ACRONYMS AND ABBREVIATIONS (CONTINUED)

LOOP	loss of offsite power
MCR	main control room
~~MELCO~~	~~Mitsubishi Electric Corporation~~
MELTAC	Mitsubishi Electric Total Advanced Controller
MFW	main feedwater
M/G	motor generator
MHI	Mitsubishi Heavy Industries, Ltd.
MOV	motor operated valve
MSLB	main steam line break
MSS	main steam supply system
NEI	Nuclear Energy Institute
NIS	nuclear instrumentation system
NRC	U.S. Nuclear Regulatory Commission
NUREG	NRC Technical Report Designation (Nuclear Regulatory Commission)
OC	operator console
OEM	original equipment manufacturer
OS	operating system
O-VDU	operational VDU
PA	postulated accident
PAM	post accident monitoring
PCMS	plant control and monitoring system
PIF	power interface
POL	problem oriented language
PRA	probabilistic risk assessment
PSMS	protection and safety monitoring system
PSS	process and post-accident sampling system
QA	quality assurance
QAP	quality assurance program
RCP	reactor coolant pump
RCS	reactor coolant system
RFI	radio frequency interference
RG	Regulatory Guide
RHR	residual heat removal
RHRS	residual heat removal system
RMS	radiation monitoring system
RPI	rod position indication
RPS	reactor protection system
RSC	remote shutdown console

DCD_07.01-45

7.0 INSTRUMENTATION AND CONTROLS

7.1 Introduction

The instrumentation and control (I&C) systems provide the capability to control and regulate the plant systems manually and automatically during normal plant operation, and provide reactor protection against unsafe plant operation. The primary purpose of the I&C systems is to provide automatic protection and exercise proper control against unsafe and improper reactor operation during steady state and transient power operations. The system also provides initiating signals to actuate safety functions, which are assigned to mitigate the consequences of faulted conditions and ensure safe shutdown. Safety functions are those actions required to achieve the system responses assumed in the safety analyses and those credited to achieve safe shutdown of the plant. The I&C system is primarily a digital system with the exception of the analog diverse actuation system (DAS). The overall I&C architecture for the US-APWR is shown in Figure 7.1-1.

The general specifications of the overall I&C system are summarized as follows:

A. Main control board

- Fully computerized
- Safety visual display units (VDUs) and non-safety operational VDUs
- Large display panel (LDP)
- Minimal conventional switches, only for regulatory compliance (e.g., Regulatory Guide [RG] 1.62 [Reference 7.1-1]), refer to Table 7.1-1

B. Safety-related I&C

- Fully digital ~~Mitsubishi Electric Corporation (MELCO) Mitsubishi Electric Total Advanced Controller (MELTAC)~~ platform for the safety-related I&C system (Mitsubishi Electric Total Advanced Controller [MELTAC] platform) DCD-07.01-45
- Four train redundant reactor protection system (RPS)
- Four train redundant engineered safety features actuation system (ESFAS)
- Four train redundant safety logic system (SLS) for component control
- Four train redundant safety-related human-system interface system (HSIS) for control and monitoring
- Two train redundant safety-related HSIS for monitoring
- Conventional switches (for train level manual actuation)

C. Non-safety I&C

- Fully digital, except analog DAS

The technical and quality requirements applied to the safety-related I&C platform are listed in the applicability matrix table of MUAP-07005. The technical and quality requirements identified in the applicability matrix table of MUAP-07005 are imposed on the applicable sub-vendors. DCD_07.01-45

7.1.1 Identification of Safety-Related Systems and Non-Safety Systems

7.1.1.1 Overview

Safety-related PSMS with safety-related portion of the HSIS consists of:

- RPS
- ESFAS and SLS
- Conventional switches (train level)
- Safety VDUs - Part of safety-related HSIS for manual operation and monitoring of critical safety functions, including PAM

A brief summary of all the safety-related systems is presented in this section, while more detailed descriptions are given in Section 7.2 for reactor trip system, Section 7.3 for engineered safety feature systems, Section 7.4 for systems required for safe shutdown, Section 7.5 for information systems important to safety, and Section 7.6 for interlock systems important to safety. Detailed descriptions of non-safety systems are described in Section 7.7 for control systems not required for safety, Section 7.8 for diverse instrumentation and control systems, and Section 7.9 for data communication systems.

Safety functions are those actions required to achieve the system responses assumed in the safety analyses and those credited to achieve safe shutdown of the plant. Some safety functions are automatically initiated by the PSMS. These same safety functions may also be manually initiated and monitored by operators using the HSIS. The HSIS is also used to manually initiate other safety functions that do not require time critical actuation and safety functions credited for safe shutdown. After manual initiation from the HSIS, all safety functions are executed by the PSMS. The HSIS also provides all plant information to operators, including critical parameters required for post accident conditions. The HSIS includes both safety-related and non-safety sections.

7.1.1.2 Reactor Trip System

The safety-related systems automatically trip the reactor and initiate engineered safety features (ESF) (if required) whenever predetermined limits are approached. The RPS maintains surveillance on nuclear and process variables which are related to equipment mechanical limitations, such as pressure, and on variables that directly affect the heat transfer capability of the reactor, such as the reactor coolant flow and temperature. When a limit is approached, the RPS initiates the signal to open the reactor trip breakers (RTBs). This action removes power from the control rod drive mechanism (CRDM) coils, permitting the rods to fall by gravity into the core. This rapid negative reactivity insertion will cause the reactor to shutdown.

Each MHI Topical and Technical Report describes applicable code, regulatory, and industry standard compliance. The code, regulatory, and industry standards in each Topical and Technical Report are also applicable to the US-APWR I&C design.

Compliance to the corresponding sections of Appendix C.I.7.1-A in RG 1.206 (Reference 7.1-7), “Digital Instrumentation and Control Systems Application Guidance”, are discussed in Subsection 7.1.3. Additionally, compliance with Appendices C.I.7.1-B, “Conformance with Institute of Electrical and Electronics Engineers (IEEE) Std 603”, and C.I.7.1-C, “Conformance with IEEE Std 7-4.3.2”, are discussed in MUAP-07004 Appendices A and B respectively. For some sections of IEEE Std 603-1991, complete compliance requires plant specific descriptions.

The technical and quality requirements for the safety-related I&C platform design and development are identified in DCD Chapter 7 and related technical reports. The design and development of the safety-related I&C platform meets all code, regulatory, and industry standards, as shown in the applicability matrix table of MUAP-07005. The technical and quality requirements identified in DCD Chapter 7 and the related technical reports are imposed on the applicable sub-vendors. DCD_07.01-45

7.1.3 Design Bases of Instrumentation and Control System

The design of the I&C system meets all code, regulatory, and industry standards, as shown in Table 7.1-2, including the specific safety requirements described in the subsections below. Since the RPS, ESFAS, SLS, and other subsystems of the PSMS use a common platform, the design bases for PSMS are listed in this subsection. The design bases that are specific to the RPS, ESFAS, SLS, or other I&C subsystems are discussed in Sections 7.2 through 7.9.

7.1.3.1 Defense-in-Depth and Diversity Concept

The architecture of the overall I&C system is based on the defense-in-depth and diversity concept. This concept defines four echelons of defense. These echelons are the control system, reactor trip system, engineered safety features actuation system, and monitoring and indicators.

Separation of functions and diversity of functions between these echelons minimize the potential for CCFs. In addition, the software applied for the PSMS has high integrity due to design simplicity and a comprehensive software quality program including independent verification and validation (V&V).

The conventional, analog, and hardwired DAS is provided per guidance of branch technical position (BTP) 7-19 (Reference 7.1-8), to accommodate beyond design basis CCFs that could adversely affect all safety-related and non-safety control systems within all echelons. The DAS provides automated actuation of time critical safety functions. In addition, the DAS allows the operator to monitor critical safety functions and to manually actuate safety-related process systems, using equipment that is diverse from the PSMS and PCMS. For more detailed discussion on diversity and defense-in-depth features, refer to Topical Report MUAP-07006.

operation. In addition to the MCR, the HSI also includes the RSC, TSC, EOF, and local control stations, such as auxiliary equipment control console. Refer to Chapter 18 for a full discussion of all HSI issues.

7.1.3.13 Quality of Components and Modules

The quality of PSMS components and modules and the quality of the PSMS design process are controlled by a program that meets the requirements of American Society of Mechanical Engineers (ASME) NQA-1-1994 (Reference 7.1-13). Conformance to ASME NQA-1-1994 is described further in Section 17.5.

The MELTAC platform ~~has been commercially dedicated in accordance with EPRI TR-107330 (Reference 7.1-33) and TR-106439 (Reference 7.1-34), and~~ is ~~now~~ maintained and manufactured as Class 1E equipment that meets the requirements of ASME NQA-1-1994 (Reference 7.1-13). ~~Conformance to ASME NQA-1-1994 is described further in the MELTAC Platform Technical Report (Reference 7.1-3).~~ DCD_07.01-45 DCD_07.01-45

7.1.3.14 System Calibration, Testing and Surveillance

Testing from and including the sensors of the PSMS through to and including the actuated equipment and HSI is accomplished in a series of overlapping sequential tests and calibrations. The majority of the tests are conducted automatically, through self-diagnosis. The remaining manual tests may be performed with the plant at full power. There are no exceptions for testing at power in PSMS.

In addition to perform self-diagnostic features, the redundant system inputs measurements channel from different trains are continuously compared to each other. This automated CHANNEL CHECK is performed in the PCMS; and deviations are alarmed in the MCR. A failure of this automated CHANNEL CHECK function is detected by the self-diagnostic function of the PCMS, and the failure is alarmed in the MCR. In addition, the operability of CHANNEL CHECK function can be manually checked during CHANNEL CARIBRATION.

The test frequency for manual tests is based on an uncertainty and reliability analysis, reference Subsection 7.2.2.7 and 7.2.3.5, respectively, for additional information. This analysis demonstrates the need to conduct most manual tests for PSMS equipment no more frequently than once per 30 months, which allows for fuel cycles up to 24 months plus 6 months to accommodate 25% margin for consistency with technical specification surveillance interval compliance. Therefore conducting manual tests for PSMS equipment on-line or off-line, during refueling shutdown, is at the discretion of the plant owner.

Periodic routine calibration will be performed for the field located transmitters of each safety-related instrument loop. Due to the digital design of the control platform in the US-APWR, a traditional calibration method will be performed from the sensor through the analog to digital converter to the digital display (VDU). During this calibration, the digital display (VDU) will provide the instrument output. As in a traditional calibration, the measured value on the display will be compared to an expected range. Calibration points encompass the trip setpoint to confirm required accuracy at the trip setpoint value(s).

In some cases, it is advantageous to employ signals derived from instrumentation that are also used in the protection trains. This practice reduces the need for separate non-safety instrumentation, which would require additional penetrations into reactor pressure boundaries and introduce the need to additional maintenance in hazardous areas. For each parameter where instrumentation is shared, the PCMS receives four redundant signals from each train of the RPS. The signal selection algorithm (SSA), within the PCMS, receives input from all safety-related process trains but passes only the second highest operable process signal value to the control system's automation algorithms. The reactor control systems also have a modified SSA using an average calculation process. (This average calculation for select signals in the reactor control system is different from the description in MUAP-07004 Subsection 4.2.5.) The SSA excludes process inputs that are failed or taken out of service for maintenance or testing.

The SSA of the PCMS ensures the PCMS does not take erroneous control actions based on a single instrument channel failure or a single RPS train failure. As such, a single failure will not cause the PCMS to take erroneous control actions that challenge the PSMS, while the PSMS is in a degraded operability state due to a failed instrument channel or failed RPS train.

The SSA is continuously tested as follows:

- The PCMS employs the same self-test features as the PSMS. These features are described in Subsection 4.1.5 of MUAP-07005.
- The basic software configuration and application software configuration, within the PCMS controller, is periodically confirmed by the same manually initiated method described in Subsection 4.1.4.1.c of MUAP-07005.

Since the SSA uses only digital values obtained from the PSMS via the unit bus, all functions of the SSA are completely covered by self-testing; no additional manual tests are required. The digital values obtained from the PSMS are confirmed during CHANNEL CALIBRATION for the safety-related sensors.

This SSA within the PCMS allows the RPS to have one instrument channel inoperable or bypassed at all times except the neutron flux monitoring function while still complying with General Design Criteria (GDC) 24 (Reference 7.1-14) and IEEE Std 603-1991 (Reference 7.1-15). As described in the probabilistic risk assessment (PRA) the RPS meets the plant reliability goals with only three channels in operation except the neutron flux monitoring function. Refer to the PRA Technical Report (Reference 7.1-16).

The shared instrumentation signals are interfaced through fiber optic data networks. As such, an electrical fault in the PCMS cannot propagate to the protection channel. Refer to MUAP-07004 Subsection 4.2.5 for additional details.

7.1.3.17 Life Cycle Process

MHI applies ~~its MELCO's safety system~~ fully digital platform for the safety-related I&C system, MELTAC, to the PSMS of the US-APWR. ~~Full details of the life cycle process for the MELTAC safety platform basic software, including quality assurance (QA), management, development, installation, maintenance, training, operation, and the software safety plan are discussed in MUAP-07005 Section 6.0.~~ The life cycle process

DCD_07.01-45

for the PSMS application software, including QA, management, development, installation, maintenance, training, operation, and the software safety plan are discussed in The US-APWR Software Program Manual (Reference 7.1-18), including BTP 7-14 (Reference 7.1-17) compliance. ~~The life cycle process for the MELTAC platform basic software is described in JEXU-1012-1132, The Basic Software Program Manual (Reference 7.1-35).~~ The US-APWR Software Program Manual (MUAP-07017) also controls the basic software life cycle process of the MELTAC Platform. DCD_07.01-45

7.1.3.18 Quality Assurance Program

The overall quality assurance program (QAP) for the US-APWR I&C systems is described in Chapter 17. ~~The specific QAP for the MELTAC platform is described in MUAP-07005 Section 6.0. These QAPs address all requirements of Title 10, Code of Federal Regulations (CFR), Part 50, Appendix B (Reference 7.1-19), and IEEE Std 7-4.3.2-2003 (Reference 7.1-20).~~ DCD_07.01-45

7.1.3.19 Identification

I&C equipment identification follows the guidance of RG 1.75, which endorses IEEE Std 384-1992 (Reference 7.1-22). The following color coding is provided on tags used for the identification of I&C system cabinets and for stand alone components, such as field instruments.

Identification shall not require frequent use of reference material.

- Train A: Red with white lettering
- Train B: Green with white lettering
- Train C: Blue with white lettering
- Train D: Yellow with black lettering
- Non-safety train: White with black lettering

This color coding is consistent with the color coding defined in Subsection 8.3.1.1.8 identification of class 1E electrical equipment and cables.

For computer-based systems, the configuration management plan describes the identification process for software. To ensure that the required computer system hardware and software are installed in the appropriate system configuration, the system meets the following identification criteria specific to software systems:

- Firmware and software identification ensures that the correct software is installed in the correct hardware component.
- The software has a means to retrieve identification from the firmware by using software maintenance tools.
- Physical identification requirements of the digital computer system hardware are in accordance with the identification requirements in IEEE Std 603-1991.

Various redundancy configurations are utilized as described in the MELTAC Platform Technical Report (Reference 7.9-1) Subsection 4.1.1.1.

I/O can be located in close proximity to the controller or in locations remote from the controller. Remote I/O is utilized for both PCMS and PSMS applications.

7.9.1.5 Maintenance Network

The maintenance network is a non-safety system that allows for monitoring the status of the PSMS and PCMS equipment failure indications and diagnostics, updating setpoints and constants, and the installation of new application software. PSMS controllers are normally not connected with the maintenance network. PSMS controllers that are temporarily connected to the maintenance network are declared inoperable and the functions that become inoperable due to inoperability of that controller (if any) are managed by the technical specifications. There is communication independence for the maintenance networks for each train. However, since all maintenance networks are non-safety, no electrical independence is required and there are locations in the plant where all maintenance networks are in close physical proximity. The following description is applicable to the maintenance network for any one train.

The major components of the maintenance network are the switching hub and MELTAC engineering tool. The maintenance network interfaces to the system management module of each controller via qualified E/O converters.

Security-Related Information - Withheld Under 10 CFR 2.390

DCD_07.01-45

Security-Related Information - Withheld Under 10 CFR 2.390

7.9.1.6 Station Bus

The station bus provides information to plant and corporate personnel and to the EOF and ERDS. The station bus receives information from the DCS via the unit management computer. The unit management computer provides a firewalled interface, which allows only outbound communication. There are no other connections from external sources to the DCS.

7.9.1.7 External Network Interface

The only interface from the PCMS and PSMS to external networks is via the firewall within the unit management computer. The unit management computer provides an outbound only interface to the plant Station Bus to allow communication to EOF computers, the NRC (via ERDS), corporate information systems and plant personnel computers.

7.9.2 Design Basis Information

7.9.2.1 Quality of Components and Modules

The PSMS includes the safety bus, data links, I/O bus, and safety VDU communications. The Quality of PSMS components and modules is described in Subsection 7.1.3.13.

7.9.2.2 Software Quality

The safety-related portions of the DCS are part of the PSMS. The non-safety portions of the DCS are part of the PCMS. All portions of the DCS handles the communication protocol and self-diagnosis, and application software, which handles the actual data being transmitted. ~~Software Quality of basic software is described in MELTAC Platform Technical Report (Reference 7.9-1) Section 6.1.~~ DCD_07.01-45

MHI applies ~~its MELCO's safety system~~ fully digital platform for the safety-related I&C system, MELTAC to PSMS and PCMS systems of US-APWR.

7.9.2.3 Performance Requirements

DCS in digital I&C system of the US-APWR meets the performance of required functions. The performance of the digital I&C system including DCS conforms to the guideline of BTP 7-21(Reference 7.9-15). The Response Time Technical Report (Reference 7.9-16) provides the response time of safety-related I&C system. The report demonstrates that the safety-related I&C system meets the response time requirement from safety analysis. The simplified block diagrams of the RT and ESF functions propagation paths and response time of each path in the safety-related I&C system are provided. The