ACKNOWLEDGEMENTS AND DISCLAIMERS

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

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

Copyright Holtec International © 2022, all rights reserved

Revision Log

Revision	Description of Changes
0	Initial Issue.
1	Minor changes and additions made to Sections 2.1 and 3.1.2 based on NRC staff feedback during the pre-application meeting held on October 4, 2022.

Copyright Holtec International © 2022, all rights reserved

Executive Summary

This White Paper is written to describe the SMR-160 I&C Architecture for explanatory purposes with the NRC. This is part of the pre-application activities that support the development of a construction permit application (CPA) as part of a two-step license approach under Title 10 of the Code of Federal Regulations (CFR) Part 50, "Domestic licensing of production and utilization facilities". The objective is to familiarize NRC staff with the I&C design of the SMR-160 and solicit feedback on the compliance of the design with applicable regulations and identify any areas that the NRC identifies may be higher potential licensing risk that require a more thorough discussion.

Copyright Holtec International © 2022, all rights reserved

Table of Contents

1.0 Introduction 6
1.1 Purpose 6
1.2 Objective 6
1.3 Abbreviations 6
2.0 I&C Architecture 8
2.1 Overview 8
2.2 Plant Safety System 10
2.3 Diverse Actuation System 12
2.4 Plant Control System 14
2.5 Human System Interface 14
3.0 Key Design Features 18
3.1 Communication Networks 18
3.2 Enhanced Voting Logic 21
3.3 Fail Safe Design 27
3.4 [[ ]] 27
3.5 [[ ]] 28
3.6 Capability for Testing and Calibration 34
4.0 References 35

Copyright Holtec International © 2022, all rights reserved

List of Figures

Figure 2-1 SMR-160 I&C/HSI Architecture 9
Figure 2-2 PSS Configuration 11
Figure 2-3 DAS Configuration 13
Figure 2-4 Main Control Room Mockup 15
Figure 3-1 DAS Instrument Interface 21
Figure 3-2 DAS Component Interface 21
Figure 3-3 2oo4 Voting Logic 22
Figure 3-4 One Measurement Channel Failure 23
Figure 3-5 Two Measurement Channel Failures, One in Each Division 24
Figure 3-6 Two Measurement Channel Failures, in a Single Division 24
Figure 3-7 Interdivisional Communication Failure in One Division 25
Figure 3-8 Interdivisional Communication Failure in Both Divisions 25
Figure 3-9 [[ ]] 26
Figure 3-10 RTB Configuration 27
Figure 3-11 Maintenance Bypass Interlock Logic 30
Figure 3-12 [[ ]] 31
Figure 3-13 [[ ]] 32
Figure 3-14 [[ ]] 33
Figure 3-15 [[ ]] 33
Figure 3-16 [[ ]] 34

Copyright Holtec International © 2022, all rights reserved

1.0 INTRODUCTION

1.1 Purpose

The purpose of this whitepaper is to describe the design of the SMR-160 I&C systems. The I&C systems used for the SMR-160 are based on platforms developed by Mitsubishi Electric Corporation (MELCO). MELCO submitted the Safety System Digital Platform - MELTAC - Topical Report [1] to the NRC to obtain approval of the MELTAC Nplus S platform for use as a safety related I&C system in a nuclear power plant. This document will be referred to as the MELTAC Topical Report throughout this document. The METAC Topical report received a safety evaluation for use in Class 1E applications via the Safety Evaluation for Mitsubishi Electric Total Advanced Controller (MELTAC) Platform Topical Report and Supporting Documents [2], which is referred to as the MELTAC Safety Evaluation throughout this document.

This whitepaper will describe the system architecture used for the design in the I&C systems including: [[

]]

- Other features with an impact on licensing

1.2 Objective

The objective is to familiarize NRC staff with the I&C design of the SMR-160 and solicit feedback on the compliance of the design with applicable regulations and identify any areas that the NRC identifies may be higher potential licensing risk that require a more thorough discussion.

1.3 Abbreviations

AOO	Anticipated Operational Occurrences
ATWS	Anticipated Transient Without Scram
CCP	Component Control Processor
CCF	Common Cause Failure
DAS	Diverse Actuation System
DPP	Diverse Protection Processor
EIS	Excore Instrumentation System
EOP	Emergency operating Procedure
ESF	Engineered Safety Feature
HSI	Human System Interface
I&C	Instrumentation and Control
LCO	Limiting Condition for Operation
LDP	Large Display Panel
[[	]]
MB	Maintenance Bypass

Copyright Holtec International © 2022, all rights reserved

MCR	Main Control Room
MELCO	Mitsubishi Electric
MELTAC	Mitsubishi Electric Total Advanced Controller
MIS	Manual Initiation Switch
MXS	Master Transfer Switch
OB	Operating Bypass
PA	Postulated Accident
PAM	Post-Accident Monitoring
PCS	Plant Control System
PSS	Plant Safety System
RMS	Radiation Monitoring System
RPP	Reactor Protection Processor
RSF	Remote Shutdown Facility
RT	Reactor Trip
RTB	Reactor Trip Breaker
SDCV	Spatially Dedicated, Continuously Visible
SFC	Single Failure Criteria
ST	Shunt Trip
UV	Under Voltage
VDU	Visual Display Unit
2oo3	Two Out of Three
2oo4	Two Out of Four

Copyright Holtec International © 2022, all rights reserved

2.0 I&C ARCHITECTURE

2.1 Overview

The entirety of the I&C and human-system interfaces (HSI) for the SMR-160 is called the SMR-160 I&C/HSI, and it is developed by MELCO. The SMR-160 I&C/HSI design described in this document is based on the requirements for the control and safety of the SMR-160, industry codes and standards, and applicable regulations.

The SMR-160 I&C/HSI is comprised of three integrated digital systems that operate independently. Each system has its own HSI.

The Plant Control System (PCS) indirectly monitors safety plant instrumentation, directly monitors all non-safety plant instrumentation, and controls all non-safety plant components to keep the plant within safety parameters. [[

]] The PCS is comprised of one non-safety-related division designated by the purple dash line shown in Figure 2-1.

Plant Safety System (PSS) monitors all safety plant instrumentation and has automatic and manual initiation for reactor trip (RT) and engineered safety features (ESF). The PSS is the credited Class 1E system to mitigate design basis accidents (DBAs) and achieve safe shutdown. Each Division of the PSS is powered from separate divisions of Class 1E power distribution of the SMR-160. [[

]] for RG 1.97 Type B and C variables. The SMR-160 design has no Type A variables. The PSS is comprised of two independent safety divisions designated by the red dash line shown in Figure 2-1.

Diverse Actuation System (DAS) monitors safety instrumentation and controls safety and non-safety components to mitigate DBAs and achieve safe shutdown, with a concurrent common cause failure (CCF) in the PSS. DAS also includes ATWS mitigation functions. [[

]] The DAS is comprised of one non-safety division designated by the blue dash line shown in Figure 2-1.

Copyright Holtec International © 2022, all rights reserved

[[

]]

Figure 2-1 SMR-160 I&C/HSI Architecture

Copyright Holtec International © 2022, all rights reserved

2.2 Plant Safety System

The PSS provides monitoring and displays for all safety related plant instrumentation, automated actuation, and manual control of all safety related plant components. The PSS generates Reactor Trip (RT) and Engineered Safety Feature (ESF) protective functions. Additionally, the PSS provides Post Accident Monitoring (PAM) indication to meet Regulatory Guide 1.97 [3] requirements.

The PSS is based upon the MELTAC Nplus S platform, which has received generic approval for reactor protection use from the NRC via the MELTAC Safety Evaluation [2]. [[

]]

[[

]] The digital signal is compared to an applicable RT or ESF setpoint and if exceeded, the bistable logic for that channel is satisfied. [[

]]

The major components and subsystems of the PSS and their interconnections are shown in Figure 2-2. Each division contains the following major components and sub systems: [[

]]

The reactor trip signals from each division are sent to its respective Reactor Trip Breakers (RTB). [[

]] Each circuit breaker opens by de-energizing the Under Voltage (UV) coil or energizing the Shunt (ST) coil. [[

]]

Copyright Holtec International © 2022, all rights reserved

[[

]]

Figure 2-2 PSS Configuration

Copyright Holtec International © 2022, all rights reserved

2.3 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 AOO and PA with a concurrent CCF in the PSS. [[

]] It also performs ATWS functions as required to meet 10 CFR 50.62 requirements. The DAS uses a single division configuration containing the following major components (reference Figure 2-3): [[

]]

The DAS is powered by redundant non-safety-related power sources. These power sources each originate from a UPS, which is backed-up by the SMR-160 non-safety-related station battery and a non-safety-related diesel generator. The two power sources allow the DAS to remain powered during maintenance of components (e.g., power supply, inverter, battery) on either power source.

[[

]]

[[

]]

[[

]]

[[

]]

Copyright Holtec International © 2022, all rights reserved

[[

]]

Figure 2-3 DAS Configuration

Copyright Holtec International © 2022, all rights reserved

[[

]]

Differences in the SMR-160 I&C design from that outlined in the MELTAC Topical Report relate to the interface between the PSS and DAS and are as follows: [[

]]

2.4 Plant Control System

The PCS is a single division system that provides indirect monitoring of plant safety instrumentation, 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: [[

]]

2.5 Human System Interface

The HSI in the MCR consists of the following major equipment, which is shown in an example mockup in Figure 2-4: [[

]]

Copyright Holtec International © 2022, all rights reserved

[[

]]

Figure 2-4 Main Control Room Mockup

Copyright Holtec International © 2022, all rights reserved

The Safety Console [[

]] perform the following key functions:

1. Receive Plant measurement channel values and the Initiation, Actuation, and Bypass statuses [[ ]].
2. Receive the component and interlock status [[ ]]
3. Receive touch commands [[ ]] for display screen navigation.
4. Receive touch commands [[ ]] for manual component controls and transmit the control commands [[ ]]
5. Receive touch commands [[ ]] for RT and ESF Resets, Operating Bypass Initiation, Maintenance Bypass and transmit the commands [[ ]]
6. Provide spatially dedicated, continuously visible (SDCV) screen to display process value for accident monitoring parameters defined as Type B in IEEE Std. 497 [5].

The Operator Console is the primary interface used for all monitoring and control of the plant. It consists of: [[

]]

The operating crew utilizes the Large Display Panel which continuously displays main plant parameters to collaboratively monitor plant operation.

[[

]]

[[

]]

[[

]]

Copyright Holtec International © 2022, all rights reserved

2.5.1 Manual Initiation Switches

The Main Control Room (MCR) and the Remote Shutdown Facility (RSF) are equipped with conventional switches to manually initiate RT and the system-level ESF Actuation function. These Manual Initiation Switches (MIS) are provided for each ESF function.

[[

]]

[[

]]

The ESF Actuation signal is generated by 2oo4 voting logic from the signals of MIS-U, MIS-X, MIS-Y and MIS-Z. MISs are also used for the reactor trip function. [[

]]

2.5.2 Master Transfer Switches

[[

]]

[[

]]

[[

]]

[[

]]

Copyright Holtec International © 2022, all rights reserved

[[

]]

3.0 KEY DESIGN FEATURES

3.1 Communication Networks

The MELTAC Topical Report [1] describes the various communication networks utilized in the SMR-160 I&C Systems, which are also listed below. How each of these is deployed for the SMR-160 is described in the follow-on sections. [[

]]

3.1.1 Safety Bus

[[

]]

3.1.2 Unit Bus

[[

]]

[[

]]

Copyright Holtec International © 2022, all rights reserved

[[

]]

[[

]]

[[

]]

[[ ]]

[[

]]

[[

]]

[[

]]

[[

Copyright Holtec International © 2022, all rights reserved

]]

3.1.3 Data Link

[[

]]

3.1.4 Maintenance Network

[[

]]

3.1.5 DAS I/O Bus

[[

]]

[[

]]

Copyright Holtec International © 2022, all rights reserved

[[

]]

Figure 3-1 DAS Instrument Interface

[[

]]

Figure 3-2 DAS Component Interface

3.2 Enhanced Voting Logic

3.2.1.1 Two Out of Four Voting

[[

Copyright Holtec International © 2022, all rights reserved

]]

[[

]]

Figure 3-3 2oo4 Voting Logic

[[

]]

[[

]]

Copyright Holtec International © 2022, all rights reserved

In addition, this logic also prevents spurious actuation due to a single measurement channel failure. Actuating safety functions based on all four signals, [[

]]

The 2oo4 enhanced voting logic is reconfigured in the following manner [[

]]

[[ ]] **Figure 3-4 One Measurement Channel Failure**	[[ ]]

Copyright Holtec International © 2022, all rights reserved

[[ ]] **Figure 3-5 Two Measurement Channel Failures, One in Each Division**	[[ ]]

[[ ]] **Figure 3-6 Two Measurement Channel Failures, in a Single Division**	[[ ]]

Copyright Holtec International © 2022, all rights reserved

[[ ]] **Figure 3-7 Interdivisional Communication Failure in One Division**	[[ ]]

[[ ]] **Figure 3-8 Interdivisional Communication Failure in Both Divisions**	[[ ]]

Copyright Holtec International © 2022, all rights reserved

3.2.1.2 Two out of Four plus One out of Two Voting logic

[[

]]

[[

]]

[[

]]

Figure 3-9 [[ ]]

Copyright Holtec International © 2022, all rights reserved

3.3 Fail Safe Design

The Reactor Trip function is fail-safe, as required by GDC 23. Under the following conditions the RTBs will trip the reactor: [[

]]

To enhance reliability and prevent spurious reactor trip the following configuration is used for the Reactor Trip circuit (reference Figure 3-10): [[

]]

[[

]]

[[

]]

Figure 3-10 RTB Configuration

3.4 [[ ]]

[[

]]

[[ ]]

Copyright Holtec International © 2022, all rights reserved

[[

]]

[[

]]

[[

]]

[[

]]

3.5 [[ ]]

[[

]]

[[

]]

3.5.1 Operating Bypass

Operating Bypasses (OB) block generation of RT and ESF initiation signals when a particular function would be unnecessary to keep the plant safe for the current plant condition. Most OBs are automatically initiated and automatically removed based on 2oo4 voting logic, which is executed separately within each PSS division for each OB. [[

]]

[[

]]

Copyright Holtec International © 2022, all rights reserved

[[

]]

3.5.2 Maintenance Bypass

If an input sensor is failed or needs to be taken out of service for maintenance, the sensor signal can be bypassed by a dedicated maintenance bypass function. Individual bypasses are provided for each redundant channel for all inputs to the PSS.

When a channel is bypassed using the maintenance bypass function, a partial trip from that channel is blocked from impacting the 2oo4 voting logic. If there is a spurious operation of the maintenance bypass on a channel, the remaining three channels can trip the reactor by executing the 2oo4 logic and opening the respective RTBs.

Putting a channel in maintenance bypass changes the 2oo4 voting logic to 2oo3 for the remaining channels. The details of this enhanced voting logic are discussed in section 3.2 including how the single failure criteria is being met.

[[

]]

[[

]]

[[

]]

Copyright Holtec International © 2022, all rights reserved

[[

]]

Figure 3-11 Maintenance Bypass Interlock Logic

3.5.3 RT and ESF Initiation

[[

]]

3.5.4 RT and ESF Latch Reset

Within each division of the PSS, the RT and most ESF actuation signals latch at the division level to ensure the actuation for that division proceeds to completion. Latches in each PSS division can be manually reset by initiating 2oo4 RT or ESF Latch Reset commands [[

]] There are separate latches and separate resets for each ESF function.

There is the potential for an administrative error, where latches could be erroneously reset [[

]]To mitigate all these potential errors, each PSS division includes an RT and ESF Latch Reset Permissive [[

]]

Copyright Holtec International © 2022, all rights reserved

[[

]]

[[

]]

[[

]]

Figure 3-12 [[ ]]

3.5.5 Component Level Control

[[

]]

Copyright Holtec International © 2022, all rights reserved

[[

]]

[[

]]

[[

]]

[[

]]

[[

]]

[[

]]

]]

Figure 3-13 [[ ]]

Copyright Holtec International © 2022, all rights reserved

[[

]]

Figure 3-14 [[ ]]

[[

]]

Figure 3-15 [[ ]]

Copyright Holtec International © 2022, all rights reserved

[[

]]

Figure 3-16 [[ ]]

3.5.6 PCS Disconnect

[[

]]

[[

]]

[[

]]

3.6 Capability for Testing and Calibration

All manual periodic testing can be conducted with the plant on-line. The manual periodic tests are: [[

]]

Copyright Holtec International © 2022, all rights reserved

[[

]]

The Channel Operability Tests and Actuation Logic Tests and Response Time Tests typically performed for analog protection systems are not needed for the digital SMR-160 PSS.

4.0 REFERENCES

[1] Holtec International, HI-2188331, *Safety System Digital Platform - MELTAC - Topical Report (JEXU-1041-1008),* Revision 0.

[2] Nuclear Regulatory Commission, *Safety Evaluation for Mitsubishi Electric Total Advanced Controller (MELTAC) Platform Topical Report and Supporting Documents,* November 2018.

[3] Nuclear Regulatory Commission, Regulatory Guide 1.97, *Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants,* Revision 5.

[4] Nuclear Regulator Commission, RG 5.71, *Cyber Security Programs for Nuclear Facilities,* 2010.

[5] IEEE 497, *IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations,* 2016.

Copyright Holtec International © 2022, all rights reserved