# CHAPTER 7

# INSTRUMENT AND CONTROL SYSTEMS

## Table of Contents

**Table of Contents**

**Table of Contents**

## List of Tables

## List of Figures

## Acronyms and Abbreviations

| Acronym/Abbreviation | Definition |
|---|---|
| 1oo2 | one out of two voting |
| 2oo3 | two out of three voting |
| A/E | alarm/events |
| AHR | aqueous homogeneous reactor |
| ANS | American Nuclear Society |
| BWR | boiling water reactor |
| CAAS | criticality accident alarm system |
| CAMS | continuous air monitoring system |
| CGD | commercial grade dedication |
| COTS | commercial off-the-shelf |
| CSSD | cold safe shut down |
| DCS | digital control system |
| DBE | design basis event |
| EPRI | Electric Power Research Institute |
| ESD | emergency shut down |
| ESF | engineered safety feature |
| ESFAS | engineered safety feature actuation system |
| FFPS | facility fire protection system |
| FMEA | failure modes and effects analysis |
| FICS | facility integrated control system |
| GDC | general design criteria |
| GOTS | government off-the-shelf |
| HCFD | hot cell fire detection and suppression system |
| HFE | human factors engineering |

**Acronyms and Abbreviations (cont'd)**

| Acronym/Abbreviation | Definition |
|---|---|
| HMI | human machine interface |
| IEC | International Electrotechnical Commission |
| IEEE | The Institute of Electrical & Electronic Engineers |
| IF | irradiation facility |
| ISA | Instrumentation, Systems, and Automation Society |
| ISO | International Organization for Standardization |
| IU | irradiation unit |
| $k_{eff}$ | effective neutron multiplication factor |
| LCO | limiting conditions for operation |
| LSSS | limiting safety system settings |
| LWPS | light water pool system |
| M | subcritical multiplication factor |
| MEPS | molybdenum extraction and purification system |
| MSV | mean square voltage |
| MUPS | light water pool makeup and purification system |
| NDAS | neutron driver assembly system |
| NDI | non-developmental items |
| NFDS | neutron flux detection system |
| NRC | United States Nuclear Regulatory Commission |
| OIT | operator interface terminal |
| PCLS | primary closed loop cooling system |

**Acronyms and Abbreviations (cont'd)**

| Acronym/Abbreviation | Definition |
|---|---|
| PLC | programmable logic controller |
| PRL | power range level |
| PSAR | preliminary safety analysis report |
| PSB | primary system boundary |
| PVVS | process vessel vent system |
| PWR | pressurized water reactor |
| RAMS | radiation area monitoring system |
| RCA | radiologically controlled area |
| RDS | radiation drain system |
| RICS | radiologically controlled area integrated control system |
| ROC | rate of change |
| RPCS | radioisotope process facility cooling system |
| RPF | radioisotope production facility |
| RTD | resistive temperature device |
| SCAS | sub-critical assembly system |
| SHINE | SHINE Medical Technologies, Inc. |
| SIF | safety instrumented function |
| SIL | safety integrity level |
| SIS | safety instrumented system |
| SNM | special nuclear material |
| SQAP | software quality assurance plan |
| SR | safety related |
| SRL | source range level |
| SRP | source range period |
| SSC | structures, systems, or components |
| TC | thermocouple |

**Acronyms and Abbreviations (cont'd)**

| Acronym/Abbreviation | Definition |
|---|---|
| TMR | triple modular redundancy |
| TOGS | TSV off gas system |
| TPCS | target solution vessel process control system |
| TPS | tritium purification system |
| TRPS | target solution vessel reactivity protection system |
| TS | target solution |
| TSPS | target solution preparation system |
| TSV | target solution vessel |
| UNCS | uranyl nitrate conversion system |
| V&V | verification & validation |
| WRL | wide range level |
| WRP | wide range period |

# CHAPTER 7

# INSTRUMENT & CONTROL SYSTEM

## 7a1 HETEROGENEOUS REACTOR INSTRUMENT & CONTROL SYSTEMS

The SHINE Medical Technologies, Inc. (SHINE) facility is not a reactor-based facility; therefore, this section does not apply to the SHINE facility.

# 7a2 IRRADIATION FACILITY INSTRUMENT & CONTROL SYSTEMS

## 7a2.1 SUMMARY DESCRIPTION

Within the SHINE facility, the irradiation unit (IU) cell houses the neutron driver and the TSV, which holds the target solution. The TSV is part of the subcritical assembly system (SCAS). There are eight IU cells that are contained within the irradiation facility (IF). The SHINE facility utilizes two separate, distinct, and independent systems to protect and control the neutron driver and the TSV residing in the IU cell.

### 7a2.1.1 REACTIVITY PROTECTION SYSTEMS

To protect the TSV and entire primary system boundary (PSB), SHINE uses a digital control system (DCS) designated as the TSV reactivity protection system (TRPS) which is further described in Section 7a2.4. The TRPS is responsible for monitoring various essential inputs and has the ability to mitigate abnormal or accident conditions through automated protective actions. The protective actions include opening the TSV dump valves, deenergizing the neutron driver, closing the TSV fill valves, and closing the TSV dump tank outlet valves. This system is classified as a safety-related system. See Figures 7a2.1-1 and 7a2.2-1 for an overview of the TRPS design.

### 7a2.1.2 REACTIVITY CONTROL SYSTEMS

The TSV process control system (TPCS) is used for control of normal operations, startup, and shutdown of the neutron driver and the TSV residing in the IU cell. This system is a separate digital control system and is independent from the TRPS. The TPCS is nonsafety-related and is further described in Section 7a2.3.

### 7a2.1.3 REACTIVITY DETECTION SYSTEMS

The primary means for monitoring the reactivity and power of the SCAS is with a system of redundant channel neutron flux detectors. This is an independent system called the neutron flux detection system (NFDS). It measures neutron flux outside of the TSV and provides input to the TPCS and TRPS. These are redundant and independent signal channels that represent the neutron flux in the SCAS. The NFDS has independent high flux trip settings that are input signals to the TRPS. Should the neutron flux measured at the detectors exceed the allowable operating conditions, the NFDS triggers the TRPS to perform its protective action. There is a separate independent NFDS for each IU cell in the SHINE facility. This system is further described in Section 7a2.4.3.

### 7a2.1.4 ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

The engineered safety features actuation system (ESFAS) consists of two independent safety-related analog relay trains. If the ESFAS senses essential parameters outside predefined limits, it automatically activates the engineered safety features (ESF) mitigative actions for the affected IU cell and TOGS shielded cell. In an actuation event, the ESFs move to a safe state. During activation, the ESFAS isolates systems that penetrate the IU cell and TOGS shielded cell boundaries, including the bubble-tight dampers in the radiologically controlled area (RCA) ventilation system Zone 1 (RVZ1) cells. In addition, the ESFAS signals the TRPS to actuate its

trip mechanisms. The ESFAS can isolate any individual IU cell or all of the IU cells or any combination depending on the need. This system is further described in Section 7a2.5.

### 7a2.1.5 CONTROL ROOM AND INSTRUMENT DISPLAYS

The irradiation facility (IF) is monitored and controlled from a centralized control room. The TRPS and the TPCS each have separate dedicated operator workstations complete with annunciation, alarm, and operator interface displays. The TRPS and TPCS operator workstations are electrically isolated and independent systems. Within the control room there are two consoles, containing the operator workstations, which are redundant in nature and can be operated simultaneously and independently. From these consoles, an operator can assess the state of each IU within the IF. The operator can view and trend critical measurement values from the operator interface display, one for TRPS and one for the TPCS. At the TPCS workstation, the operator can control the target solution irradiation process. During this process, the operator is provided real-time data from the essential measurements used to control and monitor the irradiation process on the TPCS displays. This system is further described in Section 7a2.6.

Additionally, the control room houses the annunciation for the radiation monitoring that occurs throughout the IF and the radioisotope production facility (RPF). The IF and RPF utilize a continuous air monitoring system (CAMS) and radiation area monitoring system (RAMS) for continuous radiological monitoring. The RAMS and CAMS are strategically placed throughout the facility to alert personnel of any potential radiation hazards. These systems are further described in Section 7a2.7.

The human-machine interface is addressed in Section 7a2.6.

## 7a2.2 DESIGN OF INSTRUMENTATION AND CONTROL SYSTEMS

There are two sections to the RCA: the IF and the RPF. This section directly addresses the evaluation of the design criteria and design basis for the instrument and controls to be employed for the IF.

The intent of Appendix A to 10 CFR 50, General Design Criteria for Nuclear Power Plants, is applied to the instrument and control design as outlined in Section 3.5a, which discusses the application of these General Design Criteria (GDC) to the IF in length. In addition to the discussion in Section 3.5a, this section sets specific guidelines and requirements for the instrument and controls for the TRPS, ESFAS, and NFDS.

### 7a2.2.1 DESIGN CRITERIA

The majority of the criteria cited herein were developed for nuclear power plants for construction and operation. The evaluation in this section takes into account that the SHINE facility is not a power reactor, but that the intent of the criteria and guidelines provides a strong basis for the design.

The applicable criteria and guidelines as they apply to the IF instrumentation and controls are presented and summarized in Table 7a2.2-1.

### 7a2.2.2 DESIGN BASIS REQUIREMENTS

The design bases for major systems utilized in the SHINE facility are detailed with the selected design criteria in Table 7a2.2-1. The design basis as it is applied to the IF and the means for compliance are discussed in this table, design criteria on the left, design bases on the right.

### 7a2.2.3 SYSTEM DESCRIPTION

In the IF, the instrumentation and controls are composed of four basic blocks or systems:

- TSV Reactivity Protection System (TRPS)
- Neutron Flux Detection System (NFDS)
- Engineered Safety Features Actuation System (ESFAS)
- TSV Process Control System (TPCS)

It is with these systems that the IF can be automatically monitored and shutdown and the operators are given an interface for monitoring and control. The TRPS and the TPCS are DCSs that function independently and are electrically isolated from one another. The NFDS is an independent and electrically isolated system whose function is to monitor the neutron flux from the TSV and relay those measurements to the TRPS and TPCS. The TRPS performs the protective actions for an IU trip (e.g., de-energize the neutron driver, open the TSV dump valves, and close the TSV fill valves, and close the TSV dump tank outlet valves). The ESFAS is utilized to isolate the IU and TOGS shielded cells. The ESFAS is constructed in two independent, redundant, electrically isolated trains. Each train of the ESFAS has the capability to isolate one or all of the IU cells. The ESFAS trip signal is an input into TRPS. There is one TRPS, one TPCS, one NFDS per IU cell (eight NFDSs), and one ESFAS. Figure 7a2.2-1 illustrates in block form the inter-relationship of the key systems.

The TPCS is discussed in greater detail in Section 7a2.3.

The TRPS and NFDS are discussed in greater detail in Section 7a2.4.

ESFAS is discussed in greater detail in Section 7a2.5.

The hardware and software descriptions including software flow diagrams for digital computer systems, description of how the operational and support requirements will be met, and a description of the methodology and acceptance criteria to establish and calibrate trip or actuation setpoints or interlock functions will be provided in the FSAR.

### 7a2.2.4 SYSTEM PERFORMANCE ANALYSIS

The IF instrumentation and controls have the capability to trip the IU and isolate the IU cell and TOGS shielded cell. The TRPS functions as the safety-related protection system for the PSB and performs the protective actions. The ESFAS performs the protective actions for isolation of the IU cell and TOGS shielded cell. This analysis discusses the safety-related TRPS design criteria and design basis.

Potential variables, conditions, or other items that will be probable subjects of technical specifications associated with the IF instrumentation and control systems are provided in Chapter 14.

#### 7a2.2.4.1 IU Trip Design Basis

This section discusses design basis information for the IU trip functions and the ESFAS actuation, including those required by Section 4 of IEEE-603-2009. The IU trip is a protective function and is part of the overall protection and safety monitoring systems for the IF. The specific equipment design basis for the instrumentation and equipment used for the IU trip functions are discussed in Section 7a2.4. The ESFAS is a mitigative system and is part of the overall protection and safety monitoring systems for the IF. The specific equipment design basis for the instrumentation and equipment used for the ESFAS actuation are discussed in Section 7a2.5.

The following discussion relates to the design bases utilized for monitoring specific signal values for IU trips and ESFAS actuation, the requirements of performance, the requirements for specific modes of operation for the TSV and the documents generating the basis.

##### 7a2.2.4.1.1 Safety Functions and Corresponding Protective/Mitigative Actions for Design Basis Events

Citation - Section 4a and 4b of IEEE-603-2009

A preliminary accident analysis has been completed and the results are detailed in Section 13a2. Conditions that result in an IU trip are discussed in Subsections 13a2.1.2, 13a2.1.3, 13a2.1.4, 13a2.1.8, and 13a2.1.9. These subsections correlate the accident condition to the IU trip.

7a2.2.4.1.2 Variables Monitored to Control Protective/Mitigative Action

Citation - Section 4d of IEEE-603-2009

The following variables are monitored for an IU trip or ESFAS actuation:

- TSV cover gas hydrogen concentration
- Neutron flux, source range and high range
- Primary closed loop cooling system (PCLS) temperature
- Status of manual emergency shut down (ESD) pushbuttons
- PCLS flow
- High radiation in RCA ventilation system

TRPS is discussed in Section 7a2.4.

ESFAS is discussed in Section 7a2.5.

7a2.2.4.1.3 Variable Monitored Having Spatial Dependence

Citation - Section 4f of IEEE-603-2009

The neutron flux is measured by three different flux detectors located nominally 120 degrees apart, surrounding the TSV, being located in the light water cooling pool. Variations in flux between these three detectors will be able to be observed by the operators.

7a2.2.4.1.4 Range of Transient and Steady-State Conditions During Normal, Abnormal, and Accident Conditions

Citation - Section 4g of IEEE-603-2009

Ranges of transient and steady-state conditions will be provided in the FSAR.

Discussions of trips are provided in Subsection 7a2.4.1.1

7a2.2.4.1.5 Functional Degradation of Safety System Performance

Citation - Section 4h of IEEE-603-2009

This section of the IEEE-603 describes what constitutes system malfunctions for safety-related and nonsafety-related devices. The safety-related systems are designed to consider those conditions having the potential for functional degradation in performance as described in Chapter 13. Manual ESD pushbuttons are also provided to allow analog IU cell trip independent of the DCSs.

7a2.2.4.2 Analysis

7a2.2.4.2.1 TSV Trip Function Conformance to Applicable Criteria

The TRPS performs an IU trip as a protective function as part of the protection system. The criteria for equipment selection are discussed in Section 7a2.4. The following discussions relate to conformance to criteria for the IU trip function.

7a2.2.4.2.1.1 General Functional Requirement Conformance

Citation - Section 5 of IEEE-603-2009, GDC-13, GDC-20

The TRPS initiates safe shutdown when the system detects an abnormal event. IU trips are discussed in Subsection 7a2.4.1.1. The monitored values and subsequent trips were determined in the accident analysis and provide a means to mitigate or reduce the consequences of the design basis event (DBE) to acceptable levels.

7a2.2.4.2.1.2 Single Failure Criterion Conformance

Citation - Section 5.1 of IEEE-603-2009, IEEE-379-2000

A postulated single failure in the TRPS or the ESFAS does not prevent an IU trip. This is accomplished by utilizing redundant or triplicate measurement devices, having multiple paths from measurement sources, utilizing diversity in measurement, and having system designs based on single failure criteria. The equipment requirements are discussed in Sections 7a2.4 and 7a2.5.

7a2.2.4.2.1.3 Independence for Control and IU Trip Conformance

Citation - Section 5.6 of IEEE-603-2009, GDC-24

The TRPS is a separate system, independent from the TPCS. The TRPS and TPCS are located in separate fire areas. See Section 9a2.3.

Where measured values come from shared components, such as the NFDS, there are appropriate electrical isolation modules in place. Electrical isolation is utilized for connections to the TRPS that could compromise the ability to perform its safety function.

IEEE 7-4.3.2-2010 provides the design criteria for safety systems including data processing function for interconnected computers.

The ESFAS is designed as two separate independent trains that are physically separated. The safety-related ESFs are separated per IEEE-384. The actuation of any one ESFAS train results in isolation of the IU and TOGS shielded cells and a subsequent IU trip and safe shutdown. ESFAS is independent of the TPCS and TRPS.

7a2.2.4.2.1.4 Derivation of System Inputs Conformance

Citation - Section 6.4 of IEEE-603-2009

To the extent possible, system inputs are derived from signals that are directly measured from the desired variables.

7a2.2.4.2.1.5 Requirements on Bypassing Trip Functions Conformance

Citation - Section 5.8, 5.9, 6.6, 6.7 of IEEE-603-2009

Trip over-ride/bypass are discussed in Subsection 7a2.4.1.1.

Channel bypass is allowed based on the nature of the signal. The triplicated voted inputs, two out of three voting (2oo3) strategy, allows a channel bypass. During a channel bypass the signal group becomes one out of two (1oo2) voting strategy. No additional channel bypass is allowed.

7a2.2.4.2.1.6 Requirements on Setpoint Determination and Multiple Setpoint Conformance

Citation - Section 6.8 of IEEE-603-2009

Subsection 7a2.2.1 and 7a2.2.2 discusses the methodology to be utilized for setpoint derivation which is ISA RP-67.04.02.

The requirements for multiple setpoints and trip criteria will be discussed in detail in the FSAR.

7a2.2.4.2.1.7 Requirements for Completion of Trip Conformance

Citation - Section 5.2 of IEEE-603-2009

The discussion of the TRPS and ESFAS and the interaction of a protective action going to completion are provided in the design. The TRPS monitors for a complete trip of the TRPS and the ESFAS and safe shutdown of the IU, and then informs the operator of the status. This becomes an alarm/event (A/E) annunciation event displayed to the operator.

Section 7a2.4 discusses the activation of the TRPS protective action.

Section 7a2.5 discusses the initiation of the ESFAS.

Section 7a2.4 discusses the operator requirement to manually reset after a trip for the TRPS.

Section 7a2.5 discusses the operator requirement to manually reset after a trip for the ESFAS.

7a2.2.4.2.1.8 Requirements for Manual Control of Trip Conformance

Citation - Section 6.2 of IEEE-603-2009

The TRPS has the ability to perform a manual activation and trip the IU. Section 7a2.4 discusses the activation of the TRPS. Manual ESD pushbuttons are also included to initiate an IU trip independent of the DCSs.

The ESFAS has the ability to perform a manual activation and isolation of the IU and TOGS shielded cells. Section 7a2.5 discusses the activation of the ESFAS.

Section 7a2.4 discusses the operator requirement to manually reset after a trip for the TRPS.

Section 7a2.5 discusses the operator requirement to manually reset after an actuation of the ESFAS.

7a2.2.5 CONCLUSION

The instrument and control system for the IF meets the stated design criteria and design basis requirements outlined in NUREG-1537. A matrix of the SHINE instrumentation and control subsystems along with a cross reference to specific design criteria is presented in Table 7a2.2-2.

**Table 7a2.2-1 Design Criteria for TSV Instrumentation and Control Systems (Sheet 1 of 12)**

| Design Criteria as Cited with Summary Intent | Design Bases As Applied to SHINE |
|---|---|
| **IEEE Std 379-2000 (R2008)**<br><br>**IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems**<br><br>**Abstract:** Application of the single-failure criterion to the electrical power, instrumentation, and control portions of nuclear power generating safety systems is covered in this standard.<br><br>**Keywords:** actuator, cascaded failure, common-cause failure, design basis event, detectable failure, effects analysis, safety system, single-failure criterion, system actuation, system logic | As Applied<br><br>This standard is applied to the design of the target solution vessel reactivity protection system (TRPS), engineered safety features (ESFs), ESF actuation system (ESFAS), and other systems, structures, or components (SSCs) that are identified as safety-related for the IF.<br><br>Means of Compliance<br><br>The TRPS uses a platform that has previously been approved for use by the NRC in safety systems. It is based on triple modular redundancy (TMR) of power supplies, processors, and input/output channels. Controls that are deemed safety-related identified in Section 13a are evaluated against the single-failure compliance for which the TRPS performs a monitor or control function. TRPS can also be tripped manually from the control room by an operator.<br><br>The NFDS is similar to systems that have been deployed in research reactors throughout the United States. The present design of the NFDS utilizes three detectors, each on a separate channel. These channels are voted 2oo3 internally in the NFDS. The NFDS system then provides two sets of triplicate relays for use and input to the TRPS and TPCS that an out of operating limits excursion has occurred.<br><br>The ESFAS system is designed as a redundant system designated as trains A and B. The ESFAS design incorporates safety relays whose function is to interrupt power to the active ESFs that have been identified in the Section 6a or 13a. A trip of either train A or B performs the ESFAS function, and brings the IU cell in question to a safe isolation state. The ESFAS can be tripped automatically from the monitored redundant sensing devices that are part of the ESFAS. It can also be tripped manually from the control room by an operator. |

**Table 7a2.2-1 Design Criteria for TSV Instrumentation and Control Systems (Sheet 2 of 12)**

| Design Criteria as Cited with Summary Intent | Design Bases As Applied to SHINE |
|---|---|
| **IEEE Std 577-2004**<br><br>**IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Facilities**<br><br>**Abstract:** This standard sets forth minimum acceptable requisites for the performance of reliability analyses for safety related systems of nuclear facilities when used to address the reliability requirements identified in regulations and other standards. The requirement that a reliability analysis be performed does not originate with this standard. However, when reliability analysis is used to demonstrate compliance with reliability requirements, this standard describes an acceptable response to the requirements.<br><br>**Keywords:** nuclear facilities, reliability analysis, safety systems | As Applied<br><br>This standard is applied to the design of the TRPS, ESFAS, and other instrumentation SSCs that are identified as safety-related for the SHINE facility.<br><br>Means of Compliance<br><br>For safety functions identified in the Section 6a or 13a, a reliability analysis of the proposed design solution is performed. This can be qualitative or quantitative in nature as described in the standard. |
| **IEEE Std 603-2009**<br><br>**IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations**<br><br>**Abstract:** Minimum functional and design criteria for the power, instrumentation, and control portions of nuclear power generating station safety systems are established. The criteria are to be applied to those systems required to protect the public health and safety by functioning to mitigate the consequences of design basis events. The intent is to promote appropriate practices for design and evaluation of safety system performance and reliability. Although the standard is limited to safety systems, many of the principles may have applicability to equipment provided for safe shutdown, post accident monitoring display instrumentation, preventive interlock features, or any other systems, structures, or equipment related to safety.<br><br>**Keywords:** actuated equipment, associated circuits, Class 1E, design, failure, maintenance bypass, operating bypass, safety function, sense and command features, sensor | As Applied<br><br>This standard is applied to the design of the TRPS, ESFAS, and other SSCs that are identified as safety-related for the SHINE facility. It describes the minimum functional and design criteria for safety systems. It does not describe what systems are to be determined as safety systems.<br><br>Means of Compliance<br><br>For safety functions identified in the Section 6a or 13a, the design conforms to the practices detailed in the standard.<br><br>Exception<br><br>The SHINE facility is not a nuclear power reactor and does not have all of the systems detailed in this standard. The intent of this standard is followed. |

**Table 7a2.2-1 Design Criteria for TSV Instrumentation and Control Systems (Sheet 3 of 12)**

| Design Criteria as Cited with Summary Intent | Design Bases As Applied to SHINE |
|---|---|
| **IEEE Std 384-2008**<br><br>**IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits**<br><br>**Abstract:** The independence requirements of the circuits and equipment comprising or associated with Class 1E systems are described. Criteria for the independence that can be achieved by physical separation and electrical isolation of circuits and equipment that are redundant are set forth. The determination of what is to be considered redundant is not addressed.<br><br>**Keywords:** associated circuit, barrier, Class 1E, independence, isolation, isolation device, raceway, separation | As Applied<br><br>This standard is applied to the design of the TRPS, ESFAS, and other instrumentation SSCs that are identified as safety-related for the SHINE facility. It describes the minimum criteria for separation and independence of systems in a physical way. It does not describe what systems are to be separate and independent, only a means to do so.<br><br>Means of Compliance<br><br>For safety functions identified in the Section 6a or 13a, the design conforms to the practices detailed in the standard.<br><br>Exception<br><br>The SHINE facility is not a nuclear power reactor and does not have all of the systems detailed in this standard. The intent of this standard is followed. |
| **IEEE Std 323-2003**<br><br>**IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations**<br><br>**Abstract:** The basic requirements for qualifying Class 1E equipment and interfaces that are to be used in nuclear power generating stations are described in this standard. The principles, methods, and procedures described are intended to be used for qualifying equipment, maintaining and extending qualification, and updating qualification, as required, if the equipment is modified. The qualification requirements in this standard, when met, demonstrate and document the ability of equipment to perform safety function(s) under applicable service conditions including design basis events, reducing the risk of common-cause equipment failure.<br><br>**Keywords:** age conditioning, aging, condition monitoring, design basis events, equipment qualification, harsh environment, margin, mild environment, qualification methods, qualified life, radiation, SR function, significant aging mechanism, test plan, test sequence, type testing | As Applied<br><br>This standard defines the methods for equipment qualification when it is desired to qualify equipment for the applications and the environments to which it may be exposed. This standard is generally utilized for qualification of Class 1E equipment located in harsh environments, and for certain post-accident monitoring equipment, but it may also be utilized for the qualification of equipment in mild environments.<br><br>Means of Compliance<br><br>For safety functions identified in the Section 6a or 13a, the design conforms to the practices detailed in the standard for those systems determined to be Class 1E and located in harsh environment. This describes those SSCs that reside within the IU cell. Not all of the safety components reside in the IU cell. As an example, isolation valve actuators that reside in the IU cell with electrical components are scrutinized with this standard, but the controlling system ESFAS that resides outside the IU cell does not require the same level of exposure per the application of this standard. The standard is applied in a graded approach based on the location of the equipment. |

**Table 7a2.2-1 Design Criteria for TSV Instrumentation and Control Systems (Sheet 4 of 12)**

| Design Criteria as Cited with Summary Intent | Design Bases As Applied to SHINE |
|---|---|
| **IEEE Std 344-2004**<br><br>**IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations**<br><br>**Abstract:** Recommended practices are provided for establishing procedures that will yield data to demonstrate that the Class 1E equipment can meet its performance requirements during and/or following one safe shutdown earthquake event preceded by a number of operating basis earthquake events. This recommended practice may be used to establish tests, analyses, or experienced based evaluations that will yield data to demonstrate Class 1E equipment performance claims or to evaluate and verify performance of devices and assemblies as part of an overall qualification effort. Common methods currently in use for seismic qualification by test are presented. Two approaches to seismic analysis are described, one based on dynamic analysis and the other on static coefficient analysis. Two approaches to experienced-based seismic evaluation are described, one based on earthquake experience and the other based on test experience.<br><br>**Keywords:** Class 1E, earthquake, earthquake experience, equipment qualification, inclusion rules, nuclear, operating basis earthquake, prohibited features, qualification methods, required response spectrum, response spectra, safe shutdown earthquake, safety function, seismic, seismic analysis, test response spectrum, test experience | As Applied and Means of Compliance<br><br>This standard is evaluated against the design of the TRPS, ESFAS, and other instrumentation SSCs that are identified as a Class 1E system for the SHINE facility. It describes seismic design requirement for equipment used in Class 1E systems. It does not describe what systems are to be determined as Class 1E systems. |

**Table 7a2.2-1 Design Criteria for TSV Instrumentation and Control Systems (Sheet 5 of 12)**

| Design Criteria as Cited with Summary Intent | Design Bases As Applied to SHINE |
|---|---|
| **IEEE Std 338-2012**<br><br>**IEEE Standard for Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems**<br><br>**Abstract:** The standard provides criteria for the performance of periodic surveillance testing of nuclear power generating station safety systems. The scope of periodic surveillance testing consists of functional tests and checks, calibration verification, and time response measurements, as required, to verify that the safety system performs its defined safety function. Post-maintenance and post-modification testing are not covered by this document. This standard amplifies the periodic surveillance testing requirements of other nuclear safety-related IEEE standards.<br><br>**Keywords:** functional tests, IEEE 338, periodic testing, risk-informed testing, surveillance testing | As Applied<br><br>This standard is applied to the design of the TRPS, ESFAS, and other instrumentation SSCs that are identified as safety-related for the SHINE facility. It describes the methods and criteria for establishing a periodic surveillance program. It does not describe what systems are to be separate and independent, only a means to do so.<br><br>Means of Compliance<br><br>For safety functions identified in the Section 6a or 13a, the design conforms to the practices detailed in the standard. |
| **IEEE Std 497-2010**<br><br>**IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations**<br><br>**Abstract:** Criteria are established in this standard for variable selection, performance, design, and qualification of accident monitoring instrumentation, and include requirements for display alternatives for accident monitoring instrumentation, documentation of design bases, and use of portable instrumentation.<br><br>**Keywords:** accident monitoring, display criteria, selection criteria, type variables | As Applied<br><br>The purpose of this standard is to establish selection, design, performance, qualification and display criteria for accident monitoring instrumentation. It provides guidance on the use of portable instrumentation and examples of accident monitoring display configurations.<br><br>Means of Compliance<br><br>For those monitoring functions determined to be required for the health and safety of public or workers during normal operation and for post-design base accident, the design conforms to the practices detailed in the standard. |

**Table 7a2.2-1 Design Criteria for TSV Instrumentation and Control Systems (Sheet 6 of 12)**

| Design Criteria as Cited with Summary Intent | Design Bases As Applied to SHINE |
|---|---|
| **IEEE Std 7-4.3.2-2010**<br><br>**IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations**<br><br>**Abstract:** Additional computer specific requirements to supplement the criteria and requirements of IEEE Std 603™-2009 are specified. Within the context of this standard, the term computer is a system that includes computer hardware, software, firmware, and interfaces. The criteria contained herein, in conjunction with criteria in IEEE Std 603-2009, establish minimum functional and design requirements for computers used as components of a safety system.<br><br>**Keywords:** commercial grade item, diversity, safety systems, software, software tools, software verification and validation | As Applied<br><br>The purpose of this standard, in conjunction with criteria in IEEE Std 603-2009, establishes minimum functional and design requirements for computers used as components of a safety-related system. The TRPS is designed as a DCS and this standard is applied to the development, more specifically related to software development. This standard also discusses commercial-grade dedication (CGD) and the method for successfully implementing the CGD approach.<br><br>Means of Compliance<br><br>The TRPS software is developed utilizing this standard. |

**Table 7a2.2-1 Design Criteria for TSV Instrumentation and Control Systems (Sheet 7 of 12)**

| Design Criteria as Cited with Summary Intent | Design Bases As Applied to SHINE |
|---|---|
| **IEEE Std 828-2012**<br><br>**IEEE Standard for Configuration Management in Systems and Software Engineering**<br><br>**Abstract:** This standard establishes the minimum requirements for processes for Configuration Management (CM) in systems and software engineering. The application of this standard applies to any form, class, or type of software or system. This revision of the standard expands the previous version to explain CM, including identifying and acquiring configuration items, controlling changes, reporting the status of configuration items, as well as software builds and release engineering. Its predecessor defined only the contents of a software configuration management plan. This standard addresses what CM activities are to be done, when they are to happen in the life cycle, and what planning and resources are required. It also describes the content areas for a CM Plan. The standard supports ISO/IEC/IEEE 12207:2008 and ISO/IEC/IEEE 15288:2008 and adheres to the terminology in ISO/IEC/IEEE Std 24765 and the information item requirements of IEEE Std 15939.<br><br>**Keywords:** change control, configuration accounting, configuration audit, configuration item, IEEE 828, release engineering, software builds, software configuration management, system configuration management | As Applied<br><br>This standard describes configuration management processes to be established, how they are to be accomplished, who is responsible for doing specific activities, when they are to happen, and what specific resources are required. The TRPS is designed as a DCS, the TRPS has safety-related function, and this standard applies to the development specifically related to software development.<br><br>Means of Compliance<br><br>The TRPS software is developed utilizing this standard. |

**Table 7a2.2-1 Design Criteria for TSV Instrumentation and Control Systems (Sheet 8 of 12)**

| Design Criteria as Cited with Summary Intent | Design Bases As Applied to SHINE |
|---|---|
| **IEEE Std 829-2008**<br>**IEEE Standard for Software and System Test Documentation**<br>**Abstract:** Test processes determine whether the development products of a given activity conform to the requirements of that activity and whether the system and/or software satisfy its intended use and user needs. Testing process tasks are specified for different integrity levels. These process tasks determine the appropriate breadth and depth of test documentation. The documentation elements for each type of test documentation can then be selected. The scope of testing encompasses software-based systems, computer software, hardware, and their interfaces. This standard applies to software-based systems being developed, maintained, or reused (legacy, commercial off-the-shelf, Non-Developmental Items). The term "software" also includes firmware, microcode, and documentation. Test processes can include inspection, analysis, demonstration, verification, and validation of software and software-based system products.<br>**Keywords:** integrity level, life cycle, test documentation, testing | As Applied<br>This standard applies to software-based systems. It applies to systems and software being developed, acquired, operated, maintained, and/or reused (e.g. legacy, modified, commercial off-the-shelf [COTS], government off-the-shelf [GOTS], or non-developmental items [NDI]). System and software test processes determine whether the outcomes of a given activity conform to the requirements of that activity and whether the development product satisfies its intended use and user needs. The determination may include analysis, demonstration, inspection, and testing of software products. The TRPS is designed as a DCS, the TRPS has safety-related functions, and this standard applies to the development specifically related to software development.<br>Means of Compliance<br>The TRPS software is developed utilizing this standard. |
| **IEEE Std 1012-2004**<br>**IEEE Standard Criteria for Software Verification and Validation**<br>**Abstract:** Software verification and validation (V&V) processes determine whether the development products of a given activity conform to the requirements of that activity and whether the software satisfies its intended use and user needs. Software V&V life cycle process requirements are specified for different software integrity levels. The scope of V&V processes encompasses software-based systems, computer software, hardware, and interfaces. This standard applies to software being developed, maintained, or reused [legacy, COTS, non-developmental items]. The term software also includes firmware, microcode, and documentation. Software V&V processes include analysis, evaluation, review, inspection, assessment, and testing of software products.<br>**Keywords:** IV&V, software integrity level, software life cycle, V&V, validation, verification | As Applied<br>The purpose of software V&V is to help the development organization build quality into the software during the software life cycle. This assessment demonstrates whether the software requirements and system requirements (i.e., those allocated to software) are correct, complete, accurate, consistent, and testable. Software V&V is performed in parallel with software development, not at the conclusion of the development effort. This standard describes a means to verify and validate the software development for the TRPS and meets the same requirements as the physical system responsible for process and safety-related functions in the SHINE facility.<br>Means of Compliance<br>The TRPS is developed utilizing this standard. |

**Table 7a2.2-1 Design Criteria for TSV Instrumentation and Control Systems (Sheet 9 of 12)**

| Design Criteria as Cited with Summary Intent | Design Bases As Applied to SHINE |
|---|---|
| **IEEE Std 1028-2008**<br><br>**IEEE Standard for Software Reviews and Audits**<br><br>**Abstract:** Five types of software reviews and audits, together with procedures required for the execution of each type, are defined in this standard. This standard is concerned only with the reviews and audits; procedures for determining the necessity of a review or audit are not defined, and the disposition of the results of the review or audit is not specified. Types included are management reviews, technical reviews, inspections, walk-throughs, and audits.<br><br>**Keywords:** audit, inspection, review, walk-through | As Applied<br><br>This standard provides minimum acceptable requirements for systematic software reviews. This standard describes organizational means for doing a review and documenting the findings. The TRPS is designed as a DCS, the TRPS has safety-related functions, and this standard applies to the development of the software for that system.<br><br>Means of Compliance<br><br>The TRPS is developed utilizing this standard. |
| **ANS-10.4-2008**<br><br>**Verification and Validation of Non-Safety-Related Scientific and Engineering Computer Programs for the Nuclear Industry**<br><br>**Abstract:** This standard provides guidelines for the V&V of non-safety related scientific and engineering computer programs developed for use by the nuclear industry. The scope is restricted to research and other non-safety-related, noncritical applications.<br><br>**Keywords:** software integrity level, software life cycle, V&V, validation, verification | As Applied<br><br>The purpose of software V&V is to help the development organization build quality into the software during the software life cycle. This standard describes a means to verify and validate the software development for the nonsafety-related systems. It is utilized for any software development in the SHINE facility that is not safety significant, i.e. nonsafety-related.<br><br>Means of Compliance<br><br>Nonsafety-related software is developed utilizing this standard. |
| **ISA 67.04.01-2006**<br><br>**Setpoints for Nuclear Safety-Related Instrumentation**<br><br>**Abstract:** This standard defines the requirements for assessing, establishing, and maintaining nuclear SR and other important instrument setpoints associated with nuclear power plants or nuclear reactor facilities.<br><br>**Keywords:** Setpoint, drift, analog channel, reliability analysis | As Applied<br><br>This standard is applied to the design of the TRPS and other instrumentation SSCs that are identified as safety-related for the SHINE facility. It describes the methods and criteria for establishing setpoints utilized in safety-related systems and maintaining the documentation thereafter.<br><br>Means of Compliance<br><br>For any safety function identified in the Section 6a or 13a that is designed with inherent setpoints, the design conforms to the practices detailed in the standard. |

**Table 7a2.2-1 Design Criteria for TSV Instrumentation and Control Systems (Sheet 10 of 12)**

| Design Criteria as Cited with Summary Intent | Design Bases As Applied to SHINE |
|---|---|
| **NUREG-0700, Rev. 2**<br><br>**Human-System Interface Design Review Guidelines**<br><br>**Abstract:** NRC staff reviews the human factors engineering (HFE) aspects of nuclear power plants in accordance with the Standard Review Plan (NUREG-0800). Detailed design review procedures are provided in the HFE Program Review Model (NUREG-0711). As part of the review process, the interfaces between plant personnel and plant's systems and components are evaluated for conformance with HFE guidelines. This document, Human-System Interface Design Review Guidelines (NUREG-0700, Revision 2), provides the guidelines necessary to perform this evaluation.<br><br>**Keywords:** Display, HMI, Human Interface System (HIS), Human-System Interface | As Applied<br><br>This comprehensive design review guide concentrates on displayed information utilized in human-interface systems. This is a sub-set of HFE, dedicated to providing informative and effective designs that assist an operator in the performance of their duties.<br><br>Means of Compliance<br><br>Both the TRPS and TPCS have their information provided to operators in a display format. This document is utilized and reviewed for the development of displays that an operator uses in connection with the TRPS and TPCS. |
| **NUREG/CR-6463**<br><br>**Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems**<br><br>**Abstract:** This report provides guidance to the NRC on auditing of programs for safety systems written in the following six high level languages: Ada, C and C++, Programmable Logic Controller (PLC) Ladder Logic, Sequential Function Charts, Pascal, and PL/M. It could also be used by those developing safety significant software as a basis for project-specific programming guidelines.<br><br>**Keywords:** Pascal, C, Ladder Logic, PL/M, Ada, C++, PLC, Programming, Sequential Function Charts | As Applied<br><br>The goal of this report is to provide guidance to the NRC for reviewing high-integrity software in nuclear power plants. Thus the focus of the report is on implementation (i.e., programming). It is a discussion of what constitutes good practices and cites examples of previously installed systems. TRPS and TPCS are DCSs and have associated programming developed for the SHINE facility. For those programming languages identified in this report, the guideline serves as suitable means to review the programming code.<br><br>Means of Compliance<br><br>Both the TRPS and TPCS have software programs developed. This document provides review guidance of any programming code for which the report was developed. |

**Table 7a2.2-1 Design Criteria for TSV Instrumentation and Control Systems (Sheet 11 of 12)**

| Design Criteria as Cited with Summary Intent | Design Bases As Applied to SHINE |
|---|---|
| **NUREG/CR-6090**<br><br>**The Programmable Logic Controller and Its Application in Nuclear Reactor Systems**<br><br>**Abstract:** The purpose of this document is to outline recommendations for guidance for the review of application of PLCs to the control; monitoring and protection of nuclear reactors.<br><br>**Keywords:** PLC, Programming, Protection Systems | As Applied<br><br>The goal of this report is to provide guidance to the NRC for implementing PLCs in the nuclear reactor power industry. It provides a complete background to a selection process for hardware, failure analysis, as well as discussion of product life cycle within the power plant. It forms a discussion of what constitutes good practices and cites examples of previously installed systems. TRPS and TPCS are DCSs and PLC-type systems and are developed for the SHINE facility.<br><br>Means of Compliance<br><br>Both the TRPS and TPCS utilize PLC type DCSs. This document provides guidance for selection design and implementation of this type of control. It is utilized for implementing the PLC design. |
| **EPRI TR-106439, 1996**<br><br>**Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications**<br><br>**Abstract:** This guideline describes a consistent, comprehensive approach for the evaluation and acceptance of commercial digital equipment for nuclear safety systems.<br><br>**Keywords:** COTS, Programming, Software, Commercial Grade Dedication | As Applied<br><br>The approach emphasizes identification of appropriate critical characteristics with subsequent verification through testing, analysis, vendor assessments and careful review of operating experience. This guide is not intended to be a new standard; it references existing industry standards and guidelines as appropriate. The guide is intended primarily for digital upgrades to safety-related systems, but it is also useful in nonsafety-related applications that require high reliability. The guidance is intended to be compatible with utility-specific change processes, including graded approaches for quality assurance.<br><br>Means of Compliance<br><br>The systems or components that require CGD utilize this guideline. |
| **Regulatory Guide 1.152, Rev.3, 2011**<br><br>**Criteria for use of Computers in Safety Systems of Nuclear Power Plants**<br><br>**Abstract:** This regulatory guide describes a method that the NRC staff deems acceptable for complying with the Commission's regulations for promoting high functional reliability, design quality, and a secure development and operational environment (SDOE) for the use of digital computers in the safety systems of nuclear power plants.<br><br>**Keywords:** Secure Development and Operational Environment, SDOE, computers | As Applied<br><br>Instrumentation and control system designs that use computers in safety systems make extensive use of advanced technology (i.e., equipment and design practices). These designs are expected to be significantly and functionally different from current designs and may include the use of microprocessors, digital systems and displays, fiber optics, multiplexing, and different isolation techniques to achieve sufficient independence and redundancy.<br><br>Means of Compliance<br><br>The TRPS and TRPS human machine interface (HMI) are developed utilizing this document. |

**Table 7a2.2-1 Design Criteria for TSV Instrumentation and Control Systems (Sheet 12 of 12)**

| Design Criteria as Cited with Summary Intent | Design Bases As Applied to SHINE |
|---|---|
| **Regulatory Guide 1.53, Rev.2, 2003**<br><br>**Application of the Single-Failure Criterion to Safety Systems**<br><br>**Abstract:** Provides methods acceptable to the NRC staff for satisfying the NRC's regulations with respect to the application of the single-failure criterion to the electrical power, instrumentation, and control portions of nuclear power plant safety systems.<br><br>**Keywords:** IEEE Std 379, Single-Failure Criterion | As Applied<br><br>The approach provides guidance for applying single-failure criterion to safety-related instrumentation and control systems. The TRPS, end-devices utilized by the TRPS, the ESFAS, and NFDS are identified as safety-related. These systems and components are evaluated via this regulatory guide.<br><br>Means of Compliance<br><br>The TRPS, ESFAS, NFDS, and safety-related end-devices are evaluated with this document. |
| **Regulatory Guide 1.97, Rev.4, 2006**<br><br>**Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants**<br><br>**Abstract:** This regulatory guide to describe a method that the NRC staff considers acceptable for use in complying with the agency's regulations with respect to satisfying criteria for accident monitoring instrumentation in nuclear power plants.<br><br>**Keywords:** IEEE Std 497, accident monitoring | As Applied<br><br>The approach provides guidance for accident monitoring in the SHINE facility. These systems and components are evaluated via this regulatory guide.<br><br>Means of Compliance<br><br>The TRPS, ESFAS, CAMS, and RAMS are designed with the use of document. |
| **Regulatory Guide 5.71, 2010**<br><br>**Cyber Security Programs for Nuclear Facilities**<br><br>**Abstract:** This regulatory guide provides an approach that the NRC staff deems acceptable for complying with the Commission's regulations regarding the protection of digital computers, communications systems, and networks from a cyber attack as defined by 10 CFR 73.1.<br><br>**Keywords:** Cyber Security, 10 CFR 73.54(a)(2), design basis threat | As Applied<br><br>The approach provides guidance for protection of digital equipment from cyber attack in the SHINE facility. These systems and components are evaluated via this regulatory guide.<br><br>Means of Compliance<br><br>Digital computer and communications systems networks associated with safety-related functions are designed with the use of document. |

## Table 7a2.2-2 IF Verification Matrix Design Criteria, Bases, Description (Sheet 1 of 10)

| Verification Matrix | Design Criterion | Design Basis Applicability | Detailed Section Reference | Functional Means |
|---|---|---|---|---|
| 1 | IEEE-379<br>Single Failure Criterion | 1) TRPS<br>2) NFDS<br>3) ESFAS<br>4) TRPS display<br>5) TRPS end devices<br>6) TRPS manual trip<br>7) ESFAS manual shutdown | 1) 7a2.4<br>2) 7a2.4<br>3) 7a2.5<br>4) 7a2.6<br>5) 7a2.4<br>6) 7a2.4<br>7) 7a2.5 | 1) TMR pre-approved platform.<br>2) Triplicate channels voted 2oo3.<br>3) Redundant independent shutdown systems.<br>4) Redundant operator interface workstations.<br>5) Redundant and triplicate sense.<br>6) Alternative manual means for TRPS trip.<br>7) Alternative manual means for ESFAS initiation. |
| 2 | IEEE-577<br>Reliability Analysis Criterion | 1) TRPS<br>2) NFDS<br>3) ESFAS<br>4) TRPS display<br>5) TRPS end devices<br>6) ESFAS end devices<br>7) ESFAS manual shutdown | 1) 7a2.4<br>2) 7a2.4<br>3) 7a2.5<br>4) 7a2.6<br>5) 7a2.4<br>6) 7a2.5<br>7) 7a2.5 | 1) TMR pre-approved platform.<br>2) Triplicate channels voted 2oo3.<br>3) Redundant independent ESF shutdown systems.<br>4) Redundant operator interface workstations.<br>5) Redundant and triplicate sense.<br>6) Redundant sense.<br>7) Diverse means for isolation, non-digital control system. |
| 3 | IEEE-603<br>Standard Criteria Safety Systems | 1) TRPS<br>2) NFDS<br>3) ESFAS<br>4) TRPS display<br>5) TRPS end devices<br>6) TRPS manual trip<br>7) ESFAS end devices<br>8) ESFAS manual shutdown | 1) 7a2.4<br>2) 7a2.4<br>3) 7a2.5<br>4) 7a2.6<br>5) 7a2.4<br>6) 7a2.4<br>7) 7a2.5<br>8) 7a2.5 | Subsection 7a.2.2.4 for detailed discussion. |
| 4 | IEEE-384<br>Independence of Class 1E Equipment & Circuits | 1) TRPS<br>2) NFDS<br>3) ESFAS<br>4) TRPS display<br>5) TRPS end devices<br>6) TRPS manual trip<br>7) ESFAS end devices<br>8) ESFAS manual shutdown | 1) 7a2.4<br>2) 7a2.4<br>3) 7a2.5<br>4) 7a2.6<br>5) 7a2.4<br>6) 7a2.4<br>7) 7a2.5<br>8) 7a2.6 | For preliminary design, the independence of equipment is sufficient to meet IEEE-603 and IEEE-379. |

**Table 7a2.2-2 IF Verification Matrix Design Criteria, Bases, Description (Sheet 2 of 10)**

| Verification Matrix | Design Criterion | Design Basis Applicability | Detailed Section Reference | Functional Means |
|---|---|---|---|---|
| 5 | IEEE-323<br>Qualifying Class 1E Equipment | 1) TRPS<br>2) NFDS<br>3) ESFAS<br>4) TRPS display<br>5) TRPS end devices<br>6) ESFAS end devices | 1) 7a2.4<br>2) 7a2.4<br>3) 7a2.5<br>4) 7a2.6<br>5) 7a2.4<br>6) 7a2.5 | This standard is for selecting and qualifying equipment. For the preliminary design effort, items such as the TRPS, NFDS, and some selected end devices are already qualified for Class 1E use. |
| 6 | IEEE-344<br>Recommended Practice for Seismic Qualification | 1) TRPS<br>2) NFDS<br>3) ESFAS<br>4) TRPS display<br>5) TRPS end devices<br>6) ESFAS end devices | 1) 7a2.4<br>2) 7a2.4<br>3) 7a2.5<br>4) 7a2.6<br>5) 7a2.4<br>6) 7a2.5 | This standard is for selecting and qualifying equipment. For the preliminary design effort, items such as the TRPS, NFDS, and some selected end devices are already qualified for Class 1E use. |
| 7 | IEEE-338<br>Criteria for the Periodic Surveillance Testing of Safety Systems | 1) TRPS<br>2) NFDS<br>3) ESFAS<br>4) TRPS display<br>5) TRPS end devices<br>6) TRPS manual trip<br>7) ESFAS end devices<br>8) ESFAS manual shutdown | 1) 7a2.4<br>2) 7a2.4<br>3) 7a2.5<br>4) 7a2.6<br>5) 7a2.4<br>6) 7a2.4<br>7) 7a2.5<br>8) 7a2.6 | This standard is for selecting equipment and provides general design criteria that will be considered during final design. |
| 8 | IEEE-497<br>Criteria for Accident Monitoring Instruments | 1) TRPS<br>2) NFDS<br>3) ESFAS<br>4) TRPS display<br>5) TRPS end devices<br>6) ESFAS end devices<br>7) RAMS<br>8) CAMS | 1) 7a2.4<br>2) 7a2.4<br>3) 7a2.5<br>4) 7a2.6<br>5) 7a2.4<br>6) 7a2.5<br>7) 7a2.7<br>8) 7a2.7 | This standard is for selecting accident monitoring equipment (specifically focused on radiation monitoring and annunciation), and provides general design criteria that will be considered during final design. |
| 9 | IEEE-7.4.3.2<br>Criteria for Digital Computers in Safety Systems | 1) TRPS<br>2) TRPS display | 1) 7a2.4<br>2) 7a2.6 | Programming software for the TRPS has been through NRC approval process. Programming must comply with the Software Quality Assurance Plan developed as part of the commitment to the design criteria outlined herein and in this standard.<br><br>The software and hardware utilized for the displays for the TRPS must also follow the guidelines set forth in this standard. The equipment selected to date and the path forward allow for a successful completion following IEEE-7.4.3.2. |

**Table 7a2.2-2 IF Verification Matrix Design Criteria, Bases, Description (Sheet 3 of 10)**

| Verification Matrix | Design Criterion | Design Basis Applicability | Detailed Section Reference | Functional Means |
|---|---|---|---|---|
| 10 | IEEE-828<br>Configuration Management in Systems and Software Engineering | 1) TRPS<br>2) TRPS display | 1) 7a2.4<br>2) 7a2.6 | Part of the overall software quality assurance program (SQAP) commitment of IEEE-7.4.3.2. |
| 11 | IEEE-829<br>Software and System Test Documentation | 1) TRPS<br>2) TRPS display | 1) 7a2.4<br>2) 7a2.6 | Part of the overall SQAP commitment of IEEE-7.4.3.2. |
| 12 | IEEE-1012<br>Criteria for Software Verification and Validation | 1) TRPS<br>2) TRPS display | 1) 7a2.4<br>2) 7a2.6 | Part of the overall SQAP commitment of IEEE-7.4.3.2. |
| 13 | IEEE-1028<br>Software Reviews and Audits | 1) TRPS<br>2) TRPS display | 1) 7a2.4<br>2) 7a2.6 | Part of the overall SQAP commitment of IEEE-7.4.3.2. |
| 14 | ANS-10.4<br>Verification and Validation for non-safety software | 1) TPCS<br>2) TPCS display | 1) 7a2.3<br>2) 7a2.6 | Part of the overall SQAP commitment of IEEE-7.4.3.2. |
| 15 | ISA 67.04.01<br>Setpoints for Nuclear Safety-Related Instruments | 1) TRPS<br>2) NFDS<br>3) ESFAS<br>4) TRPS display<br>5) TRPS end devices<br>6) ESFAS end devices | 1) 7a2.4<br>2) 7a2.4<br>3) 7a2.5<br>4) 7a2.6<br>5) 7a2.4<br>6) 7a2.5 | Part of the overall design commitment. |
| 17 | NUREG-0700, Rev. 2<br>Human-System Interface Design Review Guidelines | 1) TRPS<br>2) TRPS display<br>3) TPCS<br>4) TPCS display<br>5) ESFAS manual shutdown | 1) 7a2.4<br>2) 7a2.6<br>3) 7a2.3<br>4) 7a2.6<br>5) 7a2.5 | This standard is utilized to design and develop the safety-related and nonsafety-related systems as it pertains to control room arrangement, screen developments, and operator Interface. |
| 18 | NUREG/CR-6463<br>Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems | 1) TRPS | 1) 7a2.4 | This guideline is utilized to design, develop, and review the safety-related software. |

**Table 7a2.2-2 IF Verification Matrix Design Criteria, Bases, Description (Sheet 4 of 10)**

| Verification Matrix | Design Criterion | Design Basis Applicability | Detailed Section Reference | Functional Means |
|---|---|---|---|---|
| 19 | NUREG/CR-6090<br>PLC and applications in Nuclear Reactor Systems | 1) TRPS<br>2) TPCS | 1) 7a2.2.2.7<br>2) 7a2.2.3.2 | This guideline is utilized to design, develop, and review the safety-related and nonsafety-related software. |
| 20 | EPRI TR-106439,<br>Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications | 1) TRPS display<br>2) Safety-related instrumentation | 1) 7a2.6<br>2) 7a2.4 | This standard is utilized to design and develop the safety-related systems as it pertains to obtaining software/hardware for the TRPS, operator interface displays, and data acquisition systems. |
| 21 | Reg Guide 1.152<br>Criteria for use of Computers in Safety Systems | 1) TRPS<br>2) TRPS display | 1) 7a2.4<br>2) 7a2.6 | 1) TMR pre-approved platform.<br>2) Operator interface workstations. |
| 22 | Reg Guide 1.53<br>Single Failure Criterion Evaluation for Safety Systems | 1) TRPS<br>2) NFDS<br>3) ESFAS<br>4) TRPS display<br>5) TRPS end devices<br>6) TRPS manual trip<br>7) ESFAS manual shutdown | 1) 7a2.4<br>2) 7a2.4<br>3) 7a2.5<br>4) 7a2.6<br>5) 7a2.4<br>6) 7a2.4<br>7) 7a2.5 | 1) TMR pre-approved platform.<br>2) Triplicate channels voted 2oo3.<br>3) Redundant independent shutdown systems.<br>4) Redundant operator interface workstations.<br>5) Redundant and triplicate sense.<br>6) Alternative manual means for TRPS trip.<br>7) Alternative manual means for ESFAS initiation. |
| 23 | Reg Guide 5.71<br>Cyber Security Programs for Nuclear Facilities | 1) TRPS<br>2) TPCS<br>3) TRPS display<br>4) TPCS display | 1) 7a2.4<br>2) 7a2.3<br>3) 7a2.6<br>4) 7a2.6 | Requires design approach and implementation. |
| 24 | 10CFR 50, Appendix A,<br>GDC 2<br>Natural Phenomena | 1) ESFAS manual operator panel shutdown<br>2) TRPS manual trip | 1) 7a2.5<br>2) 7a2.4 and 7a2.6 | This criterion defines that safety systems are designed to handle natural phenomena. The safety systems are capable of performing their safety functions during and after the external events described in Chapter 13. The instrumentation and controls have the ability for the operator to manually choose to shutdown the irradiation systems should external events dictate. |

**Table 7a2.2-2 IF Verification Matrix Design Criteria, Bases, Description (Sheet 5 of 10)**

| Verification Matrix | Design Criterion | Design Basis Applicability | Detailed Section Reference | Functional Means |
|---|---|---|---|---|
| 25 | 10CFR 50, Appendix A, GDC 4 Environmental and dynamic effects design bases. | 1) TRPS<br>2) NFDS<br>3) ESFAS<br>4) TRPS display<br>5) TRPS end devices<br>6) ESFAS end devices<br>7) TRPS manual trip<br>8) ESFAS manual operator panel shutdown | 1) 7a2.4<br>2) 7a2.4<br>3) 7a2.5<br>4) 7a2.6<br>5) 7a2.4<br>6) 7a2.5<br>7) 7a2.4<br>8) 7a2.5 | This criterion is met by choosing qualified equipment, testing, and surveillance. The criteria to do so are laid out in Subsections 7a2.2.1 and 7a2.2.2 |
| 26 | 10CFR 50, Appendix A, GDC 5 Sharing of structures, systems, and components | 1) TRPS<br>2) ESFAS<br>3) TRPS display<br>4) TRPS end devices<br>5) ESFAS end devices | 1) 7a2.4<br>2) 7a2.5<br>3) 7a2.6<br>4) 7a2.6<br>5) 7a2.4<br>6) 7a2.5 | This criterion is met by having independent redundant systems with defense-in-depth. The basis of design addresses this in Subsections 7a2.2.1 7a2.2.2, and 7a2.2.3.<br><br>The exception is the sharing of the neutron flux measurement. This sensor measurement is shared between the TRPS and TPCS with appropriate isolation. The NFDS is a nuclear industry proven system that is highly reliable and systems are installed in research facilities throughout the world in a similar manner. The sharing of this specific component does not compromise the safety of the facility or impair the ability to shutdown abnormal events should they occur. |
| 27 | 10CFR 50, Appendix A, GDC 10 Reactor design | 1) TRPS<br>2) TRPS display<br>3) TPCS<br>4) TPCS display | 1) 7a2.4<br>2) 7a2.6<br>3) 7a2.3<br>4) 7a2.5 | This criterion is addressed with having the TPCS controlling the process steps of the irradiation process and the TRPS as a separate independent system monitoring for abnormal events. |
| 28 | 10CFR 50, Appendix A, GDC 12 Suppression of reactor power oscillations | 1) TRPS<br>2) NFDS<br>3) TRPS display<br>4) TRPS end devices | 1) 7a2.4<br>2) 7a2.4<br>3) 7a2.6<br>4) 7a2.4 | The instrumentation and control monitors reactivity and can suppress excessive oscillations by terminating the irradiation process and moving the target solution to a geometrically safe vessel. |

**Table 7a2.2-2 IF Verification Matrix Design Criteria, Bases, Description (Sheet 6 of 10)**

| Verification Matrix | Design Criterion | Design Basis Applicability | Detailed Section Reference | Functional Means |
|---|---|---|---|---|
| 29 | 10CFR 50, Appendix A, GDC 13 Instrumentation and control | 1) TRPS<br>2) NFDS<br>3) ESFAS<br>4) TPCS<br>5) TRPS display<br>6) TPCS display<br>7) TRPS end devices<br>8) ESFAS end devices<br>9) TRPS manual trip<br>10) ESFAS manual operator panel shutdown | 1) 7a2.4<br>2) 7a2.4<br>3) 7a2.5<br>4) 7a2.3<br>5) 7a2.6<br>6) 7a2.6<br>7) 7a2.4<br>8) 7a2.5<br>9) 7a2.4<br>10) 7a2.5 | This criterion directly addresses the instrument and controls. The instrumentation and controls provide control, protection, and means to safely mitigate the identified events described in Section 13a. |
| 30 | 10CFR 50, Appendix A, GDC 15 Reactor coolant system design | 1) TRPS<br>2) TRPS display<br>3) TRPS end devices<br>4) TRPS manual trip | 1) 7a2.4<br>2) 7a2.6<br>3) 7a2.4<br>4) 7a2.4 | This criterion directly addresses the coolant system. The instrumentation and controls provide control, protection, and means to safely mitigate the identified events described in Section 13a. |
| 31 | 10CFR 50, Appendix A, GDC 16 Containment design | 1) ESFAS<br>2) ESFAS end devices<br>3) ESFAS manual operator panel shutdown | 1) 7a2.5<br>2) 7a2.5<br>3) 7a2.5 | This criterion directly addresses the containment system. The SHINE facility does not have containment, but has confinement per NUREG-1537 definitions. The ESFAS provides monitoring of radioactivity in the IU and TOGS shielded cell ventilation. In the event radiation levels exceed predetermined values, the control and protection shall shutdown and isolate the process. |
| 32 | 10CFR 50, Appendix A, GDC 17 Electric Power Systems | 1) TRPS<br>2) NFDS<br>3) TRPS display<br>4) TRPS end devices | 1) 7a2.4<br>2) 7a2.4<br>3) 7a2.6<br>4) 7a2.4 | This criterion directly addresses the electric power system. The instrumentation and control and active ESFs are designed to fail-safe with loss of power. Upon complete loss of electric power, the de-energized state for the target solution in the TSV is to be directed to the geometrically-safe dump tank. The safety-related UPSS provides power upon loss of utility power to safety-related systems that allow for monitoring and maintaining a safe shutdown condition. See Table 3.5a-1. |

**Table 7a2.2-2 IF Verification Matrix Design Criteria, Bases, Description (Sheet 7 of 10)**

| Verification Matrix | Design Criterion | Design Basis Applicability | Detailed Section Reference | Functional Means |
|---|---|---|---|---|
| 33 | 10CFR 50, Appendix A,<br>GDC 19<br>Control Room | 1) TRPS<br>2) NFDS<br>3) ESFAS<br>4) TPCS<br>5) TRPS display<br>6) TPCS display<br>7) TRPS end devices<br>8) ESFAS end devices<br>9) TRPS manual trip<br>10) ESFAS manual operator panel shutdown | 1) 7a2.4<br>2) 7a2.4<br>3) 7a2.5<br>4) 7a2.3<br>5) 7a2.6<br>6) 7a2.6<br>7) 7a2.4<br>8) 7a2.5<br>9) 7a2.4<br>10) 7a2.5 | This criterion directly addresses the control room for the facility. The instrumentation and controls provide control, protection, and means to safely mitigate the identified events described in Section 13a. It affords the ability to have a manual initiated shutdown for the operator. |
| 34 | 10CFR 50, Appendix A,<br>GDC 20<br>Protection system functions | 1) TRPS<br>2) NFDS<br>3) ESFAS<br>4) TRPS display<br>5) TRPS end devices<br>6) ESFAS end devices<br>7) TRPS manual trip<br>8) ESFAS manual operator panel shutdown | 1) 7a2.4<br>2) 7a2.4<br>3) 7a2.5<br>4) 7a2.6<br>5) 7a2.4<br>6) 7a2.5<br>7) 7a2.4<br>8) 7a2.5 | This criterion directly addresses the protection systems for the facility. The TRPS provides protection as the safety-related protection system and the ESFAS provides mitigation as the isolation system. Both systems automatically trip upon appropriate signal which safely mitigates the identified events in Section 13a. The TRPS and the ESFAS include the ability to have a manual initiated shutdown and isolation for the operator. |
| 35 | 10CFR 50, Appendix A,<br>GDC 21<br>Protection system reliability and testability | 1) TRPS<br>2) NFDS<br>3) ESFAS<br>4) TRPS display<br>5) TRPS end devices<br>6) ESFAS end devices<br>7) TRPS manual trip<br>8) ESFAS manual operator panel shutdown | 1) 7a2.4<br>2) 7a2.4<br>3) 7a2.5<br>4) 7a2.6<br>5) 7a2.4<br>6) 7a2.5<br>7) 7a2.4<br>8) 7a2.5 | This criterion directly addresses the protection systems and the ability to tolerate single failure of any component and the requirement for online surveillance of any channel used for safety. The system is presently designed as either dual or triplicate sensing for the safety-related sensing measurements. For the triplicate systems, namely analog channels, there is online surveillance. For the dual redundant systems, namely discrete inputs, there is to be a periodic surveillance schedule developed for the facility. |

**Table 7a2.2-2 IF Verification Matrix Design Criteria, Bases, Description (Sheet 8 of 10)**

| Verification Matrix | Design Criterion | Design Basis Applicability | Detailed Section Reference | Functional Means |
|---|---|---|---|---|
| 36 | 10CFR 50, Appendix A, GDC 22 Protection system independence | 1) TRPS<br>2) NFDS<br>3) ESFAS<br>4) TRPS display<br>5) TRPS end devices<br>6) ESFAS end devices<br>7) TRPS manual trip<br>8) ESFAS manual operator panel shutdown | 1) 7a2.4<br>2) 7a2.4<br>3) 7a2.5<br>4) 7a2.6<br>5) 7a2.4<br>6) 7a2.5<br>7) 7a2.4<br>8) 7a2.5 | This criterion directly addresses the protection system independence as it relates to natural phenomena and influence from other systems during operation including loss of redundant channels. The TRPS is triple modular redundant so the likelihood of complete loss of all channels is very low. The ESFAS is designed with two independent trains, each one capable of initiating a safe shutdown. Additionally, the TPCS acts as a diverse defense-in-depth system that is monitoring the process to allow operator action if required. |
| 37 | 10CFR 50, Appendix A, GDC 23 Protection system failure modes | 1) TRPS<br>2) ESFAS | 1) 7a2.4<br>2) 7a2.5 | This criterion directly addresses the protection system failure mode. The TRPS and ESFAS are designed to fail-safe upon loss of electric power and loss of instrument air. The target solution is placed in a geometrically safe vessel upon loss of power. |
| 38 | 10CFR 50, Appendix A, GDC 24 Separation of protection and control systems | 1) TRPS<br>2) NFDS<br>3) ESFAS<br>4) TPCS<br>5) TRPS display<br>6) TPCS display<br>7) TRPS end devices<br>8) ESFAS end devices<br>9) TRPS manual trip<br>10) ESFAS manual operator panel shutdown | 1) 7a2.4<br>2) 7a2.4<br>3) 7a2.5<br>4) 7a2.3<br>5) 7a2.6<br>6) 7a2.6<br>7) 7a2.4<br>8) 7a2.5<br>9) 7a2.4<br>10) 7a2.5 | This criterion directly addresses the separation of the protection system from the control system. The TRPS, ESFAS, and TPCS are designed as independent systems with the exception of sharing isolated signals from the NFDS. The TRPS acts as the safety-related means to protect the PSB, the ESFAS as the SR means for isolation, and the TPCS can act as independent means for monitoring and controlling the TSV. These three systems are isolated and electrically independent systems. |
| 39 | 10CFR 50, Appendix A, GDC 25 Protection system requirements for reactivity control malfunctions | 1) TRPS<br>2) NFDS<br>3) TRPS display<br>4) TRPS end devices<br>5) TRPS manual trip | 1) 7a2.4<br>2) 7a2.4<br>3) 7a2.6<br>4) 7a2.4<br>5) 7a2.4 | This criterion directly addresses the protection system design to ensure that specified acceptable target solution design limits are not exceeded for any single malfunction of the TPCS. The TRPS and TPCS are designed as independent systems so that any malfunction of the TPCS that creates an abnormal event would trip the TRPS independent of the TPCS control state. See Table 3.5a-1. |

**Table 7a2.2-2 IF Verification Matrix Design Criteria, Bases, Description (Sheet 9 of 10)**

| Verification Matrix | Design Criterion | Design Basis Applicability | Detailed Section Reference | Functional Means |
|---|---|---|---|---|
| 40 | 10CFR 50, Appendix A, GDC 26 Reactivity control system redundancy and capability | 1) TPCS<br>2) TRPS | 1) 7a2.3<br>2) 7a2.4 | The reactivity control system for the SHINE subcritical assembly consists of two redundant dump valves and associated operators, either of which can safely shutdown the subcritical assembly and bring the Target Solution to a shutdown state in the TSV Dump Tank. Each dump valve and associated flow path provides drain capability for the TSV that exceeds the fill capacity by significant margin. Each dump valve is highly reliable and meets stringent quality assurance standards. Further, concurrent failure of both dump valves would not result in a critical system or accident scenario unless other malfunctions occurred concurrently, which is highly unlikely.<br><br>While not a direct reactivity control system, the neutron driver is also de-energized by the protection system when an IU shutdown is required. This shutdown of the neutron driver decreases the fission power of the subcritical assembly to essentially zero in normal and accident conditions. |
| 41 | 10CFR 50, Appendix A, GDC 27 Combined reactivity control systems capability | N/A | N/A | This criterion is not applicable to the SHINE system. Sufficient capacity to shutdown the Subcritical Assembly exists as the TSV Dump Tank is designed to be subcritical by geometry for the most reactive uranium concentration in solution. |
| 42 | 10CFR 50, Appendix A, GDC 28 Reactivity limits | 1) TPCS | 1) 7a2.3 | Reactivity is only directly adjusted in the system during the target solution fill process and the dump process. The TSV dump valves can only reduce the reactivity of the system upon opening. Indirect reactivity changes occur during the irradiation process due to temperature, power, and pressure changes. The amount and rate of reactivity increases during the fill and irradiation processes are limited through physical and control system design to ensure that the effects of postulated reactivity accidents can neither (1) result in damage to the PSB greater than limited local yielding, nor, (2) sufficiently disturb the TSV, its support structures or other TSV internals to impair significantly the capability to drain the TSV. |

**Table 7a2.2-2 IF Verification Matrix Design Criteria, Bases, Description (Sheet 10 of 10)**

| Verification Matrix | Design Criterion | Design Basis Applicability | Detailed Section Reference | Functional Means |
|---|---|---|---|---|
| 43 | 10CFR 50, Appendix A, GDC 29 Protection against anticipated operational occurrences | 1) TRPS<br>2) NFDS<br>3) ESFAS<br>4) TPCS<br>5) TRPS display<br>6) TPCS display<br>7) TRPS end devices<br>8) ESFAS end devices<br>9) TRPS manual trip<br>10) ESFAS manual operator panel shutdown | 1) 7a2.4<br>2) 7a2.4<br>3) 7a2.5<br>4) 7a2.3<br>5) 7a2.6<br>6) 7a2.6<br>7) 7a2.4<br>8) 7a2.5<br>9) 7a2.4<br>10) 7a2.5 | This criterion directly addresses the protection system's and the control system's ability to function with high reliability for all operational occurrences which requires a safety action. The TRPS, ESFAS, and TPCS are designed as completely independent systems so that any measured malfunction that creates an off-normal event would trip the TRPS or the ESFAS. The TRPS platform is specifically chosen for its high reliability and fault tolerance and recognized as such by the NRC as a pre-qualified platform. The TPCS is capable of high reliability due to its selection criteria, which is effectively similar in terms of reliability and fault tolerance as the TRPS. |

## 7a2.3 TSV PROCESS CONTROL DESCRIPTION

### 7a2.3.1 TPCS DESCRIPTION

The TPCS utilizes a high integrity controller typically specified for use in the process industry. The TPCS supports the activities required to perform the various functional modes expected of the irradiation process. The TPCS interfaces with the display systems in the control room discussed in Section 7a2.6.

The system utilizes redundancy with high self-diagnostic functionality for the internal design of subsystems within the controller system to meet the stringent demands required by the process. This includes the power supply to the power bus, input and output channels, and the main processor units. This forms the basis for a very robust and reliable digital controller.

### 7a2.3.2 TSV PROCESS CONTROL SYSTEMS

The TPCS is responsible for running the batch process for each IU cell. The TPCS controls the four modes of the irradiation unit:

a. Mode 1 Startup Mode: Filling the TSV
b. Mode 2 Irradiation Mode: Operating mode (neutron driver active)
c. Mode 3 Post-Irradiation Mode: TSV Dump Valves open
d. Mode 4 Transfer to RPF Mode: TSV Dump Tank Outlet Valves open

#### 7a2.3.2.1 Mode 1 - Startup Mode

The startup mode is the first and most technical of the four modes for the operator to implement for the IU cell irradiation process. This step moves target solution that is ready for irradiation from the TS hold tank to the TSV. This procedure is done by energizing a pump dedicated to that IU cell and controlling the volume of TS that enters the TSV. The process calculates the subcritical multiplication factor designated as M. The neutron flux level is monitored during this entire process, plotting the 1/M versus the fill volume (height). This is compared to a predicted graph that gives a band of acceptance for the 1/M value as it follows the amount of fill. The procedure requires that the operator wait for the neutron count rate to stabilize between each incremental step, which takes increasingly more time as the process approaches the target value. A typical fill of approximately [ Proprietary Information ] is expected to take 3-4 hours to complete. Sufficient permissives and interlocks to ensure that the vessel is ready to be filled safely are provided.

#### 7a2.3.2.2 Mode 2 - Irradiation Mode

The TSV inlet isolation valves are closed. TPCS and TRPS check their permissive/interlock tables, and when all of the attributes are satisfied, the instrumentation and controls allow the neutron driver to be energized and enables the tritium purification system (TPS) to add purified tritium to the target chamber.

With the neutron driver energized and the tritium being supplied to the target chamber, the irradiation process has started. With no abnormal events, the IU continues in this operation step for approximately 5-6 days. The TRPS and TPCS monitor the target solution during irradiation. Abnormal events that result in a measured parameter exceeding acceptable limits initiate an automatic trip of the ESFAS or the TRPS, or both.

At the completion of prescribed irradiation period, the system is ready to transfer from the irradiation mode and to the post-irradiation mode.

#### 7a2.3.2.3 Mode 3 - Post-Irradiation Mode

The neutron driver is de-energized and tritium delivery to the target chamber is stopped. This sequence moves the target solution from the TSV to the TSV dump tank, and holds the solution in the TSV dump tank for decay.

The TPCS opens the dump valves. The TSV level indication is utilized to verify that the TSV is empty. The TSV dump valves remain open to ensure that the vessel is completely drained.

After [ Proprietary Information ] of decay time, the TS in the dump tank can be transferred to the first stage of molybdenum extraction.

#### 7a2.3.2.4 Mode 4 - Transfer to RPF Mode

The TPCS checks the permissive/interlock tables, and if the attributes are satisfied, the dump valves are closed. With the valve position confirmed, the TPCS checks the permissive/interlock tables, and if the attributes are satisfied, the TPCS allows the transfer of the contents of the TSV dump tank to the RPF.

This pumped transfer is coordinated between the RPF operator and the IU cell operator. When ready to transfer, the TSV dump tank outlet isolation valves are opened. These remain open until the TS batch is pumped from the TSV dump tank.

### 7a2.3.3 SEQUENCE & INTERLOCK SUMMARY

The sequence and interlock methodology ensures that no improper step can be made that would result in an unsafe condition in the IU cell process. The operator can only perform those tasks or functions available in a specific step of process and the TCPS validates the sequence interlock/ permissive tables to assure the proper operating sequence.

## 7a2.4 TSV REACTIVITY PROTECTION SYSTEM

### 7a2.4.1 TRPS DESCRIPTION

The TRPS utilizes a digital control platform previously approved by the NRC for use with safety systems. This platform forms the basis for the safety-related structures, systems, and components (SSCs) that are actively controlled and make up the reactivity protection system. Preliminary design has selected a triple modular redundancy (TMR) PLC as the platform for the TRPS. This DCS utilizes the premise of triple modular redundancy for the internal design of subsystems within the controller system. This includes power supply to the power bus, input and output modules, and the main processor units. This forms the basis for an extremely robust and reliable digital controller. The TRPS interfaces with the display systems in the control room discussed in Section 7a2.6.

When the TRPS measures an abnormal event in an IU, it starts protective action by initiating a TSV trip of the affected IU cell. The following monitored parameters initiate a trip:

a. High $H_2$ concentration in the PSB.
b. High neutron flux, source range and high range.
c. Low temperature of the PCLS.
d. High temperature of the PCLS.
e. Loss of PCLS flow.
f. ESFAS trip input signal.
g. Manual trip pushbutton.

TRPS trip provides the following protective actions:

a. Open TSV dump valves to drain target solution to TSV dump tank.
b. Close TSV fill valves.
c. Close TSV dump tank outlet valves.
d. De-energize neutron driver.

#### 7a2.4.1.1 TSV Trips Description (Functional)

This section identifies the various modes of operation and initiating events that are monitored resulting in a TRPS trip. With the exception of the transition from startup mode to irradiation mode, sensor measurement values are treated similarly and their activation of the TRPS trip is discussed. This discussion relates to each TSV/IU cell individually. The control functions are identical and independent for each TSV/IU cell.

##### 7a2.4.1.1.1 PSB High Hydrogen Concentration Trip

Signal Type - Analog

The TRPS monitors the hydrogen gas concentration in the TOGS gas with two independent sets of continuous gas analyzers. These analyzers monitor the gas composition for hydrogen utilizing sampling ports that are on the TOGS, just downstream from the hydrogen gas recombiners.

The TRPS activates protective action whenever the 1oo2 exceeds the high hydrogen concentration setpoint. The trip is automatic and not delayed.

7a2.4.1.1.2 TSV High Neutron Flux (Source Range and High Range)

Signal Type - Analog

The TRPS monitors the neutron flux surrounding the TSV with a set of triplicate neutron detectors. These signals are part of the NFDS and passed on to the TRPS. These detectors measure the flux outside the TSV, spaced approximately 120 degrees apart in the light water pool.

The source range trip is used during fill operations. After the fill operation is complete, the source range trip is blocked and the high range trip provides protection during irradiation operations.

The TRPS activates protective action whenever the two closest flux level measurements in a voted triad (2oo3) exceed the high flux setpoint. The trip is automatic and not delayed.

7a2.4.1.1.3 PCLS Under Temperature Trip Signal Type - Analog

The TRPS monitors the internal temperature of the PCLS with one set of triplicate thermocouples. These thermocouples measure the temperature of the water in the closed loop cooling system.

The TRPS activates protective action whenever the two closest temperatures in a voted triad (2oo3) exceed the low temperature setpoint. The trip is automatic and not delayed.

7a2.4.1.1.4 PCLS Over Temperature Trip Signal Type - Analog

The TRPS monitors the internal temperature of the PCLS with one set of triplicate thermocouples. These thermocouples measure the temperature of the water in the closed loop cooling system.

The TRPS activates protective action whenever the two closest temperatures in a voted triad (2oo3) exceed the high temperature setpoint. The trip is automatic and not delayed.

7a2.4.1.1.5 PCLS Loss of Flow Trip Signal Type - Analog

The TRPS monitors the flow rate of the PCLS with flow meters. These two flow meters (one redundant) measure water flow in the primary closed loop cooling system.

The TRPS activates mitigative action whenever the measured flow decreases below the acceptable level. The trip is automatic and not delayed.

7a2.4.1.1.6 ESFAS Actuation Trip

Signal Type - Discrete

The TRPS monitors the ESFAS with two independent inputs from each train of the ESFAS. These inputs are discrete relay contact switches with each connected to the TRPS.

The TRPS activates protective action whenever the 1oo2 logic activates from each ESFAS train. The trip is automatic and not delayed.

7a2.4.1.1.7 Manual IU Trip

Signal Type - Discrete

The manual IU trip utilizes two pushbutton switches located in the main control room. A switch is dedicated to an individual TRPS input. Each switch provides the ability to shutdown the IU.

The manual switch activates the TRPS trip. An analog shutdown method independent of the DCSs is also included in the design.

7a2.4.1.1.8 IU Trip Reset

Signal Type - Discrete

Once the TRPS has been activated, it takes an operator to manually reset the TRPS. This is done from the TRPS human machine interface (HMI) panel using the TRPS reset function. The TRPS requires input from the operator to be reset. If the conditions that caused a trip are still present or present but not bypassed, then the reset would be unsuccessful.

7a2.4.2 SYSTEM PERFORMANCE ANALYSIS

System analysis discussed in Subsection 7a2.2.4.

7a2.4.3 NFDS DESCRIPTION

The NFDS provides the measurement of the thermal power and neutron flux of the subcritical assembly. In the IU cell, the TSV is surrounded by flux detectors. A neutron flux of approximately up to [ Proprietary Information ] neutron/$cm^2$-s at the outer surface of the vessel is expected when the neutron driver is operating at full power. The flux detectors are placed outside the SASS wall submerged in the light water pool at a distance to allow measurement within the detector’s range. There is one NFDS for every IU cell.

The preliminary design utilizes three wide-range guarded fission chambers as the detectors with each representing a separate channel. A wide-range detector is able to span the necessary decade with sufficient sensitivity to provide feedback measurement to the operator while filling, as well as accurately monitoring to full operating power.

The NFDS calculates and displays five different values:

- Source range level (SRL)
- Source range period (SRP)
- Wide range level (WRL)
- Wide range period (WRP)
- High range level (HRL)

The SRL signal is determined by utilizing the fission chamber as a pulse counter. The source range signal is displayed from 0.1 to $10^5$ cps on a logarithmic scale. The derivative of this signal is the SRP, calculated and displayed as -30 to + 3 seconds.

The WRL signal is calculated from a combination of counting and mean square voltage (MSV) techniques. Both signals are continuously monitored and the appropriate value is displayed. The counting technique covers the lower decades while the MSV covers the upper decades of power, with a minimum of two decades of overlap. The WRL is displayed as $10^{-8}$ to 200 percent power on a logarithmic scale. The WRL is continuously monitored and the derivative represents the WRP displayed as -30 to + 3 seconds.

The HRL signal is derived from a linear amplification of the DC current in the guarded fission chamber. This signal is then displayed as 0 to 125 percent as a linear scale.

The NFDS monitors the power levels and provides trip functions at a set value. The trip value is adjustable and can be set over the entire monitored range. The relays de-energize to trip, so upon loss of power to the signal processor, it fails to a safe condition. The bistable trip circuits utilize the voting interface internal to the NFDS equipment that allows for 2oo3 voting scheme with the ability to manually select any one channel for maintenance or channel verification. During channel calibration and maintenance the output trips are changed to 1oo2 voting scheme until placed back in service. These setpoints are managed under the setpoint management plan as dictated in the design criteria, ISA 67.04.01.

There are six isolated analog device interface channels in the signal processors. These are configured to represent any of the measured / calculated values in the signal processor section. The six isolated outputs are configured to represent the WRL for each individual channel measurement, three going to the TRPS and three to the TPCS. These values are displayed on the static display within the TRPS and TPCS.

## 7a2.5 ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

### 7a2.5.1 ESFAS DESCRIPTION

The ESFAS provides the means to activate the ESFs used to mitigate possible consequences of the postulated accident scenarios described in Chapter 13. The ESFs are designed as fail-safe so that removing electric power results in the component assuming the position that provides greater safety. The ESFAS configuration is such that each IU cell can be activated independently. The configuration is also segmented such that there are two independent trains, A and B. Each train acts independently and has the capability to mitigate possible consequences solely on its own.

Train A and train B exist as separate enclosures installed in different physical locations in the facility. Both train A and train B are Class 1E systems and routing of train A and train B takes physically separate paths as described in IEEE-384.

Figure 7a2.5-1 shows a typical circuit for power interruption for a powered coil. The ESFs are designed to fail-safe upon loss of power. The ESFAS removes power from each ESF during activation. The ESFAS utilizes two specially designed safety relays in series for each end device that is controlled. Figure 7a2.5-2 shows a typical panel layout for a single train. Train A and train B are of similar design. Each train to each IU cell is capable of individual testing. For each train A or train B, and each IU cell, actuation is required to complete its protection function prior to being reset.

The ESFAS relays have the ability to accept dual inputs, differentiate between relay inputs monitoring for ground faults or cross faults, have internally redundant contacts, and most importantly, offer the user the ability to actively monitor the function and status of the relay itself. The health status of each relay is an input to the TPCS so that pre-emptive maintenance can occur before loss of function.

Each IU cell signal trip sensing circuit is comprised of a pair of ESD pushbutton contacts on the ESFAS manual operator panel in series with the ESFAS initiating devices. Any one of these trip circuits can initiate the ESFAS and trip the specific IU cell ESFAS.

Once tripped, the means for resetting the ESFAS is a manual reset pushbutton on the ESFAS manual operator panel. A manual reset pushbutton is provided for each train, which physically resets train A or train B individually for an IU cell. The ESFAS is qualified to IEEE 323 and IEEE 344.

### 7a2.5.2 ESFAS MANUAL OPERATOR PANEL

The ESFAS manual operator panel is located in the control room. It has the capability to manually initiate a trip of any train of any IU cell individually. The ESFAS manual operator panel indicates a trip, an over-ride / bypass, and has the capability to reset the individual train. The panel also includes a ‘Bulb Check’ so that surveillance can be made of the visual indicating lamps. Figure 7a2.5-3 shows a layout for such a panel.

The operator has the ability to test each IU cell train A and train B between IU cycles. Periodic testing of the ESFAS trains will be included in the surveillance requirements.

### 7a2.5.3 ESFAS INITIATING SIGNALS FOR ACTUATION

When the ESFAS receives an initiating signal from a monitored sensor it actuates the ESFs for the affected IU cell. The following monitored parameters initiate a trip:

a. High radiation in the ventilation system (RVZ1).
b. Manual trip ESD pushbutton.

ESFAS trip provides the following mitigative actions:

a. Close PCLS isolation valves.
b. Close tritium delivery and return isolation valves.
c. Close LWPS supply and return isolation valves.
d. Close IU cell bubble-tight dampers.
e. Input signals to TRPS for TSV trip.

### 7a2.5.4 ESFAS TRIPS DESCRIPTION (FUNCTIONAL)

This subsection identifies the various modes of operation and initiating events that are monitored resulting in an ESFAS trip. The control functions are identical and independent for each IU cell system.

#### 7a2.5.4.1 High Radiation in IU cell ventilation (RVZ1)

Signal Type - Discrete

The ESFAS monitors the level of the radioactivity in the IU cell ventilation (RVZ1) with two independent sets of radiation detectors. These gamma type detectors utilize discrete relay contact switches with each one going to the ESFAS. Each detector has an additional discrete relay that is a status input to the TRPS.

The ESFAS activates whenever the 1oo2 logic detects radioactivity in the IU cell ventilation. The sensitivity of these devices is calibrated to trip at a pre-determined value. The trip is automatic and not delayed.

#### 7a2.5.4.2 ESFAS Manual Trip

Signal Type - Discrete

The manual ESFAS trip utilizes two control switches located in the main control room. A control switch is dedicated to each ESFAS train. Each switch provides the ability to actuate the ESFAS with no interaction with the TRPS or the TPCS.

The manual emergency pushbutton activates the ESFAS trip of each respective train whenever one is activated.

#### 7a2.5.4.3 ESFAS Trip Reset

Signal Type - Discrete

Once the ESFAS has been activated, it takes an operator to manually reset the ESFAS. This is done from the ESFAS manual operation panel using the ESFAS reset pushbutton. This reset pushbutton re-energizes the safety relays for both trains simultaneously. The ESFAS cannot be reset by the digital controller (TRPS / TPCS). If the conditions that caused a trip are still present, then it would be expected that the reset would be unsuccessful.

### 7a2.5.5 SYSTEM PERFORMANCE ANALYSIS

The system performance analysis is discussed in Subsection 7a2.2.4.

## 7a2.6 CONTROL CONSOLE AND DISPLAY INFORMATION

### 7a2.6.1 OPERATOR INTERFACE DESRIPTION

The operator has direct visualization of essential values and has the ability to monitor and control the irradiation process from TPCS in the control room. Monitoring of the TRPS is provided in the control room. The TRPS and the TPCS each have a minimum of three dedicated displays:

a. Static display that shows critical measurement values and performs the function of annunciator panel. This display panel cannot be modified as it is a fixed display.

b. Alarm / event annunciator display panel. This panel displays any event or alarm that has been defined in the development process. The display is semi-static, in that it performs the function of an alarm printer. This display allows the operator to acknowledge current events and alarms, and forms the historical record of events.

c. Dynamic interface display panel (the HMI panel). This is the panel that allows the operator to perform tasks, change modes, enable/disable over-rides, essentially anything that requires an operator to allow, perform, or modify a task or event.

Each set of displays are arranged in a workstation group. This group comprises all of the displays and the keyboard/mouse that is utilized to interface with each system. The workstation group also includes a set of displays that are part of the radiological integrated control system (RICS). The RICS display development is in covered in Section 7b.

Each HMI for each system, TRPS, TPCS, and RICS has separate color printers. These printers allow the operator to output any display for reference. The screen development follows the design criteria and basis as defined in Subsections 7a2.2.1 and 7a2.2.2.

In the control room, there are two identical workstations. Each workstation has the same capabilities and allows for usage simultaneously. Figure 7a2.6-1 shows the graphic representation of the display description described above. Figure 7a2.6-2 shows a plan view layout of the control room.

### 7a2.6.2 CONTROL ROOM AND DISPLAY ACCESS

Access to the control room is controlled. TRPS and TPCS have security access. Only those personnel with appropriate authorization have access to make changes to the TRPS and TPCS interface displays.

### 7a2.6.3 OPERATOR INTERFACE DATA ENTRY

Operator display interfaces that require data entry from a touchscreen, mouse or keyboard shall require two steps: data entry and confirmation. The two step process is for requests that result in an input or change of state going to the TRPS or the TPCS. The confirmation display offers the operator the option to continue or cancel the requested action.

### 7a2.6.4 DISPLAY INTERFACE HARDWARE AND SOFTWARE

As described in Subsection 7a2.2.1, the hardware and software used on the TRPS is designed according to IEEE-603 and IEEE 7-4.3.2 as a requirement of the safety classification. The TPCS is designed under the guidelines as a non-safety system. This requires appropriate isolation of signals and communication, as well as prioritization of commands between safety-related and nonsafety-related systems.

### 7a2.6.5 HUMAN FACTORS ENGINEERING

The development of the displays and interface systems for both the TRPS and TPCS is guided by good human factors engineering practices. These criteria are listed in Subsection 7a2.2.1. NUREG-0700 is utilized for development of the displays for the safety-related and nonsafety-related systems.

### 7a2.6.6 STATIC ANNUNCIATOR/FIXED STATUS DISPLAY

A static annunciator display will be used for the TRPS for all eight cells on one dedicated display.

### 7a2.6.7 ALARM/EVENT DISPLAY

The TRPS and the TPCS are both specified with alarm/event (A/E) displays. The A/E displays indicate the recorded events that have been pre-programmed as significant. The DCS includes functions programmed into an A/E display. The function of the A/E display is to act as the first out. Each IU cell shall have a corresponding block or window that displays the A/Es that have occurred, with a rolling screen showing the most recent at the bottom, and the oldest at the top.

The operator interface panel allows the operator to select a specific IU cell A/E history and display that information on the operator interactive HMI display.

### 7a2.6.8 TRPS/TPCS HUMAN MACHINE INTERFACE (HMI)

The TRPS and the TPCS HMI act as the interface displays for the operator. For the TRPS, the functions identified are to allow the operator access to the A/E display for the TRPS and to perform bypass or over-ride selection for TRPS related tasks or equipment.

For the TPCS, the functions allow the operator access to the A/E display for the TPCS, perform bypass or over-ride selection for TPCS related tasks or equipment, and control the sequence and tasks in each process step.

The HMI display development is similar for each IU cell. The function of each action and display has the same format between screens.

### 7a2.6.9 TRPS/TPCS AND DISPLAY INDEPENDENCE

The functionality of the displays, computer systems, or HMI utilized for the TRPS or the TPCS workstations in no way impairs the operational function of the TRPS or the TPCS.

The TRPS and TPCS are each kept as electrically isolated systems. This includes communication cabling and networking to the various display systems that are employed to make up the workstations for the control room.

Potential variables, conditions, or other items that will be probable subjects of technical specifications associated with the TRPS, TPCS and display instrumentation are provided in Chapter 14.

## 7a2.7 RADIATION MONITORING SYSTEMS

### 7a2.7.1 RADIATION MONITORING SYSTEMS

The objective of the radiation monitoring system is to provide SHINE facility control room personnel with a continuous record and indication of radiation levels at selected locations where radioactive materials may be present, stored, handled, or inadvertently introduced. The system is also designed to ensure that there is accurate and reliable information concerning radiation safety as related to personnel safety. The design considerations for the radiation monitoring system include the following:

- Provision of supervisory information to SHINE facility operators so that in the event of an accident resulting in a release of radioactive material, decisions on deployment of personnel can be made properly.

- Indication and recording in the control room of the gamma and airborne radiation levels in the selected areas as a function of time, and, if necessary, alarming to indicate any abnormal radiation condition. These indicators aid in maintaining plant contamination levels as low as reasonably achievable (ALARA) and in minimizing personnel exposure to radiation.

- Provision of local alarms and/or indicators positioned at key points throughout the SHINE facility where a substantial increase in radiation levels might be of immediate importance to personnel frequenting or working in the area.

- Provision of input to the ESFAS and RICS.

See Section 7b.6 for discussion on the criticality accident alarm system (CAAS).

### 7a2.7.2 RADIATION MONITORING SYSTEM DESCRIPTION

The SHINE facility is equipped with a centralized airborne radiation monitoring system that monitors gamma and beta (tritium) radiation levels. Continuous air monitors (CAM) and radiation area monitors (RAM) are incorporated into the overall facility monitoring scheme. The SHINE facility radiation monitoring system provides the following:

- Overall facility radiation monitoring and alarming coverage.
- Local and control room monitoring display and alarming.
- Radiation monitoring and alarming in the event of a release of radioactive material to the environment.
- Signal input interface with SHINE facility safety systems (e.g., ESFAS and RICS).

### 7a2.7.3 RADIATION MONITOR LOCATIONS

RAMs are located in areas where personnel may be present and where radiation levels could become significant based upon the following considerations:

- Occupancy status of the area including time requirements of personnel in the area, the proximity to primary and secondary radioactive sources, and shielding.
- Potential for increase in the background radioactivity level.
- Desirability of surveillance of infrequently visited areas.

CAMs are located in work areas where there is a potential for airborne radioactivity. The CAMs have the capability to detect derived air concentrations (DAC) within a specified time.

Beta monitors are strategically placed around the tritium purification system (TPS) gloveboxes to detect and alarm for tritium leaks.

### 7a2.7.4 RADIATION MONITORING EQUIPMENT DESCRIPTIONS

#### 7a2.7.4.1 CAM Equipment Description

CAM units consist of a particulate measuring channel with a filter to capture particulate. Air is forced through the system by a pump assembly.

The sample is withdrawn from inside the appropriate area, room, or cell through an isokinetic nozzle with the sampling volume flow at a known fixed rate so that the accumulation of radioactive particles can be interpreted as a quantitative sample. After passing through the nozzle, the sample is drawn through tubing and through a fixed or moving filter tape before being discharged to the atmosphere. The samplers also have a purging system for flushing the volume cell surrounding the gas sample chamber with clean air for purposes of calibration and the removal of crust activity. Replaceable liners are changed out periodically when contamination becomes excessive. Flow regulating ensures that flow through the filters remains constant.

Each instrument channel includes a detector, preamplifier, count rate meter, and a power supply. The detector is a scintillation counter having a gamma sensitive crystal and a photo multiplier whose output pulses are counted by the rate meter.

Each readout module is equipped with a light that illuminates when the radiation level exceeds preset limits. The setpoint is adjustable over the entire detection range. Pressing a button causes the meter to indicate the alarm setpoint. Visible alarms are accompanied by a simultaneous audible alarm that sounds in the control room. A normally energized light de-energizes when there is a detector signal failure, circuit failure, power failure, or failure due to a disconnected cable. Power for the monitors that initiate a safety signal is provided from the uninterruptible electrical power supply system (UPSS). Loss of power and signal failure is monitored for each detector.

CAMs are provided with a check source. This check source simulates a radiation field and is used as a convenient operational and gross calibration check of the detectors and readout equipment.

CAM calibration includes, where practical, exposures to the specific isotopes that the particular system monitors in the field. Instrument calibrations are performed at prescribed frequencies. Electronic test signal and/or radioactive check source drift indication may also be a cause for CAM recalibration.

The tritium beta monitor detector unit is housed in an environmentally suitable container that can be mounted on a wall, or other suitable surface.

The detectors are designed to be operational over a wide range of temperatures. The design of the detectors will meet expected normal and abnormal environmental design conditions, as appropriate.

7a2.7.4.2 RAM Equipment Description

The RAM detector unit is housed in an environmentally suitable container that is mounted in a duct, on a wall, or other suitable surface. The sensitivity of each detector is sufficient to have the alarm setpoint an order of magnitude higher than the detection threshold.

The detectors are designed to be operational over a wide range of temperatures. The design of the detectors will meet expected normal and abnormal environmental design conditions, as appropriate.

Saturation is not expected to adversely affect operation of the detector within its calibrated range.

Sensors are mounted as close as practical to the most probable radiation sources with no objects, persons, pillars, and piping serving as shielding. The sensors are also mounted so as to minimize inaccuracies due to any directionality of the detector.

7a2.7.4.3 Audible and Visual Alarm Devices

When the radiation exceeds predetermined levels, alarms actuate in the control room and at selected detector locations.

The alarms consist of:

- An “alert” light illuminates when the radiation level exceeds preset limits. The setpoint is adjustable.
- A “high” alarm red light illuminates when radiation levels exceed a predetermined alarm setpoint. The setpoint is adjustable.
- A “failure” alarm sounds when either the power or the channel's electronics fail.

The visual alarms are accompanied by a simultaneous audible alarm annunciator both at the selected detector locations and in the control room. The annunciator windows for the monitors are located in the control room. The alarm can be manually reset when the alarm conditions are corrected. The local alarm horns and warning lights remain on until the radiation level is below the present level.

Specified RAMs also trigger the ESFAS or RICS. The ESFAS or RICS incorporates safety relays whose function is to interrupt power to the active ESFs that have been identified in Chapter 13. The ESFAS or RICS can be tripped manually from the control room by an operator.

Refer to Subsection 7a2.2.4 for discussion of safety function performance analysis.

Potential variables, conditions, or other items that will be probable subjects of technical specifications associated with the radiation monitoring instrumentation are provided in Chapter 14.

## 7a2.8 REFERENCES

**ANS, 2003.** Criticality Accident Alarm System, ANS-8.3:R2003, American Nuclear Society, 2003.

**EPRI, 1996.** Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications, EPRI TR-106439, Electric Power Research Institute, 1996, Website: http://pbadupws.nrc.gov/docs/ML1033/ML103360462.pdf.

**IEEE, 1987.** IEEE Guide For General Principles Of Reliability Analysis Of Nuclear Power Generating Station Safety Systems, IEEE Std 572:1987, IEEE Power & Energy Society, The Institute of Electrical and Electronics Engineers, Inc., 1987.

**IEEE, 2000.** IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems, IEEE Std 379:2000, IEEE Power & Energy Society, The Institute of Electrical and Electronics Engineers, Inc., 2000.

**IEEE, 2002.** IEEE Standard for Software Quality Assurance Plans, IEEE Std 730:2002, IEEE Power & Energy Society, The Institute of Electrical and Electronics Engineers, Inc., 2002.

**IEEE, 2003.** IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations, IEEE Std 323:2003, IEEE Power & Energy Society, The Institute of Electrical and Electronics Engineers, Inc., 2003.

**IEEE, 2004b.** IEEE Standard Criteria for Software Verification and Validation, IEEE Std 1012:2004, IEEE Power & Energy Society, The Institute of Electrical and Electronics Engineers, Inc., 2004.

**IEEE, 2004c.** IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Facilities, IEEE Std 577:2004, IEEE Power & Energy Society, The Institute of Electrical and Electronics Engineers, Inc., 2004.

**IEEE, 2005.** IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations, IEEE Std 344:2005, IEEE Power & Energy Society, The Institute of Electrical and Electronics Engineers, Inc., 2005.

**IEEE, 2008a.** IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits, IEEE Std 384:2008, IEEE Power & Energy Society, The Institute of Electrical and Electronics Engineers, Inc., 2008.

**IEEE, 2008b.** IEEE Standard for Software and System Test Documentation, IEEE Std 829:2008, IEEE Power & Energy Society, The Institute of Electrical and Electronics Engineers, Inc., 2008.

**IEEE, 2008c.** IEEE Standard for Software Reviews and Audits, IEEE Std 1028:2008, IEEE Power & Energy Society, The Institute of Electrical and Electronics Engineers, Inc., 2008.

**IEEE, 2009a.** IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, IEEE Std 603:2009, IEEE Power & Energy Society, The Institute of Electrical and Electronics Engineers, Inc., 2009.

**IEEE, 2010a.** IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations, IEEE Std 497:2010, IEEE Power & Energy Society, The Institute of Electrical and Electronics Engineers, Inc., 2010.

**IEEE, 2010b.** IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, IEEE 7-4.3.2, IEEE Power & Energy Society, The Institute of Electrical and Electronics Engineers, Inc., 2010.

**IEEE, 2012a.** IEEE Standard for Configuration Management in Systems and Software Engineering, IEEE Std 828:2012, IEEE Power & Energy Society, The Institute of Electrical and Electronics Engineers, Inc., 2012.

**IEEE, 2012b.** IEEE Standard for Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems, IEEE Std 338:2012, IEEE Power & Energy Society, The Institute of Electrical and Electronics Engineers, Inc., 2012.

**ISA, 2006.** Setpoints for Nuclear Safety- Related Instrumentation, ISA 67.04.01:2006, The Instrumentation, Systems, and Automation Society, 2006.

**NRC, 1993.** The Programmable Logic Controller and Its Application in Nuclear Reactor Systems, NUREG/CR-6090, U.S. Nuclear Regulatory Commission, Washington, DC, 1993.

**NRC, 1996.** Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems, NUREG/CR-6463, U.S. Nuclear Regulatory Commission, Washington, DC, 1996.

**NRC, 2002.** Human-System Interface Design Review Guidelines, NUREG-0700, Rev. 2, U.S. Nuclear Regulatory Commission, Washington, DC, 2002.

**NRC, 2009.** Design Practices for Communications and Workstations in Highly Integrated Control Rooms, NUREG/CR-6991, U.S. Nuclear Regulatory Commission, Washington, DC, 2009.

**United States Government, 2011.** General Design Criteria, Code of Federal Regulations, Title 10, Part 50, Appendix A, Office of the Federal Register, Government Printing Office, January, 2011.

# 7b RADIOISOTOPE PRODUCTION FACILITY INSTRUMENT & CONTROL SYSTEM

## 7b.1 SUMMARY DESCRIPTION

Within the SHINE facility, the RPF houses the extraction, purification, packaging, target solution preparation and cleanup, and waste treatment systems. The systems are enclosed predominately by hot cells and glove box designs. The RICS provides for monitoring and control of safety-related components (including ESFs) within the RPF. The RICS also provides process monitoring and control of the nonsafety-related systems within the RPF.

### 7b.1.1 RICS DESCRIPTION (SR/ESF)

The RICS is a DCS that monitors and controls SR components (including ESFs) within the RPF. When the monitored safety parameters exceed normal conditions, the RICS provides mitigative action by activating the ESF for the affected area. The ESFs in the RPF provide isolation functionality and alert operators of potential contamination events. The RICS can isolate one or any combination of the isolable hot cells in the RPF. The RICS also initiates the ESF isolation between ventilation zones in the RCA. This system is further described in Subsection 7b.2.3 and Section 7b.4.

### 7b.1.2 RICS DESCRIPTION (PROCESS CONTROL)

The RICS performs as the overall production process controller. It monitors and controls the required instrumented functions within the RPF. This includes monitoring of process fluid transfers and controlled inter-equipment pump transfers of process fluids. This system is further described in Section 7b.3.

### 7b.1.3 RADIATION MONITORING

The RPF utilizes CAMS, RAMS, and the criticality accident alarm system (CAAS) for continuous monitoring of processes. The CAMS, RAMS, and CAAS are strategically placed throughout the RPF to alert personnel of any potential radiation hazards. The CAMS, RAMS, and CAAS monitor the RPF for radiation and perform alarming in the control room and locally at locations throughout the RPF. The CAAS is further described in Section 7b.6. The RAMS and CAMS are further described in 7a2.7.

Specific RAMs channels provide input to RICS for ESF functions.

### 7b.1.4 CONTROL ROOM AND INSTRUMENT DISPLAYS

The SHINE RPF is monitored and controlled from a centralized control room. The RICS has separate dedicated annunciation, alarming, and operator interface displays. The RICS operator panels and displays are electrically isolated and independent components. Within the control room, there are RICS consoles that are redundant in nature and can be operated simultaneously and independently. From these consoles, an operator can assess the state of a hot cell and other process enclosures within the RPF. The operator can view and trend essential measurement values from the operator interface display. From the RICS operator workstation, the operator controls many of the RPF processes that are not performed through manual means (such as radioisotope purification). The operator is provided real-time data from the essential measurements used to control and monitor the RPF process on the RICS displays. This system is further described in Section 7b.5.

The human-machine interface is addressed in Section 7b.5.

## 7b.2 DESIGN OF INSTRUMENTATION AND CONTROL SYSTEMS

The intent of Appendix A to 10 CFR 50, General Design Criteria for Nuclear Power Plants, is being applied to the instrument and controls as outlined in Section 3.5b, which discusses the application of these General Design Criteria (GDC) to the RPF in length.

### 7b.2.1 DESIGN CRITERIA

The applicable criteria and guidelines as they apply to the RPF instrumentation and control systems are summarized in Table 7b.2-1.

### 7b.2.2 DESIGN BASES

The design bases for major systems utilized in the RPF are detailed with the selected design criteria in Table 7b.2-1. The design basis as it is being applied to the RPF and the means for compliance are discussed in this table, design criteria on the left, design bases on the right.

**Table 7b.2-1 Design Criteria for the RPF Instrumentation and Control System (Sheet 1 of 13)**

| Design Criteria as Cited with Summary Intent | Design Bases As Applied to SHINE |
|---|---|
| **IEEE Std 379-2000 (R2008)**<br><br>**IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems**<br><br>**Abstract**: Application of the single-failure criterion to the electrical power, instrumentation, and control portions of nuclear power generating safety systems is covered in this standard.<br><br>**Keywords:** actuator, cascaded failure, common-cause failure, design basis event, detectable failure, effects analysis, safety system, single-failure criterion, system actuation, system logic | As Applied<br><br>This standard is applied to the design of the RICS, ESFs, and other instrumentation SSCs that are identified as SR in the RPF.<br><br>Means of Compliance<br><br>The RICS is a DCS designed, rated, and approved for use in safety instrumented systems as determined by ISA 84.00.01. The system will use a safety PLC as recognized by IEC 61508 conforming to a system based on redundant power supplies, processors, and input/output channels. Controls that are classified SR in the Section 6b and 13b for the RPF are evaluated against the single failure criteria.<br><br>Exception<br><br>NUREG-1537 allows for sharing and combining of systems and components with justification. This does not negate the single failure criterion; it makes an evaluation of systems mandatory where this would be a proposed design solution, which will be a function of reliability and risk. |
| **IEEE Std 577-2004**<br><br>**IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Facilities**<br><br>**Abstract:** This standard sets forth minimum acceptable requisites for the performance of reliability analyses for safety related systems of nuclear facilities when used to address the reliability requirements identified in regulations and other standards. The requirement that a reliability analysis be performed does not originate with this standard. However, when reliability analysis is used to demonstrate compliance with reliability requirements, this standard describes an acceptable response to the requirements.<br><br>**Keywords:** nuclear facilities, reliability analysis, safety systems | As Applied<br><br>This standard is applied to the design of the RICS, ESFs, and other instrumentation SSC that is identified as SR for the SHINE facility.<br><br>Means of Compliance<br><br>For SR functions identified in the Section 6b and 13b, the design performs a reliability analysis of the proposed design solution. This can be qualitative or quantitative in nature as described in the standard. |

**Table 7b.2-1 Design Criteria for the RPF Instrumentation and Control System (Sheet 2 of 13)**

| Design Criteria as Cited with Summary Intent | Design Bases As Applied to SHINE |
|---|---|
| **IEEE Std 603-2009**<br><br>**IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations**<br><br>**Abstract**: Minimum functional and design criteria for the power, instrumentation, and control portions of nuclear power generating station safety systems are established. The criteria are to be applied to those systems required to protect the public health and safety by functioning to mitigate the consequences of design basis events. The intent is to promote appropriate practices for design and evaluation of safety system performance and reliability. Although the standard is limited to safety systems, many of the principles may have applicability to equipment provided for safe shutdown, post accident monitoring display instrumentation, preventive interlock features, or any other systems, structures, or equipment related to safety.<br><br>**Keywords:** actuated equipment, associated circuits, Class 1E, design, failure, maintenance bypass, operating bypass, safety function, sense and command features, sensor | As Applied<br><br>This standard is applied to the design of the RICS, ESFs, and other instrumentation SSCs that are identified as SR for the RPF. It describes the minimum functional and design criteria for safety systems. It does not describe what systems are to be determined as safety systems.<br><br>Means of Compliance<br><br>For SR functions identified in Section 6b or 13b, the design conforms to the practices detailed in the standard.<br><br>Exception<br><br>The SHINE facility is not a nuclear power reactor and does not have all of the systems detailed in this standard. The intent of this standard is followed. |
| **IEEE Std 384-2008**<br><br>**IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits**<br><br>**Abstract**: The independence requirements of the circuits and equipment comprising or associated with Class 1E systems are described. Criteria for the independence that can be achieved by physical separation and electrical isolation of circuits and equipment that are redundant are set forth. The determination of what is to be considered redundant is not addressed.<br><br>**Keywords:** associated circuit, barrier, Class 1E, independence, isolation, isolation device, raceway, separation | As Applied<br><br>This standard is applied to the design of the RICS, ESFs, and other instrumentation SSCs that are identified as SR for the RPF. It describes the minimum criteria for separation and independence of systems in a physical way. It does not describe what systems are to be separate and independent, only a means to do so.<br><br>Means of Compliance<br><br>For any SR function identified in Section 6b or 13b, the design conforms to the practices detailed in the standard.<br><br>Exception<br><br>The SHINE facility is not a nuclear power reactor and does not have all of the systems detailed in this standard. The intent of this standard is followed. |

**Table 7b.2-1 Design Criteria for the RPF Instrumentation and Control System (Sheet 3 of 13)**

| Design Criteria as Cited with Summary Intent | Design Bases As Applied to SHINE |
|---|---|
| **IEEE Std 323-2003**<br><br>**IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations**<br><br>**Abstract:** The basic requirements for qualifying Class 1E equipment and interfaces that are to be used in nuclear power generating stations are described in this standard. The principles, methods, and procedures described are intended to be used for qualifying equipment, maintaining and extending qualification, and updating qualification, as required, if the equipment is modified. The qualification requirements in this standard, when met, demonstrate and document the ability of equipment to perform safety function(s) under applicable service conditions including design basis events, reducing the risk of common-cause equipment failure.<br><br>**Keywords:** age conditioning, aging, condition monitoring, design basis events, equipment qualification, harsh environment, margin, mild environment, qualification methods, qualified life, radiation, SR function, significant aging mechanism, test plan, test sequence, type testing | As Applied<br><br>This standard defines the methods for equipment qualification when it is desired to qualify equipment for the applications and the environments to which it may be exposed. This standard is generally utilized for qualification of Class 1E equipment located in harsh environments, and for certain post-accident monitoring equipment, but it may also be utilized for the qualification of equipment in mild environments.<br><br>Means of Compliance<br><br>For SR functions identified in Section 6b or 13b, the design conforms to the practices detailed in the standard for those systems determined to be Class 1E and located in harsh environment. This includes consideration of those SSCs that reside within the hot cells and process enclosures. Not all of the safety-related instrumented functions reside in hot cells or process enclosures. As an example, isolation dampers that reside in the hot cell with electrical components are scrutinized with this standard, but the controlling system RICS that resides outside the hot cell does not require the same level of exposure per the application of this standard. The standard is applied in a graded approach based on the location of the equipment. |

**Table 7b.2-1 Design Criteria for the RPF Instrumentation and Control System (Sheet 4 of 13)**

| Design Criteria as Cited with Summary Intent | Design Bases As Applied to SHINE |
|---|---|
| **IEEE Std 344-2004**<br><br>**IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations**<br><br>**Abstract:** Recommended practices are provided for establishing procedures that will yield data to demonstrate that the Class 1E equipment can meet its performance requirements during and/or following one safe shutdown earthquake event preceded by a number of operating basis earthquake events. This recommended practice may be used to establish tests, analyses, or experienced based evaluations that will yield data to demonstrate Class 1E equipment performance claims or to evaluate and verify performance of devices and assemblies as part of an overall qualification effort. Common methods currently in use for seismic qualification by test are presented. Two approaches to seismic analysis are described, one based on dynamic analysis and the other on static coefficient analysis. Two approaches to experienced-based seismic evaluation are described, one based on earthquake experience and the other based on test experience.<br><br>**Keywords:** Class 1E, earthquake, earthquake experience, equipment qualification, inclusion rules, nuclear, operating basis earthquake, prohibited features, qualification methods, required response spectrum, response spectra, safe shutdown earthquake, safety function, seismic, seismic analysis, test response spectrum, test experience | As Applied and Means of Compliance<br><br>This standard is used in the design of the RICS, ESFs, and other instrumentation SSCs that are identified as a Class 1E system for the RPF. It describes seismic design requirements for equipment used in Class 1E systems. It does not describe what systems are to be determined as Class 1E systems. |

**Table 7b.2-1 Design Criteria for the RPF Instrumentation and Control System (Sheet 5 of 13)**

| Design Criteria as Cited with Summary Intent | Design Bases As Applied to SHINE |
|---|---|
| **IEEE Std 338-2012**<br><br>**IEEE Standard for Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems**<br><br>**Abstract:** The standard provides criteria for the performance of periodic surveillance testing of nuclear power generating station safety systems. The scope of periodic surveillance testing consists of functional tests and checks, calibration verification, and time response measurements, as required, to verify that the safety system performs its defined safety function. Post-maintenance and post-modification testing are not covered by this document. This standard amplifies the periodic surveillance testing requirements of other nuclear safety-related IEEE standards.<br><br>**Keywords:** functional tests, IEEE 338, periodic testing, risk-informed testing, surveillance testing | As Applied<br><br>This standard is applied to the design of the RICS, ESFs, and other instrumentation SSCs that are identified as SR for the RPF. It describes the methods and criteria for establishing a periodic surveillance program. It does not describe what systems are to be separate and independent, only a means to do so.<br><br>Means of Compliance<br><br>For SR functions identified in Section 6b or 13b, the design conforms to the practices detailed in the standard. |
| **IEEE Std 497-2010**<br><br>**IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations**<br><br>**Abstract:** Criteria are established in this standard for variable selection, performance, design, and qualification of accident monitoring instrumentation, and include requirements for display alternatives for accident monitoring instrumentation, documentation of design bases, and use of portable instrumentation.<br><br>**Keywords:** accident monitoring, display criteria, selection criteria, type variables | As Applied<br><br>The purpose of this standard is to establish selection, design, performance, qualification, and display criteria for accident monitoring instrumentation. It provides guidance on the use of portable instrumentation and examples of accident monitoring display configurations.<br><br>Means of Compliance<br><br>For those monitoring functions determined to be required for the health and safety of public or workers during normal operation and for DBAs, the design conforms to the practices detailed in the standard. |

**Table 7b.2-1 Design Criteria for the RPF Instrumentation and Control System (Sheet 6 of 13)**

| Design Criteria as Cited with Summary Intent | Design Bases As Applied to SHINE |
|---|---|
| **IEEE Std 7-4.3.2-2010**<br><br>**IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations**<br><br>**Abstract:** Additional computer specific requirements to supplement the criteria and requirements of IEEE Std 603™-2009 are specified. Within the context of this standard, the term computer is a system that includes computer hardware, software, firmware, and interfaces. The criteria contained herein, in conjunction with criteria in IEEE Std 603-2009, establish minimum functional and design requirements for computers used as components of a safety system.<br><br>**Keywords:** commercial grade item, diversity, safety systems, software, software tools, software verification and validation | As Applied<br><br>The purpose of this standard, in conjunction with criteria in IEEE Std 603-2009, establishes minimum functional and design requirements for computers used as components of a safety system. The RICS is designed as a DCS and this standard is applied to system development, specifically software development. This standard also discusses CGD and the method for successfully implementing the CGD approach.<br><br>Means of Compliance<br><br>The RICS software is developed utilizing this standard. |

**Table 7b.2-1 Design Criteria for the RPF Instrumentation and Control System (Sheet 7 of 13)**

| Design Criteria as Cited with Summary Intent | Design Bases As Applied to SHINE |
|---|---|
| **IEEE Std 828-2012**<br><br>**IEEE Standard for Configuration Management in Systems and Software Engineering**<br><br>**Abstract:** This standard establishes the minimum requirements for processes for Configuration Management (CM) in systems and software engineering. The application of this standard applies to any form, class, or type of software or system. This revision of the standard expands the previous version to explain CM, including identifying and acquiring configuration items, controlling changes, reporting the status of configuration items, as well as software builds and release engineering. Its predecessor defined only the contents of a software configuration management plan. This standard addresses what CM activities are to be done, when they are to happen in the life cycle, and what planning and resources are required. It also describes the content areas for a CM Plan. The standard supports ISO/IEC/IEEE 12207:2008 and ISO/IEC/IEEE 15288:2008 and adheres to the terminology in ISO/IEC/IEEE Std 24765 and the information item requirements of IEEE Std 15939.<br><br>**Keywords:** change control, configuration accounting, configuration audit, configuration item, IEEE 828, release engineering, software builds, software configuration management, system configuration management | As Applied<br><br>This standard describes configuration management processes to be established, how they are to be accomplished, who is responsible for doing specific activities, when they are to happen, and what specific resources are required. The RICS is designed as a DCS, the RICS has SR functions, and this standard applies to system development, specifically software development.<br><br>Means of Compliance<br><br>The RICS software is developed utilizing this standard for safety function implementation. |

**Table 7b.2-1 Design Criteria for the RPF Instrumentation and Control System (Sheet 8 of 13)**

| Design Criteria as Cited with Summary Intent | Design Bases As Applied to SHINE |
|---|---|
| **IEEE Std 1028-2008**<br><br>**IEEE Standard for Software Reviews and Audits**<br><br>**Abstract:** Five types of software reviews and audits, together with procedures required for the execution of each type, are defined in this standard. This standard is concerned only with the reviews and audits; procedures for determining the necessity of a review or audit are not defined, and the disposition of the results of the review or audit is not specified. Types included are management reviews, technical reviews, inspections, walk-throughs, and audits.<br><br>**Keywords:** audit, inspection, review, walk-through | As Applied<br><br>This standard provides minimum acceptable requirements for systematic software reviews. This standard describes organizational means for doing a review and documenting the findings. The RICS is designed as a DCS, the RICS has SR functions, and this recommended standard applies to the development of the software for those systems.<br><br>Means of Compliance<br><br>The RICS is developed utilizing this standard. |
| **ANS-10.4-2008**<br><br>**Verification and validation of non-safety-related scientific and engineering computer programs for the nuclear industry**<br><br>**Abstract:** This standard provides guidelines for the V&V of non-safety related scientific and engineering computer programs developed for use by the nuclear industry. The scope is restricted to research and other non-safety-related, noncritical applications.<br><br>**Keywords:** software integrity level, software life cycle, V&V, validation, verification | As Applied<br><br>The purpose of software V&V is to help the development organization build quality into the software during the software life cycle. This standard describes a means to verify and validate the software development for the nonsafety-related systems. It is utilized for software development in the SHINE facility that is not safety significant, i.e. not safety-related.<br><br>Means of Compliance<br><br>Nonsafety-related software is developed utilizing this standard. |
| **ISA 67.04.01-2006**<br><br>**Setpoints for Nuclear Safety-Related Instrumentation**<br><br>**Abstract:** This standard defines the requirements for assessing, establishing, and maintaining nuclear SR and other important instrument setpoints associated with nuclear power plants or nuclear reactor facilities.<br><br>**Keywords:** Setpoint, drift, analog channel, reliability analysis | As Applied<br><br>This standard is applied to the design of the RICS and other instrumentation SSCs that are identified as SR for the SHINE facility. It describes the methods and criteria for establishing setpoints utilized in safety systems and maintaining the documentation thereafter.<br><br>Means of Compliance<br><br>For SR functions identified in Section 6b or 13b that is designed with inherent setpoints, the design conforms to the practices detailed in the standard. |

**Table 7b.2-1 Design Criteria for the RPF Instrumentation and Control System (Sheet 9 of 13)**

| Design Criteria as Cited with Summary Intent | Design Bases As Applied to SHINE |
|---|---|
| **ISA 84.00.01-2004 Part 1**<br><br>**Functional Safety: Safety Instrumented Systems for the Process Industry Sector - Part 1: Framework, Definitions, System, Hardware and Software Requirements**<br><br>**Abstract:** This International Standard gives requirements for the specification, design, installation, operation and maintenance of a safety instrumented system, so that it can be confidently entrusted to place and/or maintain the process in a safe state. This standard has been developed as a process sector implementation of IEC 61508.<br><br>**Keywords:** Safety Instrumented System, Safety Integrated Level, Safety Instrumented Function, SIS, SIL, SIF | As Applied<br><br>This standard can be applied to the design of safety systems for the SHINE facility, but was specifically developed for the Industrial Process Sector. The standard is made up of three parts. Part 1 lays the ground work for the safety life cycle, overall structure of safety systems, definitions utilized, and an approach to implementing safety system design engineering. The physical hardware of the RICS is a product of design based on this standard and IEC 61508. Any SR function required to be implemented by the RICS are evaluated utilizing the Part 1, 2, and 3 of this standard. The intent is to have the same reliability and risk reduction demonstrated utilizing systems in the RICS that are more readily available from the process industry, but having the same or higher documented and tested ability to reduce risk as fulfillment through other channels.<br><br>Means of Compliance<br><br>For the SR functions required of the RICS, this standard is utilized for the design and implementation. |
| **ISA 84.00.01-2004 Part 2**<br><br>**Functional Safety: Safety Instrumented Systems for the Process Industry Sector - Part 2: Guidelines for the Application of ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod) – Informative**<br><br>**Abstract:** This International Standard gives requirements for the specification, design, installation, operation and maintenance of a safety instrumented system, so that it can be confidently entrusted to place and/or maintain the process in a safe state. This standard has been developed as a process sector implementation of IEC 61508.<br><br>**Keywords:** Safety Instrumented System, Safety Integrated Level, Safety Instrumented Function, SIS, SIL, SIF | As Applied<br><br>This standard can be applied to the design of safety systems for the SHINE facility, but was specifically developed for the Industrial Process Sector. The standard is made up of three parts. Part 2 provides guidance on the specification, design, installation, operation and maintenance of safety instrumented functions and related safety instrumented systems as defined in ISA 84.00.01, Part 1. SR functions required to be implemented by the RICS are evaluated utilizing the Part 1, 2, and 3 of this standard. The intent is to have the same reliability and risk reduction demonstrated utilizing systems in the RICS that are more readily available from the process industry, but having the same or higher documented and tested ability to reduce risk as fulfillment through other channels.<br><br>Means of Compliance<br><br>For SR functions that are required of the RICS, this standard is utilized for the design and implementation. |

**Table 7b.2-1 Design Criteria for the RPF Instrumentation and Control System (Sheet 10 of 13)**

| Design Criteria as Cited with Summary Intent | Design Bases As Applied to SHINE |
|---|---|
| **ISA 84.00.01-2004 Part 3**<br><br>**Functional Safety: Safety Instrumented Systems for the Process Industry Sector - Part 3: Guidance for the Determination of the Required Safety Integrity Levels – Informative**<br><br>**Abstract:** This International Standard gives requirements for the specification, design, installation, operation and maintenance of a safety instrumented system, so that it can be confidently entrusted to place and/or maintain the process in a safe state. This standard has been developed as a process sector implementation of IEC 61508.<br><br>**Keywords:** Safety Instrumented System, Safety Integrated Level, Safety Instrumented Function, SIS, SIL, SIF | As Applied<br><br>This standard can be applied to the design of safety systems for the SHINE facility, but was specifically developed for the Industrial Process Sector. The standard is made up of three parts. Part 3 provides information on:<br>• The underlying concepts of risk, the relationship of risk to safety integrity.<br>• The determination of tolerable risk.<br>• A number of different methods that enable the safety integrity levels for the safety functions to be determined.<br><br>SR functions required to be implemented by the RICS are evaluated utilizing the Part 1, 2, and 3 of this standard. The intent is to have the same reliability and risk reduction demonstrated utilizing systems in the RICS that are more readily available from the process industry, but having the same or higher documented and tested ability to reduce risk as fulfillment through other channels.<br><br>Means of Compliance<br><br>For SR functions that are required of the RICS, this standard is utilized for the design and implementation. |

**Table 7b.2-1 Design Criteria for the RPF Instrumentation and Control System (Sheet 11 of 13)**

| Design Criteria as Cited with Summary Intent | Design Bases As Applied to SHINE |
|---|---|
| **NUREG-0700, Rev. 2**<br><br>**Human-System Interface Design Review Guidelines**<br><br>**Abstract:** NRC staff reviews the HFE aspects of nuclear power plants in accordance with the Standard Review Plan (NUREG-0800). Detailed design review procedures are provided in the HFE Program Review Model (NUREG-0711). As part of the review process, the interfaces between plant personnel and plant's systems and components are evaluated for conformance with HFE guidelines. This document, Human-System Interface Design Review Guidelines (NUREG-0700, Revision 2), provides the guidelines necessary to perform this evaluation.<br><br>**Keywords:** Display, HMI, Human Interface System (HIS), Human-System Interface | As Applied<br><br>This comprehensive design review guide concentrates on displayed information utilized in human-interface systems. This is a sub-set of HFE, dedicated to providing informative and effective designs that assist an operator in the performance of their duties.<br><br>Means of Compliance<br><br>The RICS has its information provided to operators in a display format. This document is utilized and reviewed for the development of displays that an operator uses in connection with the RICS. |
| **NUREG/CR-6463**<br><br>**Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems**<br><br>**Abstract:** This report provides guidance to the NRC on auditing of programs for safety systems written in the following six high level languages: Ada, C and C++, PLC Ladder Logic, Sequential Function Charts, Pascal, and PL/M. It could also be used by those developing safety significant software as a basis for project-specific programming guidelines.<br><br>**Keywords:** Pascal, C, Ladder Logic, PL/M, Ada, C++, PLC, Programming, Sequential Function Charts | As Applied<br><br>The goal of this report is to provide guidance to the NRC for reviewing high-integrity software in nuclear power plants. Thus the focus of the report is on implementation (i.e., programming). It is a discussion of what constitutes good practices and cites examples of previously installed systems. The RICS is a DCS and has associated programming developed for the SHINE facility. For those programming languages identified in this report, the guideline serves as suitable means to review the programming code.<br><br>Means of Compliance<br><br>The RICS has software programs developed. This document provides review guidance of any programming code for which the report was developed. |

**Table 7b.2-1 Design Criteria for the RPF Instrumentation and Control System (Sheet 12 of 13)**

| Design Criteria as Cited with Summary Intent | Design Bases As Applied to SHINE |
|---|---|
| **NUREG/CR-6090**<br>**The Programmable Logic Controller and Its Application in Nuclear Reactor Systems**<br>**Abstract:** The purpose of this document is to outline recommendations for guidance for the review of application of PLCs to the control; monitoring and protection of nuclear reactors.<br>**Keywords:** PLC, Programming, Protection Systems | As Applied<br>The goal of this report is to provide guidance to the NRC for implementing PLCs in the nuclear reactor power industry. It provides a complete background to a selection process for hardware, failure analysis, as well as discussion of product life cycle within the power plant. It forms a good discussion of what constitutes good practices and cites examples of previously installed systems. The RICS is a DCS and PLC-type system and is developed for the SHINE facility.<br>Means of Compliance<br>The RICS utilizes a PLC-type DCS. This document provides guidance for selection design and implementation of this type of control. It is utilized for implementing the PLC design. |
| **EPRI TR-106439, 1996**<br>**Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications**<br>**Abstract:** This guideline describes a consistent, comprehensive approach for the evaluation and acceptance of commercial digital equipment for nuclear safety systems.<br>**Keywords:** COTS, Programming, Software, Commercial Grade Dedication | As Applied<br>The approach emphasizes identification of appropriate critical characteristics with subsequent verification through testing, analysis, vendor assessments and careful review of operating experience. This guide is not intended to be a new standard; it references existing industry standards and guidelines as appropriate. The guide is intended primarily for digital upgrades to safety-related systems, but it is also useful in nonsafety-related applications that require high reliability. The guidance is intended to be compatible with utility-specific change processes, including graded approaches for quality assurance.<br>Means of Compliance<br>The digital systems or components that require CGD utilizes this guideline. |
| **Regulatory Guide 1.152, Rev.3, 2011**<br>**Criteria for use of Computers in Safety Systems of Nuclear Power Plants**<br>**Abstract:** This regulatory guide describes a method that the NRC staff deems acceptable for complying with the Commission's regulations for promoting high functional reliability, design quality, and a secure development and operational environment (SDOE) for the use of digital computers in the safety systems of nuclear power plants.<br>**Keywords:** Secure Development and Operational Environment, SDOE, computers | As Applied<br>Instrumentation and control system designs that use computers in safety-related systems make extensive use of advanced technology (i.e., equipment and design practices). These designs are expected to be significantly and functionally different from current designs and may include the use of microprocessors, digital systems and displays, fiber optics, multiplexing, and different isolation techniques to achieve sufficient independence and redundancy.<br>Means of Compliance<br>The RICS and RICS HMI is developed utilizing this document. |

**Table 7b.2-1 Design Criteria for the RPF Instrumentation and Control System (Sheet 13 of 13)**

| Design Criteria as Cited with Summary Intent | Design Bases As Applied to SHINE |
|---|---|
| **Regulatory Guide 1.53, Rev.2, 2003**<br><br>**Application of the Single-Failure Criterion to Safety Systems**<br><br>**Abstract:** Provides methods acceptable to the NRC staff for satisfying the NRC's regulations with respect to the application of the single-failure criterion to the electrical power, instrumentation, and control portions of nuclear power plant safety systems.<br><br>**Keywords:** IEEE Std 379, Single-Failure Criterion | As Applied<br><br>The approach provides guidance for applying single-failure criterion to safety-related instrumentation and control systems. Some end-devices utilized by the RICS are identified as SR. These systems and components are evaluated via this regulatory guide.<br><br>Means of Compliance<br><br>The RICS, ESFs, and SR end-devices are evaluated with this document. |
| **Regulatory Guide 1.97, Rev.4, 2006**<br><br>**Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants**<br><br>**Abstract:** This regulatory guide to describe a method that the NRC staff considers acceptable for use in complying with the agency's regulations with respect to satisfying criteria for accident monitoring instrumentation in nuclear power plants.<br><br>**Keywords:** IEEE Std 497, accident monitoring | As Applied<br><br>The approach provides guidance for accident monitoring in the SHINE facility. These systems and components are evaluated via this regulatory guide.<br><br>Means of Compliance<br><br>The RICS, CAAS, CAMS, and RAMS are designed with the use of document. |
| **Regulatory Guide 5.71, 2010**<br><br>**Cyber Security Programs for Nuclear Facilities**<br><br>**Abstract:** This regulatory guide provides an approach that the NRC staff deems acceptable for complying with the Commission's regulations regarding the protection of digital computers, communications systems, and networks from a cyber attack as defined by 10 CFR 73.1.<br><br>**Keywords:** Cyber Security, 10 CFR 73.54(a)(2), design basis threat | As Applied<br><br>The approach provides guidance for accident monitoring in the SHINE facility. These systems and components are evaluated via this regulatory guide.<br><br>Means of Compliance<br><br>The RICS and RICS HMI are designed with the use of document. |

### 7b.2.3 SYSTEM DESCRIPTION

The RPF instrumentation and controls are composed of four basic blocks or systems: RICS, active ESFs, radiation monitoring systems, and operator interface displays and terminals. These systems provide an interface for the operator for monitoring and control. The RICS is a DCS that functions independently and is electrically isolated from other systems in the RCA. The RICS initiates active ESF mitigative responses and controls SR and non-safety components. The ESFs in the RPF provide isolation functionality. The RICS can isolate one or any combination of the isolable cells in the RPF. The RICS also initiates the ESF isolation between ventilation zones in the RCA. The radiation monitoring systems consist of the RAMS, CAMS, and the CAAS. The radiation monitoring is discussed in Section 7b.6. The base status of radiation monitoring is shown on the RICS display system.

#### 7b.2.3.1 RICS Description

The RICS utilizes a high integrity controller specified for use in a safety instrumented system for the process industry. The RICS is sectionalized into two parts. One section is dedicated to monitoring instruments that are SR. This same section provides the control action to initiate the active ESFs within the RPF. This platform forms the basis for the monitoring and control for SR SSCs and to activate the ESFs. The system utilizes dual redundancy with high self-diagnostic functionality for the internal design of subsystems within the controller system to meet the stringent demands.

The other section of the RICS supports the activities required to perform the various functional operational modes in the RPF.

#### 7b.2.3.2 Control Room

The RPF control room is integrated with the IF control room and described in Section 7a2.6.

##### 7b.2.3.2.1 Operator Interface Description

The operator has direct visualization of critical values and has the ability to input control functions to the RICS. The RICS dedicated displays perform the following functions:

a. Static display shows critical measurement values and performs the function of annunciator panel. This is a fixed display panel that does not provide any interactive control functionality.
b. Alarm / event annunciator display panel. This panel displays any event or alarm that is defined for the process. This display allows the operator to acknowledge current events and alarms, and forms the historical record for events.
c. Dynamic interface display panel or HMI. This panel allows the operator a means to perform tasks, change modes, enable/disable overrides, and essentially anything that requires an operator input to allow, perform, or modify a task or event.

The set of displays are arranged in a workstation group. This group comprises the displays and the keyboard/mouse that are utilized to interface with the system.

Figure 7b.2-1 shows the graphic representation of the display description above for the RPF. The screen development follows the design criteria in Section 7b.2.1 and design basis as defined in Section 7b.2.2.

There is one workstation that consists of the RICS and facility integrated control system (FICS) displays in the control room. The FICS is classified as nonsafety-related and provides monitoring and control for the facility systems including lighting, HVAC, specialty gas and compressed air distribution systems, water systems, power distribution, and facility communication systems.

Additionally, the IF workstations each have RICS display and interface sections to provide the operator the ability to monitor inter-facility processes. The RICS HMI systems are fully functional and have the capability to control the RPF systems in the case of an emergency. The RICS HMIs allow for usage simultaneously. Figure 7a2.6-1 shows the graphic representation of the display description described above for the IF.

#### 7b.2.3.2.2 Process Area

In addition to HMI systems in the control room, the RPF has operator interface terminals (OITs) located adjacent to the individual hot cell and glovebox systems. These systems communicate key parameters about each system to the operator such an internal temperature and differential pressure from the RICS. Alarms and ESF activations that occur for the individual hot cell are displayed on the OITs. For some locations, the OIT is utilized to setup and initiate inter-system process fluid transfers in the RPF. The OIT handles pump and flow controls where they are required.

### 7b.2.4 SYSTEM PERFORMANCE ANALYSIS

The RPF instrumentation and controls monitor the RPF processes and ESFs when required. The SR components are managed by the RICS. The RICS provides the central decision making processor that evaluates monitored parameter from various plant instrumentation as well as from the radiation monitoring systems of the CAMS, CAAS, and RAMS. The analysis herein discusses safety as it relates to the SR components design criteria and design basis.

Potential variables, conditions, or other items that will be probable subjects of technical specifications associated with the RPF instrumentation and control systems are provided in Chapter 14.

#### 7b.2.4.1 RPF Trip and Alarm Design Basis

The design basis information for the RICS trip functions are based on the following two requirements:

1) *Double contingency principle* means that process designs should incorporate sufficient factors of safety to require at least two unlikely, independent, and concurrent changes in process conditions before a criticality accident is possible.

2) The safety program shall ensure that each SR SSC will be available and reliable to perform its intended safety function when needed.

The RICS trip and alarm annunciation are protective functions and are part of the overall protection and safety monitoring systems for the RPF. The specific equipment design basis for the instrumentation and equipment used for the RICS trip and alarming functions are discussed in Section 7b.2.2.

The following discussion relates to the design bases utilized for monitoring specific signal values for RPF trips and alarms, the requirements of performance, the requirements for specific modes of operation of RPF and RICS and the design criteria documents generating the basis noted as a citation.

7b.2.4.1.1 Safety Functions and Corresponding Protective/Mitigative Actions for Design Basis Events

Citation - Section 4a and 4b of IEEE-603-2009

The results of the accident analysis for the RPF SSCs are discussed in Section 13b. Conditions that require monitoring and the subsequent action to be taken are detailed in Section 13b. SR components identified in Section 13b, including the ESFs described in 6b, are monitored and controlled by RICS, as required.

7b.2.4.1.2 Variable Monitored to Control Protective/Mitigative Action

Citation - Section 4d of IEEE-603-2009

The following variables are monitored for RPF trip for isolation:

- The hot cell fire detection and suppression system (HCFD) is monitored for actuation. If tripped, the hot cell is isolated by the ventilation inlet and outlet dampers. This is not a SR Function.
- The facility fire protection system (FFPS) is monitored for actuation. If tripped, the RCA confinement zone of the affected area is isolated by the zone bubble-tight dampers. This is not a SR function.
- Hot cell gamma detectors are monitored in the hot cell. If acceptable gamma levels are exceeded, the hot cell is isolated by the ventilation inlet and outlet bubble-tight dampers.

The following is a preliminary list of variables to be monitored in the RPF for alarming to eliminate or reduce the exposure for the operator. The final list of variables to be monitored will be provided in the FSAR.

- Hot cell temperature – internal environment.
- Hot cell pressure – internal environment.
- Uranyl nitrate conversion system (UNCS) outlet temperature – process upset.
- Radioactive drain system (RDS) sump level – contamination exposure.
- Primary vessel vent system (PVVS) pressure – internal environment.
- PVVS flow – internal environment.
- RCA confinement zone pressure – contamination exposure.

- RCA radiation levels (CAMS, RAMS, and CAAS) – contamination or direct radiation exposure.
- Process stream pH – process upset.
- Process stream radiation – process upset.
- Valve positions within the RPF – process upset.

Tasks for the RICS are discussed in Section 7b.3.

7b.2.4.1.3 Functional Degradation of Safety System Performance

Citation - Section 4h of IEEE-603-2009

This section of the IEEE-603 describes what constitutes system malfunctions for safety-related and nonsafety-related devices. The SR components are designed to consider those conditions having the potential for functional degradation in performance as described in Chapter 13.

The manual soft trip pushbuttons on the RICS HMI allow the operator to accomplish immediate isolation of the hot cells, shielded cells, or ventilation zones as they deem necessary.

Single channel failure is covered by redundant end measurement.

7b.2.4.2 Analysis

7b.2.4.2.1 RICS Trip Function Conformance to Applicable Criteria

The RICS performs a trip as a protective function as part of the RPF safety analysis. The design criteria for selection are discussed in Subsections 7b.2.1 and 7b.2.2. The following discussions relate to conformance to criteria for the RICS trip function.

7b.2.4.2.2 General Functional Requirement Conformance

Citation - Section 5 of IEEE-603-2009, GDC-13, GDC-20

The RICS initiates and controls the ESF activation and isolation when the system detects an off-normal event appropriate for activation. RICS trips are discussed in Section 7b.4. These monitored values and subsequent trips are a result of the preliminary accident analysis in Section 13b and provide a means to mitigate or reduce the consequences from the DBA to acceptable levels.

7b.2.4.2.3 Single Failure Criterion Conformance

Citation - Section 5.1 of IEEE-603-2009, IEEE-379-2000

A postulated active single failure in the RICS or SR SSCs does not prevent the RICS from performing its protective action. This is accomplished by utilizing redundant measurement devices, and having systems design based on single failure criteria. The design criteria are discussed in Subsection 7b.2.1.

7b.2.4.2.4 Requirements on Bypassing Trip Functions Conformance

Citation - Section 5.8, 5.9, 6.6, 6.7 of IEEE-603-2009

Trip override/bypass is recognized as a design requirement. Channel bypass is allowed based on the nature of the signal. No channel bypass is allowed without a visual indication on the RICS display and recording the bypass event in the historical logging.

Periodic surveillance testing shall be governed by IEEE-338-2012.

7b.2.4.2.5 Requirements on Setpoint Determination and Multiple Setpoint Conformance

Citation - Section 6.8 of IEEE-603-2009

Table 7b.2-1 discusses the criteria to be utilized for setpoint derivation. Setpoints will be calculated in accordance with ISA RP-67.04.02.

7b.2.4.2.6 Requirements for Completion of Trip Conformance

Citation - Section 5.2 of IEEE-603-2009

The discussion of the ESF and the interaction of a mitigative action going to completion are provided in the design. The RICS monitors for a complete trip of the ESF, which includes the closure of ventilation bubble-tight dampers. Each damper is equipped with safety-related position sensors to determine full-closed position. This information is available on the operator display for the RICS and at the local OITs near the hot cell. This is an alarm/event annunciation event displayed to the operator.

Subsection 7b.4.1 discusses the activation of the ESF by the RICS.

Subsection 7b.4.1.1 discusses the alarm/event strategy.

Subsections 7b.4.1.1.4 and 7b.4.1.1.5 discuss the operator requirement to manually reset after a trip.

7b.2.4.2.7 Requirements for Manual control of Trip Conformance

Citation - Section 6.2 of IEEE-603-2009

The RICS has the ability to perform a manual activation of the ESF. Subsection 7b.4.1.1.13 discusses the activation of the ESFs in RPF.

Section 7b.4.1.1 discusses the alarm/event strategy.

Subsections 7b.4.1.1.4 and 7b.4.1.1.5 discuss the operator requirement to manually reset after a trip.

### 7b.2.5 CONCLUSION

The instrumentation and controls for the RPF meet the stated design criteria and design basis requirements outlined in NUREG-1537. A matrix of the instrumentation and controls subsystems along with a cross reference to specific design criteria is presented in Table 7b.2-2.

**Table 7b.2-2 RPF Verification Matrix Design Criteria, Bases, Description (Sheet 1 of 7)**

| Verification Matrix | Design Criterion | Design Basis Applicability | Detailed Section Reference | Functional Means |
|---|---|---|---|---|
| 1 | IEEE-379<br>Single Failure Criterion | 1) RICS<br>2) ESFs<br>3) RICS display<br>4) RICS SR end devices<br>5) ESFs manual isolation | 1) 7b.2.3<br>2) 7b.4<br>3) 7b.5<br>4) 7b.4<br>5) 7b.4 | 1) Safety DCS pre-approved platform for SIS<br>2) Redundant independent isolation components<br>3) Redundant operator interface workstations<br>4) Redundant sensor<br>5) Alternative manual means for ESF initiation |
| 2 | IEEE-577<br>Reliability Analysis Criterion | 1) RICS<br>2) ESFs<br>3) RICS display<br>4) RICS SR end devices<br>5) ESFs manual isolation | 1) 7b.2.3<br>2) 7b.4<br>3) 7b.5<br>4) 7b.4<br>5) 7b.4 | 1) Safety DCS pre-approved platform for SIS<br>2) Redundant independent isolation components<br>3) Redundant operator interface workstations<br>4) Redundant sensor<br>5) Alternative manual means for ESF initiation |
| 3 | IEEE-603<br>Standard Criteria Safety Systems | 1) RICS<br>2) ESFs<br>3) RICS display<br>4) RICS SR end devices<br>5) ESFs manual isolation | 1) 7b.2.3<br>2) 7b.4<br>3) 7b.5<br>4) 7b.4<br>5) 7b.4 | Subsection 7b.2.4 for detailed discussion |
| 4 | IEEE-384<br>Independence of Class 1E Equipment & Circuits | 1) RICS<br>2) ESFs<br>3) RICS display<br>4) RICS SR end devices<br>5) ESFs manual isolation | 1) 7b.2.3<br>2) 7b.4<br>3) 7b.5<br>4) 7b.4<br>5) 7b.4 | For preliminary design, the independence of equipment is sufficient to meet IEEE-603 and IEEE-379. |
| 5 | IEEE-323<br>Qualifying Class 1E Equipment | 1) RICS<br>2) ESFs<br>3) RICS display<br>4) RICS SR end devices<br>5) ESFs manual isolation | 1) 7b.2.3<br>2) 7b.4<br>3) 7b.5<br>4) 7b.4<br>5) 7b.4 | This standard is for selecting and qualifying equipment. RICS, ESFs, and selected SR end devices are required to be qualified for Class 1E use. |
| 6 | IEEE-344<br>Recommended Practice for Seismic Qualification | 1) RICS<br>2) ESFs<br>3) RICS display<br>4) RICS SR end devices<br>5) ESFs manual isolation | 1) 7b.2.3<br>2) 7b.4<br>3) 7b.5<br>4) 7b.4<br>5) 7b.4 | This standard is for selecting and qualifying equipment. RICS, ESFs, and selected SR end devices are required to be qualified for Class 1E use. |
| 7 | IEEE-338<br>Criteria for the Periodic Surveillance Testing of Safety Systems | 1) RICS<br>2) ESFs<br>3) RICS display<br>4) RICS SR end devices<br>5) ESFs manual isolation | 1) 7b.2.3<br>2) 7b.4<br>3) 7b.5<br>4) 7b.4<br>5) 7b.4 | This standard is for selecting equipment, general design criteria that must be considered during design. |

**Table 7b.2-2 RPF Verification Matrix Design Criteria, Bases, Description (Sheet 2 of 7)**

| Verification Matrix | Design Criterion | Design Basis Applicability | Detailed Section Reference | Functional Means |
|---|---|---|---|---|
| 8 | IEEE-497<br>Criteria for Accident Monitoring Instruments | 1) RICS<br>2) ESFs<br>3) RICS display<br>4) RICS SR end devices<br>5) CAAS<br>6) RAMS<br>7) CAMS | 1) 7b.2.3<br>2) 7b.4<br>3) 7b.5<br>4) 7b.4<br>5) 7b.6<br>6) 7b.6<br>7) 7b.6 | This standard is for selecting accident monitoring equipment (specifically target towards radiation monitoring and annunciation), general design criteria that must be considered during design. |
| 9 | IEEE-7.4.3.2<br>Criteria for Digital Computers in Safety Systems | 1) RICS<br>2) RICS display<br>3) OIT displays | 1) 7b.2.3<br>2) 7b.5<br>3) 7b.5 | Programming software for the RICS must follow the criteria. Programming must comply with the Software Quality Assurance Plan developed as part of the commitment to the Design Criteria outlined herein and in this standard.<br><br>The software and hardware utilized for the displays for the RICS and the OIT must also follow the guidelines set forth in this standard. The equipment selected to date and the path forward allow for a successful completion following IEEE-7.4.3.2. |
| 10 | IEEE-828<br>Configuration Management in Systems and Software Engineering | 1) RICS<br>2) RICS display<br>3) OIT displays | 1) 7b.2.3<br>2) 7b.5<br>3) 7b.5 | Part of the overall SQAP commitment of IEEE 7-4.3.2. |
| 11 | IEEE-829<br>Software and System Test Documentation | 1) RICS<br>2) RICS display<br>3) OIT displays | 1) 7b.2.3<br>2) 7b.5<br>3) 7b.5 | Part of the overall SQAP commitment of IEEE 7-4.3.2. |
| 12 | IEEE-1012<br>Criteria for Software Verification and Validation | 1) RICS<br>2) RICS display<br>3) OIT displays | 1) 7b.2.3<br>2) 7b.5<br>3) 7b.5 | Part of the overall SQAP commitment of IEEE 7-4.3.2. |
| 13 | IEEE-1028<br>Software Reviews and Audits | 1) RICS<br>2) RICS display<br>3) OIT displays | 1) 7b.2.3<br>2) 7b.5<br>3) 7b.5 | Part of the overall SQAP commitment of IEEE 7-4.3.2. |
| 14 | ANS-10.4<br>Verification and Validation for non-safety software | 1) RICS<br>2) RICS display<br>3) OIT displays | 1) 7b.2.3<br>2) 7b.5<br>3) 7b.5 | Part of the overall SQAP commitment of IEEE 7-4.3.2. |
| 15 | ISA 67.04.01<br>Setpoints for Nuclear Safety-Related Instruments | 1) RICS<br>2) RICS SR end devices | 1) 7b.2.3<br>2) 7b.4 | Part of the overall design commitment. |

**Table 7b.2-2 RPF Verification Matrix Design Criteria, Bases, Description (Sheet 3 of 7)**

| Verification Matrix | Design Criterion | Design Basis Applicability | Detailed Section Reference | Functional Means |
|---|---|---|---|---|
| 16 | ISA 84.00.01, Part 1,2,&3 Functional Safety: Safety Instrumented Systems for the Process Industry Sector | 1) RICS<br>2) RICS display<br>3) OIT displays | 1) 7b.2.3<br>2) 7b.5<br>3) 7b.5 | This standard is utilized to design and develop the nonsafety-related systems as it relies on safety, reliability, and functionality. |
| 17 | NUREG-0700, Rev. 2 Human-System Interface Design Review Guidelines | 1) RICS<br>2) RICS display<br>3) OIT displays | 1) 7b.2.3<br>2) 7b.5<br>3) 7b.5 | This standard is utilized to design and develop the safety-related and nonsafety-related systems as it pertains to control room arrangement, screen developments, and Operator Interface. |
| 18 | NUREG/CR-6463 Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems | 1) RICS | 1) 7b.2.3 | This guideline is utilized to design, develop, and review the safety-related software. |
| 19 | NUREG/CR-6090 PLC and applications in Nuclear Reactor Systems | 1) RICS | 1) 7b.2.3 | This guideline is utilized to design, develop, and review the safety-related and nonsafety-related software. |
| 20 | EPRI TR-106439, Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications | 1) RICS display<br>2) OIT display | 1) 7b.5<br>2) 7b.5 | This standard is utilized to design and develop the safety-related systems as it pertains to obtaining software / hardware for the RICS, operator interface displays, and data acquisition systems. |
| 21 | Reg Guide 1.152 Criteria for use of Computers in Safety Systems | 1) RICS<br>2) RICS display<br>3) OIT display | 1) 7b.2.3<br>2) 7b.5<br>3) 7b.5 | 1) Redundant safety PLC platform<br>2) RICS redundant HMI workstations<br>3) Operator interface workstations |
| 22 | Reg Guide 1.53 Single Failure Criterion Evaluation for Safety Systems | 1) RICS<br>2) ESFs<br>3) RICS display<br>4) RICS SR end devices<br>5) ESFs manual isolation | 1) 7b.2.3<br>2) 7b.4<br>3) 7b.5<br>4) 7b.4<br>5) 7b.4 | 1) High integrity safety PLC<br>2) Redundant channels for ESFs<br>3) Redundant operator interface workstations<br>4) Redundant sensor<br>5) Alternative manual means for ESFs initiation |

**Table 7b.2-2 RPF Verification Matrix Design Criteria, Bases, Description (Sheet 4 of 7)**

| Verification Matrix | Design Criterion | Design Basis Applicability | Detailed Section Reference | Functional Means |
|---|---|---|---|---|
| 23 | Reg Guide 5.71<br>Cyber Security Programs for Nuclear Facilities | 1) RICS<br>2) RICS display<br>3) OIT display | 1) 7b.2.3<br>2) 7b.5<br>3) 7b.5 | Requires design approach and implementation. |
| 24 | 10CFR 50, Appendix A, GDC 2<br>Natural Phenomena | 1) ESFs manual operator isolation<br>2) RICS manual soft trip | 1) 7b.4<br>2) 7b.2.4 | This criterion defines that safety-related systems are designed to handle natural phenomena. RICS is capable of performing its safety functions during and after the external events described in Chapter 13. The RICS has the ability for the operator to manually choose to isolate and trip the EFFs in the RPF should external events dictate. |
| 25 | 10CFR 50, Appendix A, GDC 4<br>Environmental and dynamic effects design bases. | 1) RICS<br>2) ESFs<br>3) RICS display<br>4) RICS SR end devices<br>5) CAAS<br>6) RAMS<br>7) CAMS | 1) 7b.2.3<br>2) 7b.4<br>3) 7b.5<br>4) 7b.4<br>5) 7b.6<br>6) 7b.6<br>7) 7b.6 | This criterion is met by choosing qualified equipment, testing, and surveillance. The criteria are described in Subsections 7b.2.1 and 7b.2.2. |
| 26 | 10CFR 50, Appendix A, GDC 5<br>Sharing of structures, systems, and components | 1) RICS<br>2) ESFs<br>3) RICS display<br>4) RICS SR end devices<br>5) CAAS<br>6) RAMS<br>7) CAMS | 1) 7b.2.3<br>2) 7b.4<br>3) 7b.5<br>4) 7b.4<br>5) 7b.6<br>6) 7b.6<br>7) 7b.6 | This criterion is met by having independent redundant systems with defense-in-depth. The basis of design addresses this in Subsections 7b.2.1, 7b.2.2, and 7b.2.3. This effort is completed in detailed design. |
| 27 | 10CFR 50, Appendix A, GDC 10<br>Reactor design | N/A | N/A | This criterion is addressed with having the RCS controlling the process steps of the reactivity process and the RPS as a separate independent system monitoring for off-normal events. This criterion does not apply to the SHINE RPF. |
| 28 | 10CFR 50, Appendix A, GDC 12<br>Suppression of reactor power oscillations | N/A | N/A | This criterion is addressed to traditional BWR or PWR reactor systems. This criterion does not apply to the SHINE RPF. |
| 29 | 10CFR 50, Appendix A, GDC 13<br>Instrumentation and control | 1) RICS<br>2) ESFs<br>3) RICS display<br>4) RICS SR end devices<br>5) CAAS<br>6) RAMS<br>7) CAMS | 1) 7b.2.3<br>2) 7b.4<br>3) 7b.5<br>4) 7b.4<br>5) 7b.6<br>6) 7b.6<br>7) 7b.6 | This criterion directly addresses the instrument and controls. The ICS instrumentation and controls provide control, protection, and means to safely mitigate the identified events described in Section 13b. |

**Table 7b.2-2 RPF Verification Matrix Design Criteria, Bases, Description (Sheet 5 of 7)**

| Verification Matrix | Design Criterion | Design Basis Applicability | Detailed Section Reference | Functional Means |
|---|---|---|---|---|
| 30 | 10CFR 50, Appendix A, GDC 15 Reactor coolant system design | N/A | N/A | This criterion directly addresses the coolant system. This criterion does not apply to the SHINE RPF. |
| 31 | 10CFR 50, Appendix A, GDC 16 Containment design | 1) RICS<br>2) ESFs<br>3) RICS display<br>4) RICS SR end devices<br>5) CAAS<br>6) RAMS<br>7) CAMS | 1) 7b.2.3<br>2) 7b.4<br>3) 7b.5<br>4) 7b.4<br>5) 7b.6<br>6) 7b.6<br>7) 7b.6 | This criterion directly addresses the containment system. The SHINE facility does not have containment, but has confinement per NUREG-1537 definitions. The RICS provides monitoring of radioactivity and fire in the cell and hot cell ventilation. In the event there is measured radioactivity in excess of predetermined values, the RICS isolates the process system. |
| 32 | 10CFR 50, Appendix A, GDC 17 Electric Power Systems | 1) RICS<br>2) ESFs<br>3) RICS display<br>4) RICS SR end devices<br>5) CAAS<br>6) RAMS<br>7) CAMS | 1) 7b.2.3<br>2) 7b.4<br>3) 7b.5<br>4) 7b.4<br>5) 7b.6<br>6) 7b.6<br>7) 7b.6 | This criterion directly addresses the electric power system. The RICS and active ESFs are designed to fail-safe with loss of off-site power. Upon loss of off-site power, the de-energized state for the ESFs is the safe-state. There is a safety-related UPSS that provides power upon loss of off-site power that allows for monitoring. |
| 33 | 10CFR 50, Appendix A, GDC 19 Control Room | 1) RICS<br>2) ESFs<br>3) RICS display<br>4) RICS SR end devices<br>5) CAAS<br>6) RAMS<br>7) CAMS | 1) 7b.2.3<br>2) 7b.4<br>3) 7b.5<br>4) 7b.4<br>5) 7b.6<br>6) 7b.6<br>7) 7b.6 | This criterion directly addresses the control room for the facility. The RICS provides control, protection, and means to safely mitigate the identified events described in Section 13b from the control room. It affords the ability to have a manual initiated isolation for the operator. |
| 34 | 10CFR 50, Appendix A, GDC 20 Protection system functions | 1) RICS<br>2) ESFs<br>3) RICS display<br>4) RICS SR end devices<br>5) CAAS<br>6) RAMS<br>7) CAMS | 1) 7b.2.3<br>2) 7b.4<br>3) 7b.5<br>4) 7b.4<br>5) 7b.6<br>6) 7b.6<br>7) 7b.6 | This criterion directly addresses the protection systems for the facility. The RICS provides protection as the initiator for ESF mitigative isolation of the systems in the RPF. The RICS automatically initiates a protective action upon appropriate signal which safely mitigates the identified events described in Section 13b. The RICS and the ESFs include the ability to have a manual initiated isolation from the operator. |

**Table 7b.2-2 RPF Verification Matrix Design Criteria, Bases, Description (Sheet 6 of 7)**

| Verification Matrix | Design Criterion | Design Basis Applicability | Detailed Section Reference | Functional Means |
|---|---|---|---|---|
| 35 | 10CFR 50, Appendix A, GDC 21 Protection system reliability and testability | 1) RICS<br>2) ESFs<br>3) RICS display<br>4) RICS SR end devices<br>5) CAAS<br>6) RAMS<br>7) CAMS | 1) 7b.2.3<br>2) 7b.4<br>3) 7b.5<br>4) 7b.4<br>5) 7b.6<br>6) 7b.6<br>7) 7b.6 | This criterion directly addresses the protection systems and the ability to tolerate single failures of components and the requirement for online surveillance of channels used for safety. The system is presently designed as dual sensing for the SR functions. For the RICS, periodic surveillance will be performed to verify the safety functions can be performed. |
| 36 | 10CFR 50, Appendix A, GDC 22 Protection system independence | 1) RICS<br>2) ESFs<br>3) RICS display<br>4) RICS SR end devices<br>5) CAAS<br>6) RAMS<br>7) CAMS | 1) 7b.2.3<br>2) 7b.4<br>3) 7b.5<br>4) 7b.4<br>5) 7b.6<br>6) 7b.6<br>7) 7b.6 | This criterion directly addresses the protection system independence as it relates to natural phenomena and influence from other systems during operation including loss of redundant devices. The RICS is modular redundant so the likelihood of complete loss of all monitored parameters is very low. There are redundant measurement devices for monitored parameters. The measurements are independent, thus limiting the possibility of failure. |
| 37 | 10CFR 50, Appendix A, GDC 23 Protection system failure modes | 1) RICS<br>2) ESFs | 1) 7b.2.3<br>2) 7b.4 | This criterion directly addresses the protection system failure mode. The RICS and ESFs are designed to fail-safe upon loss of electric power and loss of instrument air. The failed state is isolation for the hot cells and confinement zones. |
| 38 | 10CFR 50, Appendix A, GDC 24 Separation of protection and control systems | N/A | N/A | This criterion directly addresses the separation of the protection system from the control system. This criterion was developed for nuclear reactors. The RPF has no reactor or reactor-like systems. |
| 39 | 10CFR 50, Appendix A, GDC 25 Protection system requirements for reactivity control malfunctions | N/A | N/A | This criterion directly addresses the protection system ability to limit the control system for fuel insertion. This criterion does not apply to the system utilized by RPF. |
| 40 | 10CFR 50, Appendix A, GDC 26 Reactivity control system redundancy and capability | N/A | N/A | This criterion directly addresses the control systems ability to modify reactivity by two separate means. This criterion does not apply to the system utilized by RPF. |

**Table 7b.2-2 RPF Verification Matrix Design Criteria, Bases, Description (Sheet 7 of 7)**

| Verification Matrix | Design Criterion | Design Basis Applicability | Detailed Section Reference | Functional Means |
|---|---|---|---|---|
| 41 | 10CFR 50, Appendix A, GDC 27<br>Combined reactivity control systems capability | N/A | N/A | This criterion directly addresses the ability of the control system to handle a postulated stuck rod even after poison injection. This criterion does not apply to the RPF. |
| 42 | 10CFR 50, Appendix A, GDC 28<br>Reactivity limits | N/A | N/A | This criterion directly addresses the control systems ability to limit the reactivity rate of change. This criterion does not apply to the RPF. |
| 43 | 10CFR 50, Appendix A, GDC 29<br>Protection against anticipated operational occurrences | 1) RICS<br>2) ESFs<br>3) RICS display<br>4) RICS SR end devices<br>5) CAAS<br>6) RAMS<br>7) CAMS | 1) 7b.2.3<br>2) 7b.4<br>3) 7b.5<br>4) 7b.4<br>5) 7b.6<br>6) 7b.6<br>7) 7b.6 | This criterion directly addresses the protection system's and the control system's ability to function with high reliability for operational occurrences which require a safety action. The RICS/ESFs, CAMS, RAMS, and CAAS are designed as independent systems so that measured malfunctions that create an off-normal event either initiate a mitigative ESF action or alerts the operator of the abnormal event. The RICS is specifically chosen for its high reliability and fault tolerance and recognized as such by independent testing as a pre-qualified platform for safety-instrumented systems. |

## 7b.3 PRODUCTION FACILITY PROCESS CONTROL SYSTEMS

The RPF process control is administered by the RICS. The RICS is described in Subsection 7b.2.3. The RICS performs the following process functions:

- Monitors the valve position for routing process fluid for inter-equipment process fluid transfers. For specific transfers identified by the operator, the RICS provides a permissive to allow for the active pump in that circuit to be energized once the operator has manually configured the routing.
- Monitors and controls inter-equipment process fluid transfers in the RPF. For transport requiring a pump, the RICS controls the ability of the pump to be energized, and for specific transfers, provides controlled fluid flow transfers based on closed loop flow control. The operator initializes the transfer of fluids.
- Transfer of target solution from the TSV dump tank in an IU cell to one of the molybdenum extraction and purification systems (MEPS). The transfer is supervised by the TPCS and RICS controls RPF valve alignments.
- Transfer of prepared target solution from the target solution preparation system (TSPS) in the RPF to the TSV hold tank. This transfer is supervised by the TPCS in terms of a required permissive to fill the TSV hold tank.
- Transfer of recycled target solution that is moved from target solution recycle holding tank in the RPF to the TSV hold tank. This transfer is supervised by the TPCS. The RICS requires a permissive from the TPCS to fill the TSV hold tank.

Potential variables, conditions, or other items that will be probable subjects of technical specifications associated with the production facility process control systems are provided in Chapter 14.

### 7b.3.1 VALVE POSITION MIMIC TABLES

The RICS monitors the valve position of system piping between and into the RPF equipment. The operator in the control room can visually see on a screen the valve position that is represented on the process floor. The RICS display mimics the valve position. The position of the valves is compared against an internal logic table to determine if the appropriate path is represented on the display. The DCS assists the operator by confirming that the valve alignment is routed appropriately for transfer of process fluid from location to location.

### 7b.3.2 PUMP CONTROL

The RICS is tasked with controlling the material transfers within the RPF. In combination with mimic tables, the RICS determines if a transfer can occur as an operator requests. The confirmation from the RICS that the alignment and transfer are appropriately configured provides an additional check to insure that no transfer can occur until properly configured.

### 7b.3.3 IRRADIATION UNIT CELL TRANSFER

During transfer of the target solution from the TSV dump tank to one of the MEPS in the RPF, RICS controls valve alignments in the RPF. The TPCS validates proper valve alignment in the IU cell to allow transfer of the target solution is transferred to the MEPS. Once the permissive is given, the target solution is transferred to the MEPS as long as the valve alignment in the RPF is correct as outlined in Subsection 7b.3.1.

### 7b.3.4 FRESH TARGET SOLUTION LOADING INTO THE TSV HOLD TANK

Transfer of the target solution from the TSPS in the RPF to the TSV hold tank is performed by the RICS. The RICS controls the transfer and the TPCS performs a supervisory function. The TPCS validates proper valve alignment in the IU cell to allow transfer of the target solution to the TSV hold tank. Once the permissive is given, the RICS can transfer the target solution to the TSV hold tank as long as the valve alignment in the RPF is correct as outlined in Subsection 7b.3.1.

### 7b.3.5 RECYCLED TARGET SOLUTION LOADING INTO THE TSV HOLD TANK

Transfer of the target solution from the recycled target solution holding tank in the RPF to the TSV hold tank is performed by the RICS. The RICS controls the transfer and the TPCS performs a supervisory function. The TPCS validates proper valve alignment in the IU cell to allow transfer of the target solution to the TSV hold tank. Once the permissive is given, the RICS can transfer the target solution to the TSV hold tank as long as the valve alignment in the RPF is correct as outlined in Subsection 7b.3.1.

## 7b.4 ENGINEERED SAFETY FEATURE AND ALARMING

### 7b.4.1 SYSTEM DESCRIPTION

Process control ESFs within the RPF are activated by the RICS. An RPF ESF actuation system does not exist as a standalone system. The RICS performs the following ESF actuation functions:

- For hot cells, gloveboxes, or other cells (including the noble gas storage cell) that require isolation in the RPF, the RICS monitors parameters designated SR and when appropriate, actuates the ESF for the hot cells, gloveboxes, or other cells. The ESFs that are actively controlled are the isolation inlet and outlet bubble-tight dampers and isolation valves for other penetrations into the enclosure that are determined to require isolation during the final safety analysis. Upon recognition of an off-normal SR parameter, the RICS de-energizes the dampers and isolation valves in the system and the dampers and valves move to a closed safe-state for the affected hot cell, glovebox, or other cell. The ESF dampers and isolation valves within the RPF are designed as fail-closed dampers so that any loss of power results in closure and subsequent isolation of the hot cell, glovebox, or other cell.

- For the RCA ventilation system in the RPF, the RICS monitors parameters designated as SR and when appropriate, actuates the ESF for the specific RCA ventilation system zone. For the RCA ventilation system zones, the ESFs that are actively controlled are the inlet and outlet bubble-tight dampers for each zone. Upon recognition of a SR parameter exceeding acceptable limits for isolation, the RICS de-energizes the dampers in the system and the bubble-tight dampers move to a closed safe-state for the affected ventilation zone. The bubble-tight dampers within the RCA zone ventilation system are designed as fail-closed dampers so that loss of power results in closure of the damper and subsequent isolation of the RCA ventilation system zone.

- The internal logic of the RICS monitors the ESF and provides assurance that the ESF activation goes to completion. The ESF is reset by the operator from the RICS HMI display. The RICS is described in Subsection 7b.2.3.

#### 7b.4.1.1 RICS Trips Description (Functional Performance)

This section identifies the monitored parameters and describes the events for initiating an ESF. The monitoring and control functions are described on a parameter by parameter basis in the following.

The RICS performs one automated initiation of ESFs, for mitigation of radiation contamination. Additionally, in the event of an activation of the HCFD or the FFPS, the RICS activates dampers to isolate affected areas. The FFPS and HCFD isolation functions are not SR functions. The other automated response occurs when an active radiation monitored parameter within the isolable cell exceeds a trip level setting. In the case of an individual hot cell, glovebox, or other cell the RICS activates the ESF for bubble-tight damper isolation of the affected hot cell, glovebox, or other cell.

7b.4.1.1.1 HCFD Activation Trip

The RICS monitors signals from the HCFD for the individual cell or glovebox. These signals input to the RICS. The RICS activates the isolation of the cell or glovebox whenever the inputs indicate that the HCFD is tripped. The inlet and outlet isolation dampers close upon HCFD activation in a cell or glovebox. The trip is automatic and not delayed, and is not considered SR, as it duplicates the function performed by gamma detectors for the mitigation of radioactive releases.

7b.4.1.1.2 Hot Cell and other Process Cell Ventilation High Gamma Trip

The RICS monitors signals from redundant gamma detectors installed in the ventilation of the individual cells or gloveboxes. Each detector provides an independent channel to the RICS. The RICS activates the ESF for the cell or glovebox whenever the 1oo2 voted signal inputs indicate that the gamma detectors have exceeded the high level setpoint. The ESF ventilation inlet and outlet isolation dampers close upon high gamma detection. The trip is automatic and not delayed.

7b.4.1.1.3 RICS Manual Trip

There is a manual trip emergency switch at each hot cell or other confinement zone. Each emergency switch provides the ability for the operator to manually isolate the individual hot cell or confinement zone. The trip of this switch initiates the activation of the ESF inlet and outlet dampers for the individual hot cell or confinement zone independent of the RICS status.

7b.4.1.1.4 RICS Manual Trip Reset

Once the isolation for a cell or glovebox has been manually activated, it takes an operator to manually reset the ESF at the hot cell or confinement zone. This is done by resetting the manual switch for the specific ESF.

7b.4.1.1.5 RICS Automatic Trip Reset

Once the isolation for a cell or glovebox has been automatically activated, it takes an operator to manually reset the ESF logic within the RICS. This is done from the RICS display panel using the ESF reset switch for the specific ESF on the HMI. The ESF is reset by the RICS.

7b.4.1.2 RICS Alarm Description (Functional Performance)

This subsection identifies the monitored parameters and describes the events for initiating an alarm to the operator as a possible contamination event.

The following subsections describe the preliminary list of variables to be monitored in the RPF for alarming to eliminate or reduce the radiation exposure for the operator. The final list of variables to be monitored will be provided in the FSAR.

#### 7b.4.1.2.1 Hot Cell Differential Pressure Alarm

The RICS monitors the differential pressure of each hot cell in the RPF with independent redundant pressure sensors. These pressure sensors monitor the pressure differential that exists between the inside and outside of the hot cell. Each sensor provides an independent input to the RICS. The RICS activates an alarm locally and in the control room whenever 1oo2 in a voted pair exceeds the low differential alarm setpoint.

#### 7b.4.1.2.2 Hot Cell Over Temperature Alarm

The RICS monitors the internal temperature of each hot cell in the RPF with independent redundant sensors. Each sensor provides an independent input to the RICS. The RICS activates an alarm locally and in the control room whenever 1oo2 in a voted pair exceeds the high temperature alarm setpoint.

#### 7b.4.1.2.3 Uranyl Nitrate Conversion System Over Temperature Alarm

The RICS monitors the temperature of each UNCS in the RPF with independent redundant sensors. These sensors measure the temperature at the outlet of the UNCS. Each sensor provides an independent input to the RICS. The RICS activates an alarm locally and in the control room whenever 1oo2 in a voted pair exceeds the high temperature alarm setpoint.

#### 7b.4.1.2.4 Radioactive Drain System High Level Alarm

The RICS monitors signals from redundant level detectors installed in individual sump areas in the RDS. Each detector provides an independent input to the RICS. The RICS activates an alarm locally and in the control room whenever 1oo2 in a voted pair exceeds the high level alarm trip.

#### 7b.4.1.2.5 Leak Detection in RDS Sump Locations and PVVS Overflow / Low Point Vent

The RICS monitors signals from redundant leak detectors installed in individual sump areas in the RDS. Each detector provides an independent input to the RICS. The RICS monitors signals from redundant leak detectors installed in low points or overflow areas in the PVVS. Each detector provides an independent input to the RICS. The RICS activates an alarm locally and in the control room whenever 1oo2 in a voted pair exceeds the high level alarm trip.

#### 7b.4.1.2.6 Process Vessel Vent System Differential Pressure Alarm

The RICS monitors the differential pressure for selected sections of the PVVS with independent redundant pressure sensors. These pressure sensors monitor the pressure differential that exists between the inside and outside of the PVVS. Each sensor provides an independent input to the RICS. The RICS activates an alarm in the control room whenever 1oo2 in a voted pair exceeds the low differential alarm setpoint.

#### 7b.4.1.2.7 Process Vessel Vent System Low Flow Alarm

The RICS monitors the flow rate of the sweep gas for selected vessels in the PVVS with independent redundant flow sensors. Each sensor provides an independent input to the RICS. The RICS activates an alarm in the control room whenever 1oo2 in a voted pair exceeds the low flow alarm setpoint.

#### 7b.4.1.2.8 RCA Differential Pressure Alarm

The RICS monitors the differential pressure for selected areas between ventilation zones with independent redundant pressure sensors. These pressure sensors monitor the pressure differential that exists between the RCA ventilation zones. Each detector provides an independent input to the RICS. The RICS activates an alarm in the control room whenever 1oo2 in a voted pair exceeds the low differential alarm setpoint.

#### 7b.4.1.2.9 RPF Valve Sequence Monitoring

The RICS monitors the valve positions in the RPF that are utilized for inter-equipment process fluid transfers. Each valve has two independent sets of sensors that provide valve position information for the RICS. Each of these sensors goes to the RICS.

### 7b.4.2 ANNUNCIATION AND DISPLAY

The actuation of an ESF in the RCA is displayed on the RICS HMI and locally at the affected system with an audible alarm. The alarm annunciator display panel and the alarm / event display show the triggering event and the subsequent RICS action to activate the ESF for the specific affected system.

Once actuated, ESFs require a manual input from the operator to reset the ESF. Clearing of the triggering event is required. Once the triggering event is cleared, the ESF does not resume its normal operating position, as operator action is required.

### 7b.4.3 SYSTEM PERFORMANCE ANALYSIS

This is discussed in Subsection 7b.2.4.

Potential variables, conditions, or other items that will be probable subjects of technical specifications associated with the RICS are provided in Chapter 14.

## 7b.5 CONTROL CONSOLE AND DISPLAY INSTRUMENTATION

### 7b.5.1 SYSTEM DESCRIPTION

The control console system for the RPF is located in the control room for the SHINE facility. The control console or HMI is an extension of the RICS. The RICS is discussed in detail in Subsections 7b.2.1, 7b.2.2, 7b.2.3, 7b.2.4, 7b.2.5, 7b.3, and 7b.4. The operator for the RCA utilizes the RICS for monitoring and control of the process systems within the RPF.

In addition to the control console for the RICS, the control room has annunciator displays for the CAMS, RAMS, and the CAAS for the RPF. Section 7b.6 discusses the CAMS, RAMS, and CAAS in detail for the RPF. The operator monitors and controls the systems within the RPF from the control room.

Potential variables, conditions, or other items that will be probable subjects of technical specifications associated with the control console and displays are provided in Chapter 14.

#### 7b.5.1.1 Control Room Layout

The control room shares resources between the RPF systems and systems from the IF. In the control room, there is one dedicated workstation HMI for use by the RPF operator. The control room layout Figure 7a.2.6-2 indicates the location of the different workstations. The dedicated workstation for the RPF operator also has an interface system for the FICS. The display arrangements for this specific RPF workstation are shown in Figure 7b.2-1.

The CAMS, RAMS, and CAAS each have annunciator panel displays in the control room. The RPF operator has access to the visual and audible alarming for systems that are in the RPF. The RPF workstation interfaces with the various radiation monitoring systems so that an event or alarm is recorded and displayed on the RICS alarm / event log.

#### 7b.5.1.2 RICS HMI Displays

Design criteria for the control room display systems are described in Subsection 7b.2.1. The functional descriptions for the RICS displays are listed in Subsection 7b.2.3.2.1. The approach to the display information is similar to that of the TRPS and the TPCS displays. The RICS utilizes a static annunciation display, an alarm / event display log, and an HMI operator interface display.

#### 7b.5.1.3 RICS HMI Redundancy

The RICS HMI displays are redundant due to their inclusion in the IF workstation configuration. This inclusion is illustrated in Figure 7a.2.6-1. The ability to coordinate views of systems is important to the operational nature of the SHINE facility. The transfer of target solution from the TSPS to the TSV hold tank is a coordinated transfer between the RPF and the IF. Similarly, the transfer of target solution from the TSV dump tank to the MEPS is a coordinated transfer between the IF and RPF. Having the TPCS and RICS available simultaneously is an important operational feature of the SHINE facility.

#### 7b.5.1.4 Hot Cell Operator Interface Terminals

Each hot cell system has an OIT. This terminal is an extension of the information collected by the RICS. Each terminal displays the status for the individual system. The terminal shows current alarm status and ESF state for each hot cell. Pump controls for specific hot cells are initiated, interlocked, and controlled from a touchscreen-type OIT.

## 7b.6 RADIATION MONITORING SYSTEMS

Refer to Section 7a2.7 for discussions and details on RAMS and CAMS.

The criticality accident alarm system (CAAS) provides for continuous monitoring, indication, and recording of neutron or gamma radiation levels in areas where personnel may be present and wherever an accidental criticality event could result from operational processes. The CAAS is capable of detecting a criticality accident that produces an absorbed dose in soft tissue of 20 rads of combined neutron or gamma radiation at an unshielded distance of 2 meters from the reacting material within one minute, except for events occurring in areas not normally accessed by personnel and where shielding provides protection against a criticality. Two detectors cover each area needing CAAS coverage.

The control unit electronics actuate local and remote alarms. The locations of the detectors will be provided in the FSAR.

The CAAS detectors provide local annunciation and remote annunciation in the control room to alarm when the radiation levels exceed established setpoints. Alarming CAAS monitors communicate the location of the criticality accident alarm to the RICS. Diagrams of the CAAS and associated systems will be provided in the FSAR.

The UPSS provides emergency power to the CAAS during a LOOP.

The CAAS meets the criteria of 10 CFR 20.1501, and uses the guidance provided by ANSI/ANS 8.3-1997 (1997) and Regulatory Guide 3.71.

As a safety-related system, the CAAS will be designed to remain operational during design basis accidents, which are described in detail in Chapter 13.

## 7b.7 REFERENCES

**ANS, 2003.** Criticality Accident Alarm System, ANS-8.3:R2003, American Nuclear Society, 2003.

**ANS, 2008.** Verification and Validation of Non-Safety-Related scientific and Engineering Computer Programs for the Nuclear Industry, ANS-10-4:R2008, American Nuclear Society, 2008.

**EPRI, 1996.** Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications, EPRI TR-106439, Electric Power Research Institute, 1996.

**IEC, 2010.** Functional safety of electrical/electronic/programmable electronic safety-related systems, Part 1 – General requirements, IEC 61508-1:2010, International Electrotechnical Commission, 2010.

**IEEE, 2000.** IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems, IEEE Std 379:2000, IEEE Power & Energy Society, The Institute of Electrical and Electronics Engineers, Inc., 2000.

**IEEE, 2003.** IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations, IEEE Std 323:2003, IEEE Power & Energy Society, The Institute of Electrical and Electronics Engineers, Inc., 2003.

**IEEE, 2004.** IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Facilities, IEEE Std 577:2004, IEEE Power & Energy Society, The Institute of Electrical and Electronics Engineers, Inc., 2004.

**IEEE, 2005.** IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations, IEEE Std 344:2005, IEEE Power & Energy Society, The Institute of Electrical and Electronics Engineers, Inc., 2005.

**IEEE, 2008a.** IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits, IEEE Std 384:2008, IEEE Power & Energy Society, The Institute of Electrical and Electronics Engineers, Inc., 2008.

**IEEE, 2008b.** IEEE Standard for Software and System Test Documentation, IEEE Std 829:2008, IEEE Power & Energy Society, The Institute of Electrical and Electronics Engineers, Inc., 2008.

**IEEE, 2008c.** IEEE Standard for Software Reviews and Audits, IEEE Std 1028:2008, IEEE Power & Energy Society, The Institute of Electrical and Electronics Engineers, Inc., 2008.

**IEEE, 2009.** IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, IEEE Std 603:2009, IEEE Power & Energy Society, The Institute of Electrical and Electronics Engineers, Inc., 2009.

**IEEE, 2010a.** IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations, IEEE Std 497:2010, IEEE Power & Energy Society, The Institute of Electrical and Electronics Engineers, Inc., 2010.

**IEEE, 2010b.** IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, IEEE 7-4.3.2, IEEE Power & Energy Society, The Institute of Electrical and Electronics Engineers, Inc., 2010.

**IEEE, 2012a.** IEEE Standard for Configuration Management in Systems and Software Engineering, IEEE Std 828:2012, IEEE Power & Energy Society, The Institute of Electrical and Electronics Engineers, Inc., 2012.

**IEEE, 2012b.** IEEE Standard for Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems, IEEE Std 338:2012, IEEE Power & Energy Society, The Institute of Electrical and Electronics Engineers, Inc., 2012.

**ISA, 2004a.** Functional Safety: Safety Instrumented Systems for the Process Industry Sector - Part 1: Framework, Definitions, System, Hardware and Software Requirements, ISA 84.00.01-2004 Part 1, The Instrumentation, Systems, and Automation Society, 2004.

**ISA, 2004b.** Functional Safety: Safety Instrumented Systems for the Process Industry Sector - Part 2: Guidelines for the Application of ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod) – Informative, ISA 84.00.01-2004 Part 2, The Instrumentation, Systems, and Automation Society, 2004.

**ISA, 2004c.** Functional Safety: Safety Instrumented Systems for the Process Industry Sector - Part 3: Guidance for the Determination of the Required Safety Integrity Levels – Informative, ISA 84.00.01-2004 Part 3, The Instrumentation, Systems, and Automation Society, 2004.

**ISA, 2006.** Setpoints for Nuclear Safety- Related Instrumentation, ISA 67.04.01:2006, The Instrumentation, Systems, and Automation Society, 2006.

**NRC, 1993.** The Programmable Logic Controller and Its Application in Nuclear Reactor Systems, NUREG/CR-6090, U.S. Nuclear Regulatory Commission, Washington, DC, 1993.

**NRC, 1996.** Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems, NUREG/CR-6463, U.S. Nuclear Regulatory Commission, Washington, DC, 1996.

**NRC, 2002.** Human-System Interface Design Review Guidelines, NUREG-0700, Rev. 2, U.S. Nuclear Regulatory Commission, Washington, DC, 2002.

**NRC, 2003a.** Application of the Single-Failure Criterion to Safety Systems, R.G. 1.53, Rev.2, U.S. Nuclear Regulatory Commission, Washington, DC, 2003.

**NRC, 2003b.** Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety Related Instrumentation and Control Systems, R.G. 1.180, Rev.1, U.S. Nuclear Regulatory Commission, Washington, DC, 2003.

**NRC, 2006.** Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants, R.G. 1.97, Rev.4, U.S. Nuclear Regulatory Commission, Washington, DC, 2006.

**NRC, 2009.** Design Practices for Communications and Workstations in Highly Integrated Control Rooms, NUREG/CR-6991, U.S. Nuclear Regulatory Commission, Washington, DC, 2009.

**NRC, 2010.** Cyber Security Programs for Nuclear Facilities, R.G. 1.152, Rev.3, U.S. Nuclear Regulatory Commission, Washington, DC, 2010.

**NRC, 2011.** Criteria for use of Computers in Safety Systems of Nuclear Power Plants, R.G. 1.152, Rev.3, U.S. Nuclear Regulatory Commission, Washington, DC, 2011.

**United States Government, 2010.** Domestic Licensing of Special Nuclear Material, Code of Federal Regulations, Title 10, Part 70, Office of the Federal Register, Government Printing Office, September, 2010.

**United States Government, 2011.** General Design Criteria, Code of Federal Regulations, Title 10, Part 50, Appendix A, Office of the Federal Register, Government Printing Office, January, 2011.