Abstract

~~This topical report which is attached JEXU-1012-1002-P describes the MELTAC digital platform. MHI seeks NRC approval of this platform for application to the safety systems of the US-APWR and for replacement of current safety systems in operating plants. The MELTAC digital platform was developed by MHI and MELCO for nuclear power plants in Japan. For applications in the US, this report demonstrates conformance of the MELTAC digital platform to all applicable US Codes and Standards. These include:~~ DCD_07.01-45

- ~~Code of Federal Regulations~~
- ~~Regulatory Guides~~
- ~~Branch Technical Positions~~
- ~~NUREG-Series Publications~~
- ~~IEEE-Standards~~
- ~~Other Industry Standards~~

This MHI technical report describes the design of the safety system digital platform for the US-APWR. Technical and quality requirements specific to the hardware and software design of the safety digital platform are identified first.

A specification of the safety-related platform is also attached in this document with the design information, which demonstrates that the safety-related digital platform design conforms to NRC regulations and guidance, and meets the technical and quality requirements.

0.1 Technical and Quality Requirement of Safety-related Digital Platform

DCD_ 07.01-45

Purpose and Scope

The purpose of this document is to describe the design of the safety system digital platform for the US-APWR.

Technical and quality requirements, specific to the hardware and software design of the safety-related digital platform, are identified. To demonstrate the completeness of the design, a specification of the safety-related digital platform is also attached in this document

The other system level technical and quality requirements for the safety-related I&C systems, not described in this report (e.g., US-APWR plant specific requirements, functional specific requirements, system specific requirements, application specific requirements) are described in the US-APWR DCD Ch7 and the other associated technical reports.

Applicability of Safety-related Digital Platform

The safety-related platform design and development meets the technical and quality requirements derived from applicable regulatory requirements and guidance.

As described in DCD Section 7.1, the safety-related I&C for the US-APWR consists of a fully digital platform. The technical and quality requirements for the safety-related platform design and development are identified in the following documents.

DCD Chapter 7
"Safety I&C System Description and Design Process" (MUAP-07004)
"Safety System Digital Platform -MELTAC-" (MUAP-07005), this report
"US-APWR Software Program Manual" (MUAP-07017)
"MELTAC Platform ISG-04 Conformance Analysis" (MUAP-13018)
"US-APWR Response Time of Safety I&C System" (MUAP-09021)
"US-APWR Instrument Setpoint Methodology" (MUAP-09022)

Table 0-1 lists the applicability matrix for the safety-related platform design and development. The applicability matrix table points to the DCD and related report sections which describe the technical and quality requirements of the safety-related platform. The applicability matrix table also points to the MUAP-07005 sections which describe design information. The design information demonstrates that the safety-related digital platform design conforms to NRC regulations and guidance, and meets the technical and quality requirements.

Technical and Quality Requirement of Safety Digital Platform

The applicability matrices for the safety-related digital platform design and development are provided to demonstrate that all technical and quality requirements and design information are identified in DCD and Technical Reports.

To ensure all technical and quality requirements for the safety-related digital platform are referenced in the applicability matrix table, applicable criteria for safety requirements are listed in the applicability matrix table map table. A similar table with applicable criteria of DCD Table 7.1-2, whose criteria is same as those of SRP Table 7-1, is provided for the applicability matrix table map table. In addition, applicability of each clause of IEEE Std. 603-1991 and IEEE Std.

7-4.3.2-2003 is included. Also, links between ITAAC to the safety requirements are provided in the applicability matrix table.

DCD_07.01-45

Safety Digital Platform Design Specification

A specification of the safety-related digital platform is also attached to this document (from Section 1 to Appendix H of this document) with the design Information which demonstrates that the safety-related digital platform design conforms to NRC regulations and guidance, and meets the technical and quality requirements.

The following sections contain design information from Section 1 to Appendix H of this document:
- Section 4: Safety-related digital platform specifications
- Section 5: Safety-related digital platform qualification test specifications
- Section 6: Safety-related digital platform lifecycle and security measures
- Section 7: Safety-related digital platform reliability information
- Appendix A, B, D, E, G, and H: Safety-related digital platform detailed specifications

Other sections from Section 1 of Appendix H of this document contain reference information which supports the design information.

Specific design information for each applicable criteria is identified in the applicability matrix Table 0-1.

Table 0-1 Regulatory Requirements and Guidance Applicability Matrix for the Safety-related Platform Design and Development (Sheet 1 of 11)

DCD_07.01-45

Criteria [3]	Title	Applicability	Technical & Quality Req.[1]	Design Info.[2]	ITAAC
10 CFR 50 and 52					
50.55a(a)(1)	Quality Standards for Systems Important to Safety	X	DCD Tier 2 7.1.3.13, 7.1.3.18, 7.9.2.1, 7.9.2.2	MUAP-07005 6.0	DCD Tier 1 2.5.1-6#24
50.55a(h)(2)	Protection Systems (IEEE Std. 603-1991 or IEEE Std. 279-1971)	X	See applicability to IEEE Std. 603.		
50.55a(h)(3)	Safety Systems (IEEE Std. 603-1991)	X	See applicability to IEEE Std. 603.		
50.34(f)(2)(v) [I.D.3]	Bypass and Inoperable Status Indication	N/A			
50.34(f)(2)(xi) [II.D.3]	Direct Indication of Relief and Safety Valve Position	N/A			
50.34(f)(2)(xii) [II.E.1.2]	Auxiliary Feedwater System Automatic Initiation and Flow Indication	N/A			
50.34(f)(2)(xvii) [II.F.1]	Accident Monitoring Instrumentation	N/A			
50.34(f)(2)(xviii) [II.F.2]	Instrumentation for the Detection of Inadequate Core Cooling	N/A			
50.34(f)(2)(xiv) [II.E.4.2]	Containment Isolation Systems	N/A			
50.34(f)(2)(xix) [II.F.3]	Instruments for Monitoring Plant Conditions Following Core Damage	N/A			
50.34(f)(2)(xx) [II.G.1]	Power for Pressurizer Level Indication and Controls for Pressurizer Relief and Block Valves	N/A			
50.34(f)(2)(xxii) [II.K.2.9]	Failure Mode and Effect Analysis of Integrated Control System	N/A			
50.34(f)(2)(xxiii) [II.K.2.10]	Anticipatory Trip on Loss of Main Feedwater or Turbine Trip	N/A			
50.34(f)(2)(xxiv) [II.K.3.23]	Central Reactor Vessel Water Level Recording	N/A			
50.62	Requirements for Reduction of Risk from Anticipated Transients without Scram	N/A			
52.47(b)(1)	ITAAC for Standard Design Certification	X			DCD Tier 1
52.80(a)	ITAAC for Combined Licensee Applications	N/A			

DCD_07.01-45

Table 0-1 Regulatory Requirements and Guidance Applicability Matrix for the Safety-related Platform Design and Development (Sheet 2 of 11)

Criteria (3)	Title	Applicability	Technical & Quality Req. (1)	Design Info. (2)	ITAAC
GDC 10 CFR 50 Appendix A					
GDC 1	Quality Standards and Records	X	DCD Tier 2 7.1.3.13, 7.1.3.18, 7.9.2.1, 7.9.2.2	MUAP-07005 6.0	DCD Tier 1 2.5.1-6#24
GDC 2	Design Bases for Protection Against Natural Phenomena	X	DCD Tier 2 7.1.3.7, 7.9.2.13 MUAP-07004 6.5.6	MUAP-07005 5.0	DCD Tier 1 2.5.1-6#5 2.5.1-6#8 2.5.6-1#4
GDC 4	Environmental and Dynamic Effects Design Bases	X	DCD Tier 2 7.1.3.7, 7.9.2.11 MUAP-07004 6.5.5, 6.5.7	MUAP-07005 5.0	DCD Tier 1 2.5.1-6#7 2.5.1-6#8
GDC 10	Reactor Design	N/A			
GDC 13	Instrumentation and Control	N/A			
GDC 15	Reactor Coolant System Design	N/A			
GDC 16	Containment Design	N/A			
GDC 19	Control Room	N/A			
GDC 20	Protection System Functions	N/A			
GDC 21	Protection Systems Reliability and Testability	X	DCD Tier 2 7.1.3.10, 7.9.2.9 MUAP-07004 4.3, 4.4, 5.1.9, 6.5.2	MUAP-07005 4.1.5, 4.1.7, 4.2.3, 4.2.4, 7.0	DCD Tier 1 2.5.1-6#17 2.5.1-6#24 2.13-1#1
GDC 22	Protection System Independence	X	DCD Tier 2 7.1.3.4, 7.1.3.5, 7.1.4.1.2, 7.1.4.2.2, 7.9.2.7 MUAP-07004 4.2.7, Appendix F.1.2, F.2.2	MUAP-07005 4.1.2.3, 4.1.2.5, 4.3, 5.5, Appendix A.3, A.4, A.6, A.7	DCD Tier 1 2.5.1-6#10 2.5.6-1#6

Table 0-1 Regulatory Requirements and Guidance Applicability Matrix for the Safety-related Platform Design and Development (Sheet 3 of 11)

DCD_07.01-45

Criteria [3]	Title	Applicability	Technical & Quality Req. [1]	Design Info. [2]	ITAAC
GDC 23	Protection System Failure Modes	X	DCD Tier 2 7.1.3.10, 7.9.2.8 MUAP-07004 4.3	MUAP-07005 4.1.5, 4.2.3	DCD Tier 1 2.5.1-6#17
GDC 24	Separation of Protection and Control Systems	X	DCD Tier 2 7.1.3.16, 7.7.2.9 MUAP-07004 4.2.5.a	MUAP-07005 Appendix B (S/S Function)	DCD Tier 1 2.5.1-6#26
GDC 25	Protection System Requirements for Reactivity Control Malfunctions	N/A			
GDC 28	Reactivity Limits	N/A			
GDC 29	Protection Against AOOs	N/A			
GDC 33	Reactor Coolant Makeup	N/A			
GDC 34	Residual Heat Removal	N/A			
GDC 35	Emergency Core Cooling	N/A			
GDC 38	Containment Heat Removal	N/A			
GDC 41	Containment Atmosphere Cleanup	N/A			
GDC 44	Cooling Water	N/A			
Staff Requirements Memoranda					
SRM to SECY 93087 II.Q	Defense Against Common-Mode Failures in Digital I&C Systems	N/A			
SRM to SECY 93087 II.T	Control Room Annunciator (Alarm) Reliability	N/A			
RGs [4]					
RG 1.22	Periodic Testing of Protection System Actuation Functions	X	See applicability to GDC 21.		
RG 1.47	Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety System	N/A			
RG 1.53	Application of the Single-Failure Criterion to Safety Systems	X	See applicability to GDC 21 and 24.		
RG 1.62	Manual Initiation of Protection Actions	N/A			
RG 1.75	Independence of Electrical Safety Systems	X	See applicability to GDC 22.		

DCD_07.01-45

Table 0-1 Regulatory Requirements and Guidance Applicability Matrix for the Safety-related Platform Design and Development (Sheet 4 of 11)

Criteria (3)	Title	Applicability	Technical & Quality Req. (1)	Design Info. (2)	ITAAC
RG 1.97	Instrumentation for Light Water Cooled NPPs to Assess Plant Conditions During and Following an Accident and Criteria for Accident Monitoring Instrumentation for NPPs	N/A			
RG 1.105	Setpoints for Safety-related Instrumentation	X	MUAP-07004 6.5.4	MUAP-07005 Appendix A.5, A6, A9	
RG 1.118	Periodic Testing of Electric Power and Protection Systems	X	See applicability to GDC 21.		
RG 1.151	Instrument Sensing Lines	N/A			
RG 1.152	Criteria for Use of Computers in Safety Systems of Nuclear Power Plants	X	See applicability to IEEE Std. 7-4.3.2.		
RG 1.168	Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	X	DCD Tier 2 7.1.3.17, 7.1.4.1.5, 7.1.4.2.5, 7.9.2.2, 7.9.2.3 MUAP-07004 Appendix F.1.5, F.2.5 MUAP-07007 All Sections	MUAP-07005 4.1.3, 4.2.2, 6.0	DCD Tier 1 2.5.1-6#24
RG 1.169	Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants				
RG 1.170	Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants				
RG 1.171	Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants				
RG 1.172	Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants				
RG 1.173	Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants				

DCD_07.01-45

Table 0-1 Regulatory Requirements and Guidance Applicability Matrix for the Safety-related Platform Design and Development (Sheet 5 of 11)

Criteria [3]	Title	Applicability	Technical & Quality Req.[1]	Design Info.[2]	ITAAC
RG 1.174	An Approach for Using PRA in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis	N/A			
RG 1.177	An Approach for Plant-Specific Risk-Informed Decision Making: technical specifications	N/A			
RG 1.180	Guidelines for Evaluating Electromagnetic and Radiofrequency Interference in Safety-Related I&C Systems	X	DCD Tier 2 7.1.3.7, 7.9.2.11 MUAP-07004 6.5.7	MUAP-07005 5.3, 5.4	DCD Tier 1 2.5.1-6#7
RG 1.189	Fire Protection for Operating Nuclear Power Plants	N/A			
RG 1.200	An Approach for Determining the Technical Adequacy of PRA Results for Risk-Informed Activities	N/A			
RG 1.204	Guidelines for Lightning Protection of Nuclear Power Plants	X	DCD Tier 2 Chapter 8	MUAP-07005 5.3	DCD Tier 1 2.5.1-6#7
RG 1.209	Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants	X	See applicability to GDC 21.		
BTPs					
BTP 7-1	Guidance on Isolation of Low-Pressure Systems from the High-Pressure RCS	N/A			
BTP 7-2	Guidance on Requirements on Motor-Operated Valves in the Emergency Core Cooling System (ECCS) Accumulator Lines	N/A			
BTP 7-3	Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps Out of Service	N/A			
BTP 7-4	Guidance on Design Criteria for Auxiliary Feedwater Systems	N/A			
BTP 7-5	Guidance on Spurious Withdrawals of Single Control Rods in Pressurized Water Reactors	N/A			

DCD_07.01-45

Table 0-1 Regulatory Requirements and Guidance Applicability Matrix for the Safety-related Platform Design and Development (Sheet 6 of 11)

Criteria [3]	Title	Applicability	Technical & Quality Req.[1]	Design Info.[2]	ITAAC
BTP 7-6	Guidance on Design of I&Cs Provided to Accomplish Changeover from Injection to Recirculation Mode	N/A			
BTP 7-7	Not used	N/A			
BTP 7-8	Guidance on Application of RG 1.22	X	See applicability to RG 1.22 and GDC21.		
BTP 7-9	Guidance on Requirements for RPS Anticipatory Trips	N/A			
BTP 7-10	Guidance on Application of RG 1.97	N/A			
BTP 7-11	Guidance on Application and Qualification of Isolation Devices	X	See applicability to RG 1.75 and GDC22.		
BTP 7-12	Guidance on Establishing and Maintaining Instrument Setpoints	N/A			
BTP 7-13	Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors	N/A			
BTP 7-14	Guidance on Software Reviews for Digital Computer-Based I&C Systems	X	See applicability to RG 1.168 thru 1.173.		
BTP 7-15	Not used	N/A			
BTP 7-16	Not used	N/A			
BTP 7-17	Guidance on Self-Test and Surveillance Test Provisions	X	See applicability to RG 1.22, 1.118 and GDC21.		
BTP 7-18	Guidance on Use of Programmable Logic Controllers in Digital Computer-Based I&C Systems	N/A			
BTP 7-19	Guidance on Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based I&C Systems	N/A			
BTP 7-20	Not used	N/A			
BTP 7-21	Guidance on Digital Computer Real-Time Performance	X	DCD Tier 2 7.1.4.1.3, 7.1.4.2.3, 7.9.2.3 MUAP-07004 6.5.3, Appendix F.1.3, F.2.3	MUAP-07005 4.1.3, 4.2.2, 4.4	DCD Tier 1 2.5.1-6#31
IEEE Std. 603-1991					
1.	Scope	N/A			
2.	Definitions	N/A			

Table 0-1 Regulatory Requirements and Guidance Applicability Matrix for the Safety-related Platform Design and Development (Sheet 7 of 11)

DCD_07.01-45

Criteria [3]	Title	Applicability	Technical & Quality Req.[1]	Design Info.[2]	ITAAC
3.	References	N/A			
4	Safety System Designation	No Req.			
4.1	Design Basis Events	N/A			
4.2	Safety Functions and Corresponding Protective Actions	N/A			
4.3	Permissive Conditions for Each Operating Bypass Capability	N/A			
4.4	Variables Required to be Monitored for Protective Action	N/A			
4.5	The Minimum Criteria for Each Action Controlled by Manual Means	N/A			
4.5.1	Allowed Time and Plant Condition	N/A			
4.5.2	Justification of Permitting Initiation or Control Subsequent to Initiation	N/A			
4.5.3	Control Room Habitability	N/A			
4.5.4	Display of Variable	N/A			
4.6	Spatially Dependent Variables	N/A			
4.7	Range of Conditions for Safety System Performance	N/A			
4.8	Functional Degradation of Safety Functions	N/A			
4.9	Reliability	X	DCD Tier 2 7.2.3.5 MUAP-07004 4.3, 4.4, 5.1.9, 6.5.2	MUAP-07005 4.1.5, 4.2.3, 7.0	DCD Tier 1 2.5.1-6#24 2.13-1#1
4.10	The Critical Points in Time or the Plant Conditions	X	DCD Tier 2 7.1.4.1.3, 7.1.4.2.3, 7.9.2.3 MUAP-07004 6.5.3, Appendix F.1.3, F.2.3	MUAP-07005 4.1.3, 4.2.2, 4.4	DCD Tier 1 2.5.1-6#31
4.11	Equipment Protective Provisions	X	DCD Tier 2 7.1.3.10, 7.9.2.8 MUAP-07004 4.3	MUAP-07005 4.1.5, 4.2.3	DCD Tier 1 2.5.1-6#17

Table 0-1 Regulatory Requirements and Guidance Applicability Matrix for the Safety-related Platform Design and Development (Sheet 8 of 11)

DCD_07.01-45

Criteria (3)	Title	Applicability	Technical & Quality Req.(1)	Design Info.(2)	ITAAC
4.12	Other Special Design Basis	N/A			
5	Safety System Criteria	No Req.			
5.1	Single Failure Criterion	N/A			
5.2	Completion of Protective Action	N/A			
5.3	Quality	X	DCD Tier 2 7.1.3.13, 7.1.3.18, 7.9.2.1, 7.9.2.2	MUAP-07005 6.0	DCD Tier 1 2.5.1-6#24
5.4	Equipment Qualification	X	DCD Tier 2 7.1.3.7, 7.9.2.11, 7.9.2.13 MUAP-07004 6.5.5, 6.5.6, 6.5.7	MUAP-07005 5.0	DCD Tier 1 2.5.1-6#5, 2.5.1-6#6, 2.5.1-6#7, 2.5.1-6#8,
5.5	System Integrity	N/A			
5.6	Independence	X	DCD Tier 2 7.1.3.4, 7.1.3.5, 7.1.4.1.2, 7.1.4.2.2, 7.9.2.7 MUAP-07004 4.2.7, Appendix F.1.2, F.2.2	MUAP-07005 4.1.2.3, 4.1.2.5, 4.3, 5.5, Appendix A.3, A.4, A.6, A.7	DCD Tier 1 2.5.1-6#10 2.5.6-1#6
5.6.1	Between Redundant Portions of a Safety System				
5.6.2	Between Safety Systems and Effects of a Design Basis Event				
5.6.3	Between Safety Systems and Other Systems				
5.6.3.1	Interconnected Equipment				
5.6.3.2	Equipment in Proximity				
5.6.3.3	The Effects of a Single Random Failure				
5.6.4	Detailed Independence Criteria				
5.7	Capability for Test and Calibration	X	DCD Tier 2 7.1.3.10, 7.9.2.9 MUAP-07004 4.3, 4.4, 5.1.9, 6.5.2	MUAP-07005 4.1.5, 4.2.3, 7.0	DCD Tier 1 2.5.1-6#17
5.8	Information Displays	No Req.			
5.8.1	Displays for Manually Controlled Actions	N/A			
5.8.2	System Status Indication	N/A			

DCD_ 07.01-45

Table 0-1 Regulatory Requirements and Guidance Applicability Matrix for the Safety-related Platform Design and Development (Sheet 9 of 11)

Criteria [3]	Title	Applicability	Technical & Quality Req. [1]	Design Info. [2]	ITAAC
5.8.3	Indication of Bypasses	N/A			
5.8.4	Location of Displays	N/A			
5.9	Control of Access	X	DCD Tier 2 7.9.2.5	MUAP-07005 4.5	DCD Tier 1 2.5.1-6#12
5.10	Repair	X	DCD Tier 2 7.1.3.10 MUAP-07004 4.3	MUAP-07005 4.1.4, 4.1.5, 4.2.3	DCD Tier 1 2.5.1-6#17
5.11	Identification	N/A			
5.12	Auxiliary Features	N/A			
5.13	Multi-Unit Stations	N/A			
5.14	Human Factors	N/A			
5.15	Reliability	X	MUAP-07004 6.5.2	MUAP-07005 7.0	DCD Tier 1 2.5.1-6#24 2.13-1#1
5.16	Common Cause Failure (IEEE 603-1998)	X	DCD Tier 2 7.1.3.7, 7.1.3.13, 7.1.3.18, 7.9.2.1, 7.9.2.2	MUAP-07005 4.1.3, 4.2.2, 5.0, 6.0 MUAP-07017 All Sections	DCD Tier 1 2.5.1-6#24
6	Sense and Command Features - Functional and Design Req.	N/A			
6.1	Automatic Control	N/A			
6.2	Manual Control	N/A			
6.3	Interaction between the Sense and Command features and other Systems	X	DCD Tier 2 7.1.3.16, 7.7.2.9 MUAP-07004 4.2.5.a	MUAP-07005 Appendix B (S/S Function)	DCD Tier 1 2.5.1-6#26
6.4	Derivation of System Inputs	N/A			
6.5	Capability for Testing and Calibration	N/A			
6.6	Operating Bypasses	N/A			
6.7	Maintenance Bypass	N/A			
6.8	Setpoint	No Req.			
6.8.1	Setpoint Uncertainties	N/A			
6.8.2	Multiple Setpoints	N/A			
7	Executive Features - Functional and Design Requirements	N/A			

Table 0-1 Regulatory Requirements and Guidance Applicability Matrix for the Safety-related Platform Design and Development (Sheet 10 of 11)

DCD_ 07.01-45

Criteria [3]	Title	Applicability	Technical & Quality Req. [1]	Design Info. [2]	ITAAC
7.1	Automatic Control	N/A			
7.2	Manual Control	N/A			
7.3	Completion of Protective Action	N/A			
7.4	Operating Bypass	N/A			
7.5	Maintenance Bypass	N/A			
8	Power Source Requirements	N/A			
IEEE Std. 7-4.3.2-2003					
1.	Scope	N/A			
2.	References	N/A			
3.	Definitions and Abbreviations	N/A			
4	Safety System Designation	No Req.			
5	Safety System Criteria	No Req.			
5.1	Single Failure Criterion	No Req.			
5.2	Completion of Protective Action	No Req.			
5.3	Quality	X	DCD Tier 2 7.1.3.17, 7.9.2.2 MUAP-07004 Appendix F.1.5, F.2.5 MUAP-07007 All Sections	MUAP-07005 4.1.3, 4.2.2, 6.0	DCD Tier 1 2.5.1-6#24
5.3.1	Software Development				
5.3.1.1	Software Quality Metrics				
5.3.2	Software Tools				
5.3.3	Verification and Validation				
5.3.4	Independent V&V (IV&V) Requirements				
5.3.5	Software Configuration Management				
5.3.6	Software Project Risk Management				
5.4.	Equipment Qualification	X	DCD Tier 2 7.9.2.9	MUAP-07005 4.1.5, 4.3, 5.0, 6.0	DCD Tier 1 2.5.1-6#24
5.4.1	Computer System Testing				
5.4.2.	Qualification of Existing Commercial Computers	N/A			
5.5.	System Integrity	X	DCD Tier 2 7.1.3.6, 7.1.3.17, 7.9.2.2 MUAP-07014 All Sections	MUAP-07005 4.1.3, 4.2.2, 6.0	DCD Tier 1 2.5.1-6#24
5.5.1	Design for computer integrity				
5.5.2	Design for test and calibration	X	DCD Tier 2	MUAP-07005	DCD Tier 1

DCD_07.01-45

Table 0-1 Regulatory Requirements and Guidance Applicability Matrix for the Safety-related Platform Design and Development (Sheet 11 of 11)

Criteria[3]	Title	Applicability	Technical & Quality Req.[1]	Design Info.[2]	ITAAC
5.5.3	Fault detection and self-diagnostics		7.1.3.10, 7.9.2.9 MUAP-07004 4.3, 4.4, 5.1.9, 6.5.2	4.1.5, 4.2.3, 7.0	2.5.1-6#17
5.6	Independence	X	DCD Tier 2 7.1.3.4, 7.1.3.5, 7.1.4.1.2, 7.1.4.2.2, 7.9.2.7 MUAP-07004 4.2.7, Appendix F.1.2, F.2.2	MUAP-07005 4.1.2.3, 4.1.2.5, 4.3, 5.5, Appendix A.3, A.4, A.6, A.7)	DCD Tier 1 2.5.1-6#10 2.5.6-1#6
5.7	Capability for Test and Calibration	No Req.			
5.8	Information Displays	No Req.			
5.9	Control of Access	No Req.			
5.10	Repair	No Req.			
5.11	Identification	X	DCD Tier 2 7.1.3.19	MUAP-07005 6.2.4	DCD Tier 1 2.5.1-6#13
5.12	Auxiliary Features	No Req.			
5.13	Multi-Unit Stations	No Req.			
5.14	Human Factors	No Req.			
5.15	Reliability	X	MUAP-07004 6.5.2	MUAP-07005 7.0	DCD Tier 1 2.13-1#1
6	Sense and Command Features - Functional and Design Requirements	No Req.			
7	Executive Features - Functional and Design Requirements	No Req.			
8	Power Source Requirements	No Req.			

(1) Technical and quality requirement of the safety-related I&C platform.
(2) Design information to describe that the safety-related I&C platform design conforms to the NRC regulations and guidance, and meets the technical and quality requirements of the safety-related I&C platform.
(3) The applicable criteria in NUREG-0800 Standard Review Plan (SRP) Sec. 7.1 Rev. 5, and each clause of IEEE Std. 603-1991 and IEEE 7-4.3.2-2003 are listed in this table to ensure all technical and quality requirements for the safety-related I&C platform are included in the table.
(4) Applicable revision number of each Regulatory Guide is located in the US-APWR DCD Table 1.9.1-1.

Abstract

This Technical Report describes the design of the Mitsubishi Electric Total Advanced Controller (MELTAC) Platform and its conformance to the U.S. Nuclear Regulatory requirements for nuclear safety systems. The MELTAC platform is the basis of the Mitsubishi Heavy Industries (MHI) safety and non-safety digital I&C systems.

The MELTAC platform was developed specifically for nuclear applications. The modular structure, deterministic response time and testability can be applied to solve plant-wide needs for safety and non-safety applications. Moreover the MELTAC platform has been developed using a rigorous safety-related design process that ensures suitable hardware and software quality and reliability for critical applications such as the reactor protection system or engineered safety features actuation system.

The MELTAC platform has accumulated many years of positive performance records in various non-safety system applications such as the Plant Control and Monitoring System in nuclear plants operating in Japan. Based on its excellent performance in numerous non-safety applications, the MELTAC platform has now been applied to almost all systems throughout Japanese PWR nuclear plants under construction. These systems were shipped to the site recently.

~~The goal of this report is to seek approval from the U.S. Nuclear Regulatory Commission (NRC) for the use of the MELTAC platform for nuclear safety systems in new reactors (US-APWR).~~

DCD_07.01-45

For applications in the US, this report demonstrates conformance of the Design and Design Process to all applicable US Codes and Standards. These include:

- Code of Federal Regulations
- Regulatory Guides
- Branch Technical Positions
- NUREG-Series Publications
- IEEE-Standards
- Other Industry Standards

The information provided in this report covers the following topics to fully understand the MELTAC platform:

- The design of the hardware, software, communication network and application development tools of the MELTAC platform
- The equipment qualification of the MELTAC platform and its conformance to the corresponding U.S. standards
- The life cycle and the Quality Assurance Program of the MELTAC platform conformed to U.S. regulations
- The history of operation and the equipment reliabilities of the MELTAC platform

The complete MHI digital I&C design is described in Topical Reports and a Technical Report for the US-APWR DCD:

- Safety I&C System Description and Design Process (Technical Report for the US-APWR DCD)
- Safety System Digital Platform - MELTAC - (this report)

- HSI System Description and HFE (Human Factor Engineering) Process
- Defense in Depth and Diversity

~~The information in this Digital Platform Technical Reports is expected to be sufficient to allow the NRC to make a final safety determination regarding the suitability of the MELTAC platform for safety-related nuclear applications, on the condition of completing specific application engineering as identified in the other Topical Reports. Other documentation which has been generated during the MELTAC design process is available for NRC audit, as may be needed to allow the NRC to confirm the MELCO design and design process, as documented in this Technical Report.~~ DCD_07.01-45

List of Acronyms

AI	Analog Input
ANSI	American National Standards Institute
AO	Analog Output
ASME	American Society of Mechanical Engineers
ATWS	Anticipated Transient without Scram
BTP	Branch Technical Position
CEAS	~~MELCO~~ Corporate Electronic Archive System
CFR	Code of Federal Regulations
COTS	Commercial Off The Shelf
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DAAC	Diverse Automatic Actuation Cabinet
DAC	Design Acceptance Criteria
DAS	Diverse Actuation System
DBA	Design Basis Accident
DI	Digital Input
DO	Digital Output
DSP	Digital Signal Processor
ECC	Error Correcting Code
EEPROM	Electronically Erasable Programmable Read Only Memory
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESC	Energy Systems Center in Mitsubishi Electric Corporation
ESD	Electrostatic Discharge
ESFAS	Engineered Safety Features Actuation System
EUT	Equipment under Test
E/O	Electrical / Optical
FBD	Functional Block Diagram
FMEA	Failure Mode and Effect Analysis
FMU	Frame Memory Unit
F-ROM	Flash Electrically Erasable Programmable Read Only Memory
GBD	Graphic Block Diagram
GDC	General Design Criteria
GUI	Graphic User Interface
HSI	Human System Interface
ID	Identification
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IPL	Interposing Logic
ISO	International Standardization Organization
IT	Information Technology
ITAAC	Inspection, Test, Analysis, and Acceptance Criteria
I/O	Input/Output
I&C	Instrumentation and Control
JEC	Japanese Electrotechnical Committee

DCD_07.01-45

JIS	Japanese Industrial Standards	
JEAG	Japanese Electric Association Guide	
JEIDA	Japan Electronic Industry Development Association	
LCO	Limiting Conditions for Operation	
LED	Light Emitting Diode	
MCB	Main Control Board	
MCR	Main Control Room	
MELENS	Mitsubishi Electric Total Advanced Controller Engineering Station	
MELCO	Mitsubishi Electric Corporation	
MELTAC	Mitsubishi Electric Total Advanced Controller	
METI	Ministry of Economy, Trade and Industry	
MHI	Mitsubishi Heavy Industries, Ltd.	
MTBF	Mean Time Between Failures	
MTTR	Mean Time To Repair	
NC	Normally Close	
NO	Normally Open	
NPD	Nuclear Power Department in Mitsubishi Electric Corporation	
NRC	Nuclear Regulatory Commission	
OBE	Operational Basis Earthquakes	
PIF	Power Interface	
QA	Quality Assurance	
QAP	Quality Assurance Program	
QC	Quality Control	
RAM	Random Access Memory	
RFI	Radio Frequency Interference	
RG	Regulatory Guide	
RGB	Red/Green/Blue	
ROM	Read Only Memory	
RPR	Resilient Packet Ring	
RPS	Reactor Protection System	
RTD	Resistance Temperature Detector	
RTM	Requirements Traceability Matrix	
SSE	Safe Shutdown Earthquake	
VDU	Visual Display Unit	
V&V	Verification and Validation	
~~UCP~~	~~MELTAC US Conformance Program~~	DCD_07.01-45
UDP/IP	User Datagram Protocol Internet Protocol	
UV-ROM	Ultra-Violet Erasable Programmable Read Only Memory	
UTP	Unshielded Twist Pair Cable	
WDT	Watchdog Timer	

1.0 PURPOSE

The purpose of this report is to describe a nuclear safety Platform by Mitsubishi Electric Corporation. One common platform with a modular structure can be applied to solve most utility needs for safety applications, including new systems, component replacements and complete system replacements. The platform is referred to as Mitsubishi Electric Total Advanced Controller Platform; or simply as “MELTAC platform “.

The MELTAC platform is applied to the protection and safety monitoring system, which includes the reactor protection system, engineered safety feature actuation system, safety logic system, safety-related HSI system, and any other safety system. In addition, the MELTAC platform is applied to non-safety systems such as the Plant Control and Monitoring System. The MELTAC equipment applied for non-safety applications is the same design as the equipment for safety applications. However, there are differences in Quality Assurance methods for software design and other software life cycle processes.

~~The goal of this report is to seek approval from the U.S. Nuclear Regulatory Commission for the use of the MELTAC platform for nuclear safety systems in new reactors.~~ DCD_07.01-45

2.0 SCOPE

The scope of this report includes the hardware and software associated with the MELTAC platform. The MELTAC platform described herein encompasses design, qualification, and reliability.
~~Model numbers in this report represent current numbers at the time of this document revision. Model numbers will change as the product life cycle progresses. New models will retain the minimum functional features, performance specifications and reliability of current models.~~ DCD_07.01-45

The MELTAC platform will be used for the safety systems of ~~new plants (~~US-APWR~~)~~. DCD_07.01-45

3.0 APPLICABLE CODE, STANDARDS AND REGULATORY GUIDANCE

This section identifies conformance to applicable codes and standards. Unless specifically noted, the latest version issued on the date of this document is applicable. The following terminology is used in this section:

Plant Licensing Documentation – This refers to plant level documentation that is specific to a group of plants or a single plant, such as the Design Certification Document, Combined Operating Licensing Application, Final Safety Analysis Report, or License Amendment Request.

Equipment - This refers to the components that are the subject of this Technical Report. “Equipment” includes the MHI safety-related digital I&C systems and the MELCO safety-related digital I&C platform. “Equipment” does not include the MHI non-safety digital I&C or HSI systems nor the MELCO non-safety digital I&C or HSI platforms. It is noted that the MHI non-safety digital I&C systems utilize the MELCO non-safety digital I&C platform which is the same as the MELCO safety-related digital I&C platform. However, some QA aspects of design and manufacturing are not equivalent between safety and non-safety systems/platforms.

Code of Federal Regulations

1. 10 CFR 50 Appendix A: General Design Criteria for Nuclear Power Plants

GDC 1: Quality Standards and Records
The lifecycle process for the Basic components of the MELTAC Platform ~~The MELCO quality program that~~ that meets all requirements of 10CFR50 Appendix B is described in Section 6. This is referred to as the App.B-based QAP. ~~This program governs the re-evaluation of MELTAC development activities conducted under previous MELCO quality programs that used the requirements of 10CFR50 Appendix B as a guideline, but were not in full compliance with 10CFR50 Appendix B. The re-evaluation demonstrates that MELTAC has suitable technical characteristics and quality for nuclear safety applications, and is therefore equivalent to a product developed under a 10CFR50 Appendix B quality program.~~

DCD_07.01-45

GDC 2: Design Bases For Protection Against Natural Phenomena
This Equipment is seismically qualified. The Equipment is located within building structures that provide protection against other natural phenomena. Specific buildings and Equipment locations are described in Plant Licensing Documentation.

GDC 4: Environmental And Dynamic Effects Design Bases
This Equipment is located in a mild environment that is not adversely effected by plant accidents.

GDC 5: Sharing of Structures, Systems, and Components
In general, there is no sharing of this Equipment among nuclear power units. Any sharing is discussed in specific Plant Licensing Documentation.

Equipment reliability which is described in Section 7.3 of this report. Specific manual surveillance features are described in the Safety I&C System Description and Design Process Technical Report for the US-APWR DCD.

4. 10 CFR 50.49 Environmental Qualification Of Electric Equipment Important To Safety For Nuclear Power Plants

This Equipment is located in a mild environment. A mild environment is an environment that would at no time be significantly more severe than the environment that would occur during normal plant operation, including anticipated operational occurrences. Therefore this criteria is not applicable. This criteria is applicable to some instrumentation that interfaces to this Equipment. The qualification of this instrumentation is described in Plant Licensing Documentation.

5. 10 CFR 50.55a

(a)(1) Quality Standards for Systems Important to Safety

This Equipment is ~~was originally~~ developed under ~~a Japanese nuclear quality program that encompasses most requirements of 10CFR50 Appendix B~~ the App.B based QAP described in Section 6~~. Section 6 describes the App.B-based QAP~~, which is fully compliant to 10CFR50 Appendix B. ~~The App.B-based QAP governs the re-evaluation of previous MELTAC development, and all new MELTAC development or revisions that may occur after this re-evaluation.~~

DCD_07.01-45

(h) Invokes IEEE Std. 603-1991

See conformance to IEEE 603-1991

6. 10 CFR 50.62 ATWS Rule

The Diverse Actuation System (DAS), which is used to actuate plant systems for ATWS mitigation, is described briefly in the Safety I&C System Description and Design Process Technical Report for the US-APWR DCD, MUAP-07004, and in more depth in the Defense in Depth and Diversity Topical Report, MUAP-07006. The DAS is diverse from this Equipment for all reactor trip functions. The DAS and the safety logic system, described in MUAP-07004, utilize a common output module that interfaces to plant components. This common module is described in all Topical Reports as the Power Interface (PIF) module. To ensure compliance with the ATWS rule, the PIF module is not used for any reactor trip functions. The diversity between MELTAC and the DAS is described in the Defense in Depth and Diversity Topical Report.

7. 10 CFR 52.47

(a)(1)(iv) Resolution of Unresolved and Generic Safety Issues

(a)(1)(vi) ITAAC in Design Certification Applications

(a)(1)(vii) Interface Requirements

Conformance to the requirements in items iv thru vii, above, are described in Plant Licensing Documentation .

(a)(2) Level of Detail

The content of this Technical Report, together with the additional information described in other digital system Technical ~~Topical~~ Reports and Plant Licensing Documentation~~, is sufficient to allow the NRC staff to reach a final conclusion on all safety questions associated with the design. The information~~ includes performance requirements and design information sufficiently detailed to ~~permit the preparation of acceptance and inspection requirements by the NRC, and procurement specifications and construction and installation specifications by an applicant~~ demonstrate compliance with the regulatory requirements.

DCD_07.01-45

(b)(2)(i) Innovative Means of Accomplishing Safety Functions

In the near term, the Equipment is expected to be applied to conventional I&C safety and non-safety functions typical of new evolutionary plants. In the longer term, the Equipment is expected to be applied to more innovative safety functions as may be typical of new passive plants. All specific plant safety functions are described in Plant Licensing Documentation.

8. 10 CFR 52.79(c) ITAAC in Combined Operating License Applications

The inspections, tests, analyses and acceptance criteria that demonstrate that this Equipment has been constructed and will operate in conformity with the Commission's final safety conclusion, will be described in the Plant Licensing Documentation.

Staff Requirements Memoranda

9. SRM to SECY 93-087

II.Q Defense Against Common-Mode Failures in Digital I&C Systems
Conformance is described in the Defense-in-Depth and Diversity Topical Report.

II.T Control Room Annunciator (Alarm) Reliability
This Equipment and the MHI non-safety I&C systems can be configured at the application level to generate alarms. Alarm annunciators are provided by the MHI non-safety HSI system. Conformance to requirements for redundancy, and conformance to separation and independence criteria between safety divisions and between safety and non-safety divisions is described in the Safety I&C System Description and Design Process Technical Report for the US-APWR DCD.

NRC Regulatory Guides

10. RG 1.22 Periodic Testing of Protection System Actuation Functions

See GDC 21 conformance. The functions controlled by this Equipment can be configured at the application level to be completely testable through a combination of overlapping automatic and manual tests. The detail is described in the Safety I&C System Description and Design Process Technical Report for the US-APWR DCD.

19. RG 1.105 Setpoints for Safety-Related Instrumentation

endorses ISA-S67.04-1994 and ANS-10.4-1987

The uncertainties associated with the Equipment are described in this Technical Report. Appendix A.5 defines I/O M~~m~~odule accuracies. Appendix A.6 defines isolation module accuracies. Appendix A.9 defines accuracy of I/O power supplies. This includes uncertainties for signal conditioning modules, signal splitters, instrument loop power suppliers and analog to digital converters. The uncertainties associated with specific process instrumentation and the resulting safety-related setpoints are described in Plant Licensing Documentation. The methodology used to combine all uncertainties to establish safety-related setpoints is described in the Safety I&C System Description and Design Process Technical Report for the US-APWR DCD. The plant specific uncertainty/setpoint analysis is described in Plant Licensing Documentation.

DCD_07.01-30

20. RG 1.118 Periodic Testing of Electric Power and Protection Systems

endorses IEEE 338-1987

See conformance to GDC 21, 10CFR50.36 and RG 1.22. The Equipment can be configured so that all safety functions are tested either automatically or manually, and so that manual tests do not require any system reconfiguration, such as jumpers or fuse removal. The periodic test features are described in the Safety I&C System Description and Design Process Technical Report for the US-APWR DCD.

21. RG 1.151 Instrument Sensing Lines

endorses ISA-S67.02

Compliance is described in Plant Licensing Documentation .

22. RG 1.152 Criteria for Programmable Digital Computers in Safety Systems of Nuclear Power Plants

endorses IEEE 7-4.3.2-2003

The methods used for specifying, designing, verifying, validating and maintaining software for this Equipment conforms to these requirements. ~~The life cycle process for the original MELTAC digital platform software, that was developed in Japan and has been commercially dedicated for safety applications (see Item 46), is described in this Technical Report.~~ The life cycle process for the ~~current~~ MELTAC platform is described in the ~~MELTAC Platform Basic Software Program Manual (JEXU-1012-1132)~~ Section 6.1 of this Technical Report. The life cycle process for the system application software is described in US-APWR Software Program Manual (MUAP-07017). The methods used for ensuring a secure development and operational environment throughout the life cycle are described in these documents.

DCD_07.01-45

23. RG 1.153 1996 Criteria for Safety Systems

endorses IEEE Std 603-1991

Compliance with the General Design Criterion identified in this Regulatory Guide is discussed above. Compliance with IEEE 603-1991 is discussed below.

24. RG 1.168 Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

endorses IEEE Std 1012-1998 and IEEE Std 1028-1997

This Equipment uses processes for verification, validation, reviews and audits that conform to this Regulatory Guide. ~~The software life cycle design processes for the original MELTAC digital platform, that was developed in Japan and has been commercially dedicated for safety applications (see Item 46), are described in Section 6 of this Technical Report.~~ The software life cycle design processes for the ~~current~~ MELTAC platform is described in the ~~MELTAC Platform Basic Software Program Manual (JEXU-1012-1132)~~ Section 6.1 of this Technical Report. ~~Section 6 of this Technical Report includes references to the corresponding original MELTAC software life cycle procedures. Appendix C of this Technical Report provides a complete list of MELTAC software life cycle procedures with a cross correlation to the guidance of BTP 7-14.~~ The software life cycle design processes for plant systems are described in US-APWR Software Program Manual (MUAP-07017).

DCD_07.01-45

25. RG 1.169 Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

endorses IEEE Std 828-1990 and IEEE Std 1042-1987

This Equipment is designed and maintained using a Configuration Management process that conforms to this Regulatory Guide. ~~The Configuration Management process for the original MELTAC digital platform, that was developed in Japan and has been commercially dedicated for safety applications (see Item 46), is described in Section 6.1.5 of this Technical Report.~~ The Configuration Management process for the current MELTAC platform is described in the ~~MELTAC Platform Basic Software Program Manual (JEXU-1012-1132)~~ Section 6.1 of this Technical Report. The Configuration Management process for plant systems is described in US-APWR Software Program Manual (MUAP-07017).

DCD_07.01-45

26. RG 1.170 Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

endorses IEEE Std 829-1983

The test documentation for this Equipment conforms to this Regulatory Guide. ~~The test process and corresponding documentation for the original MELTAC digital platform, that was developed in Japan and has been commercially dedicated for safety applications (see Item 46), are described in Section 6.1.4 of this Technical Report.~~ The test process and corresponding documentation for the ~~current~~ MELTAC platform are described in the ~~MELTAC Platform Basic Software Program Manual (JEXU-1012-1132)~~ Section 6.1 of this Technical Report. The test documentation for plant systems is described in US-APWR Software Program Manual (MUAP-07017).

DCD_07.01-45

27. RG 1.171 Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

endorses IEEE Std 1008-1987

Unit testing for this Equipment conforms to this Regulatory Guide. ~~This unit testing for the original MELTAC digital platform, that was developed in Japan and has been commercially dedicated for safety applications(see Item 46), is described in Section 6.1.4 of this Technical Report.~~ The unit testing for the ~~current~~ MELTAC platform is described in the ~~MELTAC Platform Basic Software Program Manual (JEXU-1012-1132)~~ Section 6.1 of this Technical Report. Unit testing for plant systems is described in US-APWR Software Program Manual (MUAP-07017). DCD_07.01-45

28. RG 1.172 Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

endorses IEEE Std 830-1993

The Software Requirements Specifications for this Equipment conforms to this Regulatory Guide. ~~The Software Requirements Specifications for the original MELTAC digital platform, that was developed in Japan and has been commercially dedicated for safety applications (see Item 46), are described in Section 6.1.4 of this Technical Report.~~ The Software Requirements Specifications for the ~~current~~ MELTAC platform are described in the ~~MELTAC Platform Basic Software Program Manual (JEXU-1012-1132)~~ Section 6.1 of this Technical Report. The Software Requirements Specifications for plant systems are described in US-APWR Software Program Manual (MUAP-07017). DCD_07.01-45

29. RG 1.173 Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

endorses IEEE Std 1074-1995

The Software Life Cycle Process for this Equipment conforms to this Regulatory Guide. ~~The Software Life Cycle Processes for the original MELTAC digital platform, that was developed in Japan and has been commercially dedicated for safety applications (see Item 46), are described in Section 6 of this Technical Report.~~ The Software Life Cycle Processes for the ~~current~~ MELTAC platform are described in the ~~MELTAC Platform Basic Software Program Manual (JEXU-1012-1132)~~ Section 6.1 of this Technical Report. The Software Life Cycle Processes for plant systems is described in US-APWR Software Program Manual (MUAP-07017). DCD_07.01-45

30. RG 1.180 Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related Instrumentation and Control Systems

endorses MIL-STD-461E, IEC 61000 Parts 3, 4, and 6, IEEE Std C62.41-1991, IEEE Std C62.45-1992, IEEE Std 1050-1996, EPRI TR-102323

This Equipment conforms to the EMI/RFI requirements of this standard. Qualification testing for the digital platform is described in this Technical Report. Requirements and features of plant systems that ensure conformance to the platform qualification envelope are described in the Safety I&C System Description and Design Process Technical Report for the US-APWR DCD .

30.a RG 1.204 Guidelines for Lightning Protection of Nuclear Power Plants

Site specific aspects of the lightning protection requirement should be a COL item which is site dependent and will be described in individual COL applications. However, platform needs to be designed with surge resistance. Thus surge test specifications are determined by reference to IEEE 62.41, IEEE62.45, and IEEE472, and a test is conducted for the MELTAC Platform, as described in Section 5.3. DCD_07.01-45

30.~~a~~b RG1.206 Combined License Applications for Nuclear Power Plants (LWR Edition)

The level of detail provided in this report conforms to this Regulatory Guide~~ and is expected to be sufficient for the NRC staff to make a final safety determination regarding the suitability of the MELTAC platform for safety-related applications~~. This document is intended to supplement the information provided in COL applications. This document may be referenced directly or indirectly (via reference to a certified design, which references this document). Should the NRC Safety Evaluation Report for this Technical Report identify Application Specific Action Items, those open items will be addressed within an ITAAC for the certified design. DCD_07.01-45

NRC Branch Technical Positions

31. BTP 7-1 Guidance on Isolation of Low-Pressure Systems from the High-Pressure Reactor Coolant System

32. BTP 7-2 Guidance on Requirements of Motor-Operated Valves in the Emergency Core Cooling System Accumulator lines

33. BTP 7-3 Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps out of Service

34. BTP 7-4 Guidance on Design Criteria for Auxiliary Feedwater Systems

35. BTP 7-5 Guidance on Spurious Withdrawals of Single Control Rods in Pressurized Water Reactors

36. BTP 7-6 Guidance on Design of Instrumentation and Controls Provided to Accomplish Changeover from Injection to Recirculation Mode

Compliance with BTP 7-1 thru 6, above, is described in Plant Licensing Documentation.

37. BTP 7-8 Guidance for Application of Regulatory Guide 1.22

The Equipment includes extensive self-diagnostics which run continuously. The Equipment can be configured at the application level with additional manual test endorses IEEE Std 730

See conformance to RG 1.168 thru 1.173.

44. Deleted.

45. BTP 7-17 Guidance on Self-Test and Surveillance Test Provisions

See conformance to GDC 21, 10CFR50.36, RG 1.22 and RG 1.118. Surveillance testing taken together with automatic self-testing provides a mechanism for detecting all failures.

46. BTP 7-18 Guidance on Use of Programmable Logic Controllers in Digital Computer-Based I&C Systems

This Equipment is not a commercial-grade computer system;~~ it was designed originally for nuclear safety applications in Japan. Since it has been deployed in numerous non-safety nuclear applications in Japan and will be deployed in nuclear safety applications in Japan in the near future. All of this operating experience in Japan is directly applicable to expected nuclear safety applications in the US.~~

~~However, since the Japanese QA program to which MELTAC was designed, does not directly comply with 10CFR50 Appendix B, a description of the MELTAC Re-evaluation Program (MRP) is provided in Section 6.3. The MRP demonstrates that the design life cycle activities for MELTAC, including supplemental conformance activities, have resulted in a design that is equivalent to a design resulting from a 10CFR50 Appendix B program.~~

~~The MRP is a non-recurring activity applicable only to the MELTAC design life cycle, prior to US applications. All future MELTAC life cycle activities, including hardware and software design, manufacturing, testing, operations, maintenance and retirement, will be conducted under MELCO's App.B-based QAP.~~

DCD_07.01-45

47. BTP 7-19 Guidance on Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based I&C Systems

The MHI safety-related digital I&C systems utilize the MELCO safety-related digital I&C platform (ie. this Equipment). The MHI non-safety digital I&C systems utilize the MELCO non-safety digital I&C platform. The two MELCO platforms are essentially the same, however some QA aspects of design and manufacturing are not equivalent between safety and non-safety platforms. The Defense-in-Depth and Diversity Topical Report describes the functional diversity within the safety and non-safety I&C systems. The report also describes the methodology for coping with a common cause failure of all of these systems and provides and example of this methodology for one Design Basis Accident (DBA). Coping for all Design Basis Accidents (DBAs) is described in Plant Licensing Documentation.

48. BTP 7-21 Guidance on Digital Computer Real-Time Performance

The real-time performance for this Equipment conforms to this BTP. The method for determining response time performance for plant systems (including the digital platform) is described in the Safety I&C System Description and electrical independence between redundant safety divisions and between safety and non-safety divisions. Electrical independence is accomplished primarily through the use of fiber optic technology. Independence of electrical circuits is accomplished with isolators and physical separation or barriers, such as conduits. MELTAC components credited for physical, electrical, and functional isolations and independences are described in Section 4 (4.3.2.3, 4.3.3.2, 4.3.4.2) of this Technical Report. These components are used for interfaces between safety divisions and between safety and non-safety divisions, as described at the system level in MUAP-07004.

60. IEEE 420 1982 Design and Qualification of Class 1E Control Board, Panels and Racks.

Standard enclosures for this Equipment conform to this standard. These enclosures are described in this Technical Report. Equipment is clearly marked to identify safety-related division designations, as described in Section 6.2.4 Identification of Equipment. Other enclosures, including any deviations from this standard, are described in Plant Licensing Documentation.

61. IEEE 472 IEEE Guide for Surge Withstand Capability (SWC) Tests

Input/Output modules used within this Equipment conform to this standard. Conformance to surge withstand requirements is described in the EMC Qualification Report.

62. IEEE 494 1974 Method for identification of Documents Related to 1E Equipment.

The documentation for this Equipment conforms to this standard by having the term “Nuclear Safety-Related” applied on the face of each document and drawing that is provided to the licensee. ~~Generic documents and drawings used only for internal use by MELCO do not contain this designation.~~ DCD_07.01−30 DCD_07.01-45

63. IEEE 497 2002 Accident Monitoring Instrumentation for Nuclear Power Generating Stations

See conformance for RG 1.97.

64. IEEE 603 1991 Safety Systems for Nuclear Power Generating Stations

1998 version is currently not endorsed by NRC

This Equipment conforms to this standard, as augmented by RG 1.153, including key requirements for:

- Single failures
- Completion of Protective Action
- Quality
- Qualification

- Independence
- Testability
- Monitoring and Information
- Bypasses

Conformance is described in Sections 4 through 7. MUAP-07004 Appendix A provides a detailed conformance assessment at the system level.

65. IEEE 730 1989 Software Quality Assurance Plans

The Software Quality Assurance Plans are described in Section 6. ~~Common elements that do not depend on individual projects are described in [ ] for QAP Rev.1/Rev.2. QAP Rev.1/Rev.2, which applies to the original MELTAC platform that was developed in Japan, has been commercially dedicated for safety applications (see Item 46). These procedures were replaced by [ ], [ ], [ ] and [ ] to meet the requirements of 10 CFR 50 Appendix B. These~~ Detailed procedures governing this lifecycle activity are ~~part of~~ included in the App. B-based QAP which will be used specifically for US-APWR plants. Project-dependent individual elements are described in the Project Plan and the Software V&V Plan.

DCD_07.01-45

66. IEEE 828 1990 IEEE Standard for Software Configuration Management Plans

The software Configuration Management Plan is described in Section 6.1.5. ~~It is controlled by internal documents [ ] and [ ] for QAP Rev.1/Rev.2. QAP Rev.1/Rev.2, which applies to the original MELTAC platform that was developed in Japan, has been commercially dedicated for safety applications (see Item 46). These procedures were replaced by [ ] to meet the requirements of 10 CFR 50 Appendix B. This~~ Detailed procedure governing this lifecycle activity is ~~part of~~ included in the App. B-based QAP which will be used specifically for US-APWR plants.

DCD_07.01-45

67. IEEE 829 1983 Software Test Documentation

The software test documentation is described in Section 6.1.4. ~~It is controlled by internal documents [ ] and [ ] for QAP Rev.1/Rev.2. QAP Rev.1/Rev.2, which applies to the original MELTAC platform that was developed in Japan, has been commercially dedicated for safety applications (see Item 46). These procedures were replaced by [ ] and [ ] to meet the requirements of 10 CFR 50 Appendix B. These~~ Detailed procedures governing this lifecycle activity are ~~part of~~ included in the App. B-based QAP which will be used specifically for US-APWR plants.

DCD_07.01-45

68. IEEE 830 1993 IEEE Recommended Practice for Software Requirements Specifications

~~The software requirements~~ Software requirement specifications are documented in the Platform specification as an output of Requirement Phase ~~the "Safety System Digital Platform MELTAC-Nplus System Platform Specification",~~ which is described in Section 6.1.4.

DCD_07.01-45

69. IEEE 1008 1987 IEEE Standard for Software Unit Testing

Software unit testing is described in Section 6.1.4. ~~It is controlled by [ ] and [ ] for QAP Rev.1/Rev.2. QAP Rev.1/Rev.2, which applies to the original MELTAC platform that was developed in Japan, has been commercially dedicated for safety applications (see Item 46). These procedures were replaced by [ ] and [ ] to meet the requirements of 10 CFR 50 Appendix B. These~~ Detailed procedures governing this lifecycle activity are ~~part of~~ included in the App. B-based QAP which will be used specifically for US-APWR plants.

DCD_07 .01-45

70. IEEE 1012 1998 IEEE Standard for Software Verification and Validation Plans (2004 not yet endorsed by NRC)

Software V&V is described in Section 6.1.4. ~~It is controlled by [ ] for QAP Rev.1/Rev.2. QAP Rev.1/Rev.2, which applies to the original MELTAC platform that was developed in Japan, has been commercially dedicated for safety applications (see Item 46). These procedures were replaced by [ ] and [ ] to meet the requirements of 10 CFR 50 Appendix B. These~~ Detailed procedures governing this lifecycle activity are ~~part of~~ included in the App. B-based QAP which will be used specifically for US-APWR plants.

DCD_07 .01-45

71. IEEE 1016 1987 IEEE Recommended Practice for Software Design Descriptions

The software design requirement for t~~T~~he Software Design Description is documented in the Software Specifications as outputs of Design Phase ~~"Safety System Digital Platform MELTAC Nplus Software Specification",~~ which is described in Section 6.1.4.

DCD_07 .01-45

72. IEEE 1028 1997 IEEE Standard for Software Reviews and Audits

Software reviews and audits are described in Section 6.1. ~~Reviews and audits are controlled by [ ], [ ], and [ ] for QAP Rev.1/Rev.2. QAP Rev.1/Rev.2, which applies to the original MELTAC platform that was developed in Japan, has been commercially dedicated for safety applications (see Item 46). These procedures were replaced by [ ] to meet the requirements of 10 CFR 50 Appendix B. This~~ Detailed procedure governing this lifecycle activity is ~~part of~~ included in the App. B-based QAP which will be used specifically for US-APWR plants.

DCD_07 .01-45

73. IEEE 1042 1987 IEEE Guide To Software Configuration Management

Configuration Management is described in Section 6.1.5. ~~It is controlled by [ ] and [ ] for QAP Rev.1/Rev.2. QAP Rev.1/Rev.2, which applies to the original MELTAC platform that was developed in Japan, has been commercially dedicated for safety applications (see Item 46). These procedures were replaced by [ ] to meet the requirements of 10 CFR 50 Appendix B. This~~ Detailed procedure governing this lifecycle activity is ~~part of~~ included in the App. B-based QAP which will be used specifically for US-APWR plants.

DCD_07 .01-45

74. IEEE 1074 1995 IEEE Std for Developing Software Life Cycle Processes

1997 version not yet endorsed by NRC

The software life cycle process is described in Section 6. ~~It is controlled by [ ], [ ], [ ], and [ ] for QAP Rev.1/Rev.2. QAP Rev.1/Rev.2, which applies to the original MELTAC platform that was developed in Japan, has been commercially dedicated for safety applications (see Item 46). These procedures were replaced by [ ] and [ ] to meet the requirements of 10 CFR 50 Appendix B. These~~ Detailed procedures governing this lifecycle activity are ~~part of~~ included in the App. B-based QAP which will be used specifically for US-APWR plants. DCD_07.01-45

75. IEEE 497 2002 Accident Monitoring Instrumentation for Nuclear Power Generating Stations

See conformance for RG 1.97.

76. IEEE 896 1991 Standard For Futurebus+® - Logical and Physical Layers

The communication between Modules in the same Subsystem of the MELTAC platform conforms to this standard.

Other Industry Standards

77. ANS-10.4 1987 Guidelines for the Verification and Validation of Scientific and Engineering Computer Programs for the Nuclear Industry

The computer programs used to develop setpoints for this Equipment are described in the Safety I&C System Description and Design Process Technical Report for the US-APWR DCD.

78. ANSI C62.41 IEEE Recommended Practice on Surge Voltages in Low-Voltage AC Power Circuits

This Equipment conforms to the sections of this standard endorsed by RG 1.180.

79. ANSI C62.45 IEEE Guide on Surge Testing for Equipment Connected to Low-Voltage AC Power Circuits

This Equipment conforms to the sections of this standard endorsed by RG 1.180.

80. IEC 61000 Electromagnetic compatibility (Basic EMC publication)

This Equipment conforms to the following sections of this standard:

- IEC 61000-4-2: Testing and measurement techniques - Electrostatic discharge immunity tests. Basic EMC publication
- IEC 61000-4-4: Testing and measurement techniques - Electrical fast transient/burst immunity test. Basic EMC publication

- IEC 61000-4-5: Testing and measurement techniques - Surge immunity test
- IEC 61000-4-12: Testing and measurement techniques - Oscillatory waves immunity test.

81. ISA-S67.04 1994 Setpoints For Nuclear Safety-Related Instrumentation Used in Nuclear Power Plants DCD_07.01-30

See conformance to RG 1.105. The methodology used to develop setpoints for this Equipment is described in the Safety I&C System Description and Design Process Technical Report for the US-APWR DCD.

82. MIL-STD-461E Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment

This Equipment conforms to this standard as referenced in RG 1.180. This standard replaces MIL-STD-461D and MIL-STD-462D referenced in EPRI TR-102323.

83. ISO9001: 2000 International Organisation for Standardisation Quality Management Systems

~~MELCO original~~ The Quality Assurance program for the non-safety items conforms to this standard. DCD_07.01-45

Japanese Domestic Standards

84. JIS-C0704-1995 Insulation Test for Control Gear (in Japanese)

This standard is the defined as the Japanese Industrial Standard. The withstand voltage of this Equipment conforms to this standard.

85. JEC-210-1981 Control Circuit Terminal Test Voltage (in Japanese)

This standard is issued by Japanese Electrotechnical Committee. The Lightning impulse resistance of this Equipment conforms to this standard.

86. JEIDA-63-2000 Guideline for the Environmental Condition for the Industrial Information Processing and Control Equipment (in Japanese)

This standard is issued by Japan Electronics and Information Technology Industries Association. This Equipment conforms to the class B of this standard regarding dust and dirt tolerance.

87. JEAG-4101 Guidelines for Quality Assurance in Nuclear Power Plant (in Japanese)

This standard is the guidelines for the quality assurance in the nuclear power plant in Japan and issued by Japan Electric Association. This Equipment conforms to this standard.

4.1.2 Hardware Descriptions

4.1.2.1 CPU Chassis

There are several kinds of modules described in Table 4.1-3 in the CPU Chassis. This section describes each module.

DCD_07.01-45

Table 4.1-3 Module in the CPU Chassis

	Name	~~Model~~ Module Identifier	Function
Basic Function Module	CPU Module	PCPJ~~-31~~	• Executes basic software • Executes application software, including control computation processing
	System Management Module	PSMJ~~-31~~	• Communication between the redundant Subsystems • Communication with the MELTAC engineering tool. • Auxiliary DI and DO functions
Communication Module	Control Network I/F Module	PWNJ~~-31~~	Communication with the Control Network.
	Bus Master Module	PFBJ~~-31~~	• Communication with I/O • Data link communication with other Controllers This module has four communication channels.
Power Supply Module	CPU Power Supply Module	PPSJ~~-01~~ ~~PPSJ-11~~	Supplies power to the modules within the CPU chassis.
Display & Switch Module	Status Display & Switch Module	PPNJ~~-31~~	• Mode display LED • Subsystem Mode switch • Operation switch (described below) This module is only used in the redundant standby controller configuration.
	Status Display Module	~~PPNJ-32~~	• Mode display LED • Operation switch (described below) This module is used for the single controller configuration or the redundant parallel controller configuration.

~~(Note) Model numbers in this table represent current numbers at the time of this document revision. Model numbers will change as the product life cycle progresses. New models will retain the minimum functional features, performance specifications and reliability of current models.~~

4.1.2.1.1 CPU Module (PCPJ~~-31~~)

DCD_07.01-45

The CPU Module utilizes a 32-bit microprocessor, with enhanced speed due to the cache. This processor module is IEEE standard Futurebus+ compliant, and performs internal operations and data transmission with other modules (i.e. Bus Master Module, Control Network I/F Module and System Management Module) via Futurebus+.
The data transfer between the CPU Module and other modules is asynchronous. All modules have separate clocks.

This module utilizes F-ROM (Flash Electrically Erasable Programmable Read Only Memory) for storing the basic software, and F-ROM for storing the application software, such as logic symbol interconnections, setpoints and constants.
Specifications of the CPU Module are in Appendix A.1.

4.1.2.1.2 System Management Module (PSMJ~~-31~~)

DCD_07.01-45

The System Management Module monitors the status of the CPU Module and executes auxiliary controller functions that are not directly related to the CPU Module.

This module has the following functions:

- Auxiliary DI/DO for generating alarms such as fan failure.
- Ethernet interface for communicating with the MELTAC engineering tool.
- Transmits and receives the changeover signal for Redundant Subsystem configurations via a dedicated backplane bus, as shown in Figure 4.1-3. In addition, this module is provided with a 2-port memory data link used for that the Standby Mode Subsystem receives operation data from the Control Mode Subsystem.

Specifications of System Management Module are in Appendix A.2.

4.1.2.1.3 Bus Master Module (PFBJ~~-31~~)

DCD_07.01-45

The Bus Master Module has a 4 communication interface channels. Either of the following two functions can be defined for each channel.

- Communication with I/O ~~m~~Modules DCD_07.01−30
  This module is IEEE standard Futurebus+ compliant. It has 2-port memory, allowing the CPU Module to deliver process I/O data via Futurebus+. Each communication channel is capable of controlling 96 I/O ~~m~~Modules, enabling control of a maximum of 384 I/O ~~m~~Modules per Bus Master Module. DCD_07.01−30
- Data Link communication
  The Bus Master Module implements serial data link communication between controllers in separate safety divisions. The Bus Master Module employs 2-port memory to ensure communication functions do not disrupt deterministic CPU operation.
  Description of the Data Link is shown in Section 4.3.3.

Specifications of the Bus Master Module are in Appendix A.3.

4.1.2.1.4 Control Network I/F Module (PWNJ~~-31~~)

DCD_07.01-45

The Control Network I/F Module connects the Controller to the Control Network. This interface employs a Resilient Packet Ring (RPR) based on IEEE standard 802.17.

The Control Network is redundant using optical fiber as the communication medium. An optical switch unit enables optical bypass for system maintenance. The Control Network I/F Module employs 2-port memory to ensure communication functions do not disrupt deterministic CPU operation.
The description of the Control Network, including the Control Network I/F Module is shown in Section 4.3.2.

4.1.2.1.5 Status Display & Switch Module and Status Display Module (PPNJ~~-31~~)

DCD_07.01-45

~~The Status Display & Switch Module is used in a CPU Chassis configured for a Redundant Standby Controller. This module displays the mode and alarms of the Subsystems and provides the manual mode change over switch.~~ The Status Display & Switch Module and the Status Display Module are mounted in a CPU Chassis. The Status Display & Switch Module acts as a Redundant Standby Controller and the Status Display Module acts as a Redundant Parallel Controller or Single Controller. Both of these modules display the mode and alarms, and the Status Display & Switch Module also provides the manual mode change over switch.

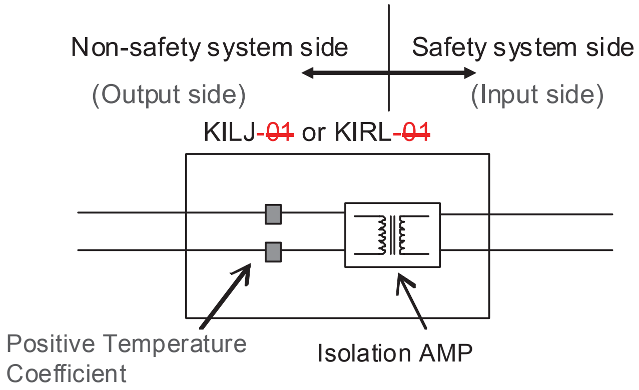
4.1.2.1.6 This section intentionally left blank ~~Status Display Module (PPNJ-32)~~

DCD_07.01-45

~~The Status Display Module is used in a CPU Chassis configured for a Redundant Parallel Controller or Single Controller. It is connected with the CPU Module by wiring on the back plane. This module displays the mode and alarms of the single Subsystems to which it is directly connected there is no connection with the other subsystems.~~

The Figure 4.1-8 shows the internal configuration diagram of the analog isolation modules KILJ~~-01~~ and KIRJ~~-01~~. For common mode faults, the input and output are electrically isolated by the isolation amplifier. The positive temperature coefficient device (e.g. PolySwitch TM) is used to limit overcurrent conditions for transverse mode faults. The positive temperature coefficient device raises its resistance value when it is heated by sustained overcurrent conditions.

DCD_07
.01-45

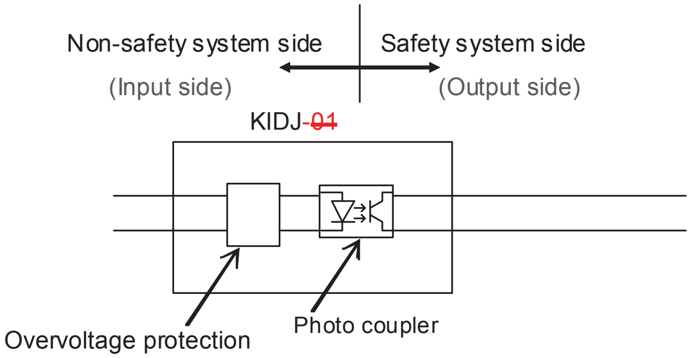


DCD_07
.01-45

Figure 4.1-8 The Internal Configuration Diagram of The Analog Isolation Modules

The Figure 4.1-9 shows the internal configuration diagram of the binary isolation module KIDJ~~-01~~. For common mode faults, the input and output are electrically isolated by a photo coupler. The over voltage protection circuit limits the current for transverse mode faults. The over voltage protection circuit consists of a transistor, FET, and high-resistance. The circuit converts to high resistance to restrict the current when a voltage that exceeds the FET gate voltage is supplied.

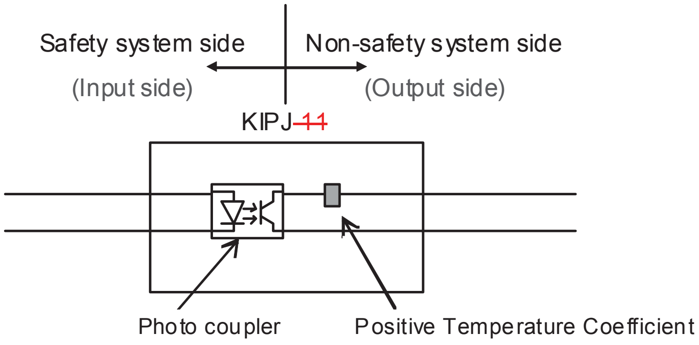
DCD_07
.01-45



DCD_07
.01-45

Figure 4.1-9 The Internal Configuration Diagram of The Digital Isolation Module

The Figure 4.1-10 shows the internal configuration diagram of pulse input isolation module KIPJ~~-11~~. The input and output are electrically isolated by a photo coupler. The positive temperature coefficient device (e.g. PolySwitch ^{TM}) is used to limit overcurrent. DCD_07.01-45



DCD_07.01-45

Figure 4.1-10 The Internal Configuration Diagram of The Pulse Input Isolation Module

KILJ~~-01~~,KIRJ~~-11~~ and KIDJ~~-01~~ were included in qualification testing for temperature and humidity, seismic and EMI described in Section 5. Isolation fault testing was conducted, as described in Section 5.5. The qualification tests for KIPJ~~-11~~ will be performed by the method as described in Section 5. DCD_07.01-45 DCD_07.01-45

Calibration of input circuit, output circuit and current limiting circuit is conducted for all modules during manufacturing. Functional input-output operation is also confirmed for all modules during production.

As shown in Figure 4.1-1, Figure 4.1-2, and Figure 4.1-3, inputs from sensors are input to the Distribution Module via the terminal unit. The Distribution Module distributes input signals to redundant I/O ~~m~~Modules. Output signals are also output via the Distribution Module.

The Distribution Module is used in accordance with the type of I/O ~~m~~Modules. Appendix A.6 shows the list of I/O ~~m~~Modules applicable to each Distribution Module. DCD_07.01−30

4.1.2.4 Power Interface Module

The Power Interface (PIF) Modules have the same I/O Bus interfaces as in the I/O M~~m~~odules. These modules receive output commands as the result of Subsystem operation, and control the power that drives the switchgears, solenoid valves, etc. for plant components. This module utilizes power semiconductor devices for controlling power. Therefore, periodic replacement is unnecessary in contrast to electro-mechanical relays. DCD_07 .01-30

The PIF Modules also receive inputs from external contacts (the status contacts of the components) and transmit component status signals to the Subsystem. The Power Interface Modules include Interposing Logic (IPL) sub-boards that control the components in direct response to external contact inputs, independent of the Subsystem output commands. There are several types of IPL sub-boards, for different types of plant components (eg. switchgears, solenoid valves, etc.). Each PIF is configured with the appropriate IPL sub-board for the component being controlled. The IPL is realized by discrete logic Integrated Circuits.

[

DCD_07 .01-30

DCD_07 .01-30

]

All currently available IPL sub-boards have been qualified, as described in Section 5. However, it is anticipated that new IPL sub-boards may be required for US applications, due to changes in plant process components, changes in DAS interfaces and changes in priority logic~~, compared to applications in Japan~~. New IPL sub-boards will maintain the same design process, qualification process, hardware technology and quality program as current IPL sub-boards. DCD_07 .01-45

The entire PIF module, including the Communications ~~I~~interface part is considered Class 1E. Therefore, the life cycle process for the development and maintenance of the firmware within the Communications ~~I~~interface part is the same as the firmware for all other MELTAC modules. During manufacturing and production, the PIF modules are all tested to confirm the soundness of communication operation, IPL logic operation, and output operation. DCD_07 .01-30 DCD_07 .01-30

Unlike electro-mechanical relays, the power semiconductor output of the PIF module does not degrade mechanically nor electrically and can be treated the same as any other general semiconductor device. Thus, the PIF modules are not considered to have any limitations in their expected service life. The components of the MELTAC platform that have a limited service life are identified in Section 7.5 Periodic Replacement Equipment (Parts) to Keep Reliability. The PIF is not included in this list.

4.1.2.6 Optical Switch

The Optical Switch is installed outside the CPU Chassis. It optically bypasses the Control Network communication line in the Control Network I/F Module during controller maintenance.

4.1.2.7 Fan Units

4.1.2.7.1 CPU Fan

The CPU Fan is installed on the top of the CPU Chassis to cool the modules within the CPU Chassis. It is equipped with a fan stop detection circuit which provides a contact signal to the System Management Module.

4.1.2.7.2 Door Fan Unit

The Door Fan Unit is installed at the top rear of the cabinet to cool internal cabinet components. It is equipped with a fan stop detection circuit which provides a contact signal to the System Management Module.

4.1.2.7.3 Power Supply Fan Units

The Power Supply Fan Units are installed at the bottom and the midsection on both the left- and right-hand sides of the cabinet to cool the power supplies, PS~~-1 and PS-2~~. It is equipped with a fan stop detection circuit which provides a contact signal to the System Management Module. DCD_07 .01-45

The fan stop detection circuit detects the decrease of fan rotation frequency by converting fan rotation frequency into a voltage pulse and monitoring the pulse length. If the pulse length reaches the length equivalent to the detected rotation frequency limit, the fan stop detection circuit de-energizes a relay, which generates a contact closing signal. Also, the same relay is deenergized if there is a power loss to the fan. Therefore, fan failure can be detected.

4.1.2.8 Power Supply Module

The Power Supply Modules convert the AC power supplied to the Chassis from two independent sources to DC power voltages suitable for the individual modules and units. Redundant Power Supply Modules are provided for CPU Chassis, I/O ~~m~~Modules, Isolation Modules, Power Interface Modules, E/O Converter Modules and fan units. DCD_07 .01−30

There are two types of Power Supply Modules. The CPU Power Supply (PS~~-1,~~ and PPSJ~~-01 and PPSJ-11~~) provides multiple outputs of +2.1VDC and +5VDC for the CPU Chassis. The I/O Power Supply (PS~~-2~~) provides +24VDC for I/O ~~m~~Modules, Isolation Modules, Power Interface Modules, E/O Converter Modules and fan units. DCD_07 .01-45 DCD_07 .01−30 DCD_07 .01-45

PPSJs~~-01 and PPSJ-11~~ are mounted in the CPU Chassis. These Power Supplies apply to the redundant parallel controller configuration. DCD_07 .01-45

PSs~~-1 and PS-2~~ are mounted outside of the chassis. These Power Supplies apply to the single controller configuration where the power supply is redundant for the CPU Chassis. PSs~~-1 and PS-2~~ are mounted on the panel cut parts that are set right and left of the cabinet chassis as shown in the Figure 4.1-11, Figure 4.1-12 and Figure 4.1-13. This mounting location was selected, rather than mounting them within the chassis for three reasons (1) this leaves space in the chassis for additional modules, (2) external mounting allows DC power to be supplied to the chassis from two redundant Power Supply Modules, (3) this location keeps the heat from the power supplies away from the modules, thereby improving module reliability.

DCD_07.01-45

Both types of Power Supply Modules are equipped with overvoltage protection that deenergizes the output when the output voltage exceeds a setting, and overcurrent protection that lowers the output voltage level when an overload or output short-circuit occurs. Both types of Power Supply Modules also provide a contact output alarm signal when an output shut-down occurs.

For a redundant standby controller configuration and a redundant parallel controller configuration, each Subsystem monitors the output condition of the other Subsystem’s Power Supply Module. For a redundant standby controller configuration, when there is a shutdown of the power supply module of the Subsystem in the Control Mode, the Subsystem in the Standby Mode shifts to the Control Mode. When there is a shutdown of the power supply module of the Subsystem in the Standby Mode, the Subsystem in the Control Mode generates an “Alarm”. For a redundant parallel controller configuration, each Subsystem warns “Alarm" if there is a shutdown of the power supply module of the other Subsystem.

The CPU Power Supply Module is also equipped with AC power input monitoring. When the AC power input is lost, it is detected by the AC power reduction detection circuit within the power supply, and an alarm signal is output to the CPU Module. When the CPU Module receives an alarm signal for loss of AC power from its own Subsystem’s Power Supply Module, the CPU Module shifts to the “Failure" Mode before the Power Supply Module output voltage level becomes lower than the operable voltage of the CPU Module.

For a redundant standby controller configuration, if the AC power input for the Subsystem in the Control Mode is lost, the Subsystem shifts to the “Failure” Mode, then the Power Supply Module outputs shuts down. The Subsystem in the Standby Mode shifts to the Control Mode by detecting a failure or a shutdown of the power supply module of the other Subsystem.

Specifications of the Power Supply Modules are in Appendix A.9.

DCD_07
.01-45

Figure 4.1-12 Cabinet External Dimensions and Rack Up, Typical Sample A

DCD_07.01-45

Figure 4.1-13 Cabinet External Dimensions and Rack Up, Typical Sample B

]

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. ~~Currently, the subsystem does not transfer to Failure, Alarm, or I/O Alarm and does not give an alarm. However, the MELTAC basic software will be modified to add an I/O Alarm for this condition. This modification is being executed as a design change under the App.B QAP (see Section 6), because this I/O Alarm was not required by the original MELTAC specification.~~ DCD_07.01-45

4.2.2.2 Application Software and MELTAC Engineering Tool

[

DCD_07
.01-45

]

4.2.3 Self-Diagnosis

[

MIC-03-07-00008

DCD_07.01-45

]

[

DCD_07 .01−30

DCD_07 .01−30

]

(4) Conformance summary to ISG-04

The conformance of ISG-04 is shown in MELTAC platform ISG-04 Conformance Analysis (~~JEXU-1015-1009~~MUAP-13018) and Appendix D of this technical report. DCD_07 .01-45

4.3.3.3 Isolation

The isolation method is basically the same as for the Control Network.
However the Data Link communication interface is implemented in the Bus Master Modules and the communication is unidirectional.

The physical, electrical, and functional isolation, based on the above figure, is as described below.

a) Physical Separation
The E/O converter module of the data link allows for distance of 1Kmeters between sending and receiving controllers. This allows the controllers to be geographically separated into separate I&C equipment rooms. For example for the PSMS of the US-APWR, the configuration of controllers for each train is described in MUAP-07004.

b) Electrical Isolation
The MELTAC platform uses fiber optics and optical to electrical converters (E/O Converter) to ensure electric Isolation. The optical communication circuit is shown in Figure 4.3-15.

c) Communication Isolation
[

DCD_07 .01-45

]

MIC-03-07-00008

DCD_07.01-45

]

(3) Conformance to ISG-04

The conformance of ISG-04 is shown in MELTAC platform ISG-04 Conformance Analysis (~~JEXU-1015-1009~~ MUAP-13018) and Appendix D of this technical report.

DCD_07.01-45

4.5 Control of Access

[

]

4.5.1 Control of Access for Hardware

[

]

4.5.2 Control of Access for Software

[

DCD_07.01-45

]

5.0 ENVIRONMENTAL, SEISMIC, ELECTROMAGNETIC AND ISOLATION QUALIFICATION

This section describes environmental, seismic, electromagnetic, surge withstand capability, electrostatic discharge and isolation qualifications of MELTAC platform.
~~This Section describes the method and the result of testing conducted for MELTAC modules.~~

~~If any module is updated, and it is determined that qualification re-testing is required by the evaluations conducted in accordance with Section 6.2.3, the module will be tested with the same method. The same method and acceptance criteria will also be used for any new MELTAC modules.~~

DCD_07.01-45

Table 5.1-1 shows the Regulatory requirements and acceptance criteria for each test.

DCD_07.01-45

Table 5.1-1 Regulatory Requirements and Reference to Acceptance Criteria for Each Test

Test item	Regulatory requirement	Reference to Acceptance Criteria
Environmental test	RG1.89	System level test: 5.1.2.1 Module level test: 5.1.2.2
Seismic test	RG1.100(IEEE 344 -2004)	Cabinet test: 5.2.2.1 Module level test: 5.2.2.2
Electromagnetic test	RG1.180	Conducted Emissions, High Frequency (CE102) Test : 5.3.2.1 Radiated Emissions, Magnetic Field (RE101) Test: 5.3.2.2 Radiated Emission, Electric Field (RE102) Test: 5.3.2.3 Conducted Susceptibility, Low Frequency (CS101) Test for Power Leads: 5.3.2.4 Conducted Susceptibility, High Frequency (CS114) Test for Power Leads: 5.3.2.5 Conducted Susceptibility, High Frequency (CS114) Test for Signal Leads: 5.3.2.6 Conducted Susceptibility, Bulk Cable Injection, Impulse Excitation (CS115) Test: 5.3.2.7 Conducted Susceptibility, Damped Sinusoidal Transients (CS116) Test: 5.3.2.8 Radiated Susceptibility, Electric Field (RS103) Test: 5.3.2.9
Surge withstand capability test	IEC 61000-4-12 IEC 61000-4-5 IEC 61000-4-4	5.3.2.10 Surge Withstand Capability, Ring Wave Test 5.3.2.11 Surge Withstand Capability, Combination Wave Test 5.3.2.12 Surge Withstand Capability, Electrically Fast Transients/bursts Test
Electrostatic discharge test	IEC 61000-4-2	5.4
Isolation test	RG1.75(IEEEStd 384-1992)	5.5

The overview of tests, test method, acceptance criteria, and test result conducted for the MELTAC modules are provided in the subsections 5.1 through 5.5. These existing tests are taken as design information which demonstrates that the MELTAC Platform environment specifications (see 4.1.1.4) are feasible designs in accordance with the Regulatory Requirements in Table 5.1-1.
~~Environmental and seismic qualifications have been verified by the tests described in Section 5.1 and 5.2, respectively. Section 5.3 describes Electromagnetic compatibility (EMC) tests. Section 5.4 describes electrostatic discharge (ESD) tests. Environmental, seismic, EMC and ESD tests have been completed. The EMC acceptance criteria are described in this Technical Reports. The results of Environmental test, Seismic test and EMC test are presented in the following test reports.~~
~~"Environmental Test Summary Report for the MELTAC Platform (JEXU-3300-2160)"~~
~~"Seismic Test Summary Report for the MELTAC Platform (JEXU-3300-2161)"~~
~~"EMC Qualification Test Summary Report for the MELTAC Platform (JEXU-1016-0022)"~~
These existing test results, which will be documented in test reports, will also be confirmed through an ITAAC to verify testing for MELTAC platform.

DCD_07.01-45

5.1 Environmental Test

5.1.1 Environmental Specification ~~and Outline of Test~~

DCD_07.01-45

The environment specifications of the MELTAC platform are shown in Section 4.1.1.4. The MELTAC platform is designed so as to continue operating without loss of functions even under the abnormal environmental conditions (temperature, humidity) of an assumed accident.

The MELTAC platform system environmental test was performed in a cabinet equipped with components of the platform. All modules, including modules that were not included in the system environmental test, were further subjected to an individual module environmental test.

Since the system environmental test, some new modules have been developed, and several modules included in the system test have been modified. All of these new or modified modules have undergone module environmental tests.

5.1.2 Contents of Environmental Test

5.1.2.1 System Level Environmental Test

The MELTAC modules mounted inside the cabinet for the system environmental tests are as follows:

- CPU Module
- System Management Module
- Bus Master Module
- Control Network I/F Module
- Touch Panel I/F Module
- Status Display & Switch Module
- Status Display Module
- Repeater Modules
- Analog Input Modules

- Analog Output Modules
- Digital Input Modules
- Digital Output Modules
- E/O Converter Modules
- Power Interface Module
- Distribution Modules
- Power Supply Modules

(1)Method

DCD_07.01-45

These modules were selected as those that were deemed necessary to confirm the safety function of a typical Reactor Protection System, including the bi-stable operation and the trip signal output.

For the system environmental tests a cabinet equipped with MELTAC modules interconnected and powered in a test configuration was placed inside a thermostatic chamber. The test configuration results in the worst case expected temperature rise across the module chassis and across the cabinet. Before, during, and after each test it was confirmed that there were no equipment failures or abnormal functions such as erroneous bi-stable operation or erroneous trip signal output, etc. To determine whether any function abnormalities occurred, the output signals were recorded on a chart recorder to capture any erroneous output during the test. In addition, the self-diagnosis function of the MELTAC platform detected no abnormalities during the test.

(2)Acceptance criteria and result

DCD_07.01-45

For the system environmental test, the correct performance of the system was verified during the following tests.

[

5.1.2.2 Module Environmental Test

[

DCD_07
.01-45

DCD_07
.01-45

DCD_07
.01−30

DCD_07
.01−30

DCD_07
.01−30

5.2 Seismic Test

5.2.1 Overview

The MELTAC platform is designed to maintain structural integrity and functional integrity during and after a design basis earthquake. Seismic testing is part of the overall system seismic qualification which ensures there is no negative affect on the safety protection function of the equipment even if an earthquake occurs during plant operation.

The Cabinet Seismic Resistance Test was performed with a MELTAC Cabinet fully loaded with MELTAC components. For the Cabinet Seismic Resistance Test, a test specimen was prepared that is typical of a safety protection system application. The test specimen was vibration-excited on a large shaker table. During the test the physical integrity and vibration characteristics of the cabinet were confirmed. All system functions were also confirmed before, during and after the excitation. For the input acceleration used for the Cabinet Seismic Resistance Test, a floor response spectrum was selected that is high enough to cover the range of power plants in Japan.
There are no components with aging mechanisms that would affect the equipment’s susceptibility to failure during these seismic tests. Therefore there was no special age related preconditioning for these tests.
The test facility for the Cabinet Seismic Resistance Test is a famous facility for conducting seismic test of large equipment for nuclear power plants. Tests were conducted on a 3-Direction large shaker table.

In addition, the Module Seismic Resistance Tests were performed for major components. For module types where structure and positions of parts are the same, and other differences would have no impact on seismic capability, such as differences in input ranges, one typical module type was selected. Modules were mounted in chassis for the Module Seismic Resistance Test. For the Module Seismic Resistance Tests, the cabinet maximum response ratio was analyzed from the cabinet seismic resistance test. The input acceleration for the Cabinet Seismic Resistance Test was multiplied by the maximum response ratio and additional margin is added to obtain the input acceleration for the chassis.
Chassis loaded with MELTAC modules were vibration-excited with this input acceleration. During and after this testing, the physical and functional integrity of the module is confirmed.

The Safety I&C System Description and Design Process Technical Report for the US-APWR DCD describes the method used to ensure the seismic testing levels bound the levels the equipment will be exposed to in actual in-plant applications.

5.2.2 Seismic Resistance Test

5.2.2.1 Cabinet Seismic Resistance Test

For the Cabinet Seismic Resistance Test, a specimen that simulates a fully loaded safety protection system cabinet was prepared. The loading configuration represents the worst case expected stress on internal mounting hardware. ~~The configuration of the Cabinet Seismic Resistance Test specimen is shown in the Seismic Qualification Test Report JEXU-1002-1080.~~ DCD_07.01-45
The major MELTAC components located inside the cabinet are as follows:

[

DCD_07.01-45

DCD_07.01-45

DCD_07.01-45

DCD_07.01-45

DCD_07.01-45

DCD_07.01-45

]

5.2.2.2 Module Seismic Resistance Test

For the Module Seismic Resistance Test, physical and functional integrity was confirmed by testing individual modules or chassis loaded with multiple modules. The following modules were included in these tests:

- CPU Module
- System Management Module
- Bus Master Module
- Control Network I/F Module
- Touch Panel I/F Module
- FMU Module
- Status Display & Switch Module
- Status Display Modules
- Repeater Modules
- I/O M~~m~~odules
- Power Interface Module
- Isolation Modules
- E/O converter Modules
- Distribution Modules
- Power Supply Modules
- Safety VDU Panel
- Optical Switch
- Ethernet Optical Isolation Device

DCD_07
.01−30

[

DCD_07
.01-45

DCD_07
.01-45

DCD_07
.01-45

DCD_07
.01-45

]

The satisfactory performance of the equipment is confirmed by means of a recorder connected to the digital and analog output modules. Digital input and the analog input levels are automatically monitored by the application software which displays an alarm in case of an error.

The occurrence of any system function abnormality, data communication abnormality, and equipment failure is confirmed by referring to the results of the self-diagnosis function of the MELTAC platform.

~~“EMC Qualification Test Summary Report for the MELTAC Platform" provides the results of the EMI/RFI emission and susceptibility tests, and surge withstand capability tests. The test report describes any test anomalies, any special plant conditions needed to meet the acceptance criteria, or any operational or interface restrictions needed to accommodate conditions where the acceptance criteria has not been met.~~ DCD_07.01-45

5.3.1 Test Configuration

The Equipment Under Test (EUT) is comprised of two cabinets - the CPU cabinet fitted with the CPU Chassis, E/O converter Chassis, Optical Switch and Power Supply modules, and the I/O cabinet fitted with the I/O Chassis, Power Interface Chassis, Isolation Chassis and Power Supply modules. In order to attain the cabinet layout similar to the actual ordinary cabinet layout, the two cabinets are placed side by side with no space in between, thus securing the integral configuration. The cabinets were tested with the doors open to duplicate worst case conditions expected during testing and maintenance. The EUT also includes the safety VDU panel that is placed separately from the two cabinets.

The safety VDU panel is supplied power from the CPU cabinet and connected with the power cable and the signal cable.

The EUT included the module types required for safety protection system applications, as shown in Table 5.3-1.

For module types where differences will have no impact on EMC test results, such as NO vs NC contacts or differences in input ranges, one typical module type was selected.

The AC power to the EUT is supplied from two systems - main and standby -. Since within the EUT both power sources have the same configuration, the tests for AC input power line of CE102, CS101, CS114 and IEC61000-4 is performed for one AC power cable.

Table 5.3-1 MELTAC Modules for the EMC Test

Module	~~Model~~ Module Identifier
CPU Module	PCPJ~~-11 (*)~~
System Management Module	PSMJ~~-11 (*)~~
Bus Master Module	PFBJ~~-11 (*)~~
Control Network I/F Module	PWNJ~~-01 (*)~~
Touch Panel I/F Module	PRSJ~~-01 (*)~~
FMU Module	PFDJ~~-01 (*)~~
Status Display Module	PPNJ~~-12 (*)~~
Repeater Module	MRPJ~~-01~~
~~Repeater Module~~	~~MRPJ-02~~
~~Repeater Module~~	~~MRPJ-21~~
Analog Input Module (Current input)	MLPJ~~-01 (*)~~
~~Analog Input Module (Current input for automatic testing)~~	~~MLPJ-02 (*)~~
Analog Input Module (RTD input)	MRTJ~~-34 (*)~~
~~Analog Input Module (RTD input for automatic testing)~~	~~MRTJ-61 (*)~~
Analog Output Module (Current output)	MAOJ~~-01 (*)~~
Analog Output Module (Voltage output)	MVOJ~~-01 (*)~~
Digital Input Module (Contact input)	MDIJ~~-04~~
~~Digital Input Module (Contact input for automatic testing)~~	~~MDIJ-06~~
Digital Input Module (Contact input for redundant parallel controller)	MDIJ~~-62~~
Digital Output Module (Relay contact output)	MDOJ~~-03~~
Digital Output Module (Relay contact output for redundant parallel controller)	MDOJ~~-61~~
Digital Output Module (Semiconductor output)	MDOJ~~-22~~
Isolation Module (Current input, Current/Voltage output)	KILJ~~-01~~
Isolation Module (RTD 4line type input, Current/Voltage output)	KIRJ~~-01~~
Isolation Module (Contact input, Semiconductor output)	KIDJ~~-01~~
Power Interface Module	DPOJ~~-21~~
E/O Converter Module (RS485)	MEOJ~~-02~~
E/O Converter Module (RS232C)	MEOJ~~-11~~
CPU Power Supply Module	PS~~-1~~
I/O Power Supply Module	PS~~-2~~
CPU Power Supply Module (Small capacity type)	PPSJ~~-01~~
CPU Power Supply Module (Large capacity type)	PPSJ~~-11~~
CPU Fan	814JND
Door Fan	815JND
Power Supply Fan	503AH0HE
Safety VDU Panel	T10DHA229
Optical Switch	RJMA~~-02~~

DCD_07.01-45

~~(NOTE) This table identifies the modules included in the EUT for the EMC qualification testing originally conducted for MELTAC. EMC qualification testing will be repeated using an EUT configured with the modules identified in Table 4.1-3; these modules will replace the modules identified by "*" in this table. The same method and acceptance criteria will apply.~~

5.3.2 Description of Tests

5.3.2.1 Conducted Emissions, High Frequency (CE102) Test

The test is performed according to the method set forth in MIL-STD-461E, as follows:

a) Method
The conducted emission from the input power lead cable of the EUT is measured to confirm that the electromagnetic conducted emission from the EUT does not exceed the specified value.

b) Test Subject
The test subject is the AC input power lead cable including return and the ground cable of the EUT.

[

DCD_07 .01-45

]

5.3.2.2 Radiated Emissions, Magnetic Field (RE101) Test

The test is performed according to the method set forth in MIL-STD-461E, as follows:

a) Method
A loop sensor is placed on the surface of the object EUT to measure and confirmed that the magnetic field radiated emission from the EUT does not exceed the specified value.

b) Test Subject
The test subjects are the EUT enclosure, the electrical cable interface and the safety VDU panel. The four surfaces are scanned in 360 degrees with the loop sensor at positions at the center of the location (height) where the module is mounted.

[

]

5.3.2.3 Radiated Emission, Electric Field (RE102) Test

The test is performed according to the method set forth in MIL-STD-461E, as follows:

a) Method
Antennas are placed at the position specified for each frequency range from the border of the setup environment including the interface cable in order to confirm that the electric field radiated emission from the EUT does not exceed the specified value.

b) Test Subject

The test subjects are the EUT enclosure, the all interface cables and the safety VDU panel.

[

DCD_07.01-45

]

5.3.2.4 Conducted Susceptibility, Low Frequency (CS101) Test for Power Leads

According to section 4 of RG1.180, the CS101 test is mentioned as the MIL-STD-461E test method that can be applied as the conducted EMI/RFI susceptibility power leads. This test method is not applied to the signal lead.
The test is performed according to the method set forth in MIL-STD-461E, as follows:

a) Method

Confirm that the EUT can withstand the signal connected to the AC input power lead.

b) Test Subject

The test subject is AC input power lead to the EUT.

[

DCD_07.01-45

]

5.3.2.5 Conducted Susceptibility, High Frequency (CS114) Test for Power Leads

The CS114 test is applicable to all interconnecting leads including the power leads of the EUT. This section describes the CS114 test that is applied to the power and control lines described in section 4.1.2 of RG1.180.
The test is performed according to the method set forth in MIL-STD-461E, as follows:

a) Method

Confirm that the EUT can withstand the RF signals coupled onto the EUT associated cabling.

b) Test Subject

One each of the AC input power cable and the control cables (input and output cables of the Digital I/O M~~m~~odules and Power Interface Module) to the EUT DCD_07.01−30

[

DCD_07.01-45

]

5.3.2.6 Conducted Susceptibility, High Frequency (CS114) Test for Signal Leads

The CS114 test is applicable to all interconnecting leads including the power leads of the EUT. This section describes the CS114 test that is applied to the signal line described in section 4.2 of RG1.180.
The test is performed according to the method set forth in MIL-STD-461E, as follows:

a) Method
Confirm that the EUT can withstand the RF signals coupled onto the EUT associated cabling.

b) Test Subject
One each of the signal cables (input and output cables of the Analog I/O M~~m~~odules, the Isolation Modules and the RGB cables) to the EUT DCD_07 .01−30

[

DCD_07 .01-45

]

5.3.2.7 Conducted Susceptibility, Bulk Cable Injection, Impulse Excitation (CS115) Test

According to section 4.2 of RG1.180, the CS115 test is mentioned as the MIL-STD-461E test method that can be applied as the conducted EMI/RFI susceptibility test along the power leads for the interconnecting signal leads. This test method is not applied to the power lead.
The test is performed according to the method set forth in MIL-STD-461E as follows:

a) Method
Confirm that the EUT can withstand the impulse signals coupled onto the EUT associated cabling.

b) Test Subject
One each of the signal cables (input and output cables of the Analog I/O M~~m~~odules, the Digital I/O M~~m~~odules, Power I~~i~~nterface Module, the Isolation Modules and the RGB cables) to the EUT DCD_07 .01−30

[

DCD_07 .01-45

]

5.3.2.8 Conducted Susceptibility, Damped Sinusoidal Transients (CS116) Test

According to section 4.2 of RG1.180, the CS116 test is mentioned as the MIL-STD-461E test method that can be applied as the conducted EMI/RFI susceptibility test along the power cables. This test method is not applied to the power lead.
The test is performed according to the method set forth in MIL-STD-461E as follows:

a) Method
Confirm that the EUT can withstand the damped sinusoidal transients coupled onto the EUT associated cabling.

b) Test Subject
One each of the signal cables (input and output cables of the Analog I/O M~~m~~odules, the Digital I/O M~~m~~odules, Power Interface Module, the Isolation Modules and the RGB cables) to the EUT DCD_07.01–30

[

DCD_07.01-45

]

5.3.2.9 Radiated Susceptibility, Electric Field (RS103) Test

The test is performed according to the method set forth in MIL-STD-461E as follows:

a) Method
Confirm that the EUT can withstand the electric field emitted from the antenna.

b) Test Subject
The test subjects are the EUT enclosure, the all interface cables and the safety VDU panel. Since the EUT enclosure is placed on the floor as in actual plant conditions, and, since its height measures 7.55 ft (2300 mm), the direction of emission of the radiated electric field to the EUT enclosure is in 4 horizontal directions. The top and the bottom parts are not likely to be affected by the electric field.

[

DCD_07.01-45

]

5.3.2.10 Surge Withstand Capability, Ring Wave Test

DCD_07 .01-45

The test is performed according to the method set forth in IEC61000-4-12 as follows. For the withstand voltage of the test, the B Medium Exposure is selected out of the location categories described in IEEE Std C62.41-1991, and the corresponding surge voltage level is applied.

a) Method
Confirm that the EUT withstands the transient damped phenomenon (Ring Wave) generated by the low-voltage power network applied to the input power lead cable.

b) Test Subject
The test subject is the AC input power lead to the EUT.

[

DCD_07 .01-45

]

5.3.2.11 Surge Withstand Capability, Combination Wave Test

DCD_07 .01-45

The test is performed according to the method set forth in IEC61000-4-5 as follows. For the withstand voltage of the test, the B Medium Exposure was selected out of the location categories described in IEEE Std C62.41-1991, and the according surge level was applied.

a) Method
Confirm that the EUT withstands the unidirectional surge generated by the over-voltage due to the transient phenomenon of switching and lightning applied to the input power lead cable.

b) Test Subject
The test subject is the AC input power lead to the EUT.

[

DCD_07 .01-45

]

5.3.2.12 Surge Withstand Capability, Electrically Fast Transients/bursts Test

DCD_07 .01-45

The test is performed according to the method set forth in IEC61000-4-4 as follows. For the withstand voltage of the test, the B Medium Exposure was selected out of the location categories described in IEEE Std C62.41-1991, and the according surge voltage level was applied.

a) Method
Confirm that the EUT withstands the electrical fast transient/burst: EFT/B applied to the input power lead cable.

b) Test Subject
The test subject is the AC input power lead to the EUT.

[

DCD_07
.01-45

]

DCD_07.01-45

]

5.5 Isolation Test

[

DCD_07
.01-45

DCD_07
.01-45
DCD_07
.01−30

DCD_07
.01-45
DCD_07
.01−30

]

DCD_07.01-45

DCD_07.01-30

Figure 5.5-1 Isolation Test Configuration of KILJ~~-01~~ for Transverse Mode Faults

DCD_07.01-45

DCD_07.01-30

Figure 5.5-2 Isolation Test Configuration of KILJ~~-01~~ for Common Mode Faults

DCD_07.01-45

DCD_07.01-30

Figure 5.5-3 Isolation Test Configuration of KIDJ~~-01~~ for Transverse Mode Faults

DCD_07.01-45

DCD_07.01-30

Figure 5.5-4 Isolation Test Configuration of KIDJ~~-01~~ for Common Mode Faults

[

DCD_07.01-45

DCD_07.01-45

DCD_07.01-45

]

6.0 LIFE CYCLE

This section describes the lifecycle process for the Basic components (basic software and hardware) of the MELTAC Platform that meets all requirements of 10CFR50 Appendix B, referred to as the App.B-based QAP. The App.B-based QAP is a quality requirement from the US-APWR DCD. The application software lifecycle is described in the US-APWR SPM “Software Program Manual, MUAP-07017” which applies to project that use the MELTAC platform. DCD_07.01-45
The App.B-based QAP also includes the requirements of NUREG-800 BTP7-14, regarding the software lifecycle process. The generic software lifecycle plans of the MELTAC platform and the summary of each process required by BTP7-14 are provided in Table 6.1-1 and Section 6.1.

The MELTAC platform specification and software development process conform to the requirements of RG1.152. Section 6.1.6 describes the management of the Secure Development Environment that is maintained for the MELTAC platform.
Section 6.2 describes the lifecycle management of the MELTAC platform.
Section 6.5 describes the lifecycle of the MELTAC Engineering Tool (MELENS).

~~In 2006, MELCO started the activities to apply MELTAC as a digital platform for Safety Systems in US nuclear facilities. At that time MELCO assessed the original QAP and the original MELTAC development process for conformance to US requirements. A deficiency regarding the IV&V required in IEEE 7-4.3.2 was identified. To compensate for this deficiency MELCO added assessment and IV&V procedures and developed [ ] which invoked those procedures. In accordance with [ ], MELCO conducted assessments of the existing Software and related documents during the period 2006-2007. These assessments resulted in additional IV&V for some software, in accordance with [ ]. This reassessment and added IV&V program is referred to as the original US Conformance Program (UCP)~~.
~~[~~

DCD_07
.01-45

~~]~~

~~The development of the [ ] is described in Section 6.3.1.~~

~~The “MELTAC Platform Basic Software Program Manual (SPM)” [ ] provides the generic plans that are followed under the [ ] for all activities related to all future activities for the MELTAC basic software life cycle. This document is applicable to any design modifications to the current MELTAC basic software to accommodate any product deficiencies and any product enhancements, and to any new MELTAC product development. The life cycle processes described in Section 6.1.3 through 6.1.12 and Section 6.2 establish the minimum requirements for the lifecycle specified in the [ ]. To preclude the need for any additional post development assessments, the [ ] includes the requirements used for the UCP described in Section 6.1.7.~~

~~[~~

~~]~~

~~Section 6.4 describes the assessment for the conformance of MELTAC to BTP 7-14.~~

~~Section 6.1 describes the lifecycle of MELTAC based on [ ].~~

~~Section 6.1.1 and 6.1.2 describes the overview of MELCO’s QA program for the current MELTAC basic software, [ ].~~

~~Section 6.1.3 through 6.1.6 describes the original design process lifecycle of MELTAC.~~

~~Section 6.1.7 describes the original UCP conducted from 2006 to 2007, [ ], and the expanded UCP conducted from 2009 to 2010, [ ].~~

~~Section 6.1.8 through 6.1.11 describes the lifecycle of MELTAC after its development phase, based on [ ].~~

~~Section 6.1.12 describes the MELTAC software safety analysis for the current MELTAC basic software, [ ].~~

~~Section 6.2 describes the quality record management, failure management, and identification of MELTAC. This section is applicable to [ ].~~

~~Sections 6.1.3 through 6.1.12 and 6.2 are applicable to the current MELTAC platform. The processes defined in these sections established the basis for the assessment of the original MELTAC development conducted in the MRP, which is described in Section 6.3.~~

DCD_07.01-45

~~The life cycle requirements described in Sections 6.1.3 through 6.1.12 and 6.2, establish the minimum requirements for the "MELTAC Platform Basic Software Program Manual (SPM)" [ ], which is used to manage the MELTAC software life cycle under the [ ].~~

6.1 MELTAC platform Life Cycle ~~Process~~Plan and Activities

DCD_07.01-45

~~This section describes key elements of the lifecycle process for the Basic components (software and hardware) of the MELTAC platform, based on [ ]. This section also includes the assessment of the original MELTAC development (prior to [ ]), which was also conducted under [ ].~~

~~The life cycle processes for [ ] establish the minimum requirements for the processes defined in the “MELTAC Platform Basic Software Program Manual (SPM)” [ ], which is used to manage the MELTAC software life cycle under the [ ].~~

The table below summarizes the summary of the MELTAC Platform Basic Software lifecycle plans or activities.

DCD_07.01-45

DCD_07.01-45

DCD_07.01-45

DCD_07.01-45

DCD_07
.01-45

DCD_07
.01-45

DCD_07.01-45

DCD_07
.01-45

6.1.1 This section intentionally left blank ~~Overview of the MELTAC Quality Assurance Program~~

DCD_07.01-45

~~As described in Section 7.1, the MELTAC platform has accumulated many years of positive performance records in various non-safety system applications such as the Plant Control and Monitoring System in nuclear plants operating in Japan. Based on its excellent performance in numerous non-safety applications, the MELTAC platform has been applied to all plant systems non-safety and safety in one of the Japanese nuclear plants under construction. These systems were shipped to the site.~~

~~The original quality assurance program (referred to as Original QAP) used for the MELTAC platform development was based on the Japanese Standard JEAG4101 and ISO9001. Since MELCO planned to apply the platform to safety systems in US nuclear facilities, the following quality assurance procedures were adopted in [ ], "NPD Procedure [ ]: Safety System Digital Platform Quality Assurance Program", hence forth referred to as [ ]. "NPD Procedure [ ]: Safety System Digital Platform Cyber Security Program", hence forth referred to as [ ], and "NPD Procedure [ ]: Safety System Digital Platform Software V&V Procedures", hence forth referred to as [ ].~~

~~Unless specifically noted, procedures applicable to software encompass all MELTAC basic software and firmware, regardless of which module or media that software may reside. These procedures address all requirements of IEEE7-4.3.2-2003, including the applicable Regulatory Guides and IEEE software standards. In addition, 10CFR Part 50 Appendix B was used as a guideline. The requirements of these quality assurance procedures are described in the Sections below.~~

~~[~~

~~]~~

~~Table 6.1-1 QA Procedures~~

DCD_
07-14
BTP-46
DCD_07
.01-45

~~[~~

DCD_
07-14
BTP-46
DCD_07
.01-45

~~]~~

~~Platform designs (hardware or software) developed prior to the [ ] (referred to as Existing Platform) will be reused for US nuclear applications. The Original QAP and records of the Existing Platform have been assessed against the [ ] procedures, to ensure suitable quality of the Existing Platform. This assessment, which was conducted under [ ], is referred to as the US Conformance Program (UCP). The result of the UCP showed the development process for the Existing Platform conformed to [ ] except the independent V&V requirement and other minor deficiencies. The MRP described in Section 6.3.1, provided an additional assessment conducted under the App. B-based QAP, using the guidance of EPRI-TR106439 and EPRI TR-107330.~~

DCD_07
.01-45

~~Therefore MELCO developed the "MELTAC US Conformance Program" (UCP), which is the combination of the corrective actions taken to compensate for differences between the Original QAP and [ ], and the assessment of the developed software by the independent V&V Team. The detail is described in Section 6.1.7.~~

~~The requirements of [ ] are described in the following sections:~~

- ~~Quality Assurance (6.1.2)~~

- ~~Management (6.1.3)~~

DCD_07.01-45

~~The requirements of [ ] are described in the following section:~~

- ~~Development (6.1.4)~~
- ~~Configuration Management (6.1.5)~~
- ~~Installation (6.1.8)~~
- ~~Maintenance (6.1.9)~~
- ~~Training (6.1.10)~~
- ~~Operation (6.1.11)~~
- ~~Software Safety Plan (6.1.12)~~

~~The requirements of [ ] are described in the following section:~~

- ~~Secure Development Environment Management (6.1.6)~~

~~The end of each section summaries the assessment of the Original QAP against the requirements of that section.~~

~~Hardware procured or manufactured prior to the App. B-based QAP will not be used for US nuclear applications. All hardware procurement, manufacturing and related testing for US applications will be conducted under the App. B-based QAP. Therefore, these areas of the product life cycle are not included in the MRP described in Section 6.3.1.~~

6.1.2 This section intentionally left blank ~~Quality Assurance Program Rev 2~~

DCD_07.01-45

~~The requirements for MELTAC platform quality assurance are set forth in various in-house procedures, in accordance with IEEE7-4.3.2-2003 and IEEE1012-2004. In addition, 10CFR Part 50 Appendix B was used as a guideline. These in-house QA procedures are shown in Figure 6.1-1 .~~

~~[~~

~~]~~

Figure 6.1-1 This figure intentionally left blank ~~Outline of In-house QA Procedures System and Relationship of Various Plans~~

[

DCD_07.01-45

]

[

]

6.1.3 Management

This section describes requirements for management of MELTAC platform development. These requirements are based on IEEE 7-4.3.2-2003 and IEEE1012-2004. ~~[~~

~~]~~

DCD_07.01-45

6.1.3.1 Organization

[

DCD_07.01-45

DCD_07-14BTP-46

DCD_07-14BTP-46

DCD_07-14BTP-46

DCD_07.01-45

DCD_07.01-45

DCD_07-14BTP-46

DCD_07.01-45

]

6.1.3.2 This section intentionally left blank ~~Project Plan~~

[

DCD_07 .01-45

]

6.1.3.3 Personnel Ability

[

DCD_07 .01-45

]

~~Existing Platform Assessment based on UCP~~

~~There is no difference between the personnel ability requirements for the Original QA Program and [ ].~~

DCD_07 .01-45

6.1.4 Development

The outline of the Software Development Plan is shown in Figure 6.1-2. A similar process is applied to hardware components. The hardware development process is described in Table 6.1-3. [

DCD_07 .01-45

DCD_07 .01-45

]

DCD_07.01-45

~~Figure 6.1-2 Outline of Software development plan~~

DCD_07
.01-45

Figure 6.1-2 Outline of Software Development Plan (SDP)

[

DCD_07
.01-45

DCD_07
.01-45

]

Table 6.1-2 Contents of Activity in Each Phase

DCD_
07-
14BTP
-46

DCD_
07-
14BTP
-46

DCD_07
.01-45

DCD_07-14BTP-46

DCD_07.01-45

DCD_07.01-45

DCD_07.01-45

[

DCD_07.01-45

DCD_07.01-45

DCD_07.01-45

]

Figure 6.1-3 Outline of Problem Tracking/Resolution Process

The hardware development process consists of the Design Team activity and the independent review and test activity by people other than the actual design staff. The activities in each phase are shown in the table below.

Table 6.1-3 Contents of Hardware Development Activity in Each Phase

[

]

~~Existing Platform Assessment based on UCP~~

~~[~~

DCD_07.01-45

DCD_07 .01-45

~~]~~
~~The detailed assessment of the Development process used for the Existing Platform is provided in Section 6.1.7.~~

6.1.5 Configuration Management

The configuration management process is in accordance with ~~NPD Standard [Q-7302]~~ the App.B-based QAP, which conforms to RG1.169 and IEEE828-1990. The key elements of the configuration management program are described below. **[**

]

DCD_07 .01-45

~~The assessment of the configuration management activities for the Existing Platform is provided in Section 6.1.5.8.~~

DCD_07 .01-45

6.1.5.1 Organization/Responsibility

[

]

6.1.5.2 Base-Line

[

DCD_ 07- 14BTP -46

DCD_07 -14BTP- 46
DCD_07 .01-45

DCD_07
-14BTP-
46

]

6.1.5.3 Other Configuration Management Items

In addition to products of the Design and V&V Teams, the following items are maintained under the Configuration Management program.
[

]

6.1.5.4 Reporting

A project Configuration Management Report is periodically generated to document the applicable version of all project products that are maintained under configuration management, including all that have been base-lined. The frequency of updating this report is defined in the Project Plan.

6.1.5.5 Change Management

[

DCD_07
.01-45

DCD_07
-14BTP-
46

DCD_07-14BTP-46

DCD_07.01-45

DCD_07-14BTP-46

]

6.1.5.6 Storage and Retrieval

[

DCD_07.01-45

]

6.1.5.7 Reviews

[

DCD_07.01-45

]

6.1.5.8 This section intentionally left blank ~~Existing Platform Assessment based on UCP~~

~~The configuration management of the Existing Platform was assessed against the current Configuration Management program. The following minor deficiencies were identified:~~

~~[~~

~~]~~

DCD_07 .01-45

6.1.6 Secure Development Environment Management

The Secure Development Environment Management Program is in accordance with ~~NPD Standard [ ]~~ the App.B-based QAP, which conforms to RG1.152. The overall Secure Development Environment Management Program ensures the followings:

a) There is no unintended code included in the software during the process of software development.

b) Unintended changes to the software installed in the system are prevented and detected.

DCD_07 .01-45

For item a), the Section 6.1.6.1 and 6.1.6.2 describe the security measures in the development process of the MELTAC platform software and the MELTAC engineering tool. These requirements and procedures are documented. The security measures in the development process of the application software are described in application level documentation. For example, for the US-APWR these activities are described in the US-APWR Software Program Manual (MUAP-07017) The US-APWR Software Program Manual also describes change management and security measures for the application software during the final integration and testing of plant systems prior to shipment.

For item b), application level documentation describes security measures in the system design which prevent unintended changes while the system is in the plant. For example, for the US-APWR these measures are described in the Safety I&C System Description and Design

Process Technical Report for the US-APWR DCD (MUAP-07004). This applies to pre-operational testing and operation. Section 6.1.6.3 describes features of the MELTAC platform, which prevent unintended changes during system operation and allow changes to be detected, should they occur.

[

DCD_07 .01-45

]

~~The Section 6.1.6.4 describes the Existing Platform assessment.~~

A compliance assessment for the MELTAC platform and its lifecycle development process, relative to RG1.152, is provided in Appendix G.

DCD_07 .01-45

6.1.6.1 Software and FPGA Development/Storage Security Measures

[

DCD_07 .01-45

MIC-04-07-00001

MIC-04-07-00001

]

MIC-04-07-00001

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

MIC-04-07-00001

DCD_07.01-45

[

]

6.1.6.3 Secure Development Environment Measures During System Operation

[

DCD_07.01−30

]

6.1.6.4 This section intentionally left blank ~~Existing Platform Secure Development Environment Assessments based on UCP~~

~~[~~

DCD_07.01-45

~~]~~

6.1.7 This section intentionally left blank ~~US Conformance Program for Previously Developed Components~~

~~[~~

DCD_07.01-45

~~]~~

6.1.7.1 This section intentionally left blank ~~Platform Design~~

~~[~~

~~]~~

6.1.7.2 This section intentionally left blank ~~Software Design~~

6.1.7.2.1 This section intentionally left blank ~~Software~~

~~[~~

DCD_07 .01-45

~~]~~

6.1.7.2.2 This section intentionally left blank ~~FPGA~~

~~[~~

~~]~~

6.1.7.3 This section intentionally left blank ~~Program Design, Coding, Unit Test~~

6.1.7.3.1 This section intentionally left blank ~~Software~~

[

DCD_07.01-45

~~]~~

6.1.7.3.2 This section intentionally left blank ~~FPGA~~

~~[~~

~~]~~

6.1.7.4 This section intentionally left blank ~~Integration Test~~

DCD_07.01-45

~~This section is composed of two parts. The first part describes the Integration Tests performed during the original UCP and the assessment of past Integration Tests. The combination of the both results fulfills the Platform Specification, which conforms to the regulatory requirements. The second part describes the Integration Tests for the expanded UCP.~~

6.1.7.4.1 This section intentionally left blank ~~Integration Test - original UCP~~

~~[~~

DCD_07
.01-45

~~]~~
~~Final assessment result - The V&V Team confirmed that all items for the existing MELTAC platform integration test satisfied the requirements of [ ].~~

~~[~~

~~]~~

~~Based on the overall UCP the V&V Team reached the conclusion that all the requirements for the safety system are met.~~

6.1.7.4.2 This section intentionally left blank ~~Integration Test - expanded UCP~~

~~[~~

~~]~~

6.1.8 Software Installation

[

DCD_07
.01-30

DCD_07
.01-45

]

~~Existing Platform Assessment based on UCP~~

~~There are no differences between the Existing Platform and the MELTAC platform for service in U.S. in terms of software installation procedures or requirements.~~

6.1.9 Maintenance

[

DCD_07.01-45

DCD_07-14BTP-46
DCD_07.01-45

]

Table 6.1-6 Information Provided in the MELTAC Maintenance Manual

Plant owners may supplement the instructions in the Maintenance Manual with plant specific procedures to address administrative issues such as work orders and approvals.

~~Existing Platform Assessment based on UCP~~
~~There are no differences between the Existing Platform and the MELTAC platform for service in U.S. in terms of maintenance procedures or requirements.~~ DCD_07.01-45

6.1.10 Training

~~MELCO supports t~~ Training that assists customers in understanding the working and proper use of the MELTAC platform is developed by the MELTAC supplier. [DCD_07-14BTP-46 DCD_07.01-45

]

This training is comprised of lecture classes and hands-on training using actual MELTAC Controllers. Below are the major trainings courses:

[

DCD_07.01−30

]

Additional application specific training is described in application level documentation. For example, for the US-APWR training is described in the US-APWR Software Program Manual (MUAP-07017).

~~Existing Platform Assessment based on UCP~~
~~There are no differences between the Existing Platform and the MELTAC platform for service in U.S. in terms of training procedures or requirements.~~ DCD_07.01-45

6.1.11 Operations

[

DCD_07.01-45

]

6.1.11.1 Hardware

The following hardware measurements and adjustments (as needed) are recommended on a periodic basis, but not more frequently than once every 24 months.

Table 6.1-7 Hardware Measurement

~~Existing Platform Assessment based on UCP~~

~~There are no differences between the Existing Platform and the MELTAC platform for service in U.S. in terms of hardware operations procedures or requirements.~~ DCD_07.01-45

Table 6.1-8 Software Upgrades Relation

DCD_07.01-45

DCD_07.01-45

DCD_07.01-45

DCD_07.01-45

~~Existing Platform Assessment based on UCP~~

~~There are no differences between the Existing Platform and the MELTAC platform for service in U.S. in terms of software operations procedures or requirements~~. DCD_07.01-45

6.1.12 Software Critical Function Analysis

[

] DCD_07.01-45

As is described in the Section 4.1.3.1 “Basic Software”, MELTAC CPU basic software consists of 9 tasks executed sequentially.

[

]

Table 6.1-9 Possible Hazards

DCD_
07.01-
45

[

DCD_
07.01-
45

]

6.2 Life Cycle Management

[

DCD_07.01-45

]

6.2.1 Quality Records Management

Quality records are collected and controlled to ensure ~~This Quality Assurance Program ensures~~ records of completed items and activities affecting quality are appropriately stored. The records and their retention times are defined.

DCD_07.01-45

6.2.2 Failure and Error Reporting and Corrective Action

~~MELCO has supported the utilities' maintenance of the shipped equipments. MELCO participates in the annual inspection and has provided 24 hours on call support service and dedicated Maintenance Team per plant in Japan. Therefore all customer's claims and Irregular Events for the shipped equipments are reported directly to MELCO, whether the plant is in operation or in the maintenance.~~

DCD_07.01-45

6.2.2.1 Policy of MELTAC Troubleshooting

When any error or failure occur, ~~Per~~ a plant maintenance team executes the primary investigation and the emergency treatment against the customer's claim and sends detailed information to the factory for the further investigation. At the factory side, the procedure of troubleshooting is prepared to solve problem and for the preventive actions for other plants.(See 6.2.2.2)

DCD_07.01-45

~~MELCO has recorded all~~ A phenomena, causes, solutions, and all information about troubles at all plants will be recorded. ~~So MELCO collects all field equipment failure and error information in-depth detail~~.
Based on this information, ~~MELCO has~~ problems will be analyzed to improve the ~~platform~~ reliability ~~to improve~~ and quality of the MELTAC platform.

DCD_07.01-45

6.2.2.2 Troubleshooting Summary

The rule, method and form of troubleshooting report to customer will be discussed ~~between MELCO and~~ with each customer, in consideration of US regulations (10CFR21) and customer's situation.
This subsection describes the general problem handling process of ~~MELCO~~ MELTAC. ~~Changes to this process are likely to occur through the normal course of MELCO's process improvements.~~ This process will likely be improved with experience.

DCD_07.01-45

[

DCD_07.01-45

DCD_07.01-45

DCD_07.01-45

]

[

DCD_07.01-45

]

6.2.3 Obsolescence Management

This section describes obsolescence management program for the MELTAC platform. ~~MELCO~~ MELTAC uses only parts with an excellent record of production continuity. Regardless, the product service life for nuclear applications covers 20 – 30 years, therefore it is inevitable that many parts will become unavailable. The following sections describe the process used to determine the availability of parts and the process used to evaluate and utilize different parts for substitution. DCD_07.01-45

The parts substitution method described in this section is primarily applicable to obsolescence management. However, MELTAC supplier ~~MELCO~~ may also use the same method of part substitution to ensure adequate parts supply from multiple sources to accommodate supply management issues or production peaks. DCD_07.01-45

6.2.3.1 Obtaining Information on Part Availability

[

DCD_07.01-45

]

6.2.3.2 Selecting Replacement Parts

[

DCD_07.01-45

]

6.2.3.3 Verification after Replacement

[

]

6.2.4 Identification

[

DCD_07.01-45

DCD_07.01-45

DCD_07.01-30

DCD_07.01-30

DCD_
07.01-
45

]

6.2.5 Reliability Database

[

DCD_07.01-45

]

6.3 This section intentionally left blank ~~Establishment of 10 CFR Part 50 Appendix B-based QA Program, and MELTAC Re-evaluation Program~~

6.3.1 This section intentionally left blank ~~Establishment of 10 CFR Part 50 Appendix B-based QA Program~~

~~[~~

DCD_07-14BTP-46

DCD_07.01-45

~~]~~

Table 6.3-1 This figure intentionally left blank ~~Relationship Between App.B-based QAP and Previous QAP~~

DCD_07.01-45

6.3.2 This section intentionally left blank ~~MELTAC Re-evaluation Program~~

~~[~~

DCD_07-14BTP-46

DCD_07.01-45

~~]~~

6.4 This section intentionally left blank ~~Basic Software Program Manual~~

~~[~~

DCD_07.01-45

DCD_07.01-45

~~]~~

6.5 MELTAC Engineering Tool Life Cycle

The MELTAC engineering tool was developed and managed under ~~MELCO~~ the QAP for non-safety items (Complies with ISO 9001). ~~It has demonstrated correct performance for nuclear applications of the MELTAC platform since 1987. Since~~ The MELTAC engineering tool is not credited for any safety-related functions (ie. the output of the MELTAC engineering tool is manually verified)~~, the UCP and MRP have not been applied to the MELTAC engineering tool~~.

DCD_07.01-45

DCD_07.01-45

The MELTAC engineering tool will continue to be managed under the ~~MELCO~~ QAP for non-safety items, and the output of the tool will continue to be manually verified. Since the tool is used to develop application software, the application development and verification process is defined in application level documentation and managed under the applicable application level QAP. For example, for the US-APWR, the application software development process, is defined in the US-APWR Software Program Manual (MUAP-07017).

DCD_07.01-45

7.0 EQUIPMENT RELIABILITY

7.1 History of Operation

Development of the MELTAC platform was started in 1985 aiming at applications in nuclear non-safety systems in the short term and applications in nuclear safety protection systems in the longer term. The first non-safety system application was in 1987. This system accumulated several years of field experience in nuclear plants. This field experience allowed improvement of the product for application to safety systems.

The first safety prototype system went through third party Qualification Test by a Japanese domestic agency during the period from 1987 to 1990. The platform's basic hardware and software design were entirely accepted.

The latest digital technology development was started in 1988 for the purpose of improvements reflecting additional field operating experience and new features to allow application of the MELTAC platform to a complete plant-wide digital I&C system.
The latest platform was first applied to nuclear plant non-safety systems in 2001.

Shown in Figure 7.1-1 is the history of the MELTAC development, the records of operation, and the application plans. The MELTAC operation status at the time of this document revision is described below.

a) Operating at five PWR plants in Japan, each for an average of ten years.
b) Used for 50 non-safety system applications per plant.
c) Combined total operation time of over 20,000,000 hours
d) No plant system has ever suffered shutdown due to software- or hardware-related problems.

The MELTAC platform has ~~now~~ been applied for total plant-wide digital upgrades at two Japanese nuclear plants. The platform is used throughout these plants, including the digital protection system and digital VDU-based main control room. The plants restarted with the complete plant-wide MELTAC system July 2009. DCD_07.01-45

The MELTAC platform has also been applied for a Japanese nuclear plant ~~under construction~~. The platform is used throughout the plant, including the digital protection system and digital VDU-based main control room. ~~The complete digital system was shipped to the plant site recently after completing a 22 month factory acceptance test.~~ Commercial operation of this plant began ~~is expected to begin~~ in late 2009. DCD_07.01-45 DCD_07.01-45

MELTAC systems are currently in production for six new nuclear plants in China. The platform is used for the digital plant protection systems.

All MELTAC operating experience to date has been encompassed in the MELTAC product described in this Technical Report. Additional experience gained through future applications is continuously encompassed in ongoing product improvements. All changes to the product are conducted under the App.B-based QAP described in Section 6. Changes to the product that also change the descriptions in this Technical Report will be identified in future licensing submittals.

Table 7.2-1 Failure rate of modules

DCD_
07.01-
45

DCD_
07.01-
45

Table 7.5-1 List of Periodic Replacement Parts

DCD_07
.01-45

For the power supplies, the estimated lifetime of the internal electrolytic capacitor was calculated based on the Arrhenius equation. For the fuses in the fan assemblies, the estimated lifetime was determined by experience for the condition under which the fuse is actually used. The replacement interval of all of the above components was determined based on applying a 20% conservatism factor to the estimated lifetimes of these subparts.

The components described above have age related failure mechanisms, however none of these aging mechanisms would significantly affect the equipment’s susceptibility to failure during any of the equipment qualification tests described in Section 5. Therefore there is no age related preconditioning prior to the qualification tests.

Other components in the MELTAC platform have no known age related failure mechanisms, therefore replacement only occurs at the time of a random failure.

7.6 Performance history of self-diagnosis function

[

]

Table 7.6-1 Number of failures

[

DCD_07.01-45

DCD_07.01-45

DCD_07.01-45

DCD_07.01-45

]

APPENDIX A HARDWARE SPECIFICATIONS

The modules described here are modules for Safety system. In addition to these, there are modules for non-safety system that have different functions.
Model numbers and specifications in this appendix represent current MELTAC modules at the time of this document revision. Model numbers and specifications will change as the product life cycle progresses. New modules will retain the minimum functional features, performance specifications and reliability of current modules.

Appendix A.1 CPU Module Specification

Item	Specification
~~CPU~~	~~PowerPC PowerQUICC II Pro 360MHz~~
Memory	DDR-SDRAM: 256Mbytes SRAM: 512kbytes Flash memory for a~~A~~pplication(main): 32Mbytes Flash memory for a~~A~~pplication(sub): 32Mbytes Flash memory for b~~B~~asic s~~S~~oftware 1: 32Mbytes
External dimensions	290×265×25(mm)
Hot-pluggability	Power supply must be disabled when plugging module off.

DCD_ 07.01-45

DCD_ 07.01-30

Appendix A.2 System Management Module Specification

Item	Specification
Communication Between Redundant Subsystems	Optical module transmission speed: 100Mbps Maximum transmission distance: 100m
System DI	Number of inputs: 32 Rated voltage: 24V (30V, maximum) external supply Contact current: 3mA Dielectric voltage: AC500V
System DO	Number of outputs: 8 Rated voltage: 24V (30V, maximum) Rated current: 50mA (100mA, maximum) Dielectric voltage: AC500V
~~CPU~~	~~PowerPC PowerQUICC II Pro 360MHz~~
Onboard memory	2-port memory:1Mbyte Dedicated transmission memory:1Mbyte Dedicated receiving memory:1Mbyte DDR-SDRAM: 128Mbytes Flash memory for Firmware: 32Mbytes
Firmware	Firmware is mounted on the Flash memory. It executes maintenance network communication function.
Ethernet I/F	Module Chassis, rear side: 10Mbps 1ch module front side: 100Mbps/10Mpbs (Speed: Automatically switched), 2ch
External dimension	290X265X20(mm)
Hot-pluggability	Power supply must be disabled when plugging module off.

DCD_ 07.01-45

Appendix A.3 Bus Master Module Specification

Item	Specification
Protocol	1:N master poling (Case of Communication with I/O) One way communication (Case of data link communication)
Configuration	Number of channels: 4 channels/module (Whether to use communication with I/O or serial data link communication can be defined for each channel.)
Interface	RS-485 transformer insulation.
Baud rate	1Mbps
Error detection method	CRC check
Transmission capacity	1kbyte/channel maximum (Case of Communication with I/O) 3kbyte/channel maximum (Case of data link communication)
Onboard memory	Dedicated transmission memory: 1Mbyte (256kbyte/channel)
External dimension	290X265X30(mm)
Hot-pluggability	Power supply must be disabled when plugging module off.

Appendix A.4 Control Network I/F Module Specification

Item	Specification
Protocol	Communication method: Cyclic Multiplexing method: RPR (Resilient Packet Ring) IEEE std 802.17
Configuration	Loop (redundant)
Medium	Optical fiber
Speed	Transmission rate: 1Gbps
Capacity	Transmission capacity: - 256kbytes, maximum for normal speed communication - 128kbytes, maximum for high speed communication Number of connected stations: - 126 stations, maximum for normal speed communication - 32 stations, maximum for high speed communication Distance between stations: - 2km, maximum
~~CPU~~	~~intel 80200 (400MHz)~~
Firmware	Firmware is mounted on the Flash memory. It executes Control Network communication function.
External dimension	290X265X30(mm)
Error detection	CRC detection
Hot-pluggability	Power supply must be disabled when plugging module off.

DCD_07.01-45

Appendix A.5 I/O Module Specification

Analog Input Module Specifications

Module ~~Model~~ Identifier	Function	Main Specifications	Remarks
MLPJ~~-01~~	Current input	AI: 1 input/module 4 to 20mA (Transmitter power supply is provided.) Input impedance: 10MΩ or greater Accuracy**: ±0.25%FS Temperature coefficient: ±50ppm/°C Firmware: Firmware is mounted on the ROM. It executes analog input function.	
~~MLPJ-02~~	~~Current input~~	~~AI: 1 input/module~~ ~~4 to 20mA (Transmitter power supply is provided.)~~ ~~Input impedance: 10MΩ or greater~~ ~~Accuracy**: ±0.25%FS~~ ~~Temperature coefficient: ±50ppm/°C~~ ~~* Auto testing function is provided.~~ ~~Firmware: same as MLPJ-01~~	~~For automatic testing *~~
MAIJ~~-61~~	Voltage input	AI: 1 input/module 0 to 10V Input impedance: 10MΩ or greater Accuracy**: ±0.25%FS Temperature coefficient: ±50ppm/°C Firmware: same as MLPJ-01	
MRTJ~~-34~~	RTD 4 line type	AI: 1 input/module 4-line Pt200Ω, 32 to 392°F (0 to 200°C) Input impedance: 10MΩ or greater Accuracy**: ±0.25%FS Temperature coefficient: ±50ppm/°C Firmware: same as MLPJ-01	
~~MRTJ-61~~	~~RTD 4 line type~~	~~AI: 1 input/module~~ ~~4-line Pt200Ω, 32 to 752°F (0 to 400°C)~~ ~~Input impedance: 10MΩ or greater~~ ~~Accuracy**: ±0.25%FS~~ ~~* Auto testing function is provided.~~ ~~Temperature coefficient: ±50ppm/°C~~ ~~Firmware: same as MLPJ-01~~	~~For automatic testing *~~

DCD_ 07.01-45

DCD_ 07.01-45

DCD_ 07.01-45

DCD_ 07.01-45

DCD_ 07.01-45

Module ~~Model~~ Identifier	Function	Main Specifications	Remarks
MRTJ-~~62~~	RTD 4 line type	AI: 1 input/module 4-line Pt200Ω, 500 to 662°F (260 to 350°C) Input impedance: 10MΩ or greater Accuracy**: ±0.25%FS ~~* Auto testing function is provided.~~ Temperature coefficient: ±50ppm/°C Firmware: same as MLPJ-01	~~For automatic testing *~~
~~MRTJ-81~~	~~RTD 4 line type~~	AI: 1 input/module 4-line Pt100Ω, 32 to 212°F (0 to 100°C) Input impedance: 10MΩ or greater Accuracy**: ±0.25%FS Temperature coefficient: ±50ppm/°C Firmware: same as MLPJ-01	
~~MRTJ-83~~	~~RTD 4 line type~~	AI: 1 input/module 4-line Pt100Ω, 32 to 392°F (0 to 200°C) Input impedance: 10MΩ or greater Accuracy**: ±0.25%FS Temperature coefficient: ±50ppm/°C Firmware: same as MLPJ-01	
MTCJ-~~43~~	Thermocouple	AI: 1 input/module 32 to 2372°F (0 to 1300°C) Input impedance: 10MΩ or greater Accuracy**: ±0.5%FS Temperature coefficient: ±350ppm/°C Firmware: same as MLPJ-01	
~~MTCJ-48~~	~~Thermocouple~~	AI: 1 input/module 32 to 752°F (0 to 400°C) Input impedance: 10MΩ or greater Accuracy**: ±0.2%FS Temperature coefficient: ±350ppm/°C Firmware: same as MLPJ-01	

DCD_07.01-45

DCD_07.01-45

~~* This is a function which, having a I/O Bus interface compatible with the external auto test device dedicated for verifying, switches AI input signal to power supply for process input calibration upon simulated input command from the external auto test device. This verifies the integrity of analog input function by inputting an input signal independent of input signal on the external field side.~~

DCD_07.01-45

** A 16 bit successive approximation type A/D converter is applied for the analog input module of the MELTAC platform. The rounding error of 16 bits sampling is approximately 1E-3%FS. This is negligible compared with the accuracy of the input device of analog input module which is 0.25%FS, as described in above table.
Consideration of cumulative error, which is a problem of integrating type A/D converters, is not necessary.

Analog Output Modules Specifications

Module ~~Model~~ Identifier	Function	Main Specifications	Remarks
MAOJ-~~01~~	Current output	AO: 1 output/module Maximum load: 600Ω Accuracy: ±0.25%FS Firmware: Firmware is mounted on the ROM. It executes analog output function.	
MVOJ-~~01~~	Voltage output	AO: 1 output/module Minimum load: 500Ω Accuracy: ±0.25%FS Firmware: same as MAOJ-01	

DCD_ 07.01-45

DCD_ 07.01-45

Digital Input Modules Specifications

Module ~~Model~~ Identifier	Function	Main Specifications	Remarks
MDIJ-~~03~~	Contact input	DI: 4 inputs/module Contact impressed voltage: DC24V Contact current: 10mA	
~~MDIJ-04~~	~~Contact input~~	DI: 4 inputs/module Contact impressed voltage: DC48V Contact current: 10mA	
~~MDIJ-05~~	~~Contact input~~	~~DI: 4 inputs/module~~ ~~Contact impressed voltage: DC24V~~ ~~Contact current: 10mA~~ ~~* Auto test function is provided.~~	~~For automatic testing *~~
~~MDIJ-06~~	~~Contact input~~	~~DI: 4 inputs/module~~ ~~Contact impressed voltage: DC48V~~ ~~Contact current: 10mA~~ ~~* Auto test function is provided.~~	~~For automatic testing *~~
MDIJ-~~61~~	Contact input	DI: 4 inputs/module Contact impressed voltage: DC24V Contact current: 10mA	For redundant parallel controller
~~MDIJ-62~~	~~Contact input~~	DI: 4 inputs/module Contact impressed voltage: DC48V Contact current: 10mA	For redundant parallel controller

DCD_ 07.01-45

DCD_ 07.01-45

DCD_ 07.01-45

* This has a serial communication interface compatible with the auto test device and contains a switching function which forcibly turns DI input ON or OFF upon simulated input command from the auto test device. It permits verification of the integrity of contact input state by forcibly inputting ON or OFF independent of the ON/OFF state on the external field-side contact.

Digital Output Modules Specifications

Module ~~Model~~ Identifier	Function	Main Specifications	Remarks
MDOJ~~-03~~	Relay contact output	DO: 4 outputs/module, normally open contact Rated load (resistive load) : AC220V 0.5A DC110V 0.3A	
~~MDOJ-04~~	~~Relay contact output~~	DO: 4 outputs/module, normally closed contact Rated load(resistive load) : AC220V 0.5A DC110V 0.3A	
~~MDOJ-61~~	~~Relay contact output~~	DO: 4 outputs/module, normally open contact Rated load (resistive load): AC220V 0.5A DC110V 0.3A	For redundant parallel controller
~~MDOJ-62~~	~~Relay contact output~~	DO: 4 outputs/module, normally closed contact Rated load (resistive load): AC220V 0.5A DC110V 0.3A	For redundant parallel controller
~~MDOJ-22~~	Semiconductor output (open collector)	DO: 2 outputs/module (power DO) Maximum impressed voltage: AC110V/DC125V Output current:1A (continuous) 6A(100msec) 10A(20msec)	

DCD_07.01-45

Pulse Input Module

Module ~~Model~~ Identifier	Function	Main Specifications	Remarks
MPIJ~~-11~~	Pulse input (for RCP rotation speed input）	Input: 1inputs/module Pulse amplitude: ±0.5V - ±60V Measurement range: 100rpm - 1500rpm	

DCD_07.01-45

Appendix A.6 Isolation Module and Distribution Module Specifications

Isolation Modules Specifications

Module ~~Model~~ Identifier	Function	Main Specifications	Remarks
KILJ~~-01~~	Current input Current/Voltage output	AI: 1 input/module 4 to 20mA Input impedance: 10MΩ or greater Accuracy: ±0.5%FS Temperature coefficient: ±100ppm/°C AO:1output/module 4 to 20mA / 0 to 10VDC (selectable)	
KIRJ~~-01~~	RTD 4 line type input Current/Voltage output	AI: 1 input/module 4-line Pt100Ω, 32 to 302°F (0 to 150°C) 4-line Pt100Ω, 32 to 392°F (0 to 200°C) 4-line Pt200Ω, 32 to 752°F (0 to 400°C) Input impedance: 10MΩ or greater Accuracy: ±0.5%FS Temperature coefficient: ±100ppm/°C AO:1output/module 4 to 20mA / 0 to 10VDC (selectable)	
KIDJ~~-01~~	Contact input Semiconductor output (open collector)	DI: 2 inputs/module Contact impressed voltage: DC48V DO: 2 outputs/module (power DO) Maximum impressed voltage : AC110VDC125V Output current: 10mA	
KIPJ~~-11~~	Pulse signal input (for RCP)	Input:1 (Pulse signal) Output: 2 (Pulse signal) Output pulse width: about 10msec Output voltage:10V±1V or output of open collector	

DCD_07.01-45

DCD_07.01-45

DCD_07.01-45

DCD_07.01-45

Distribution Modules Specifications

DCD_
07.01-30
DCD_
07.01-45

Module ~~Model~~ Identifier	Function	Applicable I/O Modules	Remarks
KIOJ~~-03~~ ~~KIOJ-04~~	For Digital I/O	MDIJ~~-03, MDIJ-04, MDIJ-05, MDIJ-06, MDIJ-61, MDIJ-62,~~ MDOJ~~-03, MDOJ-04, MDOJ-61, MDOJ-62~~	
	Distribution module for Digital I/O	MDOJ~~-22~~	
KLPJ~~-02~~ ~~KLPJ-13~~	For Current input（Active）	MLPJ~~-01, MLPJ-02~~	
	For Current input（Passive）	MLPJ~~-01, MLPJ-02~~	
KRTJ~~-03~~	For RTD input（four wire）	MRTJ~~-34, MRTJ-61, MRTJ-62, MRTJ-41, MRTJ-43~~	
KTCJ~~-02~~	For Thermocouple input	MTCJ~~-13, MTCJ-18~~	
KAIJ~~-04~~	For Voltage input	MAIJ~~-01~~	
KAOJ~~-02~~	For Current output	MAOJ~~-01~~	
KVOJ~~-02~~	For Voltage output	MVOJ~~-01~~	
KAIJ~~-06~~	For Pulse signal input (for RCP)	MPIJ~~-01~~	
KEXJ~~-02~~	For Jumper	MLPJ~~-01, MLPJ-02~~ MRTJ~~-34, MRTJ-61, MRTJ-62, MRTJ-41, MRTJ-43~~	

DCD_
07.01-45

Appendix A.7 E/O Converter Modules Specifications

Module ~~Model~~ Identifier	Function	Main Specifications	Remarks
MEOJ-~~01/02~~	Electrical/optical conversion	Electrical to Optical: 1 channel Optical to Electrical: 1 channel Electrical interface: RS-485 Optical signal: Singlemode optical fiber	
~~MEOJ-11~~	~~Electrical/optical conversion~~	Electrical to Optical: 1 channel Optical to Electrical: 1 channel Electrical interface: RS-232C Optical signal: Singlemode optical fiber	
FL SWITCH	Electrical/optical conversion	Electrical ~~I~~interface: Ethernet (RJ45 ports) Optical i~~I~~nterface: Fiber optic interface (FO ports) Optical signal: Multimode optical fiber	

DCD_07.01-45

DCD_07.01-45

DCD_07.01-30

Appendix A.8 Power Interface Modules Specifications

Module ~~Model~~ Identifier	Function	Main Specifications	Remarks
DPOJ~~-21~~	Semiconductor output Contact input	DO: 2 outputs/module (power DO) Maximum impressed voltage: AC110V/DC125V Output current: DC1.5A (continuous) AC2.0A_{rms} (continuous) 16A_{0-P} (100msec) 2.5A_{0-P}(1s) DI: 8 inputs/module Contact impressed voltage: DC48V Contact current: 10mA	

DCD_07.01-45

Appendix A.9 Power Supply Modules Specifications

Module ~~Model~~ Identifier	Function	Main Specifications	Remarks
PS~~-12~~	CPU Power Supply	Input voltage: AC85V to AC132V Frequency: 47Hz to 63 Hz Output voltage: DC5V (50A), DC2.1V (11A)	
~~PS-22~~	I/O Power Supply	Input voltage: AC85V to AC132V Frequency: 47Hz to 63 Hz Output voltage: DC24V (12A)	
PPSJ~~-03~~	CPU Power Supply (Small capacity type)	Input voltage: AC85V to AC132V Frequency: 47Hz to 63 Hz Output voltage: DC5V (30A), DC2.1V (11A)	Mounted at Mirror-split and Slide-split CPU Chassis
~~PPSJ-13~~	CPU Power Supply (Large capacity type)	Input voltage: AC85V to AC132V Frequency: 47Hz to 63 Hz Output voltage :DC5V (50A), DC2.1V (11A)	Mounted at non-split CPU Chassis

DCD_07.01-45

DCD_07.01-45

DCD_07.01-45

DCD_07.01-45

DCD_07.01-45

Appendix A.12 NIS

Module ~~Model~~ Identifier	Function	Main Specifications	Remarks
NFAN~~-G21~~	Pre Amplifier	Input: Current pulse signal (1 input/module) Pulse amplitude: 40dB Output: Voltage pulse signal (1 output/module)	・For SR[*1] ・Unit outside of NIS cabinet
		Input: Current pulse signal (1 input/module) Pulse amplitude: 40dB Output: Voltage pulse signal (1 output/module)	・For WR[*4] ・Unit outside of NIS cabinet
NHBN~~-G21~~	Pulse Amplifier	Input: Voltage pulse signal (1 input/module) Pulse amplitude: 40dB Output: Voltage pulse signal (1 output/module)	For SR[*1]
		Input: Voltage pulse signal (1 input/module) Pulse amplitude: 40dB Output: Voltage pulse signal (1 output/module)	For WR[*4]
NHCN~~-G21~~	Discrimination	Input: Voltage pulse signal (1 input/module) Discrimination level: Settable within the range of DC0 to -5V Output: Voltage pulse signal (1 output/module), DC10^{-10}~10^{-4}A (1 output/module)	For SR[*1], WR[*4]
NHDN~~-G21~~	Logarithmic Amplifier	Input: DC10^{-10}~10^{-4}A (1 input/module) Output: DC0~10V (1 output/module)	For SR[*1]
		Input: DC10^{-10}~10^{-4}A (1 input/module) Output: DC0~6.667V (1 output/module)	For WR[*4]
NDAN~~-G21~~	Signal Processing	Input: DC0~10V (1 input/module), DC0~500μA (1 input/module) Contact impressed voltage: DC24V (2 input/module) Communication i~~I~~nterface: RS-485 transformer insulation (6 channels/module) Firmware: Firmware is mounted on the ROM. It executes analog/digital transform and communication function	For SR[*1]
		Input: DC0~10V (1 input/module), DC0~500μA (1 input/module), DC0～-500μA (1 input/module) Contact impressed voltage: DC24V (2 inputs/module) Communication interface: RS-485 transformer insulation (6 channels/module) Firmware: Firmware is mounted on the ROM. It executes analog/digital transform and communication function.	For IR[*2]

DCD_07.01-45

DCD_07.01-45

DCD_07.01-45

DCD_07.01-45

DCD_07.01-30

DCD_07.01-45

DCD_07.01-30

Module ~~Model~~ Identifier	Function	Main Specifications	Remarks	
NDAN	Signal Processing	Input: DC0~10V (2 inputs/module), DC0~500μA (1 input/module) Contact impressed voltage: DC24V (2 inputs/module) Communication interface: RS-485 transformer insulation (6 channels/module) Firmware: Firmware is mounted on the ROM. It executes analog/digital transform and communication function.	For PR[*3]	DCD_07.01-45 DCD_07.01-30
NDCN~~-G21~~	Operation Panel	Communication ~~I~~interface: RS-485 transformer insulation (1 channel/module) Output: DC0~-12V (for Log Amp test signal), DC0/24V (for Pre Amp test and Pulse Amp test signal)	For SR[*1]	DCD_07.01-30
		Communication interface: RS-485 transformer insulation (1 channel/module) Output: DC0~24V (for Log Amp test signal, 8 outputs/module), DC0/24V (for test signal range select, 5 outputs/module)	For IR[*2]	DCD_07.01-45
		Communication interface: RS-485 transformer insulation (1 channel/module) Output: DC1~5V (for I/E Converter test signal, 2 outputs/module), DC0/24V (for test signal range select, 16 outputs/module)	For PR[*3]	DCD_07.01-30
NHEN~~-G21~~	High Voltage Cutting Off Circuit Card	Contact impressed voltage: DC24V (4 inputs/module) Input voltage: AC103.5~126.5V Output voltage: AC103.5~126.5V	For SR[*1]	DCD_07.01-45
NFTN~~-G21~~	Test Signal generator	Input: DC0/24V (4 inputs/module) Output: Voltage pulse signal (Output either 60,10^3,10^5 or 10^6cps)	For SR[*1]	
		Output: Voltage pulse signal (Output either 10^5,10^7 or 10^9cps for Campbell circuit test), Voltage pulse signal (Output either 10,10^3,10^5 or 10^6cps for Pulse circuit test)	For WR[*4]	DCD_07.01-45
NHFN~~-G21~~	Logarithmic Amplifier	Input: DC10^{-11}～5×10^{-3}A (1 input/module) Output: DC0~10V (1 output/module)	For IR[*2]	
		Input: DC10^{-7}~10^{-3}A (1 input/module) Output: DC5.555~10V (1 output/module)	For WR[*4]	DCD_07.01-45

Module ~~Model~~ Identifier	Function	Main Specifications	Remarks
~~NDAN-G22~~	~~Signal Processing~~	~~Input: DC0~10V (1 input/module),~~ ~~DC0~500μA (1 input/module),~~ ~~DC0～-500μA (1 input/module)~~ ~~Contact impressed voltage:~~ ~~DC24V (2 inputs/module)~~ ~~Communication interface: RS-485 transformer insulation (6 channels/module)~~ ~~Firmware:~~ ~~Firmware is mounted on the ROM.~~ ~~It executes analog/digital transform and communication function.~~	~~For IR^{*2}~~
~~NDCN-G22~~	~~Operation Panel~~	~~Communication interface: RS-485 transformer insulation (1 channel/module)~~ ~~Output: DC0~24V (for Log Amp test signal, 8 outputs/module), DC0/24V (for test signal range select, 5 outputs/module)~~	~~For IR^{*2}~~
NHMN-~~G21~~	Test Signal generator	Input: DC0~24V (for Log Amp test signal, 8 inputs/module), DC0/24V (for test signal range select, 5 inputs/module) Output: DC10^{-11}～5×10^{-3}A (1 output/module)	For IR^{*2}
NLPN-~~G21~~	Isolation Card	Input: DC0~10V (1 input/module) Output: DC0~10V (1 output/module)	For IR^{*2}
NDBN-~~G21~~	I/E Converter	Input: DC0~9mA (max) Gain: Variable Output: DC0~10V	For PR^{*3}
~~NDAN-G23~~	~~Signal Processing~~	~~Input: DC0~10V (2 inputs/module),~~ ~~DC0~500μA (1 input/module)~~ ~~Contact impressed voltage: DC24V (2 inputs/module)~~ ~~Communication interface: RS-485 transformer insulation (6 channels/module)~~ ~~Firmware:~~ ~~Firmware is mounted on the ROM.~~ ~~It executes analog/digital transform and communication function.~~	~~For PR^{*3}~~
~~NDCN-G23~~	~~Operation Panel~~	~~Communication interface: RS-485 transformer insulation (1 channel/module)~~ ~~Output: DC1~5V (for I/E Converter test signal, 2 outputs/module), DC0/24V (for test signal range select, 16 outputs/module)~~	~~For PR^{*3}~~
NHVN-~~G21~~	Detector Current Indicator	Input: DC0~10V (1 input/module) Display: Display 5 digits current value	For PR^{*3}
NHNN-~~G21~~	Test Signal generator	Input: DC1~5V (for I/E Converter test signal, 2 inputs/module), DC0/24V (for test signal range select, 8 inputs/module) Output: DC0~10mA (max) (2 outputs/module)	For PR^{*3}

DCD_07.01-45

DCD_07.01-45

DCD_07.01-45

DCD_07.01-45

DCD_07.01-45

DCD_07.01-45

DCD_07.01-45

Module ~~Model~~ Identifier	Function	Main Specifications	Remarks
~~NFAN-G22~~	~~Pre Amplifier~~	~~Input: Current pulse signal (1 input/module)~~ ~~Pulse amplitude: 40dB~~ ~~Output: Voltage pulse signal (1 output/module)~~	~~･For WR^{*4}~~ ~~･Unit outside of NIS cabinet~~
~~NHBN-G22~~	~~Pulse Amplifier~~	~~Input: Voltage pulse signal (1 input/module)~~ ~~Pulse amplitude: 40dB~~ ~~Output: Voltage pulse signal (1 output/module)~~	~~For WR^{*4}~~
~~NHDN-G22~~	~~Logarithmic Amplifier~~	~~Input: DC10^{-10}~10^{-4}A (1 input/module)~~ ~~Output: DC0~6.667V (1 output/module)~~	~~For WR^{*4}~~
NFFN~~-G21~~	Root mean square converter	Input: Voltage pulse signal (1 input/module) Output: DC10^{-7}~10^{-3}A (1 output/module)	For WR^{*4}
~~NHFN-G22~~	~~Logarithmic Amplifier~~	~~Input: DC10^{-7}~10^{-3}A (1 input/module)~~ ~~Output: DC5.555~10V (1 output/module)~~	~~For WR^{*4}~~
NFHN~~-G21~~	Mode Switching Card	Input: DC0~6.667V (1 input/module), DC5.555~10V (1 input/module) Output: Select one of above 2 points to output.	For WR^{*4}
~~NFTN-G22~~	~~Test Signal generator~~	~~Output: Voltage pulse signal (Output either 10^5,10^7 or 10^9cps for Campbell circuit test),~~ ~~Voltage pulse signal (Output either 10,10^3,10^5 or 10^6cps for Pulse circuit test)~~	~~For WR^{*4}~~
NJAN~~-G21~~	Power Supply for SR Detector	Input voltage: AC103.5~126.5V Frequency: 47 to 63Hz Output voltage: DC0~2500V	For SR^{*1}
NJBN~~-G21~~	Power Supply for IR Detector	Input voltage: AC103.5~126.5V Frequency: 47 to 63Hz Output voltage: DC0~1000V	For IR^{*2}
	Power Supply for WR Detector	Input voltage: AC103.5~126.5V Frequency: 47 to 63Hz Output voltage: DC0~1000V	For WR^{*4}
NHGN~~-G21~~	Power Supply for IR Detector	Input voltage: AC103.5~126.5V Frequency: 47 to 63Hz Output voltage: DC0~-200V	For IR^{*2}
NJCN~~-G21~~	Power Supply for PR Detector	Input voltage: AC103.5~126.5V Frequency: 47 to 63Hz Output voltage: DC0~1000V	For PR^{*3}
~~NJBN-G22~~	~~Power Supply for WR Detector~~	~~Input voltage: AC103.5~126.5V~~ ~~Frequency: 47 to 63Hz~~ ~~Output voltage: DC0~1000V~~	~~For WR^{*4}~~
501AJ0UN	Power Supply (NIS)	Input voltage: AC103.5~126.5V Frequency: 47Hz to 63 Hz Output voltage: DC24.5V (1A)	

*1: Source Range, *2: Intermediate Range, *3: Power Range, *4: Wide Range

DCD_07.01-45

DCD_07.01-45

DCD_07.01-45

DCD_07.01-45

DCD_07.01-45

DCD_07.01-45

DCD_07.01-45

DCD_07.01-45

DCD_07.01-45

DCD_07.01-45

Appendix A.13 RMS Module Specification

Module ~~Model~~ Identifier	Function	Main Specification	Remarks
MUBN1~~-01~~	Signal Converter (Analog)	Pulse to RS-485 converter Range: 10^7cpm Maximum	
MUBN2~~-01~~	Signal Converter (Pulse)	RS-485 to RS-485 protocol converter	
MURN2~~-01~~	Repeater Card	RS-485 to O/E, E/O converter	
501AJ0UR	Power Supply （RMS）	Input voltage: AC98V to AC132V Frequency: 47Hz to 63 Hz Output voltage :DC12V ， DC ± 15V ， DC24V	

DCD_07.01-45

DCD_07.01-45

DCD_07.01-45

APPENDIX C THIS APPENDIX INTENTIONALLY LEFT BLANK ~~CONFORMANCE TO BTP 7-14~~

~~The documents identified in the table below are MELCO's App.B-based QAP documents applicable to the generic MELTAC platform basic software. This table shows that MELCO's App.B-based QAP conforms to the requirements of BTP 7-14. Any exceptions to the standards and guidelines invoked by BTP 7-14 are described in the basic SPM.~~

~~Additional documents, applicable to plant specific applications, such as Factory Acceptance Test Procedures and Reports, are identified in application specific or project specific documentation.~~

~~[~~

~~]~~

DCD_07.01-45
DCD_Q07-14 BTP-45

~~(1) Software Life Cycle Process Planning~~

DCD_07
.01-45
DCD_Q
07-14
BTP-45

DCD_07.01-45
DCD_Q07-14
BTP-45

~~(2) Software Life Cycle Process Implementation~~

DCD_07
.01-45
DCD_Q
07-14
BTP-45

~~(3) Software Life Cycle Process Design Outputs~~

DCD_07
.01-45
DCD_Q
07-14
BTP-45

APPENDIX E SOFTWARE CRITICAL FUNCTION ANALYSIS

Appendix E describes the results of a specific software critical function analysis activity for the MELTAC platform basic software as described in Section 6.1.12.

The description provided in APPENDIX E is the result of the analysis conducted for the developed MELTAC. If MELTAC is updated, an analysis will be conducted in accordance with ~~MELTAC Platform Basic Software Program Manual (JEXU-1012-1132)~~ ~~MELCO~~ the App.B-based QAP. DCD_07.01-45

A condition where the MELTAC platform cannot perform a specified function and generates erroneous outputs or malfunctions (or non-operation) is defined as "a potential hazard" for MELTAC platform. Potential hazards that are identified at the platform level shall be an input to system-level hazard analyses (outside the scope of lifecycle process of MELTAC platform), including the Preliminary Hazard Analysis (PHA) that is typically performed in the beginning phases of an application project. DCD_07.01-39

The specific activity addressed in this software critical function analysis is identification and analysis of potential hazards that may adversely affect critical platform functions.
This analysis assesses the effectiveness of mitigating platform level design features which ensure the hazards are correctly detected and the platform responds as specified.

The software critical function analysis activities conducted for the MELTAC platform basic software are supplemented by the software critical function analysis activities conducted for critical application level functions, as defined by the US-APWR Software Program Manual (MUAP-07017).

Table E.2-1A Detectability of Input, Operation, and Output ~~Hazards~~ Faults

DCD_07.01-39

DCD_07.01-45

DCD_07.01-45

Table E.2-1B Detectability of Input, Operation, and Output ~~Hazards~~ Faults

DCD_07.01-39

DCD_07.01-45

DCD_07.01-45

DCD_07.01-45

DCD_07.01-45

E.2.2.1 CPU Module

DCD_07.01-45

DCD_07.01-45

DCD_07.01-45

DCD_
07.01-
45

DCD_
07.01-
45

E.2.2.2 System Management Module (SMM)

DCD_
07.01-
45

DCD_07.01-45

E.2.2.3 Bus Master Module

DCD_
07.01-
45

E.2.2.4 Control Network I/F Module

DCD_
07.01-
45

DCD_
07.01-
45

DCD_
07.01-
45

DCD_07.01-45

DCD_07.01-45

E.2.2.5 FMU Module

DCD_
07.01-
45

E.2.2.6 Touch Panel Interface Module

DCD_
07.01-
45

E.2.2.7 Safety VDU Panel

DCD_
07.01-
45

E.2.2.8 Analog Input Module

DCD_07.01-45

DCD_07.01−30

DCD_07.01-45

E.2.2.9 Analog Output Module

DCD_07.01-30

DCD_07.01-45

DCD_07.01-30

DCD_07.01-45

E.2.2.10 Digital Input Module

DCD_07.01-30

DCD_07.01-45

E.2.2.11 Digital Output Module

DCD_07.01–30

DCD_07.01-45

E.2.2.12 PIF Module

DCD_07.01-30

DCD_07.01-45

E.2.2.13 Repeater Module

DCD_07.01-30

DCD_07.01-45

E.2.2.14 Power Supply Module

DCD_07.01-45

E.2.2.15 Controller Cabinet

DCD_07.01-45

E.2.3 Analysis of Communication Functions （Detectability of external communication data faults）

DCD_07.01-39

The results obtained from analyzing the detectability of external communication data faults are described in "MELTAC Platform ISG-04 Conformance Analysis" (MUAP-13018~~JEXU-1015-1009~~).

DCD_07.01-45

The Sections that provide analysis for each fault in MUAP-13018~~JEXU-1015-1009~~ are as listed in the Analysis Columns of the Table below.

As described in the analysis of MUAP-13018~~JEXU-1015-1009~~, the MELTAC platform will not transit to failure mode due to any external communication data faults shown in the table below. Thus the external communication data faults below are all identified as mitigable faults.

DCD_07.01−39

DCD_07.01-45

[

]

DCD_
07.01−
39

DCD_
07.01-
45

DCD_
07.01−
39

DCD_
07.01-
45

~~E.3 REFERENCED DOCUMENTATION~~

~~The following table is a list of specification documentation referenced in this analysis.~~

DCD_
07.01-
45

Optical Switch

The Optical Switch bypasses the Control Network communication line in the Control Network I/F Module during controller maintenance.

POL

Problem Oriented Language.
This is the control language used in the MELTAC ~~MELCO's instrumentation~~ controllers for nuclear power plants. DCD_ 07.01-45

Power Interface Module

The Power Interface (PIF) Module receives output commands as a result of Subsystem operation, and controls the power that drives the switchgears, solenoid valves, etc. for plant components. DCD_ 07.01-30

Power Supply Fan Unit

The Power Supply Fan Units are installed at the bottom and the midsection on both the left and right-hand sides of the cabinet to cool the power supplies.

Power Supply Module

The Power Supply Modules convert the AC power supplied to the Chassis from two independent sources to DC power voltages suitable for the individual modules and units.
Redundant Power Supply Modules are provided for CPU Chassis, I/O Modules, Isolation Modules, Power Interface Modules, E/O Converter Modules and fan units. DCD_ 07.01-30

Redundant Parallel Controller

In the "Redundant Parallel" configuration, the Controller includes two Subsystems. Each Subsystem operates in Control Mode.
This configuration does not require reliance on the self-diagnosis function of the CPU part or the subsystem switching operation and therefore ensures the highest reliability of a safety system.

Redundant Standby Controller

In the "Redundant Standby" configuration, the Controller includes two Subsystems. One Subsystem operates in Control Mode while the other Subsystem operates in Standby Mode.
This configuration allows a system to maintain high reliability even when any error is detected in the Subsystem in Control Mode by the self-diagnosis function, with a backup of the Subsystem in Standby Mode (i.e., status switching when the Control Subsystem fails).

Repeater Modules

The Repeater Modules shape and amplify data communication signals between I/O Modules and Bus Master Module.
This module is used in a I/O Chassis. DCD_ 07.01-30

ROM writing tool

A ROM writing tool is to write software or FPGA binary module on nonvolatile devices (ROM) on the hardware module to be used for platform tests. DCD_ 07.01-45

Safety VDU Panel

The safety VDU panel is an HSI device which provides a color graphic display with an integral touch screen.

Safety VDU Processor

The safety VDU processor transfers operation signals received from the VDU panel to safety systems and displays information of each system on the VDU panel.

Self-Diagnosis

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.

Single Controller

In the "Single" configuration, the Controller includes one Subsystem.
The Subsystem operates in Control Mode.
This configuration can be applied when a system is multiplexed.

Standby Mode

In this mode the Subsystem tracks the data from the subsystem in the Control Mode so it can automatically transition into the Control Mode if the other Subsystem transitions to the Failure Mode.
When the Subsystem detects its own failure (through self-diagnostics), it automatically changes from the Standby Mode to the Failure Mode.

Status Display & Switch Module

The Status Display & Switch Module displays the mode and alarms of the Subsystems and provides the manual mode change over switch.
This module is used in a CPU Chassis configured for a Redundant Standby Controller.

Status Display Module

The Status Display Module displays the mode and alarms of the single Subsystems.
This module is used in a CPU Chassis configured for a Redundant Parallel Controller or Single Controller.

System Management Module

The System Management Module monitors the status of the CPU Module and executes auxiliary controller functions that are not directly related to the CPU Module such as Ethernet I/F for communicating with the Engineering Tool.

~~**US Conformance Program (UCP)**~~

~~US Conformance Program (UCP) is the combination of the corrective actions taken to compensate for differences between the MELCO's original QAP and US requirements, and the assessment of the developed software by the independent V&V Team.~~

DCD_
07.01-45

V&V

Verification and Validation.
The process of determining 1) whether the requirements for a system or component are complete and correct, 2) whether the products of each development phase fulfill the requirements or conditions imposed by the previous phase, and 3) whether the final system or component complies with specified requirements.

APPENDIX G RG 1.152 Rev 3 Compliance

The analysis provided in this appendix confirms (1) that the MELTAC secure development and operational environment features are adequate to protect the safety functions of the MELTAC platform, (2) that those features are reflected in actual MELTAC documentation and (3) that those features have been developed with adequate quality assurance. The compliance assessment in this section confirms the processes planned for MELTAC development will not compromise MELTAC secure development and operational environment features. It also confirms that the processes defined for MELTAC development will adequately encompass secure development and operational environment requirements for all new MELTAC products.

DCD_07.01-45

Compliance to RG 1.152 Rev.3 is demonstrated in two sections below. Section G.1 describes compliance for the processes used to develop the platform in each phase of the product life cycle. Section G.2 assesses the effectiveness of these defensive strategies in mitigating potential threats that could lead to unauthorized changes in life cycle output products.

This compliance description does not include the Operations and Maintenance life cycle phases, since these phases are not included in Revision 3 of RG 1.152.

G.1 MELTAC Platform Secure Development and Operational Environment(SDOE)

A procedure governs software and data secure development and operational environment management activities for the MELTAC platform basic software. Personnel involved in platform software activities are trained and qualified to this procedure.

The key management and design features related to software and data security are described in Sections 6.1.6 (Secure Development Environment Management), 6.1.6.1 (Software and FPGA Development/Storage Security Measures), 6.1.6.2 (Security Measures In Each Phase of Development Process), and 6.1.6.3 (Secure Development Environment Measures During System Operation) of this document.

The following subsections describe the methods to fulfill the requirements of RG 1.152 Rev3 Positions C2.1 through C2.5:

G.1.1 Concept and Requirements Phases (Positions C2.1 and C2.2)

DCD_07.01-45

RG 1.152 Position C 2.1 “Concept Phase” Requirements:
In the concepts phase, the licensee should identify digital safety system design features required to establish a secure operational environment for the system. A licensee should describe these design features as part of its application.
The licensee should assess the digital safety system’s potential susceptibility to inadvertent access and undesirable behavior from connected systems over the course of the system’s life cycle that could degrade its reliable operation. This assessment should identify the potential challenges to maintaining a secure operational environment for the digital safety system and a secure development environment for development life cycle phases. The results of the analysis should be used to establish design feature requirements (for both hardware and software) to establish a secure operational environment and protective measures to maintain it.
The licensee should not allow remote access to the safety system. For the purposes of this guidance, remote access is defined as the ability to access a computer, node, or network resource that performs a safety function or that can affect the safety function from a computer or node that is located in an area with less physical security than the safety system (e.g., outside the protected area). Other NRC staff positions and guidance govern unidirectional and bidirectional data communications between safety and nonsafety digital systems.
Analysis:
Security-Related Information – Withheld Under 10 CFR 2.390

RG 1.152 Position C2.2 “Requirements Phase” Requirements
The licensee should define the functional performance requirements and system configuration for a secure operational environment; interfaces external to the system; and requirements for qualification, human factors engineering, data definitions, documentation for the software and hardware, installation and acceptance, operation and execution, and maintenance.
The design feature requirements intended to maintain a secure operating environment and ensure reliable system operation should be part of the overall system requirements. Therefore, the verification process of the requirements phase should ensure the correctness, completeness, accuracy, testability, and consistency of the system’s SDOE feature.
Requirements specifying the use of pre-developed software and systems (e.g., reused software and commercial off-the-shelf (COTS) systems) should address the reliability of the safety system (e.g., by using pre-developed software functions that have been tested and are supported by operating experience).
During the requirements phase, the licensee should prevent the introduction of unnecessary or extraneous requirements that may result in inclusion of unwanted or unnecessary code.
Analysis:
Security-Related Information – Withheld Under 10 CFR 2.390

DCD_07.01-45

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 10 CFR 2.390**

DCD_07
.01-45

DCD_07.01-45

Security-Related Information – Withheld Under 10 CFR 2.390

G.1.3 Implementation Phase (Position C2.4)

RG 1.152 Position C2.4 “Implementation Phase” Requirements
In the system (integrated hardware and software) implementation phase, the system design is transformed into code, database structures, and related machine executable representations. The implementation activity addresses hardware configuration and setup, software coding and testing, and communication configuration and setup (including the incorporation of reused software and COTS products). The developer should ensure that the transformation from the system design specification to the design configuration items of the secure operational environment is correct, accurate, and complete.
The developer should implement secure development environment procedures and standards to minimize and mitigate any inadvertent or inappropriate alterations of the developed system. The developer’s standards and procedures should include testing, (such as scanning), as appropriate, to address undocumented codes or functions that might (1) allow unauthorized access or use of the system or (2) cause systems to behave outside of the system requirements or in an unreliable manner. The developer should account for hidden functions and vulnerable features embedded in the code, their purpose and their impact on the integrity and reliability of the safety system. These functions should be removed or (as a minimum) addressed (e.g., as part of the failure modes and effects analysis of the application code) to prevent any unauthorized access or degradation of the reliability of the safety system.
COTS systems are likely to be proprietary and generally unavailable for review. In addition, a reliable method may not exist for determining the complete set of system behaviors inherent in a given operating system (e.g., operating system suppliers often do not provide access to the source code for operating systems and callable code libraries). In such cases, unless the application developer can modify these systems, the developer should ensure that the features within the operating system do not compromise the required design features of the secure operational environment so as to degrade the reliability of the digital safety system.

DCD_07.01-45

Analysis:

Security-Related Information – Withheld Under 10 CFR 2.390

DCD_07.01-45

Security-Related Information – Withheld Under 10 CFR 2.390

DCD_07.01-45

G.1.4 Test Phase (Position C2.5)

RG 1.152 Position C2.5 “Test Phase” Requirements
The objective of testing the design features of the secure operational environment is to ensure that the design requirements intended to ensure system reliability are validated by the execution of integration, system, and acceptance tests where practical and necessary. Testing includes system hardware configuration (including all connectivity to other systems, including external systems), software integration testing, software qualification testing, system integration testing, system qualification testing, and system factory acceptance testing. The secure operational environment design requirements and configuration items intended to ensure reliable system operation should be part of the validation effort for the overall system requirements and design configuration items. Therefore, design configuration items for the secure operational environment are just one element of the overall system validation. Each system design feature of the secure operational environment should be validated to verify that the implemented feature achieves its intended function to protect against inadvertent access or the effects of undesirable behavior of connected systems and does not degrade the safety system’s reliability.
The developer should correctly configure and enable the design features of the secure operational environment. The developer should also test the system hardware architecture, external communication devices, and configurations for unauthorized pathways and system integrity. Attention should be focused on built-in original equipment manufacturer features.
Analysis:
Security-Related Information – Withheld Under 10 CFR 2.390

DCD_07.01-45

DCD_07.01-45

Security-Related Information – Withheld Under 10 CFR 2.390

DCD_07.01-45

Security-Related Information – Withheld Under 10 CFR 2.390

G.2 Assessment of Defensive Strategies to Prevent Unauthorized Changes

Possible unauthorized activities with regard to the development phases described in the App.B-based QAP are listed below:

[

Security-Related Information – Withheld Under 10 CFR 2.390

]

DCD_07
.01-45

G.2.1 Defense Against Unauthorized Changes in Requirements Specifications

[

Security-Related Information – Withheld Under 10 CFR 2.390

]

G.2.2 Defense Against Unauthorized Changes in Design Descriptions

[

Security-Related Information – Withheld Under 10 CFR 2.390

]

G.2.3 Defense Against Unauthorized Changes in Source Code or the Development Environment

[

DCD_07.01-45

Security-Related Information – Withheld Under 10 CFR 2.390

]

G.2.4 Defense Against Changes Masked by Misrepresentation in Test Reports

[

Security-Related Information – Withheld Under 10 CFR 2.390

]

G.2.5 Defense Against Unauthorized Changes to Approved Output Products

[

Security-Related Information – Withheld Under 10 CFR 2.390

]

Table G.2-1 - Security Measures of the Software Development/Storage Environment

Security-Related Information – Withheld Under 10 CFR 2.390

DCD_07
.01-45

[

Security-Related Information – Withheld Under 10 CFR 2.390

]

G.3 Conclusion

The scope of the MELTAC secure development and operational environment responsibilities include the Concept Phase through the Test Phase, as described in Regulatory Guide 1.152 Rev3. The combination of the information in this document on system design features, and the specific information provided in this document fully address the secure development and operational environment issues associated with the MELTAC platform.

Abstract

DCD_07.01-45

This MHI Technical Report describes the conformance analysis of the safety-related digital platform for the US-APWR against the requirements of DI&C ISG-04 “Highly-Integrated Control Rooms—Communications Issues (HICRc)”. Requirements of the conformance analysis of the safety digital platform are identified first followed by the results of the conformance analysis of the MELTAC platform, the safety-related digital platform for the US-APWR.

0.1 Requirement of Conformance Analysis

DCD_ 07.01- 45

Purpose and Scope

The purpose of this document is to describe the conformance analysis of the safety-related digital platform for the US-APWR to the requirements of DI&C ISG-04 “Highly-Integrated Control Rooms—Communications Issues (HICRc)”.

The results of the conformance analysis of the MELTAC platform, the safety-related digital platform for the US-APWR, to the requirements of DI&C ISG-04 are attached in this document.

The other level of the conformance analysis of safety-related digital I&C systems (i.e., system and application level conformance analysis), not described in this report (e.g., interdivisional communications among the safety-related systems, interdivisional communications from the non-safety systems, including operational VDU to the safety-related systems) are described in the US-APWR DCD Ch7 and the other associated technical reports.

Conformance Analysis of Safety-related Digital Digital I&C System

The safety-related digital I&C system conforms to DI&C ISG-04.

As described in DCD Section 7.1, the safety-related I&C for the US-APWR consists of a fully digital platform. The conformance of safety-related digital I&C system to ISG-04 are described in the following documents.

“Safety I&C System Description and Design Process” (MUAP-07004), for system and application level
“MELTAC Platform ISG-04 Conformance Analysis” (MUAP-13018), this report, specific for platform level

Requirement of Conformance Analysis

The requirements of ISG-04 from section 1 to 3.1 are provided as analysis criteria of safety-related digital platform. Conformance to Section 3.2 "Human Factors Considerations" and Section 3.3 "Diversity and Defense-in-Depth (D3) Considerations" is demonstrated at the system and application level. Therefore, requirements of section 3.2 and 3.3 are not provided as analysis criteria in this report, but described in MUAP-07004 Appendix E.

Conformance Analysis

To demonstrate the conformance analysis specific for safety-related digital platform, the results of a conformance analysis of the MELTAC platform to the requirements of DI&C ISG-04 is attached in this document (from Section 1 to Appendix A of this document) with following information.

- Conformance analysis result, which demonstrates that the safety-related digital platform design conforms to the requirements of DI&C ISG-04.
- Modification information, which demonstrates the design modification if it is needed to conform to the requirements of DI&C ISG-04.

For example, if the communication processor is accessing the shared memory at a time when the function processor needs to access it, the function processor should gain access within a timeframe that does not impact the loop cycle time assumed in the plant safety analyses. If the shared memory cannot support unrestricted simultaneous access by both processors, then the access controls should be configured such that the function processor always has precedence.

The safety function circuits and program logic should ensure that the safety function will be performed within the timeframe established in the safety analysis, and will be completed successfully without data from the shared memory in the event that the function processor is unable to gain access to the shared memory.

Analysis

DCD_07.01-45

3.2.1. Control Network

[

]

DCD_07.01-45

DCD_07.01−30

DCD_07.01−30

DCD_07.01-45

DCD_07.01−30

DCD_07.01−30

DCD_07.01−30

DCD_07.01-45

DCD_07.01-45

DCD_07.01-45

3.3. Analysis of Command Prioritization

The results of analyzing the command prioritization are as follows. It is noted that in MELTAC there are two priority logic functions. One is in the function processor which prioritizes safety commands over non-safety commands received via the Control Network. The second is within the PIF module which employs state based priority logic to ensure that either the primary system or the backup system can put the component in its preferred safety state.

As noted in section 2.2, Staff Positions from ISG-04 Section 2 are used as criteria.

3.3.1. ISG-04 2.1

Requirement
A priority module is a safety-related device or software function. A priority module must meet all of the 10 C.F.R. Part 50, Appendix A and B requirements (design, qualification, quality, etc.) applicable to safety-related devices or software.
Analysis

DCD_07.01-45

3.3.2. ISG-04 2.2

Requirement
Priority modules used for diverse actuation signals should be independent of the remainder of the digital system, and should function properly regardless of the state or condition of the digital system. If these recommendations are not satisfied, the applicant should show how the diverse actuation requirements are met.
Analysis

3.3.6. ISG-04 2.6

Requirement
Software used in the design, testing, maintenance, etc. of a priority module is subject to all of the applicable guidance in Regulatory Guide 1.152, which endorses IEEE Standard 7-4.3.2-2003 (with comments). This includes software applicable to any programmable device used in support of the safety function of a prioritization module, such as programmable logic devices (PLDs), programmable gate arrays, or other such devices. <abbreviated> Validation of design tools used for programming a priority module or a component of a priority module is not necessary if the device directly affected by those tools is 100% tested before being released for service. 100% testing means that every possible combination of inputs and every possible sequence of device states is tested, and all outputs are verified for every case. The testing should not involve the use of the design tool itself. Software-based prioritization must meet all requirements (quality requirements, V&V, documentation, etc.) applicable to safety-related software.
Analysis

MIC-03-07-00007

DCD_07.01-45

3.3.7. ISG-04 2.7

Requirement
Any software program that is used in support of the safety function within a priority module is safety-related software. All requirements that apply to safety-related software also apply to prioritization module software. Nonvolatile memory (such as burned-in or reprogrammable gate arrays or random-access memory) should be changeable only through removal and replacement of the memory device. Design provisions should ensure that static memory and programmable logic cannot be altered while installed in the module. The contents and configuration of field programmable memory should be considered to be software, and should be developed, maintained, and controlled accordingly.
Analysis

DCD_07.01-45

~~Appendix A. Referenced Documentation~~

~~The following table is a list of specification documentation referenced in this analysis.~~

DCD_07.01-45