7. ~~Digital communication independence from non-safety systems to the PSMS is achieved by communication processors of the~~The PSMS ~~that~~ can mitigate all identifiable design-basis communication faults of the other PSMS divisions and the non-safety DCS. DCD_07.09-27 DCD_07.09-27 S01

2.5.6.2 Inspections, Tests, Analyses, and Acceptance Criteria

Table 2.5.6-1 describes the ITAAC for the DCS.

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

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria	
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.	5. Type tests of the PSMS changeability will be performed.	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 the DCS 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.	6.i An inspection of the as-built PSMS will be performed to verify the DCS communication processors are installed.	6.i ~~C~~The DCS communication processors exist in the as-built PSMS for digital communication between redundant divisions of the PSMS and between non-safety systems and the PSMS.	DCD_07.09-26 S01 DCD_07.09-26 S01
	6.ii Type tests or analyses, or a combination of type tests and analyses of the digital communication independence will be performed.	6.ii A report exists and concludes that digital communication independence is achieved by the DCS communication processors that are independent of trip and actuation processing functions.	DCD_07.09-26 S01
	~~6.iii Type tests or analyses, or a combination of type tests and analyses of fault mitigation functions of the communication processors for the DCS will be performed.~~	~~6.iii A report exists and concludes that the communication processors for the DCS can mitigate the design basis communication faults of the DCS.~~	DCD_07.09-26 S01 DCD_07.09-27
7. ~~Digital communication independence from non-safety systems to the PSMS is achieved by communication processors of the~~The PSMS ~~that~~ can mitigate all identifiable design-basis communication faults of the other PSMS divisions and the non-safety DCS.	7. Type tests or a combination of type tests and analysis of ~~the communication processors of~~ the PSMS will be performed to verify fault mitigation functions for each design-basis communication fault of the other PSMS divisions and the non-safety DCS.	7. A report exists and concludes that ~~the communication processors of~~ the PSMS can mitigate all identifiable design-basis communication faults of the other PSMS divisions and the non-safety DCS.	DCD_07.09-27 DCD_07.09-27 S01

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. Communication independence between the MELTAC controllers in different PSMS trains is achieved by a communication controller in the Bus Master Module that is separate from the function processor in the Main CPU Module. Interdivisional communications from the PCMS to the PSMS are limited to that needed to support several PSMS functions. Communication independence between the MELTAC controllers in the PSMS and the controllers and computers of the PCMS is achieved by a communication controller in the Control Network I/F Module that is separate from the function processor in the Main CPU Module. The communication controller and the Main CPU operate asynchronously, sharing information only by means of 2-port memory that is dedicated exclusively to this exchange of information. The combination of via separate communication controllers and the 2-port memory, allow the Main CPU of the PSMS to execute all safety functions, in a fixed deterministic cycle time, and this fixed deterministic cycle time is not affected by the data communication from outside each train of the PSMS.

Also, all communication and safety functions of the PSMS are executed from non-volatile devices which can only be changed by physical withdrawal from the PSMS cabinet. Therefore any communication signals from the outside of each train PSMS cannot change the safety functions or the functions that ensure communication independence.

DCD_07.09-27

~~The communication independence from the PCMS to the PSMS is achieved by the Control Network I/F Module of the PSMS as described above. The Control Network I/F Module of the~~The PSMS can mitigate all design-basis communication faults of the non-safety DCS, such as the Unit Bus, the operational VDUs and other PCMS devices. Details regarding the design-basis communication faults and the fault mitigation functions of the PSMS are described in the MELTAC Platform Technical Report (Reference 7.9-1) Subsection 4.3.2.5.2 and Appendix H.

DCD_07.09-27 S01

(4) Functional Independence

Functional independence ensures the safety function in each PSMS train will execute correctly in the presence of any signals, valid or spurious, received from outside its train. The priority logic functions in the PSMS that ensure functional independence is maintained for each PSMS train in the presence of normal or erroneous interdivisional communication signals. The priority logic function allows each train of the PSMS to protect itself against any signals from outside its train. The priority logic function is executed from non-volatile devices which can only be changed by physical withdrawal from the PSMS cabinet. Therefore any communication signals from the outside of each train PSMS cannot change the priority logic functions that ensure functional independence.

4.1.4 MELTAC Engineering Tool

The MELTAC engineering tool (called “MELENS”) provides various functions aimed at steadier and more efficient software management during all system life cycle phases (including design, fabrication, test, adjustment and maintenance).
MELENS is installed on a non-safety Personal Computer running the Microsoft Windows Operating System.
Access to MELENS is controlled by means of the PC password (BIOS, OS) and the MELENS password.
The application software execution data generated by MELENS is downloaded to the controller via the Maintenance Network and is stored in the F-ROM of the CPU Module. The functions of MELENS are described as follows.

4.1.4.1 Function Description

The functions of MELENS are as follows.

a) Creation of Application Software

The FBDs (see Section 4.1.3.2) are created with a commercial Mitsubishi CAD software package called "RAPID". (Access to RAPID is also controlled by a password.)
MELENS has the functionality to convert RAPID FBDs to MELTAC application software GBDs.
MELENS can then be used to automatically generate (compile) the application software execution data directly from the GBD.
This automated process eliminates human translation errors.
GBDs can also be manually created (drawn) using the MELENS GUI editor.
Regardless of how the GBD is generated (automatically from RAPID or manually drawn with MELENS GUI editor), the assignment of GBDs to controllers and the assignment of Input/Output signals is manually configured using MELENS.

The outputs from both RAPID and MELENS are confirmed through manual V&V activities.

b) Download

New application software, including logic changes or changes to setpoints or constants, can be downloaded to the controllers from the MELTAC engineering tool PC via the Maintenance Network. **[**

DCD_07.09 -27 S01

]

DCD_07.09-27 S01
DCD_07.01-46
DCD_07.01-46 S01

DCD_07.01-46
DCD_07.01-46 S01
DCD_07.09-27 S01

]

[

DCD_07.01-46
DCD_07.01-46 S01

DCD_07.
09-27 S01

]

4.1.5.2.2 Bus Master Module

[

DCD_07.
01-46 S01

DCD_07.
01-46
DCD_07.
01-46 S01

DCD_07.
01-46 S01

DCD_07.
09-27 S01

DCD_07.
01-46 S01

DCD_07.
09-27

DCD_07.
09-27

]

4.1.5.2.3 Control Network I/F Module

[

DCD_07.
09-27 S01

DCD_07.
01-46 S01

DCD_07.
01-46 S01

4.3.2.5.2 Summary of Design Features for Inter-divisional Communications

This section is a summary discussion of design features for the inter-divisional communications on the Control Network.
The receiving process in the data flow from the operational VDU to the COM will be discussed in this section.
In the Control Network interface, there are design policies and network check methods that provide the necessary means to comply with the requirements of ISG-04 for communication.

[

DCD_07.09-27 S01

4.3.3.5.2 Summary of the Design Feature for the Inter-divisional Communication

This section discusses the summary of the design feature for the inter-divisional communication on the Data Link.

[

DCD_07.09-27 S01

DCD_07.09-27 S01

]

4.3.4.4.3 Communication Controller

[

DCD_07.09-27 S01

]

DCD_07.09-27 S01

Figure D.1 Conformance Map of ISG-04 (Control Network)

DCD_07.09-27 S01

Figure D.2 Conformance Map of ISG-04 (Data Link)

E.2.2.1 CPU Module

Table E.2-2A CPU Module

DCD_07.09-27 S01

DCD_07.01-46 S01

Table E.2-2B CPU Module

DCD_07.01-46 S01

DCD_07.09-27 S01

Table E.2-2C CPU Module

DCD_07.09-27 S01

DCD_07.01-46 S01

Table E.2-2D CPU Module

DCD_07.09-27 S01

DCD_07.01-46 S01

Table E.2-2E CPU Module

DCD_07.09-27 S01

DCD_07.01-46 S01

DCD_07.09-27 S01

DCD_07.01-46 S01

Table E.2-2F CPU Module

Table E.2-2G CPU Module

DCD_07.09-27 S01

DCD_07.01-46 S01

E.2.2.2 System Management Module (SMM)

Table E.2-3A System Management Module

DCD_07.09-27 S01

DCD_07.01-46 S01

Table E.2-3B System Management Module

DCD_07.09-27 S01

DCD_07.01-46 S01

Table E.2-3C System Management Module

DCD_07.09-27 S01

DCD_07.01-46 S01

Table E.2-3D System Management Module

DCD_07.09-27 S01

DCD_07.01-46 S01

Table E.2-3E System Management Module

DCD_07.09-27 S01

DCD_07.01-46 S01

Table E.2-3F System Management Module

DCD_07.09-27 S01

DCD_07.01-46 S01

E.2.2.3 Bus Master Module

Table E.2-4A Bus Master Module

DCD_07.09-27 S01

DCD_07.01-46 S01

Table E.2-4B Bus Master Module

DCD_07.01-46 S01

DCD_07.09-27 S01

Table E.2-4C Bus Master Module

DCD_07.09-27 S01

DCD_07.01-46 S01

Table E.2-4D Bus Master Module

DCD_07.09-27 S01

DCD_07.01-46 S01

E.2.2.4 Control Network I/F Module

Table E.2-5A Control Network I/F Module

DCD_07.09-27 S01

DCD_07.01-46 S01

Table E.2-5B Control Network I/F Module

DCD_07.09-27 S01

DCD_07.01-46 S01

Table E.2-5D Control Network I/F Module

DCD_07.01-46 S01

DCD_07.09-27 S01

Table E.2-5E Control Network I/F Module

DCD_07.09-27 S01

DCD_07.01-46 S01

Table E.2-5F Control Network I/F Module

DCD_07.09-27 S01

DCD_07.01-46 S01

E.2.2.5 FMU Module

Table E.2-6A FMU Module

DCD_07.01-46 S01

DCD_07.09-27 S01

Table E.2-6B FMU Module

DCD_07.09-27 S01

DCD_07.01-46 S01

DCD_07.09-27 S01

DCD_07.01-46 S01

Table E.2-6C FMU Module

Table E.2-~~7A~~6D ~~Touch Panel Interface~~ FMU Module

DCD_07.09-27 S01

DCD_07.01-46 S01

E.2.2.8 Analog Input Module

Table E.2-~~9~~8A Analog Input Module

DCD_07.09-27 S01

DCD_07.01-46 S01

E.2.2.9 Analog Output Module

DCD_07.01-46 S01

DCD_07.09-27 S01

Table E.2-~~10~~9A Analog Output Module

E.2.2.10 Digital Input Module

Table E.2-~~11~~10A Digital Input Module

DCD_07.09-27 S01

DCD_07.01-46 S01

Table E.2-10B Digital Input Module

DCD_07.01-46 S01

DCD_07.09-27 S01

E.2.2.11 Digital Output Module

Table E.2-~~12~~11A Digital Output Module

DCD_07.09-27 S01

DCD_07.01-46 S01

E.2.2.12 PIF Module

Table E.2-~~13~~12A PIF Module

DCD_07.09-27 S01

DCD_07.01-46 S01

Table E.2-~~13~~12B PIF Module

DCD_07.09-27 S01

DCD_07.01-46 S01

E.2.2.13 Repeater Module

Table E.2-~~14~~13 Repeater Module

DCD_07.09-27 S01

DCD_07.01-46 S01

E.2.2.14 Power Supply Module

Table E.2-~~15~~14 Power Supply Module

DCD_07.09-27 S01

DCD_07.01-46 S01

E.2.2.15 Controller Cabinet

DCD_07.09-27 S01

DCD_07.01-46 S01

Table E.2-~~16~~15 Controller Cabinet

G.1.2 Design Phase (Position C2.3)

RG 1.152 Position C2.3 “Design Phase” Requirements
The safety system design features for a secure operational environment identified in the system requirements specification should be translated into specific design configuration items in the system design description. Licensees should be aware that digital safety systems will be considered Critical Digital Assets and must adhere to the requirements of 10 CFR 73.54. Regulatory Guide 5.71 describes an acceptable defensive architecture to comply with 10 CFR 73.54. The architecture described in the guidance would have licensees place all digital safety systems in the highest level of their defensive architecture and only permit one-way communication (if any communication is desired) from the digital safety system to other systems in lower levels of the defensive architecture. Licensees should be aware that Section B.1.4 of Appendix B to Regulatory Guide 5.71 notes that one-way communications should be enforced using hardware mechanisms. A licensee’s adherence to the provisions of 10 CFR 73.54 will be evaluated per regulatory programs specific to that regulation. The safety system design configuration items for a secure operational environment intended to ensure reliable system operation should address control over (1) physical and logical access to the system functions, (2) use of safety system services, and (3) data communication with other systems. Design configuration items that incorporate pre-developed software into the safety system should address how this software will not challenge the secure operational environment for the safety system.
Physical and logical access control features should be based on the results of the assessment performed in the concepts phase of the life cycle. The results of this assessment may identify the need for more complex access control measures, such as a combination of knowledge (e.g., password), property (e.g., key and smart card), or personal features (e.g., fingerprints), rather than just a password.
During the design phase, measures should be taken to prevent the introduction of unnecessary design features or functions that may result in the inclusion of unwanted or unnecessary code.
Analysis:

Security-Related Information -Withheld Under 10CFR2.390

DCD_07.09-27 S01

DCD_07.09-27 S01

Security-Related Information -Withheld Under 10CFR2.390

APPENDIX H DESIGN-BASIS COMMUNICATION FAULTS

This appendix describes that the MELTAC platform can be tested to demonstrate that the data communication system can mitigate all identifiable design basis communication faults generated by communications from non-safety systems to safety systems. The design basis communication faults listed in this appendix address all the communication faults described in the ISG-04 Staff Position 1.12.
The term “abnormal conditions” in this appendix indicates the condition which is caused by the design basis communication faults.

Figure H.1 identifies the abnormal conditions (“communication message error” or “network error”), related to the communication from the non-safety system to the safety-related system. In this figure, MELTAC is defined as the operation target controller, the O-VDU is defined as the equipment that should send an operational command to MELTAC, and the other controller is defined as the equipment that should not send an operational command to MELTAC. The “X” marks in the figure indicate the points where abnormal conditions are generated; dotted line balloons indicate the content of abnormal conditions.

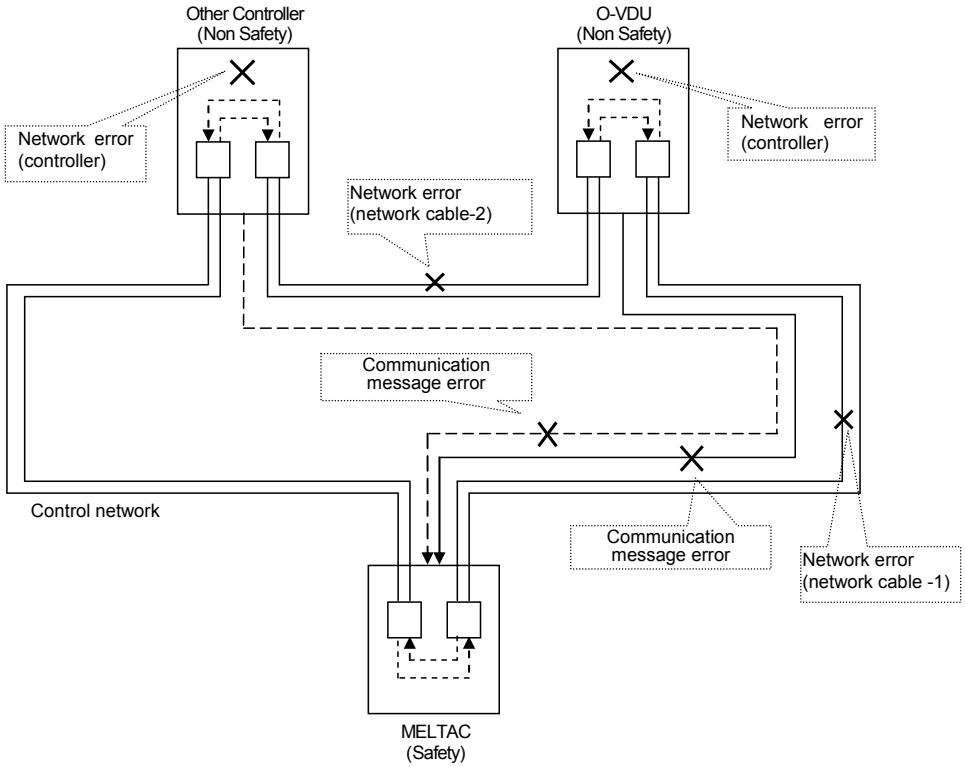


Figure H.1 Configuration on Control Network

The Control Network is redundant and can send data to both clockwise and counter clockwise directions via each controller connected. However, the network cable is physically terminated between adjacent controllers, and each cable is specific to the relevant controllers.
If a cable between controllers (e.g., ~~the~~ network cable-1 in Fig.H.1) is disconnected, this will not affect a cable between other controllers (~~the~~ e.g., network cable-2 in Fig.H.1).

DCD_07.09-27 S01

Figure H.2 shows all possible abnormal condition patterns in the communication from non-safety system to safety-related system, as shown in Figure H.1.

DCD_07.09-27

Figure H.2 Summary of Abnormal ~~Data Transmission~~ Condition Patterns

DCD_07.09-27
DCD_07.09-27 S01

[

.

DCD_07.09-27 S01

DCD_07.09-27
DCD_07.09-27 S01

DCD_07.09-27

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27

DCD_07.09-27 S01

]

DCD_07.09-27

DCD_07.09-27 S01

Table H.1 Detail of Abnormal Condition Patterns Communication ~~Communication Error Patterns Identified~~ (1/~~14~~25)

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

Table H.1 Detail of Abnormal Condition Patterns (2/25)

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

Table H.1 Detail of Abnormal Condition Patterns ~~Communication Error Patterns Identified~~ (~~2~~3/~~14~~25)

Table H.1 Detail of Abnormal Condition Patterns (4/25)

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07 09-27

DCD_07.09-27 S01

Table H.1 Detail of Abnormal Condition Patterns ~~Communication Error Patterns Identified~~ (~~3~~5/~~14~~25)

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07 09-27 S01

DCD_07.09-27

DCD_07.09-27 S01

Table H.1 Detail of Abnormal Condition Patterns ~~Communication Error Patterns Identified~~ (46/~~14~~25)

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

Table H.1 Detail of Abnormal Condition Patterns (7/25)

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

Table H.1 Detail of Abnormal Condition Patterns ~~Communication Error Patterns Identified~~ (~~5~~8/~~14~~25)

Table H.1 Detail of Abnormal Condition Patterns (9/25)

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27

DCD_07.09-27 S01

Table H.1 Detail of Abnormal Condition Patterns ~~Communication Error Patterns Identified~~ (~~6~~10/~~14~~25)

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

Table H.1 Detail of Abnormal Condition Patterns (11/25)

DCD_07.09-27

DCD_07.09-27 S01

Table H.1 Detail of Abnormal Condition Patterns ~~Communication Error Patterns Identified~~ (~~7~~12/~~14~~25)

DCD_07 09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27

DCD_07.09-27 S01

Table H.1 Detail of Abnormal Condition Patterns ~~Communication Error Patterns Identified~~ (~~8~~13/~~14~~25)

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

Table H.1 Detail of Abnormal Condition Patterns (14/25)

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27

DCD_07.09-27 S01

Table H.1 Detail of Abnormal Condition Patterns ~~Communication Error Patterns Identified~~ (~~9~~15/~~14~~25)

DCD_07 09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07 09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

Table H.1 Detail of Abnormal Condition Patterns (16/25)

DCD_07.09-27

DCD_07.09-27 S01

Table H.1 Detail of Abnormal Condition Patterns ~~Communication Error Patterns Identified~~ (~~10~~17/~~14~~25)

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

Table H.1 Detail of Abnormal Condition Patterns (18/25)

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27

DCD_07.09-27 S01

Table H.1 Detail of Abnormal Condition Patterns ~~Communication Error Patterns Identified~~ (~~11~~19/~~14~~25)

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07 09-27 S01

Table H.1 Detail of Abnormal Condition Patterns (20/25)

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27
DCD_07.09-27 S01

Table H.1 Detail of Abnormal Condition Patterns ~~Communication Error Patterns Identified~~ (~~12~~21/~~14~~25)

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27
DCD_07.09-27 S01

Table H.1 Detail of Abnormal Condition Patterns ~~Communication Error Patterns Identified~~ (~~13~~22/~~14~~25)

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

Table H.1 Detail of Abnormal Condition Patterns (23/25)

DCD_07.09-27

DCD_07.09-27 S01

Table H.1 Detail of Abnormal Condition Patterns ~~Communication Error Patterns Identified~~ (~~14~~24/~~14~~25)

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

Table H.1 Detail of Abnormal Condition Patterns (25/25)

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

Table H.2 ISG-04 Staff Position 1.12

DCD_07.09-27

No.	Communication Fault	Description
1	Message corruption	Messages may be corrupted due to errors in communications processors, errors introduced in buffer interfaces, errors introduced in the transmission media, or errors from interference or electrical noise.
2	Repeated messages	Messages may be repeated at an incorrect point in time.
3	Incorrect sequences of messages	Messages may be sent in the incorrect sequence.
4	Message reception failure	Messages may be lost, which includes both failures to receive an uncorrupted message or to acknowledge receipt of a message.
5	Delayed message	Messages may be delayed beyond their permitted arrival time window for several reasons, including errors in the transmission medium, congested transmission lines, interference, or by delay in sending buffered messages.
6	Message from unexpected source	Messages may be inserted into the communication medium from unexpected or unknown sources.
7	Wrong destination message	Messages may be sent to the wrong destination, which could treat the message as valid.
8	Over-length message	Messages may be longer than the receiving buffer, resulting in buffer overflow and memory corruption.
9	Out-of-range message	Messages may contain data that is outside the expected range.
10	Incorrect location of data	Messages may appear valid, but data may be placed in incorrect locations within the message.
11	High rate messages	Messages may occur at a high rate that degrades or causes the system to fail (i.e., broadcast storm).
12	Message header / address corruption	Message headers or addresses may be corrupted.

DCD_07.09-27 S01

[ii] "Processor" may be a CPU or other processing technology such as simple discrete logic, logic within an FPGA, an Application Specific Integrated Circuit (ASIC), etc.

3.1.10. ISG-04 1.10

Requirement
Safety division software should be protected from alteration while the safety division is in operation. On-line changes to safety system software should be prevented by hardwired interlocks or by physical disconnection of maintenance and monitoring equipment. A workstation (e.g. engineer or programmer station) may alter addressable constants, setpoints, parameters, and other settings associated with a safety function only by way of the dual-processor / shared-memory scheme described in this guidance, or when the associated channel is inoperable. Such a workstation should be physically restricted from making changes in more than one division at a time. The restriction should be by means of physical cable disconnect, or by means of keylock switch that either physically opens the data transmission circuit or interrupts the connection by means of hardwired logic. “Hardwired logic” as used here refers to circuitry that physically interrupts the flow of information, such as an electronic AND gate circuit (that does not use software or firmware) with one input controlled by the hardware switch and the other connected to the information source: the information appears at the output of the gate only when the switch is in a position that applies a “TRUE” or “1” at the input to which it is connected. Provisions that rely on software to effect the disconnection are not acceptable. It is noted that software may be used in the safety system or in the workstation to accommodate the effects of the open circuit or for status logging or other purposes.
Analysis

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27S01

DCD_07.09-27S01

3.1.11. ISG-04 1.11

Requirement
Provisions for inter-divisional communication should explicitly preclude the ability to send software instructions to a safety function processor unless all safety functions associated with that processor are either bypassed or otherwise not in service. The progress of a safety function processor through its instruction sequence should not be affected by any message from outside its division. For example, a received message should not be able to direct the processor to execute a subroutine or branch to a new instruction sequence.
Analysis

DCD_07.09-27S01

DCD_07.09-27S01

DCD_07.09-27 S01

DCD_07.09-27 S01

3.1.12. ISG-04 1.12

Refer to Section 3.2.

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27S01

DCD_07.09-27S01

DCD_07.09-27S01

DCD_07.09-27S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

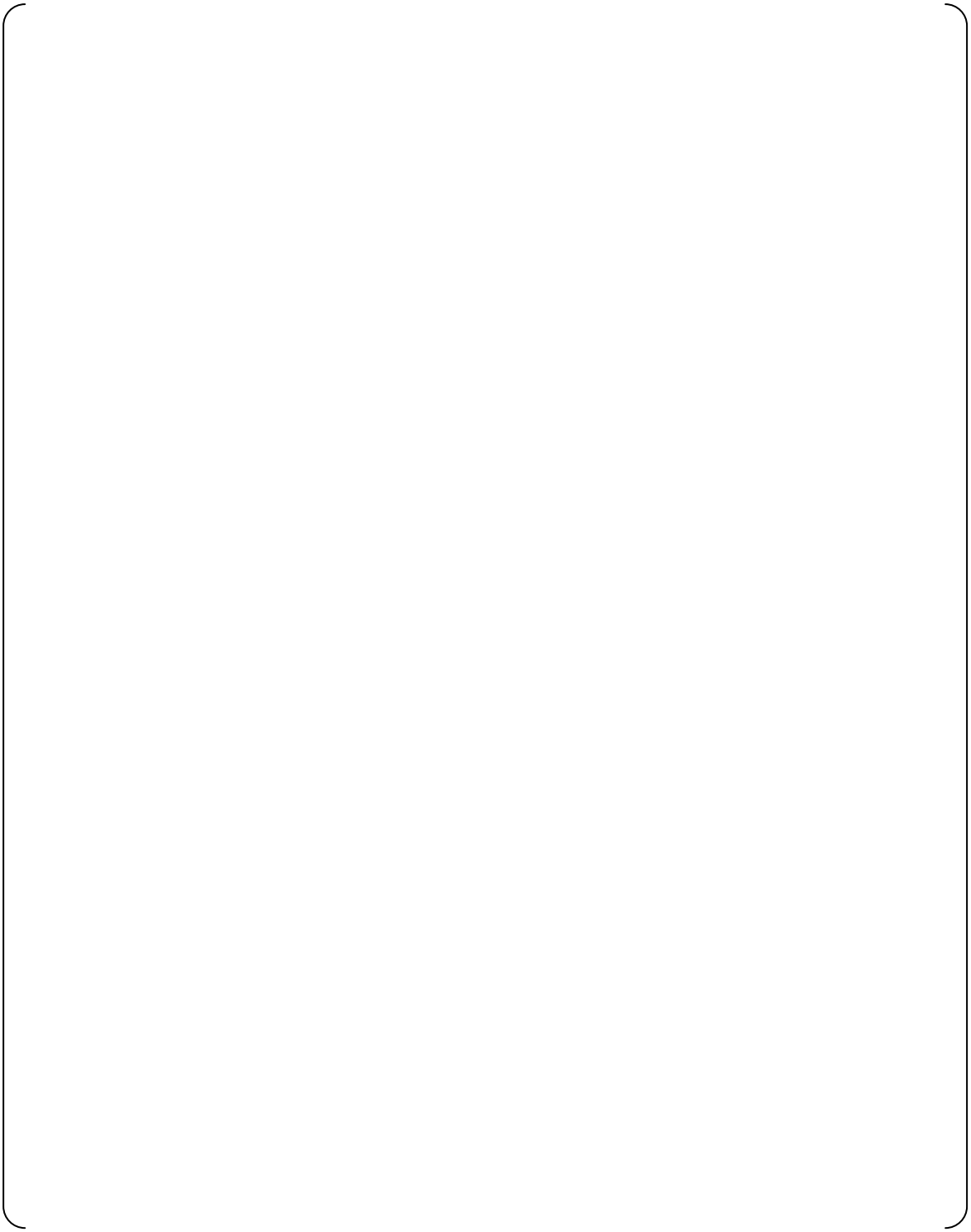
DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27S01

DCD_07.09-27S01

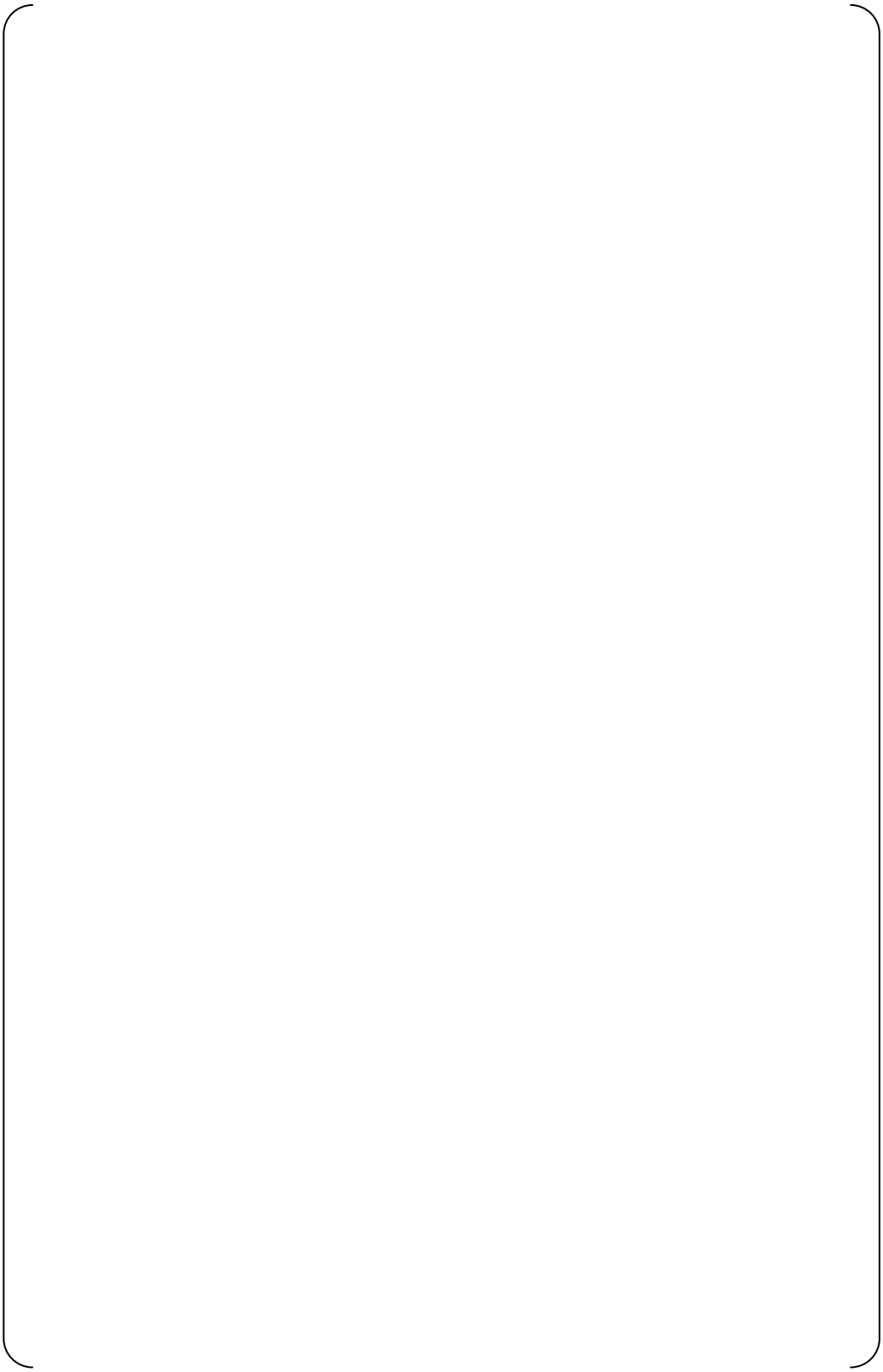
3.5.1. Message Format



DCD_07.09-27S01

DCD_07.09-27S01

Figure 3.5-1 Message Format of Operational Signal (Control Network)



DCD_07.09-27 S01

Figure 3.5-2 Message Format of Process Signal (Control Network)

Table 3.5-4 Message Field Analysis Result of Operational Signal through the Control Network

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

Table 3.5-5 Message Field Analysis Result of Process Signal through the Control Network

DCD_07.09-27 S01

DCD_07.09-27S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

Table 3.5-6 Message Field Analysis Result of Process Signal through the Data Link

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

addition, when the periodic I/O surveillance tests manually confirm the integrity of all digital functions, they also confirms that each controller can correctly execute program memory instructions, including memory instructions that control the self-diagnostic functions. Therefore, the combination of these surveillance tests confirms that the MELTAC self-diagnosis are fully operable.

7.1.3.11 Manual Testing, Bypasses, Overrides and Resets

Manual test features are specifically provided to allow periodic testing of all functions that are not automatically tested through self-diagnosis. This includes primarily sensor calibration, manual initiation functions, memory integrity check, and final actuation of plant components. These manual tests also recheck the portions of the system that are self-tested, and thereby manually confirm the integrity of self-tested components and the integrity of the self diagnostic functions. All manual tests may be conducted on-line without full system actuation and without plant disturbance. The test of output modules for plant components is conducted along with the test of plant components. Since the reliability of the digital I&C equipment is significantly higher than the reliability of the plant components, the periodic test frequency is determined by the reliability of the plant components, not the reliability of the digital I&C equipment. DCD_07.09-27

Safety-related systems may be placed in a bypass operation mode to allow manual testing and maintenance while the plant is on-line. For the RPS measurement channels, automatic bypass management logic prevents multiple bypassed conditions to ensure the minimum redundancy required by the technical specifications is always maintained. For other RPS functions, train level maintenance bypasses are administratively controlled. Maintenance bypasses may be manually initiated from the safety VDU for each respective PSMS train. To manually initiate a maintenance bypass from the operational VDU, the bypass permissive for the train must be enabled. The bypass permissive is part of the PSMS. There is one bypass permissive for each train. Administrative controls ensure the bypass permissive for only one train is enabled at any time. The manual bypass permissive is available from soft switches on the safety VDU.

The power range neutron flux trip function consists of four measurement channels with 2-out-of-4 voting logic. To detect all accident conditions and meet the single failure criterion, one measurement channel must be operable in each of four quadrants as described in Subsection 7.2.1.3. Therefore, the technical specifications require four channels, and the bypass time of one measurement channel is limited.

The outside air intake radiation monitors for the MCR Isolation function and the source and intermediate range neutron flux trip function consists of two measurement channels with 1-out-of-2 voting logic. To meet the single failure criterion, the technical specifications require two channels, and the bypass time of one measurement channel is limited.

The reactor trip on turbine trip function is initiated when all four main turbine stop valves are closed. For reliability, each valve has two position sensors arranged in a 1-out-of-2 configuration. However, this trip is an anticipatory function which is not credited in DCD Chapter 15 accident analysis. Therefore, this trip does not need to meet the single failure criterion. The technical specifications require one channel for each valve, and the bypass time of the one required channel is limited. However, the bypass time of the unrequired channel is unlimited.

The Reliability Analysis method, which demonstrates the need to conduct manual tests of the SLS outputs no more frequently than once per 24 months, is described in Section 6.5. However, this test may be conducted more frequently, if required by the reliability of the plant process components. The test frequency for the plant process components is described in the US-APWR DCD Chapter 16.

This test corresponds to tests of system outputs in conventional plants. For the PSMS, this test is also credited to confirm the program memory processing capability of the SLS and the COM controllers, the PSMS output device (including the priority logic in the Power Interface Module), the interface from the PSMS to the plant components and the plant components themselves. This test overlaps with platform self-diagnostic tests as shown in Figure 4.4-4.

- Memory Integrity Check (MIC)

[ ]

This function is used during periodic surveillance tests to confirm that the software in the controller is the same as the off-line version, and therefore has not changed. This test confirms the functional integrity of PSMS software applications without the need to perform functional logic tests. The ~~Memory Integrity Check (~~MIC~~)~~ also checks the Bus Master Module and the Control Network I/F Module to ensure that there are no frozen data bits within the 2-port memory of these modules (Note). Since most safety functions remain in an unactuated state during normal plant conditions, this periodic test ensures that trip/actuation commands can be correctly communicated between PSMS controllers when the safety functions are demanded. The ~~Memory Integrity Check (~~MIC~~)~~ is conducted with the train for the controller to be tested in a bypass condition. Administrative controls assure the remaining three trains are still in service. This ensures that performance of the MIC will not result in a loss of safety function of PSMS. DCD_07.09-27S01 DCD_07.09-27

Note: Memory bit data is valid (i.e.,~~:~~ can indicate correct “0” or “1” value), but frozen (i.e.,~~:~~ bit data does not change according to input data, such as trip or actuation request). DCD_07.09-27S01 DCD_07.09-27

As described in the MELTAC Technical Report, MUAP-07005, Section 4.1.7.2, software design of the MIC function will be performed under an approved Appendix B program. This assures that the software quality of the MIC function is equivalent to that of a safety system. Therefore, the design for surveillance testing complies with the guidance of BTP 7-17.

The following features minimize the potential for unexpected software change errors that could result in total PSMS failure between test intervals: (1) Access Control: the PSMS software is physically secured, as described in Section 7.9.2.5 of the DCD, and (2) Software Configuration Management: the PSMS software is maintained in accordance with Section 3.11 of “US-APWR Software Program Manual” (MUAP-07017).

[ ]

DCD_07.
09-27

DCD_07.
09-27

]

4.1.5.2.3 Control Network I/F Module

[

DCD_07.
09-27 S01

DCD_07.
01-46 S01

DCD_07.
01-46 S01

DCD_07.
09-27

DCD_07.
09-27

]

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 Sections 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.

DCD_07.
09-27

]

4.1.5.5.2 Output Module

[

DCD_07.
01-46 S01

DCD_07.
01-46

DCD_07.
01-46 S01

DCD_07.
01-46 S01

DCD_07.
01-46

DCD_07.
01-46 S01

DCD_07.
01-46 S01

DCD_07.
09-27

]

4.1.5.5.3 Controller Cabinet

[

]

4.1.5.6 Operations When the Hardware and Software Do Not Match

Mismatch of the module configuration in the CPU chassis:
The CPU Module detects the error and the subsystem turns to Failure mode.

Mismatch of the module configuration in the I/O chassis:
The CPU Module detects the mismatch and notifies the application software logic that the I/O signals have bad quality, as explained in Section 4.1.5.

4.1.7.2 Software Memory Integrity

DCD_07.09-27
DCD_07 09-27 S01

The Memory Integrity Check (MIC) is a function which confirms the integrity of the memory of MELTAC in the periodic test, which is categorized into the following:

1) RAM memory check
2) Software data integrity check
3) Bit-by-bit memory check by MELTAC engineering tool

The details of these three checks are described below.

[

]

DCD_07.09-27

3) Bit-by-bit memory check by MELTAC engineering tool
A function for confirming that the software in the memory and a controlled copy of the software stored off-line in the MELTAC engineering tool are the same through a bit-by-bit check, as a CPU module-specific function. Details are described below, with a comparison with the Self-diagnosis Memory Check.

The MELTAC engineering tool includes a manually initiated Memory Integrity Check (MIC) function which compares the software memory in the controller, bit by bit, with a controlled copy of the software stored off-line.
This function is used during the Software Memory Integrity Test to provide confirmation that the software in the controller is the same as the off-line version, and therefore, has not changed or failed. This test confirms the functional integrity of both the basic software and application software residing in the controller. The Software Memory Integrity Test is conducted periodically for every controller in the system.

By confirming the basic software, the Software Memory Integrity Test confirms the CPU instructions stored in F-ROM for all MELTAC functions described throughout this document, including the self-diagnostic functions. By confirming the application software, the Software Memory Integrity Test also confirms the CPU instructions stored in F-ROM for all functional

Interface from the non-safety unit bus to the COM-2 uses optical fiber to achieve electrical independence of the COM-2 from the non-safety systems. Data communication from the non-safety unit bus has its own independent communication buffer (2-port memory) in the COM-2. Only discrete (manual control signals from the operational VDU) information is transmitted across train boundaries in fixed format, fixed length and pre-defined message. The message size of the operational VDU commands is determined as a fixed value based on the maximum number of operational VDU commands. The maximum number of operational VDU commands of the US-APWR is eight (8). Although the number of effective operational VDU commands per one message is dependent on the number of manual actions taken by the operator at the operational VDU, the message size is fixed at the eight (8) manual commands regardless of the number of effective operational VDU commands. DCD_07.09-27 S01

All communication and safety functions of the COM-2 are executed from non-volatile read only memory (F-ROM or UV-ROM) and FPGA of each COM-2. The F-ROM, UV-ROM and FPGA can only be changed by physical withdrawal of the module on which the memory resides from the COM-2 cabinet. Therefore any communication signals from the non-safety unit bus cannot change the safety functions of the COM-2 or the functions that ensure communication independence.

Only possible failed signal from the outside of each train COM-2 is erroneous manual component controls signal (stop/start, open /close, bypass, lock or reset), but the priority logics in the PSMS can protect its own safety functions from this type erroneous signal as shown in Subsection 7.1.4.2.2.4 of the Functional Independence.

Based on the communication independence design described above, any failures in the unit bus or a node on the unit bus that result in malformed, incorrect or inappropriate data messages cannot adversely affect the operation of the safety function within each separate COM-2 train. This preserves communication independence between trains in accordance with the Independence Criterion (IEEE Std 603-1991, Clause 5.6).

(4) Interdivisional communication between the safety VDU trains

The only allowed interdivisional communications between the safety VDUs are limited from the safety VDU (singledivisional safety VDU) to the multidivisional safety VDUs. The safety VDUs only transmit information signals (process measurement channels and component status) by this communication that are needed to support monitoring functions of the operators to perform accident mitigation and safe shut down operation to the multidivisional safety VDU.

Interdivisional communications from the safety VDU processor to the multidivisional safety VDU processors are one way (receive only) point-to-point data link communication via the safety-related Bus Master Module in each safety VDU. The data is broadcasted from the Bus Master Module in the sending safety VDU processor to the separate Bus Master Modules in each of the two receiving multidivisional safety VDU processor trains. The hardware and software for this interdivisional communication are the same as the interdivisional communication between the RPS trains and from the RPS to the ESFAS.

Within each multidivisional safety VDU processor, communication independence is achieved by communication controllers (one per data link) in the Bus Master Module that are separate from functional processors in the CPU Module in the multidivisional safety

DCD_07
.09-27
S01

ACRONYMS AND ABBREVIATIONS (CONTINUED)

LOCA	loss-of-coolant accident	
LOOP	loss of offsite power	
MCR	main control room	
~~MELCO~~	~~Mitsubishi Electric Corporation~~	DCD_07.01-45
MELTAC	Mitsubishi Electric Total Advanced Controller	
MFW	main feedwater	
M/G	motor generator	
MHI	Mitsubishi Heavy Industries, Ltd.	
MOV	motor operated valve	
MR	Mitsubishi real-time	DCD_07.09-27 S01
MSLB	main steam line break	
MSS	main steam supply system	
MTCV	main turbine control valve	MIC-04-07-00001
NEI	Nuclear Energy Institute	
NIS	nuclear instrumentation system	
NRC	U.S. Nuclear Regulatory Commission	
NUREG	NRC Technical Report Designation (Nuclear Regulatory Commission)	
OC	operator console	
OEM	original equipment manufacturer	
OPC	overspeed protection controller	MIC-04-07-00001
OS	operating system	
O-VDU	operational VDU	
PA	postulated accident	
PAM	post accident monitoring	
PCMS	plant control and monitoring system	
PIF	power interface	
POL	problem oriented language	
PRA	probabilistic risk assessment	
PSMS	protection and safety monitoring system	
PSS	process and post-accident sampling system	
QA	quality assurance	
QAP	quality assurance program	
RCP	reactor coolant pump	
RCS	reactor coolant system	
RFI	radio frequency interference	
RG	Regulatory Guide	
RHR	residual heat removal	
RHRS	residual heat removal system	

- Consists of MELTAC platform and MR computer platform DCD_07.09-27 S01
- Duplex redundant digital architecture for each control and process monitoring subsystem
- Analog DAS

D. Data communication

- Fully multiplexed, including safety-related signals.
- Multi-drop data bus and serial data link.
- Fiber optics communication networks.

The overall I&C system consists of the safety-related protection and safety monitoring system (PSMS) with the safety-related portion of the HSIS, the non-safety plant control and monitoring system (PCMS), the non-safety DAS, and the non-safety portion of the HSIS. The HSIS consists of safety-related safety VDUs, post accident monitoring (PAM), non-safety operational VDUs, and non-safety LDP for normal plant operation. The VDU consists of VDU processors and VDU panels. The safety VDU panels and operational VDU panels are located on both the operator console (OC) in the main control room (MCR) and the remote shutdown console (RSC) in the remote shutdown room (RSR). Operational VDU panels are also provided for information only (i.e., no control capability) at the technical support center (TSC). Information to support emergency response operations (the same as provided on operational VDU panels) is provided at the emergency operations facility (EOF).

The description and/or details described in this section are based on the following Mitsubishi Heavy Industries, Ltd. (MHI) Topical and Technical Reports. If there are any inconsistencies between the Topical and Technical Reports and this chapter, the Design Control Document (DCD) has precedence.

- Safety I&C System Description and Design Process, MUAP-07004 (Reference 7.1-2)
- Safety System Digital Platform -MELTAC-, MUAP-07005 (Reference 7.1-3)
- Defense-in-Depth and Diversity, MUAP-07006 (Reference 7.1-4)
- HSI System Description and HFE Process, MUAP-07007 (Reference 7.1-5)

All nuclear steam supply systems and other I&C systems are designed and manufactured by MHI.

The I&C systems for the US-APWR are essentially the same as the I&C systems for new plants in Japan, including the Japanese advanced pressurized water reactor (APWR), and systems currently installed and being implemented for plant modernization in Japan. The I&C systems for the US-APWR are the same as the systems described in the Topical and Technical Reports, referenced above.

DCD_07.09-27 S01

Table 7.1-5 Scope of the Augmented Quality Systems

Items	Specific requirements for non-safety system	Augmented Quality	Applicable Platform
Safety Functions Controlled by O-VDUs	DI&C-ISG-04	Required	MR computer platform
Safety Parameter Display System (SPDS)	10 CFR 50.34 (f)(2)(iv), "Additional TMI-Related Requirements" regarding the SPDS Control	Required	MR computer platform
	NUREG 0737 Supplement 1, "Clarification of TMI Action Plan Requirements - Requirements for Emergency Response Capability", with respect to SPDS	Required	
Alarms for Credited Manual Operator Actions	SECY-93-087, Item II. T, "Control Room Annunciator (Alarm) Reliability"	Required	MR computer platform
Signal Selection Algorithm (SSA)	RG 1.153, "Criteria for Safety Systems"	Required	Non-safety MELTAC platform
	IEEE 603-1991, Clause 6.3 "Interaction between the Sense and Command features and other Systems"	Required	
Risk-significant non-safety I&C system	Risk-significant non-safety I&C system identified in Table 17.4-1	Required	Non-safety MELTAC platform
Diverse Instrumentation and Control System	BTP 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems"	Required	Analog hardwired circuits
	Generic Letter 85-06, "Quality Assurance Guidance for ATWS Equipment That Is Not Safety-Related"	Required	

Note)

1. Bypass and Inoperable Indication (BISI): There is no augmented quality requirement.
2. Post Accident Monitoring Instrumentation: Type A, B, C and D are implemented in the PSMS and there is no augmented requirement for Type E.
3. Leak Detection System: Seismic required systems are implemented in the PSMS and there is no augmented requirement for others.

DCD_07.09-27 S01

DCD_07.09-27 S01

7.7.2.2 Effects of Control System Operation on Accidents

For the transient response of the plant systems for AOOs and PAs, the safety analysis takes no credit for normal PCMS control actions that would lessen the effects of the event (e.g., reduction of feedwater by the SG water level control system during a SG tube rupture event). In addition, the safety analysis assumes normal control actions, that would aggravate the affects of the event and are not blocked by safety functions, will occur (e.g., increase of charging flow by the pressurizer water level control system during a SG tube rupture event).

7.7.2.3 Effects of Control System Failures

The Chapter 15 analysis of AOOs bounds all single random failures within the PCMS. This includes single failures that result in:

- A fail as-is, fail de-energized or spurious actuation of a single PCMS hardware component (e.g., input module, or output module).
- A fail as-is or fail de-energized condition of an entire PCMS control group; the control function to control group assignment are shown in Table 7.7-2.
- Spurious actuation of a single or multiple control functions (e.g., reactivity control, pressurizer control, or SG water level control) within a control group, resulting from a single software block failure.
- A spurious single command from an operational VDU.
- Stuck or dropped control rod
- Stuck control rod bank or overlap sequence error
- Spurious actuation of a normal rod motion command (spurious motion of any single bank)
- Spurious motion of multiple control banks in the predetermined overlap sequence.

The Chapter 15 analysis of AOOs credits the effects of interlocks in PCMS control groups not affected by the failure, which limit the effects of a failed PCMS control group or control function.

The following types of failures are not considered credible, since they require a series of specific successive failures in multiple software blocks:

- Multiple spurious commands from an operational VDU. Since multiple spurious commands from an operational VDU are not credible, they are not considered in the analysis of bounding AOOs. However, multiple spurious commands from an operational VDU are analyzed for their effect on the safety functions, in MUAP-07004 Appendix D and for the effect on the DCD Chapter 15 accident analysis in MUAP-07004 Appendix J. The list of manual command signals from operational VDU to PSMS is shown in Table 7.7-6. DCD_07.09-27 S01

DCD_07.09-27 S01

Table 7.7-6 Manual Command Signals from O-VDU to PSMS

Manual Command Signal	Description of Manual Command	Command Type	Permissive from S-VDU	Received System (Safety-Related System)
Bypass and Reset	Bypass command for operating bypass	Operating Bypass	Required	RPS-A/B/C/D (via COM)
Bypass and Reset	Bypass command for maintenance bypass	Maintenance Bypass	Required	RPS-A/B/C/D (via COM)
Exclusion and Reset	Command to exclude failed sensors for the average calculation of core exit temperature	Maintenance Bypass	Required	RPS-A/D (via COM)
Block and Reset	Command to block shunt trip function of the reactor trip breaker	Maintenance Bypass	Required	RPS-A/B/C/D (via COM)
Interlock Bypass	Command to bypass safety-related signal for component level control	Maintenance Bypass	Required	SLS-A/D (via COM)
Stop Lock	Lock command for pump	Lock	Required	SLS-A/B/C/D (via COM)
OFF Lock	Lock command for heater/breaker	Lock	Required	SLS-A/B/C/D (via COM)
Lock	Lock command for valve	Lock	Required	SLS-A/B/C/D (via COM)
Reset (Block)	Reset (block) command of reactor trip or ESF actuation	Reset	Required	RPS/ESFAS-A/B/C/D (via COM)
Maintenance Trip	Command to set bistable with partial trip state	Operation	Not Required	RPS-A/B/C/D (via COM)
Reactor trip or ESF actuation	Command to initiate reactor trip or ESF actuation	Operation	Not Required	RPS/ESFAS-A/B/C/D (via COM)
Start, Stop	Operation command for pump	Operation	Not Required	SLS-A/B/C/D (via COM)
ON, OFF	Operation command for heater/breaker	Operation	Not Required	SLS-A/B/C/D (via COM)
Open (Open Permission), Close	Operation command for valve	Operation	Not Required	SLS-A/B/C/D (via COM)
Auto	Operation command to enable automatic signals	Operation	Not Required	SLS-A/B/C/D (via COM)
Mode Select	Operation command to transfer control mode	Operation	Not Required	SLS-A/B/C/D (via COM)

5.1.13 Priority Logic

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

5.1.14 Bypass, Lock and Reset Operation from O-VDU

DCD_07.09-27 S01

DCD_07.
09-27
S01

DCD_07.09-27 S01

Table 5.1-1 General Characteristics of Permissive from S-VDU

DCD_07.09-27 S01

Table 5.1-2 General Characteristics of Bypass/Lock/Reset from O-VDU

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

Figure 5.1-3 Priority Between Commands from Safety VDU and Operational VDU

DCD_07.09-27 S01

DCD_07.09-27 S01

Figure 5.1-4 Priority for Manual and Automatic Signals of Safety and Non-Safety Demand

DCD_07.09-27 S01

Figure 5.1-6 ~~Manual Permissive Logic~~Priority for Operating Bypass Signal~~s~~ from Operational VDU

DCD_07.09-27 S01

Figure 5.1-7 Priority for Maintenace Bypass Signal from Operational VDU

DCD_07.09-27 S01

Figure 5.1-8 Priority for Reset Signal from Operational VDU

Appendix I Reduction of Response Time and Operator's Workload by Utilizing Integrated Operational VDU (O-VDU)

I.1 Reduction of Response Time

DCD_07.09-27 S01

DCD_07.09-27 S01

DCD_07.09-27 S01

I.2 Reduction of Operator's Workload and Potential Human Error

DCD_07.09-27 S01

DCD_07.09-27 S01

Figure I-1 Example of Screen Display Format for Operating Bypass

DCD_07.09-27 S01

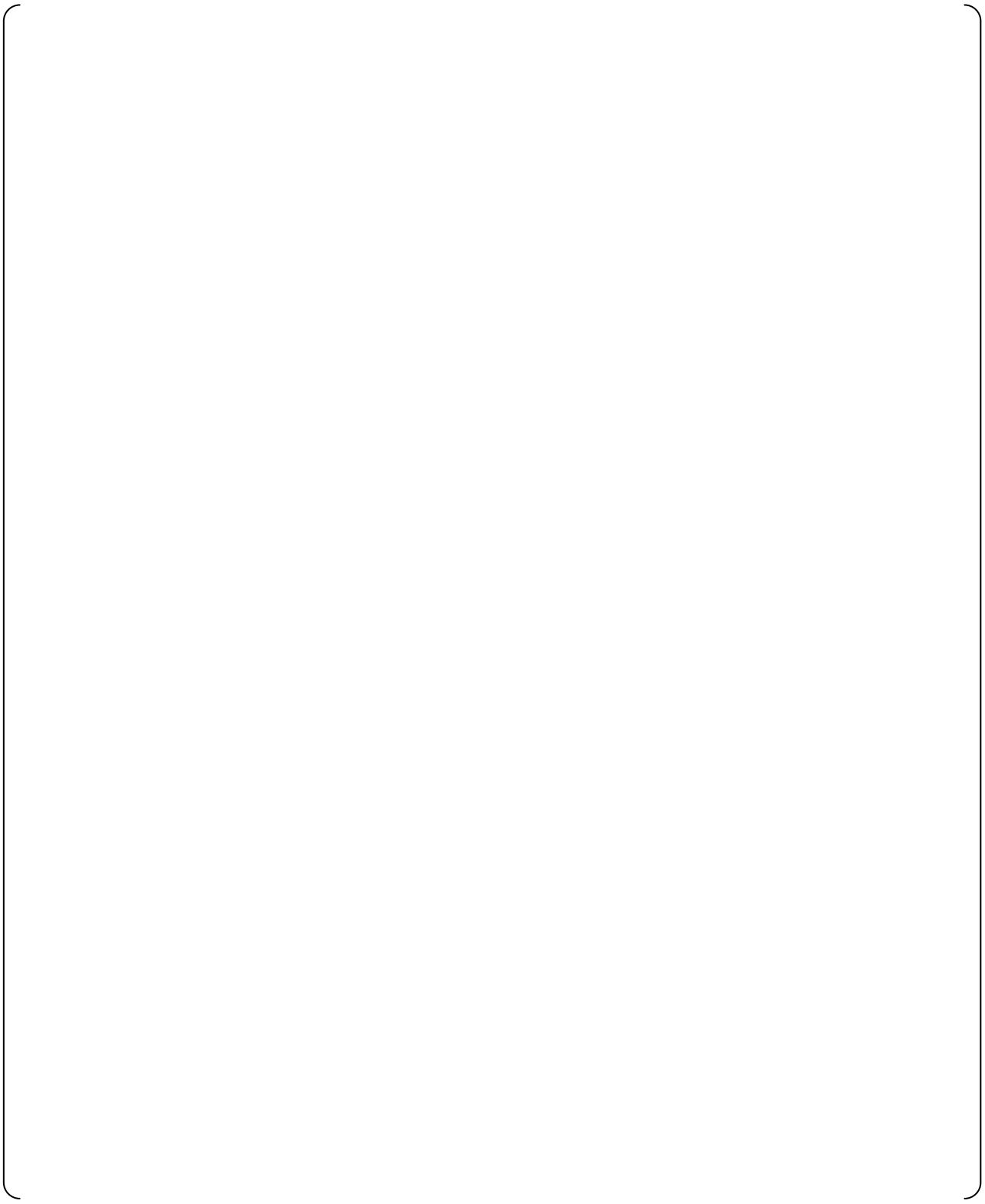


Figure I-2 Example of Operational VDU Display for CET Bypass Operation

DCD_07.09-27 S01

Figure I-3 Example of Operational VDU Display for Lock Operation

DCD_07.09-27 S01

DCD_07
.09-27
S01

DCD_07
.09-27
S01

DCD_07
.09-27
S01

DCD_07
.09-27
S01

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. 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. MIC-04-07-00001

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. Components' safe states in the state-based priority logic are shown in Table 7.8-11. MIC-04-07-00001

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~~circuits 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. DCD_07.09-27 S01

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 MIC-04-07-00001

7.8.1.2.3 ECCS Actuation

ECCS is automatically actuated on a low - low pressurizer pressure signal. 2-out-of-4 voting logic is utilized for the four pressurizer pressure low- low signals.

The interface and configuration of the pressurizer pressure signals is as described above.

Diversity from the ECCS actuation function in the PSMS is maintained from sensor input up to the power interface module. This automatic DAS ECCS function is automatically blocked when status signals are received indicating that the PSMS ECCS function has actuated correctly. Correct actuation is indicated when 2-out-of-4 status signals are received from auxiliary contacts on the motor starters controlling the Safety Injection (SI) pumps, as shown in Figure 7.8-4. The time delay of ECCS actuation by the PSMS is assumed to be 113 sec (without offsite power). Table 7.8-9 shows the breakdown of the delay time. If the SI pumps fail to start from PSMS within 120 sec allowing for 7.0 sec margin toward the above 113 sec delay time, DAS starts to actuate the SI pumps as a CCF that disables functions of the PSMS could occur. In the D3 analysis, 3 sec of response time of DAS and 5 sec of SI pump time to full flow are allowed as time margin and SI pumps are assumed to be started from DAS within 128 sec. The SI pump status signals are interfaced from the PSMS, prior to any software processing, to each DAAC, as shown in Figure 7.8-1.

7.8.2 Design Basis Information

7.8.2.1 Single Failure

Since the DAS is a non-safety system, it does not need to meet the single failure criterion for actuation. The DAS subsystems are arranged in a 2-out-of-2 configuration after taking 1-out-of-2 voting logic twice to ensure that the DAS can sustain one random component failure without spurious actuation of either manual or automatic functions. Spurious actuation of single components due to single failures in SLS power interface modules has been considered in the plant safety analysis.

The four DAAC subsystems actuate all required plant components to achieve the required safety function. The number of actuated plant components does not consider additional single failures. For example, for containment isolation valves, only one of the two valves is actuated. This non-redundant configuration is considered in determining the allowable out of service time for plant equipment in the technical specifications. However, the out-of-service condition is considered for the numbers of safety injection pumps and EFW pumps. In addition, unavailable of main steam depressurization valve of the impaired SG line is considered. The DAS actuates all four of these pumps and valves for operability while three is minimum required. The number of actuated components for each DAS function is shown in Table 7.8-5.

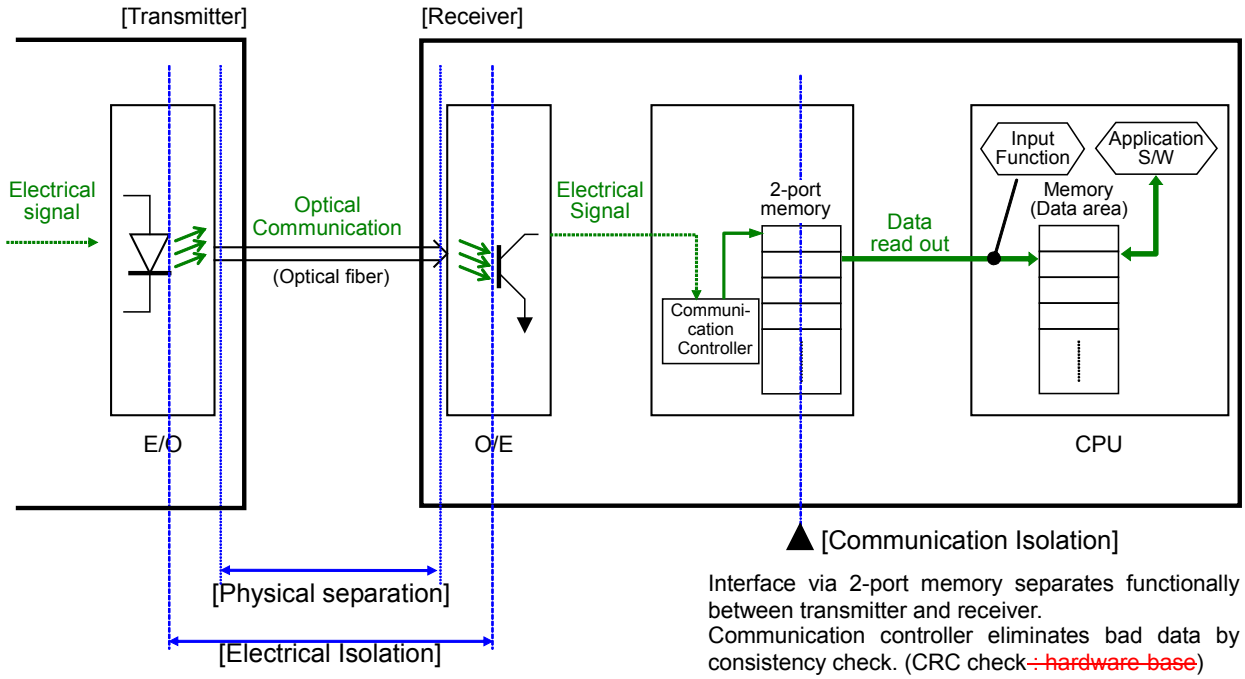
7.8.2.2 Diversity to Digital Safety and Non-Safety Systems

The DAS utilizes conventional ~~hardware~~hardwired circuits (analog circuits, solid-state logic processing, relay circuits). Therefore, a software CCF in the digital safety-related and non-safety systems (PSMS and PCMS), would not affect the DAS. In addition, the DAS hardware for anticipated transient without scram (ATWS) mitigation functions - DCD_07.09-27 S01

Table 7.8-7 Supplemental Information to MUAP-07006-P-A (Sheet 1 of 6)

No.	Items to be clarified	Corresponding Section of SER for MUAP-07006-A	Resolution	Reference Document and Section
1	The US-APWR design certification applicant shall demonstrate that the isolation devices are conventional (e.g., non software based devices) and completely testable in order to meet the independence and isolation requirements of IEEE Std and address fault-isolation criteria of IEEE-384.	3.1, 3.4	The isolation devices are conventional non software based devices, qualified by test to meet the independence and fault-isolation criteria of IEEE-384. Isolation devices are standard MELTAC platform components, described in MUAP-07005 Subsection 4.1.2.3. PSMS analog output isolation devices are functionally tested during the manual calibration described in Subsection 4.4.2 of MUAP-07004. The DAS test method described in Subsection 4.2.6 of MUAP-07004 includes functional testing of PSMS analog output isolation devices and binary input isolation devices.	Subsection 4.1.2.3 of MUAP-07005 Subsection 4.2.6 of MUAP-07004.
2	The US-APWR design certification applicant shall demonstrate the acceptability of all manual actions. Also, the concept and application-specific implementation of the priority alarms should be adequately demonstrated.	3.1.3	The acceptability of all manual actions and prompting alarms is demonstrated through analysis and preliminary verification, as documented in MUAP-07014; US-APWR D3 coping analysis. These manual actions and prompting alarms are completely verified and validated using a fully integrated full scope dynamic plant simulator, within the HFE V&V program element. The design process for the HFE V&V program element is described in Section 18.10 of the DCD and Section 5.10 of MUAP-07007(Reference 7.8-8). Completion of the HFE V&V program element is defined in Section 2.9 of DCD Tier 1.	MUAP-07014 Subsection 4.11.4 of DCD Ch.18 Section 18.10 and Section 5.10 of MUAP-07007 Section 2.9 of DCD Tier 1
3	The US-APWR design certification applicant shall demonstrate that the PIF module is not susceptible to a software CCF.	3.2.1, 3.2.2	The interposing logic part and output part of the PIF module, which are commonly used by the PSMS and DAS, utilize only conventional solid-state ~~hardware~~hardwired components, as described in Subsection 4.1.2.4 of MUAP-07005. Therefore, these portions of the PIF module are not susceptible to a software CCF.	Subsection 4.1.2.4 of MUAP-07005

DCD_07.09-27 S01



DCD_07.09-27 S01

Figure 4.2-2 Electrical Independence Features between PCMS and PSMS

5.1.5 Common Cause Failure Modes for Defense-in-Depth and Diversity Analysis

BTP 7-19 requires consideration of CCFs that "disable" the protection system. Based on this, the coping analysis described in the Defense-in-Depth and Diversity Topical Report, MUAP-07006 considers CCFs that result in a fail as-is condition in the PSMS and PCMS. The coping analysis does not consider CCFs that result in output state changes (i.e., spurious actuation to de-energized or energized state).

5.1.6 This section intentionally left blank

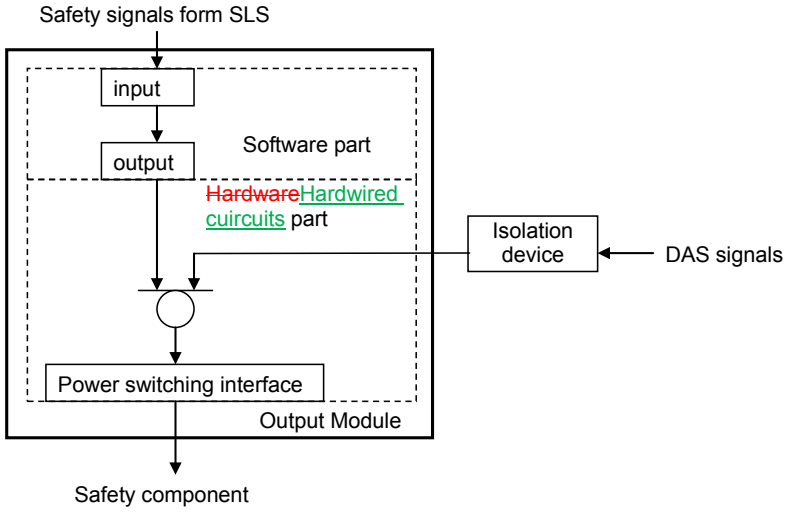
5.1.7 Output Module for PSMS and DAS

Output Modules in the PSMS interface control signals to the plant components. These same output modules are used to interface control signals from the DAS. A common Output Module provides one power interface conversion device for control of one plant component. This reduces the maintenance that would be required for two separate devices and it reduces the complexity of combining the PSMS and DAS signals via relay logic. Reduced complexity results in improved reliability.

Control signals are interfaced from the PSMS controllers to the software part of the Output Module via the controller's I/O bus. Control signals from the DAS are interfaced via conventional hardwired connections and conventional isolation modules (for the PSMS only) to the ~~hardware~~hardwired circuits part of the Output Module. The isolation modules are part of the PSMS (i.e., they are Class 1E devices). Therefore DAS output signals interface to plant components via only the ~~hardware~~hardwired circuits part of the Output Module, so CCF within the PSMS or PCMS digital platform will not affect DAS signals.
Figure 5.1-1 shows the signal interface between output module and PSMS and DAS.

DCD_07.09-27 S01

DCD_07.09-27 S01



DCD_07.09-27 S01

Figure 5.1-1 Signal Interface of Output Module

DCD_07.09-27 S01

DCD_07.09-27 S01

5.1.14 Bypass, Lock and Reset Operation from O-VDU

DCD_07.09-27 S01

7.7.2.2 Effects of Control System Operation on Accidents

For the transient response of the plant systems for AOOs and PAs, the safety analysis takes no credit for normal PCMS control actions that would lessen the effects of the event (e.g., reduction of feedwater by the SG water level control system during a SG tube rupture event). In addition, the safety analysis assumes normal control actions, that would aggravate the affects of the event and are not blocked by safety functions, will occur (e.g., increase of charging flow by the pressurizer water level control system during a SG tube rupture event).

7.7.2.3 Effects of Control System Failures

The Chapter 15 analysis of AOOs bounds all single random failures within the PCMS. This includes single failures that result in:

- A fail as-is, fail de-energized or spurious actuation of a single PCMS hardware component (e.g., input module, or output module).
- A fail as-is or fail de-energized condition of an entire PCMS control group; the control function to control group assignment are shown in Table 7.7-2.
- Spurious actuation of a single or multiple control functions (e.g., reactivity control, pressurizer control, or SG water level control) within a control group, resulting from a single software block failure.
- A spurious single command from an operational VDU.
- Stuck or dropped control rod
- Stuck control rod bank or overlap sequence error
- Spurious actuation of a normal rod motion command (spurious motion of any single bank)
- Spurious motion of multiple control banks in the predetermined overlap sequence.

The Chapter 15 analysis of AOOs credits the effects of interlocks in PCMS control groups not affected by the failure, which limit the effects of a failed PCMS control group or control function.

The following types of failures are not considered credible, since they require a series of specific successive failures in multiple software blocks:

- Multiple spurious commands from an operational VDU. Since multiple spurious commands from an operational VDU are not credible, they are not considered in the analysis of bounding AOOs. However, multiple spurious commands from an operational VDU are analyzed for their effect on the safety functions, in MUAP-07004 Appendix D and for the effect on the DCD Chapter 15 accident analysis in MUAP-07004 Appendix J. The list of manual command signals from operational VDU to PSMS is shown in Table 7.7-6. DCD_07.09-27 S01

controller. The PSMS basic software is changeable only by removing and replacing the memory device that contains the software. The PSMS application software is changeable only by removing the controller's CPU module from its chassis and placing it in a dedicated re-programming chassis.

- Acceptable safety function performance
  Normally, manual controls from the safety VDU and manual controls from the non-safety operational VDUs of the PCMS have equal priority (last-in/last-out). However, manual controls from the safety VDU can have priority over any non-safety controls from the PCMS, as follows.

- Failures of non-safety systems are bounded by the safety analysis
  Any plant condition created by the worst case erroneous/spurious non-safety data set (e.g., non-safety failure commanding spurious opening of a safety relief valve) is bounded by the plant safety analysis.

DCD_07.09-27 S01

DCD_07.09-27 S01

g. Failures of Non-Safety Systems are Bounded by the Safety Analysis

Any plant condition created by the worst case erroneous/spurious non-safety data set (e.g., non-safety failure commanding spurious opening of a safety relief valve) is bounded by the plant safety analysis. This analysis is based on spurious communication of a single data set (i.e., one erroneous control command) because spurious communication of multiple erroneous control commands caused by a single hardware or software block failure is not considered credible. The basis for this credible failure mode is described in Appendix C. DCD_07.09-27 S01

Multiple spurious commands from the operational VDU which may be caused by software common cause failures (CCFs) are analyzed for the effect on the safety functions in Appendix D and for the effect on the safety functions in Appendix D and for the effect on the DCD Chapter 15 accident analysis in Appendix J. DCD_07.09-27 S01

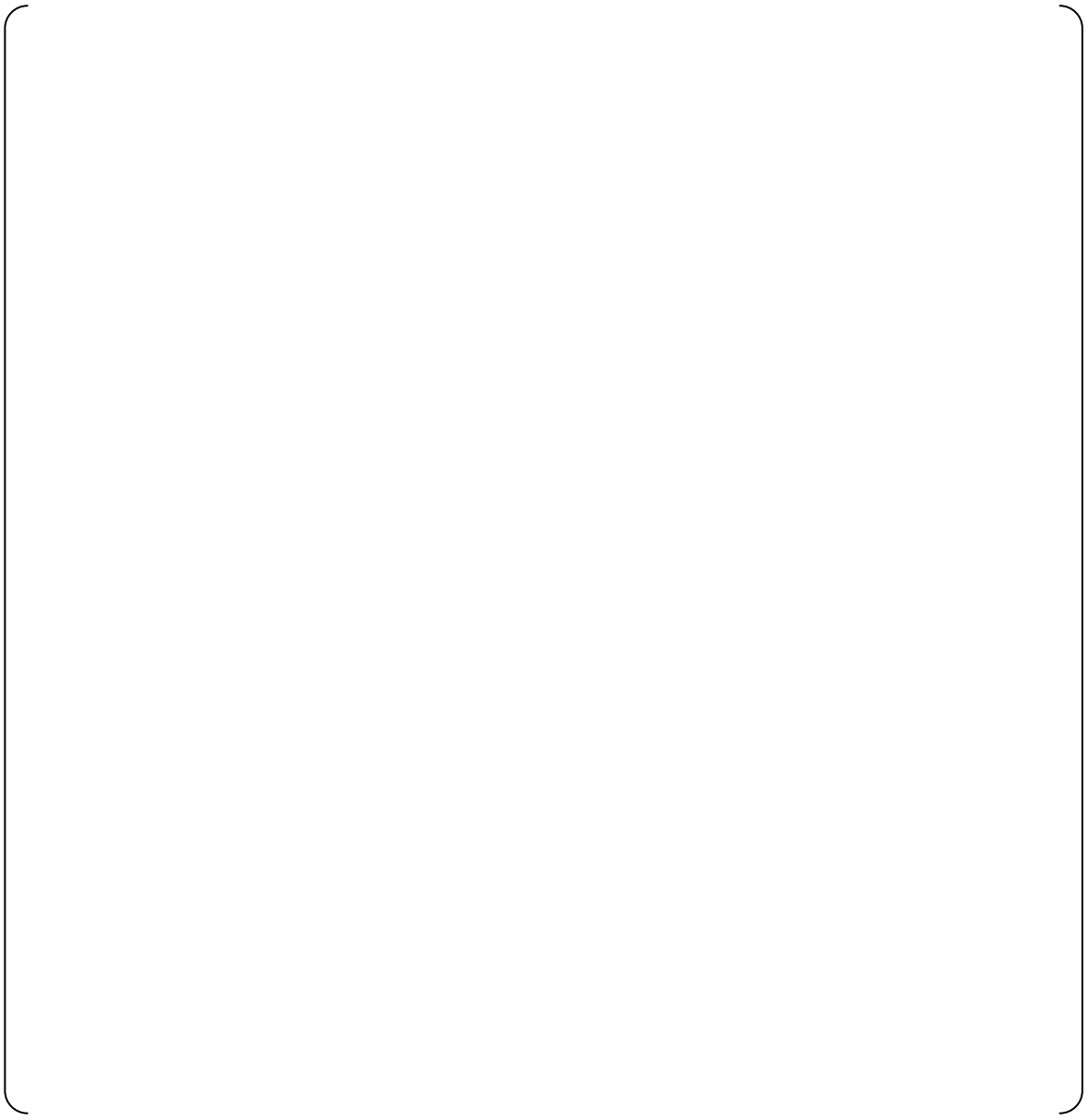


Figure B.5.6-1 Software Isolation (Non-Safety VDU / Safety-Related System)

Appendix C Prevention of Multiple Spurious Commands and Probability Assessment

C.1. Prevention of Multiple Spurious Commands

DCD_07
.09-27
S01

DCD_07
.09-27
S01

DCD_07
.09-27
S01

DCD_07
.09-27
S01

DCD_07
.09-27
S01

DCD_07
.09-27
S01

DCD_07
.09-27
S01

(PSMS). The reasons to select the unit bus communication from the PCMS to the PSMS are as follows;

- The unit bus communication from the PCMS to the PSMS enhances the performance of the safety functions of the PSMS as described below.
- The unit bus communication conforms to IEEE Std 603-1991 (Reference 7.9-9) and other related regulatory requirements as described in Subsections 7.1.4, Subsection 7.9.2.7 and the Safety I&C Technical Report (Reference 7.9-2).
- The unit bus communication conforms to the all ISG-04 requirements (Reference 7.9-17) as described in Appendix E of the Safety I&C Technical Report (Reference 7.9-2).
- The reliability of the unit bus communication is higher than a conventional hardwired interface because it has fewer hardware interface devices and it has a redundant architecture. The continuous self-diagnostic functions of the unit bus communication ensure there are no undetected latent failures, as there can be in the hardware interfaces.
- Based on higher reliability, immediate failure detection and short repair time, the availability of the unit bus communication is higher than for hardwired interfaces.

The main signals transmitted through the unit bus are:

- Manual operation signals transmitted from the operational VDUs in the MCR and RSR to the PSMS and PCMS. The manual controls of the safety-related systems from the operational VDUs reduce the task burden of accessing controls through the separate train safety VDUs. In addition, due to the advanced graphical user interface, the operational VDUs reduce human performance error, than the safety VDUs. The detail descriptions to enhance the performance of the safety function from the standpoint of the Human Factor Engineering design are described in DCD Chapter 18. Signals to the PSMS are blocked by automatic safety-related signals and logic in the PSMS, which ensures priority of all safety functions. All safety-related components controlled by the PSMS have automated safety-related signals and priority logic. No manual controls of the safety-related systems from the operational VDUs are expected in the accident analysis in DCD Chapter 15, because the all safety-related systems can be manually controlled by the safety VDUs.
- The PSMS does not receive any process signals (analog signals) from the non-safety PCMS, including the operational VDU, via the data communication (unit bus) interface. DCD_07.09-27 S01
- Process and alarm signals transmitted from the PSMS to the LDP and operational VDUs in all operating locations, MCR, RSR, and TSC and to the computer systems such as process recording computer system, alarm logic computer, etc.
- Process and alarm signals transmitted in PCMS.