A Holtec International Company

SMR, LLC		8002
Company		**Project No.**
HI-2251395	0	11 Dec 2025
Company Record No.	**Revision**	**Issue Date**
Report		Non-Proprietary
Record Type		**Proprietary Classification**
Nuclear		No
Quality Class		**Export Control Applicability**

Record Title:

SMR-300 Instrumentation and Control Architecture Licensing Topical Report

Proprietary Classification

Export Control Status

Export Control restrictions do not apply to this record.

ACKNOWLEDGEMENT AND DISCLAIMER

Acknowledgement: This material is based upon work supported by the Department of Energy Office of Nuclear under Award Number DE-NE0009055.

DATA RIGHTS NOTICE

PROPRIETARY INFORMATION NOTICE

This is a non-proprietary version of the “SMR-300 Instrumentation and Control Architecture Licensing Topical Report,” from which the proprietary information has been removed. The header of each page in this enclosure carries the notation “Non-Proprietary Information.” Portions of the enclosure that have been removed are indicated by open and closed brackets as shown here [[ ]].

Revision Log

Revision	Description of Changes
0	Initial Issue.

Executive Summary

The purpose of this SMR-300 Instrumentation and Control (I&C) Architecture Licensing Topical Report (LTR) is to define the system architecture configuration of the safety-related SMR-300 Plant Safety System (PSS). The PSS implements a four-channel, two-division architecture using the Mitsubishi Electric Total Advanced Controller (MELTAC)-Nplus S digital I&C platform. This LTR describes how the qualified MELTAC platform elements are integrated to form an I&C architecture for the SMR-300 that supports compliance with Nuclear Regulatory Commission (NRC) regulatory requirements and fundamental design principles for safety-related digital I&C systems, including independence, redundancy, deterministic behavior (predictability and repeatability), and diversity in support of defense-in-depth. This LTR also includes supporting information on the non-safety-related Plant Control System (PCS) and the Diverse Actuation System (DAS) to the extent necessary to demonstrate compliance with applicable regulatory requirements.

The objective of this LTR is to obtain NRC approval of the non-site-specific SMR-300 PSS architectural configuration as a referenceable licensing design basis for future safety-related digital I&C applications. This approval will confirm that the defined architecture, when implemented using the MELTAC-Nplus S platform and the processes described herein, provides an acceptable basis for meeting applicable NRC regulatory requirements and guidance for I&C safety system design and performance.

Statement of Limitations

This report references the revised MELTAC Platform LTR, which is currently under review by the NRC as of the date of this report's issuance. Should the technical content of the Platform LTR be revised to support issuance of the final Safety Evaluation (SE), this report will be updated as necessary to reflect the approved platform configuration.

Table of Contents

List of Figures

List of Tables

1.0 INTRODUCTION

1.1 Purpose

The purpose of this SMR-300 Instrumentation and Control (I&C) Architecture Licensing Topical Report (LTR), hereinafter referred to as the "Architecture LTR," is to define the system architecture configuration of the SMR-300 Plant Safety System (PSS) implemented using the Mitsubishi Electric Total Advanced Controller (MELTAC[1])-Nplus S digital I&C platform. This Architecture LTR builds on the MELTAC-Nplus S Platform Topical Report submitted by Mitsubishi Electric Corporation (MELCO) and the associated U.S. Nuclear Regulatory Commission (NRC) Safety Evaluation (SE) [1], which established the design acceptability of the platform's hardware, software, and development processes. This Architecture LTR describes how those qualified platform elements are integrated to form a four-channel, two-division safety system architecture for the SMR-300. This Architecture LTR demonstrates that this configuration supports compliance with NRC regulatory requirements and fundamental design principles for safety-related digital I&C systems, including independence, redundancy, deterministic behavior (predictability and repeatability), and diversity in support of defense-in-depth.

1.2 Background

The SMR-300 I&C systems are based on digital platforms developed by MELCO, specifically the MELTAC-Nplus S platform. MELCO received an approved SE from the NRC for the "Safety System Digital Platform – MELTAC – Topical Report" [1], which authorizes use of the MELTAC platform and its Nplus S components in safety-related applications that satisfy the limitations and conditions of the SE.

MELCO subsequently revised the MELTAC platform LTR to Revision 3 [2], which incorporates enhancements to the MELTAC platform, including updated excore instrumentation units, modifications to the Power Interface (PIF) Module, enhanced self-diagnostic capabilities, and expanded use of the Control Network. Throughout this Architecture LTR, the term "Platform LTR" refers to Revision 3 to the MELTAC platform LTR. The NRC is reviewing this updated Platform LTR in two phases. The draft SE for Phase 1 has been issued [3].

1.3 Scope

This Architecture LTR defines the architecture of the SMR-300 PSS, which performs safety-related functions in accordance with the requirements of Title 10 of the Code of Federal Regulations (10 CFR) Part 50. The scope of this report is limited to an architectural-level description of the PSS and includes supporting information on the Plant Control System (PCS) and the Diverse Actuation System (DAS) only to the extent necessary to demonstrate compliance with applicable regulatory requirements. This Architecture LTR is not site-specific and describes the architecture relative to a single SMR-300 unit.

This Architecture LTR provides the following architectural-level information:

- A description of the four-channel, two-division design used in the PSS
- The use of the MELTAC-Nplus S digital platform as the implementation basis for the PSS architecture

[1] MELTAC® is a registered trademark of Mitsubishi Electric Corporation (MELCO).

- Communication and interfaces between redundant divisions of the PSS, and between divisions and channels, and between the PSS and non-safety-related systems (PCS and DAS)
- Adherence of the I&C systems architecture to the fundamental design principles of independence, redundancy, deterministic behavior (predictability and repeatability), and diversity in support of defense-in-depth
- Adherence of the PSS architecture to § 50.55a(h), IEEE Std 603-1991 [4], and IEEE Std 7-4.3.2-2016 [5]

This report does not address the specific safety analyses performed under Chapter 15 of the safety analysis report, or the detailed reactor trip (RT) and engineered safety feature (ESF) actuation functions associated with those analyses. These topics will be addressed in future licensing submittals. Consequently, evaluations requiring detailed functional analysis of the RT and ESF are outside the scope of this report.

This report does not address all plant-specific action items (PSAIs) in the Platform LTR SEs [1] [3]. PSAIs will be addressed in future licensing submittals.

1.4 Objective

The objective of this Architecture LTR is to obtain NRC approval of the SMR-300 PSS architectural configuration as a referenceable licensing design basis for future safety-related digital I&C applications. This approval will confirm that the defined architecture, when implemented using the MELTAC-Nplus S platform and the processes described herein, provides an acceptable basis for meeting applicable NRC regulatory requirements and guidance for I&C safety system design and performance.

NRC approval of this Architecture LTR will establish the acceptability of:

- The overall four-channel, two-division PSS architecture, including its communication, voting, and interface structures;
- The use of MELTAC-Nplus S platform components within that architecture; and
- The framework of analyses, verifications, and validations necessary to demonstrate compliance at the plant-specific level.

This Architecture LTR does not define plant-specific application logic, setpoints, or instrumentation configurations. Future licensees or applicants referencing this LTR (e.g., as part of an operating license application or license amendment request) will provide plant-specific analyses, system logic, and configuration details that demonstrate conformance with the architecture and implementation processes approved by the NRC in this report.

By obtaining NRC approval of the SMR-300 PSS architecture as described herein, subsequent licensing submittals can leverage this report to streamline regulatory review and avoid duplication of architectural-level evaluations already accepted by the NRC.

1.5 Acronyms and Abbreviations

1oo2, 2oo3, 2oo4...	X-Out-Of-N (Voting Logic)
A-VDU	Alarm Visual Display Unit
A-VDU-P	Alarm Visual Display Unit Processor
AOO	Anticipated Operational Occurrence
ATWS	Anticipated Transients Without Scram
BISI	Bypassed or Inoperable Status Indication
BTP	Branch Technical Position
CBP	Channel Bistable Processor
CCF	Common-Cause Failure
CCP	Component Control Processor
CFR	Code of Federal Regulations
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CRDM	Control Rod Drive Mechanism
D3	Diversity and Defense-in-Depth
D-HSI	Diverse Human System Interface
DAS	Diverse Actuation System
DBE	Design Basis Event
DO	Digital Output
DPL	Diverse Protection Logic
DPM	Dual Port Memory
EQ	Environmental Qualification
ESF	Engineered Safety Feature
F-ROM	Flash Read-Only Memory
FMEA	Failure Modes and Effects Analysis
GDC	General Design Criterion
HFE	Human Factors Engineering
HSI	Human System Interface
I&C	Instrumentation and Control
I/O	Input/Output
IEEE	Institute of Electrical and Electronics Engineers
IPL	Interposing Logic
ISG	Interim Staff Guidance
LDP	Large Display Panel
LDP-P	Large Display Panel Processor
LTR	Licensing Topical Report
MCR	Main Control Room
MELCO	Mitsubishi Electric Corporation
MELTAC	Mitsubishi Electric Total Advanced Controller
MIC	Memory Integrity Check
MIS	Manual Initiation Switch
MXS	Master Transfer Switch
NRC	Nuclear Regulatory Commission
NSREER	Non-Safety-Related Electrical Equipment Room
O-VDU	Operational Visual Display Unit
O-VDU-P	Operational Visual Display Unit Processor
P-VDU	Procedure Visual Display Unit
P-VDU-P	Procedure Visual Display Unit Processor

PAM	Post-Accident Monitoring
PCS	Plant Control System
PDI	PIM Digital Input
PDO	PIM Digital Output
PIF	Power Interface
PIM	Power Interface Module
POL	Problem Oriented Language
PSAI	Plant-Specific Action Item
PSS	Plant Safety System
RG	Regulatory Guide
RPP	Reactor Protection Processor
RSF	Remote Shutdown Facility
RT	Reactor Trip
RTB	Reactor Trip Breaker
S-VDU	Safety Visual Display Unit
S-VDU-P	Safety Visual Display Unit Processor
SE	Safety Evaluation
SFC	Single-Failure Criterion
SMR	Small Modular Reactor
SREER	Safety-Related Electrical Equipment Room
SSC	Structures, Systems, and Components
ST	Shunt Trip
Std	Standard
TD	Time Delay
UV	Undervoltage
Vac	Voltage in Alternating Current
Vdc	Voltage in Direct Current
VDU	Visual Display Unit
WDT	Watchdog Timer

2.0 DESIGN BASIS

The SMR-300 I&C architecture was developed based on the regulatory requirements of 10 CFR Part 50 and the guidance provided in DNRL-ISG-2022-01 [6] and its associated references. The following sections identify the applicable NRC regulatory requirements and guidance used for development of the SMR-300 I&C architecture.

2.1 Regulatory Requirements

Table 2-1 identifies the applicable 10 CFR Part 50 regulations for the SMR-300 I&C systems, including the architecture. Full compliance will be demonstrated as part of future SMR-300 licensing submittals.

Table 2-1 Applicable 10 CFR Part 50 Requirements

Regulation	Subject of Requirement
§ 50.34(b)(2)(i)	Final safety analysis report contents
§ 50.34(f)(2)(iv)	Safety parameter display console

Regulation	Subject of Requirement
§ 50.34(f)(2)(v)	Bypass and inoperable status indication
§ 50.34(f)(2)(xi)	Direct indication of relief and safety valve position
§ 50.34(f)(2)(xii)	Auxiliary feedwater system initiation and flow indication
§ 50.34(f)(2)(xiv)	Containment isolation systems
§ 50.34(f)(2)(xvii)	Accident monitoring instrumentation
§ 50.34(f)(2)(xviii)	Inadequate core cooling indication
§ 50.34(f)(2)(xix)	Accident monitoring instrumentation following core damage
§ 50.34(f)(2)(xx)	Power for pressurizer relief valves, block valves, and level indicators
§ 50.34(f)(2)(xxii)	Failure modes and effects analysis of integrated control system
§ 50.34(f)(2)(xxiii)	Anticipatory reactor trip on loss of main feedwater or turbine trip
§ 50.36(c)(1)(ii)(A)	Technical specifications for limiting safety system settings
§ 50.36(c)(3)	Technical specifications for surveillance requirements
§ 50.49	Environmental qualification of electric equipment
§ 50.54(jj)	Quality standards
§ 50.55(i)	Quality standards
§ 50.55a(h)	Codes and standards for protection and safety systems
§ 50.62	Reduction of risk from anticipated transients without scram (ATWS) events
Appendix A, GDC 1	Quality standards and records
Appendix A, GDC 2	Design bases for protection against natural phenomena
Appendix A, GDC 4	Environmental and dynamic effects design bases
Appendix A, GDC 5	Sharing of structures, systems, and components
Appendix A, GDC 10	Reactor design

Regulation	Subject of Requirement
Appendix A, GDC 12	Suppression of reactor power oscillations
Appendix A, GDC 13	Instrumentation and control
Appendix A, GDC 15	Reactor coolant system design
Appendix A, GDC 16	Containment design
Appendix A, GDC 19	Control room
Appendix A, GDC 20	Protection system functions
Appendix A, GDC 21	Protection system reliability and testability
Appendix A, GDC 22	Protection system independence
Appendix A, GDC 23	Protection system failure modes
Appendix A, GDC 24	Separation of protection and control systems
Appendix A, GDC 25	Protection system requirements for reactivity control malfunctions
Appendix A, GDC 28	Reactivity limits
Appendix A, GDC 29	Protection against anticipated operational occurrences
Appendix A, GDC 64	Monitoring radioactivity releases
Appendix B	Quality assurance criteria

2.2 Regulatory Guidance

Table 2-2 identifies the applicable regulatory guides (RGs) used in the development of the SMR-300 I&C systems, including the architecture.

Table 2-2 Applicable Regulatory Guidance

Document Number	Document Title
RG 1.22 Rev. 0	Periodic Testing of Protection System Actuation Functions
RG 1.47 Rev. 1	Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems
RG 1.53 Rev. 2	Application of the Single-Failure Criterion to Safety Systems

Document Number	Document Title
RG 1.62 Rev. 1	Manual Initiation of Protection Actions
RG 1.75 Rev. 3	Criteria for Independence of Electrical Safety Systems
RG 1.97 Rev. 5	Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants
RG 1.105 Rev. 4	Setpoints for Safety-Related Instrumentation
RG 1.118 Rev. 3	Periodic Testing of Electric Power and Protection Systems
RG 1.151 Rev. 2	Instrument Sensing Lines
RG 1.152 Rev. 4	Criteria for Programmable Digital Devices in Safety-Related Systems of Nuclear Power Plants
RG 1.153 Rev. 1	Criteria for Safety Systems
RG 1.168 Rev. 2	Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
RG 1.169 Rev. 1	Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
RG 1.170 Rev. 1	Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
RG 1.171 Rev. 1	Software Unit Testing for Digital Computer Software Used in Safety Systems in Nuclear Power Plants
RG 1.172 Rev. 1	Software Requirement Specifications for Digital Computer Software and Complex Electronics Used in Safety Systems of Nuclear Power Plants
RG 1.173 Rev. 1	Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
RG 1.180 Rev. 2	Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems
RG 1.204 Rev. 1	Guidelines for Lightning Protection of Nuclear Power Plants
RG 1.209 Rev. 0	Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants

3.0 ARCHITECTURE OVERVIEW

The SMR-300 I&C architecture consists of three primary systems, as shown in Figure 3-1:

- Plant Safety System (PSS) – PSS is the system responsible for RT and ESF actuations and safety monitoring. PSS consists of four channels and two divisions. PSS provides the primary interface for the operator to perform intra-divisional, inter-divisional or component-level control of safety equipment. PSS also provides primary means for the operator to perform post-accident monitoring (PAM) system functions.
- Plant Control System (PCS) – PCS is the system responsible for control of the plant and provides the primary interface for the operators to control and monitor the plant. PCS provides an enhanced interface for the operator to support a safety function. PCS also provides enhanced means for the operator to perform PAM system functions.
- Diverse Actuation System (DAS) – DAS is the system that provides a diverse means to perform automatic and manual RT and specific ESF functions. DAS also provides diverse means for the operator to perform PAM system functions.

These systems are arranged to maintain independence and separation between safety-related and non-safety-related systems and between redundant portions of the safety system, and provide operators with the necessary interfaces for monitoring and control. The detailed architectural designs of these systems are described in Section 4.0, and adherence to the fundamental design principles is discussed in Section 5.0 of this report.

3.1 System Classifications

The structures, systems, and components (SSCs) of the SMR-300 I&C systems are classified following the guidance in IEEE Std 603-1991 as Class 1E or non-Class 1E. The classifications of the SMR-300 I&C systems discussed in this report are captured in Table 3-1.

Table 3-1 I&C System Classification

System	Classification
Plant Safety System (PSS)	Class 1E
Plant Control System (PCS)	Non-Class 1E
Diverse Actuation System (DAS)	Non-Class 1E

3.2 Communication Interfaces

As illustrated in Figure 3-1, the communication interfaces between systems and subsystems of the SMR-300 I&C architecture are designed to ensure safety and enhance reliability of the systems.

[[

]]

3.3 Control Stations

[[

]]

Figure 3-1 SMR-300 I&C Architecture

[[

]]

4.0 SYSTEMS

The SMR-300 I&C systems are described in this section with a focus on the PSS and its interfaces. Other systems are described to show their interfaces to the PSS and support a description of the overall I&C Architecture.

4.1 Plant Safety System

The SMR-300 PSS is a digital, safety-related I&C system that provides automatic and manual control of safety functions and components. The PSS monitors plant conditions in accordance with PAM requirements and initiates limiting actions to ensure protection and mitigation during operational states and design basis events (DBEs).

The PSS includes subsystems that continuously monitor safety-related instrumentation affecting the fission process, reactor core integrity, reactor cooling systems, and containment. When monitored parameters exceed predetermined setpoints, the system automatically initiates RT and ESF actuations. Manual operator control of reactor trip breakers (RTBs) and other safety components is also supported by the PSS.

4.1.1 PSS Configuration

The PSS utilizes a four-channel, two-division configuration, with the two independent and redundant divisions designated as Division A and Division B (Figure 4-1). Each division is comprised of the reactor protection processor (RPP), the PSS component control processor (PSS-CCP), the PSS human system interface (PSS-HSI) (including the S-VDU, MIS, and MXS), and the RTB. The channel bistable processors (CBPs) are channelized processors that perform bistable processing for their respective channel sensor inputs. Refer to Section 4.1.1.1 of the Platform LTR for additional information on the configuration concepts.

[[

]]

This configuration allows each division's RPP to independently perform two-out-of-four (2oo4) voting logic for the RT and ESF functions, without reliance on the other division. Refer to Section 4.1.3.1 of this report for additional information on the voting logic.

If an RT condition is met through the 2oo4 logic, the RPP directly initiates the RT signal to its respective RTBs. There are four RTBs in total, two in each division. Refer to Section 4.1.3.5 of this report for additional information on RT initiation.

For ESF functions, the RPP transmits actuation signals to the PSS-CCP within the same division via Safety Bus communication, and the PSS-CCP send the ESF actuation signals to [[ ]]

ESF actuation signals from the DAS, which provides a diverse backup actuation path in the event of a PSS failure due to software CCFs, are also routed via hardwired, electrically isolated connections directly to [[

]]

The S-VDU serves as the operator interface for initiating RT, managing bypass conditions, and monitoring and operating safety components via the Safety Bus. Refer to Section 4.2 of the Platform LTR for additional information on the S-VDU.

Manual RT is supported via two independent paths: [[

]]

Figure 4-1 PSS Configuration

[[

]]

4.1.2 PSS Communications

4.1.2.1 Safety Bus

[[

]]

4.1.2.2 Data Link

[[

]]

4.1.2.3 Unit Bus

[[

]]

4.1.2.4 Maintenance Network

[[

]]

4.1.3 PSS Design Features

4.1.3.1 2oo4 Coincidence Voting

Coincidence voting is used to determine when actuations are necessary. 2oo4 voting logic is shown in Figure 4-2 and is used for the following actuation types:

- Automatic RT actuation
- Automatic ESF actuation
- Interlock actuation
- Operating bypass permissive
- MXS (see Section 4.1.3.8 of this report)

For each distinct function, [[

]]

The 2oo4 voting has provisions for initiating maintenance bypass on a channel, as discussed in Section 4.1.3.2 of this report.

Figure 4-2 2oo4 Coincidence Voting

[[

]]

4.1.3.2 Maintenance Bypass

If a channel fails or needs to be taken out of service for maintenance, the channel signal, including bistable output, can be bypassed using a dedicated maintenance bypass function. Individual bypasses are provided for each redundant channel for all inputs to the PSS. A bypassed parameter and channel status are indicated in the MCR through both the PSS and PCS, consistent with the guidance in RG 1.47 [7].

When a channel is bypassed using the maintenance bypass function, a partial trip from that channel is blocked from impacting the 2oo4 voting logic, which inherently changes the 2oo4 voting logic to 2oo3 for the remaining channels.

A maintenance bypass interlock is provided to prevent multiple redundant channels from the same process measurement from being bypassed at the same time. The maintenance bypass interlock logic is shown in Figure 4-3.

This mechanism provides the capability for testing and calibration of safety system equipment of a channel, while retaining the capability of the safety systems to accomplish their safety functions.

Figure 4-3 Maintenance Bypass Interlock Logic

[[

]]

4.1.3.3 ESF Initiation and Reset

The actuation logic for each ESF function uses a standard set of logic, as shown in Figure 4-4. Each actuation logic function is initiated automatically by some specific set of logic for that function. Each function can also be manually initiated by the operator. Once initiated, the

function is latched at the division level. A manual reset is provided for the operators to reset the function once allowed by the divisional permissive.

[[

]]

Figure 4-4 ESF Initiation and Reset Logic

[[

]]

4.1.3.4 Operating Bypasses

Operating bypasses are used when a set of protection logic is not necessary based on the plant conditions. An operating bypass can be initiated and reset automatically by the PSS or manually by the operator. The standard logic shown in Figure 4-5 shows all available options for an operating bypass.

[[

]]

Figure 4-5 Operating Bypass Logic

[[

]]

4.1.3.5 RT Initiation and Reset

The PSS monitors plant parameters to provide protective action, including RT, to prevent safety limits from being exceeded. The PSS initiates an RT when required by removing power to the control rod drive mechanisms (CRDMs), causing control rods to drop and trip the reactor. Figure 4-6 shows the RT logic.

A manual RT can be initiated by touch screen controls or a physical RT switch. [[

]] Initiation from any of these locations will call for both divisions to open the RTBs. The physical RT switch is located on the safety console. The two contacts of the physical switch are inputs to a hardwired AND gate,

which directly initiates the RT signal for the division. This division's RT signal also generates a logical RT signal through an OR gate, which is combined with the RT signal from other division [[ ]] Therefore, each manual RT initiates an RT in both divisions. A manual reset is provided for the operators to reset the RT initiation once allowed by the divisional permissive.

[[

]]

Figure 4-6 RT Logic

[[

]]

The RT initiation signal de-energizes the undervoltage (UV) coils and energizes shunt trip (ST) coils on the RTB, as shown in Figure 4-7. [[

]]

[[

]] This ensures that if there is a complete failure of the RPPs in both PSS divisions, all RTBs will be actuated to ensure an RT.

The RT function is fail-safe design, as required by General Design Criterion (GDC) 23. Under the following failure conditions, the RTBs will trip the reactor:

- RPPs fail due to failure of both divisions
- RPPs fail due to loss of power in both divisions

The fail-safe output is caused by loss of power, or the conditions outlined in Section 4.1.5 of the Platform LTR.

RTBs are configured with two parallel breakers in each division. An RT occurs if both breakers in either division open.

Figure 4-7 RTB Configuration

[[

]]

4.1.3.6 Prioritization Between PSS and PCS

[[

]]

Figure 4-8 Open Component Prioritization Logic

[[

]]

Figure 4-9 Close Component Prioritization Logic

[[

]]

[[

]]

Figure 4-10 Lockout Component Prioritization Logic

[[

]]

[[

]]

4.1.3.7 Prioritization Between PSS and DAS

The prioritization between the PSS and DAS is accomplished on the PIM. Each PIM controls a single component. Interposing logic (IPL) within the PIM implements the priority function used for a diverse actuation signal.

[[

]]

The prioritized state can be selected for individual components controlled with two outputs or one output as discussed below.

Components Controlled with Two Outputs

[[

]]

Figure 4-11 Components Controlled with Two Outputs

[[

]]

Components Controlled with One Output

[[

]]

Figure 4-12 Components Controlled with One Output

[[

]]

4.1.3.8 PSS-HSI

Each division of the PSS-HSI consists of two S-VDUs, one MIS (hardware switch for RT), and two MXSs. The SMR-300 utilizes the MCR as the primary location from which operators oversee and manipulate plant processes and components. The RSF is an alternate location from which the operators may assume plant control if the MCR requires evacuation. MXS is used to transfer control between the MCR and RSF.

S-VDU

The S-VDU is a touch-panel display that allows operators to monitor process values and component status and to operate safety components. [[

]]

S-VDUs are installed in both the MCR and the RSF, enabling operators to perform monitoring and control from either location to support safe-shutdown strategies. As seen in Figure 4-1, each S-VDU is driven by a dedicated S-VDU processor (S-VDU-P), which communicates with the RPP and the PSS-CCP [[ ]]

The S-VDU supports monitoring and control of actuation of safety-related functions at the system and component levels. Functions implemented on the S-VDU include:

- Process value monitoring
- PAM
- Alarm monitoring
- Maintenance bypass operation
- Bypass status monitoring and inoperable system indication
- Components operation
- Components lockout operation
- Components status monitoring
- Manual operating bypass operation
- System-level manual initiation of RT and ESF functions (via software switches)

Automatic safety function initiations do not depend on the operation of the S-VDU.

Detailed information on the MELTAC S-VDU and S-VDU-P is described in Section 4.2 of the Platform LTR.

MIS

The MISs are hardware manual switches to initiate the RT function, [[
]] in the MCR and RSF.

[[

]]

Refer to Section 4.1.3.5 and 4.1.3.3 of this report for details on the software RT and ESF manual initiation.

MXS

MXS is a hardware device that provides manual transfer of control authority between the MCR and the RSF. MXSs are momentary contact switches without latching capability, generating only transient signals when actuated.

Each CBP (U, X, Y, and Z) is equipped with two MXSs for each channel: one located in the MCR and one located in the RSF. The MXS signals are transmitted from the CBP to the RPP [[

]] This configuration requires the operation of at least two MXSs at a given location to issue a valid enable command.

MCR/RSF disable and enable functions are interlocked so that the new location cannot be enabled prior to disabling the current location. This interlock is applicable to the transfer in either direction.

The enable/disable signal is sent from the RPP to the PCS-CCP. The PSS-CCP receives operational signals from both the S-VDU of the MCR and the S-VDU of the RSF. Then one of them is selected according to the enable/disable signal.

Each MXS input is directly wired to the CBP input modules through isolation devices. This isolation device prevents electrical faults to the CBP caused by a fire outbreak in the MCR or the RSF. MXS signal is also sent to the PCS [[ ]] to transfer control of the PCS between the MCR and RSF.

4.1.4 Testing and Calibration

The integrity of the PSS is tested through both automatic and manual testing. While in service, the PSS performs automatic testing via self-diagnostics. Manual tests can be conducted during plant operation or maintenance without any physical reconfiguration of the PSS. The tests provide overlapping coverage to ensure that the entire PSS is tested. Testing of the PSS is completed in accordance with IEEE Std 338-1987 [8].

Figure 4-13 shows the scope of each test.

Figure 4-13 Testing Scope

[[

]]

4.1.4.1 Self-Diagnostic Testing

The PSS performs self-diagnostic functions that continuously and automatically monitor and detect failures. The self-diagnostic function is described in Sections 4.1.5 and 4.2.3 of the Platform LTR.

The self-diagnosis features of the PSS include the following:

[[

]]

4.1.4.2 Channel Check Test

The channel check test compares signals from redundant sensors and detects any channel that deviates significantly from the others. Signals from sensors U, X, Y, and Z are routed [[ ]] where the channel check algorithm is executed. The algorithm automatically detects deviations, generates alarms, and transmits them to the A-VDU for operator monitoring. This test runs continuously; no operator action is required.

A channel check test confirms the operability of the signal path through the sensor, I/O module, I/O bus, and RPP. The configuration of the channel check test is shown in Figure 4-14.

Figure 4-14 Channel Check Test Configuration

[[

]]

4.1.4.3 Channel Calibration

Channel calibration verifies the accuracy of each CBP input module. The channel of a single parameter under test is placed in maintenance bypass and a reference signal from an external source is injected into the CBP input module. The signal is transmitted from the I/O module to [[ ]] and the operator verifies the indicated value on the S-VDU (or O-VDU).

This test confirms the accuracy of the input module and the operability of [[ ]] The bypass is then cleared, and the steps are repeated for the remaining channels. The configuration of the channel calibration test is shown in Figure 4-15.

Figure 4-15 Configuration of Channel Calibration Test

[[

]]

4.1.4.4 RTB Test

The RTB operability test is conducted using manual testing. The test confirms the operability of the following items by opening each RTB from the S-VDU or the O-VDU:

- Signal path from the RPP I/O module to the ST coil
- Signal path from the RPP I/O module to the UV coil
- Signal path from the RPP I/O module for fail-safe function to the UV coil
- RTB opening operation by energizing the ST coil
- RTB opening operation by de-energizing the UV coil

This test sends two test commands to each RTB. One of the commands energizes the ST coil and the other de-energizes the UV coil. Only one signal is sent at a time so that the operability of the UV coil and the ST coil are confirmed separately.

This test includes fail-safe operability. The fail-safe operability is carried out using four test commands from [[

]]

In this test, the operability of the signal path [[ ]] to the RTB is confirmed. The operation signal is sent [[

]] The operability of [[

]] are also validated.

[[

]]

The configuration of the RTB test is shown in Figure 4-16.

Figure 4-16 Configuration of RTB Test

[[

]]

4.1.4.5 MXS Test

The MXS is a manual test using hardware switch. The operator actuates the MXS and verifies operability by confirming the RPP feedback on the S-VDU. When actuated, the MXS input is

received by the CBP input module, transmitted to the RPP, processed by the RPP central processing unit (CPU), and the MXS signal is transmitted [[ ]] where the switch status is displayed. The MXS test is performed by operating each MXS installed in the MCR and the RSF individually. Voting logic associated with the MXS is described in Section 4.1.3.1 of this report.

The test confirms the operability of the switch, the CBP input module, the CBP CPU, the Data Link between the CBP and the RPP, the RPP CPU, the Safety Bus, and the S-VDU.

The configuration of the MXS test is shown in Figure 4-17.

Figure 4-17 Configuration of MXS Test

[[

]]

4.1.4.6 MIS Test

The MIS is a hardware switch. The operator operates the MIS and confirms its operability by checking the feedback signals from the RPP on the S-VDU. [[

]] These feedback signals are displayed on the S-VDU.

[[

]]

The hardware switches are tested by operating them one by one for all the MISs installed in the MCR and the RSF during periodic testing.

In this test, the operability of the hardware switch, [[
]] is confirmed.

The configuration of MIS test is shown in Figure 4-18.

Figure 4-18 Configuration of MIS Test

[[

]]

4.1.4.7 Component Test

The component test is conducted to verify the operability of components that are not covered by the self-diagnostic function. This test confirms the integrity of the following:

- The analog circuitry of the output module (including the final output device of the module)
- The priority logic between the PSS-CCP and the DAS
- The signal path from the PSS-CCP output module to the component

The test is performed during periodic testing by manually operating the component [[
]]

[[

]]

Figure 4-19 shows the signal flow and feedback during the component test.

Figure 4-19 Signal Flow and Feedback during Component Test

[[

]]

During the test, both the safe state and the non-safe state of the component are manually operated from the VDU.

For each operation, the corresponding feedback signal is confirmed on the VDU display to verify that the PSS-CCP output and input paths function properly. [[

]] Figure 4-20 shows the signal path in the component test.

Figure 4-20 Component Test of Priority Logic between PSS and DAS

[[

]]

This test verifies the operability and integrity of the PSS-CCP output module, the hardwired circuit, and the connected component, and provides evidence of the correct operation of the signal path and feedback loop. The successful completion of this test serves as a prerequisite for the priority test.

4.1.4.8 Priority Test

The priority test (safe-state priority) verifies that the safe-state command generated by the DAS has higher priority than a simultaneous non-safe-state command from the S-VDU.

[[

]]

This test demonstrates the correct implementation of the safe-state priority logic in the PSS-CCP. Figure 4-21 shows the signal route in safe state.

Figure 4-21 Priority Test (Safe State) of Priority Logic between PSS and DAS

[[

]]

4.1.4.9 S-VDU Test

The S-VDU test confirms the operability of the S-VDU touchscreens installed in the MCR or the RSF. For each test, the following are verified to be working correctly:

1) The S-VDU generates signals corresponding to touch operation of the operator.
2) The generated signal is transmitted to the S-VDU-P.
3) Upon receiving the touch-signal, the S-VDU-P processes the signal and generates feedback signal.
4) The feedback signal generated by the S-VDU-P is transmitted to the S-VDU.
5) Feedback signal is displayed on the S-VDU.

The test is described in Section 4.2.4 of the Platform LTR. Figure 4-22 shows the configuration of the S-VDU Test.

Figure 4-22 Configuration of S-VDU Test

[[

]]

4.1.4.10 Memory Integrity Check

[[

]]

4.2 Plant Control System

The PCS is a single division system that provides monitoring for all non-safety-related plant instrumentation, automatic control and component control logic for all non-safety-related plant components and application programs to assist plant operators. [[

]]

The PCS interfaces with the PSS in the following ways:

[[

]]

4.2.1 Signal Selection Algorithm

In some cases, control action must be made based on a process parameter that is also used for protection functions. Rather than using a single sensor that is manually selected by the operator, as is done in many operating plants, the PCS performs a signal selection algorithm on the four measurement channels.

To ensure that failure of a single channel in the PSS does not cause a response in the PCS that could lead to a safety system actuation, the signal selection algorithm is used. The PCS receives four channels from the PSS via the Unit Bus and performs a 2nd-High signal selection algorithm on the four channels. The same 2nd-High signal selection is used by the PSS in cases where a single variable needs to be displayed on the S-VDU. Below is an explanation of how the algorithm functions.

The signal selection algorithm selects and outputs the second highest signal with respect to the input values. A cross-comparison of normal channel input values, excluding that of any excluded signal, is conducted. A channel that deviates from two or more channels is changed to the error state and the condition is alarmed. When one or two channels are in an error state, the second highest signal is output. When three channels are in an error state, the normal channel is output. When all channels are in an error state, the channel selection state of the previous selection state is held. When two or more channels of the normal channels of the previous operation cycle are identified as being in error, only the channel farthest from the average value of the current operation cycle is regarded as in error.

This algorithm design ensures that a single failure of a channel or a channel being taken out for maintenance has no detrimental effect on the PCS control functions.

For cases where RT or ESF demands are used for control signals in the PCS, both PSS divisions independently send their RT and ESF actuation demands to the PCS. Depending on the system function, AND/OR logic is used to combine the demands from both divisions into one control action.

4.3 Diverse Actuation System

The DAS provides diverse, independent monitoring and displays for plant instrumentation and diverse, independent automated actuation and manual control of selected plant components to cope with anticipated operational occurrences (AOOs) and postulated accidents with a concurrent CCF in the PSS.

The DAS performs the following key functions:

[[

]]

4.3.1 Interface between PSS and DAS

The DAS receives instrumentation signals from the PSS to perform its own RT and ESF actuation logic. This interface is described in Section 4.1.8 of the Platform LTR.

[[

]] The prioritization logic within the PIM is described in Section 4.1.3.7 of this report and in Sections 4.1.8 and 4.1.2.4 of the Platform LTR. The component position feedback is transmitted to the DAS through an isolation device.

This interface between PSS and DAS is detailed in Section 5.4.2 of this report.

5.0 FUNDAMENTAL DESIGN PRINCIPLES

5.1 Independence

This section provides the basis for the independence of the PSS in accordance with Clause 5.6 of IEEE Std 603-1991, as required by § 50.55a(h), and in accordance with Clause 5.6 of IEEE Std 7-4.3.2-2016, as endorsed with clarifications by RG 1.152 [9]. These standards define independence requirements between (1) redundant portions of a safety system, (2) safety systems and the effects of a DBE, and (3) safety systems and other systems.

This assessment evaluates how the PSS design satisfies these requirements across the following four aspects of independence:

- Physical independence
- Electrical independence
- Communications independence
- Functional independence

Clause 5.6.2 of IEEE Std 603-1991 specifies that qualification of equipment in accordance with Clause 5.4 of IEEE Std 603-1991 is an acceptable method for demonstrating independence from the effects of a DBE. Since the PSS equipment is qualified under the plant's Environmental Qualification (EQ) Program to meet this requirement, a separate evaluation of DBE-related independence is not addressed in this report.

5.1.1 Physical Independence

The physical independence of the PSS is established in accordance with Clause 5.6.3.2 of IEEE Std 603-1991 and the separation requirements of RG 1.75 [10], which endorses IEEE Std 384-1992 [11] with clarifications.

The design ensures that no single DBE can disable redundant portions of the safety system or cause adverse interactions between safety-related and non-safety-related systems. Physical independence is achieved through (1) spatial separation, (2) qualified structural barriers, and (3) independent routing of power and signal circuits.

The PSS has a four-channel, two-division configuration consisting of Division A and Division B. Each division is installed in a separate safety-related electrical equipment room (SREER) and contains two channelized CBPs, an RPP, a PSS-CCP, and two S-VDU-Ps. Each SREER is designated as an independent fire zone and is qualified as a seismic Category I, safety-related structure.

Non-safety-related equipment is housed in a separate non-safety-related electrical equipment room (NSREER), which is physically separated from the SREERs by qualified structural barriers. The MCR is also isolated from adjacent equipment rooms by qualified structural barriers to prevent fire or environmental propagation.

Within each SREER, the PSS cabinets are arranged to maintain the required physical and electrical independence. Channelized independence within each division is ensured by physical separation of the two CBPs (CBP-U and CBP-X in the Division A SREER, CBP-Y and CBP-Z in the Division B SREER). Each CBP is powered from a dedicated breaker and feeder within the divisional redundant electrical system, and its signal and power cables are routed in separate conduits or trays in accordance with IEEE Std 384-1992. Where spatial limitations occur, qualified barriers are installed. Cable entries and termination panels are segregated to prevent fault or fire propagation between channels.

Separation between systems in the same divisional room is achieved by housing the processors in separate cabinets and segregating their I/O wiring. Inter-processor communication uses fiber-optic connections, which are inherently isolated and require no additional physical separation from current-carrying circuits.

The overall arrangement ensures that within a division, no single internal electrical fault, localized fire, heat source, or mechanical failure can simultaneously disable multiple channels or processors, and that between divisions, no event can propagate across structural or electrical boundaries.

Detailed plant-specific layout drawings and cable routing configurations will be provided in the plant-specific licensing submittal.

5.1.2 Electrical Independence

The PSS achieves electrical independence through dedicated Class 1E power supplies, signal path separation, and electrical isolation between redundant safety divisions and between safety and non-safety systems. The design meets the applicable requirements of Clause 5.6 of IEEE Std 603-1991 and the requirements of RG 1.75 and the endorsed IEEE Std 384-1992.

5.1.2.1 Electrical Independence Between Redundant Portions of PSS

Each redundant portion of the PSS, including all channels and divisions, is designed to operate as an electrically independent unit, from signal acquisition and processing through actuation. Electrical independence is maintained throughout all safety-related portions of the system, ensuring that no credible electrical fault or malfunction in one redundant portion can degrade or disable another, consistent with the criteria of IEEE Std 603-1991 and IEEE Std 384-1992.

Each channel of the PSS employs dedicated Class 1E field instrumentation and CBPs that are not shared with other channels. Each CBP transmits bistable outputs to both divisions' RPP

through unidirectional fiber-optic Data Links, which provide inherent electrical isolation. There is no communication path between CBPs. Each CBP receives power from its associated divisional power group [[ ]] through independent breakers and feeders, but its signal circuits are fully isolated from both divisions and from other channels. This configuration ensures that any electrical transient or fault within one channel cannot propagate to another channel or division.

Each division is powered by an independent divisional Class 1E power supply system. Processors within a division are supplied from dedicated breakers and feeders that are part of the division's redundant electrical supply system, ensuring that a failure of any single feeder or breaker does not propagate to other processors. There is no shared power between Division A and Division B, and no power is shared between processors within a division.

Within each division, the RPP and the PSS-CCP are electrically independent from each other and from the CBPs. Each RPP provides actuation commands to their associated PSS-CCP via the fiber optic Safety Bus, and the PSS-CCPs actuate the divisional ESF components. There are no shared power, control, or I/O circuits between RPPs, PSS-CCPs, or CBPs of different channels or divisions.

The RTB trip signals from the two divisions are combined through a qualified isolation device, providing fail-safe actuation logic while preserving divisional electrical independence, as described in Section 4.1.3.5 of this report.

Cable routing and raceway segregation conform to the physical and electrical separation requirements described in Section 5.1.1 of this report, ensuring that power, control, and instrumentation circuits of redundant channels and divisions are isolated from one another.

These design provisions ensure that any single electrical failure is isolated within the affected redundant portion of the PSS and cannot compromise the operability of other portions.

5.1.2.2 Electrical Independence Between PSS and Non-Safety Systems

Electrical independence between the safety system (PSS) and non-safety systems (PCS and DAS) is achieved through two dedicated and electrically isolated interface mechanisms: (1) one with the PCS [[

]]

The PCS interface utilizes fiber-optic communication, which serves as isolation devices that protect the electrical integrity of the safety system from PCS-originated faults.

For the DAS, electrical isolation is provided by an analog isolation module and a digital isolation device, which are classified as part of the safety system and operate solely [[ ]] This module and device are qualified in accordance with IEEE Std 384-1992 to provide electrical isolation under credible fault conditions. Refer to Sections 4.1.2.3 and 5.5 of the Platform LTR for details on the isolation module and isolation qualification testing.

5.1.2.3 Power Sources

Electrical independence is achieved through independent and redundant power distribution systems. Separate Class 1E power feeds Division A and Division B independently with redundant 120 Vac power, while non-Class 1E power supplies the non-safety systems. A separate Class 1E 120 Vac supply is dedicated to each division, with physical separation maintained between divisions and between safety and non-safety systems. These

configurations conform to IEEE Std 384-1992 by ensuring that electrical faults in non-Class 1E systems do not affect safety systems, and that a fault within one Class 1E safety division does not compromise the independence or operability of the other division. Figure 5-1 illustrates the Class 1E power distribution configuration for the PSS.

Figure 5-1 Class 1E Power Distribution Configuration for PSS

[[

]]

5.1.3 Communication Independence

The PSS communication system is designed to satisfy the independence criteria of Clause 5.6 of IEEE Std 603-1991 and Clause 5.6 of IEEE Std 7-4.3.2-2016. These standards require independence between redundant divisions of the safety system and between safety and non-safety systems. The communication design ensures that faults, malfunctions, or abnormal behavior in one division or in a non-safety system cannot compromise the ability of a safety division to perform its required functions.

5.1.3.1 Communication Design Principles

As discussed in Section 4.1.2 of this report, the PSS employs two inter-division communication interfaces: [[

]] The design of both communication paths incorporates key principles, such as asynchronous architecture, predefined fixed format and structure mapped to predefined locations in the dual port memory (DPM), deterministic operation, communication isolation, no handshaking or interrupts, and software integrity to ensure communication independence, determinism, and fault isolation (see Section 4.3 of the Platform LTR). No software code or executable instructions are transmitted across communication interfaces. All software is stored in non-volatile memory.

5.1.3.2 Communication Independence Between Redundant Portions of PSS

Communication independence among the redundant portions of the PSS, including both channels and divisions, is achieved through the use of the [[ ]], which follows the design principles described in Section 5.1.3.1 of this report. [[

]] is described in Section 0 of this report.

[[

]]

Each CBP performs bistable processing for its own sensor inputs and transmits bistable outputs to both RPP-A and RPP-B through the dedicated [[ ]] No communication occurs between CBPs.

Within each division, the RPP communicates with its associated PSS-CCP via [[

]]

CBPs, RPPs and PSS-CCPs are connected to the [[ ]] for interface with the PCS; however, there is no communication [[

]]

Since all communication interfaces are both electrically and communicationally isolated, any failure or abnormal behavior in one channel or division cannot propagate to another redundant portion of the PSS. Each division's RPP continues to operate independently based on the bistable input data from the four channelized CBPs.

Therefore, [[ ]] and communication architecture provide communication independence, ensuring that a fault or failure in one channel or division does not compromise the safety functions of any other redundant portion.

5.1.3.3 Communication Independence Between PSS and Non-Safety Systems

The PSS communicates with the PCS [[ ]] This network operates on a deterministic scan cycle and employs a full-duplex, dual-ring topology with separate one-way paths for sending and receiving. This architecture ensures communication independence, fault tolerance, and timing predictability.

The PSS Unit Bus interface consists of a CPU module, which executes the safety functions, and a Control Network interface module that manages the Unit Bus communication.

All communication adheres to the design principles described in Section 5.1.3.1 of this report, including asynchronous operation, fixed memory mapping, and non-handshaking transmission. These principles ensure communication independence and deterministic behavior between safety and non-safety systems.

[[

]]

[[

]]

5.1.4 Functional Independence

Functional independence is achieved by ensuring that each safety channel and division perform its required functions independently of other systems, including redundant channels, divisions, and non-safety systems.

Functional independence seeks to prevent safety function failures by ensuring that physically and electrically independent safety channels and divisions (with the exception of coincidence voting) do not depend on information from other independent safety channels and divisions or non-safety systems. Functional independence is achieved by:

1) Making sure safety functions are not inhibited or delayed by other channels and divisions (data independence)
2) Receiving only signals to support or enhance safety functions (communication independence)
3) Keeping effect of the received data within the assumptions/analysis
4) Treating application specific data in an application specific manner [[ ]]

The following subsections describe how the PSS design satisfies these requirements in accordance with Clause 5.6 of IEEE Std 603-1991 and Clauses 5.6 and 5.5.4 of IEEE Std 7-4.3.2-2016.

5.1.4.1 Functional Independence Between Redundant Portions of PSS

The functional independence of the PSS, including both channels and divisions, is achieved through the 2oo4 voting architecture and the fully independent functional design of each redundant portion.

Each CBP operates independently, processing its own sensor inputs, executing bistable logic, and providing bistable outputs to both divisions. No CBP shares processing resources, memory, or logic with other CBPs, ensuring functional independence among channels.

If one CBP or sensor fails, or communication with one channel is lost, the remaining three channels continue to provide bistable results to both RPP-A and RPP-B, allowing each RPP to perform 2oo3 voting without loss of safety function.

Each division contains its own RPP and PSS-CCP, which execute protection and actuation logic independently of the other division. No shared processing, memory, or control logic exists between divisions. Communication between RPP-A and RPP-B is restricted to predefined safety-related signals (see Section 5.1.3.2 of this report).

If one division's RPP fails, the other division's RPP continues to receive bistable outputs from all four CBPs and performs 2oo4 voting, maintaining protective action. If an entire division and its two associated CBPs fail, the remaining division performs 2oo2 voting using the two remaining CBPs and continues to execute the required safety functions.

The PSS architecture satisfies the single-failure criterion (SFC), as a failure at the channel, processor, or division level does not compromise the other redundant portions' ability to execute their required safety functions.

This ensures that both channels and divisions perform their safety functions independently, and that a failure or loss of communication in one redundant portion cannot prevent the others from performing the required safety functions.

RTBs are grouped by division, with RTBs A1 and A2 assigned to Division A, and RTBs B1 and B2 to Division B. Each RTB can be tripped either by energizing the ST coil or by de-energizing the UV coil. The trip logic is executed independently within each division, and RT can be achieved by opening both RTBs in one division without reliance on the other. In the event of dual-division failure, fail-safe modules in both RPPs ensure trip activation by removing power from the UV coils.

5.1.4.2 Functional Independence Between PSS and Non-Safety Systems

[[

]]

PCS Interface

[[

]]

DAS Interface

The PSS maintains functional independence from the DAS. The DAS receives redundant process signals and component status inputs from the PSS for diverse actuation and monitoring purposes. To mitigate the effects of single-point failures, the DAS implements 2oo4 voting logic before generating actuation signals.

Actuation outputs from the DAS are transmitted to the PIM within the PSS-CCP via qualified isolation devices. [[

]]

[[

]]

This mechanism ensures that functional independence is maintained, and that a single system fault does not compromise the safety function of the component.

5.2 Redundancy

The PSS is designed with a multilayered redundancy architecture to satisfy the SFC, as defined in GDC 21, GDC 24, Clause 5.1 of IEEE Std 603-1991, Clause 5.1 of IEEE Std 7-4.3.2-2016, and IEEE Std 379-2000 [12]. These regulatory criteria require that the loss or malfunction of any single component or subsystem must not prevent the execution of required safety functions during DBEs, and that the system must remain testable without compromising redundancy.

Section 5.1 of this report describes that the four-channel, two-division configuration of the PSS has physical, electrical, communication, and functional independence. The combination of independence and redundancy provides the basis for demonstrating that the PSS satisfies the SFC in accordance with the applicable regulatory standards.

A complete set of failure modes and effects analysis (FMEA) for all system components will be developed and submitted as part of the plant-specific licensing submittal.

The following sections describe how the redundancy features ensure that no single failure prevents the required safety functions from being performed and how all single failures are identifiable through testing or diagnostics.

In future licensing submittals, plant-specific analyses will be required to demonstrate that, for each DBE identified in the plant's licensing basis, the safety system performance can be achieved relying on only a single division of the PSS.

5.2.1 Redundant Configuration

The PSS is configured with a four-channel, two-division architecture, in which both the channels and divisions are designed to operate independently to perform the required safety functions. Dedicated processors, logic, actuation devices, and power supplies are provided for each redundant portion, ensuring physical, electrical, communication, and functional independence. Section 4.1.1 of this report provides a detailed configuration description of the PSS.

5.2.1.1 Channel-Level Redundancy

The PSS incorporates four redundant and independent protection channels, designated as Channels U, X, Y, and Z, [[

]]

Each channel provides a physically and electrically isolated signal path from the sensor to the bistable output. System behavior under channel failures is discussed in Section 5.2.2.1 of this report.

5.2.1.2 Division-Level Redundancy

Divisions A and B are designed in accordance with Clause 5.6.1 of IEEE Std 603-1991, Clause 5.6.1 of IEEE Std 7-4.3.2-2016, and IEEE Std 379-2000 to provide electrical, functional, and physical redundancy.

Each division is equipped with its own power supplies, I/O modules, Control Network (Safety Bus), processors, and actuation paths, and is located in a separate SREER to prevent common-cause vulnerabilities.

Two divisions operate concurrently and independently in executing their safety functions. Either division can independently execute RT and ESF actuation upon valid input conditions, ensuring that the loss or failure of one division does not affect the operation of the other.

[[

]] System behavior under division failure is described in Section 5.2.2.3 of this report.

5.2.1.3 RTB Redundancy

The RTB serves as the final actuation device for the RT function. The PSS employs a division-based redundant RTB configuration. Division A operates RTBs A-1 and A-2, while Division B operates RTBs B-1 and B-2. Each RTB is controlled through independent trip logic, digital output channels, and Class 1E power supplies. The RTBs are equipped with both ST and UV coils to support independent actuation paths and fail-safe functionality. System response to RTB failures is discussed in Section 5.2.2.3 of this report.

5.2.1.4 Electrical Power Redundancy

Each division is equipped with two redundant power sources, and each power source is designed to supply uninterrupted power and batteries to Class 1E loads under normal and abnormal operating conditions, including DBEs.

Within each division of the PSS, the power supply module for each subsystem in the division is configured redundantly. The redundant power supply modules distribute power to the CPU and I/O chassis. See Figure 5-1 of this report for the Class 1E power distribution configuration for the PSS. System behavior under power supply failures is described in Section 5.2.2.5 of this report.

5.2.2 System Response to Single Failures

The PSS is designed to meet the SFC in accordance with GDC 21, GDC 24, Clause 5.1 of IEEE Std 603-1991, Clause 5.1 of IEEE Std 7-4.3.2-2016, and IEEE Std 379-2000. These regulatory criteria state that no single failure shall prevent the performance of required safety functions during DBEs, and that the system must remain testable without compromising redundancy.

Section 5.2.1 of this report describes how redundancy is architecturally implemented at multiple levels (channels, divisions, processors, RTBs, and power). This section explains how those features ensure that representative single failures are tolerated in a manner consistent with the SFC.

5.2.2.1 Single Channel Failure

Sensor Failure

In the event of a single measurement sensor failure, the abnormality is detected through the channel-check algorithm and continuous self-diagnostics performed within each CBP during normal operation. Upon detection, the failed channel is bypassed, and an alarm is issued to the operator. The voting logic in the RPP automatically transitions from the 2oo4 configuration to a 2oo3 voting configuration based on the remaining three valid bistable inputs, ensuring that the protective function is maintained without operator action. This automatic reconfiguration satisfies the SFC by ensuring that actuation logic does not rely on a failed or bypassed channel.

CBP Failure

The CBPs consist of four independent processors, each performing bistable processing using its own dedicated sensor inputs. Since each CBP operates independently and does not communicate with other CBPs, failure in one CBP does not affect the operation or bistable outputs of the remaining redundant channels.

If a single CBP fails, the three unaffected CBPs continue transmitting valid bistable outputs to both RPP-A and RPP-B through unidirectional Data Links. The RPP performs 2oo3 voting, ensuring that the safety function is maintained in compliance with the SFC. The abnormal condition is detected by self-diagnostics, and the failed channel is bypassed in the voting logic. An alarm is generated to alert the operator.

Maintenance Bypass

Each division of the RPP independently supports the maintenance bypass function. Bypass commands are issued [[ ]] and are internally validated by [[

]]

5.2.2.2 Single RPP Failure

The RPPs are configured redundantly across the two divisions. Even if the RPP in one division fails, the RPP in the other division continues to receive bistable outputs [[ ]] and independently performs 2oo4 voting to determine the required RT or ESF actuation.

Since the RPPs are configured to have physical, electrical, communication, and functional independence, failure in one division's RPP does not affect the operation or protective capability

of the other division. Therefore, a single RPP failure does not impair the safety function of the PSS.

5.2.2.3 Single Division Failure

In the event of a complete failure of one division, the remaining division retains the capability to perform all required safety functions. Divisions A and B have physical, electrical, communication, and functional independence, with separate power supplies, I/O modules, Safety Buses, and processors. Within each division, processor redundancy is provided [[ ]] ensuring that a single processor fault is automatically managed without impairing the division's functionality.

[[

]]

This configuration ensures that the failure of one division does not compromise the safety functions of the other.

Each division is also equipped with two RTBs, each with independent trip logic, output channels, and ST/UV coils supplied from dedicated Class 1E power. A failure in one coil, output path, or even an entire breaker does not prevent trip capability, as the redundant coil or breaker provides an alternative actuation path. The UV coil design incorporates a passive fail-safe mechanism, such that the loss of control power results in an automatic breaker trip. This architecture provides assurance of reliable operation under single-failure conditions of control logic, output channels, or trip coils. Through division-level redundancy, dual actuation paths, and passive trip logic, the design satisfies the redundancy and fail-safe requirements. See Section 4.1.3.5 of this report for details on the RT function.

Accordingly, even with processors or RTB faults in one division, the unaffected division remains capable of executing the required safety functions independently.

5.2.2.4 Non-Safety System Failure

The PSS is designed to provide assurance that failures originating in the PCS and the DAS cannot compromise the ability of the PSS to perform its required safety functions. This is consistent with GDC 24, which requires separation of protection and control functions, and with IEEE Std 603-1991 and IEEE Std 379-2000 requirements for functional independence.

[[

]]

5.2.2.5 Electrical Power Failure

The evaluation of power-related failures in this section is limited to the internal I&C power supply system of the PSS. Failures originating from external power sources or station-level Class 1E power supply interfaces are addressed in the plant's electrical power system analysis and are outside the scope of this section.

Each division of the PSS receives redundant 120 Vac Class 1E power from the station power distribution system. These redundant feeds provide assurance that the loss of a single 120 Vac source does not impact on the operability of the PSS. The interface between the Class 1E power sources and the PSS internal supply modules, including the redundant 120 Vac inputs to each division, is illustrated in Figure 5-1 of this report.

Within each PSS cabinet, the internal I&C power supply system is designed with redundant supply modules for the redundant CPUs and with redundant supply modules equipped with automatic auctioneering circuits for the I/O chassis. If one module or distribution path fails, the alternate module automatically continues to provide uninterrupted power to the CPUs, I/O chassis, and actuation logic within the division. This design eliminates single points of vulnerability and ensures that a single internal supply failure does not impair the ability of the division to perform required safety functions.

Accordingly, even with the loss of one internal power supply module, the redundancy of the internal I&C power supply system ensures that the PSS continues to perform all required safety functions.

5.2.2.6 Shared Component Failure

Consistent with Clause 5.6 of IEEE Std 379-2000, both shared and non-shared system failures must be evaluated. Non-shared failures within each redundant portion of the PSS are addressed in Sections 5.2.2.1 through 5.2.2.5 of this report, which demonstrate that such failures are isolated within the affected redundant portion while the other channel or division continues to perform all required safety functions.

This section addresses failures in components shared either between redundant safety portions of the PSS or between the PSS and non-safety systems. [[

]] Each of these components has been evaluated to verify that a single failure does not compromise the performance of required safety functions.

Sensor

The PSS shares its process-protection parameters with the PCS [[ ]] to keep operators and the PCS working with a consistent data set. In the PCS-CCP, the signal selection algorithm processes the four measurement channel inputs to determine a single representative value for PCS control and indication, as discussed in Section 4.2.1 of this report. This prevents a single spurious or failed channel from causing erroneous PCS control actions that could lead to unnecessary PSS actuation. All selection processing is performed in the PCS and does not affect the PSS actuation logic or independence.

Process parameters required by the DAS are passively shared from all PSS CBPs. The signals are distributed at the PSS distribution modules upstream of any digital processing and then provided to the DAS as hardwired inputs via PSS isolation modules. This arrangement maintains electrical independence between the PSS and the DAS.

Data Link Failure

[[

Unit Bus Failure

[[

]]

See Section 5.1.4 of this report for additional details on functional independence.

Distribution Module Failure

Each sensor signal is routed through a dedicated distribution module, which replicates the signal to both the PSS and the DAS. A failure of a distribution module affects only the single associated channel. After bypassing the channel, the system compensates for this failure by automatically transitioning the voting logic from 2oo4 to 2oo3, thus maintaining the ability to generate a protective action based on the remaining three inputs. Because each module is dedicated to a single channel, a single module failure does not propagate to other inputs or divisions.

PIM failure

The PIM receives control commands [[

]]

5.2.3 Testability

The PSS is equipped with extensive testing capabilities so that all single failures are detected. These capabilities are achieved through a combination of continuous self-diagnostics, channel check functions, periodic manual surveillance tests, and channel calibration. Since these testing methods are implemented with overlapping and complementary coverage to prevent gaps in

detection coverage, design features provide assurance that undetectable failures are eliminated within the architecture. See Section 4.1.4 of this report for details on testing and calibration.

This section describes the layered testability concept of the PSS to ensure that all single failures are either detected or managed without impairing the execution of required safety functions. Accordingly, the testability features support and demonstrate compliance with the SFC.

5.2.3.1 Automatic Testing

Automatic testing functions operate continuously during normal plant operation. These include hardware-based and software-based self-diagnostics, watchdog timers (WDTs), memory status checks, and feedback verification of input and output signals. The channel check functions compare signals from redundant channels to identify abnormal deviations. Any detected fault generates an alarm, and critical errors trigger automatic transfer of functions to the redundant processor within the same division. Details on testing information are provided in Sections 4.1.5 and 4.2.3 of the Platform LTR.

5.2.3.2 Manual Surveillance and Calibration

Periodic manual testing supplements automatic diagnostics for components not continuously monitored, such as the RTBs, MXSs, MICs, component tests, and operator interface devices. Channel calibration is performed at defined intervals to verify accuracy of input modules. During calibration or maintenance testing, the affected channel is placed in maintenance bypass.

5.2.3.3 Maintenance Bypass [[ ]]

The maintenance bypass function allows safe removal of a channel or component from service without impairing redundancy. [[

]]

5.2.3.4 Cascade Failure Review

Consistent with Clause 5.3 of IEEE Std 379-2000, the PSS architecture is designed with physical, electrical, communication, and functional independence (see Section 5.1 of this report), [[ ]] automatic isolation features, and periodic testing to ensure that a single fault does not propagate to other components. As a result, no cascade failures are introduced.

5.3 Predictability and Repeatability

The PSS is structured to support predictable and repeatable execution of credited safety functions, in accordance with the requirements of Clauses 5.2 and 5.5 of IEEE Std 603-1991 and the guidance provided in RG 1.152. To achieve this, the system employs fixed-cycle processing, a deterministic communication architecture, and timing allocations verified through architectural modeling and system testing.

This section outlines the following aspects of the system design that support predictable and repeatable behavior:

- Allocation of response time margins for credited safety functions
- Deterministic behavior in processing and communication
- Identification and mitigation of design-level factors that may impact consistent logic execution

5.3.1 Response Time Allocation for Safety Functions

The PSS defines the processing of input signals and the generation of corresponding actuation outputs. The total response time, excluding inherent sensor delay, is defined as the time measured from the sensor output, through the PSS processing time, to the actuation at the field device.

For RT functions, the timing path consists of four defined time delay (TD) stages, as illustrated in Figure 5-2.

[[

]]

Figure 5-2 Signal Path and Time Allocation for RT

[[

]]

For ESF actuation, the signal path includes only TD1 and TD2, as the actuation results in direct electrical output to field equipment as illustrated in Figure 5-3.

[[

]]

Figure 5-3 Signal Path and Time Allocation for ESF Actuation

[[

]]

The limiting response time for RT and ESF actuation functions is defined based on the system design basis. Within the limit, an appropriate portion is allocated to internal processing, including I/O operations, CPU execution, and the Data Link. This allocation approach ensures deterministic and predictable execution of safety functions in accordance with the SMR-300 I&C system requirements. The detailed timing allocation values will be provided in future plant-specific licensing documentation.

The timing segments in Figure 5-2 and Figure 5-3 are described in the architectural timing model of the I&C system, as outlined in Section 5.3.2 of this report, and are used to confirm that system execution remains within the deterministic timing constraints required for safety function performance.

5.3.2 Deterministic System Response

The PSS is designed to execute safety functions through a fixed-cycle and time-bounded logic structure. Safety-related input signals are processed within a predefined sequence of processing steps that ensure consistent system behavior under all credited operating conditions. Refer to Sections 4.4.1 and 4.4.2 of the Platform LTR for fundamental cycle and application processing time details.

Within the CBP, the RPP, and the PSS-CCP, safety logic is executed cyclically with time constraints allocated to each processor. The processing follows a predefined sequence of input acquisition and bistable logic in the CBP, 2oo4 voting and RT actuation in the RPP, and control logic processing and component control output generation in the PSS-CCP. These operations are performed within a predetermined execution time frame defined for each processor cycle.

[[

]]

The internal timing allocation for these cycles is derived from the MELTAC platform's time budget model, as described in Section 4.4 of the Platform LTR. This allocation encompasses the timing contributions from analog and digital input processing, communication buffering, CPU logic execution, and inter-processor data exchange.

In addition to logic determinism, the system maintains timing predictability in data communication through a structured and isolated architecture. [[

]] These design features ensure bounded and repeatable data exchange and support the overall deterministic behavior of the PSS.

5.3.3 Design-Level Factors Affecting Predictable Logic Execution

The PSS addresses design-level factors that may affect predictable and repeatable execution of safety functions. These factors are categorized into four areas: processing-level factors, configuration and resource-related factors, communication and data consistency factors, and non-safety interface factors. Each category is mitigated through system architecture, communication design, and diagnostic strategies.

- Processing-level factors, such as timing uncertainty, complex logic, and event-driven behavior, are mitigated through fixed-cycle CPU execution. Safety logic (e.g., bistable logic, 2oo4 voting, RT/ESF actuation) is executed [[

]]

- Configuration and resource-related factors, such as runtime reconfiguration or online modification of safety-related logic and parameters settings, are prevented by design. In addition, [[

]]

- Communication and data consistency factors, such as stale or inconsistent data due to sensor delays or communication faults, and undetected latent failures across safety divisions or non-safety systems, are mitigated by the communication architecture as described in detail in Section 5.1.3 of this report. [[

]]

- Non-safety interface factors, such as spurious manual actuation signals and unpredictable communication anomalies (e.g., delays, malformed data, or signal interference), are mitigated through architectural isolation, [[

]]

5.4 Diversity and Defense-in-Depth

The SMR-300 I&C Architecture includes features to mitigate the impact of a CCF on the PSS. A diversity and defense-in-depth (D3) assessment following BTP 7-19 [13] and the guidelines in NUREG/CR-6303 [14] is performed to identify portions of the architecture susceptible to software CCF and identify alternate means of accomplishing safety functions in the presence of a software CCF. A plant-specific D3 analysis will be provided in future licensing submittals.

5.4.1 Echelons of Defense

As defined in Section 2.2 of NUREG/CR-6303, the “echelons of defense” are specific applications of the principle of defense-in-depth to the arrangement of I&C systems for the purpose of operating the plant or shutting down. All four echelons depend on the sensors to determine when to perform their functions, and the safety concern is to ensure that no more than one echelon is disabled by a common sensor failure.

5.4.1.1 Control System Echelon

The PCS automatically controls the non-safety components of the plant and can be manually operated from the MCR or RSF. The PCS provides controls and maintains the plant within the operating conditions. The PCS is not credited for safety actuation and is not relied upon for the performance of any PSS safety function.

5.4.1.2 RT Echelon

The PSS provides automatic and manual means to demand an RT that causes the control rods to shut down the reactor. To mitigate a software based CCF, the DAS also provides a diverse means for automatically and manually initiating an RT.

5.4.1.3 ESF Actuation System Echelon

The PSS provides automatic and manual means to initiate ESF functions. To mitigate a software based CCF, the DAS also provides a diverse means for automatically and manually initiating ESF functions.

5.4.1.4 Monitoring and Indication Echelon

The PSS-HSI provides monitoring and indication and supports manual actions, but is not credited for automatic actuation. To mitigate a software based CCF, the D-HSI on the DAS console provides a diverse monitoring/indication means.

5.4.2 PSS and DAS Interfaces

The SMR-300 I&C design conservatively assumes that a digital CCF removes the entire functionality of the PSS, [[

]] Under this assumption, the design implements the DAS to ensure the plant can be brought to and maintained in a safe, stable state even when safety functions of the PSS are unavailable. The PSS uses a microprocessor-based platform (MELTAC-Nplus S) executing digital safety logic,

whereas the DAS is hardwired, analog-only with no microprocessors, software, or firmware. This technological split prevents digital failure mechanisms (i.e., software errors, CPU faults, digital CCF) from propagating to the DAS.

The CCF's affected boundary of impact encompasses all safety functions performed by the PSS, including associated logic and output paths. In contrast, the input path to the DAS is outside the affected boundary. Input signals from sensors are branched [[

]]

Figure 5-4 is a functional block diagram of the signal input applied to the CBP and the DAS interface.

Figure 5-4 Signal Input – CBP and DAS Interface

[[

]]

The DAS independently controls selected plant components regardless of PSS outputs. [[

]]

Figure 5-5 illustrates a functional block diagram of the signal output applied to the PSS-CCP and the DAS interface.

Figure 5-5 Signal Output – PSS-CCP and DAS Interface

[[

]]

6.0 REFERENCES

[1] Mitsubishi Electric Corporation, "Safety System Digital Platform - MELTAC - Topical Report," JEXU-1041-1008-P(R2)-A, May 2019 (ADAMS Accession No. ML19135A097).

[2] Mitsubishi Electric Corporation, *Safety System Digital Platform - MELTAC - Topical Report,* JEXU-1041-1008-P(R3), June 2023 (ADAMS Accession No. ML23167C171).

[3] USNRC, "Draft Safety Evaluation by the Office of Nuclear Reactor Regulation for Mitsubishi Electric Corporation's Topical Report, Revision 3 'Mitsubishi Electric Total Advanced Controller Platform' Phase 1," July 2025, (ADAMS Accession No. ML25139A555).

[4] Institute of Electrical and Electronics Engineers, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," IEEE Std 603-1991, June 1991.

[5] Institute of Electrical and Electronics Engineers, "IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations," IEEE Std 7-4.3.2-2016, January 2016.

[6] USNRC, "Safety Review of Light-Water Power Reactor Construction Permit Applications," DNRL-ISG-2022-01, October 2022.

[7] USNRC, "Bypassed an Inoperable Status Indication for Nuclear Power Plant Safety Systems," RG 1.47 Rev. 1, February 2010.

[8] Institue of Electrical and Electronics Engineers, "IEEE Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems," IEEE Std 338-1987, August 1988.

[9] USNRC, "Criteria for Programmable Digital Devices in Safety-Related Systems of Nuclear Power Plants," RG 1.152 Rev. 4, July 2023.

[10] USNRC, "Criteria for Independence of Electrical Safety Systems," RG 1.75 Rev. 3, February 2005.

[11] Institute of Electrical and Electronics Engineers, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits," IEEE Std 384-1992, June 1992.

[12] Institute of Electrical and Electronics Engineers, "IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," IEEE Std 379-2000 (R2008), March 2008.

[13] USNRC, "Guidance for Evaluation of Defense in Depth and Diversity to Address Common-Cause Failure Due to Latent Design Defects in Digital Instrumentation and Control Systems," BTP 7-19 Rev. 9, May 2024.

[14] Lawrence Livermore National Laboratory, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," NUREG/CR-6303, December 1994.