7.8 Diverse Instrumentation and Control Systems

The DAS is the non-safety diverse instrumentation and control system for US-APWR. The DAS provides monitoring, control and actuation of safety and non-safety systems required to cope with abnormal plant conditions concurrent with a CCF that disables all functions of the PSMS and PCMS. The DAS includes an automatic actuation function, HSI functions located at the diverse HSI panel (DHP), and interfaces with the PSMS and PCMS. The design basis and detailed system description for the DAS are described in the D3 Topical Report (Reference 7.8-1). Table 7.8-7 shows the supplemental information to Topical Report MUAP-07006-P-A, which is necessary to be clarified. The D3 Coping Analysis Technical Report (Reference 7.8-2) demonstrates the ability to maintain all critical safety functions and achieve hot standby using the DAS.

MIC-04-07-00001

Add "There are differences between the D3 Topical Report (Reference 7.8-1) and the DCD which are due to design changes of the DAS that are applicable to the US-APWR. The scope, applicability and design differences from the D3 Topical Report (Reference 7.8-1) are described in Table 7.8-10."

The DA ally diverse and indepe MS, so that a beyond design AS functions. In addition, the DA uation of automatic and manua is designed to prevent spuriou ated fires. The DAS interfac f the SLS are isolated within t fety-related logic within the SLS (not affected by a CCF) ensures that control commands originating in the DAS or SLS, which correspond to the desired safety function, always have priority. Therefore, there is no adverse interaction of the DAS with safety functions and no erroneous signals resulting from CCF in the SLS that can prevent the safety function. For a figure of the DAS system architecture, refer to Figure 4.2-6 of MUAP-07004.

Within the DAS, manual actuation is provided for systems to maintain all critical safety functions (Refer to Table 7.8-1). For conditions where there is insufficient time for manual operator action, the DAS provides automatic actuation of required plant safety functions needed for accident mitigation. Key parameter indications, diverse audible and visual alarms, and provisions for manual controls are located in a dedicated independent DHP located in the MCR. Conventional hardwired logic hardware and relays for automatic actuation are installed in four diverse automatic actuation cabinets (DAACs), each located in a separate Class 1E electrical room. Each DAAC is powered by a separate Class 1E UPS via qualified isolation device. During plant on-line operation, the system can be tested manually without causing component actuation that would disturb plant operations.

7.8.1 System Description

The DAS consists of manual HSI functions, which include automatic actuation functions. These functions are located in the DHP and the DAAC, respectively. In addition, the DAS consists of interfacing connections with the PSMS and CRDM motor-generator sets. The DAS receives inputs from qualified analog isolation devices located in the RPS or directly from plant components. The DAS provides outputs which interface to the SLS power interface modules via qualified isolation devices located in the SLS or directly to plant components.

Table 7.8-7 Supplemental Information to MUAP-07006-P-A (Sheet 2 of 6)

No.	Items to be clarified	Corresponding Section of SER for MUAP-07006-A	Resolution	Reference Document and Section
4	The US-APWR design certification applicant shall identify the specific controls and indications for the DHP and address human factors aspects for the DAS and PSMS system-level manual actuation means.	3.2.1, 3.2.2, 3.2.3	The specific controls and indications for the DHP are identified in DCD Table 7.8-1 and Table 7.8-2, respectively. Since the PSMS system level actuation controls are located on the OC and the DAS system level actuation controls are located on the DHP, and the use of the DHP controls is prompted by unique DHP alarms, there is little potential for human performance error. The HFE V&V program element described in DCD Section 18.10 ensures that the system level manual actuation means provided in PSMS and DAS, are used appropriately and without human performance error.	DCD Table 7.8-1 and 7.8-2. DCD Section 18.10.
5	The US-APWR design certification applicant shall provide the final determination of the setpoints and the response time of the DAS.	3.2.2	The DAS setpoints and time delay settings are shown in DCD Table 7.8-6. These values are demonstrated to be acceptable in MUAP-07014, Defense-in-Depth and Diversity Coping Analysis	DCD Table 7.8-6 MUAP-07014
6	The US-APWR design certification applicant shall demonstrate that the acceptability of the QA process used for the DAS meets the guidelines of GL 85-06.	3.2.2, 4.0	The QA process used for the DAS meets the guidelines of GL 85-06 as described in DCD Subsection 7.8.2.7. ~~To comply with GL 85-06 the DAS QA program will comply with 10 CFR 50 Appendix B as described in MUAP-07006 Subsection 6.2.1.7.~~	DCD Subsection 7.8.2.7 ~~MUAP-07006 Subsection 6.2.1.7~~

MIC-04-07-00001

Delete this description.

Delete this description.

Table 7.8-7 Supplemental Information to MUAP-07006-P-A (Sheet 4 of 6)

No.	Items to be clarified	Corresponding Section of SER for MUAP-07006-A	Resolution	Reference Document and Section
9	The US-APWR design certification applicant shall address the partial failures of the PCMS/ PSMS and demonstrate an adequa to cope wi modes.	3.2.3	Single failures that result in partial failure of the PSMS do not impact the PSMS safety functions, as demonstrated in ~~DCD Tables 7.2-8 and 7.3-7~~. The evaluation of partial common-cause failures of the PCMS/ PSMS and an adequate D3 strategy to cope with such failure modes are provided in MUAP-07014, Defense-in-Depth and Diversity Coping Analysis.	~~DCD Tables 7.2-8 and 7.3-7~~ MUAP-07014
10	The US-APWR design certification applicant shall provide an acceptable defense-in-depth and diversity strategy for a LBLOCA concurrent with a CCF of the PSMS.	3.3.2	An acceptable D3 strategy for a LBLOCA concurrent with a CCF of the PSMS is described in MUAP-07014, Defense-in-Depth and Diversity Coping Analysis.	
	(The resolution of Future Licensing Submittals described in Section 10 of MUAP-07006-A are follows)			
11-1	Changes in implementation detail, as needed	1.0, 2.0	Application specific designs are described in Section 7.8	DCD Section 7.8
11-2	Specific description of the PSMS and the DAS functions	2.0	~~Subsection 7.2 and 7.3~~ describes specific description of the PSMS; the DAS functions are in Section 7.8	~~DCD Section 7.2, 7.3 and 7.8~~
11-3	Specific I&C functions implemented within the DAS	3.1 GDC 13	DCD Figure 7.2-2 Sheet 14 describes specific DAS functions.	DCD Figure 7.2-2

MIC-04-07-00001

MIC-04-07-00001

Change "DCD Tables 7.2-8 and 7.3-7" to "Appendix G of MUAP-07004".

Change "DCD Tables 7.2-8 and 7.3-7" to "Appendix G of MUAP-07004".

Change "Subsection 7.2 and 7.3" to "Sections 7.1, 7.2, 7.3, 7.4, 7.5, 7.6 and 7.9".

Change "DCD Section 7.2, 7.3 and 7.8" to "DCD Sections 7.1, 7.2, 7.3, 7.4, 7.5, 7.6 and 7.9 for PSMS DCD Section 7.8 for DAS".

Add Table 7.8-10 (Sheet 1 of 2).

MIC-04-07-00001

Table 7.8-10 Applicability of MUAP-07006-P-A (Reference 7.8-1) (Sheet 1 of 2)

Section of MUAP-07006	Applicability to US-APWR DCD Chapter 7	Reasons for Design Differences	Applicable Description in DCD Chapter 7 and Technical Report
1.0	Applicable	-	-
2.0	Applicable	-	-
3.0	Applicable with updated Codes and Standards	Applicability for the US-APWR with updated Codes and Standards is summarized.	DCD Chapter 7 Table7.1-2 Section 7.8
4.0	Applicable except Figure 4.0-1	The overall architecture of the I&C system is updated.	DCD Chapter 7 Figure 7.1-1
4.1	Applicable	-	-
5.0	Applicable	-	-
5.1	Applicable	-	-
5.2	Applicable	-	-
5.3	Applicable	-	-
5.4	Applicable	-	-
5.5	Applicable	-	-
5.6	Applicable	-	-
6.0	Applicable except Figure 6.0-1	The DAS architecture is revised to protect against potential CCF concurrent with risk-significant external events.	MUAP-07004 Figure 4.2-6
6.1	Applicable except Table 6.1-1 Table 6.1-2 Table 6.1-3 Table 6.1-4 and Figure 6.1-1	The functional design features are updated to accommodate US-APWR plant requirement.	DCD Chapter 7 Table 7.8-1 Table 7.8-3 Table 7.8-5 Table 7.8-2 and Figure 7.2-2 (Sheet 14 of 21)
6.2	Applicable	-	-
6.2.1	Applicable	-	-
6.2.1.1	Applicable	-	-
6.2.1.2	Applicable	-	-
6.2.1.3	Applicable	-	-
6.2.1.4	Applicable	-	-
6.2.1.5	Applicable	-	-
6.2.1.6	Applicable	-	-
6.2.1.7	Applicable except 10CFR50 App.B applicability	The DAS is designed with augmented quality to meet QA requirement of GL 85-06.	DCD Chapter 7 Subsection 7.8.2.7
6.2.2	Applicable	-	-
6.2.2.1	Applicable	-	-
6.2.2.2	Applicable except Figure 6.2-3	The functional design features are updated to accommodate US-APWR plant requirement.	DCD Chapter 7 Figure 7.8-2
6.2.2.3	Applicable	-	-
6.2.2.4	Applicable	-	-
7.0	Applicable	-	-

Add Table 7.8-10 (Sheet 2 of 2).

MIC-04-07-00001

Table 7.8-10 Applicability of MUAP-07006-P-A (Reference 7.8-1) (Sheet 2 of 2)

Section of MUAP-07006	Applicability to US-APWR DCD Chapter 7	Reasons for Design Differences	Applicable Description in DCD Chapter 7 and Technical Report
7.1	Applicable	-	-
7.2	Applicable	-	-
7.2.1	Applicable	-	-
7.2.2	Applicable	-	-
7.2.3	Applicable	-	-
7.2.4	Applicable	-	-
7.2.5	Applicable	-	-
7.2.6	Applicable	-	-
7.3	Applicable	-	-
7.3.1	Applicable	-	-
7.3.2	Applicable	-	-
7.3.3	Applicable	-	-
7.4	Applicable	-	-
7.5	Applicable	-	-
7.6	Applicable	-	-
7.7	Applicable	-	-
7.8	Applicable	-	-
7.9	Applicable	-	-
7.10	Applicable	-	-
7.11	Applicable	-	-
7.12	Applicable	-	-
7.12.1	Applicable	-	-
7.12.2	Applicable	-	-
7.12.3	Applicable	-	-
7.13	Applicable	-	-
7.14	Applicable	-	-
8.0	Applicable	-	-
8.1	Applicable	-	-
8.2	Applicable	-	-
8.3	Not Applicable	The automatic ECCS actuation function is added to cope with a LBLOCA concurrent with a CCF of the PSMS.	DCD Chapter 7 Section 7.8.1.2.3
8.3.1	Not Applicable		
9.0	Applicable	-	-
9.1	Applicable	-	-
9.2	Applicable	-	-
9.3	Not Applicable	The automatic ECCS actuation function is added to cope with a LBLOCA concurrent with a CCF of the PSMS.	DCD Chapter 7 Section 7.8.1.2.3
9.4	Applicable	-	-
10.0	Applicable	-	-
11.0	Applicable	-	-
Appendix A	Applicable	-	-
Appendix B	Applicable	-	-
Appendix C	Applicable	-	-

7.8 Diverse Instrumentation and Control Systems

The DAS is the non-safety diverse instrumentation and control system for US-APWR. The DAS provides monitoring, control and actuation of safety and non-safety systems required to cope with abnormal plant conditions concurrent with a CCF that disables all functions of the PSMS and PCMS. The DAS includes an automatic actuation function, HSI functions located at the diverse HSI panel (DHP), and interfaces with the PSMS and PCMS. The design basis and detailed system description for the DAS are described in the D3 Topical Report (Reference 7.8-1). Table 7.8-7 shows the supplemental information to Topical Report MUAP-07006-P-A, which is necessary to be clarified. The D3 Coping Analysis Technical Report (Reference 7.8-2) demonstrates the ability to maintain all critical safety functions and achieve hot standby using the DAS.

The DAS design consists of conventional equipment that is totally diverse and independent from the MELTAC platform of the PSMS and PCMS, so that a beyond design basis CCF in these digital systems will not impair the DAS functions. In addition, the DAS includes internal redundancy to prevent spurious actuation of automatic and manual functions due to a single component failure. The DAS is designed to prevent spurious actuations due to postulated earthquakes and postulated fires. The DAS interfaces with the safety-related process inputs and outputs of the SLS are isolated within these safety-related systems. In addition, hardwired safety-related logic within the SLS (not affected by a CCF) ensures that control commands originating in the DAS or SLS, which correspond to the desired safety function, always have priority. Therefore, there is no adverse interaction of the DAS with safety functions and no erroneous signals resulting from CCF in the SLS that can prevent the safety function. For a figure of the DAS system architecture, refer to Figure 4.2-6 of MUAP-07004.

MIC-04-07 -00001

Within the DAS, manual actuation is provided for systems to maintain all critical safety functi sufficient time for manual opera ed plant safety functions needed for accident mitigation. Key parameter indications, diverse audible and visual alarms, and provisions for manual controls are located in a dedicated independent DHP located in the MCR. Conventional hardwired logic hardware and relays for automatic actuation are installed in four diverse automatic actuation cabinets (DAACs), each located in a separate Class 1E electrical room. Each DAAC is powered by a separate Class 1E UPS via qualified isolation device. During plant on-line operation, the system can be tested manually without causing component actuation that would disturb plant operations.

Add "Components' safe states in the state-based priority logic are shown in Table 7.8-11."

7.8.1 System Description

The DAS consists of manual HSI functions, which include automatic actuation functions. These functions are located in the DHP and the DAAC, respectively. In addition, the DAS consists of interfacing connections with the PSMS and CRDM motor-generator sets. The DAS receives inputs from qualified analog isolation devices located in the RPS or directly from plant components. The DAS provides outputs which interface to the SLS power interface modules via qualified isolation devices located in the SLS or directly to plant components.

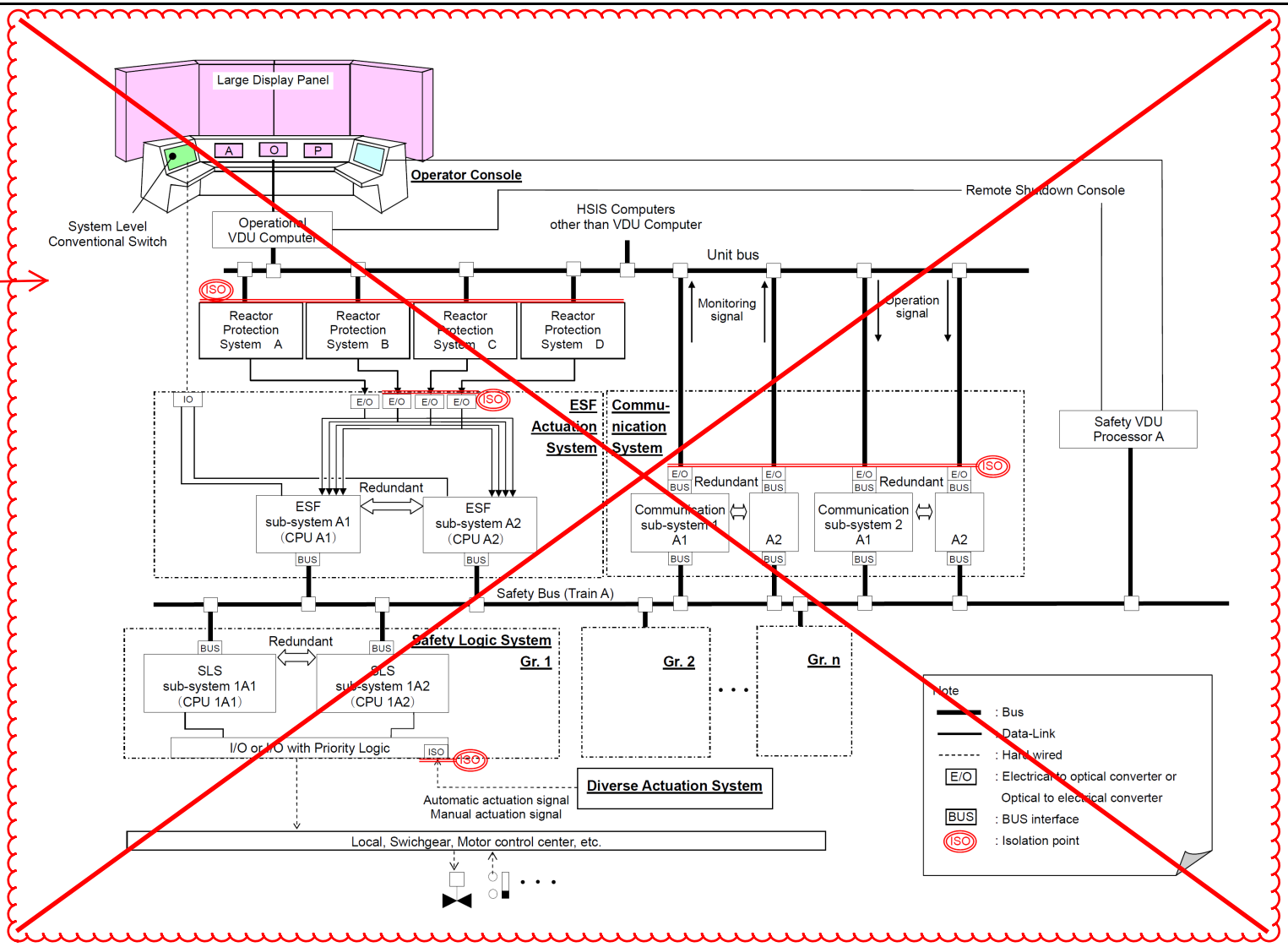
Add Table 7.8-11.

MIC-04-07-00001

Table 7.8-11 Safe State in State-Based Priority Logic

Component	Required Position	Safe State in Priority Logic	Remarks
Reactor Trip	Trip	Trip	DAS signal has no interface to PSMS.
Turbine Trip Solenoid Valves	Open	Open	PSMS and DAS have only open signal.
EFW Pumps	Start	Start	
Safety Injection Pump	Start	Start	
Safety Depressurization Valve	Open/ Closed	Open	Safe state is determined as the position opposite to the most frequent position of operation.*1
Main Steam Depressurization Valve	Open/ Closed	Open	Safe state is determined as the position opposite to the the most frequent position of operation.*1
SG Blowdown Isolation Valve	Closed	Close	
MFW Regulation Valve	Closed	Close	
EFW Control Valve	Open/ Closed	Close	Safe state is determined as the position opposite to the the most frequent position of operation.*1
CV Isolation Valves	Closed	Close	
Main Steam Line Isolation Valves	Closed	Close	

Note 1: Though a spurious demand signal same as the normal position would be undetectable, the opposite demand signal can reposition the component as necessary. In case of spurious demand signal opposite to the normal position, spurious repositioning of the component can be detectable by the BISI alarm and be corrected.

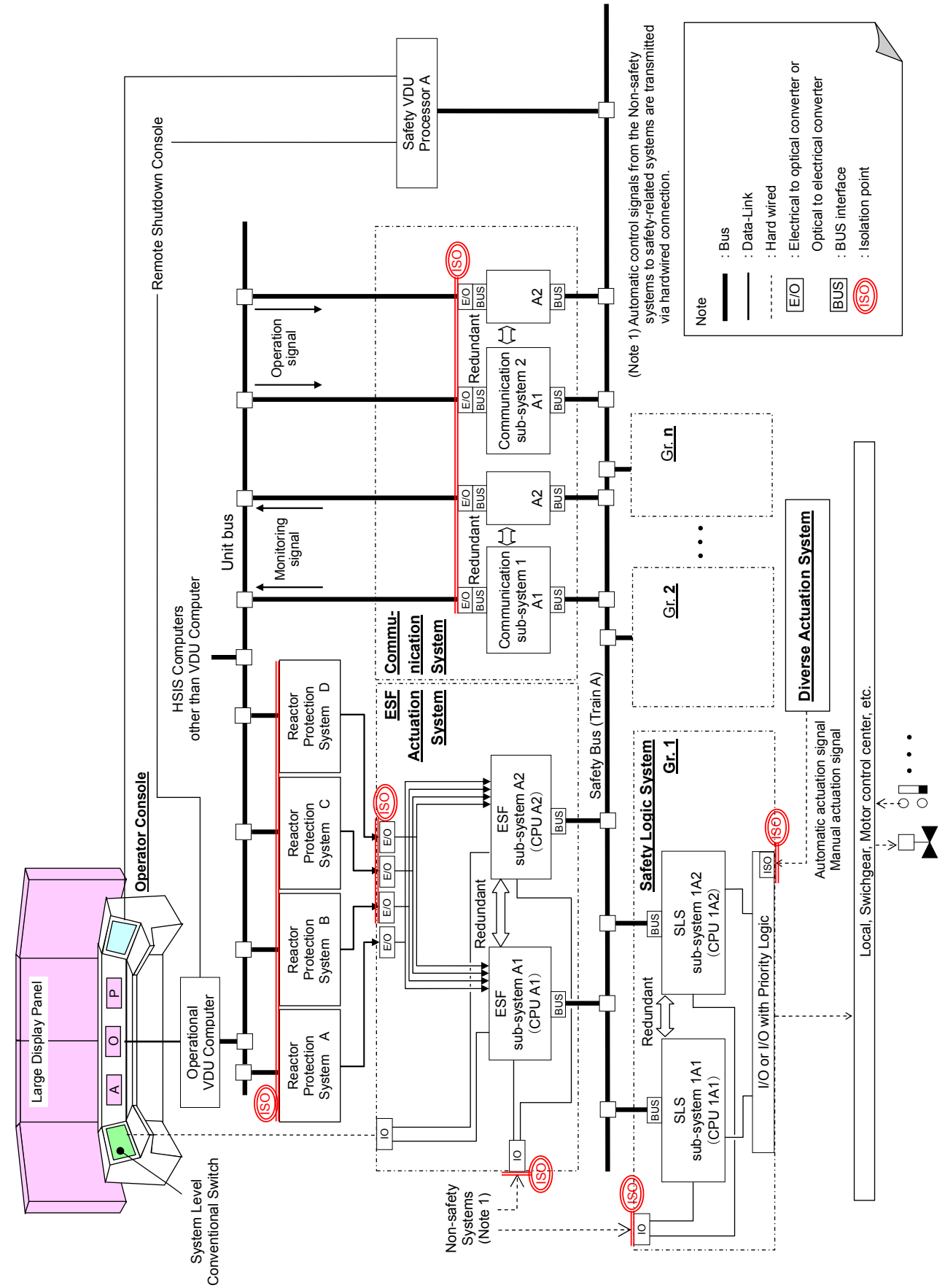


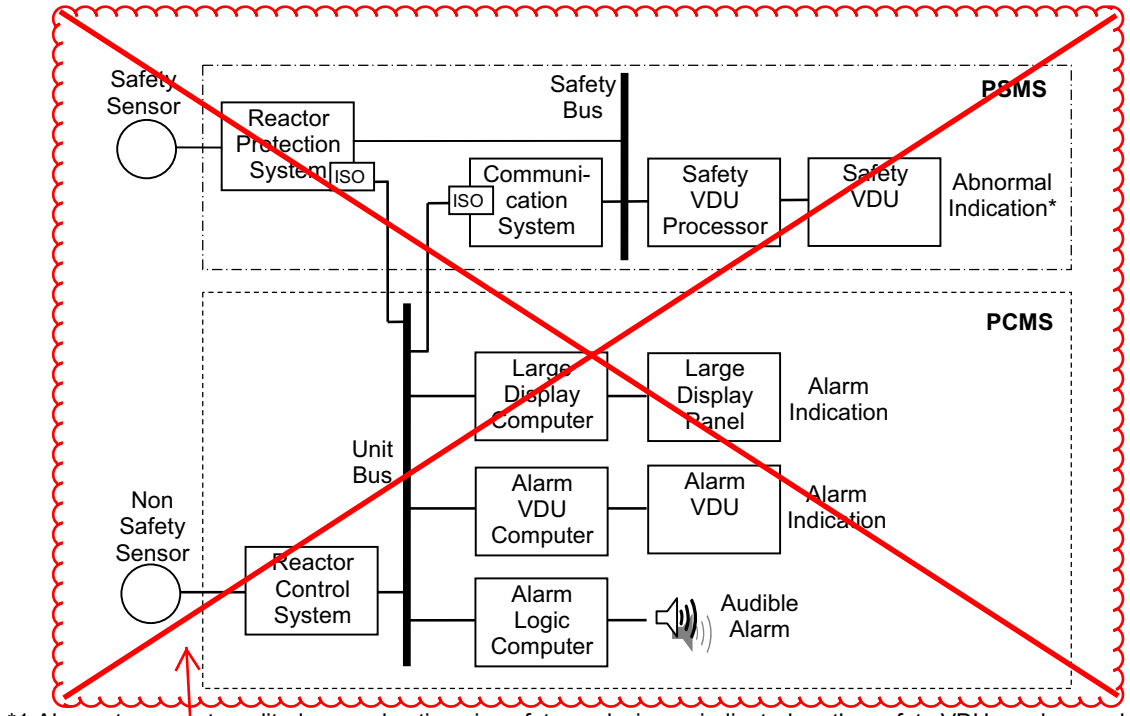
Change this figure as shown in the next page.

Figure 7.3-1 Configuration of Engineered Safety Features Actuation System and Safety Logic System

Attachment 3-1 to Response to ACRS Subcommittee Questions (1/4)

MIC-04-07-00001


Operator Console
Large Display Panel
A
O
P
Operational VDU Computer
System Level Conventional Switch
Remote Shutdown Console
HSIS Computers other than VDU Computer
Unit bus
Operation signal
Monitoring signal
Safety VDU Processor A
Reactor Protection System A
Reactor Protection System B
Reactor Protection System C
Reactor Protection System D
ESF Actuation System
Commu-nication System
ESF sub-system A1 (CPU A1)
ESF sub-system A2 (CPU A2)
Redundant
Communication sub-system 1 A1
Communication sub-system 2 A1
A2
E/O
BUS
ISO
IO
Safety Bus (Train A)
Safety Logic System
Gr. 1
Gr. 2
Gr. n
SLS sub-system 1A1 (CPU 1A1)
SLS sub-system 1A2 (CPU 1A2)
I/O or I/O with Priority Logic
Diverse Actuation System
Automatic actuation signal
Manual actuation signal
Non-safety Systems (Note 1)
Local, Swichgear, Motor control center, etc.
(Note 1) Automatic control signals from the Non-safety systems to safety-related systems are transmitted via hardwired connection.
Note
: Bus
: Data-Link
: Hard wired
: Electrical to optical converter or Optical to electrical converter
: BUS interface
: Isolation point



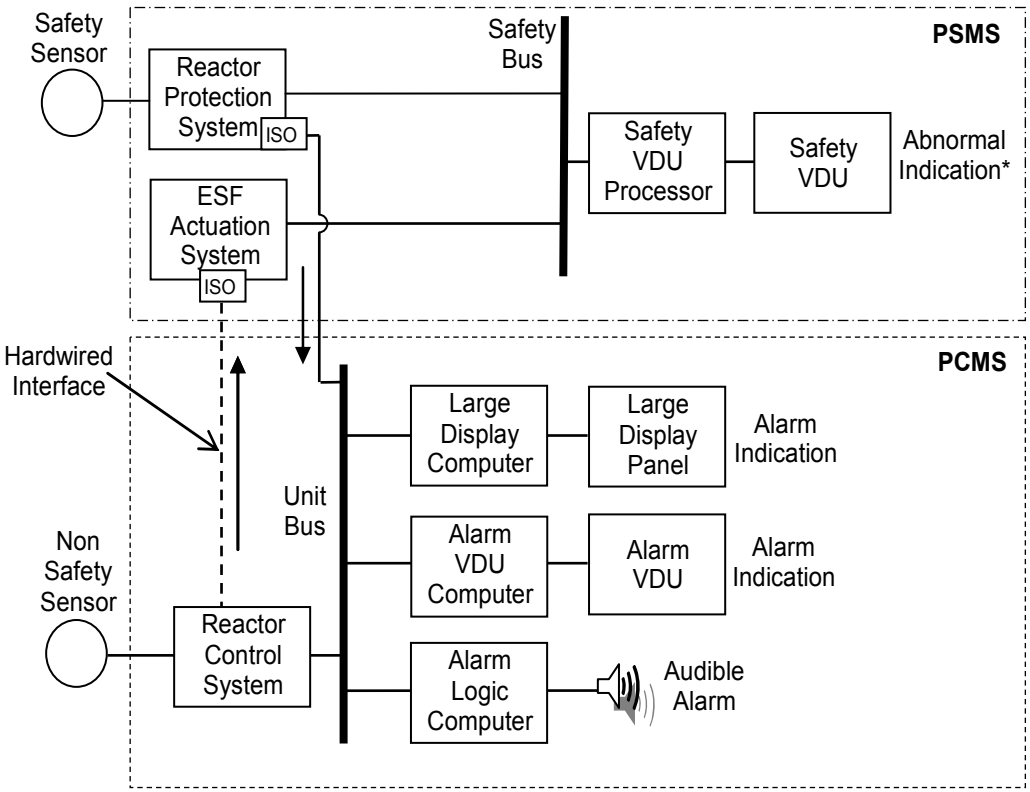
*1 Alarms to prompt credited manual actions in safety analysis are indicated on the safety VDU as abnormal indications.

Change this figure as shown in the next page.

MIC-04-07 -00001

Figure 7.5-4 Alarm System Configuration

MIC-04-07
-00001



MIC-04-07
-00001

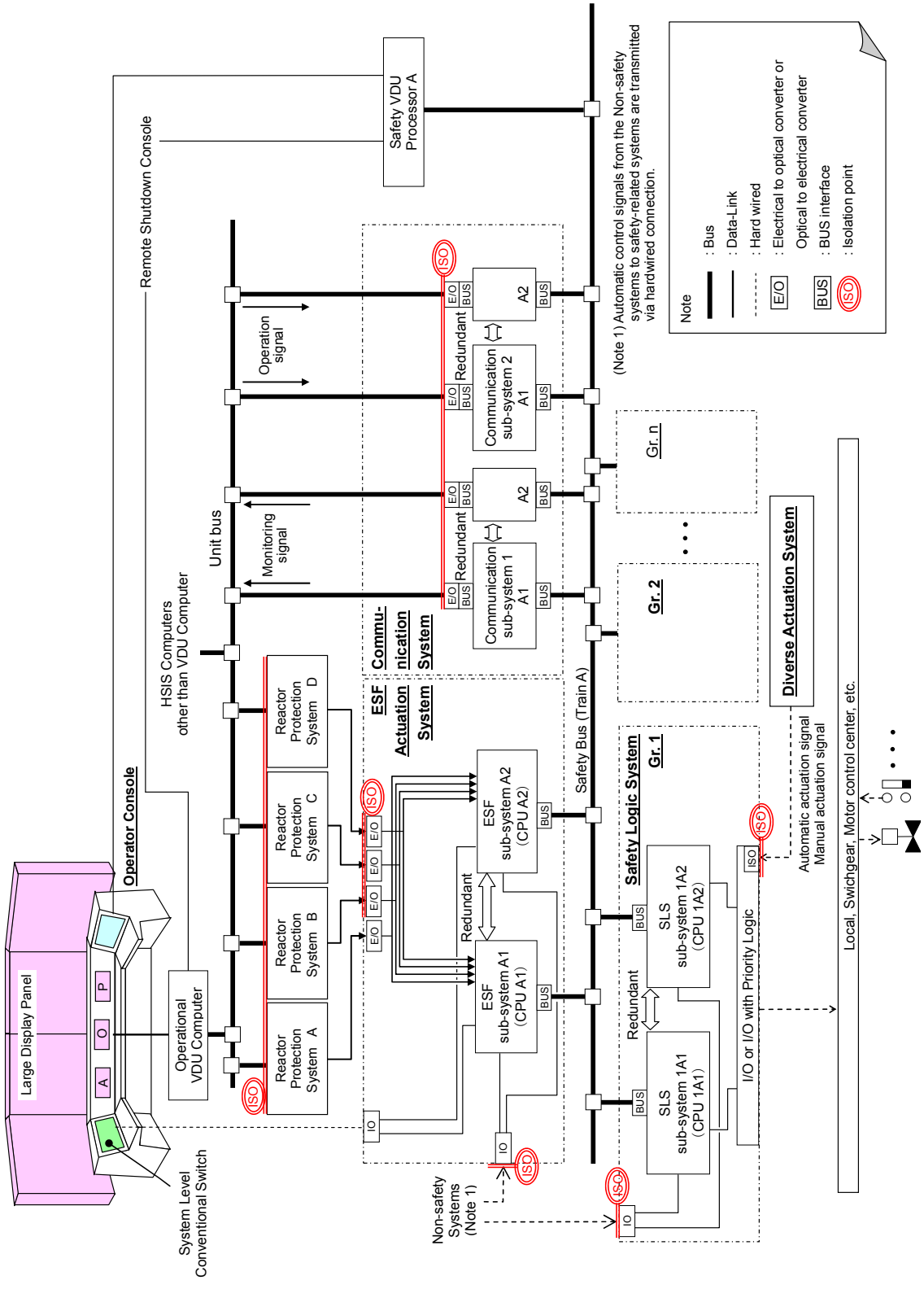


Figure 4.1-5 Configurations of the ESFAS, SLS, and Safety-Related HSI

Add " through a qualitative analysis that compares the time available to the time required" after "actions".

Technical Report MUAP-07014 also confirms t
manual operator actions. The HSI on the DHP is designed, verified, and validated in accordance with the HFE program described in Chapter 18.

MIC-04-07-00001

7.8.3.3 Conformance to BTP 7-19

Topical Report MUAP-07006 Appendix A provides a detailed description for the conformance of BTP 7-19 (Reference 7.8-7).

7.8.4 Combined License Information

No additional information is required to be provided by a COL Applicant in connection with this section.

7.8.5 References

Add
"All credited manual operator actions identified in the D3 Coping Analysis Technical Report (Reference 7.8-2) are analyzed in accordance with the Task Analysis Implementation Plan Technical Report (Reference 7.8-12) to quantitatively confirm adequate margin between time available and time required. In addition, the credited manual actions identified in the D3 Coping Analysis Technical Report (Reference 7.8-2) are verified and validated as described in the Human Factors Verification and Validation Implementation Plan Technical Report (Reference 7.8-13).".

)6-P-A Rev.2 (Proprietary) and
, September 2009.

ysis, MUAP-07014-P Rev.5
on-Proprietary), September 2011.

Process, MUAP-07004-P Rev.7
on-Proprietary), May 2011.

UAP-07005-P Rev.8 (Proprietary)
y), July 2011.

oment That Is Not Safety-Related,
Generic Letter 89-06.

7.8-6 Requirements for Reduction of Risk from Anticipated Transients Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants, NRC Regulations Title 10, Code of Federal regulations, 10 CFR Part 50.62.

7.8-7 Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems, BTP 7-19 Revision 5, March 2007.

7.8-8 HSI System Description and HFE Process, MUAP-07007-P Rev.5 (Proprietary) and MUAP-07007-NP Rev.5 (Non-Proprietary), November 2011.

7.8-9 US-APWR Instrument Setpoint Methodology, MUAP-09022-P Rev.3 (Proprietary) and MUAP-09022-NP Rev.3 (Non-Proprietary), July 2013.

MIC-04-07-00001

Add
"7.8-12 Task Analysis Implementation Plan, MUAP-13009-P Rev.0 (Proprietary) and MUAP-13009-NP Rev.0 (Non-Proprietary), August 2013.

7.8-13 Human Factors Verification and Validation Implementation Plan, MUAP-10012-P Rev.3 (Proprietary) and MUAP-10012-NP Rev.3 (Non-Proprietary), August 2013.".

7.8 Diverse Instrumentation and Control Systems

The DAS is the non-safety diverse instrumentation and control system for US-APWR. The DAS provides monitoring, control and actuation of safety and non-safety systems required to cope with abnormal plant conditions concurrent with a CCF that disables all functions of the PSMS and PCMS. The DAS includes an automatic actuation function, HSI functions located at the diverse HSI panel (DHP), and interfaces with the PSMS and PCMS. The design basis and detailed system description for the DAS are described in the D3 Topical Report (Reference 7.8-1). Table 7.8-7 shows the supplemental information to Topical Report MUAP-07006-P-A, which is necessary to be clarified. The D3 Coping Analysis Technical Report (Reference 7.8-2) demonstrates the ability to maintain all critical safety functions and achieve hot standby using the DAS.

The DAS design consists of conventional equipment that is totally diverse and independent from the MELTAC platform of the PSMS and PCMS, so that a beyond design basis CCF in these digital systems will not impair the DAS functions. In addition, the DAS includes internal redundancy to prevent spurious actuation of automatic and manual functions due to a single component failure. The DAS is designed to prevent spurious actuations due to postulated earthquakes and postulated fires. The DAS interfaces with the safety-related process inputs and outputs of the SLS are isolated within these safety-related systems. In addition, hardwired safety-related logic within the SLS (not affected by a CCF) ensures that control commands originating in the DAS or SLS, which correspond to the desired safety function, always have priority. Therefore, there is no adverse interaction of the DAS with safety functions and no erroneous signals resulting from CCF in the SLS that can prevent the safety function. For a figure of the DAS system architecture, refer to Figure 4.2-6 of MUAP-07004.

Within the DAS, manual actuation is provided for systems to maintain all critical safety functions (Refer to Table 7.8-1). For conditions where there is insufficient time for manual operator action, the DAS provides automatic actuation of required plant safety functions needed for accident mitigation. Key parameter indications, diverse audible and visual alarms, and provisions for manual controls are located in a dedicated independent DHP located in the MCR. Conventional hardwired logic hardware and relays for automatic actuation are installed in four diverse automatic actuation cabinets (DAACs), each located in a separate Class 1E electrical room. Each DAAC is powered by a separate Class 1E UPS via qualified isolation device. During plant on-line operation, the system can be tested manually without causing component actuation that would disturb plant operations.

MIC-04-07-00001

7.8.1 System Description

The DAS consists of manual HSI functions, which include automatic actuation functions. These functions are located in the DHP and the DAAC, respectively. In addition, the DAS

Add "The DAS and PSMS share diverse Class 1E power sources within each separate train. Although these power sources are shared, the diversity between these power sources prevents the possibility of CCF. As shown in DCD Figure 7.1-4, the diverse Class 1E power sources are the UPS and the transformer. The UPS is powered diversely by the Class 1E GTG, the Class 1E Battery and the offsite power. Thus, the Class 1E power system itself has sufficient diversity and availability to assure power to the PSMS and DAS. Therefore, a separate power from Class 1E power sources is not required for the DAS power. Also, the PSMS and the DAS can be powered from the alternate non-safety GTG. In addition, the DAS power supply circuits are isolated from the Class 1E power sources system by qualified isolation devices (i.e., circuit breakers)." as fourth paragraph of Section 7.8.

7.3.1.2.3 Control of Interlocks Important to Safety

The SLS provides interlocks, which operate to reduce the probability of specific events occurring or to verify the state of a safety-related system. These include interlocks to prevent over pressurization of low-pressure systems and interlocks to ensure availability of ESF systems. Interlocks important to safety are discussed in Section 7.6.

7.3.1.2.4 Functional Allocation in SLS Controllers

For Functional Allocation in SLS Controllers, refer to MUAP-09020 “Function Assignment Analysis for Safety Logic System” (Reference 7.3-11).

MIC-04-07
-00001

7.3.1.3 Engineered Safety Features

For the US-APWR, the ESF consists of the ECCS, containment isolation systems, CSS, EFWS, annulus emergency exhaust system, and MCR HVAC system. These systems

Add
"7.3.1.2.5 Equipment Protection

Equipment features designed to protect against electrical faults or mechanical faults which can prevent the component from assuming its required position, have priority over the manual and automatic ESF actuation demand signals from the SLS or DAS, in accordance with IEEE Std. 603-1991 Section 7.3. These protections are installed in the wiring circuits of the safety-related switchgear, motor control center or distribution panel, downstream of the SLS and DAS. An electrical or mechanical fault in one of these components is a single failure. Therefore the other trains which are not subject to that fault are available to achieve the safety functions.

Other process related equipment protection signals, such as low pressure or low level signals, provide equipment protection only through an interface to the SLS application software. Thermal overload signals for the safety-related motor operated valves, which also interface to the SLS application software, are normally active, but are automatically bypassed within the SLS application software, when there is an ESF actuation demand signal, in accordance with RG 1.106 (Reference 7.3-13). Since these signals are not interfaced to any circuits downstream of the SLS, they are inherently bypassed by the DAS signals which interface with the PIF modules."

spatially dependent sensors that are required for the ESF actuation functions are described in Subsection 7.2.1.3 and identified in Table 7.3-4.

7.3.1.5 ESF Initiating Signals, Logic, Actuation Devices and Manual Controls

The following subsections provide a functional description of ESF actuation signals, actuated systems/components and initiating logic for actuating each ESF function.

Except as noted in specific sections below, all actuation signals are latched at the train level, whether automatically or manually initiated, and require manual reset. Latching ensures the protective action goes to completion and ensures that components remain in their safety position after the completion of protective action. Manual reset can be initiated after the completion of proactive action.

7.3-5 Physical Independence of Electric Systems, Regulatory Guide 1.75 Revision 3, February 2005.

7.3-6 Setpoints for Safety-Related Instrumentation, Regulatory Guide 1.105 Revision 3, December 1999.

7.3-7 IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, IEEE Std 603-1991.

7.3-8 IEEE Standard Design for Digital Computers in Safety Systems of Nuclear Power Generating Stations, IEEE Std 7-4.3.2-2003.

7.3-9 Standard Criteria for Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems, IEEE Std 338-1987.

7.3-10 Periodic Testing of Protection System Actuation Functions, Regulatory Guide 1.22 Revision 0, February 1972.

7.3-11 Function Assignment Analysis for Safety Logic System, MUAP-09020-P Rev.2 (Proprietary) and MUAP-09020-NP Rev.2 (Non-Proprietary), May 2011.

7.3-12 US-APWR Instrument Setpoint Methodology, MUAP-09022-P Rev.3 (Proprietary) and MUAP-09022-NP Rev.3 (Non-Proprietary), July 2013.

MIC-04-07 -00001

Add
"7.3-13 Thermal Overload Protection for Electric Motors on Motor-Operated Valves, Regulatory Guide 1.106 Revision 1, March 1977.".

The MCCs provide thermal overload protection to the motor operated valves in accordance with RG 1.106 (Reference 8.3.1-11). The thermal overload protection ~~devices are continuously bypassed. Alarms are provided in the MCR. During normal control modes or manual testing, motor operated valves are protected by manual de-energizing based on thermal overload alarm.~~

Delete.

MIC-04-07-00001

8.3.1.1.2.6 Testing of AC Systems during Power Operation

Add "are normally active, but are automatically bypassed, when there is an ESF actuation demand signal." after "protection".

All Class 1E circuit breakers ar tion. During periodic testing of Class tures actuation system, such as safety injection, containment spray, and containment isolation are actuated thereby causing appropriate circuit breaker or contactor operation. The 6.9kV and 480V switchgear circuit breakers and control circuits can also be tested independently while individual equipment is shutdown. These circuit breakers can be placed in test position and exercised without operation of the associated equipment. The use of jumpers or other temporary test arrangements which would bypass protective functions is not required to verify system capability to operate except during startup testing.

The testing of ac power systems is performed in accordance with IEEE Std 308, 338 and 603 (Reference 8.2-4) as endorsed by RG 1.32, 1.118 and 1.153 (Reference 8.3.1-19, 8.3.1-24 and 8.3.1-5). Bypassed and inoperable status indication is provided based on RG 1.47 (Reference 8.3.1-23) as described in Section 7.5.1.2. Surveillance testing of Class 1E ac power systems is described in detail in Chapter 16.

8.3.1.1.2.7 Sharing of Systems and Equipment between Units

The US-APWR is a single unit design, so there is no sharing of safety-related systems or components between units.

8.3.1.1.2.8 Class 1E Electrical Equipment Qualification

The electrical equipment identified as safety-related is qualified as Class 1E and is designated as seismic category I. The Class 1E equipment and components are capable of withstanding the environmental conditions to which they are exposed. The Class 1E equipment qualification meets the requirements of IEEE Std 323 (Reference 8.3.1-6), IEEE Std 344 (Reference 8.3.1-12) and applicable equipment standards.

8.3.1.1.3 Class 1E Standby Power Sources

GTG is used as Class 1E standby power sources for the US-APWR. Design of the Class 1E standby power sources for US-APWR is based on the use of qualified GTG for Class 1E applications based on the advantages shown below:

- The GTG is more reliable and has fewer components and auxiliary systems than diesel generators.
- The GTGs do not have cooling water requirements.

which prevent unintended changes during system operation and allow changes to be detected, should they occur.
[

]
The Section 6.1.6.4 describes the Existing Platform assessment.

6.1.6.1 Software and FPGA Development/Storage Security Measures

[

MIC-04-07-0
0001

]

MIC-04-07-0
0001

Figure 6.1-4 Security Measures of the Software Development/Storage Environment

[

]

Table 6.1-4 Security Measures of the Software Development/Storage Environment

MIC-04-07-001

MIC-04-07-001

[

MIC-04-07-001

]

Once actuated, either manually or automatically, the DAS signals are latched at the system level. This ensures all DAS functions actuate to completion. The DAS latches can be reset from the defeat switch located on the OC.

The overall DAS architecture is described in Topical Report MUAP-07006 Section 4.0. For manual and automatic system level, actuations from the DAS refer to functional logic diagram Figure 7.2-2 sheet 14.

7.8.1.1 Diverse HSI Panel

The DHP, which is located in the MCR, consists of conventional hardwired switches, conventional indicators for key parameters of all critical safety functions, and audible and visual alarms. The DHP installed equipment is used for manual control and actuations credited in the defense-in-depth and diversity coping analysis. Actuation status of each safety-related system actuated from the DHP can be confirmed by monitoring the safety function process parameters displayed on the DHP. The DHP is powered by a Class 1E UPS and located in the MCR. Also, the DHP is qualified as Seismic Category II.

7.8.1.1.1 Manual Actuation Switches

System level manual actuation is provided on the DHP for all automated functions and for systems required to maintain critical safety functions, which may not be automatically actuated. The following manual actuations are provided from conventional switches on the DHP:

- Reactor trip/turbine trip/MFW isolation: one switch
- EFW actuation: one switch
- ECCS: one switch
- Containment isolation: one switch
- EFW isolation and flow control: four switches (one per SG)
- Control of main steam depressurization valve: four swit
- ssurization valve: one switch
- line isolation valve: four switches (one per SG)

Add "in the power breaker for DHP" after "switch".

Add "in the power breaker for DHP" after "switch".

Delete.

To prevent spurious actuation due to a failure of any of the above switches, a separate manual actuation permissive switch is provided. The permissive switch is located in the MCR, but physically separated from the DHP to minimize the effect of fire propagation. The DAS permissive switch is powered by a Class 1E UPS that is separate from the power to the DHP. Signals from the manual actuation switches and permissive switch are interfaced separately from the MCR to each DAAC; refer to MUAP-07004 Section 4.2.6. To prevent spurious DAS actuation due to the MCR fire, all DAS manual actuation signals are blocked when the MCR/RSR transfer is activated, refer to the Safety I&C Technical Report (Reference 7.8-3) Figure 4.2-1.

MIC-04-07-00001

Add "in the power breaker for DHP" after "switch".

Add "in DHP" after "switches".

Add "in the power breaker for DHP" after "switch".

7.8.2.8 Defense-In-Depth and Diversity

The defense-in-depth and diversity approach is based on the following principles:

- Minimize the potential for CCF
- Cope with CCF for AOOs

DAS is implemented to mitigate the adverse effects/impacts from digital I&C both hardware and software common cause failure (CCF). It is not to minimize the potential or extent of software CCF.

A detailed description of each principle is provided in Topical Report MUAP-07006 Section 5.0.

7.8.2.9 Fire Protection

~~Fire~~ protection for the DAS is described in MUAP-07004 Subsection 6.5.8.

MIC-04-07-00001

Change to
"The DAS defeat switch which bypasses the automatic actuation functions of the DAAC is located on Operator Console in the MCR. The DAS permissive switch in the power breaker for DHP which enables the manual actuation functions of the DHP is located in the MCR adjacent to the DHP, but physically separated from the DHP manual actuation switches to minimize the effect of fire propagation. These DAS defeat and permissive switches and related cables are physically and electrically isolated from other circuits in the MCR, including the DHP, by fire barriers in accordance with IEEE 384-1992 (Reference 7.8-11) (i.e., in accordance with isolation between Class 1E and non-Class 1E circuits).

The DAS manual actuation function from the DHP in the MCR and automatic functions from the DAACs are disabled if the MCR/RSC Transfer switch is in the RSC position. Therefore, spurious manual actuation signals from the DHP can not be initiated as a result of a fire event in the MCR.

The DAS defeat switch on the Operator Console in the MCR can be manually actuated during plant heatup and cooldown conditions to prevent actuation of the DAS when it is not needed. The DAS defeat switch is in the enable position during normal plant operating conditions. DAS automatic functions are also disabled by the MCR/RSR transfer switch which allows achieving cold shutdown from the RSC without unnecessary DAS actuation.

For details, fire".

- ~~Containment integrity~~
- RCS integrity
- Secondary heat sink

Technical Report MUAP-07014 also confirms that there is sufficient time for all credited manual operator actions. The HSI on the DHP is designed, verified, and validated in accordance with the HFE program described in Chapter 18.

7.8.3.3 Conformance to BTP 7-19

Topical Report MUAP-07006 Appendix A provides a detailed description for the conformance of BTP 7-19 (Reference 7.8-7).

7.8.4 Combined License Information

No additional information is required to be provided by a COL Applicant in connection with this section.

7.8.5 References

7.8-1 Defense-in-Depth and Diversity, MUAP-07006-P-A Rev.2 (Proprietary) and MUAP-07006-NP-A Rev.2 (Non-Proprietary), September 2009.

7.8-2 Defense-in-Depth and Diversity Coping Analysis, MUAP-07014-P Rev.5 (Proprietary) and MUAP-07014-NP Rev.5 (Non-Proprietary), September 2011.

7.8-3 Safety I&C System Description and Design Process, MUAP-07004-P Rev.7 (Proprietary) and MUAP-07004-NP Rev.7 (Non-Proprietary), May 2011.

7.8-4 Safety System Digital Platform -MELTAC-, MUAP-07005-P Rev.8 (Proprietary) and MUAP-07005-NP Rev.8 (Non-Proprietary), July 2011.

7.8-5 Quality Assurance Guidance for ATWS Equipment That Is Not Safety-Related, Generic Letter 85-06.

7.8-6 Requirements for Reduction of Risk from Anticipated Transients Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants, NRC Regulations Title 10, Code of Federal regulations, 10 CFR Part 50.62.

7.8-7 Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems, BTP 7-19 Revision 5, March 2007.

7.8-8 HSI System Description and HFE Process, MUAP-07007-P Rev.5 (Proprietary) and MUAP-07007-NP Rev.5 (Non-Proprietary), November 2011.

7.8-9 US-APWR Instrument Setpoint Methodology, MUAP-09022-P Rev.3 (Proprietary) and MUAP-09022-NP Rev.3 (Non-Proprietary), July 2013.

MIC-04-07-00001

Add
"7.8-11 Criteria for Independence of Class 1E Equipment and Circuits, IEEE Std 384-1992.".

ACRONYMS AND ABBREVIATIONS (CONTINUED)

RSR	remote shutdown room
RT	reactor trip
RTB	reactor trip breaker
RTD	resistance temperature detector
RTP	rated thermal power
RV	reactor vessel
RVWL	reactor vessel water level
RWSP	refueling water storage pit
SBLOCA	small break loss-of-coolant accident
SDCV	spatially dedicated continuously visible
SG	steam generator
SGTR	steam generator tube rapture
SIP	safety injection pump
SIS	safety injection system
SLS	safety logic system
SPDS	safety parameter display system
SPM	Software Program Manual
SRM	staff requirements memorandum
SRP	Standard Review Plan
SRSS	square root sum of the squares
SSA	signal selection algorithm
S-VDU	safety VDU
T_{avg}	average temperature
T_{cold}	cold temperature
T_{hot}	hot temperature
TSC	technical support center
UHS	ultimate heat sink
UPS	uninterruptible power supply
UV-ROM	Ultra-Violet Erasable Programmable Read Only Memory
VCT	volume control tank
V&V	verification and validation
VDU	visual display unit

MIC-04-07-00001

Add "WDT watchdog timer"

i. The supplier may have a 10 CFR 50 Appendix B quality program with previously qualified Class 1E software.

ii. Other software may be sufficiently simple to allow for 100% testing.

iii. Other software may be commercially dedicated in accordance with EPRI TR-107330 (Reference 7.1-33) or TR-106439 (Reference 7.1-34), as applicable.

d. Safety or non-safety equipment credited in the diversity and defense-in-depth analysis - Only analog equipment is planned to be used. If equipment with embedded software must be employed, conformance to the diversity and defense-in-depth analysis will be demonstrated.

e. All qualification and analysis documentation will be maintained in accordance with MHI's quality assurance program.

7.1.3.9 Redundancy Within Divisions and Systems

To prevent disturbance of the plant caused by a single failure of the safety-related or non-safety I&C systems, a redundant configuration is applied. Failed components, including CPU, I/O modules, and communication modules, are detected by self-diagnostic features. Redundant components are arranged in configurations for continuous parallel operation or standby operation, as described in MUAP-07005 Subsection 4.1.1.1. For standby op[...]nt stand-by component[...]e uninterrupt[...]

Add "which consist of software based detection functions and hardware based detection circuits, such as watchdog timers (WDTs)" after "features".

Ac power for the I&C s[...] the power supplies with[...] failure of the electric po[...]

Change to "If any failures that disable safety functions are detected by these self-diagnostic features, alarms are generated in the MCR and safety-related signals are forced into a predetermined safe status, such as, “fail-safe” for reactor trip signals and “fail as-is” for the ESF actuation signals as shown in Figure 7.1-8. Lower priority alarms are generated in the MCR for other failures that do not disable the safety functions, such as a failure of one controller in a parallel redundant pair; where a".

7.1.3.10 Self-Diagn[...]

The integrity of digital I&C components is continuously checked by their self-diagnostic features. These self-diagnostic features result in early detection of failures and allow on-line repair that improves system availability. Information about detected failures is gathered through networks and provided to maintenance staff in a comprehensive manner. ~~In addition, the self-diagnostic features control~~ redundant controller configuration~~, to maintain all system functions,~~ even in the presence of failures. The self-diagnosis is always working in the digital control system but does not affect system operation. Therefore, there is no [...] and compliance to the single failure c[...]

MIC-04-07-00001

MIC-04-07-00001

Change ", to maintain all system functions," to " is employed to maintain all system functions".

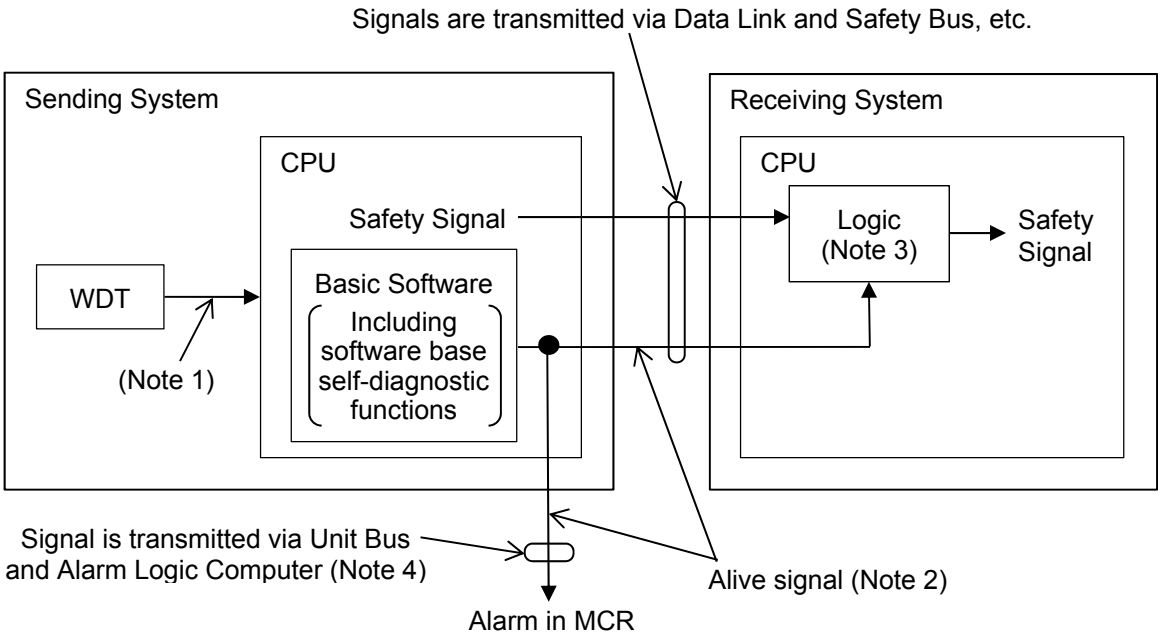
MIC-04-07-00001

Continuous self-diagnostic features allow elimination of most of the manual surveillance testing required for technical specification compliance. Manual testing and manual calibration verification are specifically provided for functions with no self-diagnosis. The [...]memory [...]diagnosis. For [...]PSMS [...]cted to the [...]by an

Add "There are numerous self-diagnostic functions and WDT functions within the different modules of the MELTAC digital platform. Each WDT is continuously reset (avoiding timeout) based on the cyclical execution of the module's function. A WDT times out when the cyclical execution is interrupted, indicating a failure. A WDT timeout within one module is detected by another module in the same controller or in another controller through loss of data communication with the failed module. This other module/controller then generates an alarm signal for the failure. The details of the self-diagnostic functions and the WDTs are described in MUAP-07005 Subsection 4.1.5.".

Add Figure 7.1-8.

MIC-04-07-00001



Note 1) Detection of the WDT timeout means that the CPU cyclic operation is stopped.
Note 2) The Alive signal is updated normally. The Alive is not updated if the CPU of sending system is stopped.
Note 3) If the Alive signal is not updated, the safety signal is forced in the pre-determined position, such as, “fail safe” for the Reactor Trip signals, and “fail as is” for the ESF actuation signals in the receiving system.

Figure 7.1-8 Self-diagnostic Features

Figure 4.1-16 Remaining Time Diagnosis

[

]

MIC-04-07-00001

Each detected error is categorized into the three types (Failure, Alarm and I/O Alarm) as below.

1) Failure

The fatal abnormality by which the Subsystem cannot continue its functions is categorized as the Failure.
When the Subsystem detects this type of error, it transits to the Failure mode.
[MIC-04-07-00001

] MIC-04-07-00001

In the Failure mode, on the other hand, the processing of input/output and operation are stopped, although the processing of sending the own status data of the Failure mode is continued.
[MIC-04-07-00001

] MIC-04-07-00001

In case of redundant standby controller configuration, when the Subsystem in the Control mode changes to the Failure Mode and the Subsystem in the Standby mode changes from the Standby Mode to the Control Mode and continues the control function.

When there is no Subsystem which communicates with the controller's Output Module, the Output Module transits to the Failure mode which is "as-is mode" or "off mode". This mode is preset at the application level ~~set preliminarily~~. MIC-04-07-00001 MIC-04-07-00001

2) Alarm

The minor abnormality with which the Subsystem can continue its functions is categorized as the Alarm. This includes the error of the Controller Cabinet.
When the Subsystem detects this type of error, it does not change its mode and only warns of the alarm. This abnormality is communicated to other systems for alarming via Data Link or the Control Network, as configured at the application level. MIC-04-07-00001

3) I/O Alarm

The abnormality of I/O is categorized as the I/O Alarm.
When the Subsystem detects this type of error, it does not change its mode and only warns of the alarm. This abnormality is communicated to other systems for alarming via Data Link or the Control Network, as configured at the application level. MIC-04-07-00001
In case of redundant standby controller configuration, when the I/O Alarm occurs in the Redundant I/O in the Control Mode, the Subsystem stops to use this I/O, switches the other I/O from the Standby mode to the Control Mode, and continues the processing of input/output.
When the I/O Alarm occurs in the Single Input Module, the last good input values are retained and the application software is informed of the abnormal state of the input signals. For digital inputs, the input values are kept at the last value (1 or 0) before the error occurred. For analog inputs, the input values are kept at the last engineering value before the error occurred.
Based on the error flag, the application software can be programmed for a predetermined control action.

4.1.5.1 Coverage of Self-diagnosis

Coverage of Self-diagnosis of the controller is shown in Figure 4.1-17.

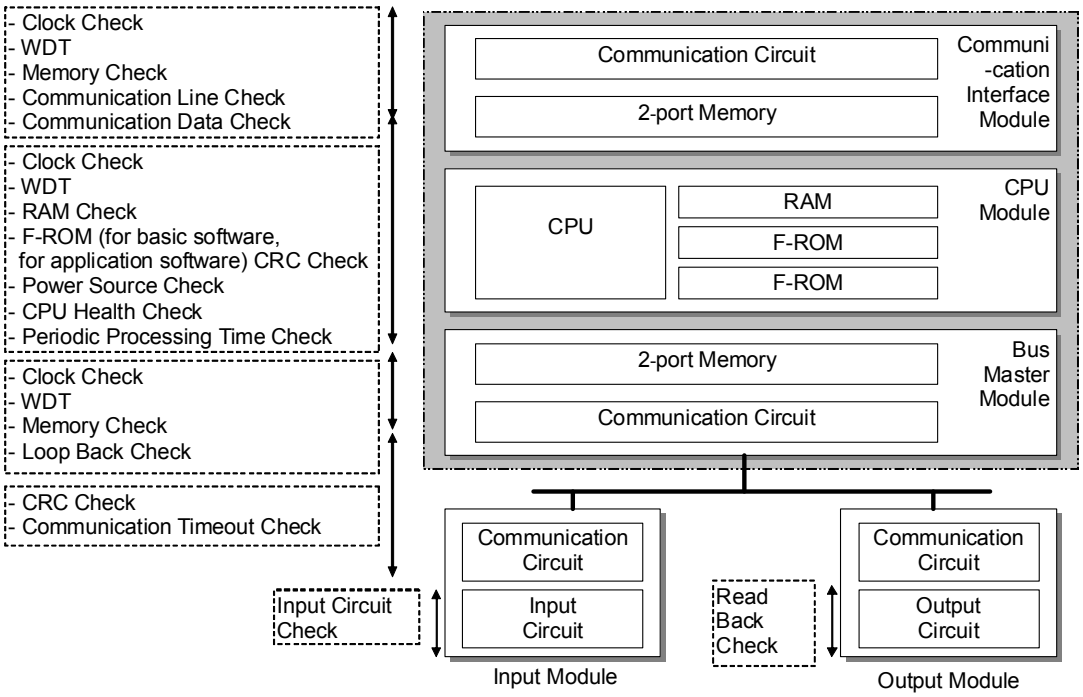


Figure 4.1-17 Coverage of Self-diagnosis function of the controller

4.1.5.2 Self-diagnosis of the controller

The self-diagnosis of the processor modules is described below.
Each diagnosis item is shown with the timing of diagnosis classified as follows:
- Initialization: At the time of initialization
- Self-diagnosis: Once per cycle in the constant cycle operation
- Remaining Time Diagnosis: Periodically in the remaining time of constant cycle operation, but not every cycle.
- Constant: On a constant basis by Hardware

4.1.5.2.1 CPU Module

[

]

MIC-04-07-000 01

[

MIC-04-07-00001

MIC-04-07-00001

MIC-04-07-00001

MIC-04-07-00001

MIC-04-07-00001

MIC-04-07-00001

]

4.1.5.2.2 Bus Master Module

[

MIC-04-07-00001

MIC-04-07-00001

MIC-04-07-00001

MIC-04-07-00001

MIC-04-07-000 01

MIC-04-07-000 01

MIC-04-07-000 01

MIC-04-07-000 01

MIC-04-07-000 01

]

4.1.5.2.3 Control Network I/F Module

[

MIC-04-07-000 01

MIC-04-07-00001

]

4.1.5.3 Self Diagnosis of Power Supply Modules in the CPU Chassis

[

]

4.1.5.4 Self-diagnosis of the Communication System

See Section 4.3.2.4 and 4.3.3.4. Communication System errors are categorized as “Failure” or “Alarm”, depending on the redundancy configuration of the controller.

4.1.5.5 Self-diagnosis of I/O Modules

The self-diagnosis of the I/O Mmodules is described below.

MIC-04-07-000 01

4.1.5.5.1 Input Module

[

MIC-04-07-000 01

MIC-04-07-000 01

MIC-04-07-000 01

MIC-04-07-00001

]

4.1.5.5.2 Output Module

[

MIC-04-07-00001

MIC-04-07-00001

MIC-04-07-00001

MIC-04-07-00001

MIC-04-07-00001

MIC-04-07-00001

]

4.1.5.5.3 Controller Cabinet

[

MIC-04-07-00001

4.1.5.7 Watchdog timer (WDT)

This section provides a description of the WDT architecture and how WDT timeout errors are processed in the MELTAC modules. [

]

4.1.5.7.1 Architecture of the WDT

The following describes the detailed WDT mechanism. Figure 4.1-18 shows the WDT mechanism, taking the CPU Module as an example. The left-side of the figure represents the elements related to the WDT in the CPU Module. The right-side of the figure shows the WDT behavior, regarding count-up, counter reset, and timeout when the counter value reaches a predefined value.
The flow of the WDT operations and controls is as follows:

(1)The WDT consists of a counter with a hardware clock generator, and predefined timer value (for WDT timeout).
(2)After initialization, the timer starts to count up.
(3)The basic software resets the timer to zero at regular intervals (i.e. for each operation cycle)
(4)If the basic software does not reset the WDT within a predefined timer value, then the WDT times out and the controller transitions to a Failure mode (see section 4.1.5) with an alarm indication.

The mechanism of other modules is the same as that of the CPU Module.

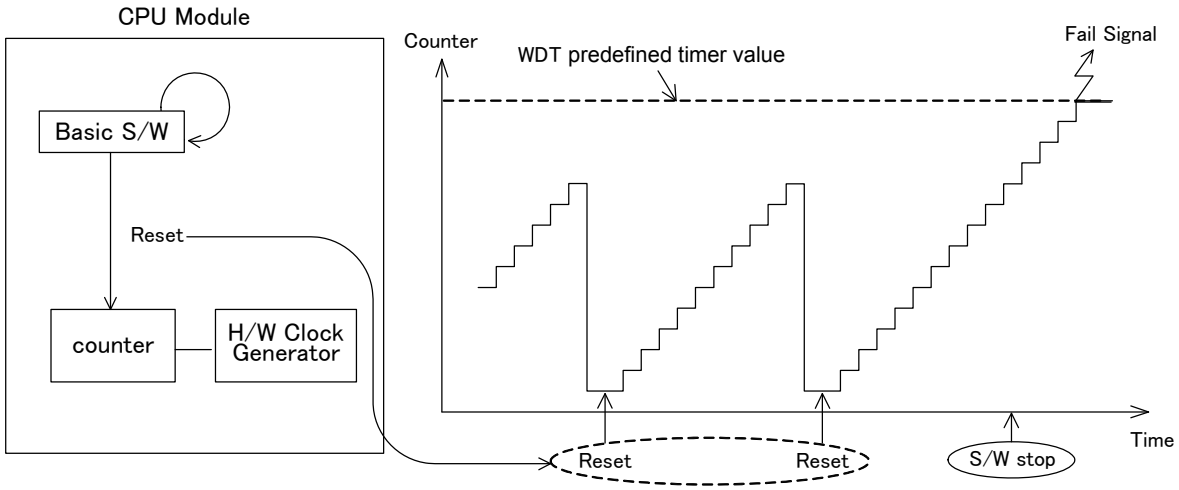


Figure 4.1-18 Mechanism of WDT (CPU Module)

4.1.5.7.2 WDT Timeout process (per Module)

[

MIC-04-07-0000 1

]

Figure 4.1-19 WDTs mounted in MELTAC platform

MIC-04 -07-000 01

Table 4.1-6 WDT Timeout process (1/3)

Mod	Timeout occurrence part	Transition of own controller	Process signal output	No	Communication path to other controllers	Information passed to other controllers	How it is shown from other controllers

Table 4.1-6 WDT Timeout process (2/3)

Mod	Timeout occurrence part	Transition of own controller	Process signal output	No	Communication path to other controllers	Information passed to other controllers	How it is shown from other controllers

Table 4.1-6 WDT Timeout process (3/3)

Mod	Timeout occurrence part	Transition of own controller	Process signal output	No	Communication path to other controllers	Information passed to other controllers	How it is shown from other controllers

ACRONYMS AND ABBREVIATIONS (CONTINUED)

DNB	departure from nucleate boiling
E/O	electrical to optical (or optical to electrical)
ECCS	emergency core cooling system
EFW	emergency feedwater
EFWS	emergency feedwater system
EHGS	turbine electro-hydraulic governor control system
EMI	electromagnetic interference
EOF	emergency operations facility
EOP	emergency operating procedure
EPG	emergency procedure guideline
ERDS	emergency response data system
ESF	engineered safety features
ESFAS	engineered safety features actuation system
ESW	essential service water
ESWS	essential service water system
FLB	feedwater line break
FMEA	failure modes and effects analysis
FPGA	Field Programmable Gate Array
F-ROM	Flash Electrically Erasable Programmable Read Only Memory
GDC	General Design Criteria
GTG	gas turbine generator
HEPA	high-efficiency particulate air
HFE	human factors engineering
HJTC	heated junction thermocouple
HSI	human-system interface
HSIS	human-system interface system
HVAC	heating, ventilation, and air conditioning
I&C	instrumentation and control
I/O	input/output
IAS	instrument air system
ICC	inadequate core cooling
IEEE	Institute of Electrical and Electronics Engineers
ITAAC	inspections, tests, analyses, and acceptance criteria
ITV	industrial television
LBLOCA	large break loss-of-coolant accident
LCSR	loop current step response
	rge display panel
LOCA	loss-of-coolant accident

MIC-04-07-00001

Add "IV intercept valve".

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
	tory Commission
NUREG	NRC Technical Report Designation (Nuclear Regulatory Commission)
OC	operator console
OEM	original equipment manufacturer
OS	operating system
O-VDU	operational VDU
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

MIC-04-07-00001

Add "MTCV main turbine control valve".

MIC-04-07-00001

Add "OPC overspeed protection controller".

7.7.1.1.11.1 Plant Startup and Shutdown

During plant startup and shutdown, the difference between measured steam header pressure and a pressure setpoint is used to generate a turbine bypass demand signal. This mode is used for low-power conditions (up through turbine synchronization). This mode is also used during plant cooldown for decay heat removal between hot standby and entry conditions for the RHR system.

The steam header pressure control mode is manually selected by the operator. The pressure setpoint is manually adjusted by the operator to obtain the desired reactor coolant temperature.

7.7.1.1.11.2 Normal Operation

In this mode, the turbine bypass control function is in a standby condition to modulate the turbine bypass valve to control T_{avg} to a reference temperature derived from turbine inlet pressure.

7.7.1.1.11.3 Load Rejection

The US-APWR is designed to sustain a full load rejection, without generating a RT, atmospheric steam relief, or actuating a pressurizer or main steam line safety relief valve(s).

Full load rejection means an event when the main generator is cut off from transmission system either by tripping the main transformer breaker or the switchgear breaker without causing a turbine trip or the main generator trip. In this scenario, the main turbine control valve is immediately fully closed, and four banks of turbine bypass valves are tripped opened, to fully dump excess steam to the condenser.

MIC-04-07-00001

Reactor power is decreased by automatic control of control rods. The automatic turbine bypass control function, in conjunction with other control systems, is provided to

Add "The main turbine control valves (MTCVs) and intercept valves (IVs) are controlled by the overspeed protection controller (OPC) upon a loss of load, as described in DCD Subsection 10.2.2.3.1.5. All of the MTCVs and IVs are fully closed by the OPC in response to a full load rejection event. After the turbine speed falls below the rated speed following the OPC action, the MTCVs and IVs are reopened, and the turbine resumes normal speed control by the turbine control system." as third paragraph.

the reactor control system, is sufficient to handle load rejections (i.e., a step load decrease of 100% of the rated load.)

The turbine bypass control function prevents a large increase in reactor coolant temperature following a large, sudden load decrease. The error signal is the difference between the lead-lag compensated selected T_{avg} and the reference T_{avg} (designated T_{ref}), which is based on turbine inlet pressure and a difference between the nuclear power signal and the turbine inlet pressure. The lead-lag compensation for the T_{avg} signal compensates for lags in the plant thermal response and in valve positioning. The addition of the difference between the nuclear power signal and the turbine inlet pressure with a

heat removal system, containment spray system, and essential service water system, are mechanically separated in each train.

Change to "because".

Delete.

- There are no automatic interlocks required to preclude inadvertent inter-ties between redundant trains of the CCWS ~~since~~ a single failure of one CCW pump would not cause pump run out in the other CCW pump ~~during an accident condition~~, even if the isolation valves between safety trains remain open and there is sufficient time margin for manual isolation. The header tie line isolation valve is manually closed within 24 hours after an ECCS signal to establish separation of the two trains within a subsystem as described in Subsection 9.2.2.2.

Delete.

MIC-04-07-00001

- Redundant I&C trains are protected from inadvertent inter-ties, such as those cause by electrical faults, by qualified isolation devices described in Subsection 7.1.3.5.

- Inadvertent inter-ties between safety-related systems and the DAS are discussed in Section 7.8.

- Redundant mechanical trains (i.e., redundant CCW trains) are protected as discussed in Subsection 7.6.1.5.

7.6.4 Combined License Information

No additional information is required to be provided by a COL Applicant in connection with this section.

7.6.5 References

7.6-1 HSI System Description and HFE Process, MUAP-07007-P Rev.5 (Proprietary) and MUAP-07007-NP Rev.5 (Non-Proprietary), November 2011.

7.6-2 IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, IEEE Std 603-1991.

7.6-3 IEEE Standard Design for Digital Computers in Safety Systems of Nuclear Power Generating Stations, IEEE Std 7-4.3.2-2003.

7.6-4 Safety I&C System Description and Design Process, MUAP-07004-P Rev.7 (Proprietary) and MUAP-07004-NP Rev.7 (Non-Proprietary), May 2011.

7.6-5 Combined License Applications for Nuclear Power Plants (LWR Edition), Regulatory Guide 1.206 Revision 0, June 2007.

7.5.1.1.3.1 Degrees of Subcooling

The degrees of subcooling variable utilizes sensors for reactor coolant cold and hot leg temperatures, core exit temperature, and reactor coolant pressure.

The saturation temperature is calculated from the minimum pressure input. The temperature subcooled margin is the difference between saturation temperature and the sensor temperature input.

Two temperature subcooled margin presentations are available as follows:

- RCS saturation margin - the temperature saturation margin based on the difference between the saturation temperature and the maximum temperature from the resistance temperature detectors (RTDs) in the hot and cold legs.
- Upper head satu re saturation margin based on the difference between the saturation temperature and the core exit temperature.

Add "the" after "with".

Add "." after "tube."

7.5.1.1.3.2 Reactor Vessel Water Level

Delete.

Delete.

The RVWL probe assembly measures reactor coolant liquid inventory ~~above the fuel alignment plate~~ with discrete heated junction thermocouple (HJTC) sensors located at different levels within a separator tube ~~ranging from the top of the fuel alignment plate to the RV head.~~ The basic principle of operation is the detection of a temperature difference between adjacent heated and unheated thermocouples.

MIC-04-07-00001

Change to "The span of this measurement ranges is from the bottom of the hot leg to the top of the reactor vessel".

The HJTC sensor consists of a thermocouple another thermocouple positioned away from the with relatively good heat transfer properties, the adjacent thermocouples is small. In a fluid with the temperature difference between the thermocouples is large.

Two RVWL probe assemblies provide two channels of HJTC instruments. Each HJTC probe assembly includes six HJTC sensors. The two probe assemblies are assigned to two electrically independent trains.

The heater power for the HJTC is supplied by a dedicated heater power supply for HJTC.

7.5.1.1.3.3 Core Exit Temperature

There are 39 core exit thermocouples. Thermocouples are threaded into individual guide tubes that penetrate the RV closure head through seal assemblies and terminate at the exit flow end of the fuel assemblies. All thermocouples are arranged in two safety trains and one non-safety train; the two safety trains are independent. The two safety trains interface with the RPS and provide signals for PAM. Core exit thermocouples provide a measure of core heat up via measurement of core exit fluid temperature.

2.5.6 Data Communication Systems

2.5.6.1 Design Description

The data communication systems (DCS) consist of:

- Plant-wide unit bus
- Safety bus (for each PSMS division)
- Data links for point-to-point communication
- Input/Output (I/O) bus
- Maintenance network for each PSMS division and the PCMS

The DCS is a distributed and highly interconnected system as shown in Figure 2.5.6-1, which has communication independence to prevent electrical and communication processing faults in one safety division (or the non-safety PCMS) from adversely affecting the performance of safety functions in other divisions. Qualified fiber-optic isolators are used to prevent electrical faults from transferring between divisions, and between safety and non-safety systems. Communication faults are prevented through data integrity verification.

A non-redundant non-safety multi-drop maintenance network is provided separately within each PSMS division and within the PCMS. The maintenance network is used to transmit signals between the engineering tools and the PSMS or PCMS system management module of each controller.

1. Deleted.

2. Deleted.

3. The DCS provides external networks with a communications link via the unit management computer (UMC) which is connected to the unit bus. ~~The UMC provides a firewalled~~ interface, which allows only outbound communication from the unit bus to external networks. There are no other connections from external sources to the DCS.

MIC-04-T1-00001

Change to "The isolation device, which is located between the UMC and the station bus, provides a hardware-based unidirectional".

~~a~~ facility area that provides ~~s~~iles, pipe breaks and flooding.

5. The PSMS application setpoints, constants and application software are changeable only by removing the CPU module that contains the memory devices from the controller and placing it in a dedicated re-programming chassis.

6. Digital communication independence is achieved by communication processors that are independent of RT and ESF actuation processing functions of the redundant divisions of the PSMS, and also between non-safety systems and the PSMS.

Table 2.5.6-1 Data Communication Systems Inspections, Tests, Analyses, and Acceptance Criteria (Sheet 1 of 2)

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
1. Deleted.	1. Deleted.	1. Deleted.
2. Deleted.	2. Deleted.	2. Deleted.
3. The DCS provides external networks with a communications link via the unit management computer (UMC) which is connected to the unit bus. The ~~UMC provides a firewalled~~ interface, which allows only outbound communication from the unit bus to external networks. There are no other connections from external sources to the DCS.	3. Inspection and analyses of the as-built DCS will be performed.	3 A report exists and concludes that: (1) the as-built DCS provides external networks with a communications link via the as-built unit management computer (UMC), which is connected to the as-built unit bus; (2) the as-built ~~UMC provides a firewalled~~ interface, which allows only outbound communication from the as-built unit bus to external networks; and (3) there are no other connections from external sources to the as-built DCS.
the DCS are located in a facility area that provides protection from accident related hazards such as missiles, pipe breaks and flooding.	nspection and analyses will be performed on the safety-related portion of the as-built DC	4. A report exists and concludes that the safety- related portions of the as-built DCS are located area that rom ards such aks and

Change to "The isolation device, which is located between the UMC and the station bus, provides a hardware-based unidirectional".

Change to "isolation device, which is located between the UMC and the station bus, provides a hardware-based unidirectional".

MIC-04-T1-00001

Security-Related Information – Withheld Under 10 CFR 2.390

Change to "The isolation device, which is located between the unit management computer and the station bus, provides a hardware-based unidirectional interface which allows only outbound communication.".

7.9.1.6 Station Bu

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.

MIC-04-07-00001

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.

MIC-04-07-00001

Change to "hardware-based unidirectional interface provided by the isolation device. The hardware-based unidirectional interface".

7.9.2 Design Basis

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.

MHI applies its MELCO's safety system digital platform 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

conformance of BTP 7-21 and how the safety-related I&C system meets the performance requirements are also addressed in the Response Time Technical Report.

7.9.2.3.1 System Deterministic Timing

All DCS communication protocols allow calculation of a deterministic data communication response time. The time calculation includes the number of nodes on the network, data traffic, network topology, node processing cycle time, and network throughput. The methods used for real-time performance calculations are described in the MELTAC Platform Technical Report (Reference 7.9-1) Section 4.4.

7.9.2.3.2 Real-Time Performance

Real-time performance is determined by performing response time analysis for all safety-related functions. For each safety function an analysis has been performed which demonstrates the actual system response time is less than the response time required by the plant safety analyses. Refer to MUAP-07004 Subsection 6.5.3 for the related details. Response times for the RTS and ESFAS functions are listed in Tables 7.2-3 and 7.3-4 respectively.

7.9.2.3.3 Time Delays within the DCS

Data propagation delays due to data communication in the DCS are incorporated into response time analysis. Response time calculations, which encompass the controller and all components connected to the DCS, include these data propagation delays. DCS response time calculations are validated through sample tests, during system integration testing, refer to the Safety I&C Technical Report (Reference 7.9-2) Subsection 6.5.3.

7.9.2.3.4 Data Rates and Bandwidth

The data rates and bandwidths for the sections of the DCS are listed in the MELTAC Platform Technical Report (Reference 7.9-1) as follows:

- Control network: Table 4.3-2.
- Data links: Subsection 4.3.3.
- Maintenance network: Subsection 4.1.4.2.
- I/O bus: Appendix A.3.
- Safety VDU communication: Appendix A.11 and A.12.

7.9.2.3.5 Interfaces with other DCS

The only interface from the DCS 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 the EOF computers, the NRC (via ERDS), corporate information systems, and plant personnel computers.

MIC-04-07-00001

Change to "hardware-based unidirectional interface provided by the isolation device. The hardware-based unidirectional interface".

Security-Related Information – Withheld Under 10 CFR 2.390

MIC-04-07-00001

7.9.2.6 Cyber Security

The use of computer systems for various functions at nuclear power plants including digital I&C systems increases the potential for threats from cyber intrusions.

7.9.2.7 Independence

The DCS ensures electrical independence between PSMS trains and between the PSMS and PCMS to meet the single failure criterion. Summary descriptions of the independence design are described below.

Each PSMS and PCMS controller/processor protects itself against DCS errors or failures that could disrupt its internal application functions, thereby ensuring communications independence. For more detailed discussion on the methods used to ensure independence between digital systems in different trains and between safety-related and non-safety systems refer to Subsections 7.1.3.4, 7.1.3.5 and 7.1.4 and MUAP-07004 Appendix A.5.6,Appendix B.5.6 and Appendix F.

(1) Physical Independence

The four trains of the PSMS are physically independent from each other and from the non-safety systems. Cabinets for each train of the PSMS are located in a separate plant equipment room fire area (one per train). These fire areas are separate from the fire areas where non-safety systems are located. All PSMS DCS cables, with the exception of its maintenance networks, are routed in accordance with IEEE Std 384-1992 (Reference 7.9-5) to ensure physical independence of each train. PSMS maintenance network cables, which are non-safety, are routed with other non-safety cables, including PCMS DCS cables.

(2) Electrical Independence

Each train of the PSMS is powered from the independent class 1E power source. The four trains of the PSMS are electrically independent from each other and from the PCMS. To ensure electrical independence, fiber optic cables or qualified isolation devices are used to interface all signals between the PSMS trains and between the PSMS and the PCMS. In addition, electrical independence is maintained within the PSMS and PCMS, where the communication interfaces cross fire areas of the MCR and RSR.

(3) Communication Independence

Communication independence ensures the deterministic processing of the safety functions within each PSMS train is not disrupted by the interdivisional communication.

MIC-04-09 -00001

These links will include both verbal and data communications. ~~A firewall system~~ is provided to protect the plant broadband systems. The use of these alternate links provides access to the nationwide telephone system. They allow the plant to operate and meet regulatory requirements.

Change to "An isolation device, which provides a hardware-based unidirectional interface,".

9.5.2.2.5.2 Emergency Communications

Effective emergency onsite and ...led by the onsite PABX and the offsite emergency ...e systems allow for communications during norm... ...ing design basis accidents, fire, and LOOP.

The offsite communication system is located in the offsite emergency response center identified in 10 CFR 50.47 (b)(8). It is described by the COL Applicant. The effectiveness of the over all Emergency Response Plan pursuant to 10 CFR 50.47 (b)(8) (Ref. 9.5.2-2) is addressed by the COL Applicant.

The PA/PL, PABX, and plant radio systems are normally used for intra-plant normal and emergency communications with the SPTS providing additional capability and backup.

Radiation and fire alarms have priority over page. When the page system receives alarm inputs from the fire or radiation panels, it automatically provides audible messages and tone annunciation in accordance with specified schedules.

The following radio systems provide both in-plant and plant-to-offsite emergency communications:

- Crisis management radio systems in accordance with the intent of NUREG-0654 (Ref. 9.5.2-24)
- Fire brigade radio system, in accordance with BTP SPLB 9.5-1, position C.5.g(4) (Ref. 9.5.2-25)

The emergency offsite communication system, including the crisis management radio system, is addressed by the COL Applicant. The fire brigade radio system is site-specific, consisting of a base unit, mobile units, and portable units, also is addressed by the COL Applicant.

9.5.2.3 Safety Evaluation

Plant communication systems are not required to mitigate a design basis accident, however they are important to safety. These systems are needed to support effective normal and off-normal operations as well as to coordinate on-site and off-site responses during abnormal or emergency events. The off-site communications systems within the one-site operations support center provide for emergency response following a design basis accident. Redundant communication paths and technologies are employed to minimize the possibility of complete loss of on-site and off-site communications.

- A data communication system establishes the interface and link with the TSC, the EOF, and the ERDS and allows data exchange with the plant. The TSC receives plant information from the unit bus.

- The EOF and the ERDS receive plan

- The following countermeasures are

  • The plant instrumentation and control (I&C) and HSI systems do not link to external networks. An exception is the link from unit management computer to the station bus.

  • Communication from the unit management computer to the station bus is restricted one direction. ~~A dedicated transmission protocol is used which is not general-purpose, such as transmission control protocol/internet protocol, user datagram protocol, etc.~~

  • Communication between the station bus and the TSC, the EOF or the ERDS (NRC) is also one direction and uses a dedicated transmission protocol.

  • If a computer system, which has a general-purpose local area network, is connected to the station bus, an adequate gateway processor with a firewall function is inserted.

  • The firewall program currently used is MISTY®, which uses 128-bit code key. This firewall program is safer than the data encryption standard code, which is more typically used in the U.S. Alternate firewall programs may be used in the future, as the security features of new technology evolve.

• Safety Parameter Display System (SPDS)

  The SPDS provides a display of plant parameters from which the safety status of operation may be assessed in the MCR, the TSC, and the EOF. The SPDS provides the following functions:

  - The primary function of the SPDS is to help operating personnel in the MCR make quick assessments of the plant safety status.

  - Duplication of the SPDS displays in the TSC and the EOF improves the exchange of information between these facilities and the MCR and assists corporate and plant management in the decision-making process.

  - The SPDS is operated during normal operations and during all classes of emergencies.

  - The SPDS has the flexibility to allow future modifications to be incorporated, such as the capability to handle operator interaction and diagnostic analysis.

Add "via isolation device which provides hardware-based unidirectional interface" after "direction".

Delete.

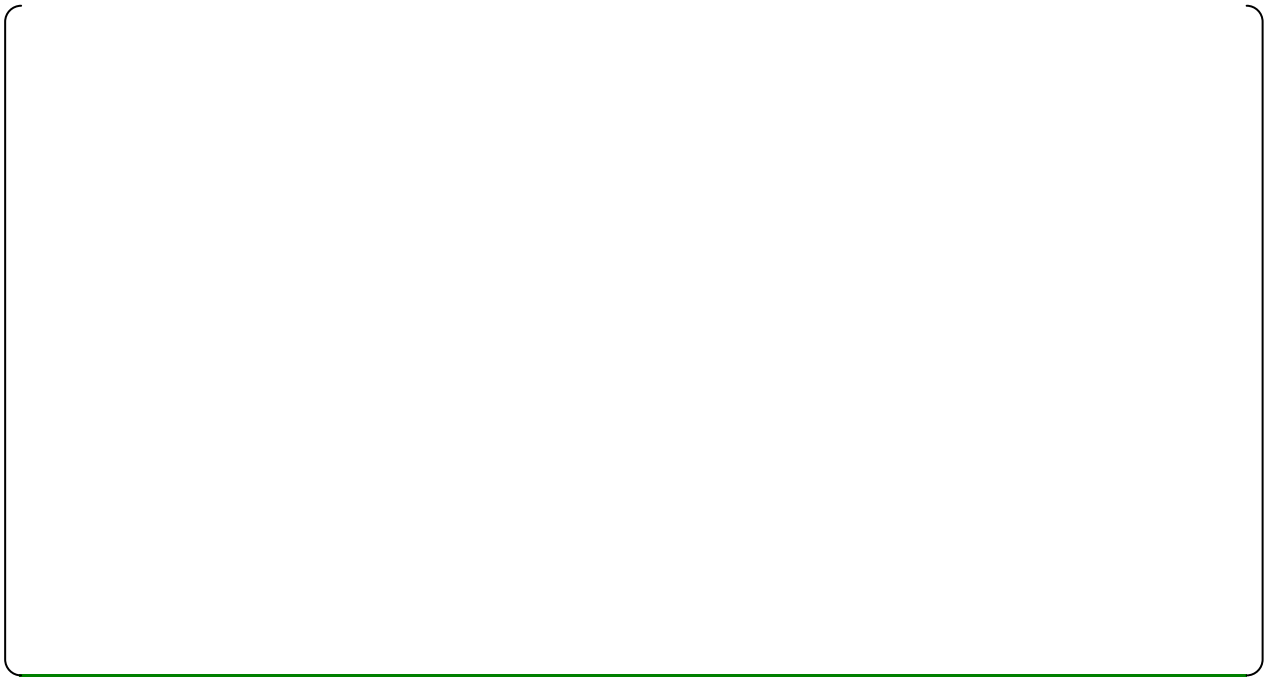
MIC-04-13-00001

4.2.7 Digital Data Communication

The following digital data communication interfaces are provided in the I&C system;

- The Unit bus provides bi-directional communication between safety-related and non-safety systems for only non-safety functions. The safety-related system and non-safety system are functionally isolated by dedicated communication processors in each safety-related system controller, and priority logic within the safety train that ensure safety-related functions have priority over all non-safety functions. Unit bus uses optical fiber to achieve electrical independence of each train. Physical separation between safety-related and non-safety system is accomplished by locating the safety and non-safety trains in different areas. The Unit bus uses the Control Network digital communication technology described in the Platform Technical Report, MUAP-07005 Section 4.3.2.
- Communications between different trains are one way data link communication between RPS trains, from RPS to ESFAS and safety VDU trains. Functional separation is achieved by communication controllers that are separate from functional processors and voting logic that processes the data from the different trains. Each data link uses optical fiber to achieve electrical independence of each train. Physical separation between safety trains is achieved by locating in different areas. These interfaces are the data link digital data communication technology described in the MELTAC Platform Technical Report, MUAP-07005 Section 4.3.3.
- Bi-directional communications between controllers in one(1) safety train are performed by the Safety Bus. The Safety Bus provides deterministic cyclical data communication. Functional independence is provided by separate communication processors within each controller. Fiber optic cable is provided to enhance EMI susceptibility. The Safety Bus uses the Control Network digital communication technology described in the MELTAC Platform Technical Report, MUAP-07005 Section 4.3.2.
- Bidirectional communication between controllers and their respective I/O modules is provided by the I/O Bus described in the MELTAC Platform Technical Report, MUAP-07005 Section 4.1.
- Bidirectional communication between the PSMS controllers and the MELTAC engineering tool is provided by the Maintenance Network described in the MELTAC Platform Technical Report, MUAP-07005 Section 4.3.4. The PSMS controllers are normally disconnected from the Maintenance Network. Temporary connections are made for equipment trouble shooting and periodic surveillance. Temporary connections are managed by administrative controls and plant technical specifications.
- The station bus provides information to plant and corporate personnel and to the EOF and ERDS. The station bus receives information from the PCMS and PSMS via the unit management computer. The isolation device, which is located between the unit management computer and the station bus, provides a hardware-based unidirectional interface which allows only outbound communication. There are no other connections from external sources to the PCMS and PSMS. In addition, the only interface from the PCMS and PSMS to external networks is via the hardware-based unidirectional interface provided by the isolation device. The hardware-based unidirectional interface 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. The interface with station bus and external networks is shown in Figure 4.2-7.

MIC-04-07-00001



MIC-04-07-00001

Figure 4.2-7 Interfaces with Station Bus and External Networks

- 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.

Change to "US-APWR design".

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).

MIC-04-07-00001

MIC-04-07-00001

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 Subsignal details.

Add "Attachments 6A.12 and 6A.13".

Add "for the PSMS model".

7.1.3.17 Life Cycle Process

MHI applies its MELCO's safety system digital platform, 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 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) controls the basic software life cycle process of the MELTAC Platform.

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).

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

if its measurement exceeds its predefined setpoint. Each RPS train sends its own partial trip signal to each of the other three RPS trains over isolated serial data links. Each train will generate a reactor trip signal if any two or more trains of the same variable are in the partial trip state.

The reactor trip signal from each of the four RPS trains is separately sent to a corresponding reactor trip breakers. Each RPS train has two reactor trip breakers. The reactor is tripped when reactor trip signals are generated by any two or more RPS trains.

Delete.

MIC-04-07-00001

For the RPS ~~and the PRA safety goals~~, the Single Failure Criterion (IEEE Std 603-1991, Clause 5.1) and the Control-Protection Interaction Criteria (GDC 24 and IEEE Std 603-1991, Clause 5.6.3.3) are met with only three trains in service. Therefore, these requirements are met even when the one RPS train and its corresponding reactor trip breakers are out of service (in a bypass condition, etc). The only exception is the neutron flux measurement channel from the sensor to the RPS input function, and the four trains of these measurement channel in service are required to meet the Single Failure Criterion (IEEE Std 603-1991, Clause 5.1) and the Control-Protection Interaction Criteria (GDC 24 and IEEE Std 603-1991, Clause 5.6.3.3).

The bypass condition (allowable bypass time, etc.) of each reactor trip function in the RPS and the reactor trip breakers is controlled by the US-APWR technical specifications, DCD Chapter 16.

7.1.4.1.2 Independence

The four trains of the RPS maintain physical independence, electrical independence, communication independence and functional independence.

7.1.4.1.2.1 Physical Independence

The four trains of the RPS are physically independent from each other and from the non-safety systems. The physical independence design conforms to RG 1.75 (Reference 7.1-22), which endorses IEEE Std 384-1992 (Reference 7.1-23), which is referred from IEEE Std 603-1991 (Reference 7.1-15, Clause 5.6).

Cabinets for each train of the RPS are located in a separate plant equipment room fire area (one per train). These fire areas are separate from the fire areas where non-safety systems are located, and separate from the fire areas of the main control room (MCR) and the remote shutdown room (RSR). In addition to these plant equipment room fire areas, physical separation is also maintained between trains for instrumentation inputs and plant component control outputs interfaced with RPS cabinets.

All RPS controllers and I/O modules are located within the RPS cabinets. The RPS cabinet doors are normally locked by keys. The equipment rooms are also accessible only with the appropriate security access (e.g., key or security card). Since the RPS is distributed to four separately accessible secured areas (one per train), these access controls meet the Single Failure Criterion (IEEE Std 603-1991, Clause 5.9).

The physical independence for the conventional manual reactor trip actuation switches is an exception to the design of separate fire areas for each train of the RPS. All four trains of these reactor trip switches are installed in the MCR. The switches for each train have

controller also has two redundant subsystems. The outputs of the redundant subsystems are combined in the power interface (PIF) modules in the SLS, along with control signals from the DAS, to interface with ESF system plant components. Conventional hardwired logics within the PIF module gives priority to any output signal from subsystem 1, subsystem 2 or DAS which demands the safe state of the component (i.e., the state required to execute the ESF system function). The multidivisional safety VDUs receive monitoring signals from all four train safety VDUs and each train multidivisional safety VDU can provide the information of four train critical safety functions for the safe shutdown. Therefore, each multidivisional safety VDU has 100% monitoring capabilities to provi[illegible]ation to achieve the safety functions for the safe shutdown, and there are only two multidivisional safety VDU trains within the PSMS for the US-APWR.

Delete.

For the ESF system ~~and the PRA safety goals~~, the Single Failure Criterion (IEEE Std 603-1991, Clause 5.1) are met with only three trains in service, including the train A and D to accommodate two mechanical train systems, for the four train system (the ESFAS, SLS, safety VDU, system level ESF actuation switch and COM) and two trains in service for the two train system (the multidivisional safety VDU). The only exception is the Containment Phase B isolation function, which requires four trains due to the distribution of the two train related components to all four trains, and the four trains of these functions in service are required to meet the Single Failure Criterion (IEEE Std 603-1991, Clause 5.1). Therefore, the US-APWR technical specifications, DCD Chapter 16, require only three operable trains, including train A and train D, except the Containment Phase B functions. The bypass condition (allowable bypass time, etc.) for test and maintenance of the functions performed by each ESAFS, SLS, safety VDU, system level ESF actuation switch, multidivisional safety VDU and COM is controlled by the US-APWR technical specifications, DCD Chapter 16.

MIC-04-07-00001

7.1.4.2.2 Independence

The four trains of the ESFAS, SLS, COM, safety-related HSIS maintain physical independence, electrical independence, communication independence and functional independence.

7.1.4.2.2.1 Physical Independence

Each train of the ESFAS, SLS, COM and safety-related HSIS are independent from each other and from non-safety systems. The physical independence design and secure access design are the same as for the RPS, and therefore conforms to RG 1.75 (Reference 7.1-22), which endorses IEEE Std 384-1992 (Reference 7.1-23) which is referred from IEEE Std 603-1991 (Clause 5.6 and 5.9).

Cabinets for each train of the ESFAS, SLS, COM and safety VDU Processor are located in a separate plant equipment room fire area (one per train). These fire areas are separate from the fire areas where non-safety systems are located, and separate from the fire areas of the MCR and the RSR. In addition to these plant equipment rooms fire areas, physical separation are also maintained between trains for instrumentation inputs and plant component control outputs interfaced with ESFAS and SLS.

Only exception is the system level ESF actuation switches and the safety VDU Panel. All four trains of the safety-related HSIS, including safety VDU are installed in the MCR and

- The EFW isolation function actuated by low main steam line pressure can be manually bypassed if the P-11 interlock is present. This operating bypass is automatically removed when the P-11 interlock clears.

- The manual bypass for high pressurizer water level initiation signal for CVCS isolation can only be actuated when the P-11 interlock is present. This operating bypass is automatically removed when the P-11 interlock clears.

All operating bypasses, either manually or automatically initiated, are automatically removed when the plant moves to an operating condition for which the protective action would be required if an accident occurred. Status indication is provided in the MCR for all operating bypasses.

7.3.1.6.4 Manual Overrides

Manual overrides must be manually initiated. These manual overrides can be manually initiated separately within each PSMS train when the plant process permissive condition is sensed by the PSMS input channel(s). The following is a list of train level manually initiated overrides:

- The ECCS actuation can be manually overridden at the train level when the P-4 interlock is present (RTB open). This manual override is automatically removed when the P-4 interlock clears (RTB closed). In MUAP-07004 Appendix D (e), this override is referred to as a reset.

- The block cooldown turbine bypass valve actuation by low-low T_{avg} may be manually overridden at the train level. This manual override cannot be initiated until after automatic system level actuation. The manual override may be manually reset by the operator at any time, and is automatically reset when the low-low T_{avg} initiation signal returns to normal. This signal blocks the cooldown turbine bypass valves. In MUAP-07004 Appendix D (b), this override is referred to as an operating bypass.

7.3.1.7 Interlocks

The interlocks for initiating and automatically removing operating bypasses are discussed above. The interlocks for manual overrides are discussed above. The interlocks for resetting system level actuation and channel level actuation are discussed in Subsection 7.3.1.6 for each specific safety function. The interlocks for maintenance bypasses are discussed in Subsection 7.1.3.11.

7.3.1.8 Redundancy

There are four redundant ESF trains for all ESF systems, except as specifically identified in Subsection 7.3.1.5. In addition, within each train, ESFAS and SLS controllers are redundant. Therefore, a single controller failure or a single controller taken out of service for maintenance of a redundant pair, has no adverse effect on the safety function and will not result in a limiting condition of operation (LCO) of the Technical Specification. The

reliability of the ESFAS/SLS, as ~~analyzed~~ in the PRA, is based on having two controllers in service. MIC-04-07-00001

7.3.1.9 Diversity

Change to "described".

All ESF[illegible] initiated from signals that originate in the RPS. Manual actuation of ESF system[illegible] that bypasses the RPS.

Add "Technical Report Attachment 6A.13 (Reference 7.3-14)".

The SLS receives signals from the DAS to actuate ESF plant components. These signals are interfaced from DAS via qualified isolation devices within the SLS. The SLS provides priority logic to combine the DAS and SLS signals and to ensure the safe state always has priority. The DAS/SLS interface is described in The D3 Topical Report (Reference 7.3-3) Sections 6.2.1.3 and 6.2.4, and shown in Figure 7.3-1.

7.3.1.10 Defense-In-Depth/Design Features

The ESFAS and SLS implement the ESF system echelon of defense-in-depth scheme, as described in Subsection 7.1.3.1.

7.3.1.11 Turbine Trip to Prevent Unnecessary Emergency Core Cooling System Actuation

The turbine is tripped on a reactor trip or high-high SG water level in any SG. Turbine trip on RT is an un-credited non-safety function in the safety analysis. However, turbine trip on RT is assumed in the safety analysis in order to prevent unnecessary ECCS actuation and to shift to the safe shutdown state by appropriate actions after AOO and PA conditions. Turbine trip on RT cannot be completely designed as Class 1E because the equipment to execute the turbine trip is located in the turbine building, which is seismic category II. Therefore, turbine trip on RT is designed as reliably as possible by applying the following design concepts:

(1) Turbine trip on reactor trip is controlled by the PSMS and electrical circuits outside the controllers are appropriately separated from Class 1E circuits per IEEE Std 384-1992 (Reference 7.3-4) and RG 1.75 (Reference 7.3-5).

(2) The cables in the turbine building are routed in dedicated raceways.

(3) Four turbine trip solenoid valves are arranged in a 1-out-of-2 configuration. A trip will be generated by train A or train D. The power for each turbine trip solenoid valve is supplied by a separate Class 1E power source (one per train).

The turbine trip signals are interfaced from the SLS, which receives RT signals from the RTBs. The design is shown in Figure 7.3-4.

7.3.1.12 Block Turbine Bypass and Cooldown Valves

There are two ESFAS trains for block turbine bypass and cooldown valves, train A and train D.

7.3-5 Physical Independence of Electric Systems, Regulatory Guide 1.75 Revision 3, February 2005.

7.3-6 Setpoints for Safety-Related Instrumentation, Regulatory Guide 1.105 Revision 3, December 1999.

7.3-7 IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, IEEE Std 603-1991.

7.3-8 IEEE Standard Design for Digital Computers in Safety Systems of Nuclear Power Generating Stations, IEEE Std 7-4.3.2-2003.

7.3-9 Standard Criteria for Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems, IEEE Std 338-1987.

7.3-10 Periodic Testing of Protection System Actuation Functions, Regulatory Guide 1.22 Revision 0, February 1972.

7.3-11 Function Assignment Analysis for Safety Logic System, MUAP-09020-P Rev.2 (Proprietary) and MUAP-09020-NP Rev.2 (Non-Proprietary), May 2011.

7.3-12 US-APWR Instrument Setpoint Methodology, MUAP-09022-P Rev.3 (Proprietary) and MUAP-09022-NP Rev.3 (Non-Proprietary), July 2013.

MIC-04-07-00001

Add;

7.3-14 US-APWR Probabilistic Risk Assessment, MUAP-07030 Rev.3 (Proprietary), June 2011.

The safety VDUs and the multidivisional safety VDUs for each train are isolated from each other and from non-safety systems.

IEEE Std 497-2002 (Reference 7.5-2) provides principles for the selection and categorization of PAM variables. Table 7.5-1 provides a summary of these selection criteria and source documents for each PAM variable type.

Table 7.5-2 provides the US-APWR design attributes applied to each variable type.

Table 7.5-3 provides a list of US-APWR PAM variables, their ranges, monitored functions or systems, quality and variable type. Tables 7.5-6 through 7.5-10 summarize the specific PAM variables by variable type and their associated required functions. Additional information regarding the bases for the selection of the PAM variables included in Table 7.5-3 is provided in Appendix H of the Safety I&C Technical Report (Reference 7.5-5).

The COL Applicant is to provide a description of site-specific PAM variables, which are Type D variables for monitoring the performance of the UHS and Type E variables for monitoring the meteorological parameters.

Instrumentation for monitoring severe accidents is discussed in Subsection 19.2.3.3.7. which summarizes the necessary equipment survivability for achieving and maintaining shutdown of the plant and maintaining containment integrity for severe accidents. ~~A detailed description of the analysis on equipment survivability, including instruments required for severe accident monitoring, is provided in Chapter 15 of the PRA Technical Report(Reference 7.5-15).~~

Delete.

MIC-04-07-00001

The Type A, B, and C variables/instrument functions are those determined by the application of the NRC-endorsed PAM instrumentation determination process, which is based on supporting the site-specific AOPs and EOPs, as stipulated in RG 1.97 Rev. 4 (Reference 7.5-1. The PAM variables in Table 7.5-3 are verified upon completion of the EOPs and AOPs.

7.5.1.1.1 Variable Classifications and Signal Processing Design

The following clarifications are provided for the design attributes identified in Tables 7.5-1 and 7.5-2:

1. Single Failure: The design ensures that at least one measurement channel is available after each single failures. Process measurement channels are interfaced to redundant trains of the RPS. Component status signals are interfaced to redundant trains of the SLS. PAM information is then interfaced to redundant safety-related HSI and non-safety HSI for display.

2. Seismic Qualification: RPS, SLS, and safety-related HSI are seismically qualified, as previously described. PAM measurement channels are generically qualified by the instrument OEM. Specific analysis for the US-APWR demonstrates this qualification bounds the seismic levels for the specific instrument location.

3. Environmental Qualification: RPS, SLS, and safety-related HSI are environmentally qualified, as previously described. These systems are located in

7.8.1.2.1 Reactor Trip, Turbine Trip and Main Feedwater Isolation

Reactor trip, turbine trip and MFW isolation are automatically actuated on the following signals:

- Low pressurizer pressure: 2-out-of-4 voting logic of the four pressurizer pressure low signals.
- High pressurizer pressure: 2-out-of-4 voting logic of the four pressurizer pressure high signals.
- Low SG water level: 2-out-of-4 voting logic of the one SG water level low signals from each SG.

The four pressurizer pressure signals are interfaced from each of the four PSMS trains. This configuration allows the DAS to meet the target reliability of the PRA with one channel continuously bypassed or inoperable.

MIC-04-07-00001

To support the single failure criterion for all PSMS functions, there are four SG water level signals (one per each train A, B, C, and D) on each SG. However, for the DAS, which does not need to meet the single failure criterion, from each SG.

Add "Refer to PRA Technical Report Attachments 6A.12 and 6A.13 (Reference 7.8-10) for the DAS model".

The reactor trip is actuated by tripping the non-safety CRDM motor-generator set. This actuation leads to de-energizing the power for the CRDM by a means that is diverse from the RTB to release the control rods for gravity insertion into the reactor core. Diversity from the PSMS is maintained from sensor-inputs to final actuators.

The Turbine Trip is actuated by opening the solenoid valves for turbine trip. Diversity from the RT function in the PSMS is maintained from sensor-input up to the power interface module.

The MFW isolation is actuated by closing the MFW regulation valve. Diversity from the feedwater isolation function in the PSMS is maintained from sensor input up to the power interface module.

These DAS actuation functions are automatically blocked when all the following conditions are established (indicating correct actuation of the PSMS):

- Status signals are received indicating that the minimum combination of the RTBs have actuated for the RT function. This is referred to as the P-4 interlock. The logic for the P-4 interlock is the same as in the PSMS, as shown in Figure 7.8-2. The P-4 interlock is processed independently in each DAAC. Signals from all RTBs are interfaced from the PSMS, prior to any software processing, to each DAAC, as shown in Figure 7.8-1.
- The turbine emergency trip oil pressure trip signal is generated when oil pressure channels exceed the trip setpoint.

Technical Report MUAP-07014 also confirms that there is sufficient time for all credited manual operator actions. The HSI on the DHP is designed, verified, and validated in accordance with the HFE program described in Chapter 18.

7.8.3.3 Conformance to BTP 7-19

Topical Report MUAP-07006 Appendix A provides a detailed description for the conformance of BTP 7-19 (Reference 7.8-7).

7.8.4 Combined License Information

No additional information is required to be provided by a COL Applicant in connection with this section.

7.8.5 References

7.8-1 Defense-in-Depth and Diversity, MUAP-07006-P-A Rev.2 (Proprietary) and MUAP-07006-NP-A Rev.2 (Non-Proprietary), September 2009.

7.8-2 Defense-in-Depth and Diversity Coping Analysis, MUAP-07014-P Rev.5 (Proprietary) and MUAP-07014-NP Rev.5 (Non-Proprietary), September 2011.

7.8-3 Safety I&C System Description and Design Process, MUAP-07004-P Rev.7 (Proprietary) and MUAP-07004-NP Rev.7 (Non-Proprietary), May 2011.

7.8-4 Safety System Digital Platform -MELTAC-, MUAP-07005-P Rev.8 (Proprietary) and MUAP-07005-NP Rev.8 (Non-Proprietary), July 2011.

7.8-5 Quality Assurance Guidance for ATWS Equipment That Is Not Safety-Related, Generic Letter 85-06.

7.8-6 Requirements for Reduction of Risk from Anticipated Transients Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants, NRC Regulations Title 10, Code of Federal regulations, 10 CFR Part 50.62.

7.8-7 Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems, BTP 7-19 Revision 5, March 2007.

7.8-8 HSI System Description and HFE Process, MUAP-07007-P Rev.5 (Proprietary) and MUAP-07007-NP Rev.5 (Non-Proprietary), November 2011.

7.8-9 US-APWR Instrument Setpoint Methodology, MUAP-09022-P Rev.3 (Proprietary) and MUAP-09022-NP Rev.3 (Non-Proprietary), July 2013.

MIC-04-07-00001

Add;

7.8-10 US-APWR Probabilistic Risk Assessment, MUAP-07030 Rev.3 (Proprietary), June 2011.

ACTIONS (continued)

If the Manual Reactor Trip Function cannot be restored to OPERABLE status within the allowed 72 hour Completion Time, the unit must be brought to a MODE in which the requirement does not apply. To achieve this status, the unit must be brought to at least MODE 3 within 6 additional hours (78 hours total time). The 6 additional hours to reach MODE 3 is reasonable, based on operating experience, to reach MODE 3 from full power operation in an orderly manner and without challenging unit systems.

With the unit in MODE 3, ACTION C would apply to any inoperable Manual Reactor Trip Function if the Rod Control System is capable of rod withdrawal or one or more rods are not fully inserted.

The Completion Time of 72 hours is justified because two trains are adequate to perform the safety function , and there are three automatic actuation trains and two other Manual Reactor Trip trains OPERABLE. In addition, the Completion Time considers that the Manual Reactor Trip Function, for the inoperable Manual Reactor Trip Function, can be actuated from the Safety VDU[Replace with "supported by".] fore, the ability to initiate a manual [Replace with "insights".]tor Trip through ment remains functional in all three .

The Completion Time of 72 hours is also ~~justified in~~ the US-APWR reliability and risk ~~analyses, the summary and result of~~ which are documented in FSAR Chapter 19 (Ref. 10). [Delete.]

MIC-04-16-00001

C.1, C.2.1, and C.2.2

Condition C appl[Add "Appendix B".]tor Trip Function in MODE 3, 4, or 5 with the Rod Control System capable of rod withdrawal or one or more rods not fully inserted.

ACTIONS (continued)

This action addresses the train orientation for this Function. With one required train inoperable, the inoperable train must be restored to OPERABLE status within 72 hours. If the affected Function cannot be restored to OPERABLE status within the allowed 72 hour Completion Time, the unit must be placed in a MODE in which the requirement does not apply. To achieve this status, action must be initiated within the same 72 hours to ensure that all rods are fully inserted, and the Rod Control System must be placed in a condition incapable of rod withdrawal within the next hour. The additional hour provides sufficient time to accomplish the action in an orderly manner. With rods fully inserted and the Rod Control System incapable of rod withdrawal, this Function is no longer required.

The Completion Time of 72 hours is justified because two trains are adequate to perform the safety function, and there are three automatic actuation trains and two other Manual Reactor Trip Functions OPERABLE. In addition, the Completion Time considers that the Manual Reactor Trip Function, for the inoperable Manual Reactor Trip train, can be actuated from the Safety VDU for the ability to initiate a manual Reactor Trip through ment remains functional in all three

Replace with "supported by".

Replace with "insights".

The Completion Time of 72 hours is also ~~justified in~~ the US-APWR reliability and risk ~~analyses~~, ~~the summary and result of~~ which are documented in FSAR Chapter 19(Ref. 10).

MIC-04-16-00001

Delete.

D.1, D.2.1, and D.2.2

Condition D app Add "Appendix B". actor Trip Functions in MODE 3, 4, or 5 with the Rod Control System capable of rod withdrawal or one or more rods not fully inserted:

- RTBs,
- RTB Undervoltage and Shunt Trip Mechanisms, and
- Automatic Trip Logic.

BASES

ACTIONS (continued)

This action addresses the train orientation for these Functions. With one required train inoperable, the inoperable train must be restored to OPERABLE status within 48 hours. If the affected Function(s) cannot be restored to OPERABLE status within the allowed 48 hour Completion Time, the unit must be placed in a MODE in which the requirement does not apply. To achieve this status, action must be initiated within the same 48 hours to ensure that all rods are fully inserted, and the Rod Control System must be placed in a condition incapable of rod withdrawal within the next hour. The additional hour provides sufficient time to accomplish the action in an orderly manner. With rods fully inserted and the Rod Control System incapable of rod withdrawal, these Functions are no longer required.

The Completion Time of 48 hours is justified because the two remaining OPERABLE trains Replace with "supported by". rm the safety function. In addition, the Completion Tir wo remaining OPERABLE trains Replace with "insights". ave continuous automatic self-testing for the Automatic Trip Logic.

The Completion Time of 48 hours is also ~~justified in~~ the US-APWR reliability and risk ~~analyses~~, ~~the summary and result of~~ which are documented in FSAR Chapter 19 (Ref. 10). MIC-04-16-00001

Delete.

E.1.1, E.1.2, E.2.1, E.2.2, and E.3

Condition E appl Add "Appendix B". e Neutron Flux (High Setpoint) Function.

With one channel inoperable, the inoperable channel must be placed in the trip condition within 72 hours. This results in a partial trip condition requiring only one-out-of-three logic for actuation of the two-out-of-four trips.

The Completion Time of 72 hours to place the inoperable channel in the trip condition is justified because the three remaining OPERABLE channels are adequate to perform the safety function. In addition, the Completion Time considers that the three remaining OPERABLE channels have continuous automatic self-testing and continuous automatic CHANNEL CHECKS. In addition, with the remaining three OPERABLE channels, the SSA within the PCMS ensures the control

ACTIONS (continued)

systems can withsta[Replace with "supported by".]he control system without causing erroneous control s[y]n would otherwise require the [Replace with "insights".]on function actuation.

The Completion Time of 72 hours is also ~~justified in~~ the US-APWR reliability and risk ~~analyses~~, ~~the summary and result of~~ which are documented in FSAR Chapter 19 (Ref. 10). MIC-04-16-00001

[Delete.]

In addition to placing the inoperable channel in the trip condition, THERMAL POWER must be reduced to ≤ 75% RTP within 78 hours. Reducing the power level prev[Add "Appendix B".]re with radial power distributions beyond the design limits. With one of the NIS power range detectors inoperable, 1/4 of the radial power distribution monitoring capability is lost.

As an alternative to the above Required Actions, the inoperable channel can be placed in the trip condition within 72 hours and the QPTR monitored once every 12 hours as per SR 3.2.4.2, QPTR verification. Calculating QPTR every 12 hours compensates for the lost monitoring capability due to the inoperable NIS power range channel and allows continued unit operation at power levels < 75% RTP. The 12 hour Surveillance Frequency is consistent with LCO 3.2.4, "QUADRANT POWER TILT RATIO (QPTR)."

As an alternative to the above Required Actions, the plant must be placed in a MODE where this Function is no longer required OPERABLE. Seventy-eight hours are allowed to place the plant in MODE 3. The 78 hour Completion Time includes 72 hours for channel corrective maintenance and an additional 6 hours for the MODE reduction as required by Required Action E.3. This is a reasonable time, based on operating experience, to reach MODE 3 from full power in an orderly manner and without challenging plant systems. If Required Actions cannot be completed within their allowed Completion Times, LCO 3.0.3 must be entered.

The Required Actions are modified by a Note that allows placing one channel in bypass for up to 12 hours while performing surveillance testing, or setpoint adjustments when a setpoint reduction is required by other Technical Specifications, provided the other channels are OPERABLE, or two channels are OPERABLE and one is placed in the trip condition. With one channel bypassed, the system can detect all anomalies, but it cannot also sustain a single failure.

BASES

ACTIONS (continued)

The Bypass Time of 12 hours is justified because the remaining OPERABLE channels are a[Replace with "supported by".]e safety function. In addition, the Bypass Time consider[Replace with "insights".]PERABLE channels have continuous tomatic self-testing and continuous automatic CHANNEL CHECKS.

The Bypass Time of 12 hours is also ~~justified in~~ the US-APWR reliability and risk ~~analyses~~, ~~the summary and result of~~ which are documented in FSAR Chapter 19 (Ref. 10). [Delete.]

MIC-04-16-00001

Required Action E.2.2 has been modified by a Note which only requires SR 3.2.4.2 to be performed if the Power Range Neutron Flux input to QPTR becomes inoper[Add "Appendix B".]onent in the Power Range Neutron Flux Channel which renders the High Flux Trip Function inoperable may not affect the capability to monitor QPTR. As such, determining QPTR using the movable incore detectors once per 12 hours may not be necessary.

F.1 and F.2

Condition F applies to the following Reactor Trip Functions:

- High Power Range Neutron Flux (Low Setpoint),
- High Power Range Neutron Flux Rate (Positive Rate), and
- High Power Range Neutron Flux Rate (Negative Rate).

BASES

ACTIONS (continued)

With one channel inoperable, the inoperable channel must be placed in the trip condition within 72 hours. Placing the channel in the trip condition results in a partial trip condition requiring only one-out-of-three logic for actuation of the two-out-of-four trips.

The Completion Time of 72 hours to place the inoperable channel in the trip condition is justified because the three remaining OPERABLE channels are adequate to perform the safety function. In addition, the Completion Time considers that the three remaining OPERABLE channels have continuous automatic self-testing and continuous automatic CHANNEL CHECKS.

In addition, with the remaining three OPERABLE channels, the SSA within the PCMS ensure[Replace with "supported by".] can withstand an input failure to the [Replace with "insights".]ol system wi[Replace with "supported by".]us control system operation, which [Replace with "insights".]otherwise require the protection function actuation.

The Completion Time of 72 hours is also ~~justified in~~ the US-APWR reliability and risk ~~analyses~~, ~~the summary and result of~~ which are documented in FSAR Chapter 19 (Ref. 10). MIC-04-16-00001

[Delete.]

If the inoperable channel cannot be placed in the trip condition within the specified Completion Time, the unit must be placed in a MODE where these Functions are no[Add "Appendix B".] An additional 6 hours are allowed to place the unit in MODE 3. Six hours is a reasonable time, based on operating experience, to place the unit in MODE 3 from full power in an orderly manner and without challenging unit systems.

The Required Actions are modified by a Note that allows placing one channel in bypass for up to 12 hours while performing surveillance testing, provided the other channels are OPERABLE, or two channels are OPERABLE and one is placed in the trip condition. With one channel bypassed, the system can detect all anomalies, but it cannot also sustain a single failure.

The Bypass Time of 12 hours is justified because the remaining OPERABLE channels are a[Replace with "supported by".]e safety function. In addition, the Bypass [Replace with "insights".]me consider[Replace with "supported by".]PERABLE channels have continuous tomatic self-testing and continuous automatic CHANNEL CHECKS.

The Bypass Time of 12 hours is also ~~justified in~~ the US-APWR reliability and risk ~~analyses~~, ~~the summary and result of~~ which are documented in FSAR Chapter 19 (Ref. 10). MIC-04-16-00001

[Delete.]

[Add "Appendix B".]

ACTIONS (continued)

The Completion Time of 72 hours to place the inoperable channel in the trip condition is justified because the two remaining OPERABLE channels are adequate to perform the safety function. The Completion Time also considers that the two remaining OPERABLE channels have continuous automatic self-testing.

In addition, the two remaining OPERABLE channels have continuous automatic CHANNEL CHECKS, except for Turbine Trip – Turbine Emergency Trip Oil Pressure. This additional justification is not needed for Turbine Eme ure, because this is an ction that is fety analysis.

Replace with "insights".

Replace with "supported by".

For all functions (except Turbine Trip – Turbine Emergency Trip Oil Pressure), the Completion Time of 72 hours is also ~~justified in~~ the US-APWR reliability and risk ~~analyses, the summary and result of~~ which are documented in FSAR Chapter 19 (Ref. 10).

Delete.

MIC-04-16-00001

The Required Actions are modified by a Note that allows placing one required channel in bypass for up to 12 hours while performing surveillance testing, provided the other required ch , or one required channel is OPERABLE and the other required channel is placed in the trip condition. With one required channel bypassed, the system can detect all anomalies, but it cannot also sustain a single failure.

Add "Appendix B".

BASES

ACTIONS (continued)

The Bypass Time of 12 hours is justified because the remaining OPERABLE channels are adequate to perform the safety function. The Bypass Time also considers that the remaining OPERABLE channels have continuous automatic self-testing.

In addition the remaining OPERABLE channels have continuous automatic CHANNEL CHECKS, except for Turbine Trip – Turbine Emergency Trip Oil Pressure. This additional justification is not needed for Turbine Trip – Turbine Emergency Trip Oil Pressure because this is an anticipatory function that is credited in the analyses.

Replace with "insights".

Replace with "supported by".

The Bypass Time of 12 hours is also ~~justified in~~ the US-APWR reliability and risk ~~analyses, the summary and result of~~ which are documented in FSAR Chapter 19 (Ref. 10).

MIC-04-16-00001

Delete.

M.1 and M.2

Add "Appendix B".

Condition M applies to the ECCS Actuation input in MODES 1 and 2. These actions address the train orientation of the RTS for these Functions. With one required train inoperable, 24 hours are allowed to restore the train to OPERABLE status or the unit must be placed in MODE 3 within the next 6 hours.

The Completion Time of 24 hours is justified because the two remaining OPERABLE trains are adequate to perform the safety function. In addition, the Completion Time of 24 hours for two remaining OPERABLE trains have continuous automatic self-testing.

Replace with "insights".

Replace with "supported by".

The Completion Time of 24 hours is also ~~justified in~~ the US-APWR reliability and risk ~~analyses, the summary and result of~~ which are documented in FSAR Chapter 19 (Ref. 10).

MIC-04-16-00001

Delete.

The Completion Time of 6 hours is reasonable, based on operating experience, to reduce power in an orderly manner and without challenging unit systems.

Add "Appendix B".

The Required Actions have been modified by a Note that allows placing one required train in bypass for up to 4 hours while performing surveillance testing, provided the other required trains are OPERABLE.

BASES

ACTIONS (continued)

The Bypass Time of 4 hours is justified because the remaining OPERABLE trains are adequate to perform the safety function. In addition, the Bypass considers PERABLE trains have continuous hatic self-

Replace with "insights".

Replace with "supported by".

The Bypass Time of 4 hours is also ~~justified in~~ the US-APWR reliability and risk ~~analyses~~, ~~the summary and result of~~ which are documented in FSAR Chapter 19 (Ref. 10).

MIC-04-16-00001

Delete.

N.1 [and N.2]

Add "Appendix B".

Condition N applies to the RTBs in MODES 1 and 2. These actions address the train orientation of the RTS for the RTBs. With one required train inoperable, 24 hours are allowed for train corrective maintenance to restore the train to OPERABLE status.

The Completion Time of 24 hours is justified because the two remaining OPERABLE trains are adequate to perform the safety function. In addition, letion Time remaining OPERABLE trains e continuou g.

Replace with "insights".

Replace with "supported by".

The Completion Time of 24 hours is also ~~justified in~~ the US-APWR reliability and risk ~~analyses~~, ~~the summary and result of~~ which are documented in FSAR Chapter 19 (Ref. 10).

MIC-04-16-00001

Delete.

[Required Action N.2 allows the option to apply the requirements of Specification 5. Add "Appendix B". k Informed Completion Time.]

O.1 and O.2

Condition O applies to the P-6 and P-10 interlocks. With one or more channels inoperable, the associated interlock must be verified to be in its required state for the existing unit condition within 1 hour or the unit must be placed in MODE 3 within the next 6 hours. Verifying the interlock status manually accomplishes the interlock's Function.

The Completion Time of 1 hour is based on operating experience and the minimum amount of time allowed for manual operator actions.

ACTIONS

Replace with "insights".

Replace with "supported by".

The Completion Time of 48 hours is also ~~justified in~~ the US-APWR reliability and risk ~~analyses~~, ~~the summary and result of~~ which are documented in FSAR Chapter 19 (Ref. 10).

MIC-04-16-00001

Delete.

[Required Action Q.2 allows the option to apply the requirements of Specification 5.~~5~~ Add "Appendix B". k Informed Completion Time.]

R.1 [and R.2]

Condition R applies to the RTS Automatic Trip Logic in MODES 1 and 2. These actions address the train orientation of the RTS for these Functions. With one required train inoperable, 24 hours are allowed to restore the train to OPERABLE status.

The Completion Time of 24 hours is justified because the two remaining OPERABLE required trains are adequate to perform the safety function. In addition, the Comp that the two remaining OPERABLE trains eac omatic self-testing.

Replace with "insights".

Replace with "supported by".

The Completion Time of 24 hours is also ~~justified in~~ the US-APWR reliability and risk ~~analyses~~, ~~the summary and result of~~ which are documented in FSAR Chapter 19 (Ref. 10).

MIC-04-16-00001

Delete.

[Required Action R.2 allows the option to apply the requirements of Specification 5.~~5~~ Add "Appendix B". k Informed Completion Time.]

The Required Actions have been modified by a Note that allows placing one required train in bypass for up to 4 hours while performing surveillance testing, provided the other required trains are OPERABLE.

The Bypass Time of 4 hours is justified because the remaining OPERABLE trains are adequate to perform the safety function. In addition, the Bypass considers ERABLE trains have continuous atic self-t

Replace with "insights".

Replace with "supported by".

The Bypass Time of 4 hours is also ~~justified in~~ the US-APWR reliability and risk ~~analyses~~, ~~the summary and result of~~ which are documented in FSAR Chapter 19 (Ref. 10).

MIC-04-16-00001

Delete.

Add "Appendix B".

ACTIONS (continued)

U.1 and U.2

Condition U applies to the following Reactor Trip Functions:

- Overtemperature ΔT,
- Overpower ΔT,
- High Pressurizer Pressure, and
- Low SG Water Level.

With one required channel inoperable, the inoperable channel must be placed in the trip condition within 1 hour and restored to OPERABLE status in 72 hours.

This Condition applies to functions that operate on two-out-of-three logic and have channels that are shared with the control systems. Normally the SSA can prevent erroneous control system operations. However, when there are less than three OPERABLE required channels, the SSA cannot prevent erroneous control system operation due to an input failure. With two OPERABLE required channels and one required channel in the trip condition, if a channel failure occurs in an OPERABLE required channel and results in erroneous control system operation, the remaining OPERABLE required channel can provide a plant trip. However, the channel that causes the erroneous control system operation cannot be credited as the single failure; therefore, this configuration does not satisfy the single failure criteria. To satisfy the single failure criteria, three required channels must be restored to OPERABLE status within 72 hours.

The Completion Time of 1 hour to place the failed channel in the trip condition is based on operating experience and the minimum amount of time allowed for manual operator actions.

The Completion Time of 72 hours to restore the inoperable channel is justified because the two remaining OPERABLE channels are adequate to perform the safety function. In addition, the two remaining OPERABLE s have con testing and continuous automatic checks.

Replace with "insights".

Replace with "supported by".

The Completion Time of 72 hours is also ~~justified in~~ the US-APWR reliability and risk ~~analyses~~, ~~the summary and result of~~ which are documented in FSAR Chapter 19 (Ref.10).

MIC-04-16-00001

Delete.

Add "Appendix B".

ACTIONS (continued)

These Functions do not have to be OPERABLE below the P-7 setpoint because there is insufficient heat production to generate DNB conditions below the P-7 setpoint.

The Completion Time of 1 hour to place the failed channel in the trip condition is based on operating experience and the minimum amount of time allowed for manual operator actions.

The Completion Time of 72 hours to restore the inoperable channel is justified because the two remaining OPERABLE channels are adequate to perform the safety function. In addition, the two remaining OPERABLE have con -testing and continuous automatic . CHECK

Replace with "insights".

Replace with "supported by".

The Completion Time of 72 hours is also ~~justified in~~ the US-APWR reliability and risk ~~analyses~~, ~~the summary and result of~~ which are documented in FSAR Chapter 19 (Ref.10).

MIC-04-16-00001

Delete.

Add "Appendix B".

Bypass of a required channel is not allowed because there are only three required chann are also used for control. If a failure were to occur in one of the two remaining required control channels, a plant transient could occur that would require a plant trip, but a plant trip would not occur with only one remaining OPERABLE required channel.

X.1

If the Required Action and associated Completion Time of Condition W is not met, the unit must be placed in which THERMAL POWER is below P-7. Six hours are allowed to reduce THERMAL POWER to below P-7 if the inoperable channel cannot be restored to OPERABLE status or placed in trip within the specified Completion Time.

The Completion Time of 6 hours is reasonable, based on operating experience, to reduce THERMAL POWER to below P-7 from full power in an orderly manner and without challenging unit systems.

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.1.4

SR 3.3.1.4 is the performance of a TADOT. This test shall verify RTB train OPERABILITY by actuation of the two RTBs for each train to their trip state. Each RTB may be actuated together or individually.

The RTB train test shall include three separate but overlapping tests: (1) The Undervoltage test for verification of RTB operability using only the Undervoltage Trip Mechanism, (2) The Shunt Trip test for verification of RTB operability using only the Shunt Trip Mechanisms, and (3) The Manual Reactor Trip test for verification of RTB operability using the hardwired switches. The Undervoltage test shall bypass the Shunt Trip Mechanism, so each RTB actuates using only the Undervoltage Trip Mechanism. The Shunt Trip test shall bypass the Undervoltage Trip Mechanism, so each RTB actuates using only the Shunt Trip Mechanism. The Manual Reactor Trip test shall actuate the RTB with both mechanisms. Figure 4.4-1 of MUAP-07004 (Ref. 6) describes an acceptable overlapping method for conducting these three separate tests that confirms OPERABLE status.

[The Surveillance Frequency of every 62 days on a STAGGERED TEST BASIS applies to all four RTB trains. This Surveillance Frequency is justified based on industry experience. The Surveillance Frequency also considers the added reliability of the US-APWR RTB configuration, which includes redundant RTBs within each train and the overall two-out-of-four train configuration. Since each test actuates each RTB to its required trip state, the STA IS results in each RTB being tested every 248 da ethod being tested every 744 days.

Replace with "supported by".

The TADOT STAGGERED TEST BASIS Surveillance Frequency of 62 days, with each RTB tested every 248 days, and each trip method ultimately tested every 744 days, is also ~~justified in~~ the US-APWR reliability and risk ~~analyses, the summary and result of~~ which are documented in FSAR Chapter 19 (Ref. 10).

MIC-04-16-00001

Replace with "insights".

Add "Appendix B".

Delete.

SURVEILLANCE REQUIREMENTS (continued)

The complete OPERABILITY check from the measurement channel input device to the Reactor Trip Breaker is performed by the combination of the continuous automatic self-testing for the digital devices (the RPS and data communication interfaces), the continuous automatic CHANNEL CHECK (SR 3.3.1.1 and SR 3.3.1.7), the CHANNEL CALIBRATION (SR 3.3.1.8, SR 3.3.1.9 and SR 3.3.1.10), the MIC (SR 3.3.1.6) and the TADOT (SR 3.3.1.4 and SR 3.3.1.11). The CHANNEL CALIBRATION, the MIC and the TADOT, which are manual tests, overlap with the continuous automatic self-testing and confirm the functioning of the continuous automatic self-testing.

[The Surveillance Frequency ~~is~~ ed because the software ~~is~~ checked omatic self-testing.

Replace with "insights".

Replace with "supported by".

The Surveillance Frequency of 24 months is also ~~justified in~~ the US-APWR reliability and risk ~~analyses~~, ~~the summary and result of~~ which are documented in FSAR Chapter 19 (Ref. 10).

MIC-04-16-00001

Delete.

OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]

Add "Appendix B".

SR 3.3.1.7

Performance of the CHANNEL CHECK within 4 hours after reducing power below P-6 and [once every 12 hours thereafter OR in accordance with the Surveillance Frequency Control Program] ensures that gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the parameter indicated on one channel to a similar parameter on other channels. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the

BASES

SURVEILLANCE REQUIREMENTS (continued)

[As appropriate, each channel's response must be verified every 24 months on a STAGGERED TEST BASIS. Testing of the final actuation devices (i.e., RTBs) is included in the testing. Response times cannot be determined during unit operation because equipment operation is required to measure response times. Experience has shown that these components usually pass this SR when performed at the 24 months Surveillance Frequency. Therefore, the Surveillance Frequency was concluded to be acceptable from a reliability standpoint. OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]

SR 3.3.1.12 is modified by a Note stating that neutron detectors are excluded from RTS RESPONSE TIME testing. This Note is necessary because of the difficulty in generating an appropriate detector input signal. Excluding the detectors is acceptable because the principles of detector operation ensure a virtually instantaneous response.

REFERENCES

1. Regulatory Guide 1.105, Revision 3, "Setpoints for Safety Related Instrumentation."
2. FSAR Section 7.2.
3. FSAR Chapter 15.
4. IEEE-603-1991.
5. 10 CFR 50.49.
6. MUAP-07004-P, Revision 7, “Safety I&C System Description and Design Process.”
7. MUAP-07005-P, Revision 8, “Safety System Digital Platform -MELTAC-.”
8. 10 CFR 50.36.
9. FSAR Section 6.2.1.
10. FSAR Chapter 19.
11. MUAP-09021-P, Revision 3, “Response Time of Safety I&C System.”
12. MUAP-09022-P, Revision 3, “Safety I&C Instrument Setpoint Methodology.”
13. FSAR Section 7.1

MIC-04-16-00001

Add "Appendix B".

ACTIONS (continued)

This action addresses the train orientation of the PSMS for the functions listed above. If one required train is inoperable, 72 hours are allowed to return it to an OPERABLE status. Note that for Containment Spray and Phase B Isolation, failure of one or both channels in one train renders the train inoperable. Condition B, therefore, encompasses both situations.

The Completion Time of 72 hours is justified because (1) for ECCS two trains are adequate to perform the safety function and there are three required automatic actuation trains and two other required Manual Initiation trains OPERABLE, (2) for Containment Spray three trains are adequate to perform the safety function and there are four automatic actuation trains and three other Manual Initiation trains OPERABLE, or (3) for Containment Phase A Isolation one train is adequate to perform the safety function and there are two automatic actuation trains and one other Manual Initiation train OPERABLE. The Completion Time also considers that all trains of ECCS can be initiated by the Manual Initiation Function from the two remaining trains, and Containment Spray can be initiated by the Manual Initiation Function from any two of the three remaining trains.

In addition, the Completion Time considers that each train of all Functions can be manually initiated from the Safety VDU for that train. Therefore, nitiation throu oment remains functional in all trains.

Replace with "insights".

Replace with "supported by".

The Completion Time of 72 hours is also ~~justified in~~ the US-APWR reliability and risk ~~analyses~~, ~~the summary and result of~~ which are documented in FSAR Chapter 19 (Ref. 11).

MIC-04-16-00001

Delete.

If the train cannot be restored to OPERABLE status, the unit must be placed in a MODE in which ~~the~~ Add "Appendix B". This is done by placing the unit in at least MODE 3 within an additional 6 hours (78 hours total time) and in MODE 5 within an additional 30 hours (108 hours total time). The allowable Completion Times are reasonable, based on operating experience, to reach the required unit conditions from full power conditions in an orderly manner and without challenging unit systems.

ACTIONS (continued)

C.1, C.2.1, and C.2.2

Condition C applies to the Actuation Logic and Actuation Outputs for the following Functions:

- Containment Phase A Isolation, and
- Containment Phase B Isolation.

This action addresses the train orientation of the PSMS. If one train is inoperable, 24 hours are allowed to restore the train to OPERABLE status.

The Completion Time of 24 hours is justified because the remaining OPERABLE train(s) ~~are adequate to perform~~ the safety function. In addition, ~~the Completion Time~~ maining OPERABLE train(s) each ~~ntinuous aut~~

Replace with "supported by".

Replace with "insights".

The Completion Time of 24 hours is also ~~justified in~~ the US-APWR reliability and risk ~~analyses~~, ~~the summary and result of~~ which are documented in FSAR Chapter 19 (Ref. 11).

MIC-04-16-00001

Delete.

If the train cannot be restored to OPERABLE status, the unit must be placed in a MODE ~~in~~ Add "Appendix B". t apply. This is done by placing the unit in at least MODE 3 within an additional 6 hours (30 hours total time) and in MODE 5 within an additional 30 hours (60 hours total time). The Completion Times are reasonable, based on operating experience, to reach the required unit conditions from full power conditions in an orderly manner and without challenging unit systems.

The Required Actions are modified by a Note that allows placing one train in bypass for up to 4 hours while performing surveillance testing, provided the other train(s) are OPERABLE. This 4 hour bypass time is reasonable based on operating experience that 4 hours is the average time required to perform a train surveillance.

BASES

ACTIONS (continued)

The Bypass Time of 4 hours is justified because the remaining OPERABLE train(s) are adequate to perform the safety function. In addition, the Bypass me considers t ERABLE train(s) have continuous utomatic self-te

Replace with "insights".

Replace with "supported by".

The Bypass Time of 4 hours is also ~~justified in~~ the US-APWR reliability and risk ~~analyses~~, ~~the summary and result of~~ which are documented in the FSAR Chapter 19 (Ref. 11).

MIC-04-16-00001

Delete.

D.1, D.2.1, and D.2.2

Add "Appendix B".

Condition D applies to:

- High Containment Pressure, and
- High-High Containment Pressure.

If one required channel is inoperable, 72 hours are allowed to restore the channel to OPERABLE status or to place it in the trip condition. Failure of one channel places the Function in a two-out-of-two configuration, when the failed channel does not result in a trip channel. This configuration provides adequate plan protection, but does not meet the single failure criteria. Therefore, within 72 hours the inoperable channel must be tripped to place the Function in a one-out-of-two configuration that satisfies the single failure criteria.

The Completion Time of 72 hours is justified because the two remaining OPERABLE channels are adequate to perform the safety function. In addition, the Completion Time considers that the two remaining OPERABLE channels have continuous automatic self-testing and continuous automatic CHANNEL CHECKS.

BASES

ACTIONS (

Replace with "insights".

Replace with "supported by".

The Completion Time of 72 hours is also ~~justified in~~ the US-APWR reliability and risk ~~analyses~~, ~~the summary and result of~~ which are documented in FSAR Chapter 19 (Ref. 11).

MIC-04-16-00001

Delete.

Failure to restore the channel inoperable to OPERABLE status or place it in the trip conditi Add "Appendix B". ires the unit be placed in MODE 3 within the following 6 hours and MODE 4 within the next 6 hours.

The allowed Completion Times are reasonable, based on operating experience, to reach the required unit conditions from full power conditions in an orderly manner and without challenging unit systems. In MODE 4, these Functions are no longer required OPERABLE.

The Required Actions are modified by a Note that allows placing one required channel in bypass for up to 12 hours while performing surveillance testing, provided the other required channels are OPERABLE, or one required channel is OPERABLE and the other required channel is placed in the trip condition.

The Bypass Time of 12 hours is justified because the remaining OPERABLE required channels are adequate to perform the safety function. In addition, the Bypass Time considers that the remaining OPERABLE required channels i continuous and continuous automatic CHANNEL CKS.

Replace with "insights".

Replace with "supported by".

The Bypass Time of 12 hours is also ~~justified in~~ the US-APWR reliability and risk ~~analyses~~, ~~the summary and result of~~ which are documented in FSAR Chapter 19 (Ref. 11).

MIC-04-16-00001

Delete.

Add "Appendix B".

ACTIONS (continued)

E.1, E.2.1, and E.2.2

Condition E applies to:

- Containment Spray - High-3 Containment Pressure, and
- Containment Phase B Isolation - High-3 Containment Pressure.

If one required channel is inoperable, 72 hours are allowed to restore the channel to OPERABLE status. Failure of one channel places the Function in a two-out-of-two configuration, when the failed channel does not result in a trip channel. This configuration provides adequate plant protection, but does not meet the single failure criteria. Therefore, within 72 hours the inoperable channel must be restored to OPERABLE status. Tripping a channel, as in Condition D, is undesirable because a single failure would then cause spurious Containment Spray initiation. Spurious spray actuation is undesirable because of the cleanup problems presented.

The Completion Time of 72 hours to restore the inoperable channel is justified because the two remaining OPERABLE channels are adequate to perform the safety function. In addition, the Completion Time considers that [illegible] remaining C[illegible]have continuous automatic [illegible]ng and con[illegible]ANNEL CHECKS.

Replace with "insights".

Replace with "supported by".

The Completion Time of 72 hours is also ~~justified in~~ the US-APWR reliability and risk ~~analyses~~, ~~the summary and result of~~ which are documented in FSAR Chapter 19 (Ref. 11).

MIC-04-16-00001

Delete.

Add "Appendix B".

ACTIONS (continued)

Failure to restore the required number of channels to OPERABLE status within 72 hours, requires the unit be placed in MODE 3 within the following 6 hours and MODE 4 within the next 6 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required unit conditions from full power conditions in an orderly manner and without challenging unit systems. In MODE 4, these Functions are no longer required OPERABLE.

The Required Actions are modified by a Note that allows placing one required channel in bypass for up to 12 hours while performing surveillance testing, provided the other required channels are OPERABLE. Bypassing with another channel in trip, as in Condition D, is undesirable because a single failure during surveillance testing would then cause spurious Containment Spray initiation. Spurious spray actuation is undesirable because of the cleanup problems presented.

Bypass Time of 12 hour is justified because the remaining OPERABLE channels are adequate to perform the safety function. In addition, the ~~remaining OPERA~~ ~~ontinuous automatic self-testing and ~~nuous autom~~ ~~KS~~.

Replace with "insights".

Replace with "supported by".

The Bypass Time of 12 hours is also ~~justified in~~ the US-APWR reliability and risk ~~analyses~~, ~~the summary and result of~~ which are documented in FSAR Chapter 19 (Ref. 11).

MIC-04-16-00001

Delete.

F.1, F.2.1, and F.2.2

Add "Appendix B".

Condition F ~~applies to Loss of Offsite~~ Power.

BASES

ACTIONS (continued)

In addition, the Completion Time for the Manual Initiation Function considers that each train can be manually initiated from the Safety VDU for that train. Therefore, through safe remains functional i

Replace with "insights".

Replace with "supported by".

For all Functions, the Completion Time of 72 hours is also ~~justified in~~ the US-APWR reliability and risk ~~analyses, the summary and result of~~ which are documented in FSAR Chapter 19 (Ref. 11).

MIC-04-16-00001

Delete.

If the Function cannot be returned to OPERABLE status, the unit must be placed in MODE 3 within the next 6 in the following 6 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required unit conditions from full power in an orderly manner and without challenging unit systems. In MODE 4, the unit does not have any analyzed transients or conditions that require the explicit use of the protection functions noted above.

Add "Appendix B".

For the Loss of Offsite Power Function a Note is added to allow placing one channel in bypass for up to 4 hours while performing surveillance testing, provided the other channels on the same bus are OPERABLE, or one channel is OPERABLE and the other is placed in the trip condition.

The Bypass Time of 4 hours is justified because the Function remains fully OPERABLE ition, the Bypass Time considers that each OPERABLE automatic self-testing.

Replace with "insights".

Replace with "supported by".

The 4 hour bypass time is also ~~justified in~~ the US-APWR reliability and risk ~~analyses, the summary and result of~~ which are documented in FSAR Chapter 19 (Ref. 5).

MIC-04-16-00001

Delete.

G.1, G.2.1, and G.2.2

Add "Appendix B".

Condition G applies to the Actuation Logic and Actuation Outputs for the;

- Emergency Feedwater Isolation,
- CVCS Isolation,
- Turbine Trip Functions, and
- Main Steam Relief Line Isolation

ACTIONS (continued)

The action addresses the train orientation of the PSMS for these Functions. If one train is inoperable, 24 hours are allowed to restore the train to OPERABLE status.

The Completion Time of 24 hours is justified because the remaining OPERABLE train is adequate to perform the safety function. In addition, the Completion Time considers that the remaining OPERABLE train has continuous automatic

Replace with "insights".

Replace with "supported by".

The Completion Time of 24 hours is also ~~justified in~~ the US-APWR reliability and risk ~~analyses~~, ~~the summary and result of~~ which are documented in FSAR Chapter 19 (Ref. 11).

MIC-04-16-00001

Delete.

If the train cannot be returned to OPERABLE status, the unit must be brought to MODE 3 within 6 hours and MODE 4 within the following 6 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required unit conditions from full power conditions in an orderly manner and without challenging unit systems. Placing the unit in MODE 4 removes all requirements for OPERABILITY of the protection channels and actuation functions. In this MODE, the unit does not have analyzed transients or conditions that require the explicit use of the protection functions noted above.

Add "Appendix B".

The Required Actions are modified by a Note that allows placing one train in bypass for up to 4 hours while performing surveillance testing, provided the other train is OPERABLE.

The Bypass Time of 4 hours is justified because the remaining OPERABLE train is adequate to perform the safety function. In addition, the Bypass Time considers that the remaining OPERABLE train has continuous automatic testing.

Replace with "insights".

Replace with "supported by".

The Bypass Time of 4 hours is also ~~justified in~~ the US-APWR reliability and risk ~~analyses~~, ~~the summary and result of~~ which are documented in FSAR Chapter 19 (Ref. 11).

MIC-04-16-00001

Delete.

Add "Appendix B".

BASES

ACTIONS (continued)

J.1 [and J.2]

Condition J applies to the Actuation Logic and Actuation Outputs for the Emergency Feedwater Actuation.

The action addresses the train orientation of the PSMS for this Functions.

If one required train is inoperable, 72 hours are allowed to restore the train to OPERABLE status.

The Completion Time of 72 hours is justified because the two remaining OPERABLE trains are ~~adequate to perform~~ the safety function. In addition, ~~the~~ pletion Time ~~considers that~~ remaining OPERABLE trains ~~have~~ ve continuou g.

Replace with "insights".

Replace with "supported by".

The Completion Time of 72 hours is also ~~justified in~~ the US-APWR reliability and risk ~~analyses~~, ~~the summary and result of~~ which are documented in FSAR Chapter 19 (Ref. 11).

MIC-04-16-00001

Delete.

[Required Action J.2 allows the option to apply the requirements of Specification 5 isk Informed Completion Time.]

Add "Appendix B".

The Required Actions are modified by a Note that allows placing one required train in bypass for up to 4 hours while performing surveillance testing, provided the other required trains are OPERABLE.

The Bypass Time of 4 hours is justified because the remaining OPERABLE trains are adequate to perform the safety function. In addition, the Bypass ~~Time~~ considers t ERABLE trains have continuous matic self-te g.

Replace with "insights".

Replace with "supported by".

The Bypass Time of 4 hours is also ~~justified in~~ the US-APWR reliability and risk ~~analyses~~, ~~the summary and result of~~ which are documented in FSAR Chapter 19 (Ref. 11).

MIC-04-16-00001

Delete.

Add "Appendix B".

ACTIONS (continued)

K.1

Condition K applies to the failure of one Containment High Range Area Radiation channel. Since the three Containment High Range Area Radiation channels measure the same parameter, failure of a single channel does not result in loss of the radiation monitoring Function for any event.

If one required channel is inoperable, 72 hours are allowed to restore the channel to OPERABLE status. Failure of one channel places the Function in a two-out-of-two configuration.

The Completion Time of 72 hours to restore the inoperable channel is justified because the two remaining OPERABLE channels are adequate to perform the safety function. In addition, the Completion Time considers that [redacted]maining OP[redacted]ve continuous automatic [redacted]g and conti[redacted]NNEL CHECKS.

Replace with "insights".

Replace with "supported by".

The Completion Time of 72 hours is also ~~justified in~~ the US-APWR reliability and risk ~~analyses~~, ~~the summary and result of~~ which are documented in FSAR Chapter 19, (Ref. 11).

Delete.

Add "Appendix B".

MIC-04-16-00001

ACTIONS (continued)

With one required channel inoperable the inoperable channel must be placed in the trip condition within 1 hour and restored to OPERABLE status in 72 hours.

This Condition applies to functions that operate on two-out-of-three logic and have channels that are shared with the control systems. Failure of one channel places the Function in a two-out-of-two configuration, when the failed channel does not result in a trip channel. Normally the SSA can prevent erroneous control system operations. However, when there are less than three OPERABLE channels, the SSA cannot prevent erroneous control system operation due to an input failure. With two OPERABLE channels and one channel in the trip condition, if a channel failure occurs in an OPERABLE channel and results in erroneous control system operation, the remaining OPERABLE channel can provide a plant trip. However, the channel that causes the erroneous control system operation cannot be credited as the single failure; therefore, this configuration does not satisfy the single failure criteria. To satisfy the single failure criteria, three channels must be restored to OPERABLE status within 72 hours.

The Completion Time of 1 hour to place the failed channel in the trip condition is based on operating experience and the minimum amount of time allowed for manual operator actions.

The Completion Time of 72 hours to restore the inoperable channel is justified because the two remaining OPERABLE channels are adequate to perform the safety function. In addition, the Completion Time considers that the two remaining OP ve continuous automatic ting and contin NNEL CHECKS.

Replace with "insights".

Replace with "supported by".

The Completion Time of 72 hours is also ~~justified in~~ the US-APWR reliability and risk ~~analyses~~, ~~the summary and result of~~ which are documented in FSAR Chapter 19, (Ref.11).

MIC-04-16-00001

Delete.

Bypass of a required channel is not allowed because there are only three required chan s are also used for control. If a failure were to occur in one of the two remaining control channels, a plant transient could occur that would require a plant trip, but a plant transient would not occur with only one remaining OPERABLE channel.

Add "Appendix B".

ACTIONS (continued)

If one required train is inoperable, 24 hours are allowed to restore the train to OPERABLE status.

The Completion Time of 24 hours is justified because the remaining OPERABLE trains are adequate to perform the safety function. In addition, the Completion Time considers that the remaining OPERABLE trains each continuous automatic self-testing

Replace with "insights".

Replace with "supported by".

The Completion Time of 24 hours is also ~~justified in~~ the US-APWR reliability and risk ~~analyses, the summary and result of~~ which are documented in FSAR Chapter 19 (Ref. 11).

MIC-04-16-00001

Delete.

Add "Appendix B".

[Required Action Q.2 allows the option to apply the requirements of Specification 5 Risk Informed Completion Time. This Required Action is not applicable in MODE 4, because Risk Informed Completion Times are only applicable to MODES 1, 2 and 3.]

The Required Actions are modified by a Note that allows placing one required train in bypass for up to 4 hours while performing surveillance testing, provided the other required trains are OPERABLE. This 4 hour Bypass Time is reasonable based on operating experience that 4 hours is the average time required to perform a train surveillance.

The Bypass Time of 4 hours is justified because the remaining OPERABLE trains are adequate to perform the safety function. In addition, the Bypass Time considers that the remaining OPERABLE trains have continuous automatic self-testing

Replace with "insights".

Replace with "supported by".

The Bypass Time of 4 hours is also ~~justified in~~ the US-APWR reliability and risk ~~analyses, the summary and result of~~ which are documented in FSAR Chapter 19 (Ref. 11).

MIC-04-16-00001

Delete.

Add "Appendix B".

ACTIONS (continued)

R.1 and R.2

Condition R applies to the Actuation Logic and Actuation Outputs for the following functions:

- ECCS Actuation, and
- Containment Spray,

If the Required Action and associated Completion Time of Condition Q are not met, the unit must be placed in a MODE in which the LCO does not apply. This is done by placing the unit in at least MODE 3 within 6 hours and in MODE 5 within an additional 30 hours (36 hours total time). The Completion Times are reasonable, based on operating experience, to reach the required unit conditions from full power conditions in an orderly manner and without challenging unit systems.

S.1 [and S.2]

Condition S applies to the Actuation Logic and Actuation Outputs for the;

- Main Steam Line Isolation,
- Main Feedwater Isolation, and
- Block Turbine Bypass and Cooldown Valves.

The action addresses the train orientation of the PSMS for these Functions.

If one train is inoperable, 24 hours are allowed to restore the train to OPERABLE status.

The Completion Time of 24 hours is justified because the remaining OPERABLE train is adequate to perform the safety function. In addition, the Completion Time considers the ~~redundancy~~ remaining OPERABLE train has ~~redundant~~ automatic

Replace with "insights".

Replace with "supported by".

The Completion Time of 24 hours is also ~~justified in~~ the US-APWR reliability and risk ~~analyses~~, ~~the summary and result of~~ which are documented in FSAR Chapter 19 (Ref. 11).

MIC-04-16-00001

Delete.

Add "Appendix B".

ACTIONS (continued)

[Required Action S.2 allows the option to apply the requirements of Specification 5.5.18 to determine a Risk Informed Completion Time.]

The Required Actions are modified by a Note that allows placing one train in bypass for up to 4 hours while performing surveillance testing, provided the other train is OPERABLE.

The Bypass Time of 4 hours is justified because the remaining OPERABLE train is adequate to perform the safety function. In addition, the Bypass Time considers that the E train has continuous automatic testing.

Replace with "insights".

Replace with "supported by".

The Bypass Time of 4 hours is also ~~justified in~~ the US-APWR reliability and risk ~~analyses, the summary and result of~~ which are documented in FSAR Chapter 19 (Ref. 11).

MIC-04-16-00001

Delete.

T.1 and T.2

Add "Appendix B".

Condition T applies to the Actuation Logic and Actuation Outputs for the following functions:

- Main Steam Line Isolation,
- Main Feedwater Isolation,
- Emergency Feedwater Actuation, and
- Block Turbine Bypass and Cooldown Valves.

Condition T applies when the Required Action and associated Completion Time for Condition J or S have not been met. If the train cannot be returned to OPERABLE status, the unit must be brought to MODE 3 within the next 6 hours and MODE 4 within the following 6 hours (12 hours total time). Placing the unit in MODE 4 removes all requirements for OPERABILITY of the protection channels and actuation functions. In this MODE, the unit does not have analyzed transients or conditions that require the explicit use of the protection functions.

The allowed Completion Times are reasonable, based on operating experience, to reach the required unit conditions from full power conditions in an orderly manner and without challenging unit systems.

BASES

ACTIONS (continued)

The Completion Time of 48 hours is justified because the two remaining OPERABLE trains are adequate to perform the safety function. In addition, the Completion Time [Replace with "supported by".] o remaining OPERABLE trains [Replace with "insights".] have continuou ng.

The Completion Time of 48 hours is also ~~justified in~~ the US-APWR reliability and risk ~~analyses~~, ~~the summary and result of~~ which are documented in FSAR Chapter 19 (Ref. 11). [Delete.]

MIC-04-16-00001

If the train cannot be restored to OPERABLE status, the unit must be placed in MODE 3 ~~wi~~ [Add "Appendix B".] d MODE 4 within the following 6 hours. In MODE 4, the unit does not have any analyzed transients or conditions that require the explicit use of the interlock function noted above.

The allowed Completion Times are reasonable, based on operating experience, to reach the required unit conditions from full power in an orderly manner and without challenging unit systems.

SURVEILLANCE REQUIREMENTS

The SRs for each ESFAS Function are identified by the SRs column of Table 3.3.2-1.

A Note has been added to the SR Table to clarify that Table 3.3.2-1 determines which SRs apply to which ESFAS Functions.

Note that each channel of process protection supplies all trains of the ESFAS. However, when testing a channel, it is only necessary to manually verify that the channel is OPERABLE in its respective division. This is because the interface to other divisions is automatically verified through continuous automatic self-testing. Continuous automatic self-testing is confirmed through periodic MIC. The CHANNEL CALIBRATION is performed in a manner that is consistent with the methods and assumptions of Specification 5.5.21, Setpoint Control Program (SCP).

SR 3.3.2.1

Performance of the CHANNEL CHECK ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the parameter indicated on one channel to a similar parameter on other channels. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value. Significant deviations between instrument channels could be an indication of excessive instrument drift in one of the channels or of something even more serious. A CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

SURVEILLANCE REQUIREMENTS (continued)

Replace with "insights".

Replace with "supported by".

The Surveillance Frequency of 24 months is also ~~justified in~~ the US-APWR reliability and risk ~~analyses~~, ~~the summary and result of~~ which are documented in FSAR Chapter 19 (Ref. 11).

Delete.

Add "Appendix B".

OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk a[illegible]he Surveillance Frequency Control Program.]

MIC-04-16-00001

SR 3.3.2.3

SR 3.3.2.3 is the performance of a TADOT for the Actuation Outputs of all ESFAS Functions, and the Actuation Outputs of the Manual Control of ESF Components Function. This surveillance test actuates the outputs of the SLS.

Therefore, this test is typically conducted in conjunction with testing the plant process components. Since this test is conducted in conjunction with testing for plant process components, this test may be conducted more frequently, as may be required for the plant process components.

[The Surveillance Frequency of 24 months is adequate, based on industry operating experience, considering instrument reliability and operating history data of solid state Actuation Output devices.

OR The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.]

BASES

SURVEILLANCE REQUIREMENTS (continued)

REFERENCES

1. NUREG-0737, “Clarification of TMI Action Plan Requirements.”
2. FSAR Section 7.3.
3. FSAR Chapter 15.
4. IEEE-603-1991.
5. 10 CFR 50.49.
6. MUAP-07004-P , Revision 7, “Safety I&C System Description and Design Process.”
7. MUAP-07005-P , Revision 8, “Safety System Digital Platform -MELTAC-.”
8. MUAP-09021-P, Revision 3, “Response Time of Safety I&C System.”
9. 10 CFR 50.36.
10. FSAR Section 15.7.4.
11. FSAR Chapter 19.
12. MUAP-09022-P, Revision 3, “US-APWR Instrument Setpoint Methodology.”
13. Regulatory Guide 1.105, Revision 3, “Setpoints for Safety Related Instrumentation.”
14. FSAR Chapter 9.4.1.2.2.

Add "Appendix B".

MIC-04-16-00001

BASES

ACTIONS (Continued)

The Completion Time of 6 hours is justified because the two remaining OPERABLE undervoltage devices for each bus are adequate to perform the safety function. Since the undervoltage devices are dedicated for each of the four Class 1E busses, and two undervoltage devices are adequate to perform the safety function of each bus, the LOP Class 1E GTG Start Instrumentation Function continues to meet the single failure criterion (i.e., three GTGs will still ... additional undervoltage device ... one bus).

Replace with "insights".

Replace with "supported by".

The Completion Time of 6 hours is also ~~justified in~~ the US-APWR reliability and risk ~~analyses~~, ~~the summary and result of~~ which are documented in FSAR Chapter 19 (Ref. 5).

MIC-04-16-00001

Delete.

A Note is added to allow placing one channel in bypass for up to 4 hours while performi... Add "Appendix B". ... provided the other channels on the same bus are OPERABLE, or one channel is OPERABLE and the other is placed in the trip condition.

The Bypass Time of 4 hours is justified because the remaining OPERABLE channels are adequate to perform the safety function. In addition, the Bypass Time consi... OPERABLE channels have continuous automatic s...

Replace with "supported by".

Replace with "insights".

The 4 hour Bypass Time is also ~~justified in~~ the US-APWR reliability and risk ~~analyses~~, ~~the summary and result of~~ which are documented in FSAR Chapter 19 (Ref. 5).

MIC-04-16-00001

Delete.

Add "Appendix B".

B.1

Condition B applies when two or more loss of voltage or two or more degraded voltage channels per required Class 1E 6.9 kV bus are inoperable.

Required Action B.1 requires restoring all but one channel per required Class 1E 6.9 kV bus to OPERABLE status. The 1 hour Completion Time should allow ample time to repair most failures and takes into account the low probability of an event requiring an LOP start occurring during this interval.

C.1

Condition C applies when one train of the LOP Actuation Function is inoperable for a required bus, or when the Required Action and associated Completion Time for Condition A or B are not met.

BASES

REFERENCES

1. FSAR Section 8.3.1.

2. MUAP-07004-P, Revision 7, “Safety I&C System Description and Design Process.”

3. MUAP-07005-P, Revision 8, “Safety System Digital Platform -MELTAC-.”

4. 10 CFR 50.36.

5. FSAR Chapter 19.

6. FSAR Chapter 15.

7. MUAP-09022-P, Revision 3, “US-APWR Instrument Setpoint Methodology.”

MIC-04-16-00001

Add "Appendix B".

MIC-04-07-001

The ~~PRA safety goals, the~~ Single Failure Criterion, and GDC24 are met with only three trains in service. Therefore, these requirements are met even when one RPS train and its corresponding RTA train are bypassed. Therefore, bypass of one complete RPS/RTA train is permitted for a limited time period consistent with the reliability of the remaining three trains. Interlocks between RPS trains prevent bypassing two RPS trains or two RTA trains.

It is noted that the PSMS and PCMS share sensors. The method used to ensure this sensor sharing does not compromise conformance to the Single Failure Criterion or GDC 24 while a train is bypassed is discussed below.

b. Engineered Safety Features Actuation Function in RPS

In addition, to the requirements for a reactor trip for anticipated abnormal transients, adequate instrumentation and controls are provided to sense accident situations and initiate the operation of necessary Engineered Safety Features (ESF). The occurrence of a limiting fault, such as a loss of coolant accident (LOCA) or a steam line break, requires a reactor trip plus actuation of one or more ESF in order to prevent or mitigate damage to the core and reactor coolant system (RCS) components, and ensure containment vessel integrity.

In order to accomplish these design objectives, the RPS receives signals from various sensors and transmitters for actuation of ESF systems.

The RPS uses selected plant parameters to determine if predetermined safety-related limits are being exceeded. These parameters and safety-related limits are monitored in various combinations which are indicative of primary or secondary system boundary ruptures. Once the required logic combination is completed, the RPS sends the appropriate actuation signals to the ESFAS for event mitigation.

To actuate ESF systems the RPS interfaces with the following equipment:

- Sensors
- Engineered Safety Features Actuation System

Four sensors, each in separate trains, normally monitor each variable which is used for engineered safety features (ESF) actuation. (These sensors may be monitoring the same variable for a reactor trip function as well.) Analog measurements are converted to digital form by analog-to-digital converters within each of the four trains of the RPS. Following required signal conditioning or processing, the measurements are compared against the setpoints for the ESF to be generated. This signal conditioning, processing and comparison is done independently within each of the four trains of the RPS. When the measurement exceeds the setpoint, the output of comparison results in a partial actuation signal for that train. Each RPS train sends its own partial actuation signal to each of the other three RPS trains over isolated serial data links. Each RPS train will generate a system level ESF actuation signal if two or more redundant trains of a single variable are in the partial actuation state.

4.2.2 ESF Actuation System (ESFAS)

The ESFAS consists of one train for each mechanical ESF train in the plant. For the US-APWR some ESF systems have four trains, others have two trains. Since the ESFAS is common to all ESF systems, there are four ESFAS trains for the US-APWR.

Plant specific technical specifications identify manual surveillance tests that confirm input signal calibration and propagation through the digital system. Manual surveillance tests are also provided to confirm command propagation through the digital system and correct control of plant components. These manual surveillance tests, along with the self-diagnosis and Memory Integrity Checks discussed above, are credited to eliminate manual surveillance tests of functional logic and algorithms, setpoints and constants.

5.1.10 Unrestricted Bypass of One Safety-Related Instrument Channel

The PSMS includes multiple trains from sensors to actuated device with complete electrical isolation and independence.

For system functions with four redundant (non-spatially dependent) instrument channels, one instrument channel may be bypassed continuously without violating any design criteria. The system adheres to all criteria with only three instrument channels in operation, as follows:

MIC-04-07-00001

Specification LCO is expected for two or more instrument channels bypassed or out of service.

MIC-04-07-00001

5.1.11 Minimum Inventory of HSI

Class 1E HSI is provided by the safety VDUs for all safety-related indications and controls. Spatially Dedicated Continuously Visible (SDCV) displays are provided for all critical safety function parameters and for bypassed and inoperable conditions. This data is obtained from the PSMS and PCMS. SDCV HSIs are provided for manual initiation of reactor trip and ESFAS. Additional SDCV HSIs may be provided to ensure timely operator actions for specific plant events. The complete minimum inventory of SDCV HSI is described in the HSI system Topical Report, MUAP-07007. These are also described in DCD Chapter 18.

5.1.12 Computer Based Procedures

Computer based procedure allows operators to access relevant display formats which are hyper linked from the procedure and shown on the operational VDU. Operator accesses and operates the required control switch quickly from the linked display formats on the operational VDU, if necessary.

5.1.13 Priority Logic

The means by which the failure will come to the attention of the plant operation/maintenance staff are identified. This could be by automatic detection or manual testing.

Local Failure Effect
The consequent effect(s) of the failure on the component or on its adjunct components are described. Symptoms and local effects including dependent failure are also provided.

Effect on Protective Function or Plant
For safety-related systems the effect of the failure on the ability to complete the protective function or spurious actuation of the protective function is described, including identification of any degradation in performance or degree of redundancy. For non-safety functions the effect of the failure on the plant is described. Any plant challenges that are outside the boundary conditions of the Plant Safety Analysis are discussed. For safety-related and non-safety functions mitigating design features that prevent or limit the failure effects are discussed.

Failures that are undetectable or result in effects that violate the system design basis are specifically highlighted. These failures are specifically justified or the system design is modified.

Table 6.5-1 Deleted

The FMEA for safety-related I&C system is provided in the US-APWR DCD Chapter 7.

6.5.2 Reliability Analysis Method

The reliability of the safety-related I&C system to perform its safety-related functions is analyzed in the Probabilistic Risk Assessment (PRA).

This analysis starts with the simplified block diagram discussed above for the FMEA. This block diagram shows the major components that must operate correctly for actuation of the safety-related function. The Mean Time Between Failure (MTBF) is identified for each component. The MTBF for components of the MELTAC platform are provided in the MELTAC Platform Technical Report. The MTBF for other components is obtained from industry handbooks or manufacturers publications. The actual reliability data and the source of the data for these components is identified in plant licensing documentation. The system reliability is calculated based on this system model and the MTBF of each component.

The reliability analysis credits internal redundancy within each train, and it credits all four available trains for each system.

However, the reliability analysis credits only three of four instrument channels for each measured parameter. This conservative approach ensures that the system meets the required PRA goals while operating in a degraded condition. Based on this there are no Limiting Conditions of operation expected for extended operation with an instrument channel out of service. Refer to MUAP-07030 Attachments 6A.12 and 6A.13.

MIC-04-07-00001

The reliability analysis credits the immediate detection of module failures that are tested by self-diagnosis. For failures in components that are manually tested and calibrated, the reliability analysis is based on a 24 month surveillance interval.

each other and isolated from non-safety systems. Isolation ensures functional and communications independence and independence for fires and electrical faults. The design life of PSMS components is maximized when operated continuously in a controlled ventilation environment. The PSMS will operate reliably for extended periods with loss of ventilation.

A.4.9 Reliability

The reliability analysis methods for the PSMS are described in Section 6.5.2. This analysis ensures that the PSMS meets the reliability requirements assumed in the Probabilistic Risk Assessment (PRA). The PSMS includes either N trains or N+1 trains, depending on the application. N is the number of trains needed to meet the single failure criterion and the number of trains needed to meet the ~~PRA goals~~single failure criterion.

MIC-04-07-00001

A.4.10 The Critical Points in Time or the Plant Conditions

The PSMS automatically initiates appropriate protective actions when a plant condition monitored by the system reaches a preset level. The critical points in time are determined by the PSMS response time modeled in the accident analysis. The PSMS is designed and tested to meet the response times assumed in the accident analysis.

The operator can reset the PSMS system level actuation signal using minimum two distinct and deliberate actions. There are no automatic resets of the system level actuation signals.

A.4.11 Equipment Protective Provisions

No credible single failure of an equipment protective device prevents the initiation or accomplishment of a safety function at the system level.

The PSMS continuously checks internal conditions such as power supply and digital component operability. Components are automatically shut down under component failure conditions that may lead to unpredictable system performance. These checks are conducted independently within each train of the PSMS, therefore a spurious shutdown of PSMS equipment will only affect one train.

The equipment protective features are designed to place the safety systems in a safety state, or into a state that has been demonstrated to be acceptable, if the safety-related equipment fails or the equipment protective device operates. Each protection function has different characteristics and therefore different techniques are used to achieve a fail-safe design. Examples of protective features for selected functions include:

- Reactor trip circuits are designed to fail in the tripped state.
- Engineered safety features actuated components are designed to fail into a de-energized state or fail as-is. The de-energized state applies to failures that result in complete loss of component control. The as-is state is selected for failures that impair control but do not result in complete loss of component control. These states has been demonstrated to be

The US-APWR DCD Subsections 7.1.3.19 describes distinct train color coding for labels and name tags.

In accordance with IEEE-494, PSMS end-user documentation is identified “Nuclear Safety Related”. End-user documentation includes:

(1) Drawings such as instrument diagrams, functional control diagrams, one line diagrams, schematic diagrams, equipment arrangements, cable and tray lists, wiring diagrams
(2) Instrument data sheets
(3) Design specifications
(4) Instruction manuals
(5) Test specifications, procedures, and reports
(6) Device lists

A.5.12 Auxiliary Features

The PSMS is built on the digital platform described in the MELTAC Platform Technical Report. All components of this platform, with the exception of the MELTAC engineering tool Personal Computer, are safety-related and conform to the requirements for safety systems. Other auxiliary features such as electrical power sources and building HVAC are described in the US-APWR DCD Subsection 7.1.1.10, Chapters 8 and 9.

The PSMS includes safety related functions such as reactor trip and ESF actuation. It also includes the following associated non-safety functions:

- Alarm signal generation
- Indications for RG 1.97 Rev.4 Type D variables
- Indications for system actuation status
- Cabinet temperature monitoring
- Door open monitoring
- Input power monitoring

These associated non-safety functions are not isolated from the PSMS. Therefore they are considered part of the safety system.

A.5.13 Multi-Unit Stations

There is no sharing of PSMS components between units.

A.5.14 Human Factors

The Human Factors Engineering program applied to the PSMS functions is described in the HSI Topical Report.

A.5.15 Reliability

The PSMS reliability is used in the Probabilistic Risk Assessment (PRA). That analysis is described in the US-APWR DCD Chapter 19, and MUAP-07030 Attachments 6A.12 and 6A.13. The component level reliability which is the basis for the PRA analysis is described in

MIC-04-07-00 001

All Operating Bypasses, either manually or automatically initiated, are automatically removed when the plant moves to an operating regime where the protective action is required if an accident occurred. Status indication is provided in the control room for all Operating Bypasses.

A.6.7 Maintenance Bypass

These bypasses may be manually initiated from the S-VDU or O-VDU. To manually initiate a Maintenance Bypass from the O-VDU the Bypass Permissive for the train must be enabled.

a. Input Channel Bypass

The safety system is designed to permit the unrestricted bypass for maintenance, test, or repair of any one protection input channel in the group of channels monitoring a selected variable. This bypass is accomplished during power operation without causing initiation of a protective function. The system also meets the single failure criterion while permitting power operation for an indefinite period of time with one channel of the selected variable bypassed. Indication is provided in the control room if some part of the system has been administratively bypassed or taken out of service.

With one channel bypassed, the RPS does not permit the bypass of a second channel in the group monitoring the same variable. An attempt to apply multiple bypasses is blocked, and trip/actuation is not triggered by the attempt.

Except for two channel function, there are four protection channels for each actuation function. Accident and reliability analyses assume that one of these channels is in the bypass mode at the time of the accident. This assumption precludes potential limitations that might have otherwise been placed on the use of the bypass feature.

For each input, the technical specifications limit the period allowed for two channels to be out of service (i.e., either two failed in a non-trip state or one in bypass and one failed in a non-trip state). The time specified in the technical specifications is supported in the probabilistic and risk insights ~~determined by~~ considering the probability of the event the significance of the input to event mitigation.

MIC-04-07-00 001

b. Train Level RPS Bypass

Each RPS train takes inputs from one or more input process sensors, performs compensation or other calculation which terminates in one or more bistable functions where the process variable is compared against setpoints. The coincidence logic portion of the RPS receives the partial trip outputs from these comparisons and combines them with the partial trip status of the other channels to initiate a reactor trip or ESF actuation.

Each RPS train has the ability to bypass all partial trip input signals from the other trains. This function is useful if an entire RPS train is taken out of service. When an entire RPS train is bypassed each individual channel for that train is bypassed and therefore subject to the alarms and interlocks described above for individual input channels. Therefore, if input channels are previously bypassed the RPS train level bypass may be blocked or alarmed. In the same manner, if an RPS bypass is already active, any attempt to put additional input channels in bypass is alarmed / blocked.