also the most flexible echelon of defense. Like the other three echelons, operators are dependent upon accurate sensor information to perform their tasks, but, given information, time, and means, can perform previously unspecified logical computations to react to unexpected events. The monitoring and indication echelon includes Class 1E and non-Class 1E manual controls, monitors, and indicators required to operate equipment nominally assigned to the other three echelons." (NUREG/CR-6303, paragraph 2.2.4)

The functions required by the monitoring and indicator system echelons are provided by the manual controls, displays, and indicators in the main control room, which includes information from the NCIS and SCIS. The safety monitoring, manual reactor trip, and manual ESF actuation functions are included in the SCIS. The NCIS provides non-safety monitoring and manual controls to maintain operating limits during normal plant operation.

3.0 Reactor Protection System

The NuScale integrated reactor protection system (RPS) (see Figure 3-1) incorporates key attributes including independence, redundancy, determinism, multi-layered diversity, and diagnostics. The RPS is designed to ensure the NuScale reactor is maintained in a safe condition and aligns with the fundamental design aspects of the NuScale reactor— simple, highly reliable, and safe.

[[

]]3(a)-(c)

[[

]]3(a)-(c)

3.1.1 Sensors and Detectors

The process sensors are responsible for measuring different process parameters such as pressure, temperature, and level. Each process parameter is measured using different sensors [[ ]]3(a),(c)

The neutron flux detectors are responsible for measuring neutron flux from a reactor shutdown condition to 120 percent of full power. The three types of neutron flux detectors used in the RPS architecture are source range, intermediate range, and power range. Figure 3-2 illustrates the sensors and detectors associated with each separation group.

[[

]]3(a),(c)

Figure 3-2. Sensors and detectors

3.1.2 Signal Conditioning

[[

]]3(a),(c)

[[

]]3(a),(c)

Figure 3-3. Signal conditioning block

3.1.3 Trip Determination

[[

]]$^{3(a)-(c)}$

Figure 3-4. Trip determination block

3.1.4 Reactor Trip System

The RTS is a functional block within the RPS that includes four independent measurement channels that monitor plant parameters. Each measurement channel trips when the sensed parameter exceeds a predetermined set point. The RTS keeps the reactor operating within a safe region by automatically shutting down the reactor whenever the limits of safe operation are approached. The safe operating region is defined by several considerations, such as mechanical or hydraulic limitations on equipment and heat transfer phenomena.

The RTS monitors process variables that are directly related to equipment mechanical limitations, such as pressurizer pressure and pressurizer water level. It also monitors variables that directly affect the heat transfer capability of the reactor, such as reactor coolant temperatures.

Other trip functions in the RTS, such as over-temperature delta-temperature, are calculated from multiple process variables, including reactor coolant temperature, pressurizer pressure, and neutron flux. Whenever a direct process variable or calculated variable exceeds a set point, the reactor is shut down to protect against damage to fuel cladding or loss of system integrity, which could lead to the release of radioactive materials into the containment vessel.

[[

]]$^{3(a)-(c)}$

[[

]]3(a)-(c)

Figure 3-5. Reactor trip system

3.1.5 Engineered Safety Features Actuation System

The ESFAS consists of four independent measurement channels that monitor plant parameters that activate the operation of the ESF systems. Each measurement channel trips when the parameter exceeds a predetermined set point.

The ESFAS logic is arranged so that no single failure can prevent a safeguards actuation when required, and no single failure in a single measurement channel can generate an unnecessary safeguards actuation. The ESFAS provides both automatic and manual initiation of critical systems, such as the emergency core cooling system and the decay heat removal system.

[[

]]3(a)-(c)

[[

]]3(a)-(c)

Figure 3-6. Engineered safety features actuation system

3.2 Independence

The RPS is designed to ensure a high level of independence between the key elements. This includes independence between the four separation groups of sensors and detectors, the four separation groups of trip determination, the four separation groups of the RTS, the two divisions of the ESFAS circuitry, and the two divisions of the ESF equipment.

[[

]]3(a)-(c)

3.3 Redundancy

The RPS design incorporates redundancy in multiple areas of the architecture. The redundancy within the RPS includes four separation groups of sensors and detectors, trip determination and RTS, and two divisions of ESFAS circuitry (see Figure 3-1).

[[

]]3(a)-(c)

3.4 Determinism

The RPS incorporates a deterministic design. [[

]]3(a)-(c)

3.5 Multi-Layered Diversity

The RPS utilizes a multi-layered diversity approach. The design attributes of the RPS are intentionally implemented to eliminate the concern for software-based or software logic-based common-cause failure (CCF).

[[

]]3(a)-(c)

[[

]]3(a)-(c)

Figure 3-7. Multi-layered diversity within the RPS

[[

]]3(a)-(c)

[[

]]3(a)-(c)

Figure 3-8. Example of multiple safety functions to mitigate an AOO

[[

]]3(a)-(c)

[[

]]3(a)-(c)

Figure 3-9. Example of mitigation of an AOO when a CCF occurs

3.6 Simplicity

The RPS architecture is designed specifically for the NuScale reactor. Its design is intended to complement the safe and simple attributes of the NuScale reactor. The RPS implements straightforward design techniques to realize this simple, highly reliable, and safe design.

The key design techniques include the following:

[[

]]$^{3(a)-(c)}$

3.7 Testing and Diagnostics

The RPS incorporates a combination of continuous self-testing and periodic surveillance testing. This test strategy ensures all detectable failures are identified and announced to the station personnel.

The self-test features provide a comprehensive diagnostic system ensuring system status is continually monitored. All detectable failures are announced to station personnel, and an indication of the impact of the failure is provided to determine the overall status of the system. The self-test features maintain separation group and channel independence. The self-test features ensure system integrity is maintained at all times.

[[

]]$^{3(a)-(c)}$

[[

]]$^{3(a)-(c)}$

4.0 Diversity and Defense-in-Depth Analysis—NUREG/CR-6303 Guidelines Evaluation

NUREG/CR-6303 describes a method for analyzing CCF vulnerability of computer-based protection systems. NUREG/CR-6303 provides fourteen guidelines for performing a diversity and defense-in-depth analysis. This report focuses on the reactor protection system (RPS), which consists of the reactor trip system (RTS) and the engineering safety features actuation system (ESFAS). Because this report only describes the NuScale RPS and not the overall NuScale I&C architecture, these guidelines have not been assessed at this time. A future revision of this report will contain an evaluation of the NuScale I&C design against the guidelines of NUREG/CR-6303.

5.0 References

5.1 Source Documents

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

5.1.2 Institute of Electrical and Electronics Engineers, IEEE Standard 384-1981, "IEEE Criteria for Independence of Class 1E Equipment and Circuits."

5.1.3 Institute of Electrical and Electronics Engineers, IEEE Standard 323-2003, "Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations."

5.1.4 Institute of Electrical and Electronics Engineers, IEEE Standard 7-4.3.2-2003, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations."

5.1.5 U.S. Nuclear Regulatory Commission, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," NUREG-0800, Sections 7.1, 7.2, and 7.3, Revision 5, March 2007.

5.1.6 U.S. Nuclear Regulatory Commission, "Guidance on Self-Test and Surveillance Test Provisions," Branch Technical Position 7-17, Rev. 5, March 2007.

5.1.7 U.S. Nuclear Regulatory Commission, "Guidance for Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems," Branch Technical Position 7-19, Rev. 5, March 2007.

5.1.8 U.S. Nuclear Regulatory Commission, "Guidance on Digital Computer Real-Time Performance," Branch Technical Position 7-21, Rev. 5, March 2007.

5.1.9 U.S. Nuclear Regulatory Commission, "Periodic Testing of Protection System Actuation Functions," Regulatory Guide 1.22, Rev. 0, February 1972.

5.1.10 U.S. Nuclear Regulatory Commission, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems," Regulatory Guide 1.47, Rev. 1, February 2010.

5.1.11 U.S. Nuclear Regulatory Commission, "Application of the Single-Failure Criterion to Safety Systems," Regulatory Guide 1.53, Rev. 2, November 2003.

5.1.12 U.S. Nuclear Regulatory Commission, "Periodic Testing of Electric Power and Protection Systems," Regulatory Guide 1.118, Rev. 3, April 1995.

5.2 Referenced Documents

5.2.1 U.S. Nuclear Regulatory Commission, "Method for Performing Diversity and Defense-in-Depth Analysis of Reactor Protection Systems," NUREG/CR-6303, Rev. 1, December 1994.