

# **Safety System Digital Platform - MELTAC - Topical Report**

**Non-Proprietary Version**

**TAC No. MF4228  
Issue Date: February 5, 2019**

## **Contents**

**PART 1: Final Safety Evaluation for “SAFETY SYSTEM DIGITAL PLATFORM MELTAC”, including**

NRC Transmittal Letter dated November 5, 2018, and  
Safety Evaluation Report (SER) dated November 5, 2018

**PART 2: Request for Additional Information (RAI), including**

NRC Transmittal Letter dated June 29, 2016, and  
RAI Questions

**PART 3: Responses to RAI, including**

MELCO Transmittal Letters dated July 21, 2016 and August 10, 2016,  
Responses to RAI dated July 21, 2016 and August 10, 2016,  
MELCO Transmittal Letter dated September 23, 2016,  
Responses to RAI dated September 23, 2016,  
MELCO Transmittal Letter dated October 7, 2016,  
Responses to RAI dated October 7, 2016,  
MELCO Transmittal Letter dated October 17, 2016,  
Responses to RAI dated October 17, 2016,  
MELCO Transmittal Letter dated March 17, 2017,  
Responses to RAI dated March 17, 2017,  
MELCO Transmittal Letter dated May 31, 2017,  
Responses to RAI dated May 31, 2017, and  
MELCO Transmittal Letter dated August 31, 2017

**PART 4: Safety System Digital Platform - MELTAC - Topical Report, JEXU-1041-1008, Revision 1**



## **PART 1**

### **Final Safety Evaluation for “SAFETY SYSTEM DIGITAL PLATFORM MELTAC”, including:**

NRC Transmittal Letter dated November 5, 2018

Safety Evaluation Report (SER) dated November 2018



**UNITED STATES  
NUCLEAR REGULATORY COMMISSION**  
WASHINGTON, D.C. 20555-0001

November 5, 2018

Mr. Jay Sneddon  
Nuclear Systems Department Manager  
Mitsubishi Electric Power Products, Inc.  
547 Keystone Drive  
Warrendale, PA 15086

**SUBJECT: FINAL PROPRIETARY SAFETY EVALUATION FOR "SAFETY SYSTEM  
DIGITAL PLATFORM – MELTAC" (CAC NO. MF4228; EPID L-2014-TOP-0006)**

Dear Mr. Sneddon:

By letter dated April 30, 2014 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML14121A415), Mitsubishi Electric Corporation (MELCO) submitted for U.S. Nuclear Regulatory Commission (NRC) staff review the topical report (TR); "Safety System Digital Platform – MELTAC [Mitsubishi Electric Total Advanced Controller]." By letter dated September 25, 2018, the NRC staff issued its draft safety evaluation (SE) on the MELTAC digital platform (ADAMS Accession No. ML18081A611).

By letter dated October 5, 2018 (ADAMS Accession No. ML18281A004), MELCO provided comments on the NRC draft SE. The comments provided by MELCO were related to the identification of proprietary information in the draft SE, and one term correction.

The NRC staff has found that MELTAC TR is acceptable for referencing in licensing applications for nuclear power plants to the extent specified and under the limitations delineated in the TR and in the enclosed final SE. The final SE defines the basis for our acceptance of the TR.

Our acceptance applies only to material provided in the subject TR. We do not intend to repeat our review of the acceptable material described in the TR. When the TR appears as a reference in license applications, our review will ensure that the material presented applies to the specific plant involved. License amendment requests that deviate from this TR will be subject to a plant-specific review in accordance with applicable review standards.

In accordance with the guidance provided on the NRC website, we request that MELCO publish accepted proprietary and non-proprietary versions of the TR within three months of receipt of this letter. The accepted-for-use version shall incorporate this letter and the enclosed final SE after the title page. Also, it must contain historical review information, including NRC requests for additional information (RAIs) and your responses. The accepted versions shall include a "-A" (designating accepted) following the TR identification symbol.

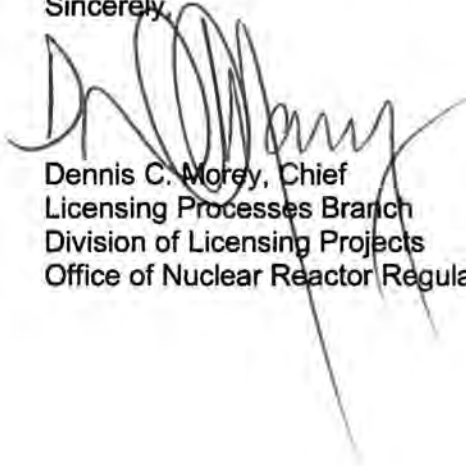
As an alternative to including the RAIs and RAI responses behind the title page, if changes to the TRs were provided to the NRC staff to support the resolution of RAI responses, and the NRC staff reviewed and accepted those changes as described in the RAI responses, there are two ways that the accepted version can capture the RAIs:

1. The RAIs and RAI responses can be included as an Appendix to the accepted version.
2. The RAIs and RAI responses can be captured in the form of a table (inserted after the final SE) which summarizes the changes as shown in the accepted version of the TR. The table should reference the specific RAIs and RAI responses which resulted in any changes, as shown in the accepted version of the TR.

If future changes to the NRC's regulatory requirements affect the acceptability of this TR, MELCO will be expected to revise the TR appropriately. Licensees referencing this TR would be expected to justify its continued applicability or evaluate their plant using the revised TR.

If you have any questions or require any additional information, please feel free to contact the NRC Project Manager for the review, Joseph Holonich at (301) 415-7297 or [joseph.holonich@nrc.gov](mailto:joseph.holonich@nrc.gov).

Sincerely,

A handwritten signature in black ink, appearing to read 'Dennis C. Morey', is written over the typed name and title.

Dennis C. Morey, Chief  
Licensing Processes Branch  
Division of Licensing Projects  
Office of Nuclear Reactor Regulation

Docket No.: 99902039

Enclosure:  
Final Safety Evaluation

**U.S. NUCLEAR REGULATORY COMMISSION STAFF**

**SAFETY EVALUATION FOR**

**MITSUBISHI ELECTRIC TOTAL ADVANCED CONTROLLER (MELTAC)**

**PLATFORM TOPICAL REPORT AND SUPPORTING DOCUMENTS**

**CAC NO. MF4228; EPID L-2014-TOP-0006**



**Principal Contributors:**

**Rich Stattel  
Samir Darbali  
Dinesh Taneja**

**November 2018**



## Table of Contents

<b>1.0</b>	<b><u>INTRODUCTION AND BACKGROUND</u></b>	- 3 -
<b>2.0</b>	<b><u>REGULATORY EVALUATION</u></b>	- 5 -
<b>3.0</b>	<b><u>TECHNICAL EVALUATION</u></b>	- 10 -
3.1	<u>System Background</u>	- 10 -
3.2	<u>System Description</u>	- 10 -
3.2.1	<u>MELTAC platform Hardware and Architecture</u>	- 14 -
3.2.1.1	<u>MELTAC Central Processing Unit Chassis</u>	- 15 -
3.2.1.1.1	<u>CPU Module</u>	- 16 -
3.2.1.1.2	<u>System Management Module</u>	- 16 -
3.2.1.1.3	<u>Status-Display-and-Switch Modules</u>	- 16 -
3.2.1.1.4	<u>Bus-Master Module</u>	- 17 -
3.2.1.1.5	<u>Control Network I/F Module</u>	- 17 -
3.2.1.1.6	<u>CPU Power Supply Module</u>	- 17 -
3.2.1.2	<u>Input / Output Chassis</u>	- 17 -
3.2.1.2.1	<u>I/O Modules</u>	- 17 -
3.2.1.2.2	<u>I/O Power Supply Modules</u>	- 18 -
3.2.1.3	<u>Terminal Unit</u>	- 18 -
3.2.1.4	<u>Distribution Module</u>	- 18 -
3.2.1.5	<u>Isolation Chassis</u>	- 18 -
3.2.1.5.1	<u>Isolation Modules</u>	- 18 -
3.2.1.5.2	<u>Power-Interface Module</u>	- 18 -
3.2.1.6	<u>Safety Visual Display System</u>	- 19 -
3.2.1.6.1	<u>Safety Visual Display Unit Panel</u>	- 19 -
3.2.1.6.2	<u>S-VDU Processor</u>	- 19 -
3.2.1.7	<u>Watchdog Timer</u>	- 20 -
3.2.2	<u>MELTAC System Communication</u>	- 20 -
3.2.2.1	<u>Control Network (Intra-Divisional Communication)</u>	- 21 -
3.2.2.2	<u>Data Link (Inter-Divisional Communication)</u>	- 21 -
3.2.2.3	<u>Data Link Isolation / Independence</u>	- 22 -
3.2.2.4	<u>Maintenance Network (Safety to Non-Safety Communication)</u>	- 23 -
3.2.2.5	<u>Maintenance Workstation</u>	- 23 -
3.2.2.6	<u>MELTAC Reprogramming Chassis</u>	- 24 -
3.2.2.7	<u>MELTAC Controller Communication Busses</u>	- 24 -
3.3	<u>MELTAC Software Architecture</u>	- 24 -
3.3.1	<u>MELTAC Basic Software</u>	- 24 -
3.3.2	<u>MELTAC Application Software</u>	- 25 -
3.4	<u>MELTAC Re-evaluation Program</u>	- 25 -
3.5	<u>Software Development Process</u>	- 30 -
3.5.1	<u>Software Development Lifecycle Process Planning</u>	- 31 -
3.5.1.1	<u>Software Management Plan</u>	- 32 -
3.5.1.2	<u>Software Development Plan</u>	- 33 -
3.5.1.3	<u>Software Quality Assurance Plan</u>	- 35 -
3.5.1.4	<u>Software Integration Plan</u>	- 36 -
3.5.1.5	<u>Software Safety Plan</u>	- 36 -
3.5.1.6	<u>Software Verification and Validation Plan</u>	- 37 -
3.5.1.7	<u>Software Configuration Management Plan</u>	- 38 -
3.5.1.8	<u>Software Test Plan</u>	- 39 -
3.5.2	<u>Software Implementation Documentation</u>	- 39 -
3.5.2.1	<u>Safety Analysis</u>	- 40 -
3.5.2.2	<u>V&amp;V Analysis and Reports</u>	- 40 -

3.5.2.3	<u>Configuration Management Activity</u>	- 41 -
3.5.2.4	<u>Testing Activity</u>	- 42 -
3.5.2.5	<u>Requirements Traceability Evaluation</u>	- 42 -
3.5.2.6	<u>Failure mode and Effect Analysis</u>	- 43 -
3.5.2.7	<u>Reliability Analysis</u>	- 44 -
3.5.3	<u>Software Lifecycle Process Design Outputs</u>	- 45 -
3.5.3.1	<u>Software Requirements Specification</u>	- 46 -
3.6	<u>Equipment Qualification</u>	- 46 -
3.6.1	<u>Atmospheric (Temperature and Humidity)</u>	- 48 -
3.6.2	<u>Electromagnetic Interference / Radio Frequency Interference</u>	- 49 -
3.6.2.1	<u>EMI/RFI Interference</u>	- 50 -
3.6.2.2	<u>EMI/RFI Susceptibility</u>	- 50 -
3.6.2.3	<u>Surge Withstand Capability</u>	- 50 -
3.6.2.4	<u>Electrostatic Discharge Withstand Testing</u>	- 51 -
3.6.2.5	<u>Electromagnetic Compatibility Test Acceptance Criteria Evaluation</u>	- 51 -
3.6.3	<u>Seismic Qualification</u>	- 51 -
3.7	<u>MELTAC platform Integrity Characteristics</u>	- 54 -
3.7.1	<u>MELTAC Platform Response Time</u>	- 54 -
3.7.2	<u>Determinism</u>	- 55 -
3.7.3	<u>Self-diagnostics / Test and Calibration Capabilities</u>	- 56 -
3.7.4	<u>Setpoint Determination Methodology</u>	- 57 -
3.8	<u>Diversity and Defense-in-Depth</u>	- 58 -
3.9	<u>Communications</u>	- 58 -
3.9.1	<u>DI&amp;C-ISG-04 Compliance</u>	- 58 -
3.9.1.1	<u>DI&amp;C-ISG-04, Staff Position 1 - Interdivisional Communications</u>	- 59 -
3.9.1.2	<u>DI&amp;C-ISG-04, Section 2 - Command Prioritization</u>	- 73 -
3.9.1.3	<u>DI&amp;C-ISG-04, Section 3 - Multidivisional Control and Display Stations</u>	- 78 -
3.10	<u>Compliance to IEEE Std. 603-1991 Requirements</u>	- 83 -
3.10.1	<u>IEEE Std. 603-1991 Clause 4, "Safety System Designation"</u>	- 83 -
3.10.2	<u>IEEE Std. 603-1991 Clause 5, "Safety System Criteria"</u>	- 85 -
3.10.3	<u>IEEE Std. 603-1991 Clause 6, "Sense and Command Features – Functional and Design Requirements"</u>	- 91 -
3.10.4	<u>IEEE Std. 603-1991 Clause 7, "Execute features – functional and design requirements"</u>	- 92 -
3.10.5	<u>IEEE Std. 603-1991 Clause 8, "Power Source Requirements"</u>	- 92 -
3.11	<u>Conformance with IEEE Std. 7-4.3.2-2003</u>	- 93 -
3.11.1	<u>IEEE Std. 7-4.3.2-2003 Clause 5, "Safety System Criteria"</u>	- 93 -
3.12	<u>Secure Development and Operational Environment</u>	- 105 -
3.12.1	<u>RG 1.152, Revision 3, Regulatory Position 2.1, "Concepts Phase" Identification and Description of Secure Operational Environment Design Features</u>	- 106 -
3.12.2	<u>RG 1.152, Revision 3, Regulatory Position 2.2, "Requirements Phase"</u>	- 107 -
3.12.3	<u>RG 1.152, Revision 3, Regulatory Position 2.3, "Design Phase"</u>	- 109 -
3.12.4	<u>RG 1.152, Revision 3, Regulatory Position 2.4, "Implementation Phase"</u>	- 111 -
3.12.5	<u>RG 1.152, Revision 3, Regulatory Position 2.5, "Test Phase"</u>	- 113 -
4.0	<b>SUMMARY</b>	- 113 -
5.0	<b>LIMITATIONS AND CONDITIONS</b>	- 114 -
5.1	<b>GENERIC OPEN ITEMS</b>	- 114 -
5.2	<b>PLANT SPECIFIC ACTION ITEMS</b>	- 114 -
6.0	<b>REFERENCES</b>	- 117 -
<b>Appendix A, Comments on Draft Safety Evaluation and Response</b>		

## **1.0 INTRODUCTION AND BACKGROUND**

The Mitsubishi Electric Total Advanced Controller (MELTAC) platform is a computer based programmable-logic controller (PLC) consisting of a pre-defined set of hardware and software components which was developed for nuclear applications. MELTAC system processors are designed to be loaded with plant specific-application software to implement various nuclear plant safety system functions.

Safety-related instrumentation and control (I&C) systems based on the application of the MELTAC platform are designed to provide protection against unsafe reactor operation during steady-state and transient-power operations. They can also be used to initiate selected protective functions to mitigate the consequences of design-basis events and accidents, and to safely shut down the plant by either automatic means or manual actions.

The MELTAC platform was initially designed, qualified, and manufactured in accordance with Japan nuclear safety and quality standards. The MELTAC platform is based on microprocessor and Field Programmable Gate Array (FPGA) technologies and is being evaluated for general application within safety systems of nuclear power generating stations in accordance with US NRC regulations. As such, this SE (SE) addresses criteria that apply to digital equipment for use in US nuclear power plant safety systems.

By letter dated April 30, 2014 (Ref. 1), as supplemented by the letters in Table 1.0-1 below, Mitsubishi Electric Corporation (MELCO) requested U. S. Nuclear Regulatory Commission (NRC) acceptance for use of the "Safety System Digital Platform – MELTAC – Topical Report" hereafter referred to as the MELTAC Licensing Topical Report (LTR).

Table 1.0-1 List of Supplemental Letters from MELCO

<b><u>Supplement</u></b>	<b><u>Date</u></b>	<b><u>Reference</u></b>
Support Documents for SE of the MELTAC platform LTR	9/26/2014	2
Support Documents for SE of the MELTAC platform LTR	12/30/2014	3
Support Documents for SE of the MELTAC platform LTR	1/30/2015	4
Support Documents for SE of the MELTAC platform LTR	3/31/2015	5
Support Documents for SE of the MELTAC platform LTR	4/17/2015	6
Support Documents for SE of the MELTAC platform LTR	4/28/2015	7
Support Documents for SE of the MELTAC platform LTR	5/29/2015	8
Support Documents for SE of the MELTAC platform LTR	6/18/2015	9
Support Documents for SE of the MELTAC platform LTR	7/6/2015	10
Support Documents for SE of the MELTAC platform LTR	7/7/2015	11
Support Documents for SE of the MELTAC platform LTR	2/19/2016	12
Support Documents for SE of the MELTAC platform LTR	3/28/2016	13
Support Documents for SE of the MELTAC platform LTR	4/27/2016	14
Support Documents for SE of the MELTAC platform LTR	6/6/2016	15
Support Documents for SE of the MELTAC platform LTR	6/21/2016	16
RAI Response Submittals	7/21/2016 to 8/10/2016	17 - 19
Support Documents for SE of the MELTAC platform LTR	9/16/2016	20
RAI Response Submittals	9/23/2016	21
Support Documents for SE of the MELTAC platform LTR	9/30/2016	22
RAI Response Submittals	10/7/2016	23
RAI Response Submittals	10/17/2016	24
Support Documents for SE of the MELTAC platform LTR	10/18/2016	25
Support Documents for SE of the MELTAC platform LTR	11/1/2016	26
RAI Response Submittals	3/17/2017	27
Request for Exclusion from SER for MELTAC platform LTR	4/1/2017	28
RAI Response Submittals	5/31/2017	29
Support Documents for SE of the MELTAC platform LTR	7/31/2017	30
RAI Response Submittals	8/31/2017	31



These supplemental documents provide additional information to clarify and support the technical positions documented in the MELTAC LTR (Ref. 14). The MELTAC LTR was accepted for review by letter dated May 20, 2015 (Ref. 34).

On June 29, 2016, the NRC staff issued Requests for Additional Information (RAIs) (Ref. 35). MELCO provided the responses to these RAIs as identified in Table 1.0-1 above.

The NRC staff conducted an audit at the MELCO facilities in Warrendale, PA on November 27 through 30, 2017. The audit plan is provided as Reference 32. The purpose of this audit was to evaluate the effectiveness of MELCO software development activities and to confirm that processes described in the LTR are being effectively implemented to achieve a high quality system that can be used to perform safety-related functions in a nuclear facility.

During the site audit, several requirement thread reviews were performed. The NRC staff confirmed how system requirements had been implemented and tested during the MELTAC development processes. In addition, MELCO showed how the Requirements Traceability Matrices (RTMs) were used to trace requirements to design-development activities performed. Performance characteristics and functional capabilities of MELTAC platform based systems were observed. The results of the audit are documented in the "Regulatory Audit Report for the MELTAC Digital Platform Licensing Topical Report" (Ref. 33).

This SE of the MELTAC platform includes review of the development and test plans, specifications and procedures to design, and perform verification and validation (V&V) of the standardized MELTAC circuit boards described in the LTR. This SE scope also includes the processes used for development of MELTAC basic and application software. The SE scope excludes evaluation of the integration and testing of plant specific system applications, factory acceptance test of plant systems, or maintenance activities to support installed plant systems.

Section 2.0 of this SE identifies the applicable regulatory bases and corresponding guidance and regulatory acceptance criteria to which the NRC staff evaluated the MELTAC platform LTR (Ref. 14). Section 3.0 of this SE provides the technical evaluation of the MELTAC platform LTR. Section 4.0 provides the NRC staff conclusion and Section 5.0 provides limitations and conditions that apply to applicants or licensees that reference for use the MELTAC platform LTR in safety systems of nuclear power generating stations. Section 6.0 provides a list of applicable references.

## **2.0 REGULATORY EVALUATION**

NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," which is referred to as the Standard Review Plan (SRP), sets forth a method for reviewing compliance with applicable sections of Title 10 of the *Code of Federal Regulations* (10 CFR) Part 50, "Domestic Licensing of Production and Utilization Facilities." Chapter 7, "Instrumentation and controls," of NUREG-0800, Rev. 7, dated August 2016 was used by the NRC staff to establish acceptance criteria for this review. SRP Chapter 7 addresses the requirements for I&C systems in nuclear power plants based on light-water reactor designs. SRP Chapter 7 and Interim Staff Guidance (ISG), which augments and supplements SRP Chapter 7, principally establish the review process for digital I&C systems applied in this evaluation.

The suitability of a digital I&C platform for use in safety systems depends on the quality of its components; quality of the design process; and its Environmental Qualification (EQ), along with consideration of system implementation characteristics such as real-time performance, independence, and support of on-line surveillance requirements as demonstrated through the digital I&C platform's verification, validation, and qualification efforts. Because MELTAC equipment is intended for use in safety systems and for Safety-Related applications, the platform LTR was evaluated for compliance with the criteria of Institute of Electrical and Electronics Engineers (IEEE) Standard (Std.) 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and SRP Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603." The MELTAC LTR (Ref. 14) was similarly evaluated against the criteria of IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," and Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std. 7-4.3.2."

SRP Chapter 7, Table 7-1, "Regulatory Requirements, Acceptance Criteria, and Guidelines for I&C Systems Important to Safety," identifies design criteria and regulations from 10 CFR Part 50 that are applicable to I&C systems and relevant to the general review of the suitability of a digital I&C platform for use in safety-related applications. Many of the review criteria of the SRP depend on the design of an assembled system for a particular application, whereas the subject LTR presents the elements of hardware and system software in the MELTAC platform that can be used in a variety of safety applications. Since no plant specific application of the platform as a safety system was provided with the LTR, this SE is limited to the evaluation of compliance with the relevant regulations and guidance documents to the degree to which they can be satisfied at the platform level. In effect, fulfillment of system-level requirements can only be partially evaluated generically based on the capabilities and characteristics of the MELTAC platform.

Determination of compliance with all applicable regulations remains subject to a plant specific licensing review of a complete system design based on the MELTAC platform. Plant-specific action items (PSAIs) have been established to identify criteria that should be addressed by an applicant or licensee referencing the LTR (see Section 5.2). These criteria are provided to facilitate an applicant's or licensee's establishment of compliance with the acceptance criteria identified in SRP Chapter 7, Table 7-1 and regulations in 10 CFR Part 50, that are applicable to a digital I&C system and that were in effect at the time of the MELTAC platform review. The PSAIs identified in Section 5.2 do not obviate an applicant's or licensee's responsibility to adequately address new or changed acceptance criteria or regulations that apply in addition to those used to perform this SE when making a changes to its facility.

The following regulations are applicable to the MELTAC LTR (Ref. 14):

- 10 CFR 50.54, "Conditions of licenses," (jj) and 10 CFR 50.55(i), "Conditions of construction permits, early site permits, combined licenses, and manufacturing licenses," require that structures, systems, and components must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed.
- 10 CFR 50.55a, "Codes and standards,"(h), incorporates the 1991 version of IEEE Std. 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," by reference, including the correction sheet dated January 30, 1995.

- 10 CFR Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants"
  - General Design Criterion (GDC) 1, "Quality standards and records"
  - GDC 2, "Design bases for protection against natural phenomena"
  - GDC 4, "Environmental and dynamic effects design bases"
  - GDC 13, "Instrumentation and control"
  - GDC 19, "Control room"
  - GDC 20, "Protection system functions"
  - GDC 21, "Protection system reliability and testability"
  - GDC 22, "Protective system independence"
  - GDC 23, "Protective system failure modes"
  - GDC 24, "Separation of protection and control systems"
  - GDC 25, "Protection system requirements for reactivity control malfunctions"
  - GDC 29, "Protection against anticipated operational occurrences"
- 10 CFR Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants"

SRP Chapter 7, Table 7.1, identifies Regulatory Guides (RGs), branch technical positions (BTPs), and industry standards that contain information, recommendations, and guidance and, in general, provide an acceptable basis to implement the above requirements for both hardware and software features of safety-related digital I&C systems. Based on the scope of the MELTAC platform and the limitations of a platform level review, the following guides and positions are determined to be relevant for consideration in this SE:

- RG 1.22, Revision 0, "Periodic Testing of Protection Actuation Functions," describes a method acceptable to the NRC staff for inclusion of actuation devices in the periodic tests of the protection system during reactor operation.
- RG 1.47, Revision 1, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems," describes a method acceptable to the NRC staff for complying with IEEE Std. 603-1991 in regard to bypassed and inoperable status indication for nuclear power plant safety systems.
- RG 1.53, Revision 2, "Application of the Single-Failure Criterion to Safety Systems," describes a method acceptable to the NRC staff for satisfying the NRC's regulations as they apply to the single-failure criterion to the electrical power, instrumentation, and control portions of nuclear power plant safety systems.
- RG 1.62, Revision 1, "Manual Initiation of Protective Actions," describes a method acceptable to the NRC staff for complying with the NRC's regulations as they apply to the means for manual initiation of protective actions provided (1) by otherwise automatically initiated safety systems or (2) as a method diverse from automatic initiation.
- RG 1.75, Revision 3, "Criteria for Independence of Electrical Safety Systems," describes a method acceptable to the NRC staff for satisfying physical independence of the circuits and electrical equipment that comprise or are associated with safety systems.

- RG 1.89, Revision 1, "Environmental Qualification of Certain Electronic Equipment Important to Safety for Nuclear Power Plants," describes a method acceptable to the NRC staff for complying with the NRC's regulations as they apply to qualification of electric equipment important to safety for service in nuclear power plants to ensure that the equipment can perform its safety function during and after a design basis accident.
- RG 1.97, Revision 4, "Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants," describes a method acceptable to the NRC staff for providing instrumentation to monitor variables for accident conditions.
- RG 1.100, Revision 3, "Seismic Qualification of Electrical and Active Mechanical Equipment and Functional Qualification of Active Mechanical Equipment for Nuclear Power Plants," describes a method acceptable to the NRC staff for satisfying the seismic qualification.
- RG 1.105, Revision 3, "Setpoints for Safety-Related Instrumentation," describes a method acceptable to the NRC staff for complying with the NRC's regulations for ensuring that setpoints for safety-related instrumentation are initially within and remain within the technical specification limits.
- RG 1.118, Revision 3, "Periodic Testing of Electric Power and Protection Systems," describes a method acceptable to the NRC staff for complying with the NRC's regulations as they apply to periodic testing of electric power and protection systems.
- RG 1.152, Revision 3, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," describes a method acceptable to the NRC staff for complying with the NRC's regulations as they apply to high functional reliability and design requirements for computers used in safety systems of nuclear power plants.
- RG 1.153, Revision 1, "Criteria for Safety Systems," endorsed IEEE Std. 603-1991 as a method acceptable to the NRC staff for satisfying the NRC's regulations with respect to the design, reliability, qualification, and testability of the power, instrumentation, and control portions of the safety systems of nuclear power plants prior to IEEE Std. 603-1991 incorporation by reference into the regulations.
- RG 1.168, Revision 2, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," describes a method acceptable to the NRC staff for complying with the NRC's regulations as they apply to the verification and validation of safety system software.
- RG 1.169, Revision 1, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," describes a method acceptable to the NRC staff for complying with the NRC's regulations as they apply to the configuration management of safety system software.
- RG 1.170, Revision 1, "Software Test Documentation for Digital Computer software Used in Safety Systems of Nuclear Power Plants," describes a method acceptable to the NRC staff for complying with the NRC's regulations as they apply to test documentation of safety system software.

- RG 1.171, Revision 1, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," describes a method acceptable to the NRC staff for complying with the NRC's regulations as they apply to the unit testing of safety system software.
- RG 1.172, Revision 1, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," describes a method acceptable to the NRC staff for complying with the NRC's regulations as they apply to preparation of software requirement specifications for safety system software.
- RG 1.173, Revision 1, "Developing software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," describes a method acceptable to the NRC staff for complying with the NRC's regulations as they apply to the development processes for safety system software.
- RG 1.180, Revision 1, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," describes a method acceptable to the NRC staff for design, installation, and testing practices to address the effects of electromagnetic and radio-frequency interference (EMI/RFI) and power surges on safety-related I&C systems.
- RG 1.209, "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants," March 2007, describes a method acceptable to the NRC staff for satisfying the environmental qualification of safety-related computer-based I&C systems for service in mild environments at nuclear power plants.
- DI&C-ISG-04, Revision 1, "Task Working Group #4: Highly-Integrated Control Rooms—Communications Issues (HICRc)," describes methods acceptable to the NRC staff to prevent adverse interactions among safety divisions and between safety-related equipment and equipment that is not safety-related.
- Digital I&C-ISG-06, Revision 1, "Task Working Group #6: Licensing Process," describes the licensing process that may be used in the review of license amendment requests associated with digital I&C system modifications in operating plants originally licensed under 10 CFR Part 50.

The NRC staff also considered applicable portions of the branch's technical positions in accordance with the review guidance established within SRP, Chapter 7 in accordance with 10 CFR 50.34, "Contents of applications; technical information," (h)(3), as follows:

- Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603"
- Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std. 7-4.3.2"
- BTP 7-8, Revision 6, "Guidance on Diverse Instrumentation and Control Systems"
- BTP 7-11, Revision 6, "Guidance on Application and Qualification of Isolation Devices"
- BTP 7-12, Revision 6, "Guidance on Establishing and maintaining Instrument Setpoints"
- BTP 7-14, Revision 6, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems"
- BTP 7-17, Revision 6, "Guidance on Self-test and Surveillance Test Provisions"



- BTP 7-18, Revision 6, "Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems"
- BTP 7-19, Revision 6, "Guidance for Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems"
- BTP 7-21, Revision 6, "Guidance on Digital Computer Real-Time Performance"

### **3.0 TECHNICAL EVALUATION**

The following subsections identify and describe the MELTAC platform's components and evaluate these components and the processes used to develop them against the regulatory evaluation criteria identified in Section 2.0 of this SE.

#### **3.1 System Background**

The MELTAC platform development began in 1985 with the initial goal of being applied to non-safety-related applications and long term goal of being used for safety-related applications. The same equipment design is used for both non-safety-related and safety-related applications. Equipment designated for use in safety applications uses quality assurance (QA) methods for software design life cycle processes that are different from those used for non-safety-related MELTAC systems. MELTAC components that can be used in safety applications are identified as "MELTAC Nplus S" while components that can be used only in non-safety-related applications are identified as "MELTAC Nplus." These identifier distinctions apply to all aspects of MELTAC, including hardware, software documentation and engineering tools. Components unique to the MELTAC Nplus platform for non-safety-related applications are not discussed in this SE except to the extent of their interface with MELTAC Nplus S components in safety systems.

The MELTAC platform's components were originally designed, implemented, and qualified in compliance with the Japanese Electrical Association Guide (JEAG)-4101 and International Organization for Standardization (ISO)-9001. Because the MELTAC platform was not originally developed in accordance with currently endorsed NRC standards and regulations, MELCO performed a commercial grade dedication of the MELTAC platform to qualify it for use in safety-related applications for U.S. nuclear power plants.

The nuclear QA program employed for MELTAC was originally developed based on Japanese nuclear QA standards. This original QA program has since been revised to comply with 10 CFR Part 50 Appendix B. MELCO activities are now performed under the 10 CFR Part 50 Appendix B-compliant QA program as documented in the "MELCO Quality Manual" (Ref. 5). Furthermore, activities to develop I&C systems for US nuclear power plants will be performed under the 10 CFR Part 50 Appendix B-compliant quality program documented in the "Instrumentation & Controls U.S. Quality Manual" (Ref. 17).

#### **3.2 System Description**

The MELTAC platform is a digital computer based I&C PLC that uses qualified building blocks which can be assembled to produce safety-system applications such as reactor protection systems and engineered safety-features actuation systems. MELTAC building blocks are categorized as follows:

### Controller / Subsystem

The MELTAC controller includes a Central Processing Unit (CPU) chassis which contains either one or two subsystems (depending on the redundancy configuration required by the application), a switch panel, status display (switch) modules, and a fan unit. Each Subsystem includes power supply modules, CPU modules, control network interface (I/F) modules, a system management module and bus master modules. The controller includes one or more Input and Output (I/O) chassis which contain the systems I/O modules. The MELTAC platform includes a variety of I/O modules that can interface with various plant components. These modules are listed in Table 3.2-1 below.

### Safety Visual Display Unit

The MELTAC platform Safety Visual Display unit (S-VDU) consists of a special purpose MELTAC controller, peripherals, and a Liquid Crystal Display (LCD) touch screen.

### Control network

The control network is used to communicate safety-related data between multiple controllers (when used), and between controllers and the S-VDU processor(s) in the same division.

### Data Link

The data link is used to transmit process signals between the controllers that are in different safety divisions.

The numbers and types of components included in a MELTAC safety system design are defined by the application specific design requirements and by the number of slots available in the platform chassis modules.

Tables A.1 through A.17 in Appendix A, "Hardware Specification" of the MELTAC LTR (Ref. 14) list the Nplus S qualified components of the MELTAC platform requested to be reviewed by the NRC under this SE. On April 15, 2017, MELCO submitted a scope change request (Ref. 28) to remove modules associated with the nuclear instrumentation and radiation monitor from the scope of the MELTAC LTR. Because of this scope reduction, the NRC staff did not review MELTAC platform modules listed in Sections A.12, or A.13 of the MELTAC LTR. The resulting MELTAC Nplus S-qualified, platform-components list is provided below as Table 3.2-1.

**Table 3.2-1: MELTAC Nplus S Qualified Platform Components**

Category	Component	Module (Qualified Building Blocks)	Identifier (App. A)	Notes
CPU Chasis (3 Types) Mirror-split / Side-split / Non-split (Table 4.1.2-2)	SubSystem	Chassis	ZCAJS	Note 1
		CPU module	PCPJ	
		system management module	PSMJ	
		status display and switch module	PPNJ	

Category	Component	Module (Qualified Building Blocks)	Identifier (App. A)	Notes
		Control network IF module	PWNJ	
		bus master module	PFBJ	
	optical switch	optical switch	RJMA	
	CPU fan	fan module	KFNJ	Note 2
IO chassis	IO chassis	Digital / Analog IO modules	ZIOJS	
		PIF module	ZEHJS	Note 3
		Isolation module	ZISJS	Note 3
		optical Conversion module	ZMEJS	Note 3
	repeater module	For Subsystem-A	MRPJ-1	
		For Subsystem-B	MRPJ-2	
		For Subsystem-A/B Double Size	MRPJ-3	
	IO modules (Appendix A.4 - 9)	Current Input	MLPJ	
		Voltage Input	MAIJ	
		RTD 4 Line Type Input	MRTJ	
		Thermocouple K Type Input	MTCJ	
		Current Output	MAOJ	
		Voltage Output	MVOJ	
		Digital Input	MDIJ	
		digital output	MDOJ	
		Pulse Input Isolation module	MPIJ	
Isolation modules		Analog Isolation module	KILJ	
		Analog Isolation module	KIRJ	
		Pulse Input Isolation module	KIPJ	
Distribution modules		For Digital IO	KIOJ	
		For Current Input (Active)	KLPJ	
		For Current Input (Passive)		



Category	Component	Module (Qualified Building Blocks)	Identifier (App. A)	Notes
		For RTD Input (4 Wire)	KRTJ	
		For Thermocouple Input	KTCJ	
		For Voltage Input	KAIJ	
		For Current Output	KAOJ	
		For Voltage Output	KVOJ	
		For Pulse Signal Input	KAIJ	
Termination Unit		Terminal Unit module	PSND	Note 2
Power Supply modules	Power Supply (PS)	CPU Power Supply	PS-CPU	Note 3
		I/O Power Supply	PS-IO	
	Power Supply (PPSJ)	CPU Power Supply	PPSJ (S Capacity)	Note 3
		CPU Power Supply	PPSJ (L Capacity)	
Power Interface Modules		Built in Contact PS	DPOJ	
S-VDU Panel		S-VDU Panel module	T10DH	
		Frame Memory Unit	PFDJ	
		Electrical/optical Conversion module	MEOJ	

Note 1: The reprogramming version of the CPU chassis (ZCAJS-A23) is not accepted for use in operational safety systems. Only the ZCAJS without the -A23 suffix may be installed in the safety system. The re-programming chassis may be used to perform reprogramming activities only.

Note 2: The KFNJ fan Assembly module and the PSND Termination Unit module were not included in the platform qualification equipment during testing and are therefore not qualified for use in safety-related applications. This is generic open item 1. See Section 5.1.

Note 3: These modules were not included in the platform qualification equipment during equipment qualification (EQ) testing but were qualified by analysis. See Section 6.0, "Qualification by Analysis" of the summary of MELTAC platform EQ (Ref. 31) for additional information on qualification of these items.

Figure 3.1-1 shows a picture of the MELTAC CPU chassis for a redundant standby controller configuration. A description of the MELTAC platform hardware is provided in the following sections.



**Figure 3.1-1: MELTAC platform modules in CPU chassis**

(Source - Figure 4.1.1-4 of MELTAC platform LTR)

### 3.2.1 MELTAC platform Hardware and Architecture

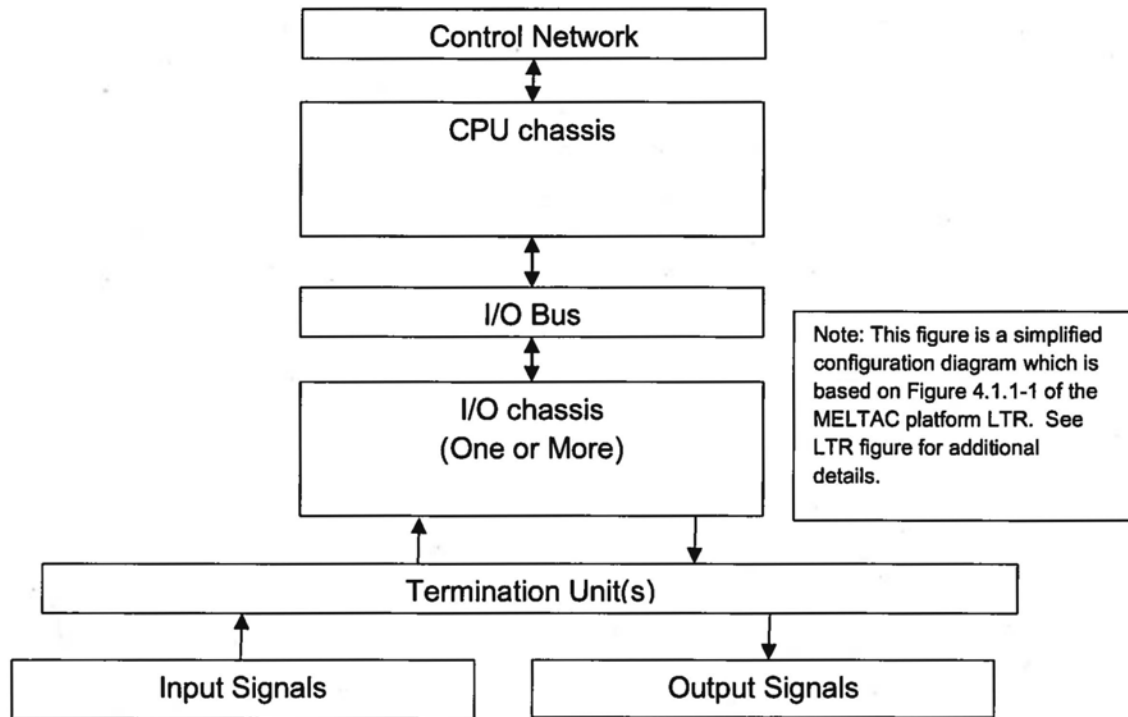
The MELTAC platform is built from a set of modular, standardized components, including chassis, electronic boards, and cabling, to implement a variety of nuclear safety I&C systems applications. The MELTAC component modules are connected to the chassis backplane as shown in Figure 3.1-1. A safety system based on the MELTAC platform may include electronic boards listed in Table 3.1-1.

The MELTAC LTR (Ref. 14) describes three possible controller configurations which can be used for safety system applications.

- **Single Controller** – Includes only one subsystem which operates as the controlling processor.
- **Redundant Parallel Controller** – Includes two subsystems with both operating as controlling processors in parallel.
- **Redundant Standby Controller** – Includes two subsystems with one operating as a controlling processor and the other operating in a standby mode, ready to automatically take control if a controlling processor failure occurs.

The redundant configurations are designed to improve system reliability and are not intended to address the single failure criteria of IEEE Std. 603-1991. The redundant subsystems are therefore not required to be independent from each other. The NRC staff evaluation of the MELTAC redundant configurations is therefore limited to reliability criteria for safety I&C systems as specified in IEEE Std. 603-1991 Section 5.15.

The architecture of each MELTAC subsystem includes a control network, a CPU chassis with one or more I/O chassis connected through an I/O bus, and field connections to input and output devices through a Termination Unit as depicted in Figure 3.2.2-1.



**Figure 3.2.2-1: MELTAC Subsystem Architecture Configuration**

The I/O modules installed in the I/O chassis receive process input signals through the Termination Units. Signals are converted into digital signals which are distributed to the CPU chassis through the I/O bus. A bus master module in the CPU chassis receives input data and transfers it to the CPU module through the CPU chassis backplane via the I/O bus. Control-function logic is performed by the CPU and system-output signals such as safety-actuation signals are sent to the output modules through the I/O bus in the reverse direction.

The CPU chassis includes a fan assembly to provide forced air cooling to the CPU electronics components, a CPU module, a system-management module, a status-display module, a bus-master module and a control-network interface. Each of these subcomponents is described in the following subsections.

#### 3.2.1.1 MELTAC Central Processing Unit Chassis

The MELTAC CPU chassis is a structure which houses various CPU module components. It includes slots for insertion of subsystem components, a status display and switch module, and a

CPU fan. Subsystem components that can be inserted into a CPU chassis are: CPU modules, system-management modules, control-network-interface modules, and bus-master modules.

There are two types of CPU chassis available for use. One is a mirror-split chassis design which supports the redundant standby controller configuration and the other is a non-split CPU chassis which can be used for all available configurations (i.e., single controller, redundant parallel, and redundant standby).

A CPU fan is installed on the top of the CPU chassis to cool the modules installed in the CPU chassis. The CPU fan is equipped with a fan stop detection circuit which provides a contact signal to the system management module. The fan-stop-detection circuit controls a relay, which generates an input to the MELTAC controller when a fan failure or loss of fan power is detected.

#### 3.2.1.1.1 CPU Module

The CPU module executes the MELTAC basic software and application software to control computational processing and safety functions assigned to the MELTAC platform based safety system.

The CPU module uses a 32-bit microprocessor. This processor module performs internal operations and shares data with other modules within the CPU chassis via a backplane data bus. Data transfer between the CPU module and other modules is accomplished in an asynchronous manner such that all modules operate with separate clock signals. This module uses flash-read only memory (F-ROM) for storing the basic software and application software, setpoints, and constants.

#### 3.2.1.1.2 System Management Module

The system-management module monitors the status of the CPU module and executes auxiliary controller functions not directly related to the CPU module as described below.

The system-management module contains an auxiliary digital input / digital output (DI/DO) which can be configured to generate alarms such as fan failure. The system-management module also has an ethernet interface for communicating with the MELTAC engineering tool when it is connected (see Section 3.2.2.5 of this SE).

When the system is configured in one of the two redundant modes of operation described in Section 3.2.2 of this SE, the system-management module transmits and receives the changeover signal through a dedicated backplane bus to manage controller operational modes during system operation. The system-management module has a two port memory data link for communicating operation data between the standby mode subsystem and the control mode subsystem.

#### 3.2.1.1.3 Status-Display-and-Switch Modules

The status display-and-switch module or status-display module are mounted in the CPU chassis. The status display-and-switch module is used when the redundant-standby controller configuration is implemented to display the mode and alarms of the subsystem and to provide a means of performing manual operating mode change over using a switch. Operating modes include control mode and standby mode. These modes of operation are used to support the redundant parallel and redundant standby system configurations.



The status-display module is used when the redundant-parallel controller or single-controller configurations are implemented. This module displays the mode and alarms of the subsystem.

#### 3.2.1.1.4 Bus-Master Module

The bus-master module has four communication interface channels. Each interface channel can be defined to either control communication with I/O modules or to establish serial data link communication with controllers in a different safety division as follows.

When used to control communication with I/O modules, each communication channel is capable of controlling 96 I/O modules, enabling control of a maximum of 384 I/O modules per bus master module.

When used to implement serial data link communication between controllers in other safety divisions, two port memory access configuration is used to ensure that communication functions do not disrupt deterministic CPU operation.

#### 3.2.1.1.5 Control Network I/F Module

The control network I/F module facilitates connection of the controller to the control network. This interface employs a resilient packet ring (RPR) based on IEEE Std. 802.17, "IEEE Standard for Information Technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements Part 17: Resilient packet ring (RPR) access method and physical layer specifications." The control network uses optical fiber as a communication medium. An optical switch unit enables optical bypass for node maintenance. This module employs a two port memory to ensure that communication functions do not disrupt deterministic CPU module operation.

#### 3.2.1.1.6 CPU Power Supply Module

The CPU power-supply modules convert 120 VAC power to provide multiple outputs of +2.1 VDC and +5 VDC to the CPU chassis for distribution to installed CPU modules. CPU power-supply modules are equipped with overvoltage protection that de-energize 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. CPU Power Supply modules provide a contact output alarm signal when an output shutdown occurs.

#### 3.2.1.2 Input / Output Chassis

The MELTAC input / output (I/O) chassis is a structure which houses various MELTAC I/O module components. The I/O modules are mounted in one or more dedicated I/O chassis'. One I/O chassis can accommodate 16 I/O modules.

##### 3.2.1.2.1 I/O Modules

The I/O modules in the MELTAC platform provide the input and output functions and signal conditioning functions, including signal conversion and noise reduction.

The MELTAC platform includes several types of analog and digital modules to accommodate various I/O signal interfaces. The modules mounted in the chassis are connected to the bus

master modules in the CPU chassis via repeater modules. Repeater modules are used to shape and amplify data communication signals to be transferred to and from the I/O bus. Data transfer occurs through the I/O bus.

#### 3.2.1.2.2 I/O Power Supply Modules

The I/O power supplies convert 120 VAC power to provide +24 VDC for I/O modules, isolation modules, power interface modules, electrical to optical (E/O) converter modules, and fan Units. I/O power supply modules are equipped with overvoltage protection that de-energizes 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. I/O Power Supply modules provide a contact output alarm signal when an output shutdown occurs.

#### 3.2.1.3 Terminal Unit

Terminal units provide an electrical connection interface between external field cables and the MELCO distribution and I/O modules. There are two types of terminal units available in the MELCO platform: one for analog I/O and one for Digital signal I/O.

#### 3.2.1.4 Distribution Module

Distribution modules distribute input signals to system I/O modules. Distribution modules also provide surge absorption functionality between the I/O modules and the terminal unit. A variety of distribution modules are available in the MELTAC platform. The type of distribution module used is dependent on the type of I/O module being interfaced.

#### 3.2.1.5 Isolation Chassis

The MELTAC platform includes an isolation chassis which is a structure that houses various MELTAC isolation module components when such components are required for a system design.

##### 3.2.1.5.1 Isolation Modules

Isolation modules provide electrical isolation between equipment in different safety divisions. Analog isolation modules receive analog input signals or pulse input signals and transmit corresponding analog output signals. Isolation modules do not rely on software processing to perform their functions.

Electrical isolation is provided between the I/O signals within the isolation module. The isolation modules are mounted in dedicated isolation chassis. A single isolation chassis can accommodate 14 isolation modules.

##### 3.2.1.5.2 Power-Interface Module

Power-interface (PIF) modules receive output commands resulting from subsystem operation, and control power to actuate plant components. There are several types of PIF modules sub-boards available to support different types of plant components. Each PIF module is configured with the appropriate sub-board for compatibility with the component being controlled.

PIF modules receive output commands from the MELTAC safety processors via the I/O bus connections to the I/O chassis backplane. PIF modules are used to control power to drive the switchgears, solenoid valves, etc. for actuation of plant components.

PIF modules use power semiconductor devices for controlling power instead of electromechanical relays to eliminate the need for periodic replacements. The PIF modules can also be used to receive inputs from external contacts to support transmission of component status signals to the subsystem.

#### 3.2.1.6 Safety Visual Display System

The MELTAC Safety Visual Display system consists of a Safety Visual Display unit (S-VDU) panel and S-VDU processors.

##### 3.2.1.6.1 Safety Visual Display Unit Panel

The S-VDU panel is an human-system interface (HSI) device which displays safety-system operational screens and provides a touch screen operator interface to enable operators to interact with the safety system. The S-VDU panel consists of a color-graphic display with an integral touch-screen-operator interface.

The S-VDU panel receives analog video signals from the S-VDU processor. Inputs signals from the operator-touch-screen interactions are transmitted to the S-VDU processor in the form of x-y coordinate data using a serial communications interface.

##### 3.2.1.6.2 S-VDU Processor

The S-VDU processor interfaces with MELTAC safety controllers to support all S-VDU display and operator interface functions. S-VDU processors receive data from safety controllers within the same division via the control network. The S-VDU processor organizes the static data of pre-configured screens with the live plant data and then displays those combined images on the S-VDU panel by means of the analog video signal interface. S-VDU processors store static data for each pre-configured display screen in accordance with application defined requirements.

S-VDU processors have a single subsystem architecture which is similar to that of the safety controller subsystems. The software structure of the S-VDU processors is based on the same design as that of the MELTAC basic software.

Operators perform manual actions by touching an operation switch image displayed on the S-VDU panel. The results of a touch screen operation are sent in the form of x-y coordinate data from the S-VDU panel to the S-VDU processor. This is an RS-232C point to point serial communications interface, which is converted from electrical to optical, to increase the transmission distance. The S-VDU processor converts the x-y coordinate data received from the S-VDU panel to plant control data and sends the data to the safety function controllers via the control network.

The control network interface receives live plant data from the safety function controllers within the assigned division, and sends the plant control data to the safety function controllers via the control network. The control network and S-VDU display system are both intra-divisional. No cross channel data is exchanged between S-VDU processors belonging to different safety

divisions and S-VDU processors of different divisions are operationally independent from each other.

### 3.2.1.7 Watchdog Timer

Several modules of the MELTAC platform incorporate the use of watchdog timers (WDT) to monitor processor performance and to initiate predefined failure states when controller processor failures are detected.

[ The NRC staff reviewed the detailed description of WDT functionality, provided in Section 4.1.5.7 of the MELTAC LTR (Ref. 14). This section includes figure 4.1.5-3, which shows the architectural arrangement of WDTs within various platform modules. There is a predefined timer value associated with each WDT. During operation, the WDT timer continuously counts up and the basic software resets the timer value to zero at regular intervals. The WDT counter functions independently from the processor such that a failure of the monitored processor cannot prevent the WDT timeout function from occurring. If the basic software fails to reset the WDT within the predefined timer value, then the WDT times out and causes the controller to transition to its failure state which is predefined for each safety system application. A plant-specific action to define required system failure states is contained in PSAI 5.2.7. An alarm indication is also actuated when a WDT time-out occurs.

### 3.2.2 MELTAC System Communication

The Communication component of the MELTAC platform is composed of three types of data communication. These are:

- Control network communication
- Data link communications
- Maintenance network communications

All three of these communication types incorporate the following design bases principles:

- Asynchronous communication is used. The CPU module and the communication controller tasks are executed asynchronously.
- Communications are performed by means of shared two port memory. This allows data to be communicated between the two digital components with no synchronization.
- The CPU module performs no communication handshaking that could disrupt deterministic safety logic processing. The digital processing components that execute the safety functions are separate from digital processing components that perform communications functions such as protocol management and handshaking.
- Predefined data size and structure are used during data transfer to ensure deterministic communication.
- Electrical communication processing faults in one electrical division (or controller) cannot adversely affect performance of the safety function in other divisions (or controllers).



### 3.2.2.1 Control Network (Intra-Divisional Communication)

Control-network communication is used to support data exchange between processor nodes of a single safety division. Processor nodes can include the CPU application processors, component control processors, and S-VDU processors.

The control network can be used as an interface to non-safety-related systems such as plant computers. If a MELTAC control network is implemented in this way, communications independence must be established between the safety-related MELTAC based system and the connected non-safety-related system to ensure the requirements of IEEE Std. 603-1991, Section 5.6.3 are met. ISG 04 Section 3.1 also provides guidance on how independence criteria can be met when interfacing between safety-related and non-safety-related systems.

The control-network communicates plant process data and control signal data using a resilient packet ring (RPR) configuration based on IEEE Std. 802.17 over a gigabit ethernet physical layer with a deterministic periodic cycle. Control network communications are implemented only within a single safety division (i.e., Intra-division communication). Inter-divisional communication for support of safety-related functions is implemented using data link interfaces as described in Section 3.2.3.2 below.

Each control network node includes a control network I/F module which transfers data to and from the associated controllers data memory through a two port memory device. The control network I/F modules are interconnected in a ring configuration. Each connected module communicates through an optical switch using four independent optical cables: two for transmission and two for reception. Optical switches are used to allow any subsystem on the control network that is halted, failed or disconnected for maintenance to be bypassed in order to maintain the network ring topology.

Optical switches are designed to switch to a node bypass mode when de-energized. Bypassing of a control network node allows continued communication among other nodes of the network. Because each optical switch is powered by its associated control I/F module, a loss of power to a control network I/F module results in a node bypass so that network ring topology can be maintained.

The ring network topology is designed to be fault tolerant. Control network communications are initiated to the ring in both clockwise and counterclockwise directions to all connected nodes. When a single node failure occurs, the communications network automatically reconfigures the communications paths to maintain data communication pathways between all remaining operable nodes on the ring. The reconfiguration of communication paths causes a momentary disruption of data communication on the control network; however, this disruption would only affect the division of the failed component. Therefore, such a failure would not adversely affect the safety function response performance (See Section 3.7.1 for NRC evaluation of MELTAC platform response time performance).

### 3.2.2.2 Data Link (Inter-Divisional Communication)

Data-link communication is used to transmit process signals between the controllers in different safety divisions or trains. Data-link communication may also be used to send data to a non-safety-related MELTAC controller. The data link uses a broadcast protocol with a one Megabit per second throughput, and does not use communication handshaking. This means that all transmitted data from a division communication controller is transferred to the

communication controllers of all connected divisions. The MELCO data link interfaces use the recommended standard (RS)-485 serial communication signal standards which is also known as telecommunications industry association (TIA)-485. RS-485 specifies electrical characteristics of the generator and the receiver components of the communication interface.

Data-link interfaces can also be configured to interface with non-safety-related systems such as plant computers. If a MELTAC data link is implemented in this way, communications independence must be established between the safety-related MELTAC based system and the connected non-safety-related system to ensure the requirements of IEEE Std. 603, Section 5.6.3 are met. ISG 04 Section 3.1 provides guidance on how independence criteria can be met when interfacing between safety-related and non-safety-related systems.

The MELTAC data-link interfaces operate in full duplex mode such that dedicated links are established for separate transmit and receive functions. Data is not sent in two directions for any of the individual communication ports so these ports are characterized as unidirectional ports.

The data link is interfaced to controllers of different safety divisions through bus master modules which include individual communications controllers and a two port memory to support independent operation of the communications modules and the CPU safety application logic processors. Each bus-master module has four communication ports. Each of these ports can be configured to be either a transmit port or a receive port depending on specific application requirements. The bus-master module produces electrical output signals to drive the communications output ports. The output is typically divided into three signal lines to support connectivity to three other independent safety divisions. Each output is converted into an optical signal by an E/O converter module. The transmission port for each of the E/O converter modules is connected by an optical cable to the reception port of an electrical to optical (E/O) converter module in another safety division. This is commonly referred to as a point-to point communications configuration.

Data is broadcasted periodically on a continuing basis to the receiving controllers without regard for the operating status of the receiving communications controllers. Bus-master module communication controllers include two port memory for storage and transfer of data to and from the destination CPU in a manner that maintains independence between the communications processors and the CPU safety logic processors in each safety division.

### 3.2.2.3 Data Link Isolation / Independence

The physical, electrical, and functional isolation between connected nodes of a data link communications interface include the following:

#### Physical Separation

The E/O Converter module of the data link allows for a distance of up to one kilometer between sending and receiving controllers. This allows the controllers to be geographically separated into separate areas of the plant.

#### Electrical Isolation

The MELTAC platform uses fiber optics and E/O converters to establish electric isolation between data link nodes of different safety divisions.

### Communication Isolation

A two port shared access memory configuration is used in conjunction with the unidirectional point-to-point data link communications functions which are described in Section 3.2.3.2 of this SE. This two port shared access memory establishes communications independence between the different safety divisions of a MELTAC based safety system. See Section 3.9.1.1 of this SE for a detailed evaluation of MELTAC data link independence characteristics.

#### 3.2.2.4 Maintenance Network (Safety to Non-Safety Communication)

Each MELTAC safety division includes a maintenance network to support connection of one or more non-safety-related maintenance workstations with any of the system safety-related processors or to the S-VDU. The workstations include MELTAC engineering tool application programs.

The maintenance network is used to communicate between the controllers or S-VDU processor and the MELTAC engineering tool. During normal system operation, the safety system controllers (including safety-related processors and S-VDUs) are disconnected from the maintenance network at the controller end.

Safety system controllers can be connected to the maintenance network periodically to support equipment maintenance. A connection signal can be configured in the application software to generate an alarm in the main control room (MCR) when the MELTAC engineering tool is connected.

#### 3.2.2.5 Maintenance Workstation

The maintenance workstation in a MELTAC safety system is a non-safety-related computer with the MELTAC engineering tool software that is connected to a single safety division maintenance network. Each safety division has a separate maintenance network that is isolated from the maintenance networks of all other divisions. Separate maintenance workstations for each division are connected to these maintenance networks. A maintenance workstation can only be connected to the maintenance network of a single safety division.

The MELTAC engineering tool is used to access and modify the data table of the controller when connected. The MELTAC engineering tool can be used to download new application software to a CPU module, however, this capability is disabled in the operating CPU chassis. In order to perform software downloads, CPU modules must first be installed into a dedicated external reprogramming chassis.

The MELTAC maintenance workstation running the engineering tool can be used to perform the following functions:

- Display self-test diagnostics reported from all plant safety system processors within the division.
- Store copies of software for all processors within the division.
- Conduct the manually initiated memory integrity check using stored software.
- Control the updating of software for any processor within the division. Software updates can only be performed when a processor is taken out-of-service and declared inoperable

by plant technical specifications and the processor CPU module is removed and transferred to a dedicated reprogramming chassis.

- Control simulated input values for troubleshooting processors within the division. This function can only be performed when a processor is taken out-of-service and declared inoperable by plant technical specifications.

### 3.2.2.6 MELTAC Reprogramming Chassis

[

] The reprogramming chassis is separate and independent from the on-line controller chassis and should never be installed into an operational MELTAC system cabinet. CPU software changes cannot be performed for a CPU module that is installed in a CPU controller chassis that does not have this hard wired connection.

Any basic or application software changes to a CPU module must be performed with the CPU module installed into a reprogramming chassis. The reprogramming chassis is connected to a MELTAC engineering network with a connected maintenance workstation running the MELTAC engineering tool to provide Read-Write access to the F-ROM and thus CPU basic and application software.

### 3.2.2.7 MELTAC Controller Communication Busses

There are two communication busses within each MELTAC controller; the first is the Futurebus+ and the second is the I/O bus. The Futurebus+ bus is the backplane bus in the CPU chassis. This bus is used to support communication between modules that are installed within a CPU chassis.

The I/O bus is the backplane bus in the I/O chassis. The I/O bus supports communications between the CPU chassis and the I/O modules installed in the I/O chassis. The bus master module and the I/O modules are connected to the I/O bus. The bus master module in the CPU chassis controls I/O bus communications by sending output and input data requests to the I/O module. The addressed I/O modules respond to requests from the bus master module by sending requested data through the I/O bus or by setting output signals to the requested values. This communication method is common to all MELTAC platform I/O modules, including the power interface modules.

## 3.3 MELTAC Software Architecture

The MELTAC platform consists of two types of software, basic software and application software.

### 3.3.1 MELTAC Basic Software

MELTAC basic software is common application independent software that performs single task processing to achieve deterministic behavior by adherence to proprietary design principles. These design principles are described in Section 4.1.3.1 of the MELTAC topical report (Ref. 14) and are evaluated separately in Section 3.7 of this SE.

The processes within the basic software and the order of their execution are:

- Initialization
- Timer Reset
- Mode Management / Redundant System Management
- Input
- Operation
- Self-diagnostics
- Output
- Tool Communication
- Redundant System Communication
- Remaining Time Diagnostics
- Constant Cycle Monitoring

### 3.3.2 MELTAC Application Software

MELTAC application software is a computer program designed to perform a group of coordinated tasks, and activities to achieve safety system functional requirements based on the application for which the MELTAC will be used.

The application software of the MELTAC platform is designed using the MELTAC engineering tool. Application software for functional algorithms is designed by combining graphical function blocks using the graphical user interface (GUI) of the MELTAC engineering tool. MELTAC application software is stored in the CPU flash-read only memory (F-ROM) and is subsequently accessed for execution purposes by the CPU safety processor.

The GUI-based programming language used for MELCO application development is called a problem-oriented language (POL). POL allows application software to be developed by graphically interconnecting conventional function blocks. Application software is then converted into execution data that is executed directly by the operation process of the basic software.

### 3.4 MELTAC Re-evaluation Program

The MELTAC platform was originally developed to comply with the Japanese nuclear quality programs. As such it was not developed to the quality standards required for use in U.S. nuclear safety applications. To facilitate use of the MELTAC platform in the United States, MELCO performed a re-evaluation of the MELTAC platform design and design processes using the commercial grade dedication processes defined in 10 CFR Part 21, "Reporting of Defects and Noncompliance." This re-evaluation effort is hereafter referred to as the MELTAC re-evaluation program (MRP).

In order to establish technical and quality characteristics equivalent to those required of a system developed under a 10 CFR 50 Appendix B QA program, MRP activities were performed by an independent MELCO organization that was not involved in the MELTAC platform design development. As such, the 10 CFR 50 Appendix B QA program was used to govern activities associated with the MRP.

MELCO is not currently on the nuclear procurement issues committee (NUPIC) list or included on an approved-vendor list. Therefore, an application referencing the MELTAC LTR (Ref. 14) must confirm that MELCO is added to the NUPIC list and/or confirm the MELCO quality processes conform to the utility's 10 CFR Part 50 Appendix B QA program – i.e., be put on the

applicant's approved vendor list (see Section 5.2 of this SE). The NRC staff used the following guidance to evaluate the MRP.

#### Regulatory Analysis of MRP

Clause 5.4.2 of IEEE Std. 7-4.3.2-2003 provides elaboration of the IEEE Std. 603-1991 criteria as it should be applied to qualifying existing commercial digital systems. In addition, Electric Power Research Institute (EPRI)-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-related Applications in Nuclear Power Plants," and EPRI-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," provide more detailed guidance on the commercial grade dedication of digital systems. These EPRI reports (Refs. 37 and 38 respectively) were reviewed by NRC and were determined to be acceptable for use in commercial grade dedication of digital I&C systems. It is noted that RG 1.152, Revision 3, also refers to EPRI-TR106439 as containing acceptable guidance for commercial grade dedication of computers for safety systems.

SRP, Appendix 7.0-A also identifies EPRI-TR106439 as providing an acceptable method for dedicating commercial grade digital equipment for use in nuclear power plant safety applications. EPRI-106439 references several of the verification methods described in EPRI-5652, "Guideline for the Utilization of Commercial Grade Items in Nuclear Safety-related Applications (NCIG-07)," as being appropriate for supporting commercial grade dedication.

#### Quality Assurance Program Inspection

An NRC inspection of MELCO energy systems center (ESC) was performed in December 2011 (Ref. 39). The purpose of the limited scope inspection was to assess MELCO's compliance with the provisions in 10 CFR Part 21, and selected portions of 10 CFR 50, Appendix B. This inspection found that:

- MELCO is effectively implementing its QA and 10 CFR Part 21 programs in support of MELTAC platform development.
- MELCO's 10 CFR Part 21 program and procedures were consistent with the regulatory requirements in 10 CFR Part 21.
- MELCO is effectively implementing its QA program and the associated 10 CFR Part 21 procedures.
- MELCO's design control program requirements are consistent with the regulatory requirements of 10 CFR Part 50 Appendix B, Criterion III.
- MELCO's design control procedures were being effectively implemented.
- MELCO's commercial grade dedication process adequately identified and verified the critical characteristics of the MELTAC platform that provide assurance that the platform will perform its safety function satisfactorily.
- The process implemented by MELCO is consistent with regulatory requirements associated with QA, including software development and commercial grade dedication.
- MELCO's design control procedures were consistent with the requirements of 10 CFR 50 Appendix B, Criterion III.
- The process implemented by MELCO is consistent with regulatory requirements associated with software development.
- The NRC staff inspection team determined the implementation of MELCO's commercial grade dedication program is consistent with the regulatory requirements.



Two instances of incomplete documentation were identified during this inspection. The first identified that no documentation of burn-in test performance was available. The second identified that the MELTAC safety system digital platform system specification failed to demonstrate adequate and complete compliance with applicable regulatory requirements. Neither of these instances of non-conformance were identified as having immediate safety concerns, however, MELCO performed corrective actions to resolve each. These corrective actions included documentation to support the MRP and procedure changes to ensure generation of required documentation when changes are made to the MELTAC system design. The NRC staff accepted MELTAC's resolution of these non-conformance items (Ref. 40).

#### MELCO QA Program Commercial Grade Dedication Processes

Section 6.0 of the MELTAC LTR (Ref. 14) describes the commercial grade dedication processes followed for the MELTAC platform by MELCO to comply with US nuclear regulatory requirements. MELCO used a document titled "Quality Manual Based on U.S. Nuclear Regulations" (Ref. 18) to establish programs and basic measures for implementation to ensure that products of the energy systems center, MELCO meet the U.S. regulations, standards, and quality requirements of prospective MELTAC customers. The Mitsubishi Electric Corporation, Energy Systems Center is the entity that furnishes safety systems and equipment for the MELTAC platform. Information to supplement the MELCO quality manual is also provided in a summary of MELTAC platform QA (Ref. 24).

The MELTAC quality assurance program is based on the requirements and recommendations of American Society of Mechanical Engineers, Nuclear quality assurance (NQA)-1-1994, "Quality Assurance Requirements for Nuclear Facility Applications." However, several exceptions and clarifications to this criteria are noted in the summary of MELTAC platform QA (Ref. 24). Among these exceptions are the use of EPRI TR-106439 and 107330 to support MELCO ESC commercial grade dedication activities.

Section 3.23 of the MELCO ESC summary of MELTAC platform QA identifies use of the commercial grade dedication guidance contained in EPRI TR-107330 which defines a set of critical PLC characteristics for generic (undefined) nuclear safety applications, and EPRI TR-106439 which contains the NRC approved guidelines for the evaluation and acceptance of commercial grade digital equipment. That section describes a strategy that MELCO followed during the MRP effort to qualify and accept the MELTAC platform under its 10 CFR Part 50, Appendix B compliant QA program.

MELCO ESC manuals and major QA plan procedures are listed in Table 1 of the MELCO ESC summary of MELTAC platform QA document. The quality procedures governing the commercial grade dedication processes include the following:

- Supplier Commercial Grade Survey Personnel Qualification Procedure
- Commercial Grade Item Acceptance Procedure
- Supplier Commercial Grade Survey Procedure
- Special Test and Inspection Procedure for Commercial Grade Item Acceptance
- Commercial Grade Service Acceptance
- Special Test and Inspection Procedure for Commercial Grade Service Acceptance
- Source Verification Procedure for Commercial Grade Service Acceptance

The MELCO quality procedures require preparation of a commercial grade dedication plan and a commercial grade dedication report to show compliance with EPRI TR-106439. The roles and responsibilities for MELCO personnel performing dedication process of commercial products is defined in the MELCO ESC Quality Manual.

The dedication process used during the MRP for the MELTAC platform contained two components of commercial grade dedication. These were: assessment of critical characteristics and assessment of built-in quality. The results of the MRP evaluation and dedication activities are documented in an MRP report (Ref. 3).

The MRP team created a compliance matrix to address the criteria of EPRI TR-107330, Table 1-1 and a compliance matrix to address the criteria of EPRI TR-106439 Tables, 6-4a, 6-4b, and 6-4c. These matrices correlate the EPRI requirements to the technical characteristics of the MELTAC digital platform and show how and where compliance with these criteria is achieved. These matrices also identify criteria where the MELTAC platform design was determined to be non-compliant and where alternate methods were used to satisfy criteria. For these cases a justification is provided which explains the reason for non-compliance as well as a description of alternative means used to address the criteria.

The NRC staff reviewed these tables (within Reference 3) and determined the MELCO commercial grade dedication effort met the criterion of EPRI TR-106439, and EPRI TR-107330 and, is therefore, acceptable. The MELCO MRP report provides adequate documentation of the performance of commercial grade dedication activities and provides references to records that support commercial grade dedication findings. The MRP report also summarizes the results of the assessment for the critical characteristics of the MELTAC platform.

The MRP review team evaluation results confirmed that required platform critical characteristics had been implemented in the MELTAC platform design. MELTAC platform critical characteristics include physical, performance and dependability characteristics. Because the software development lifecycle processes are critical characteristics of the MELTAC platform, the MRP review team also performed an evaluation of the MELTAC software lifecycle processes based on BTP 7-14 and established a baseline for MELTAC platform hardware and software which serves as a starting point for the MELCO 10 CFR 50 Appendix B controlled processes that will be used for subsequent development and maintenance activities.

Because the application software and hardware configuration will be plant application specific, the scope of the dedication activities is limited to the MELTAC platform hardware identified in Section 3.2.1 of this SE and MELTAC basic software.

In the MELTAC LTR (Ref. 14) and in Reference 3, MELCO stated that upon completion of the MRP, the platform including its software will be maintained under its 10 CFR 50, Appendix B compliant QA program. Furthermore, MELCO noted that if new boards are developed, or existing boards are modified, these activities will be performed in accordance with its Appendix B program and existing life cycle processes. The components will therefore be tested and qualified to maintain EQ to US standards.

Based on the information provided, the NRC staff found the hardware and software comprising the MELTAC platform, and described in the MELTAC LTR (Ref. 14), were properly dedicated and accepted into the MELCO 10 CFR 50, Appendix B compliant QA program. The NRC staff found the software life cycle for the MELTAC basic software followed a rigorous development process and that software plans are adequate for controlling future development activities.



## MELTAC Verification and Dedication Methods

The MRP team used verification methods 1 (Special Tests and Inspections of the MELTAC equipment) and four (Acceptable Performance Record of the MELTAC platform) to verify that MELTAC critical characteristics meet specified acceptance criterion. The MRP report identifies the applied verification method used for each of the MELTAC critical characteristics. The results of this report are summarized below.

### Identification and Verification of Critical Characteristics

The MELTAC platform is comprised of the hardware components described in Section 3.2.1 and software described in Section 3.3 of this SE. The scope of dedication activities performed by MELCO during the MRP to dedicate and qualify the MELTAC platform included both hardware and software elements of the design.

MELCO's MRP report identifies critical characteristics for the MELTAC platform and documents the results of the MRP teams' technical characteristics assessment. Critical characteristics of the MELTAC platform include physical, performance and dependability characteristics.

### Critical Characteristics – Physical

Per the guidance in EPRI-106439 and IEEE Std. 7-4.3.2-2003, critical physical characteristics of the digital system should address the size, mounting, power requirements, hardware model number, software version number, and data communications of system components. EPRI TR-106439 further notes that "special tests and inspections" (i.e., Method 1 per EPRI NP-5652) are typically appropriate for verifying these characteristics.

The NRC staff reviewed the MELTAC technical characteristics provided in Table 4-3 of the MRP Report (Ref. 3) and determined that physical characteristics of the MELTAC system were adequately identified as platform critical characteristics. These critical characteristics included the size, mounting and power requirements for MELTAC components.

The NRC staff also confirmed that requirements for the MELTAC basic software were included as critical characteristics of the MELTAC platform. These software critical characteristics included software version control via configuration management and data communications aspects of the design.

The NRC staff concludes that MELCO has identified and verified critical physical characteristics associated with the MELTAC platform in a fashion that is consistent with the guidance of EPRI TR-106439 and IEEE Std. 7-4.3.2-2003.

### Critical Characteristics – Performance

Per the guidance on EPRI TR-106439 and IEEE Std. 7-4.3.2-2003, performance characteristics are the functionality required from the device, as well as the performance attributes associated with that functionality. Performance characteristics may include items such as response time, memory allocation, reliability, required embedded functions and environmental qualification requirements. In addition, failure management and "must-not-do" functions are also considered performance characteristics for digital systems. EPRI-106439 further notes that "special tests and inspections", commercial grade surveys and supplier/item performance records (i.e.,

Methods 1, 2, and 4 per EPRI NP-5652) are typically appropriate for verifying these characteristics.

The performance characteristics are described at a high level in the LTR and at more detailed levels in the module specifications in appendix A and CPU module FPGA specification (Ref. 25).

The NRC staff reviewed the module specifications provided in Appendix A of the MELTAC LTR (Ref. 14) and in reference 25 and concludes that MELCO has identified and verified critical performance characteristics associated with the MELTAC platform in a fashion that is consistent with the guidance of EPRI TR-106439 and IEEE Std. 7-4.3.2-2003.

#### Critical Characteristics – Dependability

Per the guidance on EPRI TR-106439 and IEEE Std. 7-4.3.2-2003, dependability characteristics are those characteristics that address attributes that typically cannot be verified through inspection and testing alone and are generally affected by the process used to produce the device. This guide defines these attributes as critical characteristics to ensure that they are adequately addressed and documented during the dedication process.

The MRP team evaluated the processes used to produce MELTAC platform software and found them to be consistent with the requirements of IEEE Std.7-4.3.2 and other referenced standards. The MRP team defined platform development processes as critical characteristics of the MELTAC platform. These critical characteristics were therefore adequately addressed and documented during the MRP dedication process. The NRC also evaluated the MELTAC software development processes and determined they are acceptable. See Section 3.5 of this SE.

The NRC staff concludes that MELCO has identified and verified critical dependability characteristics associated with the MELTAC platform in a fashion that is consistent with the guidance of EPRI TR-106439 and IEEE Std.7-4.3.2-2003.

### 3.5 Software Development Process

Digital I&C safety systems must be designed, developed, installed, and tested to quality standards commensurate with the importance of the safety functions to be performed. The development of safety system software should progress according to a formally defined software life cycle. Implementation of an acceptable software life cycle provides the necessary software quality. There are two categories of software used in a MELTAC based safety system: basic software, and application software as described in Section 3.3 of this SE.

#### MELTAC Basic Software

The MELTAC platform software program manual (SPM) (Ref. 2) describes the MELTAC basic software development life cycle phases. The MELTAC basic software development lifecycle consists of the following phases:

- Planning Phase
- Requirements Phase
- Design Phase

- Implementation Phase
- Integration Phase
- Validation Phase
- Installation Phase
- Operations and Maintenance Phase

MELCO has committed to follow the design process described in BTP 7-14 for development activities associated with updating MELTAC basic software. Section 2.0 of the MELTAC platform SPM includes a table (Table 2.0-1) which correlates these MELCO defined phases with activity groups defined in BTP 7-14. Section 3.5.1 of this SE describes this process.

#### MELTAC Plant Application Software

MELCO will develop the application software for plant specific applications of the MELTAC platform to implement plant specific I&C and logic functions. The MELTAC platform application SPM (Ref. 30) describes the development lifecycle plans for MELTAC application software. The MELTAC application software development lifecycle consists of the following phases:

- Plant Requirements Phase
- System Requirements Phase
- Design Phase
- Implementation Phase
- Test Phase
- Installation Phase
- Operations and Maintenance Phase

MELCO has committed to follow the design process described in BTP 7-14 for development of application software. Section 2.2.1 of the MELTAC platform application SPM provides an overview of the MELCO defined Phases and Section 3.0 provides an outline of the MELTAC software development program. The NRC staff determined that this MELTAC application SPM is closely aligned with Activity Groups defined in BTP 7-14.

An applicant or licensee referencing the MELTAC LTR (Ref. 14) should provide application specification(s) to define the requirements necessary for the development of the plant specific applications. An applicant or licensee referencing the MELTAC LTR should also confirm that the development of its application software followed the development process of the MELTAC platform application SPM (Ref. 30). This is PSAI 5.2.2.

#### 3.5.1 Software Development Lifecycle Process Planning

IEEE Std.603-1991 requires that the quality of components and modules be established and maintained in accordance with a QA program. IEEE Std.7-4.3.2-2003 amplifies this requirement for software quality. SRP BTP 7-14 describes the basis for accepting software for safety functions as including confirmation that acceptable plans were prepared to control software development activities.

SRP BTP 7-14, Section B.2.1, "Software Life Cycle Process Planning," identifies the software life cycle planning information subject to review in terms of the software plans. SRP BTP 7-14, Section B.2.2, "Software Life Cycle Process Implementation," identifies software documents and

products subject to review to evaluate whether the software life cycle development process produced acceptable design outputs.

MELCO provided two software program manuals (SPMs). One SPM addresses the software development processes for platform basic software (Ref. 2) and a second SPM addresses the development processes for platform application software (Ref. 30). The basic software is software that operates the various MELTAC components and is independent of the specific application. The following subsections include the NRC staff evaluations of each of the MELTAC software lifecycle planning processes described in the two SPMs. The NRC staff approved the use of these plans as stated in the individual plan evaluation sections below.

#### 3.5.1.1 Software Management Plan

The software management plan (SMP) describes the management aspects of the software development project. SRP BTP 7-14, Section B.3.1.1, describes acceptance criteria for software management plans. RG 1.173 endorses IEEE Std. 1074-2006, "IEEE Standard for Developing Software Life Cycle Processes." IEEE Std. 1074-2006 describes, in terms of inputs and outputs, a set of processes and constituent activities that are commonly accepted as comprising a controlled and well-coordinated software development process. IEEE Std. 1074-2006, Chapter 3, "Project Management Process," describes an acceptable approach for software project management. It states that project management processes are, "the processes that initiate, monitor, and control software projects throughout the software life cycle."

The MELCO SMP is provided as Section 3.1 of the MELTAC platform SPM (Ref. 2) and as Section 3.1 of the MELTAC platform application SPM (Ref. 30). These two SMP's describe the management principles used for the development of MELTAC basic and application software for each phase of the associated software development life cycle. Both of these SMP's define the organizational structure of personnel involved in the development activities and describe the roles and responsibilities of key personnel and functional teams within the MELCO organization. The MELTAC SMPs also describe methods used for execution of development activities and for providing oversight of these activities.

For MELTAC basic software Development, functional teams include; a design team, a QA team, a V&V team, and a manufacturing department. Development of basic MELTAC software is performed by the design team. The QA team is responsible for assuring all activities performed throughout the MELTAC lifecycle follow required regulations, standards, and the processes defined in the SPM itself. The QA team is also responsible for assuring that MELCO policies and procedures are administered and correctly followed. The V&V team is responsible for confirming the correctness of the MELTAC basic software. The manufacturing department manufactures the hardware components of a MELTAC safety system and installs the basic software onto each hardware module.

For MELTAC application software development, functional teams include; a design team, a QA team, a V&V team, and a project management organization. Development of MELTAC application software is performed by the design team. The V&V team is responsible for confirming the correctness of the MELTAC application software. The QA team is responsible for assuring all activities performed throughout the MELTAC application development lifecycle follow required regulations, standards, and the processes defined in the SPM. The QA team is also responsible for assuring that MELCO policies and procedures are administered and

correctly followed. The project management team oversees project activities for all organizations involved in the development processes.

Both of the MELTAC SMPs define the level of independence established between each of the designated teams. Aspects of independence between these teams include management, budget and schedule considerations. The QA team and the V&V team are independent from the design team and from the manufacturing department and project management team.

A level of independence between the V&V team and the design section is established by specifying different reporting structures within the MELTAC ESC organization. The managers to which the V&V team and the design team report are administratively and financially independent of one another. This relationship between the design team and the V&V team is illustrated in Figure 3.1-1 of the MELTAC platform SPM and in Figure 2.1-1 of the MELTAC platform application SPM.

The NRC staff determined that required elements of a SMP are incorporated into the MELTAC SPMs. The NRC staff finds that the MELTAC SPMs establish adequate organization and authority structure for the platform and application design, the procedures to be used, and the relationships between major development activities. The NRC staff finds that the management structure described in the MELTAC SPMs provide for adequate project oversight, control, reporting, review, and assessment of MELTAC basic and application software. The NRC staff concludes that the MELTAC SPMs meet the requirements for software management planning as outlined in IEEE Std. 1074-2006 as endorsed by RG 1.173 and, are therefore, acceptable.

#### 3.5.1.2 Software Development Plan

The software development plan (SDP) describes the plan for technical project development. Section B.3.1.2 of BTP 7-14 describes characteristics expected of a software development plan for digital system development activities. The BTP indicates that the use of the software development plan should result in "a careful and deliberate development process which will result in high-quality software". Based on the BTP guidance, the NRC staff review focused on the definition of the development organization, identification of project risks, definition of lifecycle phase inputs and outputs, identification of methods and tools to be used, and identification of standards being followed.

The MELCO SDP is provided as Section 3.2 of the MELTAC platform SPM (Ref. 2) and as Section 3.2 of the MELTAC platform application SPM (Ref. 30). These two SDP's describe the activities required for MELTAC basic and application software for each of the defined lifecycle phases.

The NRC staff notes that the original development of MELTAC basic software was performed using the Japanese nuclear QA program processes. Subsequent dedication of MELTAC basic software was performed as part of the MRP that is described in Section 6.2 of the MELTAC LTR (Ref. 14). An evaluation of the MRP is included in Section 3.4 of this SE.

Section 2.0 of the MELTAC platform and platform application SPMs defines the software lifecycle phases used for the development of MELTAC basic and application software. The life cycles defined in each of these SPM's is consistent with a classic waterfall model like the model discussed in Section 2.3.1 of NUREG/CR-6101. The MELTAC basic and application software development lifecycle phases are listed in Section 3.5 of this SE.



The models used for MELTAC software development assume that each phase of the lifecycle is completed in sequential order from concept to the retirement phase. The NRC staff finds the MELCO choice of software lifecycle acceptable because the waterfall model is well suited for projects with known and stable requirements and where few changes to requirements are anticipated. Since MELCO selected an acceptable software life cycle model, the guidance criteria of IEEE Std. 1074-2006, Clause 2.4 has been satisfied. The following items are part of the SDP.

#### MELTAC software Life Cycle Tasks (Inputs & Outputs)

BTP 7-14, Section B.3.1.2.4 states that an applicant should identify which tasks are included with each life cycle phase, and state the life cycle inputs and outputs. Table 3.2-2 of the MELTAC platform SPM and Tables 3.2-1 through 5 of the MELTAC platform application SPM identify tasks which are performed for MELTAC basic and application software during the software lifecycle processes and identify the phases during which each task is performed. The SPMs also define the responsibilities for completion of software tasks.

#### MELTAC Software Integrity

The software integrity level (SIL) assigned to all MELTAC basic and application software is Level 4 as defined in IEEE Std. 1012-2004. No other types of software are included within the scope of the MELTAC SPMs. Therefore, no SIL scheme is specified.

IEEE Std. 1012-2004 provides guidance for establishment of a SIL scheme. The NRC endorsement of this standard provided in RG 1.168 states that software used in nuclear power plant safety systems should be assigned integrity level 4 or the equivalent, as demonstrated by a mapping between the applicant or licensee approach and integrity level 4 as defined in IEEE Std. 1012-2004. Because MELTAC basic and application software is used in safety systems to support safety-related functions, the NRC staff finds the SIL approach used in the MELTAC SPMs acceptable.

#### Management and Oversight of the Software Development Processes

The MELTAC SPMs specify responsibilities for ensuring that the design V&V and QA activities are conducted in accordance with the SPMs. The corrective action programs used during MELTAC software development processes are defined in Section 3.3.4.2.4 of the MELTAC platform SPM and in Section 3.3.5.4 of the MELTAC platform application SPM. These programs are designed to promptly identify and correct conditions adverse to safety and quality. These programs provide oversight to ensure that development processes will be followed and deviations from the established processes will be discovered in time to take necessary corrective actions.

The NRC staff determined the MELTAC software development plans are consistent with the criteria provided by IEEE Std. 1074-2006, "IEEE Standard for Developing Software Life Cycle Processes," as endorsed by RG 1.173. In addition, the MELTAC SPMs acceptably address the software development planning activities of BTP 7-14. The SPMs describe acceptable methods of organizing the software life cycle activities. The NRC staff, therefore, finds the MELTAC software development plans as applied to the MELTAC basic and application software to be acceptable.

### 3.5.1.3 Software Quality Assurance Plan

Section B.3.1.3 of BTP 7-14 describes the review criteria for software QA plans (SQAP). The SQAP shall conform to the requirements of 10 CFR Part 50, Appendix B, and the applicant's overall QA program. The regulation at 10 CFR Part 50, Appendix B states that the applicant shall be responsible for the establishment and execution of the QA program. The applicant may delegate the work of establishing and executing the QA program, or any part thereof, but shall retain responsibility for the QA program. The SQAP would typically identify which QA procedures are applicable to specific software processes, identify particular methods chosen to implement QA procedural requirements, and augment and supplement the QA program as needed for software.

IEEE Std. 7-4.3.2-2003, Clause 5.3.1, which is endorsed by RG 1.152 provides guidance on software quality assurance. IEEE Std. 7-4.3.2-2003, Clause 5.3.1, states that computer software shall be developed, modified, or accepted in accordance with an approved software QA plan. The SQAPs for MELTAC software are provided as Section 3.3 of the MELTAC platform SPM (Ref. 2) and as Section 3.3 of the MELTAC platform application SPM (Ref. 30). These two MELTAC SQAPs describe the methodology used for ensuring high quality of MELTAC basic and application software throughout the associated software development life cycle. The scope of the MELCO SQAPs includes both MELTAC basic software and MELTAC application software. Both of these software types are classified as SIL 4 as defined in IEEE Std. 1012-2004. The MELTAC platform SQAP applies to the original software that was developed under a Japanese QA program and was subsequently dedicated for use in safety-related applications as part of the MRP.

QA requirements for MELTAC basic and application software are defined in the MELTAC SQAPs. Quality assurance activities are; monitoring of process related metrics, procedure reviews, performance of software audits, performance of software tests, problem reporting, corrective action processing, media and supplier control, training, management and record keeping. These activities are supported by QA methods that are also described in the MELTAC SQAPs. The MELTAC SQAPs include a discussion of QA tasks and the responsibilities of the organizations performing software QA activities.

Documents associated with the performance of software QA activities are designated as QA Records in accordance with the MELCO 10 CFR 50, Appendix B QA program. Section 3.3.4.3, "Record Keeping" defines documentation identification and storage requirements for these records.

During the regulatory audit, the NRC staff reviewed several MELCO QA procedures made available for review and interviewed MELCO personnel to assess the SQA program effectiveness. The SQAPs were found to conform to the requirements of 10 CFR Part 50, Appendix B, and the MELCO overall QA program. The SQAPs identify which QA procedures are applicable to specific software processes. They also identify particular methods for implementing QA procedural requirements. The NRC staff found the SQAPs used to MELTAC software development to be an effective augmentation to the overall MELCO QA programs. During the audit, the NRC staff found the MELCO QA department has sufficient authority and organizational freedom, including sufficient independence from cost and schedule to ensure that the effectiveness of the QA organization is not compromised.

The NRC staff determined the MELTAC SQAPs in conjunction with the activities defined in the MELTAC independent V&V plans (described in Section 3.5.1.6 of this SE) are compliant with

the requirements of IEEE Std. 730-2002. Therefore, they provide reasonable assurance that high quality MELTAC basic and application software capable of performing assigned safety functions is produced for MELTAC digital I&C systems.

#### 3.5.1.4 Software Integration Plan

BTP 7-14, Section B.3.1.4 describes expectations for software integration plans. Note: software integration in this context refers to integration of the software with hardware components, rather than integration of various MELTAC hardware components. The section indicates that such plans should contain information on tests to be performed on the integrated hardware / software system. The NRC staff review focused on the clarity and completeness of the integration plans, with specific emphasis on the treatment of error handling / fault management functions and any non-conformances found during testing.

IEEE Std. 1074-2006, "IEEE Standard for Developing Software Life Cycle Processes," Clause A.1.2.8, "Plan Integration," contains an acceptable approach relating to planning for integration. The software Integration Plans for MELTAC basic software are provided as Section 3.4 of the platform SPM (Ref. 2) and as Section 3.4 of the MELTAC application SPM (Ref. 30). Each of these plans describes three types of activities performed to accomplish integration requirements. These are:

- Integrate individual software units into complete executable modules,
- Integrate Executable modules into MELTAC Hardware modules, and
- Integration V&V testing of MELTAC hardware and software.

These three types of integration activities align closely with the phases of integration described in Section 3.1.7 of NUREG/CR-6101.

The MELTAC software integration plans (SIntPs) establish coordination with the MELTAC test plans and include discussions of tools, techniques, and methodologies needed to perform integration activities for MELTAC basic and application software components. The NRC staff determined the MELTAC SIntPs provide an adequate documented method for performing both basic and application software integration activities.

#### 3.5.1.5 Software Safety Plan

The acceptance criteria for a software safety plan (SSP) are contained in the SRP, BTP 7-14, Section B.3.1.9, "Software Safety Plan (SSP)" and Section B.3.2.1, "Acceptance Criteria for Safety Analysis Activities." These sections state that the SSP should provide a general description of the software safety effort, and the intended interactions between the software safety organization and the general system safety organization. It further states that NUREG/CR-6101, Section 3.1.5, "Software Safety Plan," and Section 4.1.5, "Software Safety Plan," contain guidance on SSPs. RG 1.173, Section C.3, "Software Safety Analyses," contains guidance on safety analysis activities while NUREG/CR-6101 also addresses guidance for these analyses.

The MELTAC SSPs are provided as Section 3.9 of the platform SPM (Ref. 2) and as Section 3.9 of the MELTAC platform application SPM (Ref. 30). The MELTAC SSPs describe safety analysis activities which are conducted for each phase of the basic and application software lifecycles. The MELTAC SSPs include descriptions of the methods used for mitigation of potential software hazards pertaining to MELTAC basic and application software.

MELCO does not have a dedicated software safety organization, however, the MELTAC SSPs define intended interactions between the design team and the V&V team by defining organization responsibilities. Both the design team and the V&V team have responsibilities to perform software safety activities and to ensure the requirements of the SSPs are followed. MELCO uses V&V anomaly reports to document software safety concerns and to track actions taken to address these concerns. Documentation requirements for ensuring safety analysis activities have been successfully accomplished for each life cycle activity group are specified in the MELTAC SSPs. The NRC verified this during the regulatory audit. The NRC staff determined that software safety documentation shows that system safety requirements have been acceptably addressed for each activity group.

The NRC staff determined that planning for MELTAC basic and application software safety is appropriate for the MELTAC platform and is therefore acceptable. Furthermore, the NRC staff concludes that software safety planning as executed by the MELTAC SSPs provides acceptable assurance that software safety activities will be effective in resolving safety issues presented during the design and development of basic and plant application software.

#### 3.5.1.6 Software Verification and Validation Plan

The acceptance criteria for software V&V plans (SVVPs) are contained in SRP BTP 7-14, Section B.3.1.10, "Software V&V Plan (SVVP)." This SE states that RG 1.168, which endorses IEEE Std. 1012-2004, "IEEE Standard for Software Verification and Validation," provides methods acceptable to the NRC staff for meeting the regulatory requirements as they apply to V&V of safety system software. RG 1.168 specifically notes that software to be used in safety systems should be assigned SIL 4, as defined in IEEE Std. 1012-2004. The review guidance emphasizes independence of the review organization, the quantity and quality of V&V staff and documentation of V&V activities. The NRC staff review focused on the above noted aspects of V&V.

The MELTAC SVVPs are provided as Section 3.10 of the SPM (Ref. 2) and as Section 3.10 of the MELTAC platform application SPM (Ref. 30). The MELTAC SVVPs provide general descriptions of the software verification and validation effort by describing V&V activities that are conducted for each phase of the basic and application software lifecycles.

The SIL assigned to all MELTAC basic and application software is level 4 as defined in IEEE Std. 1012-2004. No other types of software are included within the scope of the MELTAC SPMs. Therefore no SIL scheme is specified. Because MELTAC basic and application software is used in safety systems to support safety-related functions, the NRC staff finds the SIL approach used in the MELTAC SPMs acceptable.

The MELTAC SMPs (Section 3.1 of the software program manuals) describe the MELCO development organization which includes several functional teams. Functional teams include; a design team, a QA team, a V&V team, and a manufacturing department. The level of independence established between each of these four teams is also defined in the software SMPs. Aspects of independence between these teams include management, budget and schedule. The QA team and the V&V team are independent from the design team and from the manufacturing department.

The MELTAC SVVPs further states:

...the V&V Manager, the V&V team Manager, and V&V team Members shall be technically, organizationally and financially independent of the design team ...

The NRC staff confirmed the levels of independence established by reviewing independent V&V (IVV) documentation and by performing an audit at the MELCO facilities in Warrendale PA. During this audit, the NRC staff performed interviews with members of the design, V&V and QA organizations. The NRC staff determined that an adequate level of independence exists between these organizations and that an appropriate level of technical competence is established and maintained within the independent V&V staff.

The MELTAC SVVPs define a minimum set of V&V activities to be performed for each of the product development lifecycle phases. One of these activities is to prepare a project specific V&V task manual during the concept phase. Updates to the V&V task manual are performed during each of the subsequent phases. The NRC staff reviewed the updated V&V task manual for MELTAC basic software and determined the tasks to be consistent with tasks specified in IEEE 1012-2004 for SIL Level 4 software.

The NRC staff finds the MELTAC SVVPs for basic and application software to be consistent with the criteria of IEEE Std. 1012-2004, "IEEE Standard for Software Verification and Validation," as endorsed by RG 1.168.

#### 3.5.1.7 Software Configuration Management Plan

The acceptance criteria for software configuration management plans (SCMPs) is contained in SRP BTP 7-14, Section B.3.1.11, "Software Configuration Management Plan (SCMP)," and Section B.3.2.3, "Acceptance Criteria for software Configuration Management Activities." These sections state that both: (1) RG 1.173 that endorses IEEE Std. 1074-2006, Clause A.1.2.2, "Plan Configuration Management," and (2) RG 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," that endorses IEEE Std. 828-2005, "IEEE Standard for Configuration Management Plans," provide an acceptable approach for planning configuration management. SRP BTP 7-14, Section B.3.1.11 further states that additional guidance can be found in IEEE Std. 7-4.3.2-2003, Clause 5.3.5, "Software configuration management," and in Clause 5.4.2.1.3, "Establish configuration management controls." NUREG/CR-6101, Section 3.1.3, "Software Configuration Management Plan," and Section 4.1.3, "Software Configuration Management Plan," also contain guidance on configuration management.

The MELTAC SCMPs are provided in Section 3.11 of the SPM (Ref. 2) and as Section 3.11 of the MELTAC platform application SPM (Ref. 30). The SCMPs are applicable to all MELTAC basic and application software as well as software tools used in the development of MELTAC software. The MELTAC SCMPs describe methods for identifying basic and application software configuration items. The SCMPs also define methods used to establish and maintain configuration control when changes to basic or application software are made as well as methods for recording and reporting the status of MELTAC software changes.

A configuration control board is used to approve changes to MELTAC software and to establish new baselines. The MELTAC SCMP establishes criteria for establishment of a configuration control board and describes the configuration control processes used during software development. These processes include change initiation, change control and change approval. During a regulatory audit (Ref. 33), the NRC staff observed MELCO's use of configuration management tools to control access to documents and MELTAC software files, manage change



requests, and track changes. The NRC staff also reviewed configuration management guidance documents and procedures as well as configuration management sheets. The NRC staff's observations during the audit support a finding of reasonable assurance that appropriate configuration management activities are being performed.

The NRC staff concludes that MELTAC SCMPs conform to the requirements identified in IEEE Std. 828-2005, as endorsed by RG 1.169. This meets the criteria of BTP 7-14, Clause 3.4.1.7 and is therefore acceptable.

#### 3.5.1.8 Software Test Plan

The acceptance criteria for a software test plan (STP) are contained in SRP BTP 7-14, Section B.3.1.12, "Software Test Plan." Section B.3.1.12 of BTP 7-14 contains review guidance for software test plans. Pointers are provided to the endorsements in RGs 1.170 which endorses IEEE Std. 829-2008, "Test Documentation" and 1.171 which endorses IEEE Std. 1008-1987. Among the key attributes expected of a software test plan are description of the test organization(s), testing strategy, testing criteria and testing records.

The MELTAC STPs are provided as Section 3.12 of the SPM (Ref. 2) and as Section 3.12 of the MELTAC platform application SPM (Ref. 30). The MELTAC STPs describe testing activities performed on the basic and application software of the MELTAC platform. The MELTAC STPs are used in conjunction with the SVVPs to identify required test activities to be performed by the V&V team. The STPs provide details of test methods and tools used during test activities and establish minimum content requirements for test documents.

The NRC staff determined the MELTAC STPs cover all testing performed on MELTAC basic and application software. Platform basic software testing includes component V&V testing, integration V&V testing, system testing, and acceptance testing. The MELTAC STPs provide mapping between these MELTAC testing activities and testing activities called for in IEEE Std. 1012-2004.

The NRC staff found that test responsibilities are assigned to appropriate personnel and that adequate provisions for re-test are included to address situations where test failures occur. MELTAC test failures are documented in V&V anomaly reports. The processes for addressing V&V anomaly reports are described in Section 3.10.5, "V&V Reporting Documentation Requirements" of the MELTAC SVVPs. The process for resolving V&V anomalies includes performance of regression analysis to determine the extent to which V&V activities shall be repeated. Regression tests may be required after any modification to the basic software as determined by the results of the regression analysis activity. The MELTAC STPs assign responsibility for test definition, design, and performance to the V&V team.

The NRC staff determined the software test plans as implemented in the MELTAC STPs and SVVPs are sufficiently comprehensive to demonstrate that a MELTAC based safety system will perform its required safety functions. See Section 3.5.2.2 of this SE for evaluation of system V&V activity results. This meets the criteria of BTP 7-14, Clause 3.1.12 and is therefore acceptable.

#### 3.5.2 Software Implementation Documentation

This SE summarizes the evaluation of the software implementation-documentation of the MELTAC platform basic software. This documentation corresponds with the software life cycle

process implementation information described in SRP BTP 7-14, Section B.2.2, "Software Life Cycle Process Implementation." and Section B.3.2, "Acceptance Criteria for Implementation."

#### 3.5.2.1 Safety Analysis

The acceptance criteria for software safety analysis activities are contained in the SRP, BTP 7-14, Section B.3.2.1, "Acceptance Criteria for Safety Analysis Activities." This SE states: (1) the documentation should show that the system safety requirements have been adequately addressed for each activity group; (2) no new hazards have been introduced; (3) the software requirements, design elements, and code elements that can affect safety have been identified; and that all other software requirements, design, and code elements will not adversely affect safety. Further guidance on safety analysis activities can be found in NUREG/CR-6101 and RG 1.173, Section C.3, "Software Safety Analyses."

The NRC staff reviewed the assessments of the software safety activities provided in the V&V task reports (see Section 3.5.2.2 of this SE) and determined that safety analyses activities were performed in accordance with the MELTAC SVVP. The V&V task reports provide objective evidence that the system safety requirements have been correctly implemented, and provide reasonable assurance that no new hazards were introduced into the system as a result of software development activities. Software elements that have the potential to affect safety were identified, and safety problems and resolutions identified during the analyses were documented and dispositioned in an appropriate manner. Software requirements, including design and code elements, have been implemented in a manner which will not adversely affect the safety of a MELTAC based safety system. The NRC staff has determined that the safety analysis activities are acceptable and are compliant with SRP BTP 7-14, Section B.3.2.1.

#### 3.5.2.2 V&V Analysis and Reports

The MELTAC SVVP (Section 3.10 of Reference 2) describes the V&V tasks that are to be carried out during development of the MELTAC basic software. SRP, BTP 7-14, Section B.3.2.2, "Acceptance Criteria for Software Verification and Validation Activities," states that the acceptance criterion for software V&V implementation is that the tasks in the SVVP have been carried out in their entirety. Documentation should exist that shows that the V&V tasks have been successfully accomplished for each life cycle activity group. In particular, the documentation should show that the requirements, design, code, integration, and installation design outputs satisfy the appropriate software development functional and process characteristics.

The NRC staff reviewed the following V&V task reports to evaluate the degree to which MELTAC basic software V&V activities have been accomplished.

- CPU Module (PCPJ-31) FPGA Specification V&V Task Report (Ref. 25)
- MELTAC Controller Software Specification V&V Task Report (Ref. 25)
- Controller Program Specification V&V Task Report (Ref. 25)
- CPU Module (PCPJ-31) Source Code V&V Task Report (Ref. 25)
- CPU Module (PCPJ-31) FPGA Unit Test Task Report (Ref. 25)
- Controller Source Code V&V Task Report (Ref. 25)
- Controller Unit Test V&V Task Report (Ref. 25)

The NRC staff determined the MELTAC V&V task reports adequately describe a detailed and thorough V&V effort. The MELTAC SVVP was implemented in a manner which supports the development of basic software which will perform all required safety functions. The NRC staff found that activities performed and documented in the V&V task reports provide reasonable assurance that V&V efforts were effectively implemented to support the development of a software product that is suitable for use in safety-related nuclear applications. The V&V task reports are written such that the information reviewed, level of detail, and findings of the V&V effort are understandable and informative. The V&V task reports provide adequate documentation to show that V&V tasks were successfully accomplished for each software life cycle phase.

Problems identified during the V&V effort were entered into the MELCO corrective action program as anomaly reports. Problem descriptions and actions required to correct or mitigate each problem were adequately documented. The NRC staff reviewed examples of problem reports during the regulatory audit and found them to be consistent with the established processes. The NRC staff concludes that the software development functional and process characteristics of the V&V effort are acceptable. V&V activities performed for the MELTAC basic software development are acceptable and are compliant with SRP BTP 7-14, Section B.3.2.2.

#### 3.5.2.3 Configuration Management Activity

The MELTAC SCMP (Section 3.11 of Reference 2) describes the software configuration management (SCM) tasks that are to be carried out by MELCO (see Section 3.5.1.7 of this SE). The acceptance criteria for SCM activities are identified in BTP 7-14, Section B.3.2.3, "Acceptance Criteria for Software Configuration Management Activities." This acceptance criterion requires that the tasks in the software configuration management plan be carried out in their entirety. Documentation should exist that shows that the configuration management tasks for that activity group have been successfully accomplished. In particular, the documentation should show that: (1) configuration items have been appropriately identified; (2) configuration baselines have been established for the activity group; (3) an adequate change control process has been used for changes to the product baseline; and that appropriate configuration audits have been held for the configuration items created or modified for the activity group.

The MELTAC configuration management sheets provide documentation of configuration management activities performed during each phase of MELTAC platform development. The configuration management sheets include the system configuration status accounting, which identifies the baseline documents and versions at the end of each life cycle phase. These include plans, specifications, schematics, test procedures, test reports, and MELTAC source code.

MELCO maintains and controls MELTAC design documentation and program files as QA records. Changes to controlled files are tracked and can only be changed by using an approved software change process. During the regulatory audit (Ref. 33), the NRC staff reviewed the MELCO procedures for performing software changes and conducted an exercise involving making a sample software change using these procedures.

Configuration management sheets which are documents used control design configurations do not contain accounting of records associated with independent V&V activities. V&V records are instead managed under a separate IVV process and these documents were listed in V&V tables

within the associated module test reports. The tables identifying V&V records, were found to provide adequate traceability and control over the configuration of these records. During the audit, the NRC staff evaluated several configuration management sheets for various MELTAC components to ascertain the configuration status of those modules and associated records and to confirm that configuration status accounting processes were correctly implemented and were effective in controlling the MELTAC platform integrity.

The NRC staff determined the software configuration management processes and activities performed meet the requirements of IEEE Std. 828-1998 and American National Standards Institute/IEEE Standard 1042-1987 and are, therefore, acceptable. The MELTAC basic software configuration management activities adequately addresses the guidance in BTP 7-14, Section B.3.2.3.

#### 3.5.2.4 Testing Activity

The acceptance criterion for testing activities is contained in the SRP, BTP 7-14, Section B.3.2.4, "Acceptance Criteria for Testing Activities." This SE states that RG 1.168 Rev. 2, Section 7.2, and RG 1.170, Rev. 1 that endorses IEEE Std. 829-2008, "IEEE Standard for Software Test Documentation," and RG 1.171, Rev. 1 that endorses IEEE Std. 1008-1987, "IEEE Standard for Software Unit Testing", identify acceptable methods to satisfy software testing requirements.

The NRC staff reviewed basic software test activities as presented in Sections 3.12.2 for unit V&V tests and in 3.12.3.3 for Integration V&V tests. These testing activities for the MELTAC platform basic software were found to be consistent with the requirements of the controller software specification (Ref. 25), the CPU module CPUCNT\_FPGA specification (Ref. 25), and the I/O function program specification (Ref. 25). The test programs provided comprehensive test coverage of an integrated MELTAC platform based system. The NRC staff observed appropriate adherence to the test program procedures during the regulatory audit. Discrepancies discovered during the test performance were appropriately documented and addressed using the MELCO anomaly reporting process. The NRC staff confirmed proper resolution of test discrepancies by reviewing documentation during the regulatory audit. Test results and verification of test completion were documented in the MELTAC V&V task reports (References 25, and 29). The NRC staff found that the MELTAC software test activities adequately address the guidance in BTP 7-14, Section B.3.2.4 for the basic software.

The MELTAC platform LTR does not address testing activities associated with application software. Therefore, plant application software testing activities for MELTAC platform based safety systems must be performed during plant application development and thus could not be evaluated in this SE. Section 5.2.2 of this SE identifies additional application development activities including test related actions which must be addressed during specific plant application development.

#### 3.5.2.5 Requirements Traceability Evaluation

Evaluation criteria for the use of requirements traceability matrices (RTM) is contained in SRP, BTP 7-14. A definition for RTM is provided in Section A.3. Here it is stated that: "An RTM shows every requirement, broken down in to sub-requirements as necessary, and what portion of the software requirement, software design description, actual code, and test requirement addresses that system requirement." This is further clarified in Section B.3.3, "Acceptance Criteria for Design Outputs," in the subsection on Process Characteristics. This SE criteria

states that the RTM should show what portion of the software requirement, software design description, actual code, and test requirement addresses each system requirement.

A description of the process used by MELCO to perform MELTAC requirements traceability is provided in the summary of MELTAC platform V&V (Ref. 29). This document also describes the documentation structure and the categorization scheme used for MELTAC platform design documents. Establishment and verification of requirements traceability are defined as V&V activities that are performed throughout the product development lifecycle.

MELCO does not maintain a single RTM for the MELTAC platform. Instead, separate RTMs are created for each module of the MELTAC platform. The summary of MELTAC platform V&V includes a list of RTMs associated with these components.

The NRC staff reviewed these RTM's and used them to perform thread audits for several selected requirements during an audit in Warrendale, PA. The results of this audit are documented in Reference 33.

The NRC staff observed that requirements traceability tables show each of the requirements delineated in the system and hardware requirements specifications, as well as, the FPGA specifications, are broken down into sub-requirements for the MELTAC platform. The traceability matrices indicate which portion of the implementation documents and test requirements are being credited to address each system requirement. The NRC staff determined that requirements tracing processes provide reasonable assurance that all requirements are correctly implemented in the MELTAC platform hardware and software and are, therefore, acceptable.

#### 3.5.2.6 Failure mode and Effect Analysis

RG 1.53 describes a method acceptable to the NRC staff for satisfying the NRC's regulations as they apply to the single-failure criterion to the electrical power, instrumentation, and control portions of nuclear power plant safety systems. RG 1.53 endorses IEEE Std. 379-2000, and IEEE Std. 379-2000, Clause 5.5 identifies failure mode and effects analysis (FMEA) as a method to address common-cause failures when performing analysis to demonstrate that the single-failure criterion has been satisfied. Although no specific regulatory guidance on the format, complexity or conclusions of the FMEA exists, the FMEA should identify potential failure modes within a system to determine the effects of these failures on the system. The expectation is that each potential failure mode should be identified, and its effects should be determined. The FMEA should demonstrate that single-failures, including those with the potential to cause a non-safety-related system action (i.e., a control function) that results in a condition requiring protective action (i.e., a protection function), cannot adversely affect the protection functions.

The NRC staff reviewed the MELTAC platform FMEA methodology described in Section 7.3 of the MELTAC LTR (Ref. 14). The results of FMEAs for specific MELTAC platform module hardware and basic software are summarized in the summary of MELTAC platform reliability (Ref. 15). A MELTAC platform CPU module circuit block level FMEA (Ref. 25) was also provided as a supplement to the MELTAC LTR.

The NRC staff reviewed the MELTAC FMEA methodology and referenced documentation and determined the level of detail is appropriate for module level components of the MELTAC platform. The FMEA methods used by MELCO were found to be consistent with IEEE



Std. 379-2000 as endorsed by RG 1.53, Rev. 2. The MELTAC FMEA considers single detectable failures concurrent with identifiable but non-detectable failures, failures caused by the single failure and failures resulting in spurious system safety function actuations. The MELTAC FMEA results indicated that several of the platform modules rely upon application software functions for detection of failures.

Because the failure analysis were performed at platform component level, these FMEAs did not demonstrate that input signals or system level failures or failures that would cause a MELTAC based safety system to revert to a predefined safe state. The fail-safe states for MELTAC safety functions are also not generically defined and must be determined as a specific application development activity. These FMEAs also do not account for communication interface failures and the effects they would have on system level performance. Therefore, a system level FMEA should be performed during plant specific application development to identify potential system level failure modes and to determine the effects of these failure modes on plant safety. PSAI 5.2.7 of this SE identifies additional actions which must be addressed during specific plant application development.

Based on the NRC staff review of the MELTAC failure analysis, there is reasonable assurance that credible MELTAC component level failure modes have been properly identified and evaluated. Therefore, the criteria of RG 1.53 pertaining to platform component failure modes and effects are satisfied. However, system-level failure modes will need to be addressed during plant application development.

#### 3.5.2.7 Reliability Analysis

IEEE Std. 603-1991, Clause 4.9 requires the identification of the methods used to determine that the reliability of the safety system design is appropriate for each such design, and the identification of the methods used to verify that reliability goals imposed on the system design have been met; however, as discussed within RG 1.152 and DI&C-ISG-06, the NRC's acceptance of the reliability of digital I&C systems is based on deterministic criteria for both hardware and programming, and the NRC staff does not endorse the concept of quantitative reliability goals as a sole means of meeting its regulations for reliability of digital computers used in safety systems.

Nevertheless, IEEE Std. 603-1991 further requires in Clause 5.15 that for those systems for which either quantitative or qualitative reliability goals have been established, appropriate analysis of the design shall be performed in order to confirm that such goals have been achieved. IEEE Std. 603-1991, Clause 6.7 requires that when sense and command features are in maintenance bypass, the safety system shall remain capable of accomplishing its safety function while continuing to meet the single-failure criterion.

Similarly, IEEE Std. 603-1991, Clause 7.5 requires that when one portion of a redundant safety system executes features is placed into a maintenance bypass condition, the remaining redundant portions should provide acceptable reliability. DI&C-ISG-06 states that the reliability and availability analysis should justify that the degree of redundancy, diversity, testability, and quality provided in the safety system design is adequate to achieve functional reliability commensurate with the safety functions to be performed with further consideration of the effect of possible failures and the design features provided to prevent or limit its effects.

Section 7.2 of the MELTAC LTR (Ref. 14) describes the methodology used to determine the reliability of a generic redundant parallel controller based on the MELTAC design. This

configuration was used to provide an example model of how reliability is determined using the processes described in the LTR. The same method will be used for determining the reliability of controllers using different architectures. A summary of MELTAC platform reliability document (Ref. 4) was also submitted to support this evaluation. This summary describes the reliability and failure modes and effects analyses performed to support MELTAC platform based systems. The scope of these analyses includes all MELTAC platform hardware components and MELTAC basic software including firmware used for MELTAC modules. MELTAC application software could not be included because the LTR is generic in nature and does not define any particular plant safety application specific design.

The NRC staff determined the summary of MELTAC platform reliability document contains platform reliability information that can be used to demonstrate conformance to plant specific reliability goals. Because plant and system specific reliability goals are not provided in the MELTAC LTR (Ref. 14) and instead must be established on a plant specific basis, the NRC staff was unable to make a safety determination for this criteria. Section 5.2.8 of this SE identifies additional actions which must be addressed during specific plant application development.

### 3.5.3 Software Lifecycle Process Design Outputs

SRP BTP 7-14, Section B.2.3, "Software Life Cycle Process Design Outputs," identifies software documents and products subject to review to evaluate whether the software life cycle development process produced acceptable design outputs. The following documents are included in the review guidance:

- Software requirements specification
- Hardware and software architecture description
- Software design specification
- Code listings
- Build documents
- Installation configuration tables
- Operations manuals
- Maintenance manuals
- Training manuals

Since the MELTAC LTR (Ref. 14) does not identify a plant specific application, many of the documents identified in SRP BTP 7-14 are not relevant for generic review of the platform. Specifically, operations, maintenance, and training manuals primarily relate to the installed system and support the licensee as end product user. Thus, review of these documents is most appropriate in the context of a specific project. Given that the design of a specific application is not within the scope of this review, some design outputs that are more particularly focused on application software as the object of the development process are not available for review.

MELTAC application software is designed, configured, compiled, and implemented using the MELTAC engineering tool. Build documents and configuration tables for application software, are not included within the scope of this SE. The MELTAC platform basic software was developed prior to the establishment of the MELCO Appendix B quality assurance Program so some design outputs are not aligned to BTP 7-14, and thus were evaluated from other documents that contained this information. Documents containing the SRS and SDS were submitted for review. Thus, the evaluation of the available design outputs that correspond to

MELTAC basic software was focused on the requirements and design documents submitted to support the MRP dedication effort.

#### 3.5.3.1 Software Requirements Specification

The acceptance criterion for software requirements specifications (SRS) is contained in SRP BTP 7-14, Section B.3.3.1, "Requirements Activities - Software Requirements Specification." This SE states that RG 1.172 endorses IEEE Std. 830, "IEEE Recommended Practice for Software Requirements Specifications." That standard describes an acceptable approach for preparing software requirements specifications for safety system software. Additional guidance is also provided in NUREG/CR-6101, Section 3.2.1 "Software Requirements Specification," and Section 4.2.1, "Software Requirements Specifications."

BTP 7-14 emphasizes clarity in the requirements and specifically cites thread audits as a method to check for completeness, consistency and correctness. The NRC staff review in this area focused on clarity and completeness of requirements and relied on the thread audits to demonstrate that requirements were traceable through applicable design basis documentation. The following specification documents were provided to the NRC to support evaluation of the MELTAC SRS documentation:

1. CPU Module (PCPJ-31) CPUCNT\_FPGA Specification (Ref. 25)
2. Input / Output function Program Specification (Ref. 25)

Additionally, Appendix B of the MELTAC LTR (Ref. 14) contains functional Symbol software specifications.

Based on the information provided, the MELTAC platform SRS documentation was found to conform to the characteristics necessary to facilitate the development of quality software and programmable logic for use in nuclear safety applications. The NRC staff determined that each of the MELTAC platform requirements evaluated was appropriately included in the associated SRS documentation. The NRC staff determined that the SRS documentation is adequately controlled by vendor processes. The NRC staff also identified a PSAI 5.2.2 to ensure vendor application software development processes are implemented in accordance with the SPMs.

#### 3.6 Equipment Qualification

The purpose of performing EQ testing for a safety system are (1) to demonstrate that the system will not experience failures due to abnormal service conditions of temperature, humidity, electrical power, radiation, electromagnetic interference, radio frequency interference, electrical fast transient, electrostatic discharge, power surge, or seismic vibration, and (2) to verify those tests meet the plant specific requirements.

Criteria for EQ of safety-related equipment are provided in 10 CFR Part 50, Appendix A, GDC 2, and GDC 4. Additionally, the regulation at 10 CFR 50.55a(h) incorporates by reference the requirements of IEEE Std. 603-1991 which addresses both system-level design issues and quality criteria for qualifying devices. RG 1.209 endorses and provides guidance for compliance with IEEE Std. 323-2003, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," for qualification of safety-related computer-based I&C systems installed in mild environment locations.

To comply with the requirements of GDC 4, 10 CFR 50.49, "Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants," and IEEE Std. 603-1991, an applicant must demonstrate through environmental qualification that I&C systems meet design-basis and performance requirements when the equipment is exposed to normal and adverse environments. Section 50.49 does not include requirements for seismic, and dynamic qualification, protection of electric equipment against other natural phenomena and external events, and equipment located in a mild environment.

Because MELTAC equipment was commercially dedicated for use in safety-related applications, the guidance of SRP Chapter 7, Appendix 7.0-A (page 7.0-A-17), Section 3.8, "Review of the Acceptance of Commercial-Grade Digital Equipment," was also considered by the NRC staff during this evaluation. This SRP section contains guidance for the review of commercial equipment and identifies Clause 5.4.2 of IEEE Std. 7-4.3.2, "Qualification of Existing Commercial Computers" as endorsed by RG 1.152 as an acceptable set of fundamental requirements for the commercial grade dedication EQ process.

Section 5.4.2 of SRP Chapter 7, Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std. 7-4.3.2," states that EPRI TR-106439, and EPRI TR-107330, provide specific guidance for the evaluation of commercial grade digital equipment and existing PLCs.

EPRI TR-107330 presents a specification in the form of a set of requirements to be applied to the generic qualification of PLCs for application and modification to safety-related I&C systems in nuclear power plants. It is intended to provide a qualification envelope corresponding to a mild environment that should meet regulatory acceptance criteria for a wide range of plant specific safety-related applications. The qualification envelope that is established by compliance with the guidance of EPRI TR-107330 consists of the maximum environmental and service conditions for which qualification was validated and the range of performance characteristics for the PLC platform that were demonstrated under exposure to stress conditions. Applicants using the MELTAC platform are obligated to verify that the environmental requirements of the application are bounded by the qualification envelope established. See Sections 5.2.4 and 5.2.5 of this SE for associated PSAIs.

MELCO used the guidance provided in EPRI TR-107330 to establish the testing approach to meet the requirements of IEEE Std. 323-2003 and other NRC guidance. The qualification program developed for the MELTAC addressed EQ for a mild, controlled environment, such as a main control room and auxiliary electrical equipment rooms. The basis for the testing program was conformance with the guidance contained in EPRI TR-107330, Section 4.3. The results of the qualification program establish the qualification envelope of the MELCO MELTAC platform. Table 3-3 lists EQ documentation prepared as part of the qualification program for the MELTAC platform.

**Table 3-3 MELTAC platform EQ Documentation**

<b>Document Title</b>	<b>MELCO Document Identification</b>	<b>Reference Number</b>
Summary of MELTAC platform Equipment Qualification	JEXU-1041-1023	31
Test Specification for EQ Testing	JEXU-1028-1222-P	25
Test Specification for Seismic Qualification Testing	JEXU-1028-1223-P	25
Test Specification for Electrostatic Discharge Qualification Testing	JEXU-1028-1224-P	25

Test Specification for EMC Qualification Testing	JEXU-1028-1225-P	25
Test Specification for Isolation Qualification Testing	JEXU-1028-1226-P	25
Test Specification for Environmental Qualification Testing	JEXU-1028-1236-P	25

### Equipment subjected to EQ Testing

The test specifications listed in Table 3-3 defined the MELTAC platform components and configurations that were subject to the test environments. Section 5.1.1.3 of the summary of MELTAC platform EQ specifically identifies test subject, equipment under test (EUT) layouts and EUT configurations used during the various EQ tests performed. The NRC staff reviewed these specification's and verified that all MELTAC components as identified in Table 3.2-1 of this SE were either subjected to the applicable test environments or were qualified by analysis based on similar designs to equipment that was subjected to the test environments. The process used for qualifying components by analysis and the results of analyses performed are described in Section 6.0 of the summary of MELTAC platform EQ. The NRC staff also verified the configurations used during testing to be representative of expected plant safety system installations.

**Data Collection** – The qualification test procedures that were used during MELTAC EQ testing are described in the summary of MELTAC platform EQ. Test Equipment used to verify proper system operation during testing was described in Section 5.1.1.4 of the summary of MELTAC platform EQ. The NRC staff reviewed this information and confirmed that all test equipment used to verify EUT performance was adequately identified and documented within the test reports.

#### 3.6.1 Atmospheric (Temperature and Humidity)

Table 4.1.1-2 of the MELTAC LTR (Ref. 14) specifies the temperature and humidity qualification requirements to be 32 to 122 degrees Fahrenheit (°F) (0 to 50 degrees Celsius (°C)) and 10 to 95 percent relative humidity (RH). The specification also states that cabinet temperature rise should be limited to 18 °F (10°C).

Environmental temperature and humidity qualification testing of the MELTAC platform test specimen was performed in accordance with EPRI TR-107330. The NRC staff evaluated the MELTAC EQ test results to determine compliance with the criteria of RG 1.209 and IEEE Std. 323-2003 for mild environment installations. The MELTAC test specimen performance requirements were verified during and following exposure to specified abnormal environmental conditions according to a time varying profile as outlined in IEEE Std. 323-2003. The NRC staff confirmed that EPRI TR-107330, Sections 4.3.6, "Environmental Requirements" and 6.3.3, "Environmental Testing Requirements" criteria were met.

The test configuration was designed to produce the worst case expected temperature rise across the module chassis and across the cabinet. The MELTAC equipment under test (EUT) was monitored before, during and after each test to confirm that no equipment failures or abnormal functions occurred. System self-diagnostics were also functioning and no system abnormalities were detected during tests. The self-diagnostics functions were confirmed to be operating at the completion of the test. Acceptance criteria for atmospheric tests were defined in the test procedures used and are summarized in Tables 5-20 through 5-24 of the summary of MELTAC platform EQ document.



Section 4.3.6.2 of EPRI TR-107330 requires that the generic PLC meet its performance requirements over abnormal environmental conditions of 40 °F to 120 °F (4.4 to 48.9 °C) and 10 percent to 95 percent RH (non-condensing). MELTAC temperature and humidity environmental test levels equaled or exceeded these conditions including applied margins and therefore this criteria was met.

Section 4.3.6.3 of EPRI TR-107330 requires that the test PLC operate for the environmental (temperature and humidity) withstand profile given in Figure 4-4 of the TR. Temperature test profiles used for MELTAC testing are provided in the summary of MELTAC platform EQ (Ref. 31). These profiles were found by the NRC staff to be compliant with the methodology outlined in Section 4.3.6.3 of EPRI TR-107330. A pre-qualification acceptance test was performed prior to subjecting the MELTAC EUT to the environmental conditions profile and a series of operability checks was performed at various environmental conditions during profile execution. The MELTAC EUT operated satisfactorily during these tests and all operability tests were completed satisfactorily. The NRC staff determined that MELTAC platform equipment is acceptable for use in EPRI TR 107330 specified temperature and humidity environments.

### 3.6.2 Electromagnetic Interference / Radio Frequency Interference

RG 1.180, endorses MIL-STD-461E, "Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment," and IEC 61000 series standards for the evaluation of the impact of EMI, RFI and power surges on safety-related I&C systems, and to characterize the electromagnetic (EM) emissions from the I&C systems.

EPRI TR-107330 includes EM compatibility (EMC) testing as part of the overall program to generically qualify a PLC for safety-related application in a nuclear power plant (NPP). Specific criteria for electromagnetic emissions, EMI susceptibility, electrostatic discharge withstand, power surge withstand, and isolation capability are given in Sections 4.3, "Hardware Requirements," and 4.6, "Electrical," of the guide while the qualification approach is specified in Section 6.3, "Qualification Tests and Analysis Requirements."

EPRI TR-102323, "Guideline for Electromagnetic Interference Testing in Power Plants," provides alternatives to performing site-specific EMI/RFI surveys to qualify digital safety I&C equipment for a plant's electromagnetic environment. In a SE issued in 1996, the NRC staff concluded that the recommendations and guidelines in EPRI TR-102323 provide an adequate method for qualifying digital I&C equipment for a NPP's EM environment without the need for plant specific EMI/RFI surveys if the plant specific EM environment is confirmed to be similar to that identified in EPRI TR-102323.

EMC and RFI qualification testing for the MELTAC platform is described in Section 5.3 of the MELTAC platform LTR (Ref. 14). EMC and ESD testing of the MELTAC EUT was performed from September 4 through September 7, 2015, at EMC Japan Corp. in Sagami-hara Japan. The MELTAC EUT was installed in the EMI/RFI chamber within a simple cabinet structure that did not enclose the PLC chassis. Wiring connections and grounding were in accordance with the manufacturer's recommendations.

The AC power to the EUT was supplied from two systems: main and standby. Each of these power sources was similarly configured. The AC input power line for the CE102, CS101, CS114 and International Electrotechnical Commission (IEC) 61000-4 tests were verified by testing both of these AC power cables individually.

The MELTAC platform EUT components were subjected to EMI/RFI testing to demonstrate compliance with the applicable EMI/RFI emissions and susceptibility requirements of NRC RG 1.180. The specific test configuration of the MELTAC equipment is described in Section 5.3.1, "Test Configuration" of the MELTAC platform LTR.

The following sections describe the EMI/RFI tests performed.

#### 3.6.2.1 EMI/RFI Interference

EMC testing was performed in accordance with its EMC qualification test specification (Ref. 25). The specific EMI/RFI Emissions tests performed are listed below:

- MIL-461E, CE101: Conducted Emissions, AC and DC Power Leads, 120 Hertz (Hz) to 10 kilo Hz (kHz)
- MIL-461E, CE102: Conducted Emissions, AC and DC Power Leads, 10 kHz to 2 mega Hz (MHz)
- MIL-461E, RE101: Radiated Emissions, Magnetic Field, 30 Hz to 100 kHz
- MIL-461E, RE102: Radiated Emissions, Electric Field, 2 MHz to 1 giga Hz (GHz), 1 GHz to 10 GHz

#### 3.6.2.2 EMI/RFI Susceptibility

EMI/RFI Susceptibility tests performed are as follows:

- MIL-461E, CS101: Conducted Susceptibility, 120 Hz to 150 kHz
- MIL-461E, CS114: Conducted Susceptibility, 10 kHz to 30 MHz
- MIL-461E, CS115: Conducted Susceptibility, Bulk Cable Injection, Impulse Excitation
- MIL-461E, CS116: Conducted Susceptibility, Damped Sinusoidal Transients 10 kHz to 100MHz
- MIL-461E: RS-103: Radiated Susceptibility, Electric Field, 30 MHz to 1 GHz, 1 GHz to 10 GHz

Note: RG 1.180, Section 4.3.1, "RS101 – Radiated Susceptibility, Magnetic Fields" allows exemption from RS101 testing if equipment is not to be used in environments with strong sources of magnetic fields. MELTAC platform equipment was not tested or qualified to RS101 criteria. Therefore, MELTAC equipment is not qualified for use in environments with strong magnetic fields. The NRC staff determined that as long as this installation environment restriction is in place, RS101 testing does not need to be performed. See PSAI 5.2.6.

#### 3.6.2.3 Surge Withstand Capability

MELCO performed Surge Withstand testing on the MELTAC platform in accordance with RG 1.180, Revision 1. Specifically, the Surge Withstand Testing included:

- IEC 61000-4-12, Surge Withstand Capability, Ring Wave
- IEC 61000-4-5, Surge Withstand Capability, Combination Wave
- IEC 61000-4-4, Surge Withstand Capability, Electrically Fast Transients / Bursts

#### 3.6.2.4 Electrostatic Discharge Withstand Testing

EPRI TR-107330, Section 4.3.8, requires that the test specimen under qualification be tested for immunity to the ESD test levels specified in EPRI TR-102323, Revision 1.

Electro Static Discharge (ESD) testing was performed in accordance with its ESD qualification test specification (Ref. 25).

#### 3.6.2.5 Electromagnetic Compatibility Test Acceptance Criteria Evaluation

The EMC test acceptance criteria for the MELTAC EUT included monitoring of equipment performance before, during and after each test. Detailed test acceptance criteria are described in the summary of MELTAC platform EQ (Ref. 31). The NRC staff reviewed these acceptance criteria and confirmed test results as follows:

- The MELTAC EUT met allowable equipment emission limits as specified in RG 1.180, Revision 1, for conducted and radiated emissions.
- The MELTAC EUT operated as intended during and after application of the EMI/RFI test levels specified in RG 1.180 for conducted and radiated susceptibility.
- Evaluation of normal MELTAC EUT operating performance data (inputs, outputs, and diagnostic indicators) demonstrated operation as intended, including the following specific operational performance criteria:
  - The main processors and coprocessors continued to function
  - The transfer of I/O data was monitored during tests and no interruptions were noted
  - The emissions did not cause the discrete I/O states to change
  - Analog I/O levels did not vary by more than 3 percent and calibration accuracy was checked following tests

The NRC staff reviewed the "EMC Test Report," MELCO Document No. JEXU-1041-1046 and determined that the tested MELTAC system met the EMI/RFI test acceptance criteria discussed above and is qualified for operation up to the tested limits described above.

Before using the MELTAC platform equipment in safety-related systems in nuclear power plant, licensees must determine that plant specific EMI requirements do not exceed the capabilities of the MELTAC system as approved in this SE. This determination and the suitability of the MELTAC system for a particular plant and application are the responsibility of the licensee. This is PSAI 5.2.4.

#### 3.6.3 Seismic Qualification

RG 1.100, Revision 3 describes methods that the NRC staff considers acceptable for use in seismic qualification of electrical and active mechanical equipment. The RG provides an endorsement of IEEE Std. 344-2004 with exceptions and clarifications. Clause 4, of IEEE Std. 344-2004, states:

The seismic qualification of equipment should demonstrate an equipment's ability to perform its safety function during and/or after the time it is subjected to the forces resulting from one Safe Shutdown Earthquake (SSE). In addition, the

equipment must withstand the effects of a number of Operating Basis Earthquakes (OBEs) prior to the application of a SSE.

An OBE is a seismic event during which all equipment necessary for continued plant operation without undue risk to the health and safety of the public is required to remain functional. An SSE is the maximum considered earthquake in the design of a nuclear power plant and the earthquake for which structures, systems and components (SSCs) important to safety are designed to remain functional.

RG 1.61 establishes evaluation guidance for applicants and licensees regarding the acceptable damping values that the NRC staff should use in the seismic response analysis of nuclear power plant SSCs.

Section 4.3.9 of EPRI TR-107330 provides additional guidance for establishing seismic withstand requirements for digital protection systems.

Table 4.1.1-2, "Environmental Specifications," of the MELTAC platform LTR specifies the seismic qualification requirements to be 2.5 G (Horizontal) and 1 G (Vertical) for the MELTAC Cabinet at the floor mounting and at 10 G (Horizontal) and 2 G (Vertical) for all MELTAC modules at chassis mounting.

To demonstrate that the MELTAC platform meets the requirements for electrical and active mechanical equipment and functional qualification of active mechanical equipment for nuclear power plants as defined in RG 1.100, MELCO subjected representative MELTAC equipment to accelerated aging followed by seismic stimulation testing to represent SSE conditions. The accelerated aging method used was determined to be equivalent or more severe than aging that would occur during five OBE. The NRC staff determined that the aging methods used for the MELTAC equipment were compliant with the seismic aging guidance provided in Section 8.1.5.2 of IEEE Std. 344-2004 and is therefore acceptable.

In addition to demonstrating functional operation and physical integrity under the specified conditions, a resonance search procedure was conducted to confirm no abnormalities in cabinet structure and no resonance points in the frequency range of 5 Hz to 20Hz.

Seismic Testing was performed in accordance with the requirements of RG 1.100 Revision 3, and IEEE Std. 344-2004. Seismic tests were performed at the Mitsubishi electric corporation energy systems center in November of 2015 and from February to May of 2017. The test equipment used during these tests was capable of producing seismic frequencies in the range of 1 to 2000 Hz. A system level cabinet test specimen intended to represent a fully loaded safety protection system was used during the qualification test. The NRC staff reviewed the equipment test subject list as well as the equipment under test layout configurations and confirmed that reasonable representative configurations were employed.

The NRC staff also confirmed that all MELTAC platform components identified in Table 3.2-1 of this SE are addressed by the representative qualification tests performed. Some MELTAC components were represented by other similar modules that were tested and were thus qualified by analysis. Section 6 of the summary of MELTAC platform EQ identifies modules that were not tested and includes analyses for each such module which provides justification for qualified use in safety systems. The NRC staff found this to be acceptable.

A summary of seismic test results was provided in Section 5.2.2, "Results of Seismic Qualification Testing" of the summary of MELTAC qualification testing document (Ref. 31). Resonance tests confirmed no abnormalities in cabinet or component structures and that no resonance points existed within the subject frequency ranges.

Sine beat wave tests were performed at MELTAC cabinet and module levels at several frequencies with EUT energized to achieve accelerated aging prior to subjecting the test specimen to SSE conditions. Cabinet and component physical integrity and correct functional operation of EUT were verified before, during, and after excitation.

Section 5.2.1 of the MELCO platform LTR states that "input acceleration levels used for Cabinet Seismic Resistance Test is set high enough to cover the floor response spectrum range of power plants in the U.S." Due to the generic applicability of this SE, the NRC staff was not able to confirm the accuracy of this statement for all U.S. plants; however, an applicant referencing the MELTAC LTR will need to confirm that MELTAC platform equipment seismic qualification levels are within plant specific design basis seismic conditions for SSE and OBE earthquakes. This is a PSAI.

Acceleration levels specified for generic plant SSE in EPRI TR-107330 are 14 G at frequencies above 3 Hz and 10 G for OBE events. Because the MELTAC platform equipment was not tested to acceleration levels greater than 10 G in any direction, it does not meet the criteria for generic seismic qualification at plant sites having greater than 10 G postulated plant specific SSE acceleration levels.

The NRC staff reviewed the seismic test specifications and confirmed the acceleration levels to be consistent with MELTAC cabinet and component specifications. The NRC staff reviewed the test frequency spectra and confirmed that specified qualification motion acceleration levels were achieved for the qualification frequency range.

The results of the seismic test show that:

- Seismic testing of the MELTAC EUT was performed in accordance with the criterion of IEEE Std. 344-2004.
- The MELTAC EUT met all applicable performance requirements during and after application of the seismic test vibration levels.
- Results of the operability test performed after seismic testing show that exposure to the seismic test conditions had no adverse effect on the MELTAC EUT performance.
- The seismic test results demonstrate that the MELTAC platform is suitable for qualification as Category I seismic equipment as defined in RG 1.29, Rev. 5, "Seismic Design Classification for Nuclear Power Plants."
- The seismic test results demonstrate that the representative equipment mounting configurations used during testing are adequate to support seismic qualification of MELTAC based safety systems.

The NRC staff reviewed these results and confirmed that the seismic acceleration levels to which the representative platform components were tested met or exceeded the seismic resistance specifications for the MELTAC platform as provided in Section 4.1.1.4 of the MELTAC LTR (Ref. 14).



Based on review of the MELTAC seismic test results and supporting analysis, the NRC staff determined that the MELTAC platform does not fully satisfy the guidance criteria of EPRI TR-107330 because seismic withstand was not demonstrated for the specified maximum acceleration of 14G for a generic SSE. However, the NRC staff finds that seismic qualification of the MELTAC platform has been acceptably demonstrated for OBE and SSE events up to accelerations of 10 G. The use of MELTAC system equipment for the performance of safety system functions in a nuclear power plant, requires licensees to determine that MELTAC system seismic withstand capabilities do not exceed plant specific seismic requirements. A plant using the MELTAC platform is therefore required to establish plant specific seismic criteria for the system to be installed. Licensees referencing the LTR should ensure their plant specific in-equipment response spectra (IERS) are enveloped by the MELTAC platform test response spectrum qualification envelope (see PSAI 5.2.5).

### 3.7 MELTAC platform Integrity Characteristics

SRP Chapter 7, Appendix 7.1-C, Section 5.5, "System Integrity," states that a special concern for digital computer-based systems is confirmation that the real time performance of the system is adequate to ensure completion of protective actions within the critical time periods identified within Clause 4.10 of IEEE Std. 603-1991. SRP BTP 7-21, "Guidance on Digital Computer Real-Time Performance," provides supplemental guidance to evaluate the real-time performance of digital systems and architectures, and discusses the identification of bounding real-time performance specifications and the verification of these specifications to demonstrate real-time performance. Below is the NRC staff evaluation of the system performance.

#### 3.7.1 MELTAC Platform Response Time

GDC 20, 21, 23, and 25 of Appendix A to 10 CFR Part 50 constitute general requirements for timely operation of the protection features. To support these requirements, SRP BTP 7-21 provides the following guidance:

- The feasibility of design timing may be demonstrated by allocating a timing budget to components of the system architecture to ensure that an entire system meets its timing requirements.
- Timing requirements should be satisfied by design commitments.

Two regulations provide the basis for this guidance. The first is 10 CFR 50.55a(h) and its incorporation of IEEE Std. 603-1991 by reference. The second is 10 CFR 50.36(c)(1)(ii)(A) which provides basis for timing requirement commitments by requiring the inclusion of the limiting safety systems settings for nuclear reactors in the plant technical specifications, "so chosen that automatic protective action will correct the abnormal situation before a safety limit is exceeded."

Each licensee using the MELTAC platform should provide plant specific response time performance requirements for the system. The actual response time of an MELTAC platform-based system will be determined by its overall configuration; therefore, each licensee must determine that the MELTAC platform response time characteristics are suitable for its plant specific application (see PSAI 5.2.3). The following information addresses the use of MELTAC platform response time characteristics in support of future plant specific suitability determinations.

The MELTAC LTR (Ref. 14), Section 4.4 describes platform response time performance characteristics. Response times for a MELTAC platform based safety system are determined by combining the response times of individual control processes. When a MELTAC application is developed, a time response calculation is performed to determine the total response time for the specific application. The MELTAC LTR describes the method to be used for performing a time response calculation and provides examples of response time calculations.

Actual system response times will vary depending on the number and types of control processes being used, the CPU configuration being implemented and the number of data transfers required to complete a safety action. The method described in the MELTAC LTR (Ref. 14) provides a means of estimating the application process minimum and maximum response times once the application details become available and the application design is developed. This method includes allocation of a timing budget to components of the MELTAC system architecture.

MELTAC platform-based system response time components are: acquire and condition input signal that represents the start of a response time performance requirement, transmit the signal to the MELTAC CPU module, perform logic processing, generate an output signal, and transmit the output to the output module. These MELTAC platform response time components do not include (1) the earlier plant process delays through the sensor input to the platform and (2) the latter delays through a final actuating device to affect the plant process. Therefore, the licensee's plant specific safety function response time design bases should address these response time components separately from the response time performance requirements specified for the licensee's MELTAC platform-based system (see Section 5.2.3). Testing must also be performed to confirm MELTAC response time performance to assure that plant specific time response requirements are met. Section 5.2.3 provides a PSAI for completion of response time testing prior to operation of the MELTAC based system.

### 3.7.2 Determinism

The review guidance of SRP Chapter 7, Appendix 7.1-C, Section 6.1, "Automatic control," identifies considerations that address digital computer-based systems for the evaluation of the automatic control capabilities of safety system command features. This review guidance advises that the evaluation should confirm that the system's real time performance is deterministic and known. SRP BTP 7-21 discusses design practices for computer-based systems that should be avoided, and these practices include non-deterministic data communications, non-deterministic computations, interrupts, multitasking, dynamic scheduling, and event-driven design. SRP BTP 7-21 further states that methods for controlling the associated risk to acceptable real time performance should be described when such practices are employed.

EPRI TR-107330 provides specifications and guidance intended to achieve an execution cycle with deterministic behavior that ensures an application and its constituent tasks will be completed within specified time limits. In particular, EPRI TR-107330, Section 4.4.1.3, "Program Flow Requirements," specifies that, where scanning of the inputs and application program execution are performed in parallel, methods should assure that the input scan and application program execution are completed each cycle.

MELTAC control Processes are performed by the CPU module in accordance with a cyclic and deterministic Fundamental Process cycle. Section 4.4.1 of the MELTAC LTR describes each of the control processes included in this Fundamental Cycle and provides a method for calculating

the processing time of this cycle. This method provides a means of determining the minimum and maximum cycle time based upon the MELTAC hardware configuration and software application details. Once, known, this theoretical minimum overall response time provides assurance that each consecutive process is completed prior to initiation of the next cyclic process. The theoretical maximum overall response time provides assurance that each consecutive process is completed just after initiation of the next cyclic process and would therefore require an additional cycle to ensure process task completion.

The NRC staff determined that design features, operation of the MELTAC system, and MELCO's commitments to perform timing analysis and tests provide sufficient confidence that MELTAC based safety systems will operate deterministically to meet the recommendations of BTP 7-21 and is therefore acceptable.

### 3.7.3 Self-diagnostics / Test and Calibration Capabilities

The regulation at 10 CFR Part 50, Appendix A, GDC 21 requires in part that the protection system be designed for in-service testability commensurate with the safety functions to be performed. It also requires a design that permits periodic testing of its functioning when the reactor is in operation, including the capability to test channels independently to determine failures and losses of redundancy that may have occurred.

MELTAC self-diagnostics test functions (described in Section 4.2.3 of the MELTAC LTR) can be used to support compliance to GDC 21. However, determination of full compliance with this criteria is dependent on the specific safety system design as well as the plant specific safety functions performed by the system. Therefore, determination of GDC 21 compliance remains an application specific evaluation item. See PSAIs 5.2.7 and 5.2.14 for additional information on self-diagnostics criterion. IEEE Std. 603-1991, Clause 5.7 states that the safety system shall have the capability for test and calibration while retaining the capability to accomplish its safety function, and that this capability be provided during power operation, and shall duplicate, as closely as practicable, performance of the safety function.

IEEE Std. 603-1991 Clause 5.7 allows exceptions to testing and calibration during power operation. MELTAC self-diagnostics test functions can be used to support justification for such exceptions or to support compliance with system test and calibration requirements. However, determination of full compliance with this criteria is dependent on the specific safety system design as well as the plant specific safety functions performed by the system. Therefore, determination of IEEE 603-1991, Clause 5.7 compliance remains an application specific evaluation item. See PSAI 5.2.13.

SRP, Chapter 7, Appendix 7.1-C, Section 5.7, "Capability for Test and Calibration," includes criteria for test provisions of digital computer based systems. It states that licensees should address the increased potential for system failures such as data errors and computer lockup. The NRC staff reviewed the self-diagnostics features of the MELTAC platform provided in Section 4.2.3 of the MELTAC LTR (Ref. 14) and found that MELTAC self-diagnostics functions have the capability to sufficiently address the potential for MELTAC system failures by identifying expected failures and providing the capability to annunciate such failures to the operator.

SRP BTP 7-17, "Guidance on Self-Test and Surveillance Test Provisions," states that automatic diagnostics and self-test features should preserve channel independence, maintain system integrity, and meet the single-failure criterion during testing. Additionally, the benefits of

diagnostics and self-test features should not be compromised by additional complexity that may result from the implementation of diagnostics and self-test features. The scope and extent of interfaces between safety software and diagnostic software such as self-test routines should be designed to minimize the complexity of the integrated software.

The NRC staff found that MELTAC system self-diagnostics do not adversely affect channel independence or system integrity. The MELTAC self-diagnostics can be used to support the single-failure criterion during testing however, compliance with single failure criteria must be addressed on an application specific basis. See PSAI 5.2.13.

EPRI TR-107330 provides guidance and requirements applicable to PLC-based system's diagnostics and test capability so that the combination of self-diagnostics and surveillance testing will detect failures that could prevent a PLC from performing its intended safety function. The range of conditions for which diagnostics or test capabilities are to be provided includes processor stall, executive program error, application program error, variable memory error, module communications error, module loss of configuration, excess scan time detection, application not executing, and field device (e.g., sensor, actuator) degradation or fault. The means of detection include WDTs, checksum for firmware and program integrity, read/write memory tests, communications monitoring, configuration validation, heartbeat, and self-diagnostics or surveillance test support features. EPRI TR-107330 identifies diagnostics that are executed upon power-up and diagnostics that run continuously thereafter.

Sections 4.1.5, & 4.2.3 of the MELTAC LTR (Ref. 14) describe the self-diagnostics and maintenance features provided in the MELTAC platform. The MELTAC platform performs tests and self-test diagnostics of the system (including tests of I/O boards and communication interfaces). MELCO considers that a combination of self-tests, periodic testing, and surveillance are necessary to successfully detect failures and support effective maintenance of the system. Specifically, periodic surveillance tests are performed to detect failures or problems that are not detectable by self-diagnostic functions. Maintenance activities including periodic surveillance testing will be defined based on the system and plant specific application requirements. In addition, how failures are managed will be defined in the failure management for a plant specific application. See Section 5.2.7 of this SE for additional information on specifying failure states of the safety system.

#### 3.7.4 Setpoint Determination Methodology

A MELTAC platform setpoint methodology (Ref. 5) was provided by MELCO to support the NRC staffs evaluation of IEEE 603-1991, Clause 6.8, "Setpoints" criterion. Though determination of safety system setpoints is a plant specific activity that cannot be evaluated at the generic platform level, the methods used for performing this activity are outlined in the document provided. See PSAI 5.2.9.

The NRC staff reviewed the MELTAC setpoint methodology using the criteria of IEEE Std. 603-1991, Clause 6.8, BTP 7-12, Rev. 6, and RG 1.105. The methodology considers factors that have the potential to affect the instrument uncertainties for sense and command features of a MELTAC based system. The MELTAC contribution to instrument uncertainties is analyzed and determined to be less than 0.25% of full scale calibration. Other factors considered in the method include power supply voltage and frequency variance, operating temperature and humidity, pressure, vibration / seismic acceleration, radiation exposure, instrument drift and the effects of design basis events. The NRC staff determined the methods outlined in the MELTAC setpoint methodology to be compliant with the criteria of RG 1.105.

These methods therefore provide an acceptable process for determining setpoints to be used in a MELTAC based safety system.

### 3.8 Diversity and Defense-in-Depth.

The regulation at 10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991 and the correction sheet dated January 30, 1995. The regulation at 10 CFR 50.62, "Requirements for reduction of risk from anticipated transients without scram (ATWS) events for light-water-cooled nuclear power plants," requires in part various diverse methods of responding to an ATWS; 10 CFR Part 50, Appendix A, GDC 21 requires in part that "no single failure results in the loss of the protection system"; GDC 22 requires in part "that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions ... not result in loss of the protection function ... Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function"; GDC 24 requires in part that "interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired"; and GDC 29 requires in part defense against anticipated operational transients "to assure an extremely high probability of accomplishing ... safety functions."

The NRC staff requirements memorandum on SECY 93-087, "Policy, Technical, And Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," dated July 21, 1993, describes the NRC position on diversity and defense-in-depth (D3) requirements to compensate for potential common-cause programming failure. Guidance on the evaluation of D3 is provided in SRP BTP 7-19. The four-point position within BTP 7-19 was developed in recognition that programming design errors are credible common mode error sources for nuclear power plants that incorporate digital protection systems. In addition, NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," summarizes several D3 analyses and presents a method for performing such analyses.

D3 is a strategy that is applied to the overall I&C system architecture in the context of a specific plant design. D3 should be addressed in the context of plant safety-related and non-safety-related I&C systems. Because the LTR does not propose a specific I&C system for a specific plant application, this SE cannot determine the adequacy of the MELTAC platform against the guidance in BTP 7-19.

Thus, the performance of a plant specific D3 analysis is a plant specific action for safety-related applications of the MELTAC platform (Ref. Section 5.2.11 of this SE). BTP 7-19's D3 evaluation should demonstrate that plant vulnerabilities to common cause failures (CCFs) have been adequately addressed in the context of an overall suite of I&C systems.

### 3.9 Communications

#### 3.9.1 DI&C-ISG-04 Compliance

The NRC Task Working Group 4, "Highly Integrated Control Rooms-communications Issues," developed interim NRC staff guidance on the review of communications issues applicable to digital safety systems. DI&C-ISG-04 contains NRC staff positions on three areas of interest: (1) interdivisional communications, (2) command prioritization, and (3) multidivisional control and Display Stations. Section 4.3 of the MELTAC LTR (Ref. 14) describes the communications System used in the MELTAC platform. Section 3.2.2 of this SE describes the MELTAC System



Communication processes. A "MELTAC platform ISG-04 conformance analysis" which contains MELCO's assessment of MELTAC platform conformance to the provisions of DI&C-ISG-04, Revision 1 was provided as a supplemental document to support the NRC staffs SE (Ref. 2).

Evaluation of a safety system against this guidance is a plant specific activity that requires an assessment of a completed system design. Because the MELTAC LTR (Ref. 14) does not address specific applications or establish a definitive safety system design, the evaluation against this guidance is limited to consideration of the means provided within the platform to address issues related to interactions among safety divisions and between safety-related equipment and equipment that is not safety-related. A complete safety MELTAC system design will require further evaluation against this guidance. The following subsections provide an evaluation of each MELTAC platform communication method against applicable DI&C-ISG-04 criteria. A PSAI is included in this SE to address full compliance to each DI&C-ISG-04 clause. (Ref. PSAI 5.2.12).

#### 3.9.1.1 DI&C-ISG-04, Staff Position 1 - Interdivisional Communications

Staff Position 1 of DI&C-ISG-04 provides guidance on the review of communications, which includes transmission of data and information among components in different electrical safety divisions and communications between a safety division and equipment that is not safety-related. This ISG guidance does not apply to communications within a single safety division. This NRC staff position states that bidirectional communications among safety divisions and between safety-related and non-safety-related equipment may be acceptable provided certain restrictions are enforced to ensure that there will be no adverse impact on safety systems. It also states that systems which include communications among safety divisions and/or bidirectional communications between a safety division and non-safety-related equipment should adhere to the guidance provided in 20 points described in the NRC staff position for Interdivisional communications in DI&C-ISG-04 Rev. 1.

The methods by which the MELTAC platform either meets these points or provides an acceptable alternative method of complying with NRC regulations are discussed below. In several instances, full compliance with these points cannot be determined without a complete application system design. For those points, this evaluation will highlight features of the MELTAC platform that would support compliance with the point and provide guidance for addressing specific items during subsequent application development.

#### **Staff Position 1, Point 1**

This position states the following:

...a safety channel should not be dependent upon any information or resource originating or residing outside its own safety division to accomplish its safety function. This is a fundamental consequence of the independence requirements of IEEE Std. 603-1991. It is recognized that division voting logic must receive inputs from multiple safety divisions.

The MELTAC LTR (Ref. 14) describes a generic MELTAC platform which does not define a specific communication architecture for a safety division to be applied to all safety applications. Instead Section 4.3.3.5 of the LTR describes a "representative" reactor protection processor (RPP) safety channel using the data link communications between safety divisions. This example is presented as a typical four channel implementation of an RPP system, however,

other configurations may be used. Without a specific system with a specific application, the NRC staff is unable reach a safety conclusion on this point.

The MELTAC platform described in the LTR includes capabilities to conform to the guidance provided in staff position 1, point 1. For example, the MELTAC safety system logic processors operate asynchronously from the communication processors and all data is transferred through a two port memory module. The CPU processor modules also have diagnostic capabilities to monitor the status of each data link communication interface so that the ability to perform safety functions without reliance on external data can be retained.

The NRC staff recognizes that the MELTAC platform provides allowances for implementation of system features that could conform to the guidance provided by staff position 1, point 1. However, evaluation of this point will require plant specific analysis to verify compliance with this staff position.

### **Staff Position 1, Point 2**

This position states the following:

... the safety function of each safety channel should be protected from adverse influence from outside the division of which that channel is a member. Information and signals originating outside the division must not be able to inhibit or delay the safety function. This protection must be implemented within the affected division (rather than in the sources outside the division), and must not itself be affected by any condition or information from outside the affected division. This protection must be sustained despite any operation, malfunction, design error, communication error, or software error or corruption existing or originating outside the division.

To address this criterion, the NRC staff evaluated both the MELTAC data link which provides communications between safety divisions and the MELTAC maintenance network which provides communication links to the non-safety-related engineering tool program in the maintenance workstations.

#### Data Link:

The MELTAC data link interface includes communication independence features described in Section 4.3.3.5 of the LTR. These features include asynchronous processing of communication data through the data link by dedicated communications processors (controllers) and the use of two port memory sharing.

MELTAC data link communications features are listed below:

- Use of the two port memory sharing support information transfer
- Data Validation using cyclic redundancy checks (CRC) on received data link packets.
- Identification of erroneous data
- Ability to detect absence of data updates (i.e., identify "stale" data)
- Continuous monitoring of data link communications status
- Detection of data link communications failure

- Physical separation and electrical isolation are provided by use of fiber optic cabling between nodes of the data link.

The NRC staff determined that MELTAC safety processors can be protected from adverse influences caused by information or signals originating at the opposite side of the data link provided that safety applications are developed to perform required safety functions without reliance on data received through the data link interfaces. Establishment of functional independence however, must be addressed at the application level.

#### Maintenance Network:

The MELTAC maintenance network interface includes communication independence features described in Section 4.3.4.2 of the LTR. These features include asynchronous processing of communication data through the maintenance network by dedicated communications processors (controllers) and the use of two port memory sharing. Because the maintenance network is physically disconnected from the MELTAC safety processors (controllers) and from the S-VDU processor during normal operation, there is no potential for maintenance network activity to inhibit or delay the safety functions being performed by the MELTAC system safety processors.

The maintenance network can however be periodically connected to the safety processors for diagnostics and surveillance testing purposes. During these controlled activities, it is necessary to protect the integrity of the basic and application software. This is accomplished by storage of software in Flash ROM memory which cannot be changed from the engineering Tool unless the CPU module is relocated to a dedicated reprogramming chassis. While it is possible to make temporary changes to data and programs stored in the controller data tables during these evolutions, such changes would result in deviations from the F-ROM data and such deviations can be used to initiate system alarms to identify conditions that could affect operability of the controller.

The NRC staff determined that MELTAC safety processors can be protected from adverse influences caused by information or signals originating from the engineering network. As stated in staff position 1, point 1, the MELTAC LTR (Ref. 14) described a generic MELTAC platform and a "representative" safety channel using the data link for communication between safety divisions and the engineering network for communications between the Safety System components and Non-Safety maintenance workstations. The NRC staff recognizes that the MELTAC platform provides allowances for implementation of system features that could conform to the guidance provided by staff position 1, point 2. However, evaluation of this point will require plant specific analysis to verify compliance with this staff position.

#### **Staff Position 1, Point 3**

This position states the following:

...a safety channel should not receive any communication from outside its own safety division unless that communication supports or enhances the performance of the safety function. Receipt of information that does not support or enhance the safety function would involve the performance of functions that are not directly related to the safety function. Safety systems should be as simple as possible. Functions not necessary for safety, even if they enhance reliability, should be executed outside the safety system. A safety system designed to

perform functions not directly related to the safety function would be more complex than a system that performs the same safety function, but is not designed to perform other functions. The more complex system would increase the likelihood of failures and software errors. Such a complex design, therefore, should be avoided within the safety system.

Section 4.3.3.5 of the LTR describes a "representative" reactor protection processor (RPP) safety channel using the data link communications between safety divisions. The NRC staff recognizes that the MELTAC platform provides capabilities for implementation of system features that could affect compliance with this position. These cases would require plant specific analysis to verify compliance with this staff position. Thus, without a specific system design, the NRC staff cannot reach a safety determination on compliance with this point. This point will need to be reviewed as a PSAI. See PSAI 5.2.12.

#### **Staff Position 1, Point 4**

This position states:

...the communication process itself should be carried out by a communications processor separate from the processor that executes the safety function, so that communications errors and malfunctions will not interfere with the execution of the safety function. The communication and function processors should operate asynchronously, sharing information only by means of dual-ported memory or some other shared memory resource that is dedicated exclusively to this exchange of information. The function processor, the communications processor, and the shared memory, along with all supporting circuits and software, are all considered to be safety-related, and must be designed, qualified, fabricated, etc., in accordance with 10 CFR Part 50, Appendices A and B.

Access to the shared memory should be controlled in such a manner that the function processor has priority access to the shared memory to complete the safety function in a deterministic manner. 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 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.

Both the MELTAC data link and maintenance network communication interfaces use independent asynchronous communications processors to manage communication related tasks. These communications processors are separate from the safety function processors which execute basic and application software instructions. The safety processors do not perform any communication related functions other than to store data into memory locations that are accessible to the communications processor and the safety function processors operate asynchronously from the communications processors.

The MELTAC safety function processors share information with the communications processors by means of two port shared access memory. The two port memory is dedicated exclusively to this exchange of information for the purpose of supporting communications.

All components of the data link and maintenance network communication interfaces are classified as safety-related. The MELTAC safety function processors, communications processors, and supporting circuitry, were not originally developed under a 10CFR Part 50 Appendix B program. However, all of these components were subject to commercial grade dedication under the MELCO QA program. An evaluation of MELCO's commercial grade dedication effort is contained in Section 3.4 of this SE. These components are therefore qualified in accordance with 10 CFR Part 50, Appendix B and meet the design and qualification requirements of 10 CFR Part 50, Appendix A.

A detailed description of how the MELTAC two port memory sharing functions are performed, including a discussion of how access to the two port memory data is controlled, was provided in the MELTAC platform DI&C-ISG-04 conformance analysis (Ref. 2). The NRC staff reviewed this information and determined that the manner in which shared memory is controlled does not adversely affect the ability of the safety function processors to complete required safety functions in a deterministic manner. The two port memory can support unrestricted simultaneous access by both the communications and safety function processors. If a MELTAC safety function processor is unable to gain access to shared memory, it will continue to function and perform required safety functions design specifications within established safety analysis timing requirements. These specifications and timing requirements are application specific. The NRC staff has reviewed the design and functionality of the communications process, has examined the hardware and software used to implement this process, and concludes that the MELTAC platform provides capability for implementation of system features to conform to the guidance provided by staff position 1, point 4.

#### **Staff Position 1, Point 5**

This position states the following:

...the cycle time for the safety function processor should be determined in consideration of the longest possible completion time for each access to the shared memory. This longest-possible completion time should include the response time of the memory itself and of the circuits associated with it, and should also include the longest possible delay in access to the memory by the function processor, assuming worst-case conditions for the transfer of access from the communications processor to the function processor. Failure of the system to meet the limiting cycle time should be detected and alarmed.

The MELTAC maintenance network and data link communication interfaces use dedicated communications processors to manage communications tasks. These communications processors operate independently and asynchronously from the safety function processors that perform required safety functions as instructed by the MELTAC basic and application software. The communication and safety function processors share information by means of two port memory that is dedicated exclusively to this exchange of information.



As described previously, the manner in which shared memory is controlled within the data link and maintenance network interfaces does not adversely affect the ability of the safety function processors to complete required safety functions in a deterministic manner.

A response time calculation methodology is described in Section 4.4.1 of the MELTAC LTR (Ref. 14). This methodology is used to determine response time performance of a MELTAC system. This methodology includes consideration of memory response time, and of the circuits associated with the communication interfaces. The methodology also includes consideration for the memory access times. MELTAC self-diagnostics are used to identify conditions that could compromise system response time performance. Diagnostic functions can be configured to provide an alarm upon detection of failures that could adversely impact system time response.

Staff position 1, point 5 must be evaluated as a PSAI because the system cycle time is dependent on application software. When implementing a MELTAC safety system the licensee must review MELCO's timing analyses and validation tests for the application specific MELTAC system to verify that plant specific requirements for system response and response time requirements of the plant accident analysis are met. See PSAI 5.2.3 for additional information on this requirement.

#### **Staff Position 1, Point 6**

This position states the following:

...the safety function processor should perform no communication handshaking and should not accept interrupts from outside its own safety division.

MELTAC safety function processors and S-VDU processors do not perform communication handshaking. Instead communication control functions are performed by separate dedicated purpose communications processors. Additionally, MELTAC safety function processors, S-VDU processors and communications processors do not accept interrupts from outside of the assigned safety division.

Section 3.2.2 of this SE describes the interactions that take place between the MELTAC safety function processors and the dedicated communications processors. While the MELTAC safety function processor executes the MELTAC basic and application software, the communications processors control all communications relating to the MELTAC safety system.

The NRC staff review determined that no handshaking is performed by the MELTAC safety function processors. The MELTAC safety function processors communicate externally using only two port memory, and this process does not use handshaking or interrupts. The NRC staff, therefore, determined that the MELTAC platform complies with staff position 1, point 6.

#### **Staff Position 1, Point 7**

This position states the following:

...only predefined data sets should be used by the receiving system. Unrecognized messages and data should be identified and dispositioned by the receiving system in accordance with the pre-specified design requirements. Data from unrecognized messages must not be used within the safety logic executed by the safety function processor. Message format and protocol should be

pre-determined. Every message should have the same message field structure and sequence, including message identification, status information, data bits, etc. in the same locations in every message. Every datum should be included in every transmit cycle, whether it has changed since the previous transmission or not, to ensure deterministic system behavior.

MELCO provided an analysis of message field failures in the data link (Section 3.5 of Reference 2) to support its position of compliance with this staff position. The NRC staff limited its evaluation of compliance with this point to the data link communications interface because the maintenance network will not normally be connected to MELTAC safety function processors during plant operation. The NRC staff reviewed the analysis provided and determined that data sets used for the MELTAC data link are predefined.

The MELTAC platform safety function processors and communications processors are capable of identifying and dispositioning unrecognized or invalid messages transferred over the data link. If unrecognized messages or data are received over the data link interface, they are discarded and not used by the processors to support safety functions.

The data link Message format and protocol are pre-determined. All data link messages have the same message structure and are transferred in the same sequence. All data transferred through the data link is included in the broadcast transmission of every transmit cycle, whether it has changed since the previous transmission or not.

Based upon the above discussion on the MELTAC's use of predefined data sets, with a pre-determined format via the respective communications processors, the NRC staff concludes that the MELTAC platform meets staff position 1, point 7. Note that how corrupted or stale data is managed after being identified will be defined for a plant specific application. See PSAI 5.2.12.

#### **Staff Position 1, Point 8**

This position states the following:

...data exchanged between redundant safety divisions or between safety and non-safety divisions should be processed in a manner that does not adversely affect the safety function of the sending divisions, the receiving divisions, or any other independent divisions.

The NRC staff reviewed communications protocols used for data exchanged over the MELTAC data link interfaces and determined that dedicated communications processors with a defined protocol are designed to manage this data in a manner which cannot adversely impact safety functions performed by the MELTAC safety processors in either the source division or safety processors in the destination division(s). All divisions connected via data link interfaces are protected with the same communications processing design, which uses two port memory, data validity checks, and asynchronous communications processing.

Communication of data through the maintenance network to a non-safety-related workstation, when connected, is performed in a manner that preserves the integrity of the safety software and that does not adversely affect the safety functions of the system. When connected to the maintenance network, safety software integrity is maintained through the use of non-volatile

memory which cannot be altered unless the CPU module is physically relocated to a separate reprogramming chassis.

The NRC staff determined that the data exchange between safety divisions and between safety-related processors and non-safety-related maintenance workstations complies with staff position 1, point 8.

#### **Staff Position 1, Point 9**

This position states the following:

...incoming message data should be stored in fixed predetermined locations in the shared memory and in the memory associated with the function processor. These memory locations should not be used for any other purpose. The memory locations should be allocated such that input data and output data are segregated from each other in separate memory devices or in separate pre-specified physical areas within a memory device.

As described in Section 3.2.2.3 of this SE, data link communications is conducted as broadcast transmissions from the source communications processor to all connected receiving processors.

The receiving processors perform validation checks on all incoming message data and store this data in fixed predetermined locations in the two port shared memory. The shared memory for transmitted data is separate from the shared memory of data being received. Both memory of two port memory and memory within a CPU module are dedicated memory locations and are used for no other purpose than to facilitate the transfer of data between connected processors. The NRC staff has determined that the data exchange within MELTAC platform based systems complies with staff position 1, point 9.

#### **Staff Position 1, Point 10**

This position states the following:

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

acceptable. It is noted that software may be used in the safety system or in the workstation to accommodate the effects of the open circuit or for status logging or other purposes.

MELTAC safety function processors store the basic software and application software in a F-ROM portion of the controller memory. This memory can only be changed by physically removing the CPU circuit board from the safety system and reinstalling it into a dedicated reprogramming chassis. A description of the reprogramming chassis is provided in Section 3.2.2.6 of this SE. [

]

Communications processing logic is also protected from alteration because reprogramming of the communications processing devices also requires physical removal of the associated circuit board from the safety system chassis and removal of the memory device from the circuit board to insert into a special purpose reprogramming device.

The NRC staff determined that MELCO safety-related software and logic is adequately protected from alteration while the safety division is in operation. On-line changes to MELTAC safety system software are prevented by requiring physical disconnection of circuit boards from the safety system chassis in order to facilitate changes to software.

The MELTAC engineering tool program that runs on non-safety-related maintenance workstations has the capability of altering addressable constants, setpoints, parameters, and other settings associated with the systems safety functions. However, activities that would require such alterations are restricted and controlled using several MELTAC system features. The communications interface between MELTAC safety processors and maintenance workstations is the maintenance network and this network is normally disconnected from the safety system processors at the processor end during operation. When the maintenance network is connected for the purpose of performing maintenance or system testing, communications are processed by way of two port shared-memory. The associated MELTAC safety division is inoperable during maintenance and testing evolutions. Administrative procedures can be used by licensees to control and restrict connectivity of the maintenance network to a single division on which maintenance is to be performed.

The NRC staff determined the MELTAC interdivisional and safety to non-safety communications configuration including provisions and interlocks to control access to operational software as well as configurable parameters complies with the criteria of staff position 1, point 10.

#### **Staff Position 1, Point 11**

This position states the following:

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

MELTAC safety function processors store the basic software and application software in a F-ROM portion of the controller memory. This memory can only be changed by physically removing the CPU circuit board from the safety system and reinstalling it into a dedicated reprogramming chassis and requires the use of the MELTAC engineering tool.

The MELTAC engineering tool can be used under certain circumstances to change application data on a temporary basis. Such changes to system parameters are prevented during operation by an interlock key switch and an affected division must be declared inoperable prior to performing these changes. When temporary changes are implemented, the system automatically identifies the alteration by comparing data in F-ROM with the temporarily changes data in the system random access memory and provides a continuous indication of the system status. These deviations can be configured to activate a plant alarm to notify operators of the inoperable status of the affected controller. All application data must be returned to its unaltered value in order to clear the deviation status and to restore system operability.

MELTAC data link interfaces are not capable of sending software instructions to system safety function processors. All data transferred through the data link is stored in the two port memory for transfer to the safety function processor. The processor can thus access the data from the 2 part memory but the safety processor instruction sequence would remain under the control of the basic and application safety software instructions.

The NRC staff determined the MELTAC interdivisional and safety to non-safety communications configurations preclude the ability to send software instructions to the safety function processor. The MELCO safety function processor instruction sequence cannot be affected by messages received from outside the division during system operation. Therefore, the NRC staff determined the MELTAC platform interdivisional and safety to non-safety communication interfaces conform to the criteria of staff position 1, point 11.

#### **Staff Position 1, Point 12**

This position states the following:

...communication faults should not adversely affect the performance of required safety functions in any way. Faults, including communication faults, originating in non-safety equipment, do not constitute "single failures" as described in the single failure criterion of 10 CFR Part 50, Appendix A. This SE provides 12 examples of credible communication faults, but cautions that the possible communication faults are not limited to the list of 12.

An analysis of MELTAC data link and maintenance network communication faults was provided in Section 3.2 of the MELTAC platform DI&C-ISG-04 conformance analysis (Ref. 2). This analysis describes how various faults are handled by the MELTAC platform based system. The NRC staff confirmed that all 12 of the example faults provided in Staff Position 1, Point 12 were included in this analysis. Eight additional faults derived from NUREG/CR-6991, "Design practices for communications and workstations in highly integrated control rooms," Section 2.3 were also addressed in this analysis. Methods the MELTAC platform employs to ensure that communications faults do not affect safety functions include:

- Use of CRC to identify and handle invalid communications,
- Use of point to point communication architecture with physical configuration control for the data link network to eliminate potential for multiple data sources,



- Message sequence and timing control measures to prevent data distortion, and
- Use of broadcast communication protocols that do not rely on handshaking between the source and destination processors.

For each of the identified communications faults, the analysis determined that the effects of the fault on a MELTAC based safety system did not adversely affect the performance of required safety functions. The NRC staff, therefore, determined the MELTAC platform design complies with staff position 1, point 12.

#### **Staff Position 1, Point 13**

This position states the following:

...vital communications, such as the sharing of channel trip decisions for the purpose of voting, should include provisions for ensuring that received messages are correct and are correctly understood. Such communications should employ error-detecting or error-correcting coding along with means for dealing with corrupt, invalid, untimely or otherwise questionable data. The effectiveness of error detection/correction should be demonstrated in the design and proof testing of the associated codes, but once demonstrated is not subject to periodic testing. Error correcting methods, if used, should be shown to always reconstruct the original message exactly or to designate the message as unrecoverable. None of this activity should affect the operation of the safety-function processor.

Data link broadcast point-to-point interfaces are used for all vital communications between divisions of the MELTAC platform based systems. A detailed description of data link communication point to point interfaces is provided in Section 4.3.3.1 of the MELTAC LTR (Ref. 14). These interfaces use CRC to identify and handle invalid communications. If CRC codes calculated by a receiving communications processor are incorrect, the associated data is identified as corrupt and is discarded by the processor. Error-correcting methods are not used by the MELTAC platform design. Instead, data is periodically retransmitted over the data link and message sequence and timing control measures are used to prevent data distortion and to identify and managing data that becomes stale or is otherwise invalid.

MELTAC platform design includes provisions for ensuring that received messages are correct and are correctly understood by receiving communications and safety function processors. The MELTAC platform design includes error detection coding for identifying and managing corrupt, invalid, as well as untimely or otherwise questionable data received over data link communication interfaces. Such incorrect data can be communicated to the operator as defined by system specifications. The NRC staff, therefore, determined the MELTAC platform design complies with staff position 1, point 13.

#### **Staff Position 1, Point 14**

This position states the following:

...vital communications should be point-to-point by means of a dedicated medium (copper or optical cable). In this context, "point-to-point" means that the message is passed directly from the sending node to the receiving node without the involvement of equipment outside the division of the sending or receiving

node. Implementation of other communication strategies should provide the same reliability and should be justified.

MELTAC platform data links are configured as point-to-point communication interfaces between system divisions. A detailed description of data link communication point to point interfaces is provided in Section 4.3.3.1 of the MELTAC LTR (Ref. 14). These interfaces use dedicated fiber optic media connections to transfer messages directly from the sending nodes to receiving nodes. Point-to-point source and destination nodes of the data link are application dependent. The MELTAC platform design does not include use of equipment outside the associated sending or receiving division; however, licensees referencing the MELTAC LTR should confirm that no equipment outside of the safety division is configured for use in the transmission of messages through the data link interfaces of the system. The NRC staff, therefore, determined the MELTAC platform design is capable of compliance with Staff Position 1, Point 14 as long as plant specific design configurations do not introduce out of division dependencies.

#### **Staff Position 1, Point 15**

This position states the following:

...communications for safety functions should communicate a fixed set of data (called the "state") at regular intervals, whether data in the set has changed or not.

MELTAC data link communications use a fixed data format of data sets. A detailed description of data link communication point to point interfaces is provided in Section 4.3.3.1 of the MELTAC LTR (Ref. 14). These data sets are periodically transmitted at a predefined interval and no handshaking occurs between communication processors in either transmitting or receiving ends of the interfaces. Transmittal of data does not depend on changes in data state or content. The data sets used for the MELTAC data link are predefined and data set format and sequence are pre-determined. The NRC staff, therefore, determined the MELTAC platform design complies with staff position 1, point 15.

#### **Staff Position 1, Point 16**

This position states the following:

...network connectivity, liveness, and real-time properties essential to the safety application should be verified in the protocol. Liveness, in particular, is taken to mean that no connection to any network outside the division can cause a RTS/ESFAS communication protocol to stall, either deadlock or livelock. (Note: This is also required by the independence criteria of: (1) 10 CFR Part 50, Appendix A, GDC 24, which states, "interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired" and (2) IEEE Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations" (Source: NUREG/CR-6082, Section 3.4.3).

The MELTAC data link uses message sequence and timing control measures to identify and manage communications interface issues that could potentially affect data link network connectivity. These measures include the capability of detecting stagnant or otherwise invalid data received from the communications interface. Connectivity to processors that are outside of a division are restricted through the use of a point-to-point network architecture and the use of

broadcast data transmissions that do not rely on the use of handshaking signals between communications processors. The NRC staff reviewed the data link specifications provided in Section 4.3.3.1 of the MELTAC LTR (Ref. 14) and determined that the MELTAC data link communications protocols are not susceptible to network stalling and are therefore capable of supporting vital safety communications without adverse impact to system safety functions. As an added measure of protection from communications failures, MELTAC safety function processors run asynchronously and independently from the communications processors. As such, system safety function processors, when programmed correctly, do not rely on data link communications for safety application execution. MELTAC application programs must be programmed to respond to loss of the communication.

The NRC staff determined that safety function response to data link communication errors, including deadlock and livelock, is application dependent. The NRC staff, therefore, determined the MELTAC platform design complies with staff position 1, point 16 as long as plant specific applications are implemented in a manner which does not introduce communication data dependencies.

#### **Staff Position 1, Point 17**

This position states the following:

...pursuant to 10 CFR 50.49, the medium used in a vital communications channel should be qualified for the anticipated normal and post-accident environments. For example, some optical fibers and components may be subject to gradual degradation as a result of prolonged exposure to radiation or to heat. In addition, new digital systems may need susceptibility testing for EMI/RFI and power surges, if the environments are significant to the equipment being qualified.

Cross divisional communications for a MELTAC platform based system are performed over data link communication interfaces. The components of these interfaces are described in Section 3.2.2.2 of this SE. MELTAC platform components have been qualified for operation in a mild environment. Qualifications include seismic, temperature and humidity, and EMI/RFI.

All data link interdivisional communications are made via fiber optic media. Fiber optic cables are selected and qualified on an application-dependent basis with consideration for installed plant environments. The fiber optic cabling provides electrical isolation between safety divisions as well as EMI/RFI protection for system components. The bus master modules and the Fiber Optic Electrical to Optic Converters were subject to environmental qualifications as discussed in Section 3.6 of this SE. The generic qualification of the MELTAC platform encompasses both the hardware and the software used in the system. The MELTAC platform was qualified in accordance with the EPRI TR-102323 criteria.

As noted in Section 3.6 of this SE, the qualification of the MELTAC platform does not include the fiber optic cables used to connect the data link and control network interfaces. Therefore, a plant specific evaluation will be required for plant specific applications of a MELTAC platform that utilizes fiber optic cables to connect data link interfaces between safety divisions.

The NRC staff determined that the MELTAC platform meets the guidance provided by Staff position 1, point 17. However, as noted above, fiber optic cables used to implement data link communications for a system in safety applications will require a plant specific evaluation to verify these cables are qualified for the environment in which they will be used, in accordance

with 10 CFR 50.49 as applicable. Furthermore, safety applications using the MELTAC platform will require plant specific review to confirm that the plant specific environment is consistent with the qualification envelope defined in Section 3.6 of this SE.

#### **Staff Position 1, Point 18**

This position states the following:

...provisions for communications should be analyzed for hazards and performance deficits posed by unneeded functionality and complication.

An analysis of MELTAC data link and maintenance network communication faults was provided in Section 3.2 of the MELTAC platform DI&C-ISG-04 conformance analysis (Ref. 2). This analysis describes how system level hazards caused by various communications faults are handled by the MELTAC platform based system. However, potential hazards posed to specific safety functions, relating to interdivisional data link communications, must be analyzed at the application level.

The NRC staff determined that for the MELTAC platform, the requirement to perform failure modes and effects analyses for plant specific applications meets the intent of the guidance provided in staff position 1, point 18. However, an application specific determination of conformance with this position is required. See PSAI 5.2.12.

#### **Staff Position 1, Point 19**

This position states the following:

...the communications data rates be such that they will not exceed the capacity of a communications link or the ability of nodes to handle traffic, and that all links and nodes have sufficient capacity to support all functions. To do this, the applicant should identify the true data rate, including overhead, to ensure that communication bandwidth is sufficient to ensure proper performance of all safety functions and that communications throughput thresholds and safety system sensitivity to communications throughput issues should be confirmed by testing.

Data link communication data rate and data quantity are constant during system operation. Established communication rates are within the bandwidth capacity for each communication interface. See Section 3.7.2 of this SE for the NRC evaluation of MELTAC platform deterministic performance characteristics.

The NRC staff confirmed the deterministic response time of the communication interface is factored into the total response time of a safety function application. The total safety function response time must be confirmed through application level testing.

MELTAC communication rates can be affected by failures in the communication interface. However, because of asynchronous operation, the safety system function processors will continue to perform all programmed instructions per application design requirements. MELCO identified specific methods used during development to ensure immunity to excessive message rates. The NRC staff reviewed these methods and agrees these methods should result in conformance with this position, however, implementation of MELTAC platform safety system applications will require a plant specific review to verify conformance to the guidance of

staff position 1, point 19.

#### **Staff Position 1, Point 20**

This position states the following:

...the safety system response time calculations should assume a data error rate that is greater than or equal to the design basis error rate and is supported by the error rate observed in design and qualification testing.

A discussion of the MELCO platform response time is provided in Section 3.7.1 of this SE. To ensure that the MELCO platform meets its application system response time requirements, the execution time for all of the systems tasks is calculated and measured during system development. This calculation includes terms to address the response time of communications, memory processing and associated circuits.

Staff Position 1, Point 20, cannot be assessed for the MELCO platform and must be evaluated as a plant specific review because this time will depend on the system configuration, application software, and data link Interfaces used. When implementing a MELCO safety system the licensee must review the application specific timing analyses and validation tests for the MELCO system in order to verify that it satisfies its plant specific requirements for system response and display response time presented in the accident analysis in the plants safety analysis report.

#### **3.9.1.2 DI&C-ISG-04, Section 2 - Command Prioritization**

Section 2 of DI&C-ISG-04 provides guidance applicable to a prioritization device or software function block, which receives device actuation commands from multiple safety-related and non-safety-related sources, and sends the command having highest priority on to the actuated device.

The MELTAC platform includes a PIF module which is used to implement command prioritization functions for MELTAC based systems. A description of the PIF module is provided in Section 3.2.1.5.2 of this SE.

MELTAC PIF module design uses state-based priority logic to perform device actuation based on safety system inputs or backup system (e.g., the diverse actuation system) inputs. PIF modules receive component actuation input from the MELTAC safety CPU controllers via the I/O bus. The MELTAC PIF modules are capable of actuating plant components in direct response to external contact inputs, independently of the MELTAC controller output commands. Several types of PIF module sub-boards are available for controlling different types of plant components.

Below is the NRC staff evaluation of command prioritization.

#### **Command Prioritization Staff Position 1**

This position states the following:

...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.

MELTAC PIF modules are classified as safety-related components. PIF modules are therefore designed to meet the requirements of 10 CFR Part 50, Appendices A and B. The lifecycle processes used for the MELTAC platform are controlled under the MELCO QA program. This QA program is evaluated in Sections 3.4 & 3.5.1.3 of this SE. Therefore the MELTAC PIF modules conform to the guidance of command prioritization staff position 1.

### **Command Prioritization Staff Position 2**

This position states the following:

...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.

MELTAC PIF modules receive actuation input signals from the safety system processors via the I/O bus communications interface. The I/O bus communication interfaces of the MELTAC platform are used for communications within safety divisions. PIF modules can also receive actuation input signals via external contacts from other systems such as a non-safety-related diverse actuation system. There are no digital communications between Non-Safety Systems and the PIF modules. These modules are designed with the capability of operating independently from the MELTAC safety function processors. The state and condition of the safety system processor cannot affect the basic functionality of connected PIF modules. The NRC staff determined that MELTAC PIF modules therefore conform to the criteria of command prioritization staff position 2.

### **Command Prioritization Staff Position 3**

This position states the following:

...Safety-related commands that direct a component to a safe state must always have the highest priority and must override all other commands. Commands that originate in a safety-related channel but which only cancel or enable cancellation of the effect of the safe-state command (that is, a consequence of a Common-Cause Failure in the primary system that erroneously forces the plant equipment to a state that is different from the designated "safe state."), and which do not directly support any safety function, have lower priority and may be overridden by other commands. In some cases, such as containment isolation valve in an auxiliary feedwater line, there is no universal "safe state". The valve must be open under some circumstances and closed under others. The relative priority to be applied to commands from a diverse actuation system, for example, is not obvious in such a case. This is a system operation issue, and priorities should be assigned on the basis of considerations relating to plant system design or other criteria unrelated to the use of digital systems. This issue is outside the scope of this ISG. The reasoning behind the proposed priority ranking should be explained in detail. The reviewer should refer the proposed priority ranking and the explanation to appropriate systems experts for review.

The priority module itself should be shown to apply the commands correctly in order of their priority rankings, and should meet all other applicable guidance. It should be shown that the unavailability or spurious operation of the actuated device is accounted for in, or bounded by, the plant safety analysis.

The logic within the PIF module sub-boards can be configured to give priority to the safe state of the component, regardless of which input (system) demands the safe state. Defining safety function safe states and establishing necessary logic to achieve the safe state for all conditions are plant specific determinations. Conformance to the criteria of Command Prioritization Position 3 is therefore dependent on application specific logic configuration of the PIF module sub boards and cannot be determined on a generic basis. The NRC staff reviewed the PIF module design and agrees these modules are capable of being configured to establish compliance with this position. However, implementation of MELTAC platform safety system applications will require plant specific review to verify conformance to the guidance of command prioritization staff position 3.

#### **Command Prioritization Staff Position 4**

This position states the following:

...A priority module may control one or more components. If a priority module controls more than one component, then all of these provisions apply to each of the actuated components.

The MELTAC PIF modules are not designed to control more than one single plant component. The MELTAC PIF modules therefore conform to command prioritization staff position 4.

#### **Command Prioritization Staff Position 5**

This position states the following:

...Communication isolation for each priority module should be as described in the guidance for interdivisional communications.

MELTAC PIF modules do not contain data link communication interfaces and therefore do not communicate directly with other safety divisions. PIF modules are however capable of receiving discrete contact input signals from external systems such as a diverse actuation system. These signals are further isolated through the use of optical isolators. These actuation inputs do not use digital communications technology. Therefore, the use of external data communication inputs was not evaluated in this SE.

The NRC staff evaluated the PIF module design and determined the only communications functions performed are the I/O bus communications with the associated safety function processor which are internal to the safety division. All other signals received by PIF modules are isolated discrete signals for which the guidance for interdivisional communications does not apply. The NRC staff, therefore, determined that MELCO PIF module design complies with the criteria of command prioritization staff position 5.

### **Command Prioritization Staff Position 6**

This position states the following:

...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 Std. 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. Section 5.3.2, "Software tools" of IEEE 7-4.3.2-2003 is particularly applicable to this subject. 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.

Input actuation signals from the MELTAC safety function processors are received through the I/O bus communications interface. MELTAC PIF modules use FPGA technology for processing I/O bus communications; however, command prioritization functions are not performed by the PIF module processors. Instead, separate circuitry, which does not rely on software or logic processing, is used to ensure system actuation priorities are established. The circuitry used for command prioritization is composed of hardware based components and is therefore not subject to the criteria of IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations." Nonetheless, the development process used for the FPGA communications processors in the PIF modules was determined to be compliant with IEEE Std. 7-4.3.2 as endorsed by RG 1.152. See Section 3.11 of this SE for IEEE Std. 7-4.3.2 compliance evaluation. The NRC staff, therefore, determined that MELCO PIF module design complies with the criteria of command prioritization staff position 6.

### **Command Prioritization Staff Position 7**

This position states the following:

...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.

The I/O bus communications processors in the MELTAC PIF modules are used in support of the safety functions. These processors are safety-related and are developed in accordance with MELTAC safety development processes described and evaluated in Section 3.5 of this SE. The

non-volatile memory associated with the I/O communications processor cannot be changed on-line. Reprogramming or alteration of the PIF module communications processor requires removal of the module from the system. The NRC staff, therefore, determined that MELCO PIF module design complies with the criteria of command prioritization staff position 7.

#### **Command Prioritization Staff Position 8**

This position states the following:

...To minimize the probability of failures due to common software, the priority module design should be fully tested (This refers to proof-of-design testing, not to individual testing of each module and not to surveillance testing). If the tests are generated by any automatic test generation program then all the test sequences and test results should be manually verified. Testing should include the application of every possible combination of inputs and the evaluation of all of the outputs that result from each combination of inputs. If a module includes state-based logic (that is, if the response to a particular set of inputs depends upon past conditions), then all possible sequences of input sets should also be tested. If testing of all possible sequences of input sets is not considered practical by an applicant, then the applicant should identify the testing that is excluded and justify that exclusion. The applicant should show that the testing planned or performed provides adequate assurance of proper operation under all conditions and sequences of conditions. Note that it is possible that logic devices within the priority module include unused inputs: assuming those inputs are forced by the module circuitry to a particular known state, those inputs can be excluded from the "all possible combinations" criterion. For example, a priority module may include logic executed in a gate array that has more inputs than are necessary. The unused inputs should be forced to either "TRUE" or "FALSE" and then can be ignored in the "all possible combinations" testing.

MELTAC PIF modules do not use state-based logic. The response to PIF module inputs does not depend upon past conditions. However, testing of the PIF modules does include the application of all possible combinations of inputs and the evaluation of all of the outputs that result from each combination of inputs. The NRC staff, therefore, determined that MELCO PIF module design complies with the criteria of command prioritization staff position 8.

#### **Command Prioritization Staff Position 9**

This position states the following:

...Automatic testing within a priority module, whether initiated from within the module or triggered from outside and including failure of automatic testing features, should not inhibit the safety function of the module in any way. Failure of automatic testing software could constitute common-cause failure if it were to result in the disabling of the module safety function.

MELTAC PIF module design does not include the use of automatic testing of priority logic functions. The I/O communications processor within the PIF module does include self-diagnostics for communications and input functions. The NRC staff evaluated the communication processor functions as described in Section 4.3.3.3 of the MELTAC LTR (Ref. 14) and determined they cannot inhibit or otherwise affect the priority logic functions of the

PIF module. The NRC staff, therefore, determined that MELCO PIF module design complies with the criteria of command prioritization staff position 9.

### **Command Prioritization Staff Position 10**

This position states the following:

... The priority module must ensure that the completion of a protective action as required by IEEE Std. 603 is not interrupted by commands, conditions, or failures outside the module's own safety division.

The MELTAC PIF module receives actuation inputs from the safety processors within its assigned division through the I/O bus. There is no connection or communications interface to other divisions of the MELCO safety system. Therefore, there is no potential for completion of protective action functions or any command prioritization functions of the PIF module to be interrupted or otherwise affected by commands, conditions or failures originating in other safety divisions.

MELTAC PIF modules also receive actuation signal inputs from external systems. These signals are isolated discrete logic inputs. The NRC staff evaluated the potential effects of commands, conditions or failures of these external systems and determined that command prioritization functions including those used to support completion of a protective actions cannot be interrupted or otherwise affected by external systems. The NRC staff, therefore, determined that MELCO PIF module design complies with the criteria of command prioritization staff position 10.

#### **3.9.1.3 DI&C-ISG-04, Section 3 - Multidivisional Control and Display Stations**

Section 3 of DI&C-ISG-04 provides guidance concerning operator workstations used for the control of plant equipment in more than one safety division and for display of information from sources in more than one safety division, and applies to workstations that are used to program, modify, monitor, or maintain safety systems that are not in the same safety division as the workstation. Below is the NRC staff evaluation of the MELTAC operator workstation.

#### **Multidivisional Control and Display Station Staff Position 3.1-1**

This position states the following:

Non-safety stations receiving information from one or more safety divisions:  
All communications with safety-related equipment should conform to the guidelines for interdivisional communications.

Interdivisional communications for the MELTAC platform are conducted through the data link interfaces. These interfaces are described in Section 3.2.2.2 of this SE. The NRC staff evaluated the MELTAC data link communications features and determined them to be compliant with the criteria for interdivisional communications. However, some aspects of interdivisional communications are plant specific and, therefore, must be evaluated when a MELTAC based system is developed. Details of this evaluation are provided in Section 3.9.1.1 of this SE.

Communications between safety-related MELTAC equipment and non-safety-related equipment are conducted through maintenance network communication interfaces. These are described in



Section 3.2.2.4 of this SE. MELTAC safety processors are normally disconnected from the maintenance network during plant operations. The NRC staff evaluated the MELTAC maintenance network communications features and determined them to be compliant with the criteria for interdivisional communications. The NRC staff, therefore, determined that safety-related to non-safety-related communications conform to the guidance provided for interdivisional communications as discussed in Section 3.9.1.1 of this SE.

#### **Multidivisional Control and Display Station Staff Position 3.1-2**

This position states the following:

Safety-related stations receiving information from other divisions (safety or non-safety):

All communications with equipment outside the stations own safety division, whether that equipment is safety-related or not, should conform to the guidelines for interdivisional communications. Note that the guidelines for interdivisional communications refer to provisions relating to the nature and limitations concerning such communications, as well as guidelines relating to the communications process itself.

Both safety-related communications via data link interfaces and non-safety-related communications via maintenance network interfaces were evaluated by the NRC staff and were found to be compliant with the guidance provided for interdivisional communications as discussed in Section 3.9.1.1 of this SE.

#### **Multidivisional Control and Display Station Staff Position 3.1-3**

This position pertains to Non-safety stations controlling the operation of safety-related equipment.

The MELTAC platform design does not include provisions for operation of safety-related equipment from non-safety-related workstations. The only non-safety-related workstations included in the MELTAC platform are the maintenance workstations. A description of the MELTAC maintenance workstations is provided in Section 3.2.2.5 of this SE. These workstations communicate with safety processors and the S-VDU processors through the maintenance network communication interfaces; however, these interfaces are normally disconnected from the safety processors during plant operations. Temporary connections of safety processors to the maintenance network can be made to support maintenance and surveillance related activities and are not intended to be used for the control of safety-related equipment. Administrative control measures must be taken to ensure removal of any safety processor from service prior to connecting the processor to the maintenance network. The NRC staff, therefore, determined that MELTAC maintenance workstation design complies with the criteria of command prioritization staff position 3.1-3.

#### **Multidivisional Control and Display Station Staff Position 3.1-4**

This position states the following:

Safety-related stations controlling the operation of equipment in other safety-related divisions:

Safety-related stations controlling the operation of equipment in other divisions are subject to constraints similar to those described above for non-safety stations that control the operation of safety-related equipment.

The MELTAC platform design does not include provisions for operation of equipment in other safety-related divisions from S-VDUs. Instead, S-VDU's are only interfaced with and thus can only control equipment which is assigned to the same division as the S-VDU itself. This position also states the following:

A control station should access safety-related plant equipment outside its own division only by way of a priority module associated with that equipment. Priority modules should be designed and applied as described in the guidance on priority modules.

MELTAC S-VDU's cannot be used to control equipment in different divisions and, therefore, this criteria is not applicable to the MELTAC platform design.

This position also states the following:

A station must not influence the operation of safety-related equipment outside its own division when that equipment is performing its safety function. This provision should be implemented within the affected (target) safety-related system, and should be unaffected by any operation, malfunction, design error, software error, or communication error outside the division of which those controls are a member.

MELTAC cross divisional communication is conducted through data link communication interfaces. The NRC staff evaluated these interfaces and determined that communication of data through the data link interfaces will not influence the operation of safety-related MELTAC controllers provided application specific requirements are correctly implemented. See Section 3.9.1.1 of this SE for a detailed assessment of MELTAC data link communication interfaces. Conformance to this position is plant specific.

This position also states the following:

The extra-divisional (that is, "outside the division") control station should be able to bypass a safety function only when the affected division itself determined that such action would be acceptable.

MELTAC S-VDU's cannot be used to control equipment or to initiate safety function bypass in other divisions and therefore this criteria is not applicable to the MELTAC platform design. This position also states the following:

The extra-divisional station should not be able to suppress any safety function. (If the safety system itself determines that termination of a safety command is warranted as a result of the safety function having been achieved, and if the applicant demonstrates that the safety system has all information and logic needed to make such a determination, then the safety command may be reset from a source outside the safety division. If operator judgment is needed to establish the acceptability of resetting the safety command, then reset from outside the safety division is not acceptable because there would be no protection from inappropriate or accidental reset.)

Because MELTAC S-VDU's cannot be used to control equipment in different divisions, there is no potential for S-VDU's to suppress or otherwise affect the safety functions being performed in another safety division.

This position also states the following:

The extra-divisional station should not be able to bring a safety function out of bypass condition unless the affected division has itself determined that such action would be acceptable.

Because MELTAC S-VDU's cannot be used to control equipment in different divisions, there is no potential for S-VDU's to change the bypass state of safety functions performed in another safety division. This criteria is not applicable to the MELTAC platform design.

### **Multidivisional Control and Display Station Staff Position 3.1-5**

This position also states the following:

#### **Malfunctions and Spurious Actuations:**

The result of malfunctions of control system resources (e.g., workstations, application servers, protection/control processors) shared between systems must be consistent with the assumptions made in the safety analysis of the plant. Design and review criteria for complying with these requirements, as set forth in 10 C.F.R. § 50.34 and 50.59, include but are not limited to the following: Control processors that are assumed to malfunction independently in the safety analysis should not be affected by failure of a multidivisional control and display station.

Safety VDUs within the MELTAC platform do not interface with MELTAC controllers or with Safety VDUs in other safety divisions. The NRC staff, therefore, determined that MELTAC S-VDU's are functionally independent from equipment and processors in other divisions. Failures of S-VDU processor cannot affect the operation of MELTAC controllers or equipment in other safety divisions. The MELTAC platform design is therefore compliant with this criterion. However, compliance to plant safety analysis requirements remains a plant application specific criteria and must be addressed during application development.

This position also states the following:

Control functions that are assumed to malfunction independently in the safety analysis should not be affected by failure of a single control processor. Safety and control processors should be configured and functionally distributed so that a single processor malfunction or software error will not result in spurious actuations that are not enveloped in the plant design bases, accident analyses, ATWS provisions, or other provisions for abnormal conditions. This includes spurious actuation of more than one plant device or system as a result of processor malfunction or software error. The possibility and consequences of malfunction of multiple processors as a result of common software error must be addressed.

The MELTAC platform is designed to maintain functional independence between system S-VDU's and safety function processors. Compliance to plant safety analysis requirements is plant specific and must be addressed during application development.

This position also states the following:

No single control action (for example, mouse click or screen touch) should generate commands to plant equipment. Two positive operator actions should be required to generate a command. For example: When the operator requests any safety function or other important function, the system should respond "do you want to proceed?" The operator should then be required to respond "Yes" or "No" to cause the system to execute the function. Other question-and-confirm strategies may be used in place of the one described in the example. The second operation as described here is to provide protection from spurious actuations, not protection from operator error. Protection from operator error may involve similar but more restrictive provisions, as addressed in guidance related to Human Factors.

The NRC staff reviewed the S-VDU design and determined it to be capable of meeting this criteria. However, compliance is dependent on plant specific design and must be evaluated during plant specific application development.

This position also states the following:

Each control processor or its associated communication processor should detect and block commands that do not pass the communication error checks.

S-VDU processors communicate using data link or control network interfaces. The NRC staff evaluated both of these communication interfaces and determined adequate communication error detection and handling features are incorporated. See Section 3.9.1.1 of this SE for evaluation of error handling functions.

Multidivisional control and display stations should be qualified to withstand the effects of adverse environments, seismic conditions, EMI/RFI, power surges, and all other design basis conditions applicable to safety-related equipment at the same plant location. This qualification need not demonstrate complete functionality during or after the application of the design basis condition unless the station is safety-related. Stations which are not safety-related should be shown to produce no spurious actuations and to have no adverse effect upon any safety-related equipment or device as a result of a design basis condition, both during the condition and afterwards. If spurious or abnormal actuations or stoppages are possible as a result of a design basis condition, then the plant safety analyses must envelope those spurious and abnormal actuations and stoppages. Qualification should be supported by testing rather than by analysis alone. D3 considerations may warrant the inclusion of additional qualification criteria or measures in addition to those described herein.

The NRC staff confirmed the S-VDU's were included in the qualification test system configuration. As such, a representative S-VDU device was subjected to all qualification test conditions and performance of the test system VDU was monitored during and following each

environmental test case. See Section 3.6 , "Equipment Qualification" of this SE for results of the MELTAC platform EQ evaluation.

Loss of power, power surges, power interruption, and any other credible event to any operator workstation or controller should not result in spurious actuation or stoppage of any plant device or system unless that spurious actuation or stoppage is enveloped in the plant safety analyses.

Compliance to plant safety analysis requirements is plant application specific and must be addressed during application development.

The design should have provision for an "operator workstation disable" switch to be activated upon abandonment of the main control room, to preclude spurious actuations that might otherwise occur as a result of the condition causing the abandonment (such as control room fire or flooding). The means of disabling control room operator stations should be immune to short-circuits, environmental conditions in the control room, etc. that might restore functionality to the control room operator stations and result in spurious actuations.

MELTAC platform based systems are capable of being designed to meet the criteria of this clause however, specific criteria for control room abandonment are plant specific and must be addressed during application development.

Failure or malfunction of any operator workstation must not result in a plant condition (including simultaneous conditions) that is not enveloped in the plant design bases, accident analyses, and ATWS provisions, or in other unanticipated abnormal plant conditions.

Compliance to plant design basis, accident analysis, and ATWS requirements are plant application specific and must be addressed during application development.

### 3.10 Compliance to IEEE Std. 603-1991 Requirements

For applicable nuclear power generating stations, the regulation at 10 CFR 50.55a(h) requires that safety systems must meet the requirements stated in IEEE Std. 603-1991 and the correction sheet dated January 30, 1995. The NRC staffs evaluation is based on the guidance contained in SRP Chapter 7, Appendix 7.1-C which provides acceptance criteria for this standard. This NRC staff evaluation also addresses the RG 1.153 endorsement of IEEE Std. 603-1991.

A summary of compliance with IEEE Std. 603 and IEEE Std. 7-4.3.2 (References 8 and 9) was submitted to the NRC to support this evaluation. For its evaluation, the NRC staff referred to Table 3 of References 8 and 9 document which provides references to other supporting material. The results of this evaluation are documented as follows. Compliance with IEEE Std. 603 criteria is a plant specific action. See PSAI 5.2.13.

#### 3.10.1 IEEE Std. 603-1991 Clause 4, "Safety System Designation"

Clause 4 of IEEE Std. 603-1991 states that a specific basis shall be established for the design of each safety system of the nuclear power generating station. SRP Chapter 7, Appendix 7.1-C, Section 4, "Safety System Designation" provides acceptance criteria for these requirements.



The determination and documentation of the design basis for a safety system is a plant specific activity that is dependent on the plant design. Since the MELTAC LTR (Ref. 14) does not address a specific application of the platform, the design basis for a safety system is not available for review and no evaluation of the MELTAC platform against these regulatory requirements could be performed. Nevertheless, MELCO provided a summary of compliance to the criteria of IEEE Std. 603 in Reference 8. This summary provides a cross-reference of IEEE Std. 603-1991 criteria and information in the MELTAC platform topical report that can be used to address certain items within Clause 4. The NRC staff reviewed these assessments as follows.

#### Clause 4.7 Range of Conditions for Safety System Performance

This clause states that the range of transient and steady-state conditions of both motive and control power and the environment (e.g., voltage, frequency, radiation, temperature, humidity, pressure, and vibration) during normal, abnormal, and accident circumstances throughout which the safety system shall perform shall be documented.

The MELTAC platform LTR (Ref. 14) partially addresses this criteria by establishing documentation for the qualified range of operation of a MELTAC based safety system. Table 4.1.1-2 of the MELTAC LTR documents the range of environmental conditions to which the MELTAC platform components are qualified to operate. Section 5.0 of the MELTAC LTR documents additional details of MELTAC qualifications and provides references to specific qualification standards, test procedures and test reports that provide a basis for the MELTAC component qualifications. This documentation can be used to support a plant specific application of the MELTAC platform provided that plant specific environmental conditions do not exceed the established conditions to which the MELTAC platform is qualified.

#### Clause 4.8 Functional Degradation of Safety System Performance

This clause states that conditions having the potential for functional degradation of safety system performance and for which provisions shall be incorporated to retain the capability for performing the safety functions (e.g., missiles, pipe breaks, fires, loss of ventilation, spurious operation of fire suppression systems, operator error, and failure in non-safety-related systems) shall be documented.

The MELTAC platform design partially addresses this criteria by incorporating design features that establish independence between the safety system components of a MELTAC based safety system and non-safety-related systems connected via isolation devices and the MELTAC maintenance network communication interfaces. The documentation provided in the MELTAC LTR (Ref. 14) can be credited for compliance with functional independence and isolation requirements of IEEE Std. 603.

#### Clause 4.9 Reliability

This clause states methods to be used to determine that the reliability of the safety system design is appropriate for each safety system design and any qualitative or quantitative reliability goals that may be imposed on the system design shall be documented.

The MELTAC platform LTR (Ref. 14) partially addresses this criteria by providing documented basis for the platform self-diagnostics functions. MELTAC self-diagnostic capabilities are described in Section 4.1.5 of the LTR and an evaluation of these platform features is provided in

Section 3.7.3 of this SE. Section 4.2.3 of the LTR also describes self-diagnostics capabilities of the MELTAC platform.

Section 7.0 of the LTR also partially addresses this criteria by providing documentation of methods used to assess MELTAC module reliability. A summary of MELTAC platform reliability (Ref. 4) also provides a documented basis for establishing compliance with plant system reliability goals. Section 3.5.2.7 of this SE documents the NRC evaluation of the reliability characteristics of a MELTAC safety system. This information can be used to support an application of the MELTAC platform.

### 3.10.2 IEEE Std. 603-1991 Clause 5, "Safety System Criteria"

Clause 5 of IEEE Std. 603-1991 requires that safety systems maintain plant parameters with precision and reliability, within acceptable limits established for each design basis event. The power, I&C portions of each safety system are required to be comprised of more than one safety group of which any one safety group can accomplish the safety function.

The establishment of safety groups that can accomplish a given safety function is a plant specific activity and the LTR scope does not include specific applications. Therefore, the following evaluations against the requirements of IEEE Std. 603-1991, Section 5 are limited to capabilities and characteristics of the MELTAC platform that are relevant to satisfy each requirement.

The following clauses were not evaluated because addressing compliance with this guidance is a plant specific activity that depends on the system design. Therefore, NRC staff determinations are not provided for these clauses.

- Clause 5.2, Completion of Protective Action
- Clause 5.8 Information Displays
- Clause 5.9, Control of Access
- Clause 5.11, Identification
- Clause 5.12, Auxiliary Features
- Clause, 5.13, Multi-unit Stations
- Clause 5.14, Human Factor Considerations

### IEEE Std. 603-1991, Clause 5.1, "Single Failure Criterion"

This clause requires:

...the safety system be able to perform its safety function required for a design basis event in the presence of: (1) any single detectable failure within the safety systems concurrent with all identifiable, but non-detectable, failures, (2) all failures caused by the single failure, and (3) all failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions.

Determination that no single failure within the safety system can prevent required protective actions at the system level is a plant specific activity that requires an assessment of a full system design. A platform-level assessment can only address those features and capabilities that support adherence to the single failure criterion by a system design based on the specified

platform. Since the MELTAC LTR (Ref. 14) does not address a specific application for approval, the evaluation against this requirement is limited to consideration of the means provided within the MELTAC platform to address failures. The NRC staff evaluation of the capabilities and characteristics of the MELTAC platform that are relevant to the single-failure criterion are documented in Section 3.7.3, self-diagnostics and test and calibration capabilities, and Section 3.5.2.6, "Failure Mode and Effects Analysis," of this SE. Licensee's using MELTAC platform can use this information to support a plant specific application.

IEEE Std. 603-1991, Clause 5.3, "Quality"

Clause 5.3 of IEEE Std. 603-1991 states:

...the components and modules within the safety system must be of a quality that is consistent with minimum maintenance requirements and low failure rates, and that safety system equipment be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed QA program. SRP Chapter 7, Appendix 7.1-C, Section 5.3, "Quality," provides acceptance criteria for the quality requirement. This acceptance criteria states that the QA provisions of 10 CFR Part 50, Appendix B, apply to a safety system.

The MELTAC platform was originally developed under a Japanese nuclear quality program which was not assessed by the NRC to be compliant to 10 CFR 50, Appendix B. MELCO subsequently performed a re-evaluation of the MELTAC platform design and design processes. This re-evaluation, referred to as the MELTAC re-evaluation Program (MRP), was conducted in accordance with the 10 CFR Part 21 commercial grade dedication process by an organization that was independent from the platform design organization.

MELCO uses an 10 CFR 50, Appendix B based QA program to govern all activities related to development of MELTAC platform components and systems. The MELCO 10 CFR 50, Appendix B based QA program was also used to govern the MRP commercial grade dedication activities.

The MELCO 10 CFR 50, Appendix B based QA program is established by the quality manual, which was submitted to the NRC as a supplemental document to support this SE (Ref. 5). MELCO also submitted a summary of MELTAC platform QA document to support this evaluation (also contained in Reference 5).

The NRC staff reviewed these documents and confirmed that the platform is now maintained under the MELCO 10 CFR 50, Appendix B based QA program, which is intended to satisfy the requirements of 10 CFR 50, Appendix B during all phases of the product life cycle. The MELCO 10 CFR 50, Appendix B based QA program governs all aspects of the MELTAC platform development including the design control process, purchasing, fabricating, handling, shipping, storing, building, inspecting, testing, operating, maintaining, repairing, and modifying of the generic platform. However, application software and its specific life cycle processes are outside the scope of this review and should be addressed in plant specific reviews. See PSAI 5.2.13.

Based on the review of the MELTAC platform development process, operating experience, life cycle design output documentation, and testing and review activities, the NRC staff finds the dedication evidence of the MELTAC platform to be acceptable for demonstrating built-in quality, and thus the MELTAC hardware and basic software show sufficient quality to be suitable for use in safety-related nuclear applications.

#### IEEE Std. 603-1991, Clause 5.4, "Equipment Qualification"

SRP Chapter 7, Appendix 7.1-C, Section 5.4, "Equipment Qualification" provides acceptance criteria for IEEE Std. 603-1991, Clause 5.4.

The qualification of the MELTAC platform under the generic service conditions required in EPRI TR-107330 were used to demonstrate the capability of a safety system based on the MELTAC platform to satisfy this requirement. The evaluation of the environmental qualification for the MELTAC platform is contained in Section 3.6 of this SE. This SE also identifies plant specific actions necessary to demonstrate that the MELTAC platform performance as bounded by its EQ satisfies the requirements of the plant specific installation environment for the plant specific and plant specific safety functions.

The NRC staff evaluation provided in Section 3.6 determined that the MELTAC platform EQ provided a type test and supporting analyses to establish a documented set of platform safety functions, range of installation conditions, and installation limitations for the MELTAC platform that is suitable for reference by licensees and conforms to RG 1.209's endorsement of IEEE Std. 323-2003 for qualification of safety-related computer-based I&C systems installed in mild environment locations. The NRC staff further determined that the MELTAC platform is capable of satisfying IEEE Std. 603-1991, Clause 5.4, for the plant specific use, as long as, a referencing applicant or licensee confirms that the application and installation have been bounded by the MELTAC platform EQ including each boundary/interface condition and installation limitation.

#### IEEE Std. 603-1991, Clause 5.5, "System Integrity"

This clause states that:

...the safety systems be designed such that the system can accomplish its safety functions under the full range of applicable conditions enumerated in the design basis. SRP Chapter 7, Appendix 7.1-C, Section 5.5, "System Integrity," provides acceptance criteria for system integrity.

Determination of system integrity is a plant specific activity that requires an assessment of a full system design against a plant specific design basis. A platform-level assessment can only address those characteristics that support fulfillment of this requirement by a system design based on the platform. Since the MELTAC LTR (Ref. 14) does not address a specific application or establish a definitive safety system design, the evaluation against this requirement is limited to consideration of the integrity demonstrated by the MELTAC platform and its features to assure a safe state can be achieved in the presence of failures. While the evaluation indicates the suitability of the platform to contribute to satisfying this requirement, a plant specific evaluation is necessary to establish full conformance with Clause 5.5.

The MELTAC platform design has several characteristics that can be used to establish a high level of system integrity. Though specific ranges of applicable conditions are not enumerated in the LTR, platform components are qualified to ranges of conditions that are typically acceptable for nuclear power plant applications. Licensee's using a MELTAC based safety system are required to ensure that enumerated plant design conditions are within the conditions for which the MELTAC platform components are qualified. For most safety applications, re-qualification of MELTAC components beyond established qualification levels will not be necessary.

MELTAC based systems are also designed to operate in a deterministic manner. The NRC staff evaluated the deterministic attributes of the MELTAC platform and the results of that evaluation are in Section 3.7.2 of this SE. Deterministic performance and high reliability are attributes of the MELTAC platform which can support compliance with system integrity criteria of Clause 5.5 of IEEE Std. 603-1991.

#### IEEE Std. 603-1991, Clause 5.6, "Independence"

This clause contains the requirements for physical, electrical, and communications independence. SRP Chapter 7, Appendix 7.1-C, Section 5.6, "Independence" provides acceptance criteria for system integrity.

The specific redundancy needed for an MELTAC platform-based safety system is intended to be defined at the system level during plant implementation. Therefore, the determination of independence is a plant specific activity that requires an assessment of a full system design. A platform-level assessment can only address those characteristics of the MELTAC platform that can support fulfillment of this requirement by a system design based on the platform. The platform's evaluation against this requirement is limited to consideration of the digital communications described in Section 3.2.2 and evaluated in Section 3.9.1 of this SE, because the MELTAC LTR (Ref. 14) does not address a specific application or establish a definitive safety system design. While the evaluation indicates the suitability of the platform to contribute to satisfying this requirement, a plant specific evaluation is necessary to establish full conformance with Clause 5.6 of IEEE 603-1991.

The NRC staff determined that conformance with IEEE Std. 603-1991, Clause 5.6 remains a plant specific activity that should take into consideration the full system design, use of a shared components, equipment installation, and the power distribution architecture. The digital communications evaluation in Section 3.9.1 of this SE can be used to support the independence criteria in Clause 5.6 of IEEE 603-1991.

The NRC staff's review of sub-clauses 5.6 are provided below.

#### IEEE Std. 603-1991, Clause 5.6.1, "Between Redundant Portions of a Safety System"

This clause states:

...the safety systems be designed such that there is sufficient independence between redundant portions of a safety system such that the redundant portions are independent of and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function during and following any design basis event requiring that safety function.

Specific redundancy needed for a MELTAC platform-based system will be defined at the system level during the plant specific implementation to accomplish the safety function during and following any design basis event requiring that safety function.

The MELTAC platform includes several design characteristics which can be used to support compliance with this position. Communication between redundant divisions of a MELTAC based safety system can be performed using data link communications interfaces. These interfaces are described in Section 3.2.2.2 and 3.2.2.3 and evaluated in Section 3.9.1 of this SE. The NRC staff determined that data link communications provide an acceptable means of



performing communications between redundant safety divisions while maintaining divisional communications independence.

MELTAC data communications are also performed using fiber optic isolator modules which provide electrical isolation between safety divisions for these interfaces. The NRC staff reviewed the isolation modules and determined they provide an acceptable means of establishing electrical independence between safety divisions of a MELTAC based safety system, so they can perform functions independently.

The MELTAC platform also includes isolation modules and an isolation chassis (described in Section 3.2.1.5 of this SE). These components are designed to establish physical and electrical isolation for analog signals between MELTAC safety system components and external systems such as recorders, and control room indicators that may be either safety-related or non-safety-related. The NRC staff determined that these components provide an acceptable means of establishing electrical independence between MELTAC safety system components and external systems.

Though compliance with this clause remains an application specific requirement, these design characteristics of the MELTAC platform discussed above can be used in a plant specific design to support conformance to the criteria of Clause 5.6.1 of IEEE 603 1991.

IEEE Std. 603-1991 Clause 5.6.2, "Between Safety Systems and Effects of Design Basis Event"  
This clause states:

...the safety systems required to mitigate the consequences of a specific design basis event must be independent of, and physically separated from, the effects of the design basis event to the degree necessary to retain the capability to meet the requirements of this standard. Clause 5.6.2 further states that EQ in accordance with 5.4 is one method that can be used to meet this requirement.

Determining the effects of design basis events and establishing the physical separation of the safety system from the effects of those events are plant specific activities. However, the qualification of the MELTAC platform under the generic service conditions required in EPRI TR-107330 can be used to demonstrate the capability of a safety system based on the platform to satisfy this requirement. The evaluation of the environmental qualification for the MELTAC platform is contained in Section 3.6 of this SE. This SE also identifies plant specific actions to demonstrate that the MELTAC platform performance, as bounded by its EQ, satisfies the requirements of the plant specific installation environment for the plant specific safety functions.

Based upon the installation of MELTAC platform equipment in a mild environment that is bounded by the EQ, as discussed and evaluated in Section 3.6 of this SE, the NRC staff determined that the MELTAC platform supports satisfying IEEE Std. 603-1991, Clause 5.6.2, after a referencing applicant or licensee adequately addresses the plant specific actions associated with confirming the application and installation have been bounded by the MELTAC platform EQ including each boundary/interface condition and installation limitation.

IEEE Std. 603-1991, Clause 5.6.3, "Between Safety Systems and Other Systems"

This clause states:

...the safety systems shall be designed such that credible failures in and consequential actions by other systems will not prevent the safety systems from meeting the requirements of this standard. This requirement is subdivided into requirements for interconnected equipment, equipment in proximity, and the effects of a single random failure. The three subsections below document the evaluation of interconnected equipment, equipment in proximity, and the effects of a single random failure separately.

Evaluation of this Clause requires identification of credible failures in and consequential actions by other systems as documented in the applicant's or licensee's plant specific design basis. The MELTAC platform provides digital communication design features that can support independence between an MELTAC platform-based safety system and other interfacing systems, which are discussed in Section 3.2.2 and evaluated in Section 3.9.1 of this SE. The MELTAC platform can also support communications interfaces to external equipment; however, the MELTAC LTR (Ref. 14) did not provide sufficient information for the NRC staff to review communication between 1E and non-1E systems. Therefore, demonstration that adequately qualified isolation devices are used where required should be performed as part of the plant specific application of the MELTAC platform based system.

#### IEEE Std. 603-1991, Clause 5.7, "Compatibility for Testing and Calibration"

This clause contains testing and calibration requirements. Determination of the test and calibration requirements that must be fulfilled depends upon the plant specific safety requirements (e.g., accuracy) that apply. In addition, the establishment of the types of surveillance necessary for the safety system to ensure detection of identifiable single failures that are only announced through testing is a plant specific activity.

Since the MELTAC LTR (Ref. 14) does not address a specific application or establish a definitive safety system design, the evaluation against this requirement is limited to consideration of the means provided within the platform to enable testing and calibration for a redundant portion of a safety system (i.e., channel). Section 3.7.3 of this SE discusses the MELTAC platform's self-diagnostic capabilities which can be used to support compliance with IEEE Std. 603-1991, Clause 5.7 criteria.

#### IEEE Std. 603-1991, Clause 5.10, "Repair"

This clause states that safety systems shall be designed to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment.

Several of the diagnostic features of the MELTAC platform design can be used to support compliance with this criterion. These include self-identification of faulted modules, on-line modular replacement capabilities, and internal redundancy options which can be implemented in an application specific design. The NRC staff determined the MELTAC platform design is generally capable of supporting timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment. However, some aspects of a system repair capabilities must be determined during application development and therefore compliance with this position should be confirmed during plant application development.

#### IEEE Std. 603-1991, Clause 5.15, "Reliability"

Clause 5.15 of IEEE Std. 603-1991 requires appropriate analysis of system designs to confirm that any established reliability goals, either quantitative or qualitative, have been met.

A summary of MELTAC platform reliability document (Ref. 4) was submitted to support this evaluation. The NRC staff reviewed this document and determined it contains platform reliability information that can be used to demonstrate conformance to plant specific reliability goals.

The evaluation against this requirement is limited to consideration of the reliability characteristics of the platform and its components. The NRC staffs review MELTAC platform reliability is further addressed Section 3.5.2.7 of this SE. This review identifies an activity to be performed as part of the plant specific application of the MELTAC platform.

Because plant and system specific reliability goals are not provided in the MELTAC LTR (Ref. 14) and instead must be established on a plant specific basis, the NRC staff was unable to make a safety determination for this criteria.

### 3.10.3 IEEE Std. 603-1991 Clause 6, "Sense and Command Features – Functional and Design Requirements"

The requirements of this clause, in addition to the requirements of Clause 5, apply to the sense and command features of a safety system.

The functional and design requirements for the sense and command features of a safety system are dependent solely on the specific application. Since the MELTAC LTR (Ref. 14) does not address a specific application of the platform, include the sensors, nor provide a specific safety system design, the functional and design requirements for a safety system are not available for review and no evaluation of the MELTAC platform against these regulatory requirements could be performed. Specifically, the following requirements were not evaluated:

- Clause 6.1 Automatic Control
- Clause 6.2 Manual Control
- Clause 6.3 Interaction Between Sense and Command Features and Other Systems
- Clause 6.4 Deviation of System Inputs
- Clause 6.6 Operating Bypass
- Clause 6.7 Maintenance Bypass

### IEEE Std. 603-1991, Clause 6.5, "Capability for Testing and Calibration"

Clause 6.5 of IEEE Std. 603-1991 requires that a means shall be provided for checking, with a high degree of confidence, the operational availability of each sense and command feature input sensor required for a safety function during reactor operation.

The MELTAC platform contains design features that can be implemented during application development to support a plant's methods to check operational availability of the system through the self-diagnostic and periodic testing. The NRC staffs review of these design features is provided in Section 3.7.3 of this SE. Because determination of specific input sensor requirements is application specific, the NRC staff considers this criteria to be a plant specific action.

## IEEE Std. 603-1991, Clause 6.8, "Setpoints"

This clause is related to determination of sense and command feature setpoints.

This requirement for setpoints primarily addresses factors beyond the scope of a digital platform (e.g., plant design basis limits, modes of operation, and sensor accuracy). The MELTAC LTR (Ref. 14) does not address a specific application or establish a definitive safety system, which is necessary to demonstrate the adequacy of setpoints that are associated with IEEE Std. 603-1991, Clause 4.4. Therefore, the setpoint uncertainty must be addressed in a plant specific analysis. The MELTAC platform Setpoint Methodology (Ref. 5) describes the approach to be used to prepare the setpoint analysis support documentation for MELTAC platform based digital safety systems. The NRC staff review of this approach is provided in Section 3.7.4 of this SE. The NRC staff determined the MELTAC Setpoint methodology provides an acceptable process for establishing setpoints in a MELTAC platform based safety system.

Because determination of setpoints is not performed at the generic platform level, compliance with this criteria to determine adequacy of established setpoints remains an application specific activity which must be performed during system development.

### 3.10.4 IEEE Std. 603-1991 Clause 7, "Execute Features – Functional and Design Requirements"

Section 7 of IEEE Std. 603-1991 contains five clauses that apply to execute features of safety systems. Execute features are the electrical and mechanical equipment and interconnections that perform a function, associated directly or indirectly with a safety function, upon receipt of a signal from the sense and command features. The scope of the execute features extends from the sense and command features output to and including the actuated equipment-to-process coupling.

Since the MELTAC LTR (Ref. 14) does not address a specific application of the platform, does not include the sensors, nor provide a specific safety system design, the functional and design requirements for a safety system were not available for review and no evaluation of the MELTAC platform against these regulatory requirements could be performed. Specifically, the following requirements were not evaluated:

- Clause 7.1 Automatic Control
- Clause 7.2 Manual Control
- Clause 7.3 Completion of Protective Action
- Clause 7.4 Operating Bypass
- Clause 7.5 maintenance Bypass

### 3.10.5 IEEE Std. 603-1991 Clause 8, "Power Source Requirements"

IEEE Std. 603-1991, Clause 8 states that those portions of the Class 1E power system that are required to provide the power to the many facets of the safety system are governed by the criteria of this document and are a portion of the safety systems, and that specific criteria unique to the Class 1E power systems can be found in IEEE Std. 308-1980.

Power supply requirements for the MELTAC platform are described in Section 4 of the MELTAC LTR (Ref. 14). In particular, the LTR identifies several power supply modules as qualified

platform components necessary to support system operation. The NRC staff included the MELTAC power supply modules in its analysis of platform EQ in Section 3.6 of this SE. However, determination of the power sources to be provided to a MELTAC platform based safety system is a plant specific activity and will need to be addressed during plant system development. See PSAI 5.2.13

### 3.11 Conformance with IEEE Std. 7-4.3.2-2003

RG 1.152, Revision 3 states that conformance with the requirements of IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," is a method that the NRC staff has deemed acceptable for satisfying the Commission's regulations with respect to high functional reliability and design requirements for computers used in safety systems of nuclear power plants. SRP Chapter 7, Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std. 7-4.3.2," contains guidance for the evaluation of the application of the requirements of IEEE Std. 7-4.3.2-2003.

The requirements of IEEE Std. 7-4.3.2-2003 supplement the requirements of IEEE Std. 603-1991 by specifying criteria that address hardware, software, firmware, and interfaces of computer-based safety systems. Consequently, the structure of IEEE Std. 7-4.3.2-2003 parallels that of IEEE Std. 603-1991. For those clauses where IEEE Std. 7-4.3.2-2003 contains no requirements beyond those found in IEEE Std. 603-1991 and SRP Chapter 7, Appendix 7.1-D contains no additional guidance, no review for compliance with IEEE Std. 7-4.3.2-2003 is required. Specifically, Clauses 4, 6, 7, and 8 were not reviewed. Thus, the subsections below are limited to those clauses where further evaluation is warranted. The review against the driving clauses of IEEE Std. 603-1991 is documented in Section 3.10 of this SE.

The NRC staffs evaluation of the MELTAC platform is limited to consideration of generic platform design features which do not depend on specific application development. All other aspects of IEEE 7-4.3.2 conformance are plant specific criteria which must be addressed during plant system development. See PSAI 5.2.14.

A summary of compliance with IEEE Std. 603 and IEEE Std. 7-4.3.2 (Ref. 8) was submitted to the NRC to support this evaluation. The NRC staff referred to Table 4 of Reference 8, which provided references to other supporting material during its SE. The results of this evaluation are documented as follows.

#### 3.11.1 IEEE Std. 7-4.3.2-2003, Clause 5, "Safety System Criteria"

Clause 5 of IEEE Std. 7-4.3.2-2003 contains requirements to supplement the criteria of IEEE Std. 603-1991, Clause 5. In addition, SRP Chapter 7, Appendix 7.1-D, Section 5 contains specific acceptance criteria for IEEE Std. 7-4.3.2-2003, Clause 5.

The implementation of a computer-based safety system is a plant specific activity. Since the MELTAC LTR (Ref. 14) does not address a specific application, the evaluation against the following requirements addresses the capabilities and characteristics of the MELTAC platform that are relevant for adherence to each requirement.

Note: The following clauses were not evaluated because they do not identify requirements beyond those of IEEE Std. 603-1991.

- Clause 5.2, "Completion of protective action"



- Clause 5.10, "Repair"
- Clause 5.12, "Auxiliary features"
- Clause 5.13, "Multi-unit stations"
- Clause 5.14, "Human factors consideration"

IEEE Std. 7-4.3.2-2016, Clause 5.1, "Single-failure criteria"

IEEE Std. 7-4.3.2-2003 does not include criteria beyond those identified in IEEE Std. 603-1991 for single failure criteria however, the current version of IEEE 7-4.3.2-2010 does include additional criteria. The NRC staff reviewed MELTAC platform design compliance with this criteria.

Clause 5.1 of IEEE Std. 7-4.3.2-2010 states that functions that are assumed to malfunction independently in the safety analysis shall not be affected by failure of a single programmable digital device.

Although this criteria is application specific and must be further addressed during safety system development, the NRC staff determined, based upon its evaluation of MELTAC FMEA (See Section 3.5.2.6) that a MELTAC platform based safety system has the capability of meeting this criteria, provided that functional independence characteristics are established in accordance with the system design basis requirements of IEEE 603-1991.

Clause 5.1 of IEEE Std. 7-4.3.2-2010 also states that functions shall be configured (e.g., functionally distributed) such that a single PDD malfunction or software error shall not result in spurious actuations that are not enveloped in the plant design bases, accident analyses, anticipated transient without scram (ATWS) provisions, or other provisions for abnormal conditions. This includes spurious actuation of more than one plant device or system as a result of a single PDD malfunction or software error.

Distribution of functions within a MELTAC based safety system is determined during application system development activities. The NRC staff considers a MELTAC subsystem, including a CPU processor module, to be a single programmable digital device for the purposes of this criteria. As such, allocation of safety functions to a single MELTAC subsystem should consider plant design bases, accident analyses, and ATWS provisions when performing these activities. This criteria is application specific and must be addressed during safety system development. IEEE Std. 7-4.3.2-2003, Clause 5.3, "Quality"

Clause 5.3 of IEEE Std. 7-4.3.2-2003 states that hardware quality is addressed in IEEE Std. 603-1998, and that software quality is addressed in IEEE/Electronic Industries Association (EIA) Std. 12207.0-1996 and supporting standards. Clause 5.3 further requires that the digital computer development process include the development activities for both computer hardware and software, the integration of the hardware and software, and the integration of the computer with the safety system. Clause 5.3 includes six sub-clauses to identify activities beyond the requirements of IEEE Std. 603-1991 that are necessary to meet quality criterion for digital computer-based systems including its software. Each sub-clause under Clause 5.3 addresses one of these six activities.

The MELTAC platform was originally developed for non-safety-related applications in compliance with the Japanese Electrical Association Guide (JEAG)-4101 and International Organization for Standardization (ISO)-9001. Subsequent to its development, MELCO

performed a commercial grade dedication of the MELTAC platform to qualify it for use in safety-related applications for U.S. Nuclear Power Plants. To support this SE, MELCO submitted a summary of MELTAC platform quality assurance document (Ref. 5). This document describes the MELCO QA processes and documentation requirements for MELTAC platform and application development activities.

The nuclear QA program employed for MELTAC is compliant with 10 CFR Part 50, Appendix B. All MELTAC platform hardware and software development and maintenance activities are governed by the MELCO 10 CFR 50, Appendix B QA program as defined in the Quality Manual, and as supplemented by the summary of MELTAC platform quality assurance document (Ref. 5).

Activities for development of MELTAC based I&C systems for US nuclear power plants will be performed under the 10 CFR Part 50, Appendix B-compliant QA program documented in the "Instrumentation & Controls U.S. Quality Manual" (Ref. 18). However, evaluation of development process implementation, including system integration activities used for plant application software, must be evaluated for compliance with Clause 5.3 criteria during plant application development.

#### IEEE Std. 7-4.3.2-2003, Clause 5.3.1, "Software Development"

Clause 5.3.1 of IEEE Std. 7-4.3.2-2003 requires an approved software QA plan consistent with the requirements of IEEE/EIA 12207.0-1996 for all software that is resident at runtime. EPRI TR-106439, as accepted by the NRC SE dated July 17, 1997, and EPRI TR-107330, as accepted by the NRC SE dated July 30, 1998, provide guidance for the evaluation of existing commercial computers and software.

The MELTAC software development processes are evaluated in Section 3.5 of this SE. The MELTAC MRP, which was based upon the commercial grade dedication process defined in 10 CFR 21, ensured the MELTAC platform has the technical critical characteristics and level of quality consistent with a product developed under a 10 CFR 50, Appendix B program. Software quality planning for the MELTAC basic software is evaluated in Section 3.5.1.3 of this SE, and it was determined by the NRC staff to be acceptable for use in nuclear safety applications however, plant application software QA planning activities must be performed in conjunction with application development activities.

#### IEEE Std. 7-4.3.2-2003, Clause 5.3.1.1, "Software Quality Metrics"

Clause 5.3.1.1 of IEEE Std. 7-4.3.2-2003 states that the use of software quality metrics shall be considered throughout the software life cycle to assess whether software quality requirements are being met.

Since the MELTAC basic software was dedicated rather than developed under the current MELCO software QA program, this requirement does not apply within the context of the original development activities for the generic MELTAC platform. Activities performed after the commercial grade dedication of the MELTAC platform are subject to the established 10 CFR 50, Appendix B compliant QA program and the MELTAC software quality assurance Plan. Section 3.3 of the MELTAC SPM (Ref. 2) is the MELTAC basic SQAP, which includes processes for tracking QA audit findings and process related metrics during platform software development activities. Software process quality metrics include: number of comments

identified during design reviews, numbers and severity levels of V&V anomaly reports, numbers of nonconformance reports, and numbers of corrective action reports.

The NRC staff determined quality metrics have been considered throughout the MELTAC basic software life cycle to assess whether software quality requirements are met. It is noted that the responsibilities for the QA manager to develop measurable data relating to the effectiveness of the MELCO software QA program should be included in plant-specific software QA plan. An evaluation of metric usage for the application software development must be conducted during plant specific application development for any system based on the MELTAC platform.

IEEE Std. 7-4.3.2-2003, Clause 5.3.2, "Software tools"

Clause 5.3.2 of IEEE Std. 7-4.3.2-2003 states that software tools used to support software development processes and V&V processes shall be controlled under configuration management, and that the tools shall either be developed to a similar standard as the safety-related software, or that the software tool shall be used in a manner such that defects not detected by the software tool will be detected by V&V activities.

The MELTAC platform software tools used to support MELTAC basic software development are used in a manner such that defects not detected by the software tool will be detected and corrected by verification and validation activities described in the MELTAC V&V Plan (Section 3.10 of the MELTAC platform SPM, Ref. 2). Software tools used for MELTAC basic software development were not themselves developed in accordance with the MELTAC 10 CFR 50, Appendix B compliant QA programs and are thus not classified as safety-related.

One function of the MELTAC engineering tool, the memory integrity checking function, is developed to the MELCO 10 CFR 50, Appendix B quality assurance program and is therefore compliant with the criteria of IEEE 7-4.3.2 Clause 5.3.2.a.

MELCO provided a MELTAC platform software tools document (Ref. 6) to support the NRCs evaluation of this criteria. This document lists and describes all software tools used during MELTAC basic software development and includes discussion of how each software tool is used. The NRC staff reviewed the MELTAC platform software tools document and confirmed these tools are used in a manner which is consistent with the criteria of IEEE 7-4.3.2, Clause 5.3.2. The NRC staff also confirmed that software tools used for MELTAC basic software development are controlled under the MELCO configuration management program. The NRC staff could not evaluate the use of software tools used for plant application development during this SE. The use and control of application software development tools must be addressed during application development.

IEEE Std. 7-4.3.2-2003, Clause 5.3.3, "Verification and Validation"

Clause 5.3.3 of IEEE Std. 7-4.3.2-2003 states that a V&V program exists throughout the system life cycle, and states that the software V&V effort be performed in accordance with IEEE Std. 1012-1998.

The NRC evaluated the MELTAC V&V program and determined it to be compliant with the criteria of IEEE 1012-2004 which is endorsed by RG 1.168. Details of this evaluation are provided in Section 3.5.1.6 of this SE.

IEEE Std. 7-4.3.2-2003, Clause 5.3.4, "Independent V&V Requirements"

Clause 5.3.4 of IEEE Std. 7-4.3.2-2003 defines the levels of independence required for the V&V effort, in terms of technical independence, managerial independence, and financial independence. This clause also requires development activities to be verified and validated by individuals or groups with appropriate technical competence who are also different than the individuals or groups who performed the development activities.

The NRC staffs evaluation (in Section 3.5.1.6 of this SE) of the MELTAC V&V processes included an assessment of the type and level of independence maintained between the design team and the V&V team at MELCO. The NRC staff determined that MELCO's V&V team is acceptably independent from the organizations performing design activities. The V&V team does not report to members of the design team and therefore managerial independence is established. The V&V team is not subject to the same budget constraints as is the design team and therefore financial independence is established. The V&V team members are trained and qualified to levels comparable to members of the design team and therefore technical competence of the V&V team is maintained and technical independence is established. The MELTAC V&V processes therefore comply with the criteria of Clause 5.3.4.

#### IEEE Std. 7-4.3.2-2003, Clause 5.3.5, "Software Configuration Management"

Clause 5.3.5 of IEEE Std. 7-4.3.2-2003 states that SCM shall be performed in accordance with IEEE Std. 1042-1987, and that IEEE Std. 828-1998 provides guidance for the development of software configuration management plans. IEEE Std. 828-2005 and IEEE Std. 1042-1987 are endorsed by RG 1.169.

The NRC staff evaluated the MELTAC Configuration Management program and determined it to be compliant with the criteria of IEEE 1042-1987, IEEE Std. 828-2005, and IEEE Std. 1042-1987 as endorsed by RG 1.169. Details of this evaluation are provided in Section 3.5.1.7 of this SE. The NRC staff also confirmed that MELCO configuration management program includes all of the minimum required activities listed in Clause 5.3.5 of IEEE Std. 7-4.3.2-2003.

#### IEEE Std. 7-4.3.2-2003, Clause 5.3.6, "Software Project Risk Management"

Clause 5.3.6 of IEEE Std. 7-4.3.2-2003 defines the risk management (RM) required for a software project. SRP Chapter 7, Appendix 7.1-D, Section 5.3.6, "Software Project Risk Management" provides acceptance criteria for software project risk management. This clause states that software project risk management is a tool for problem prevention, and will be performed at all levels of the digital system project to provide adequate coverage for each potential problem area. It also states that software project risks may include technical, schedule, or resource related risks that could compromise software quality goals, and thereby affect the ability of the safety computer system to perform safety-related functions. Additional guidance on the topic of risk management is provided in IEEE/EIA Std. 12207.0-1996, "IEEE Standard for Industry Implementation of International Standard ISO/IEC 12207: 1995 (ISO/IEC 12207) Standard for Information Technology – Software Life Cycle Processes," and IEEE Std. 1540-2001, "IEEE Standard for Life Cycle Processes B Risk Management."

The MELTAC SMP (Section 3.1 of the SPM Reference 2) includes a process for developing and maintaining a project risk matrix. Potential risks identified during any phase of the MELTAC development lifecycle process are entered into this matrix and methods of addressing and mitigating these risks are then implemented. The SMP describes risk areas to be included in

the risk matrix and provides guidance for identifying and addressing risk items that become issues to be corrected.

The MELTAC SQAP also describes several activities that can be used to identify project risks during MELTAC development. The MELTAC quality assurance process includes methods of identifying and addressing product quality issues during development as well as processes for escalating issues that pose risks to software quality or safety goals.

The NRC staff determined that risk management has been acceptably implemented within the MELTAC SPM as a tool for problem prevention. Risk management is performed at all levels of the MELTAC system project development process and the risk management processes provide adequate coverage for potential MELTAC platform software problem areas. MELTAC software project risks include technical, schedule, and resource related risks that could compromise software quality goals, or affect the ability of the MELTAC safety system to perform safety-related functions. Risk management activities associated with application software development were not evaluated as part of this SE. See PSAI 5.2.14.

#### IEEE Std. 7-4.3.2-2003, Clause 5.4, "Equipment Qualification"

Clause 5.4 of IEEE Std. 7-4.3.2-2003 defines the computer EQ required for a software project. SRP Chapter 7, Appendix 7.1-D, Section 5.4, "Equipment Qualification," provides acceptance criteria for computer EQ. This SE of Appendix 7.1-D states that in addition to the EQ criteria provided by IEEE Std. 603-1991 and Section 5.4 of SRP Chapter 7, Appendix 7.1-C, additional criteria, as defined in Sections 5.4.1 and 5.4.2, are necessary to qualify digital computers for use in safety systems. These sections are discussed below.

#### IEEE Std. 7-4.3.2-2003, Clause 5.4.1, "Computer System Testing"

Clause 5.4.1 of IEEE Std. 7-4.3.2-2003 discusses the software that should be operational on the computer system while qualification testing is being performed. SRP Chapter 7, Appendix 7.1-D, Section 5.4.1, "Computer System Testing," provides acceptance criteria for computer EQ testing. This SE states that computer EQ testing should be performed while the computer is functioning, with software and diagnostics that are representative of those used in actual operation.

Section 3.6 of this SE discusses the evaluation of the EQ program for the MELTAC platform. MELCO complied with the guidance of EPRI TR-107330 for the generic qualification of a PLC platform. EQ testing of the MELTAC representative system was performed while the test system CPU's were functioning. Test application software and diagnostics functions as described in Sections 4.1.5 and 4.2.3 of the MELTAC LTR (Ref. 14) representative of those to be used in actual operation were in operation during EQ testing.

The Test application software was specifically designed to support qualification testing of the MELCO platform while providing generic functionality of the test system. Based on the evaluation in Section 3.6 of this SE and review of the summary of MELTAC platform EQ report (Ref. 29), the NRC staff concludes that the MELTAC qualification program met the requirement for computer testing of the MELTAC platform, subject to satisfactory resolution of the PSAI in Section 5.2 of this SE.



IEEE Std. 7-4.3.2-2003, Clause 5.4.2, "Qualification of Existing Commercial Computers"

Clause 5.4.2 of IEEE Std. 7-4.3.2-2003 defines the Qualification of Existing Commercial Computers for use in safety-related applications in nuclear power plants. SRP Chapter 7, Appendix 7.1-D, Section 5.4.2, "Qualification of Existing Commercial Computers," provides acceptance criteria for computer EQ. This SE states that EPRI TR-106439 and EPRI TR-107330 provide specific guidance for the evaluation of commercial grade digital equipment and existing PLCs.

As part of the MELTAC re-evaluation program, MELCO commercially dedicated the pre-developed operating software of the MELTAC platform under the guidance of EPRI TR-106439 and generically qualified the MELTAC platform in accordance with the guidance of EPRI TR-107330.

In Section 3.4 of this SE, the NRC staff determined the generic qualification of the MELTAC platform performed during MELTAC re-evaluation dedication complies with the guidance of both EPRI TR-106430 and EPRI TR-107330.

IEEE Std. 7-4.3.2-2003, Clause 5.4.2.1, "Preliminary Phase of the COTS Dedication Process"

This clause of IEEE Std. 7-4.3.2-2003 specifies that the risks and hazards of the dedication process are to be evaluated, the safety functions identified, configuration management established, and the safety category of the system determined.

Risks and hazards associated with MELTAC based systems have been addressed within the platform development processes as described in the evaluation for clause 5.3.6. Risk management is performed at all levels of the MELTAC system project development process and the risk management processes provide adequate coverage for potential MELTAC platform software and hardware problem areas. The NRC staff determined that risk management has been adequately implemented within the MELTAC SPM as a tool for problem prevention.

IEEE Std. 7-4.3.2-2003, Clause 5.4.2.2, "Detailed Phase of the COTS Dedication Process"

This clause of IEEE Std. 7-4.3.2-2003 involves evaluation of the commercial grade item for acceptability based on detailed acceptance criteria. In particular, critical characteristics of the commercial off the shelf (COTS) item are to be evaluated and verified. The characteristics are identified in terms of physical, performance, and development process attributes. This requirement is addressed by the guidance in EPRI TR-106439. Specifically, a critical design review is specified to identify physical, performance, and dependability (i.e., development process) characteristics, which are then verified by one or more of the four methods identified in the guide.

Upon completion of the one-time MELTAC re-evaluation, MELTAC platform components are considered to be qualified for nuclear safety applications. Platform component changes or new product development activities including plant application development activities are governed by the MELCO 10 CFR 50, Appendix B QA processes and the platform development processes evaluated in this SE (see section 3.5 of this SE). Therefore, MELTAC platform components with the exception of MELTAC commercially dedicated components listed below are not considered to be COTS components and these components do not need to be dedicated as commercial grade components.

MELCO provided a summary of MELTAC platform commercial grade dedication activity (Ref. 24) to support this evaluation. The NRC staff reviewed this report and determined the commercial grade dedication activities were performed in accordance with the criteria of EPRI TR-106439 and are therefore acceptable.

The only components of the MELTAC platform that are commercially dedicated and maintained are power supply modules (PPSJ, & PS), termination units (PSND), and S-RMS DC power supply units (501AJOUR). All other components are designed and developed as safety-related components under the MELCO 10 CFR 50, Appendix B QA program and are to be developed and maintained in accordance with the MELTAC SPM.

The characteristics for each commercial grade dedication component of the MELTAC platform are identified in terms of physical, performance, and development process attributes. A critical design review is performed to identify physical, performance, and dependability characteristics, and these characteristics are verified using acceptable methods.

IEEE Std. 7-4.3.2-2003, Clause 5.4.2.3, "Maintenance of Commercial Dedication"

This clause of IEEE Std. 7-4.3.2-2003 specifies that documentation supporting commercial grade dedication of a computer-based system or equipment is to be maintained as a configuration control item. In addition, modifications to dedicated computer hardware, software, or firmware are to be traceable through formal documentation.

The only components of the MELTAC platform that are commercially dedicated and maintained are power supply modules (PPSJ, & PS), termination units (PSND), and S-RMS DC power supply units (501AJOUR). All other components are designed and developed as safety-related components under the MELCO 10 CFR 50, Appendix B QA program and are to be developed and maintained in accordance with the MELTAC SPM.

The NRC staff reviewed the summary of MELTAC platform commercial grade dedication Activity document and determined that documentation supporting commercial grade dedication of these components is maintained as a configuration control item. Modifications to dedicated MELTAC commercial grade dedication components are traceable through formal QA documentation. The processes used to dedicate and maintain MELTAC commercial grade dedication components therefore conform to Clause 5.4.2.3 of IEEE Std. 7-4.3.2.

IEEE Std. 7-4.3.2-2003, Clause 5.5, "System Integrity"

Clause 5.5 of IEEE Std. 7-4.3.2-2003 states that in addition to the system integrity criteria provided by IEEE Std. 603-1991, the digital system shall be designed for computer integrity, test and calibration, and fault detection and self-diagnostics activities. These attributes are further defined in Clause 5.5.1, "Design for Computer Integrity," Clause 5.5.2, "Design for Test And Calibration," and Clause 5.5.3, "Fault Detection And Self-diagnostics." There are no specific acceptance criteria shown in SRP Chapter 7, Appendix 7.1-D, Section 5.5, "System Integrity."

IEEE Std. 7-4.3.2-2003, Clause 5.5.1, "Design for Computer Integrity."

Clause 5.5.1 of IEEE Std. 7-4.3.2-2003 states that the computer must be designed to perform its safety function when subjected to conditions, either external or internal, that have significant potential for defeating the safety function.

The MELTAC platform includes features to provide fault tolerant capabilities. In addition, the MELTAC platform includes diagnostics and self-testing (see Section 3.7.3) that can facilitate a high-level of computer integrity. However, MELCO did not define a system architecture or application for the MELTAC platform. Instead, MELCO defined a generic platform that can be used in a wide range of applications or configurations. Therefore, the NRC staff only evaluated the features (described in Section 4.2.3 of the MELTAC LTR) provided in the generic platform. This evaluation can be used to support development of future plant specific applications.

The MELTAC platform qualification activities discussed in Section 3.6 of this SE, provide suitable evidence that the MELTAC platform is capable of maintaining plant safety when subjected to environmental conditions, external or internal, that have the potential to defeat implemented safety functions.

Based on the information provided, the NRC staff determined that features provided on the MELTAC platform can support systems performing safety functions in a reliable manner. However, determination of compliance with this criterion requires a PSAI to address system integrity for a plant specific application (see Section 5.2.3).

IEEE Std. 7-4.3.2-2003, Clause 5.5.2, "Design for Test and Calibration"

Clause 5.5.2 of IEEE Std. 7-4.3.2-2003 states that test and calibration functions shall not adversely affect the ability of the computer to perform its safety function, and that it shall be verified that the test and calibration functions do not affect computer functions that are not included in a calibration change. The clause further states that V&V, configuration management, and QA be required for test and calibration functions on separate computers such as test and calibration computers that provide the sole verification of test and calibration data, but that V&V, configuration management, and QA is not required when the test and calibration function is resident on a separate computer and does not provide the sole verification of test and calibration data for the computer that is part of the safety system.

Online self-diagnosis functions are provided in the MELTAC platform to support test and calibration requirements in general. These are described in Sections 4.1.5 and 4.2.3 of the MELTAC LTR (Ref. 14). Qualification tests performed for the MELTAC platform were conducted with self-diagnosis functions operating in conjunction with the test application performing basic functions. The performance of the MELTAC equipment during these tests demonstrated that diagnosis features did not adversely affect the ability of the system to perform its simulated functions (Ref. 31). Therefore, the NRC staff determined the diagnosis capabilities provided by the MELTAC platform conform to this requirement.

Maintenance activities performed on a MELTAC based safety system, including periodic surveillance testing, will be defined based on the plant specific system requirements. Determination of test and calibration requirements and establishment of surveillance necessary to ensure that the identifiable single failures are detected are plant specific activities (see Section 5.2.10 of this SE).

IEEE Std. 7-4.3.2-2003, Clause 5.5.3, "Fault Detection and self-diagnostics"

Clause 5.5.3 of IEEE Std. 7-4.3.2-2003 discusses fault detection and self-diagnostics, and states that if reliability requirements warrant self-diagnostics, then computer programs should contain functions to detect and report computer system faults and failures in a timely manner,

and that these self-diagnostic functions shall not adversely affect the ability of the computer system to perform its safety function, or cause spurious actuations of the safety function. Section 3.7.3 of this SE provides an evaluation of the MELTAC diagnostics and self-test capabilities. These tests and diagnostics provide functions to detect failures in the system hardware, as well as to detect system failure modes identified in the MELTAC failure modes and effects analysis (FMEA). See Section 3.5.2.6 of this SE for more information on the MELTAC FMEA.

If errors are encountered during system operation, self-diagnosis features will respond by either providing an alarm or by setting output signals to pre-defined states depending on the severity of the fault identified. Predefined states are to be defined during plant system development and application specific failure analysis should be performed for each plant specific application. Based on this information, the NRC staff determined that hardware and software based diagnostic features of the MELTAC platform provide an acceptable method of detecting and reporting computer system faults and failures in a timely manner. The MELTAC platform is therefore acceptable for providing fault detection in support of safety-related applications.

However, because MELCO did not define the actions to be taken when faults are detected, and did not identify specific self-tests or periodic surveillance testing necessary to detect and address the effects of system failures on plant safety, there may be additional fault-detection and diagnostic function requirements to provide more comprehensive coverage of identified system failures. Therefore, a plant specific evaluation is necessary to establish full conformance with Clause 5.5.3 (see Section 5.2.14 of this SE).

IEEE Std. 7-4.3.2-2003, Clause 5.6, "Independence"

Clause 5.6 of IEEE Std. 7-4.3.2-2003 states that, in addition to the requirements of IEEE Std. 603-1991, data communications between safety channels or between safety and non-safety systems shall not inhibit the performance of the safety function. SRP Chapter 7, Appendix 7.1-D, Section 5.6, "Independence," provides acceptance criteria for independence. This guidance states that the regulation at 10 CFR Part 50, Appendix A, GDC 24, "Separation of Protection And Control Systems," requires the protection system be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel that is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system, and that interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.

Establishment of communications among redundant portions of a safety system or between the safety system and other non-safety-related systems is a plant specific activity. The base platform architecture identified in the MELTAC LTR (Ref. 14) does not specify any direct connections or bi-directional communications between a MELTAC platform based safety system and any other system. Since the MELTAC LTR does not address a specific application or provide a definitive safety system design, the evaluation of the MELTAC platform against the communications independence aspect of this criteria is limited to features and capabilities of its communication interfaces. Section 3.2.2 of this SE describes communication interfaces within the scope of the MELTAC platform. Section 3.9.1 contains an evaluation of the MELTAC communications capabilities with respect to the guidance in DI&C-ISG-04.

Based on the evaluation described in this SE, the NRC staff finds that the communications capabilities of the MELTAC platform provide acceptable design features to enable communications independence when appropriately configured. However, the specific interconnections defined for an application must be determined and addressed during plant application development. See Section 5.2.14 of this SE for PSAIs.

IEEE Std. 7-4.3.2-2016, Clause 5.7, "Capability for Test and Calibration"

Clause 5.7 of IEEE Std. 7-4.3.2-2003 states that there are no requirements beyond those found in IEEE Std. 603-1991. SRP Chapter 7, Appendix 7.1-D, Section 5.7, "Capability for Test and Calibration," provides guidance for evaluating and determining acceptability of test and diagnostic software. It states that the reviewer should carefully examine the capability of the software to test itself. It includes guidance on comparing the relative complexity between diagnostics software and operational software and promotes a balance between added complexity of diagnostics and the gain of confidence in the system.

The 2016 version of IEEE 7-4.3.2 provides additional criteria to be considered. Clause 5.7 of IEEE Std. 7-4.3.2-2016 states that safety system configuration shall not require change or modification to support periodic automated or manual surveillance testing. It also states that measurement and test equipment (M&TE) used for safety systems shall not adversely affect the safety system functionality and that wireless receivers/transmitters on temporarily-connected measurement and test equipment shall be disabled prior to connecting to safety-related equipment.

The NRC staff evaluated the MELTAC self-diagnostic features for compliance with these criteria. The MELTAC platform design includes self-diagnostic features to detect failures within the MELTAC based safety system during operation. The use of wireless receivers/transmitters on temporarily-connected measurement and test equipment is not discussed in the MELTAC LTR (Ref. 14) and is therefore not evaluated or approved for use by the NRC staff. There are also no requirements for MELTAC based safety system configuration changes to support periodic automated or manual surveillance testing. Use of surveillance testing is application specific.

The NRC staff reviewed the diagnostics functions of the MELTAC platform and determined the level of complexity introduced to the MELTAC system by the diagnostic features described in Section 4.15 of the MELTAC LTR (Ref. 14) was commensurate with the safety functions to be performed and the benefits provided by these features justify their inclusion into the MELTAC platform design. The NRC staff finds that the MELTAC platform complies with the criteria of this clause.

IEEE Std. 7-4.3.2-2016, Clause 5.8, "Information Displays"

Clause 5.8 of IEEE Std. 7-4.3.2-2003 states that there are no requirements beyond those found in IEEE Std. 603-1991. However, SRP Chapter 7, Appendix 7.1-D, Section 5.8, "Information Displays," notes that, in the past, information displays only provided a display function and, therefore, required no two way communication. More modern display systems may also have included control functions and, therefore, the NRC staff reviews the capacity for information displays to ensure that incorrect functioning of the information displays does not prevent the safety function from being performed when necessary.



The 2016 version of IEEE 7-4.3.2 provides additional criteria to be considered. Clause 5.8 of IEEE Std. 7-4.3.2-2016 states that safety-related controls and indications shall be dedicated to specific safety divisions.

The MELTAC platform includes an S-VDU system which is described in Section 3.2.1.6 of this SE. The MELTAC S-VDU system components are designed and developed in accordance with the MELCO 10 CFR 50, Appendix B QA processes and are qualified to be used as safety-related components. The S-VDU system processors communicate with the MELTAC CPU modules through the MELTAC control network. The control network, described in Section 3.2.2.1 of this SE, is an intra-divisional network, which is not intended to support communications between different safety divisions. Isolation between the control networks in different safety divisions is established and maintained by not allowing interconnection of network interfaces across safety division barriers. Additionally, as stated in the MELTAC LTR (Ref. 14), "Each S-VDU can be configured to provide the human system interface for only one safety division." The NRC staff determined that as long as the design principles for isolation prescribed in Section 4.3.2.3 and in Section 4.2 of the MELTAC LTR are followed, the criteria of IEEE 7-4.3.2, Clause 5.8 are met. PSAI 5.2.17 is included to ensure that plant specific application does not introduce functional dependency between the system safety functions and the S-VDUs of the system.

#### IEEE Std. 7-4.3.2-2016, Clause 5.9, "Control of Access"

Clause 5.9 of IEEE Std. 7-4.3.2-2003 states that there are no requirements beyond those found in IEEE Std. 603-1991. For this reason, there is no additional guidance beyond that found in Section 5.9 of SRP Chapter 7, Appendix 7.1-C and RG 1.152, Revision 2.

The 2016 version of IEEE 7-4.3.2 does provide additional criteria to be considered however, this criteria is currently not endorsed by the NRC and is instead addressed by the criteria of RG 1.152, Revision 3.

The regulatory position section in RG 1.152, Revision 3, provides guidance on security regarding electronic access to a safety system. SRP acceptance criteria for this guidance can be found in SRP Chapter 7, Appendix 7.1-D, Section 9. The evaluation of the MELTAC platform against this guidance is contained in Section 3.12 of this SE.

#### IEEE Std. 7-4.3.2-2003, Clause 5.11, "Identification"

Clause 5.11 of IEEE Std. 7-4.3.2-2003 states that (1) identification requirements specific to software systems (i.e., firmware and software identification) shall be used to assure the correct software is installed in the correct hardware component, (2) means shall be included in the software such that the identification may be retrieved from the firmware using software maintenance tools, and (3) physical identification requirements of the digital computer system hardware shall be in accordance with the identification requirements in IEEE Std. 603-1991, Clause 5.11. SRP Chapter 7, Appendix 7.1-D, Section 5.11, "Identification" provides acceptance criteria and adds that the identification should be clear and unambiguous. The identification should include the revision level, and should be traceable to configuration control documentation that identifies the changes made by that revision for computer EQ.

Establishing software/firmware identification requirements and providing the means for retrieving that identification information are part of the MELCO QA Program. Section 3.5.1.7 of this SE contains the evaluation of the MELTAC SCMP as it applies to maintaining the

configuration of MELTAC basic software. The SCMP for MELTAC application software is outside of the scope of this review, and it should be evaluated for a plant specific configuration. Identification requirements specific to MELTAC basic software are used to assure the correct basic software is installed in the correct MELTAC hardware components. Identification of installed software can be performed using the MELTAC engineering tool. Physical identification of the MELTAC hardware modules was performed by MELCO by using the MELTAC engineering tool in accordance with the identification requirements in IEEE Std. 603-1991, Clause 5.11.

MELTAC configuration items are managed and controlled in accordance with the MELTAC software configuration management plan. Software version management and change control mechanisms are applied to all configuration items. The configuration information of each hardware and software component of a MELTAC based safety system is securely maintained as MELCO system configuration management records. Software versions for the assemblage of software components are defined in terms of a formally released, configuration controlled software project configuration management records.

Based on the process observed during the regulatory audit for MELTAC software identification, and configuration management records reviewed during the audit, the NRC staff determined the MELTAC platform complies with the guidance of IEEE Std. 7-4.3.2-2003, Clause 5.11 for its basic software. However, assurance that proper hardware and plant application software configuration is established and maintained is an activity that must be performed during plant application development and implementation. See Section 5.2.14 of this SE for PSAIs.

IEEE Std. 7-4.3.2-2003, Clause 5.15, "Reliability"

Clause 5.15 of IEEE Std. 7-4.3.2-2003 states that, in addition to the requirements of IEEE Std. 603-1991, when reliability goals are identified, the proof of meeting the goals shall include the software. Guidance is provided in SRP Chapter 7, Appendix 7.1-C, Section 5.15.

As stated in RG 1.152, Revision 2, the NRC staff does not endorse the concept of quantitative reliability goals as the sole means of meeting the Commission's regulations for reliability of digital computers in safety systems. Quantitative reliability determination, using a combination of analysis, testing, and operating experience, can provide an added level of confidence in the reliable performance of the computer system.

Determination of the reliability requirements for a digital safety system is a plant specific activity that requires an assessment of a full system design, including its application, system basic software, and the software life cycle processes. Since the MELTAC LTR (Ref. 14) does not address a specific plant application, nor establish a specific safety system design, the evaluation against this requirement is limited to consideration of the reliability characteristics of the MELTAC digital platform and the quality of its system basic software. Section 3.5.2.7 of this SE includes the NRC staffs assessment and evaluation of MELTAC reliability characteristics. While the evaluation indicates the platform satisfies this requirement, a plant specific evaluation of MELTAC reliability against specific plant system reliability requirements is necessary to establish full conformance with Clause 5.15. See Section 5.2.14 of this SE for PSAIs.

### 3.12 Secure Development and Operational Environment

RG 1.152, Revision 3, describes a method that the NRC considers acceptable to comply with the regulatory criteria to promote high functional reliability, design quality, and establish secure

development and operational environments for the use of digital computers in safety-related systems at nuclear power plants. The guidance for secure development and operational environments states that potential vulnerabilities should be addressed in each phase of the digital safety system life-cycle. The overall guidance provides the basis for physical and logical access controls to be established throughout the digital system development process to address the susceptibility of a digital safety system to inadvertent access and modification.

A secure development environment must be established to ensure that unneeded, unwanted and undocumented code is not introduced into a digital safety system. A secure development environment must be established to also protect against unwanted and unauthorized access or changes to the system. The MELTAC platform was originally developed under a Japanese nuclear quality program, and was not intended to conform to RG 1.152. However, the MELTAC platform was developed for nuclear power plant applications, including safety-related systems, and it included security features to prevent the effects of inadvertent access during development and operation. When the MRP (see Section 3.4 of this SE) was later conducted, the security features of the MELTAC legacy development process were assessed. This assessment encompassed compliance to RG 1.152, Revision 2, which was the latest revision at the time. The MRP assessment confirmed that (1) that the MELTAC security features were adequate to protect the safety functions of the MELTAC platform, (2) that those features were reflected in actual MELTAC documentation and (3) that those features were developed with adequate quality assurance.

Regulatory positions 2.1 – 2.5 of RG 1.152, Revision 3, identify controls that an applicant should implement during the development activities for safety-related digital systems. Sections 4.5 and 6.1.2 of the MELTAC LTR (Ref. 14) and Section 3 of the MELTAC platform SPM describe security measures taken during development of MELTAC basic software. Section 3 of the MELTAC platform application SPM describe security measures to be taken during development of MELTAC application software. A summary of the MELTAC platform conformance with RG 1.152, Revision 3 (Ref. 36) was also submitted to the NRC as supplemental information to support this evaluation. The results of this evaluation are documented as follows.

#### 3.12.1 RG 1.152, Revision 3, Regulatory Position 2.1, "Concepts Phase" Identification and Description of Secure Operational Environment Design Features

Regulatory Position 2.1 states that digital safety system design features required to establish a secure operational environment for the system should be identified, and described as part of the application.

Evaluation of a safety system against this part of the regulatory position is a plant specific activity that requires an assessment of a completed system design. The MELTAC platform design partially addresses this part of the regulatory position by incorporating design features within the platform to address a secure operational environment. These features include:

- (1) the write permission switch and dedicated reprogramming chassis to prevent unintended rewriting of the application software
- (2) the capability to implement MCR alarms for an open cabinet door, and for when the CPU power source is turned off
- (3) physical one-way communication function (data link) to avoid remote access when connecting between systems
- (4) a self-diagnostic function for detecting system abnormalities

The NRC staff finds that these secure operational environment features can be used to support a plant specific application of the MELTAC platform. Because determination of a secure operational environment is a plant specific activity, the NRC staff considers this criteria to be a plant specific action (see PSAI 5.2.15).

#### Assessment of Potential Susceptibilities

Regulatory Position 2.1 states that 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 should be assessed. 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.

Evaluation of a safety system against this part of the regulatory position is a plant specific activity that requires an assessment of the application-specific vulnerabilities.

MELCO partially addresses this part of the regulatory position by performing a vulnerability assessment of the MELTAC platform (Ref. 36). This assessment identifies the MELTAC platform development assets, vulnerabilities and secure controls to determine the risk of unwanted, unneeded and undocumented functionality being introduced during development or modification. MELCO also addressed the susceptibility to inadvertent access and undesirable behavior from connected systems by performing a hazard analysis.

The NRC staff finds that the MELTAC platform vulnerability assessment can be used to support the development of an application specific vulnerability assessment. Because evaluation of an application specific vulnerability assessment is a plant specific activity, the NRC staff considers this criteria to be a plant specific action (see PSAI 5.2.15).

#### Remote Access

Regulatory Position 2.1 states that remote access to the safety system should not be allowed. In RG 1.152, 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).

Evaluation of a safety system against this part of the regulatory position is a plant specific activity that requires an assessment of a completed system design. The MELTAC platform design partially addresses this part of the regulatory position by incorporating the data link (see Section 3.2.2.2) as a physical one-way communication to avoid remote access when connecting between systems.

The NRC staff finds the MELTAC platform's use of the data link as a secure operational environment feature can be used to support the plant specific application of the MELTAC platform. Because determination of a secure operational environment is a plant specific activity, the NRC staff considers this criteria to be a plant specific action (see PSAI 5.2.15).

#### 3.12.2 RG 1.152, Revision 3, Regulatory Position 2.2, "Requirements Phase" Definition of Secure Operational Environment functional Requirements

Regulatory Position 2.2 states that 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 should be defined. The design feature requirements intended to maintain a secure operating environment and ensure reliable system operation should be part of the overall system requirements.

The compliance of a safety system with this part of the regulatory position was not evaluated because it is a plant specific activity that requires an assessment of the safety system design (see PSAI 5.2.16).

#### Verification of Secure Development and Operational Environment Requirements

Regulatory Position 2.2 states that the verification process of the requirements phase should ensure the correctness, completeness, accuracy, testability, and consistency of the system's secure development and operational environment (SDOE) feature.

The compliance of a safety system with this part of the regulatory position was not evaluated because it is a plant specific activity that requires an assessment of the safety system design (see PSAI 5.2.16).

#### Use of Predeveloped Software and Systems

Regulatory Position 2.2 states that the requirements specifying the use of pre-developed software and systems (e.g., reused software and 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).

The MELTAC platform design addresses this part of the regulatory position because the platform and the MELTAC engineering tool are developed and maintained by MELCO exclusively for nuclear applications. MELCO does not use commercial off-the-shelf software in its MELTAC safety system.

Independent V&V is applied to the basic software configuration items, as described in the SVVP and in Section 3.5.1.6 of this SE. However, qualification and independent V&V is not applied to software tools. The software tools described in the SMP are maintained under configuration control as described within this SCMP. See Section 3.11.1 of this SE for the evaluation against the criteria of IEEE Std. 7-4.3.2-2003, Clause 5.3.2, "Software tools."

The NRC staff finds that the MELTAC platform was not developed from pre-developed systems, or using pre-developed software functions, and therefore, meets Regulatory Position 2.2.

#### Prevention of the Introduction of Unnecessary Requirements

Regulatory Position 2.2 states that the introduction of unnecessary or extraneous requirements that may result in inclusion of unwanted or unnecessary code should be prevented. Evaluation of a safety system against this part of the regulatory position is a plant specific activity that requires an assessment of a completed system design. MELCO partially addresses this part of the regulatory position by having at least one independent reviewer check the requirements specifications in order to detect and correct the insertion of requirements that have



an undesirable effect on the secure operational environment of the system. This ensures that the secure operational environment features of the MELTAC platform are not compromised by changes or new functions/products.

The NRC staff finds MELCO's process to detect and correct unnecessary requirements is acceptable and can be used to support the development of the plant specific application of the MELTAC platform. Because determination of a secure development environment is a plant specific activity, the NRC staff considers this criteria to be a plant specific action (see PSAI 5.2.15).

### 3.12.3 RG 1.152, Revision 3, Regulatory Position 2.3, "Design Phase" Translation of Secure Operational Environment Requirements into Design Configuration Items

Regulatory Position 2.3 states that 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.

Evaluation of a safety system against this part of the regulatory position is a plant specific activity that requires an assessment of a completed system design. MELCO partially addresses this part of the regulatory position by using the RTM to confirm the traceability of the MELTAC platform SDOE features from requirements to design specifications.

The NRC staff finds MELCO's process to verify the translation of SDOE requirements is acceptable and can be used to support the plant specific application of the MELTAC platform. Because determination of a secure operational environment is a plant specific activity, the NRC staff considers this criteria to be a plant specific action (see PSAI 5.2.15).

### Physical and Logical Access Controls

Regulatory Position 2.3 states that physical and logical access control features should be based on the results of the assessment performed in the concepts phase of the life cycle.

MELCO addresses this part of the regulatory position because the physical, logical and administrative access control features are based on the results of the assessment performed (see Section 3.12.1 of this SE).

Below is the NRC staff's review of how the MELTAC platform's secure development and operational environment controls, as described in Sections 4.5 and 6.1.2 of the MELTAC LTR (Ref. 14) and Section 3 of the MELTAC platform SPM, address Regulatory Position 2.3.

### Secure Development Environment Controls

The MELTAC platform secure development environment ensures that no unintended code is included in the basic software and related documentation during software development, and that unintended changes to the basic software installed in the system are prevented and detected. The MELTAC platform LTR states that the security measures in the development process of the application software are described in the application licensing document. Therefore, the review of the application software secure development environment controls implemented in a MELTAC platform-based system is a plant specific activity (see PSAI 5.2.16 of this SE). The MELTAC platform LTR and platform SPM describe the secure development environment features used for the basic software and related documentation. The MELTAC source code and

the object code are managed by the platform software development/storage environment, which is comprised of the MELCO corporate electronic archive system (CEAS) and the development / verification environment. Both the CEAS and development / verification environment are operated in accordance with the 10 CFR 50, Appendix B QA program (see Section 3.4 of this SE).

The MELCO CEAS is a dedicated storage system for the products related to nuclear power plants, including application software and the MELTAC engineering tool. MELCO implements account and password management to limit CEAS access to only personnel authorized to work on a particular development project. There is no communication between the CEAS and the MELCO corporate Information Technology (IT) network. The CEAS is physically secured, and the master data is stored in a data repository where access is restricted. The NRC staff was not able to observe these secure development environment controls, but did discuss their implementation with MELCO staff during the regulatory audit (see Ref. 33).

The development/verification environment is used by the design team to develop the basic software and MELTAC engineering tool. The development/verification environment is also where the V&V team conducts reviews and tests of the MELTAC platform. There is no communication between the development/verification environment and the MELCO corporate IT network. The development/verification environment is physically secured, and only personnel authorized to work on a particular development project can access the development computer.

The NRC staff was not able to observe these secure development environment controls, but did discuss their implementation with MELCO staff during the regulatory audit (see Ref. 33). MELCO also implements configuration control measures described in Section 3.11 of the MELTAC platform SPM to: detect unauthorized changes to controlled documents (e.g., specifications, design descriptions, and test reports); control access to the document control system and the software Development/Storage Environment; independently verify that the content of production copies of software match the controlled master copies, label controlled media and storage devices; and identify software versions that are under development, approved for production, and retired.

Additionally, the MELTAC platform application SPM states that the QA organization shall conduct periodic audits to confirm the security of the application software development process is controlled in accordance with the application SPM. During the regulatory audit, the NRC staff reviewed a sample QA Audit Report (see Ref. 33).

The NRC staff finds MELCO's secure development environment to be acceptable and can be used to develop the plant specific application of the MELTAC platform. Because determination of a secure development environment is a plant specific activity, the NRC staff considers this criteria to be a plant specific action (see PSAI 5.2.15).

#### Secure Operational Environment Controls

The review of the secure operational environment controls implemented in a MELTAC platform-based system is a plant specific activity that requires an assessment of a completed system design. However, the MELTAC platform design uses a combination of physical, logical, and administrative controls, and design features to protect the safety-related basic software and the application software from unauthorized and undetected changes.

The MELTAC platform CPU module contains two F-ROMs: one for the basic software, and one for the application software. In order to change the basic software or the application software, the CPU module has to be removed from the CPU chassis, which requires (1) opening the cabinet door, and (2) turning off the power to the CPU module. The MELTAC platform has the capability to generate an alarm signal to the MCR when the cabinet door is opened, and when the CPU power source is turned off. Alarms in the MCR can be generated via the control network, data Link, or digital output module (with isolation). The use of these alarms will be defined in the application specific design.

Changes to the basic software must be performed in MELCO's factory. Changes to the application software require (1) placing the CPU module in a dedicated reprogramming chassis, which is separate and independent from the CPU chassis, (2) using the password protected MELTAC engineering tool, and (3) activating the write permission switch on the status display module. Activation of this switch generates a signal that can be used to generate an alarm in the MCR.

Additionally, an "under simulation" signal is generated when a temporary process input value is set from the MELTAC engineering tool. This signal can also be used to generate an alarm in the MCR, thus alerting MCR personnel when process input values are changed.

The NRC staff finds that the MELTAC platform contains secure operational environment features that can be used to support the plant specific application of the MELTAC platform. Because determination of a secure operational environment is a plant specific activity, the NRC staff considers this criteria to be a plant specific action (see PSAI 5.2.15).

#### Prevention of the Introduction of Unnecessary Design Features

Regulatory Position 2.3 states that 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.

Evaluation of a safety system against this part of the regulatory position is a plant specific activity that requires an assessment of a completed system design. MELCO partially addresses this part of the regulatory position by having at least one independent reviewer as well as the independent V&V team check the software specifications in order to detect and correct the insertion of design features that have an undesirable effect on the secure operational environment of the system. The independent V&V team uses the RTM to verify that the secure operational environment features from the requirement phase are correctly translated into the design, and unauthorized functionality is not introduced into the design.

The NRC staff finds that MELCO's process to prevent the introduction of unnecessary design features or functions is acceptable and can be used to support the plant specific application of the MELTAC platform. Because determination of a secure operational environment is a plant specific activity, the NRC staff considers this criteria to be a plant specific action (see PSAI 5.2.15).

#### 3.12.4 RG 1.152, Revision 3, Regulatory Position 2.4, "Implementation Phase" Transformation from System Design Specification to Design Configuration Items

Regulatory position 2.4 states that 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.

Evaluation of a safety system against this part of the regulatory position is a plant specific activity that requires an assessment of a completed system design. MELCO partially addresses this part of the regulatory position by using the RTM to confirm the traceability of the MELTAC platform SDOE features from design specification to design configuration items.

The NRC staff finds that MELCO's process to verify the translation of SDOE design features is acceptable and can be used to support the plant specific application of the MELTAC platform. Because determination of a secure operational environment is a plant specific activity, the NRC staff considers this criteria to be a plant specific action (see PSAI 5.2.15).

#### Implementation of Secure Development Environment Procedures and Standards

Regulatory Position 2.4 states that the developer should implement secure development environment procedures and standards to minimize and mitigate any inadvertent or inappropriate alterations of the developed system.

MELCO addresses this part of the regulatory position in Reference 36 by pointing to its development environment control procedure, and by listing the physical, logical and administrative controls implemented to construct and maintain a secure development environment that minimizes unintended modifications to the system. The NRC staff finds that MELCO's secure development environment controls and procedures meet Regulatory position 2.4, can be used to support the plant specific application of the MELTAC platform, and are therefore acceptable.

#### Accounting for Hidden Functions in the Code

Regulatory Position 2.4 states that hidden functions and vulnerable features embedded in the code, their purpose and their impact on the integrity and reliability of the safety system should be accounted for.

Evaluation of a safety system against this part of the regulatory position is a plant specific activity that requires an assessment of a completed system design. MELCO partially addresses this part of the regulatory position by performing various V&V activities to identify errors in code. At least one independent reviewer, as well as the independent V&V team, check the source code. The independent V&V team also verifies the source code by performing functional and structural unit testing, which would detect and correct the insertion of functions and vulnerable features that have an undesirable effect on the secure operational environment of the system. The V&V team also performs the following secure development environment activities:

- Evaluate the processor software source code and the FPGA source code for correctness, consistency, completeness, accuracy, readability, and testability
- Verify that processor software source code, and the FPGA source code are written according to the coding rules
- Use the static analysis tool to check the processor software source code in order to identify code that could cause faults (e.g., unauthorized type conversion, use of uninitialized variables or unnecessary code); and the FPGA source code in order to

identify code that could cause faults (e.g., asynchronous circuit, invalid timing or code in the logic which cannot be synthesized).

- Conduct static analysis of each processor software source code to evaluate how any warning messages identified by the static analysis tool will affect the software operation; and of each FPGA source code to evaluate how warning messages identified by the static analysis tool will affect the FPGA operation. A V&V anomaly report is issued if there are any possible software or FPGA errors.
- Verify that the security-related processor software design specifications described in the program specification are fully, completely and correctly translated into the processor software source code; and that the security-related FPGA software design specifications described in the FPGA specification are fully, completely and correctly translated into the FPGA source code.
- Verify that the processor software design specifications and processor software source code are matched and no unintended code is incorporated in the processor software source code; and that the FPGA design specifications and FPGA source code are matched and no unintended code is incorporated in the FPGA source code.

The NRC staff finds that MELCO's process to detect and address errors in the code is acceptable and can be used to support the plant specific application of the MELTAC platform. Because determination of a secure operational environment is a plant specific activity, the NRC staff considers this criteria to be a plant specific action (see PSAI 5.2.15).

#### 3.12.5 RG 1.152, Revision 3, Regulatory Position 2.5, "Test Phase" Validation of Secure Operational Environment Design Configuration Items

Regulatory position 2.5 states that 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.

The compliance of a safety system with this part of the regulatory position was not evaluated because it is a plant specific activity that requires an assessment of the safety system design (see PSAI 5.2.16).

#### Configuration of Secure Operational Environment Design Features

Regulatory position 2.5 states that 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.

The compliance of a safety system with this part of the regulatory position was not evaluated because it is a plant specific activity that requires an assessment of the safety system design (see PSAI 5.2.16).

## 4.0 SUMMARY

The NRC staff determined the MELTAC platform, consisting of modules described in the MELTAC LTR (Ref. 14), their design features, the basic software, the operational system software, and software embedded in electronic boards and the processes used to produce them, are sufficient to support compliance with the applicable regulatory requirements for plant-specific use. This determination is applicable for use of the MELTAC platform in



safety-related applications for NPPs provided that each plant-specific application satisfies the limitations and conditions delineated in Section 5.0 of this SE and the system is properly installed and used as indicated by MELCO. The NRC staff further concludes that the MELTAC platform can be used in safety-related systems to provide reasonable assurance of adequate protection of public health, safety and security based on the technical evaluation provided in Section 3.0 of this SE. On this basis, the NRC staff determined the MELTAC platform is acceptable for use in safety-related I&C systems after addressing the limitations and conditions in Section 5.0 of this SE.

## **5.0 LIMITATIONS AND CONDITIONS**

For each generic open item and PSAI that applies to the applicant's or licensee's use of the MELTAC platform, an applicant or licensee referencing the MELTAC LTR (Ref. 14) should demonstrate that applicable items have been satisfactorily addressed. The applicable items provide limitations and conditions for the MELTAC platform's use, as reviewed by the NRC staff and documented within this SE.

### **5.1 GENERIC OPEN ITEMS**

On the basis of its review of the MELTAC platform, the NRC staff has identified the following generic open items:

- 5.1.1 Qualified Platform Components – This SE is limited to components of the MELTAC platform listed in Table 3.2-1 of this SE. Use of other components for safety-related applications is not approved by the NRC and may be subject to additional evaluation and qualification testing.
- 5.1.2 Termination Unit Module – MELCO has not conducted seismic and environmental qualification testing on the PSND Termination Unit module. Additional qualification testing of the PSND must be completed prior to implementation of these modules in safety-related applications.
- 5.1.3 CPU Fan Assembly Module – Fans used during EQ testing were functionally equivalent to the KFNJ but not the same. Additional qualification testing of the KFNJ must be completed prior to implementation of these modules in safety-related applications.

### **5.2 PLANT SPECIFIC ACTION ITEMS**

The following plant specific actions should be performed by an applicant or licensee referencing the MELTAC LTR (Ref. 14) for a safety-related system based on the MELTAC platform.

- 5.2.1 MELTAC Platform Changes – An applicant referencing the MELTAC LTR should demonstrate that the MELTAC platform used to implement the plant specific system is unchanged from the generic platform addressed in this SE. Otherwise, the licensee should clearly and completely identify any modification or addition to the generic MELTAC platform as it is employed and provide evidence of compliance by the modified platform with all applicable regulations that are affected by the changes. In addition, the applicant must verify that modules, features, and or functions that require configuration are properly configured and tested to meet application specific system requirements.

- 5.2.2 Application Software Development Process – An applicant or licensee referencing the MELTAC LTR should provide oversight to ensure the development of its application software was performed in accordance with a process that is equivalent to the one described in the MELTAC platform application software program manual (Ref. 30) and as evaluated in Section 3.5 of this SE.
- 5.2.3 System Cycle Time –The licensee must perform timing analyses and functional testing of the application implementation and system configuration to demonstrate that response time performance satisfies application specific requirements established in the plants safety analysis report.
- 5.2.4 Plant Specific Equipment Qualification – The licensee must demonstrate that the generic qualification envelope established for the MELTAC platform bounds the corresponding plant specific environmental conditions (i.e., temperature, humidity, radiation, and Electro-Magnetic Compatibility (EMC) for the location(s)), in which the equipment is to be installed. The licensee should ensure that specific equipment configuration of MELTAC components, to be installed, is consistent with that of the MELTAC equipment used for environmental qualification tests.
- 5.2.5 Plant Specific Seismic Qualification – An applicant or licensee referencing the MELTAC LTR must demonstrate that the qualified seismic withstand capability of the MELTAC platform bounds the plant specific seismic withstand requirements. See Section 3.6.3 of this SE for boundary conditions established for the MELTAC platform during Seismic testing.
- 5.2.6 Magnetic Field Installation Restrictions – An applicant or licensee referencing the MELTAC LTR must demonstrate that the MELTAC platform is not installed in areas with strong magnetic fields. See Section 3.6.2.2 for additional details of this limitation.
- 5.2.7 Failure Modes and Effects Analysis – An applicant or licensee referencing the MELTAC LTR must perform a system-level failure modes and effects (FMEA) to demonstrate that plant specific use of the MELTAC platform identifies each potential failure mode and determines the effects of each. The FMEA should demonstrate that single-failures, including those with the potential to cause a non-safety-related system action (i.e., a control function) that results in a condition requiring protective action (i.e., a protection function), cannot adversely affect the protection functions, as applicable. The applicant or licensee should ensure system failure states identified in the FMEA are consistent with system requirements and should review how errors and failures are indicated and managed upon being detected. The applicant or licensee must also demonstrate that WDT functions that are credited for initiating fail safe states upon a given failure are not susceptible to the same cause for the failure.
- 5.2.8 Application Specific System Reliability – An applicant or licensee referencing the MELTAC LTR should perform a system-level evaluation of the degree of redundancy, diversity, testability, and quality provided in a MELTAC platform-based safety system to determine if the degrees provided are commensurate with the safety functions being performed. An applicant or licensee should confirm that a resultant MELTAC platform-based system continues to satisfy any applicable reliability goals that the plant has established for the system. This plant specific action should consider the effect of possible failures, system-level design features provided to prevent or limit the failures'

effects, and any plant specific inclusion of a maintenance bypass to support plant operations.

- 5.2.9 Setpoint Methodology – An applicant or licensee referencing the MELTAC LTR should perform an analysis of accuracy, repeatability, thermal effects and other necessary data for use in determining the contribution of the MELTAC platform to instrumentation uncertainty in support of setpoint calculations. See Section 3.7.4 of this SE for additional information on MELTAC setpoint methodology.
- 5.2.10 System Testing and Surveillance – Because a combination of surveillance, software diagnostics and automatic self-tests are necessary to provide comprehensive coverage of all platform failures, the applicant or licensee referencing the MELTAC LTR must establish periodic surveillance testing necessary to detect system failures for which automatic detection is not provided. The applicant must also define appropriate surveillance intervals to provide acceptable comprehensive coverage of identifiable system failure modes.
- 5.2.11 Diversity and Defense-In-Depth Analysis – An applicant or licensee referencing the MELTAC LTR must perform a plant specific D3 analysis for safety system applications of the MELTAC platform.
- 5.2.12 DI&C ISG-04 – Although the NRC staff determined that the MELTAC platform includes features to support satisfying various sections and clauses of DI&C ISG-04, an applicant or licensee referencing the MELTAC LTR must evaluate the MELTAC platform based-system for compliance with this guidance. This SE does not address a specific application, establish a definitive safety system or protective action, or identify and analyze the impact of credible events along with its direct and indirect consequences. The applicant or licensee should consider its plant specific design basis.
- 5.2.13 IEEE Std. 603 – Although the NRC staff determined that the MELTAC platform is capable of satisfying various sections and clauses of IEEE Std.603-1991, an applicant or licensee referencing the MELTAC LTR should identify the approach taken to satisfy each applicable clause of IEEE Std. 603-1991 with consideration of the plant specific design basis.
- This SE does not address a specific application, establish a definitive safety system or protective action, or identify and analyze the impact of credible events including direct and indirect consequences. Therefore, an applicant or licensee should demonstrate that the plant specific use of the MELTAC platform satisfies the applicable IEEE Std. 603-1991 clauses in accordance with the plant specific design basis and safety system application.
- 5.2.14 IEEE Std. 7-4.3.2 – Even though the NRC staff determined that the MELTAC platform is capable of satisfying various sections and clauses of IEEE Std. 7-4.3.2-2003, an applicant or licensee referencing the MELTAC LTR should identify the approach taken to satisfy each applicable clause of IEEE Std. 7-4.3.2-2003 with consideration of the plant specific design basis.
- 5.2.15 This SE does not address a specific application, establish a definitive safety system or protective action, or identify and analyze the impact of credible events including direct and indirect consequences. Therefore, the applicant or licensee should demonstrate

that plant specific use of the MELTAC platform satisfies the applicable IEEE Std. 7-4.3.2-2003 clauses in accordance with the plant specific design basis and safety system application.

- 5.2.16 Secure Development and Operational Environment – An applicant or licensee referencing the MELTAC LTR for a safety-related plant specific application should ensure that a secure development and operational environment has been established for its plant specific application, and that it satisfies the applicable regulatory evaluation criteria of RG 1.152, Revision 3.
- 5.2.17 Safety Visual Display Unit – The S-VDU is not approved for use in a manner such that it is required to be operational when the MELTAC safety system is called upon to initiate an automatic safety function. If a licensee installs a MELTAC application that includes implementation of one or more S-VDU, the licensee must verify that automatic control functions do not depend on the operation of the S-VDU processors. The use and failure modes of the S-VDU must be addressed in the plant specific FMEA. See Section 3.5.2.6 of this SE for additional information on plant specific failure modes and effects analyses requirements.

## **6.0 REFERENCES**

1. MELCO Submittal of Topical Report for Safety Evaluation, dated April 30, 2014 (ADAMS Package Accession No. ML14121A413).
2. MELCO Submittal of Support Documentation for the "Safety System Digital platform – MELTAC – Topical Report," dated September 26, 2014, ISG-04 Conformance analysis and platform software program manual (ADAMS Package Accession No. ML14272A381).
3. MELCO Submittal of Support Documentation for Safety Evaluation of the MELTAC platform Topical Report, dated December 30, 2014 (ADAMS Package Accession No. ML14364A126).
4. MELCO Submittal of Support Documentation for Safety Evaluation of the MELTAC platform Topical Report, dated January 30, 2015 (ADAMS Package Accession No. ML15033A072).
5. MELCO Submittal of Support Documentation for Safety Evaluation of the MELTAC platform Topical Report, dated March 31, 2015, Summary of MELTAC platform QA, Quality Manual, Setpoint Methodology (ADAMS Package Accession No. ML15090A618).
6. MELCO Submittal of Support Documentation for Safety Evaluation of the MELTAC platform Topical Report, dated April 28, 2015, MELTAC platform software Tools (ADAMS Package Accession No. ML15118A659).
7. MELCO Submittal of Support Documentation for Safety Evaluation of the MELTAC platform Topical Report, dated April 17, 2015 (ADAMS Package Accession No. ML15107A283).
8. MELCO Submittal of Support Documentation for Safety Evaluation of the MELTAC platform Topical Report, Summary of Compliance to the IEEE Std. 603 and IEEE Std. 7-4.3.2, dated May 29, 2015 (ADAMS Package Accession No. ML15149A307).

9. MELCO Submittal of Support Documentation for Safety Evaluation of the MELTAC platform Topical Report, Summary of Compliance to the IEEE Std. 603 and IEEE Std. 7-4.3.2, dated June 18, 2015 (ADAMS Package Accession No. ML15169B018).
10. MELCO Submittal of Support Documentation for Safety Evaluation of the MELTAC platform Topical Report, dated July 6, 2015 (ADAMS Package Accession No. ML15187A370).
11. MELCO Submittal of Support Documentation for Safety Evaluation of the MELTAC platform Topical Report, dated July 7, 2015 (ADAMS Package Accession No. ML15188A178).
12. MELCO Submittal of Support Documentation for Safety Evaluation of the MELTAC platform Topical Report, dated February 19, 2016 (ADAMS Package Accession No. ML16050A199).
13. MELCO Submittal of Support Documentation for Safety Evaluation of the MELTAC platform Topical Report, dated March 28, 2016 (ADAMS Package Accession No. ML16088A318).
14. MELCO Submittal of Support Documentation for Safety Evaluation of the MELTAC platform Topical Report, Safety System Digital platform - MELTAC - Topical Report, dated April 27, 2016 (ADAMS Package Accession No. ML16118A322).
15. MELCO Submittal of Support Documentation for Safety Evaluation of the MELTAC platform Topical Report, dated June 6, 2016 (ADAMS Package Accession No. ML16158A193).
16. MELCO Submittal of Support Documentation for Safety Evaluation of the MELTAC platform Topical Report, dated June 21, 2016 (ADAMS Package Accession No. ML16174A306).
17. MELCO Submittal of Support Documentation for Safety Evaluation of the MELTAC platform Topical Report, dated July 21, 2016 (ADAMS Package Accession No. ML16229A116).
18. MELCO – Quality Manual Based on U.S. Regulations, dated August 31, 2016 (ADAMS Accession No. ML16223A434)
19. MELCO Submittal of Support Documentation for Safety Evaluation of the MELTAC platform Topical Report, dated August 10, 2016 (ADAMS Package Accession No. ML16223A828).
20. MELCO Schedule for Providing the Responses to the Request for Additional Information, dated September 16, 2016 (ADAMS Accession No. ML16263A114).
21. MELCO Responses to the Request for Additional Information, dated September 23, 2016 (ADAMS Package Accession No. ML16267A069).
22. MELCO Schedule for Providing the Responses to the Request for Additional Information, dated September 30, 2016 (ADAMS Accession No. ML16274A005).
23. MELCO Responses to the Request for Additional Information, dated October 7, 2016 (ADAMS Package Accession No. ML16281A277).
24. MELCO Responses to the Request for Additional Information, dated October 17, 2016, Summary of MELTAC platform commercial grade dedication Activity (ADAMS Package Accession No. ML16291A159).



25. MELCO Submittal of Support Documentation for Safety Evaluation of the MELTAC platform Topical Report, dated October 18, 2016 (ADAMS Package Accession No. ML16305A007).
26. MELCO Submittal of Support Documentation for Safety Evaluation of the MELTAC platform Topical Report, dated November 1, 2016 (ADAMS Package Accession No. ML16307A317).
27. MELCO Response to MELTAC Topical Report Revision 2 RAI#1 Regarding Item No. 7 for JEXU-1041-1008, Topical Report, dated March 17, 2017 (ADAMS Accession No. ML17080A163).
28. MELCO – Request for Exclusion from SER for MELTAC platform TR, sated April 7, 2017 (ADAMS Accession No. ML17101A525).
29. MELCO Submittal of Support Documentation for Safety Evaluation of the MELTAC platform Topical Report, dated May 31, 2017 (ADAMS Package Accession No. ML170153A185).
30. MELCO – JEXU-1041-1032-NP (R0), MELTAC platform application software program manual, dated July 31, 2017 (ADAMS Accession No. ML17214A540).
31. MELCO's Responses to MELTAC Topical Report Revision 0 RAI #1 (TAC No.MF4228) (Regarding, Items No.1 for JEXU-1041-1023, "MELTAC platform Equipment Qualification") and Submittal of MELTAC Topical Report Supporting Documentation, dated August 31, 2017 (ADAMS Accession No. ML17243A102).
32. Regulatory Audit Plan for November 28-30, 2017, Safety System Digital platform MELTAC Topical Report Revision 0, dated September 27, 2017 (ADAMS Accession No. ML17243A384).
33. Regulatory Audit Report for the MELTAC (Mitsubishi Electric Total Advanced controller) Digital platform Licensing Topical Report, dated January 24, 2018 (ADAMS Accession No. ML18011A487).
34. Acceptance Review of the "Safety System Digital platform-MELTAC [Mitsubishi Electric Total Advanced controller] - Topical Report Revision 0," dated May 20, 2015 (ADAMS Accession No. ML15121A763).
35. MELCO First Round of RAIs, dated June 29, 2016 (ADAMS Accession No. ML16124A012).
36. MELCO Submittal of MELTAC platform SDOE Vulnerability Assessment Supporting Documentation, dated November 1, 2016 (ADAMS Package Accession No. ML18040A479).
37. Safety Evaluation by Office of Nuclear Reactor Regulation of Electric Power Research Institute (EPRI)-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications," dated July 30, 1998 (ADAMS Accession No. ML12205A265).
38. Safety Evaluation by Office of Nuclear Reactor Regulation of EPRI-106439, "Guidance on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications" dated July 17, 1997 (ADAMS Accession No. ML092190664).

39. NRC Inspection Report, IR 99901410-11-202 and Notice of Nonconformance, dated January 25, 2012 (ADAMS Accession No. ML12013A353).
40. NRC staff acceptance of MELTAC's resolution of non-conformance items, dated May 1, 2012 (ADAMS Accession No. ML12118A454).

**APPENDIX A**  
**Comments on Draft Safety Evaluation and Response**

NUMBER	LOCATION	COMMENT TYPE	COMMENT	NRC RESPONSE
1	PAGE 21, Line 41	PROPRIETARY	Deemed Proprietary by MELCO Affidavit	Agreed. Redacted in nonproprietary version.
2	PAGE 25, Line 26-28	PROPRIETARY	Deemed Proprietary by MELCO Affidavit	Agreed. Redacted in nonproprietary version.
3	PAGE 67, Line 8-10	PROPRIETARY	Deemed Proprietary by MELCO Affidavit	Agreed. Redacted in nonproprietary version.
4	PAGE 116, Line 34	INCORRECT TERMINOLIGY	The term "Safety-Video Display" is used instead of "Safety Visual Display". NOTE: The LTR uses the term "Safety Visual Display" only.	Agreed. Term changed.

## **PART 2**

### **Request for Additional Information (RAI), including:**

NRC Transmittal Letter dated June 29, 2016

RAI Questions

~~OFFICIAL USE ONLY - PROPRIETARY INFORMATION~~

June 29, 2016

Gilbert W. Remley  
Nuclear Systems Department Manager  
Mitsubishi Electric Power Products, Inc.  
547 Keystone Drive  
Warrendale, PA 15086

SUBJECT: REQUEST FOR ADDITIONAL INFORMATION FOR THE "SAFETY SYSTEM  
DIGITAL PLATFORM – MELTAC – [MITSUBISHI ELECTRIC TOTAL  
ADVANCED CONTROLLER] TOPICAL REPORT REVISION 0"  
(TAC NO. MF4228)

Dear Mr. Remley:

By letter dated April 30, 2014 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML14272A382), Mitsubishi Electric Corporation (MELCO) submitted for U.S. Nuclear Regulatory Commission (NRC) staff review the topical report (TR), "Safety System Digital Platform - MELTAC - Topical Report Revision 0" (ADAMS Accession No. ML14121A413). By letters dated September 26 and December 30, 2014, January 30, March 31, and April 28, 2015 (ADAMS Accession Nos. ML14272A382, ML14364A132, ML15033A073, ML15090A620 and ML15118A661), MELCO supplemented the application.

Upon review of the information provided, the U.S. Nuclear Regulatory Commission (NRC) staff has determined that additional information is needed to complete the review. In an email exchange with Mr. Ken Krayvo representing MELCO, it was agreed that the NRC staff will receive your response to the enclosed Request for Additional Information (RAI) by mid-August, 2016. Some RAIs may need a pre-submittal discussion, so it is agreed that the NRC staff will receive response(s) by the submittal dates determined after this discussion.

~~OFFICIAL USE ONLY - PROPRIETARY INFORMATION~~



~~OFFICIAL USE ONLY - PROPRIETARY INFORMATION~~

G. Remley

- 2 -

If you have any questions regarding the enclosed RAI, please contact me at 301-415-7297 or Joseph.Holonich@nrc.gov.

Sincerely,

/RA/

Joseph J. Holonich, Sr. Project Manager  
Licensing Processes Branch  
Division of Policy and Rulemaking  
Office of Nuclear Reactor Regulation

Project No. 751

Enclosure:

1. Nonproprietary RAI questions
2. Proprietary RAI questions

<b>NOTICE:</b> Enclosure 2 transmitted herewith contains SUNSI. When separated from the enclosure 2, this transmittal document is decontrolled.
---

~~OFFICIAL USE ONLY - PROPRIETARY INFORMATION~~

~~OFFICIAL USE ONLY - PROPRIETARY INFORMATION~~

G. Remley

- 2 -

If you have any questions regarding the enclosed RAI, please contact me at 301-415-7297 or Joseph.Holonich@nrc.gov.

Sincerely,

*/RA/*

Joseph J. Holonich, Sr. Project Manager  
Licensing Processes Branch  
Division of Policy and Rulemaking  
Office of Nuclear Reactor Regulation

Project No. 751

Enclosure:

1. Nonproprietary RAI questions
2. Proprietary RAI questions

**NOTICE:** Enclosure 2 transmitted herewith contains SUNSI. When separated from the enclosure 2, this transmittal document is decontrolled.

DISTRIBUTION:

PUBLIC	RidsACRS_MailCTR	RidsNrrDprPlpb	PLPB R/F
RidsOgcMailCenter	RidsNroOd	RidsResOd	
RidsNrrLADHarrison	RBeacom	RStattel	MWaters

**ADAMS Accession No.: Package: ML16124A012; Proprietary RAIs: ML16083A111**

**Letter and nonproprietary RAIs ML16124A013**

**NRR-106**

OFFICE	DPR/PLPB/PM	DPR/PLPB/LA*	DE/EICB/BC	DPR/PLPB/BC	DPR/PLPB/PM
NAME	JHolonich	DHarrison	MWaters (RStattel for)	KHsueh	JHolonich
DATE	05/10/2016	05/26/2016	06/ 20 /2016	06/ 29 /2016	06/ 29 /2016

**OFFICIAL RECORD COPY**

~~OFFICIAL USE ONLY - PROPRIETARY INFORMATION~~

**REQUEST FOR ADDITIONAL INFORMATION #1**  
**MITSUBISHI ELECTRIC COMPANY- MELCO**  
**SAFETY SYSTEM DIGITAL PLATFORM**  
**MITSUBISHI ELECTRIC TOTAL ADVANCED CONTROLLER– MELTAC**  
**TAC NO. MF4228**

Topical Report (TR), JEXU-1041-1008, “Safety System Digital Platform – MELTAC”  
(Agencywide Document Access and Management System (ADAMS) Accession  
No. ML14121A416):

1. Title 10 of the *Code of Federal Regulations* (10 CFR) Part 50, “Domestic Licensing of Production Utilization Facilities, establishes fundamental regulatory requirements. Specifically, Appendix B, “Quality Assurance Criteria,” Criterion II, “Quality Assurance Program,” states, in part; “This program shall be documented by written policies, procedures, or instructions.” Page 0-6 of the TR states “the information provided in this report covers the life cycle and the Quality Assurance Program (QAP) of the MELTAC platform.” In other inferences throughout the document, there are references to “10 CFR Part 50 Appendix B QAP” or just “QAP” or “MELCO QAP.” The U.S. Nuclear Regulatory Commission (NRC) staff notes there is also a separate QAP for non-safety items. It is therefore unclear to the NRC staff how this requirement for specific written policies, procedures, or instructions is met and thus the staff is unable to make a regulatory compliance determination. Please provide information to identify each QAP by title, number, date, and revision which is proposed to meet the requirements (or not) as stated by 10 CFR Part 50 Appendix B, Criterion II.
2. On page 2 of the TR, the following General Design Criteria (GDC) are also applicable to the MELTAC platform. Please review criteria provided in these GDC’s and describe how the platform satisfies each GDC. If regulatory compliance is dependent on application specific development activities, please state this.
  - a. GDC 13, “Instrumentation and Control,” is applicable. MELTAC and the qualified displays, with no identified limitations within the system descriptions, will monitor variables and systems during normal operations, anticipated operational occurrences (AOOs), and accident conditions as well as those which affect the fission process and core pressure boundaries. Include a full explanation applicable to this GDC.
  - b. GDC 20, “Protection System Functions,” is applicable. MELTAC will automatically initiate reactivity control systems. Include a full explanation applicable to this GDC.
  - c. GDC 25, “Protection System Requirements for Reactivity Malfunctions,” is applicable. The MELTAC platform will be used for safety and non-safety systems for reactivity control systems without limitations identified by the topical report. Also the capability to protect against reactivity control malfunctions is not an exception therefore this requirement should be included.

Enclosure 1

3. With regard to TR page 17, item d), software is mentioned several times regarding the capabilities of the engineering tool. In each case, identify if this is referring to the application or platform software or both.
4. With regard to TR page 54, a) "Creation of Application Softwar." Criterion III, "Design Control," of 10 CFR Part 50 Appendix B states in part: "Design changes, including field changes, shall be subject to design control measures commensurate with those applied to the original design and be approved by the organization that performed the original design unless the applicant designates another responsible organization." To determine compliance with this criteria, the NRC staff needs to understand whether the MELCO development process described by this application will be used to perform design changes or if a different process to be developed by the licensee would be used. If a different process is to be used, then an application specific action item should be developed accordingly to make clear to the licensee that an appropriate safety-related development process must be established before the engineering tool is used to revise platform software.
5. With regard to TR page 55, e) in order to complete its evaluation of the MELCO platform the NRC staff needs to understand the temporary changes to field changeable process value in data table (Data Set). Please provide a description and examples of temporary changes to field changeable process values.
6. With regard TR Page 54, in Section 4.1.4.1, Function Description, subsection b) states this activity is done with the central processing unit (CPU) module in the re-programming Chassis and therefore the controller status is off line; however; subsections c), d), and e) do not include similar statements. Please provide additional information regarding controller status in relation to performing functions described in subsections c), d), and e).
7. DI&C-ISG-04, Section 1, Interdivisional Communications, Point 6, states the safety function processor should not accept interrupts from outside its own safety division. Page 56, third paragraph, states; [ .] Provide information on how the engineering tool is prevented from disrupting the controller safety functions.
8. Page 76, Section 4.1.7.2, Memory Integrity Check (MIC), describes an activity that is part of the verification program for the MIC software tool. Per ISG-06, Section D.10.4.2.3.2, the information needed for the NRC staff to reach a determination that the software tools are adequate for their intended use should be contained in the documentation for the software tool verification program. Therefore, provide the procedure for the verification of the MIC tool to demonstrate adequacy. In addition, please clarify the following: How far along is the development of the MIC? Is it currently in use by operating plants? Please explain if all of the system memory locations are checked during this activity including data locations and unused memory.

9. Page 214 of the TR discusses the generic redundant parallel controller reliability analysis and a fault tree analysis to support that controller configuration review. The NRC staff needs to review this specific analysis and additional analyses for other controller configurations and modules that are included in the MELCO platform to complete its evaluation in accordance with ISG-06 Section D.9.4.2.1.1. Please provide a description of the criteria used to determine which controller configuration will be used (i.e., single, redundant parallel or redundant standby) as well as documentation to demonstrate compliance of other possible controller configurations to this criteria.

JEXU-1041-1022, "Summary of MELTAC Platform Design" (ADAMS Accession No. ML15033A076):

1. Software Requirements Specification (SRS) and Software Design Specifications (SDS):
  - a. The summary document, JEXU\_1041-1022, states the MELCO document which contains the information for a software requirements specification is "MELTAC-Nplus S System Specification," Section 4.1, "System Specification (Platform Specification)." The summary document provides the table of contents of the system specification but not the specification itself. The NRC requires system specifications to support its safety evaluation. The NRC staff has endorsed Institute of Electrical and Electronics Engineers (IEEE) Standard 830-1998, "IEEE Recommended Practice for Software Requirements Specifications," by Regulatory Guide (RG) 1.172. Also, the NRC Standard Review Plan (SRP) Section 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems," Section B.3.3.1 provides acceptance criteria for a SRS. Additional guidance can be found in NUREG/CR-6101, Sections 3.2.1 and 4.2.1. The acceptance criteria using these references is delineated in ISG-06 Section D.4.4.3.1. The summary document points to JEXU-1024-1010, "MELTAC-Nplus S System Specification." Therefore, the staff requests this document be submitted on the docket with an analysis of conformance to the acceptance criteria, or any alternatives, to RG 1.172 and the applicable sections of the SRP, Section 7.14, specifically identified.
  - b. ISG-06, Section D.4.4.3.3, references the acceptance criteria for the software design specification including the SRP Section BTP 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems," Section B.3.3.3, "Design Activities – Software Design Specification (SDS)." This guidance provides functional and process characteristics as well as review guidance of SDSs.

Provide an explanation how the following documents, identified in Table 1 and Appendix A, provide the information for the controller CPU module to conform to the Software Design Specification guidance stated above. Also the NRC staff requests these documents be submitted on the docket:

Hardware Requirement Specification, JEXU-1024-1021,  
Hardware Specification, JEXU-1024-1051,  
Software Specification, JSX4L400,



FPGA Specification, JEXU-1024-1071.

2. Thoroughly explain the statement on page 1: "Since the development of the MELTAC Platform is ongoing, only auditable documents are listed in Appendix A." The staff needs to understand the extent of the ongoing development process and the limitations of document availability. Please identify by specific type what activities, equipment, and procedures are not complete and why the changes are taking place including those involved in the MELTAC Reevaluation Program. Also include the schedule to complete the development.
3. The MELTAC-N plus S Basic Software Update Project was not scheduled to be finished until after the NRC inspection in 2011, therefore, the NRC inspection team limited its review to completed supporting documents for the requirement, software design, implementation, and maintenance phases. (Note: this did not include testing or the test plans). Identify when this was completed or identify any activities yet to be completed, by procedure, and identify the schedule for completion.

JEXU-1042-1031, "MELTAC Platform Software Tools" (ADAMS Accession No. ML15118A661):

1. Page 4, List of Software Tools Category Used in Each Phase:
  - a. In order for the NRC staff to evaluate software tools for compliance with IEEE 7-4.3.2, Section 5.3.2, we will need to understand what the tools are used for as well as what functions they perform in relation to the MELCO safety software development processes. The software tools listed in Table 1 are not consistent with names of the software tools provided in Section 5.0, Detailed Description of Processes. Please clarify the specific function of the tools and identify what document describes the function of each tool. The response should include a description of what the rules are for using the tool correctly and what configurations or options are recommended or advised against.
    - i. By further example of what the NRC staff needs to understand is the functions of the Engineering Tool. Section 4.1.4.1, Function Description of the TR, states the functional block diagrams are converted to graphical block diagrams by the MELTAC engineering tool. Section 5.7, MELTAC Engineering Tool, does not describe this function. Please explain.
  - b. Please provide an assessment of how each tool conforms to the software tools criteria of IEEE 7-4.3.2, Section 5.3.2 for the tools listed below:
    - i. [                      ]
    - ii. [                      ]
  - c. Identify the lifecycle phases that the MIC will be used in as was done with the other software tools on Table 1.

- d. Clause 5.3.2 of IEEE 7-4.3.2 specifies that software tools used to support software development are controlled under a configuration management plan. To evaluate compliance with this requirement, the NRC needs to review plans and procedures for establishment and maintenance of tool configuration control. Please provide documentation to show how tool configurations are controlled and Identify procedures used to maintain tool configuration control.
2. Page 15, Section 5.0, of this document, "Detailed Description of Processes," does not identify the procedure used to initially select, track, and maintain the specific software tool suppliers that are identified in this section. BTP 7-14, B.3.1.11.2, states that the a description of the process used to maintain and track purchased items, such as software tools used to make the final product should be provided. BTP 7-14 goes on to state this qualification procedure should be provided, and a method of tracking tool history, bug lists, and errata sheets should enable tracking which design outputs may be affected. Please provide this qualification procedure on the docket for NRC staff review.
3. [ ], Page 23, Section 5.8.2.2 "Verification & Validation (V&V) Method," of this document states the same V&V process applies to the MIC tool as the safety system software per the MELTAC Platform Software Program Manual (SPM). The NRC staff needs to understand the applicability of the SPM to the MIC and the Appendix B process. Therefore, provide the final V&V Report, per Section 3.10.4.8 of the MELTAC Platform Software Program Manual, which was completed for the MIC tool on the docket. Also, please reference and provide the procedure which includes the instructions for completing the V&V report for software tools.
  - a. Section 5.8.1 of this description identifies the MIC function of the MELENS software is developed and managed under Appendix B but the previous page and Section 5.7 states the MELENS software is developed as non-safety. The NRC staff requests the description of [ ]. How is separation maintained for development and maintenance purposes? Is there a separate sign-on for access to the MIC function?
4. Criterion V of Appendix B of 10 CFR Part 50 requires, in part, "Activities affecting quality shall be prescribed by documented instructions," and this Criterion also states "Instructions shall include appropriate acceptance criteria." (See RAI 2 of JEXU-1041-1008). In this document, Page 24, Section 5.9.2, 2), states: "[ ]" Provide the V&V procedure that describes the acceptance criteria used to determine the write operation of the tool is successful by reading the result of the tools listed.
5. The NRC staff needs a clear understanding of where 10 CFR Part 50 Appendix B applies and where is it not applicable in order to complete the evaluation. [ ]

JEXU-1041-1018, "Summary of Compliance to the IEEE Std. 603 and IEEE Std. 7-4.3.2"  
(ADAMS Accession No. ML15149A310):

1. Regarding page 10, Table 3, of this document, IEEE 603, 5.11, Identification. Does MELCO have an identification system of hardware and software applied during the design and manufacturing of the generic platform? If so this requirement applies and the NRC needs to evaluate how it is implemented. Please provide a description of platform hardware and software identification methods to demonstrate compliance with this requirement.
2. Also on page 10, Table 3, IEEE 603, 5.14, Human Factors. This requirement includes how certain safety system design goals should be met in accordance with IEEE 1023. This includes maintenance of the displays (safety VDUs) which provides assembly/disassembly, tools required and interchangeability of parts as well as features to prevent incorrect assembly. The staff requests information including an explanation of why such an evaluation would not be required on a generic basis (versus application specific) for the safety VDUs.
3. Page 12, Table 3, IEEE 603, 6.6 and 6.7, Operating and Maintenance Bypasses. Confirm for the NRC staff that the generic platform has the capability to complete these two requirements. It is understood by the NRC staff that specific operating bypasses are defined on a plant specific basis as well as plant specific Technical Specifications govern the use of the maintenance bypass feature.

JEXU-1041-1015, "Conformance Analysis to ISG-04" (ADAMS Accession No. ML14269A141):

1. With regards to the response to Staff Position 2; the last sentence of staff position 2 is not addressed, that is "This protection must be sustained despite any operation, malfunction, design error, communication error, or software error or corruption existing or originating outside the division." Please provide additional information to demonstrate compliance with this position.
2. With regards to the response to Staff Position 3; is the "vital communication" division voting logic the only input coming from outside the division (i.e., request for actuation coming from the other divisions)? If not what are the other inputs coming from outside the division that is necessary for the generic platform?
3. With regards to the response to Staff Position 4; this is the only place the communications processor is a "to be determined" processing technology. Discussion within this section and the topical report, such as section 4.3.3.5.1, "Detailed Data Flow," identifies this as a [ ]. The NRC staff requires the technology of the communications processor to be determined and consistent with the design, process, and procedures. If this processor is yet to be determined, or is being changed, the NRC staff needs to be notified of the changes.
4. With regards to the response to Staff Position 7, the NRC staff requires additional information on the characteristics of a predefined data set used in MELTAC

communication interfaces to support its safety evaluation. This information should include message formatting and protocol, message identification, status information, as well as signal attributes such as point of signal origin and destination. Include a discussion of how unrecognized messages are handled.

5. With regard to the response to Staff Position 10, the NRC staff requires the following:
  - a. A description of what constitutes a "temporary change"
  - b. The NRC staff requests the procedure describing how user configurable constants, such as setpoints, time delays, or instrument ranges will be changed with the CPU module mounted in the dedicated re-programming chassis.
6. With regard to the response to Staff Position 12, the NRC staff does not have information needed to perform an evaluation of faults 1 through 12 identified in this staff position. Please provide a discussion of how each of these faults as well as any additional identified communications faults will be handled by the MELCO safety platform and identify any application specific features needed to support system response to such faults.

JEXU-1041-1025, "Summary of MELTAC Platform QA," Rev. 1 (ADAMS Accession No. ML15090A625):

1. Criterion XVIII, Audits, of 10 CFR Part 50 Appendix B states, in part, "audits shall be carried out to verify compliance with all aspects of the quality assurance program." This Criterion goes on to state "Audits shall be performed in accordance with check lists by appropriately trained personnel not having direct responsibility in the areas of the audit." Also, the Criterion states: "Followup action, including reaudit of deficient areas, shall be taken where indicated."

The NRC Inspection (ADAMS Accession No. ML12013A353) was limited to assess MELCO's compliance to selected portions of 10 CFR Part 50 Appendix B. Also the NRC staff review is not intended to determine compliance of the MELCO ESC QAP program to all the requirements of 10 CFR Part 50 Appendix B or 10 CFR Part 21. Rather the intent of this review is to determine if the elements of the MELTAC Platform hardware and software meet the regulatory requirements necessary to reach a reasonable safety determination. Many of the elements have their basis within the Criteria of 10 CFR Part 50 Appendix B and should be reviewed and identified in Appendix B supplier audits. Since MELCO has not fully developed and manufactured a complete MELTAC platform under its 10 CFR Part 50 Appendix B program the staff must understand the many issues identified during Mitsubishi Heavy Industries (MHI) Appendix B audits of MELCO. Please provide the resulting corrective actions for issues identified during the following MHI Appendix B audits of MELCO:

- a.
  - i. [ ]
  - ii. [ ]
  - iii. [ ]

- b. Also, provide the Appendix B audit and the corrective actions from this audit as well; [                      ].
2. Per ISG-06, Section D.2.2, the review of the NRC staff is predicated on an Appendix B compliant organization and therefore, the hardware should be dedicated in accordance with Appendix B compliant processes. This information would be in commercial grade dedication plans and reports. As identified by the NRC inspection report (ADAMS Accession No. ML12013A353), a pilot commercial grade dedication of two modules was performed since MELCO had not fully developed a complete MELTAC platform under its Appendix B program. Due to the critical nature of this one report demonstrating an Appendix B compliant process for recurring commercial grade dedication, the NRC staff requests that pilot dedication documentation JEXU-1030-1001, "S MDOJ-03/04 Commercial Grade Item Technical Evaluation," be submitted on the docket.

JEXU-1041-1023, "Summary of MELTAC Platform Equipment Qualification," Rev. 2, (ADAMS Accession No. ML16050A199):

1. Results of the testing is identified only as "acceptance criteria was met," or "test results will be added to this section upon test completion." The results should identify any failures occurring during the test as well as the changes and/or modifications that were made to the modules or the testing to complete the test satisfactorily.
2. The NRC staff needs to know the specific modules, by part number and version, included in the Equipment-under-Test (EUT) setup. Descriptions such as "performed with a MELTAC cabinet fully loaded with most, but not all, MELTAC components" and "performed with a MELTAC cabinet fully equipped with a typical configuration of the MELTAC components required for the safety protection system" do not identify the necessary information on the modules, part numbers or revisions that were qualified.
3. Many of the tests were performed per MIL-STD-461. This standard has two accompanying standards on the information that should be included in a test procedure and a test report (Document numbers: DI-EMCS-80201B and DI-EMCS-80200C, respectively). This could be used as guidance to identify different types of information that could be presented in a summary document.
4. Per ISG-06, Section D.5.2 "Information to be Provided," states that the Summary of Testing Results should be provided during Phase 2 which requires submittal 12 months prior to requested approval. In light of MELCO's phased redevelopment of modules including redesign and testing, please identify when the test results will be submitted for all modules. Per the lack of information identified in the EQ Summary document as noted in RAIs 1 – 3 above, the NRC may have to request the actual test procedures and reports to be submitted on the docket for the equipment qualification review.



## **PART 3-1**

### **Responses to RAI, including:**

Transmittal Letter, dated July 21, 2016

Transmittal Letter, dated August 10, 2016

JEXU-1041-2061 R0 (Response to TR RAI 1)

JEXU-1041-2062 R0 (Response to TR RAI 2)

JEXU-1041-2063 R0 (Response to TR RAI 3)

JEXU-1041-2064 R0 (Response to TR RAI 4)

JEXU-1041-2065 R0 (Response to TR RAI 5)

JEXU-1041-2066 R0 (Response to TR RAI 6)

JEXU-1041-2067 R0 (Response to TR RAI 7)

JEXU-1041-2068 R0 (Response to TR RAI 8)

JEXU-1041-2069 R0 (Response to TR RAI 9)

JEXU-1041-2085 R0 (Response to ISG04CA RAI 5)



July 21, 2016  
ARQ-16P002-A

Document Control Desk  
U.S. Nuclear Regulatory Commission  
11555 Rockville Pike  
Rockville, MD 20852-2738

Attention: Mr. Joseph Holonich

**SUBJECT: MELCO's response to the item No.1 for JEXU-1041-1025 "Summary of MELTAC Platform QA" of MELTAC Topical Report Revision 0 RAI#1 (TAC No.MF4882)**

With this letter, Mitsubishi Electric Corporation (MELCO) submits the documents listed in the enclosures table below to the U.S. Nuclear Regulatory Commission (NRC).

Enclosed are the documents that make up the response to the item No.1 for JEXU-1041-1025 "Summary of MELTAC Platform QA" of MELTAC Topical Report Revision 0 RAI#1 (TAC No.MF4882). As indicated in the enclosed materials, these documents contain information that MELCO considers proprietary, and therefore should be withheld from public disclosure pursuant to 10 C.F.R 2.390 (a)(4) as trade secrets and commercial or financial information which is privileged or confidential.

The proprietary information contained within these documents is extensive and non-proprietary versions of these documents will not be prepared. The accompanying affidavit, Enclosure (1) sets forth the basis on which the information identified as proprietary should be withheld from public disclosure.

Sincerely,

Hideki Matsui  
QA Manager, Energy Systems Center  
Mitsubishi Electric Corporation

**Enclosures:**

No.	Document Number	Document Title	Date of Issue
1		Affidavit of Hideki Matsui	07/21/2016
2	JEXU-1041-2087	Response to Request for Additional Information	07/20/2016
3	PQG1-HD-21005	Audit report on MELTAC	04/22/2009
4	PQG1-HD-21021	Audit report of MELCO on January 28, 2010	01/28/2010
5	PQG-HD-22021	Audit report of MELCO on July 7, 2010	07/07/2010
6	UEQ-20130381 Rev.0	Audit report of vendor quality assurance program	06/19/2013
7	JEXU-1012-6321-C	Corrective action plan and Corrective action report for Finding 1 in PQG1-HD-21005	10/27/2010
8	JEXU-1012-6322-E	Corrective action plan and Corrective action report for Finding 2 in PQG1-HD-21005	10/27/2010
9	JEXU-1012-6323-D	Corrective action plan and Corrective action report for Finding 3 in PQG1-HD-21005	01/11/2011
10	JEXU-1012-6324-D	Corrective action plan and Corrective action report for Finding 4 in PQG1-HD-21005	10/27/2010
11	JEXU-1012-6324-E	Corrective action plan and Corrective action report for Finding 4 in PQG1-HD-21005	10/27/2010
12	ARQ-09Q003-C	Corrective action plan and Corrective action report for Finding 1 in PQG1-HD-21021	09/30/2010
13	ARQ-09Q004-C	Corrective action plan and Corrective action report for Finding 2 in PQG1-HD-21021	09/30/2010
14	ARQ-09Q005-C	Corrective action plan and Corrective action report for Finding 3 in PQG1-HD-21021	09/30/2010
15	ARQ-09Q006-C	Corrective action plan and Corrective action report for Finding 4 in PQG1-HD-21021	09/30/2010
16	ARQ-09Q007-C	Corrective action plan and Corrective action report for Finding 5 in PQG1-HD-21021	09/30/2010
17	ARQ-09Q008-C	Corrective action plan and Corrective action report for Finding 6 in PQG1-HD-21021	09/30/2010
18	ARQ-09Q009-C	Corrective action plan and Corrective action report for Finding 7 in PQG1-HD-21021	09/30/2010
19	ARQ-09Q010-C	Corrective action plan and Corrective action report for Finding 8 in PQG1-HD-21021	09/30/2010
20	ARQ-09Q011-D	Corrective action plan and Corrective action report for Finding 9 in PQG1-HD-21021	10/01/2010
21	ARQ-09Q012-C	Corrective action plan and Corrective action report for Finding 10 in PQG1-HD-21021	09/30/2010
22	ARQ-09Q013-C	Corrective action plan and Corrective action report for Finding 11 in PQG1-HD-21021	09/30/2010
23	ARQ-09Q014-C	Corrective action plan and Corrective action report for Finding 12 in PQG1-HD-21021	09/30/2010

ARQ-16P002-A

No.	Document Number	Document Title	Date of Issue
24	ARQ-10Q003-B	Corrective action plan and Corrective action report for Finding 1 in PQG-HD-22021	08/26/2011
25	ARQ-10Q004-C	Corrective action plan and Corrective action report for Finding 2 in PQG-HD-22021	06/23/2011
26	ARQ-10Q005-C	Corrective action plan and Corrective action report for Finding 3 in PQG-HD-22021	06/23/2011
27	ARQ-10Q006-C	Corrective action plan and Corrective action report for Finding 4 in PQG-HD-22021	08/26/2011
28	ARQ-10Q007-C	Corrective action plan and Corrective action report for Finding 5 in PQG-HD-22021	08/02/2011
29	ARQ-10Q008-B	Corrective action plan and Corrective action report for Finding 6 in PQG-HD-22021	12/02/2011
30	ARQ-10Q009-C	Corrective action plan and Corrective action report for Finding 7 in PQG-HD-22021	11/02/2011
31	ARQ-10Q010-B	Corrective action plan and Corrective action report for Finding 8 in PQG-HD-22021	06/23/2011
32	ARQ-10Q011-B	Corrective action plan and Corrective action report for Finding 9 in PQG-HD-22021	06/23/2011
33	ARQ-10Q012-C	Corrective action plan and Corrective action report for Finding 10 in PQG-HD-22021	06/23/2011
34	ARQ-13D002-A	Corrective action plan and report for Finding 1 in UEQ-20130381 Rev.0	01/28/2014
35	ARQ-13D003-A	Corrective action plan and report for Finding 2 in UEQ-20130381 Rev.0	02/25/2014
36	ARQ-13D004-A	Corrective action plan and report for Finding 3 in UEQ-20130381 Rev.0	01/28/2014
37	ARQ-13D005-A	Corrective action plan and report for Finding 4 in UEQ-20130381 Rev.0	01/28/2014

CC: Gilbert W. Remley  
Nuclear Systems Department Manager  
Mitsubishi Electric Power Products, Inc

ARQ-16P002-A



Aug 10, 2016  
JEXU-1041-8522

Document Control Desk  
U.S. Nuclear Regulatory Commission  
11555 Rockville Pike  
Rockville, MD 20852-2738

Attention: Mr. Joseph Holonich

**SUBJECT: MELCO's responses to MELTAC Topical Report Revision 0 RAI #1 (TAC No.MF4228)  
(Regarding items No.1 through No.9 for JEXU-1041-1008, Topical Report, and item  
No.5 for JEXU-1041-1015, "Conformance Analysis to ISG-04")**

With this letter, Mitsubishi Electric Corporation (MELCO) submits the documents listed in the enclosures table below to the U.S. Nuclear Regulatory Commission (NRC).

Enclosed are the documents that make up the response to items No.1 through No.9 for JEXU-1041-1008, Topical Report; and item No.5 for JEXU-1041-1015, "Conformance Analysis to ISG-04". As indicated in the enclosed materials, these documents contain information that MELCO considers proprietary, and therefore should be withheld from public disclosure pursuant to 10 C.F.R 2.390 (a)(4) as trade secrets and commercial or financial information which is privileged or confidential.

The accompanying affidavit, Enclosure (1) sets forth the basis on which the information identified as proprietary should be withheld from public disclosure.

Sincerely,

Shigeru Sugitani  
Senior Manager, Control & Protection Systems Section  
Nuclear Power Department, Energy Systems Center  
Mitsubishi Electric Corporation

**Enclosures:**

No.	Document Number	Document Title	Date of Issue
1	-	Affidavit of Shigeru Sugitani	08/10/2016
2	JEXU-1041-2061-P	1 for JEXU-1041-1008, "Safety Digital Platform - MELTAC-"	08/10/2016
3	JEXU-1041-2061-NP		
4	JEXU-1041-2062	2 for JEXU-1041-1008, "Safety Digital Platform - MELTAC-"	08/10/2016
5	JEXU-1041-2063	3 for JEXU-1041-1008, "Safety Digital Platform - MELTAC-"	08/10/2016
6	JEXU-1041-2064	4 for JEXU-1041-1008, "Safety Digital Platform - MELTAC-"	08/10/2016
7	JEXU-1041-2065-P	5 for JEXU-1041-1008, "Safety Digital Platform - MELTAC-",	08/10/2016
8	JEXU-1041-2065-NP		
9	JEXU-1041-2066-P	6 for JEXU-1041-1008, "Safety Digital Platform - MELTAC-"	08/10/2016
10	JEXU-1041-2066-NP		
11	JEXU-1041-2067-P	7 for JEXU-1041-1008, "Safety Digital Platform - MELTAC-"	08/10/2016
12	JEXU-1041-2067-NP		
13	JEXU-1041-2068-P	8 for JEXU-1041-1008, "Safety Digital Platform - MELTAC-"	08/10/2016
14	JEXU-1041-2068-NP		
15	JEXU-1041-2069	9 for JEXU-1041-1008, "Safety Digital Platform - MELTAC-"	08/10/2016
16	JEXU-1041-2085-P	5 for JEXU-1041-1015, "MELTAC Platform ISG-04 Conformance Analysis"	08/10/2016
17	JEXU-1041-2085-NP		

CC: Gilbert W. Remley  
Nuclear Systems Department Manager  
Mitsubishi Electric Power Products, Inc



---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

8/10/2016

**SAFETY SYSTEM DIGITAL PLATFORM  
- MELTAC (MITSUBISHI ELECTRIC TOTAL ADVANCED CONTROLLER) -  
TOPICAL REPORT**

**Mitsubishi Electric Corporation**

**TAC NO.:** MF4228  
**RAI NO.:** #1  
**DATE OF RAI ISSUE:** 6/29/2016

---

**QUESTION NO.:** 1 for JEXU-1041-1008, "Safety System Digital Platform – MELTAC"

Title 10 of the *Code of Federal Regulations* (10 CFR) Part 50, "Domestic Licensing of Production Utilization Facilities, establishes fundamental regulatory requirements. Specifically, Appendix B, "Quality Assurance Criteria," Criterion II, "Quality Assurance Program," states, in part; "This program shall be documented by written policies, procedures, or instructions." Page 0-6 of the TR states "the information provided in this report covers the life cycle and the Quality Assurance Program (QAP) of the MELTAC platform." In other inferences throughout the document, there are references to "10 CFR Part 50 Appendix B QAP" or just "QAP" or "MELCO QAP." The U.S. Nuclear Regulatory Commission (NRC) staff notes there is also a separate QAP for non-safety items. It is therefore unclear to the NRC staff how this requirement for specific written policies, procedures, or instructions is met and thus the staff is unable to make a regulatory compliance determination. Please provide information to identify each QAP by title, number, date and revision which is proposed to meet the requirements (or not) as stated by 10 CFR 50 Appendix B, Criterion II.

---

**ANSWER:**

The quality assurance programs mentioned in the ToR are the following two programs:

- "MELCO's 10 CFR 50 Appendix B QAP"  
This program is fully compliant with 10 CFR 50 Appendix B. The life cycle process of the MELTAC platform for use in US safety related applications is managed under this program. This program is also compliant with 10 CFR 21.  
[  
  
]  
- "MELCO's ISO9001 QAP"  
This program manages the life cycle process of the MELTAC platform for use in non-safety

applications and the life cycle process of the MELTAC engineering tool. This program is not proposed to meet the requirements stated in 10 CFR 50 Appendix B.

[

]

MELCO will revise Abstract, Section 1.0, Section 4.1 and Section 6 of ToR to reflect the clarification above, as shown in Attachment-1.

**Impact on Technical Report**

The answer above will be added to MELTAC Platform Software Program Manual (see Attachment-2).

The answer above will be added to MELTAC Platform ISG-04 Conformance Analysis.(see Attachment-3).

## Abstract

This Topical 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 can be used for safety and non-safety Instrumentation and Control (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 operating experience in various non-safety system applications such as the reactor and turbine control systems in PWR nuclear power plants operating in Japan. Based on its excellent performance in numerous non-safety applications, the MELTAC platform has now been applied to almost all non-safety and safety systems throughout Japanese PWR nuclear power plants. The MELTAC platform has also been applied for plant-wide digital upgrades in several Japanese PWR nuclear power plants that have been completed and those currently in progress.

The goal of this report is to seek a favorable Safety Evaluation from the U.S. Nuclear Regulatory Commission (NRC) for the use of the MELTAC platform for nuclear safety systems in operating plants and new plants.

For applications in the US, this report demonstrates conformance of the MELTAC platform 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 for nuclear safety systems:

- The detailed description of the hardware and software of the MELTAC platform, including digital processing, human systems interfaces (HSI) and digital communication interfaces and the detailed description of the MELTAC application development tools
- The equipment qualification of the MELTAC platform and its conformance to the corresponding U.S. standards
- The life cycle process and the Quality Assurance Program (QAP) of the MELTAC platform and conformance to U.S. regulatory criteria
- The equipment reliability of the MELTAC platform and how that reliability is used to determine the reliability of any MELTAC safety application

ToR-1

ToR-1

The MELTAC [platform](#) was developed under a Japanese ~~QAP~~[quality assurance program compliant with ISO9001](#), and has undergone a one-time commercial grade dedication (CGD) by MELCO for use in US safety related applications. The details of that CGD program are provided in this report by reference. The MELTAC [platform](#) is now maintained and manufactured under [MELCO's quality assurance program compliant with 10 CFR 50 Appendix B](#) ("MELCO's 10 CFR 50 Appendix B QAP"), and 10 CFR 21.

ToR-1

ToR-1

Prior to implementing the MELTAC commercial grade dedication program, MELCO developed and adopted ~~the MELCO's 10 CFR 50 Appendix B QAP~~[a nuclear QAP in compliance with 10 CFR 50 Appendix B and 10 CFR 21](#). MELCO has undergone an inspection by NRC to verify the implementation of an adequate [quality assurance program](#) ~~QAP~~ in compliance with the requirements of 10 CFR 50 Appendix B and 10 CFR 21 in support of digital I&C development activities. The results of this NRC inspection are documented in NRC Inspection Report NO. 99901410/2011-202 (ADAMS Accession number ML12013A353). In NRC Inspection Report NO. 99901410/2011-202, the NRC inspection team concluded that MELCO is effective in implementing its ~~QA~~[10 CFR 50 Appendix B program](#) and 10 CFR ~~Part~~ 21 programs in support of the MELTAC platform development. The Inspection Report stated that the NRC inspectors determined that MELCO's commercial grade dedication process adequately identified and verified the critical characteristics of the MELTAC platform that provide assurance that the platform will perform its safety function satisfactorily. The Inspection Report also stated that the NRC inspectors determined that the process implemented by MELCO is consistent with regulatory requirements associated with software development. The nonconformance identified in the Inspection Report has been corrected.

ToR-1

ToR-1

MELCO also underwent a successful audit by the NRC Office of New Reactors (NRO). This NRO audit focused on reviewing the design details related to the MELTAC platform to assist in making the determination that the specifications for the digital platform to be used for the implementation of the safety I&C systems, which reflect the MELTAC platform, meet the regulatory requirements. The results of the NRO audit are documented in the "Digital Instrumentation and Controls Design Audit Report" (ADAMS Accession number ML12291A673).

The information in this Topical Report 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 future licensing submittals. 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 Topical Report.

### 3.0 APPLICABLE CODE, STANDARDS AND REGULATORY GUIDANCE

This section identifies conformance to applicable codes, standards, and regulatory guidance required by NUREG-0800 and ISG-06. Unless specifically noted, the latest version issued on the date of this Topical Report is applicable.

Appendix D shows the compliance matrix of codes, standards, and regulatory guidance required by NUREG-0800 and ISG-06. Also, Appendix D points to the corresponding location within this Topical Report that describes design information related to the applicable codes, standards, and regulatory guidance of the MELTAC platform.

#### Code of Federal Regulations

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

ToR-1

##### GDC 1: Quality Standards and Records

The lifecycle process for the Basic components of the MELTAC platform that meets all requirements of 10 CFR ~~Part~~ 50 Appendix B and 10 CFR 21 is described in Section 6. This is referred to as ~~the MELCO's quality assurance program compliant with 10 CFR 50 Appendix B and 10 CFR 21 (MELCO's 10 CFR 50 Appendix B QAP), which is also described in "Quality Manual based on U.S. Nuclear Regulations" (ESC Procedure N-G000-P)~~ App.B-based quality assurance program (QAP).

ToR-1

The MELTAC platform was developed under a Japanese quality assurance QA program compliant with ISO9001 (MELCO's ISO9001 QAP) and has undergone a one-time commercial grade dedication (CGD) by MELCO for use in US safety-related applications. The details of that CGD program are provided in this report by reference. MELTAC is now maintained and manufactured under MELCO's 10 CFR 50 Appendix B QAP.

ToR-1

##### GDC 2: Design Bases for Protection against Natural Phenomena

This Equipment is seismically qualified. The Equipment must be located within building structures that provide protection against other natural phenomena. Specific buildings and Equipment locations are described in Application Licensing Documentation.

##### GDC 4: Environmental and Dynamic Effects Design Bases

This Equipment is qualified for use in a mild environment that is not adversely affected by plant accidents as described in Section 5.

##### GDC 21: Protection System Reliability and Testability

This Equipment includes automated testing with a high degree of coverage, and additional overlapping manual test features for the areas that are not covered by automated tests. All manual tests may be conducted with the plant on line, with consideration of plant specific accessibility, and with the Equipment bypassed or out of service. Depending on the system design for a specific plant, the

Section 6 describes ~~the~~ [MELCO's 10 CFR 50 Appendix B QAP App.B-based QAP](#), which is fully compliant to 10 CFR 50 Appendix B.

ToR-1

MELCO has undergone an inspection by NRC to verify the implementation of an adequate QAP.

(h) Invokes IEEE Std. 603-1991

See conformance to IEEE Std. 603-1991

### NRC Regulatory Guides

3. RG 1.22 Periodic Testing of Protection System Actuation Functions (Rev. 0, February 1972)  
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.
4. RG 1.29 Seismic Design Classification (Rev. 4, March 2007)  
The Equipment is designated Seismic Category I.
5. RG 1.53 Application of the Single-Failure Criterion to Safety Systems (Rev. 2, November 2003)  
endorses IEEE Std. 379-2000  
See conformance to GDC 21 and 24. This Equipment can be configured at the application level so that safety functions are designed with N or N+1 divisions. Each safety division can be independent from the other safety divisions and from non-safety divisions. Independence ensures that credible single failures cannot propagate between divisions within the system and therefore cannot prevent proper protective action at the system level. Single failures considered in the divisions are described in the Failure Mode and Effect Analysis (FMEA) for each system. The FMEA method for the components of this Equipment is provided in this Topical Report. The MELTAC module level FMEA report is incorporated by reference. The module level FMEA provides input to the system level FMEA for each application. The system level FMEA is described in Application Licensing Documentation.
6. RG 1.75 Criteria for Independence of Electrical Safety Systems (Rev. 3, February 2005)  
endorses IEEE Std. 384-1992  
The MELTAC platform contains features to ensure that redundant safety divisions are physically and electrically independent of each other and physically and electrically independent of any non-safety divisions. Physical independence is maintained either by the required distance or by barriers which prevent propagation of fire or electrical faults. Electrical independence is maintained by fiber optic cable communication interfaces or conventional isolators, such as opto-couplers, relays or transformers. Conventional isolators include fault



#### 4.1.4 MELTAC Engineering Tool

The MELTAC engineering tool provides various functions aimed at steadier and more efficient software management during all system life cycle phases (including design, fabrication, test, adjustment and maintenance).

The MELTAC engineering tool is used to generate safety application software for the MELTAC controller, but the tool itself is non-safety software running on a non-safety personal computer (PC) using the Microsoft Windows Operating System. The MELTAC engineering tool was developed in accordance with [MELCO's QAP compliant with ISO9001 \(MELCO's ISO9001 QAP\)](#)~~the MELCO QAP~~ for non-safety items. Safety application software generated by the MELTAC engineering tool must be qualified by independent V&V. Access is controlled by means of the PC password (BIOS, OS) and the MELTAC engineering tool password.

ToR-1

The application software execution data generated by the MELTAC engineering tool is downloaded to the controller via the Maintenance Network and is stored in the F-ROM of the CPU Module. The functions of the MELTAC engineering tool are described as follows.

##### 4.1.4.1 Function Description

###### a) Creation of Application Software

FBDs that are created with a commercial Mitsubishi CAD software package called "RAPID" can be automatically converted to GBDs by the MELTAC engineering tool. (Access to RAPID is also controlled by a password.)

The MELTAC engineering tool is then used to automatically generate (compile) the application software execution data directly from the GBD.

This automated process eliminates human translation errors.

GBDs can also be manually created (drawn), based on legacy FBDs provided by the customer, using the MELTAC engineering tool's GUI editor.

Regardless of how the GBD is generated (automatically from RAPID or manually drawn with the MELTAC engineering tool's GUI editor), the assignment of GBDs to controllers and the assignment of I/O signals is manually configured using the MELTAC engineering tool.

GBDs (whether created automatically or manually) and the executable data output from the MELTAC engineering tool are confirmed through manual V&V activities.

###### b) Download

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

]

Table 4.1.7-1 MIC vs. SMC


[

]

The versions of the application software and the basic software are controlled through software configuration management. The application software is described in the Application Licensing Document. The basic software is controlled and maintained in accordance with [the MELCO's 10 CFR 50 Appendix B QAP](#) ~~App.B-based QAP~~ and "MELTAC Platform Software Program Manual" (JEXU-1041-1016).

ToR-1

The following table summarizes the software differences that can be detected by the MIC and SMC.

Table 4.1.7-2 Detectable Errors by the MIC and SMC



ToR-1

]

The periodic manual tests (the process input and output test, and the safety VDU test) ensure that the CPU is capable of executing instructions from both F-ROM for basic software and F-ROM for application software. This encompasses the instructions that control continuous self-diagnosis, and the instructions that control the safety functions of monitoring process

## 6.0 QUALITY ASSURANCE AND LIFE CYCLE

The MELCO quality assurance program (~~QAP~~) complies with 10 CFR 50 Appendix B (complies with ASME NQA-1-1994) and 10 CFR 21. This is referred to as ~~the MELCO's 10 CFR 50 Appendix B QAP~~ App-B based QAP.

ToR-1

The MELTAC platform was originally developed under the Japanese nuclear quality program that encompasses most of 10 CFR 50 Appendix B requirements. MELCO performed a re-evaluation of the MELTAC platform design and the design process based on the commercial grade dedication process in accordance with 10 CFR 21. This re-evaluation was performed by an independent MELCO organization that was not involved in the original MELCO development to ensure that the MELTAC platform has the technical characteristics and quality equivalent to a product originally developed under a 10 CFR 50 Appendix B program. This is referred to as the MELTAC Re-evaluation Program (MRP) (See Section 6.2). ~~The MELCO's 10 CFR 50 Appendix B QAP~~ App-B based QAP governed the re-evaluation of the previous MELTAC platform development, and governs all new MELTAC platform development or revisions that occur after this re-evaluation. The MRP (i.e.: one-time commercial grade dedication) established a baseline to demonstrate that the MELTAC platform has suitable technical characteristics and quality for nuclear safety applications in the U.S. MELTAC is now maintained as a 10 CFR Appendix B product.

ToR-1

MELCO has undergone an inspection by NRC to verify the implementation of an adequate quality assurance ~~QA~~ program in compliance with the requirements of 10 CFR 50 Appendix B and 10 CFR 21 in support of digital I&C development activities. The results of this NRC inspection are documented in NRC Inspection Report NO. 99901410/2011-202 (ADAMS Accession number ML12013A353). In this Inspection Report, the NRC inspection team concluded that MELCO is generally effective in implementing its 10 CFR 50 Appendix B program ~~QA~~ and 10 CFR 21 programs in support of the MELTAC platform development. It states that "the NRC inspectors determined that MELCO's commercial grade dedication process adequately identified and verified the critical characteristics of the MELTAC platform that provide assurance that the platform will perform its safety function satisfactorily". In addition, it states that "the NRC inspectors determined that the process implemented by MELCO is consistent with regulatory requirements associated with software development".

ToR-1

ToR-1

### 6.1 MELTAC Platform Life Cycle Plans and Activities

This section describes key elements of the life cycle process for the basic components (software and hardware) of the MELTAC platform, based on ~~the MELCO's 10 CFR 50 Appendix B QAP~~ App-B based QAP.

ToR-1

#### 6.1.1 Overview of the MELTAC Quality Assurance Program

The MELCO procedures applicable to software encompass the basic software, which includes the firmware and FPGAs on all MELTAC modules.

The MELCO procedures, processes and software life cycle for nuclear safety-related activities (hardware and software) comply with the applicable requirements given in Section 3 of this Topical Report, the "MELTAC Platform Software Program Manual" (JEXU-1041-1016), referred to here as SPM, 10 CFR 50 Appendix B, and ASME NQA-1-1994.

The SPM provides the generic plans that are followed under [MELCO's 10 CFR 50 Appendix B QAP](#)~~MELCO's App.B based QAP~~ for all activities related to the basic software life cycle conducted after the MRP. The SPM complies with the guidance of BTP 7-14 "Guidance on Software Reviews for Digital Computer-based Instrumentation and Control Systems". A summary of the basic software life cycle plans and activities is given in Table 6.1-1.

ToR-1

The QAP and software life cycle for plant specific nuclear safety-related system implementation (hardware and application software) is not described in this report.

**Table 6.1-1 MELTAC Life Cycle Plan/Activity Summary**

[illegible]

ToR-1




ToR-1

### 6.1.2 Secure Development Environment Management

The Secure Development Environment Management Program for the basic software complies with RG 1.152 as described in the SPM. The overall Secure Development Environment Management Program ensures:

- 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. This is described in further detail in Section 6.1.2.3.

These processes are applicable to the basic software and related documentations. The compliance assessment for the MELTAC platform and its life cycle development process, relative to RG 1.152, is provided in the SPM.

The security measures in the development process of the application software are described in the Application Licensing Document.

#### 6.1.2.1 Development/Storage Security Measures of the basic software

[

ToR-1

]


6.1.6 Obsolescence Management

This section describes the obsolescence management program for the MELTAC platform. MELCO uses hardware parts which have excellent production continuity. Regardless, the product service life for nuclear applications covers 20 to 30 years, so it is inevitable that many parts will become unavailable. The following sections summarize the process used to determine the availability of parts and the process used to evaluate and utilize different parts for substitution. All changes to the MELTAC platform are done under ~~the~~ [MELCO's 10 CFR 50 Appendix B QAP](#).~~MELCO App.B based QAP~~

ToR-1

The parts substitution method described in this section is primarily applicable to the obsolescence management. However, MELCO will also use the same method of parts substitution to ensure adequate parts supply from multiple sources to accommodate supply management issues or production peaks.

6.1.6.1 Obtaining Information on Part Availability

[

]

6.1.6.2 Selecting Replacement Parts

[

]

6.1.6.3 Verification after Replacement

[

]

6.1.7 Identification

[

ToR-1

ToR-1

ToR-1

]  
**6.1.8 Reliability Database**  
[

ToR-1

]

6.2 MELTAC Re-evaluation Program (MRP)

[

ToR-1

]

6.3 MELTAC Engineering Tool Life Cycle

The MELTAC engineering tool was developed and is managed under ~~the~~ MELCO's QAP compliant with ISO 9001 (MELCO's ISO9001 QAP) ~~MELCO-QAP~~ for non-safety items ~~(Complies with ISO 9001)~~. This is acceptable because the MELTAC engineering tool is not credited for any safety-related functions..

ToR-1

The MELTAC engineering tool will continue to be managed under ~~the~~ MELCO's ISO9001 QAP ~~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.

ToR-1



Design, Implementation, Test, and Operation and Maintenance). A Project Plan and a Master Test Plan are prepared before starting any project activities. A Project Plan may encompass multiple software changes and activities across multiple life cycle phases. A Master Test Plan summarizes the test activities to be performed in a project and their schedules.

### 3.1.2 Organization / Responsibilities

The basic software is developed through a combined effort of several technical sections within MELCO.

The ultimate responsibility for the development of the basic software lies with the "Design Section," which is responsible for assuring that it is structured, staffed, and qualified to meet the rigorous and technical demands for developing and maintaining the basic software.

Development of the basic software is performed by the Design Section in conjunction with the "QA Section", "V&V Team" and "Manufacturing Department".

The QA Section is responsible for assuring all activities conducted by MELCO throughout the MELTAC product life cycle (including activities of the Design Section, V&V Team and Manufacturing Department) follow the required regulations, standards, this SPM, and internal MELCO policies and procedures. QA audits are conducted independently from any activities or assessments of the Design Section, V&V Team or Manufacturing Department. MELCO maintains a 10 CFR 50 Appendix B ~~Q~~quality-~~A~~assurance ~~program~~Plan (MELCO's 10 CFR 50 Appendix B QAP) which is MELCO's quality assurance program compliant with 10 CFR 50 Appendix B and 10 CFR 21~~that is implemented via NQA-1.~~

ToR-1

The V&V Team executes independent V&V activities in accordance with the SVVP. The V&V Team is responsible for confirming the correctness of the basic software, including the portions of the software that are critical to safety functions.

The Manufacturing Department manufactures the MELTAC platform hardware modules and performs installation of the basic software on each hardware module during the production process.

The organization chart relating to MELTAC platform development and maintenance is described in Figure 3.1-1.

ToR-1

ToR-1

]

ToR-1

ToR-1

### 3.3 Software Quality Assurance Plan

#### 3.3.1 Purpose and Scope

The purpose of the Software Quality Assurance Plan (SQAP) is to describe the quality assurance requirements and methods used to assure high quality of the basic software throughout the basic software life cycle process.

The requirements of this SQAP as well as this entire SPM shall be implemented by procedures controlled in accordance with MELCO's 10 CFR 50 Appendix B Quality Assurance Program ([MELCO's 10 CFR 50 Appendix B](#) QAP). All responsible groups that are assigned activities described in this SPM shall follow these implementing procedures.

ToR-1

The quality of the following basic software life cycle process documents outputs shall be assured through the methods and processes described in this SQAP:

- Project Plan as described in the SMP
- Design documentation (Platform Specification, Software Specification, Program Specification, and FPGA Specification)
- Source code (for processor software and for FPGA)
- Test Descriptions, Test Specifications, and Test Reports (as described in the SVVP and the STP)

#### 3.3.2 Organization / Responsibilities

The organization of the groups responsible for basic software quality is described in Section 3.1.2.

The QA Section and the V&V Team shall be independent from Design Section and Manufacturing Department members. V&V Team independence is described in detail in the SVVP.

The class of the QA Manager within the overall MELCO organization hierarchy is equivalent or higher than the classes of all managers of any other organization.

The Design Section Manager is responsible for ensuring that all basic software design activities are performed as described in accordance with the SDP.

The Design Section shall generate and maintain the design outputs throughout the basic software life cycle as described in the SDP and shall also assure their correctness through reviews by Design Review Engineers.

The Design Section is responsible for performing the software safety analysis activities described in the SSP.

The V&V Team Manager is responsible for ensuring that all the V&V activities are executed independently by the V&V Team, including software safety analysis V&V activities, as described in the SVVP.

The QA Manager is responsible for assuring that the planned software development and V&V activities are appropriately conducted by these sections in accordance with this SPM and

3.1.4 Staff Position 4

Requirement
<p>The communication process itself should be carried out by a communications processor<sup>ii</sup> separate from the processor that executes the safety function, so that communications errors and malfunctions will not interfere with the execution of the safety function. The communication and function processors should operate asynchronously, sharing information only by means of dual-ported memory or some other shared memory resource that is dedicated exclusively to this exchange of information. The function processor, the communications processor, and the shared memory, along with all supporting circuits and software, are all considered to be safety-related, and must be designed, qualified, fabricated, etc., in accordance with 10 C.F.R. Part 50, Appendix A and B. Access to the shared memory should be controlled in such a manner that the function processor has priority access to the shared memory to complete the safety function in a deterministic manner.</p> <p>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.</p>
Analysis

ToR-1

3.3 Analysis of Command Prioritization (Section 2 of ISG-04)

This section provides an analysis of the MELTAC platform command prioritization features. The Staff Positions in ISG-04 Section 2 are used as criteria for this analysis.

The MELTAC platform includes a Power Interface (PIF) Module to implement priority logic. The PIF Module employs state-based priority logic to ensure that either the primary system (e.g. the safety system) or backup system (e.g. the Diverse Actuation System) can place the component in its preferred safety state. This state-based priority logic is implemented on an Interposing Logic (IPL) sub-board mounted on the PIF Module that controls the component in direct response to external contact inputs, independent of the MELTAC controller output commands. There are several types of IPL sub-boards for different types of plant components (e.g.: switchgears, solenoid valves, etc.). Each PIF Module is configured with the appropriate IPL sub-board for the component being controlled. The IPL is realized by discrete logic Integrated Circuits.

3.3.1 Staff Position 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	
{	

ToR-1



**3.3.7 Staff Position 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**

ToR-1

---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

8/10/2016

**SAFETY SYSTEM DIGITAL PLATFORM  
- MELTAC (MITSUBISHI ELECTRIC TOTAL ADVANCED CONTROLLER) -  
TOPICAL REPORT**

**Mitsubishi Electric Corporation**

**TAC NO.: MF4228**  
**RAI NO.: #1**  
**DATE OF RAI ISSUE: 6/29/2016**

---

**QUESTION NO.:** 2 for JEXU-1041-1008, "Safety System Digital Platform – MELTAC"

On page 2 of the TR, the following General Design Criteria (GDC) are also applicable to the Mitsubishi Electric Total Advanced Controller (MELTAC) platform. Please review criteria provided in these GDC's and describe how the platform satisfies each GDC. If regulatory compliance is dependent on application specific development activities, please state this.

- a. GDC 13 "Instrumentation and Control" is applicable. MELTAC and the qualified displays, with no identified limitations within the system descriptions, will monitor variables and systems during normal operations, Anticipated Operational Occurrences (AOOs) and accident conditions as well as those which affect the fission process and core pressure boundaries. Include a full explanation applicable to this GDC.
- b. GDC 20 "Protection System Functions" is applicable. MELTAC will automatically initiate reactivity control systems. Include a full explanation applicable to this GDC.
- c. GDC 25 "Protection system requirements for reactivity malfunctions" is applicable. The MELTAC platform will be used for safety and non-safety systems for reactivity control systems without limitations identified by the topical report. Also the capability to protect against reactivity control malfunctions is not an exception therefore this requirement should be included.

**ANSWER:**

MELTAC is a generic safety platform suitable for use in complying with the criteria in GDC 13, 20, 25. However, the configuration of the MELTAC platform to achieve that compliance is application dependent. Therefore, that configuration is described in plant specific application licensing documentation.

**Impact on Topical Report**

The answer above will be added to Section 3 of the Topical Report (see Attachment-1).

### 3.0 APPLICABLE CODE, STANDARDS AND REGULATORY GUIDANCE

This section identifies conformance to applicable codes, standards, and regulatory guidance required by NUREG-0800 and ISG-06. Unless specifically noted, the latest version issued on the date of this Topical Report is applicable.

Appendix D shows the compliance matrix of codes, standards, and regulatory guidance required by NUREG-0800 and ISG-06. Also, Appendix D points to the corresponding location within this Topical Report that describes design information related to the applicable codes, standards, and regulatory guidance of the MELTAC platform.

#### Code of Federal Regulations

1. 10 CFR Part 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 that meets all requirements of 10 CFR Part 50 Appendix B is described in Section 6. This is referred to as the App.B-based quality assurance program (QAP).

MELTAC was developed under a Japanese QA program and has undergone a one-time commercial grade dedication (CGD) by MELCO for use in US safety - related applications. The details of that CGD program are provided in this report by reference. MELTAC is now maintained and manufactured under MELCO's 10 CFR 50 Appendix B QAP.

##### GDC 2: Design Bases for Protection against Natural Phenomena

This Equipment is seismically qualified. The Equipment must be located within building structures that provide protection against other natural phenomena. Specific buildings and Equipment locations are described in Application Licensing Documentation.

##### GDC 4: Environmental and Dynamic Effects Design Bases

This Equipment is qualified for use in a mild environment that is not adversely affected by plant accidents as described in Section 5.

##### GDC 13: Instrumentation and control

The MELTAC platform is capable and suitable for providing monitoring and control functions to maintain variables and systems within prescribed operating ranges for normal operation, anticipated operational occurrences, and accident conditions to assure adequate safety. The monitoring and control functions implemented within the MELTAC platform that maintain the variables within the prescribed operating ranges are described in application licensing documentation.

ToR-2

##### GDC 20: Protection system functions

The MELTAC platform is capable and suitable for providing monitoring functions to sense anticipated operational occurrences and accident conditions, and to initiate and control the operation of appropriate systems(automatically and/or manually), including reactivity control systems and systems and components important to safety. The monitoring and control functions implemented within the MELTAC platform to perform these safety related functions are described in application licensing documentation.

ToR-2

#### GDC 21: Protection System Reliability and Testability

This Equipment includes automated testing with a high degree of coverage, and additional overlapping manual test features for the areas that are not covered by automated tests. All manual tests may be conducted with the plant on line, with consideration of plant specific accessibility, and with the Equipment bypassed or out of service. Depending on the system design for a specific plant, the Equipment is configured with N or N+1 redundancy, where N is the number of divisions needed for single failure compliance and to meet the plant reliability goals. For systems with N+1 redundancy, this GDC is met with one division continuously bypassed or out of service. The redundancy configuration for each plant system is described in Application Licensing Documentation.

#### GDC 22: Protection System Independence

Redundant divisions are physically and electrically isolated to ensure that failures that originate in one division cannot propagate to other divisions. Physical isolation is discussed in Application Licensing Documentation. Platform features to accommodate electrical isolation are discussed in this Topical Report.

All Equipment is qualified to ensure that the Equipment is unaffected by adverse conditions that may concurrently affect multiple divisions. The qualification limits of this equipment are described in this Topical Report. Application Licensing Documentation describes the specific analysis for each plant.

Interlocks between redundant divisions and administrative controls ensure maintenance is performed on one division at a time. Interlocks and administrative controls are described in Application Licensing Documentation.

#### GDC 23: Protection System Failure Modes

Signals are generated for all detected failures. These signals can be configured at the application level to generate alarms. Functions can be designed to fail to an actuated trip state on loss of all power, on failures that are not automatically detected, or on failures that are automatically detected and would prevent proper execution of the function. Functions can also be designed to fail to an unactuated state. The unactuated state may be desirable to avoid spurious plant transients. Compliance for reactor trip and engineered safety features actuation functions are application specific and described in Application Licensing Documentation.

#### GDC 24: Separation of Protection and Control Systems

The separation of protection and control systems is an application specific design characteristic. Redundant divisions of the protection systems are physically and electrically isolated from the non-safety control systems. Where safety sensors are shared between control and protection systems, signal selection logic is typically used in the control system to prevent erroneous control actions due to single sensor failures. Eliminating these erroneous control actions prevents challenges to the protection system while it is degraded due to the same sensor failure. Where non-safety signals control safety systems or components, logic in the safety systems is typically used to ensure prioritization of safety functions. The details regarding the separation of protection and control systems are described in Application Licensing Documentation.

GDC 25: Protection system requirements for reactivity control malfunctions

The MELTAC platform is capable and suitable for providing monitoring and control functions to assure that fuel design limits are not exceeded for any single malfunction of the reactivity control systems. The monitoring and control functions implemented within the MELTAC platform to perform this safety related function are described in application licensing documentation.

ToR-2

2. 10 CFR Part 50.55a

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

Section 6 describes the App.B-based QAP, which is fully compliant to 10 CFR 50 Appendix B.

MELCO has undergone an inspection by NRC to verify the implementation of an adequate QAP.

(h) Invokes IEEE Std. 603-1991

See conformance to IEEE Std. 603-1991

### NRC Regulatory Guides

3. RG 1.22 Periodic Testing of Protection System Actuation Functions (Rev. 0, February 1972)

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.

4. RG 1.29 Seismic Design Classification (Rev. 4, March 2007)

The Equipment is designated Seismic Category I.

5. RG 1.53 Application of the Single-Failure Criterion to Safety Systems (Rev. 2, November 2003)

endorses IEEE Std. 379-2000



---

## RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

---

8/10/2016

### SAFETY SYSTEM DIGITAL PLATFORM - MELTAC (MITSUBISHI ELECTRIC TOTAL ADVANCED CONTROLLER) - TOPICAL REPORT

Mitsubishi Electric Corporation

TAC NO.: MF4228  
RAI NO.: #1  
DATE OF RAI ISSUE: 6/29/2016

---

**QUESTION NO.:** 3 for JEXU-1041-1008, "Safety System Digital Platform – MELTAC"

With regard to TR page 17, item d), software is mentioned several times regarding the capabilities of the engineering tool. In each case, identify if this is referring to the application or platform software or both.

---

**ANSWER:**

i) "To store copies of **software** for all processors within the division, and to conduct the manually initiated Memory Integrity Check (MIC) using that stored **software**"  
The software described above means "application software and basic software".

This sentence will be revised as follows:

"To store copies of **application software and basic software** for all processors within the division, and to conduct the manually initiated Memory Integrity Check (MIC) using that stored **application software and basic software**"

ii) "To control the updating of **software** for any processor within the division, utilized only when a processor is taken out-of-service and declared inoperable by plant Technical Specifications and the processor CPU Module is removed and transferred to the dedicated Re-programming Chassis."

The software described above means "application software".

This sentence will be revised as follows:

"To control the updating of application software for any processor within the division, utilized only when a processor is taken out-of-service and declared inoperable by plant Technical Specifications and the processor CPU Module is removed and transferred to the dedicated Re-programming Chassis."

**Impact on Topical Report**

The answer above will be added to Section 4.0 of the Topical Report (see Attachment-1).

- 
- Control and drive the plant components and equipment by ESF actuation signal from the RPP
  - Receive ESF actuation signals from the RPP via the intra-division Control Network
  - Receive manual component control commands from the safety VDU processors via the intra-division Control Network
  - Receive diverse component control signals from the Diverse Actuation System (DAS), and combine the signals with the control signals from the PSS-CCPs within the hardware based Interposing Logic (IPL) of the Power Interface (PIF) Module to determine the final control command relayed to each plant component
  - Transmit the monitored status of interlocks and components to the safety VDU processors via the intra-division Control Network
- c) Each PSS division typically contains at least one safety VDU processor and safety VDU panel. The safety VDU processor and safety VDU panel consist of a special purpose MELTAC controller, peripherals, and an LCD touch screen. The safety VDU processor and safety VDU panel perform the following key functions:
- Transmit the operation signals to the RPP and PSS-CCPs via the intra-division Control Network, and can be configured to provide the human-machine interface
  - Receive plant sensor data, RT and ESF initiation, and actuation status from the RPP via the intra-division Control Network
  - Receive interlock and component status data from the PSS-CCPs via the intra-division Control Network
  - Receive touch commands from safety VDU panel
- d) There is one MELTAC engineering tool connected via Maintenance Network in each PSS division used exclusively for the following functions within that one division:
- To display self-test diagnostics reported from all PSS processors within the division
  - To store copies of application software and basic software for all processors within the division, and to conduct the manually initiated Memory Integrity Check (MIC) using that stored application software and basic software
  - To control the updating of application software for any processor within the division, utilized only when a processor is taken out-of-service and declared inoperable by plant Technical Specifications and the processor CPU Module is removed and transferred to the dedicated Re-programming Chassis
  - To control simulated input values for troubleshooting any processors within the division, only when a processor is taken out-of-service and declared inoperable by plant Technical Specification
- e) There is one Control Network in each PSS division used for the following key intra-division communication functions:
- Interlock and ESF initiation signals from the RPP to the PSS-CCPs
  - Manual control commands from the safety VDU processor to the RPP and the PSS-CCPs
  - Monitored plant sensor data, RT and ESF initiation, and actuation status from the RPP to the safety VDU processor
  - Monitored plant sensor data, interlock and component status data from the PSS-CCPs to the safety VDU processor
- f) There is one Data Link in each PSS division used for broadcasting RT and ESF initiation signals from one PSS division to each of the other divisions.

ToR-3

---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

8/10/2016

**SAFETY SYSTEM DIGITAL PLATFORM  
- MELTAC (MITSUBISHI ELECTRIC TOTAL ADVANCED CONTROLLER) -  
TOPICAL REPORT**

**Mitsubishi Electric Corporation**

**TAC NO.:** MF4228  
**RAI NO.:** #1  
**DATE OF RAI ISSUE:** 6/29/2016

---

**QUESTION NO.:** 4 for JEXU-1041-1008, "Safety System Digital Platform – MELTAC"

With regard to TR page 54, a) "Creation of Application Software." Criterion III, "Design Control," of 10 CFR 50 Appendix B states in part: "Design changes, including field changes, shall be subject to design control measures commensurate with those applied to the original design and be approved by the organization that performed the original design unless the applicant designates another responsible organization." To determine compliance with this criteria, the NRC staff needs to understand whether the Mitsubishi Electric Company (MELCO) development process described by this application will be used to perform design changes or if a different process to be developed by the licensee would be used. If a different process is to be used, then an application specific action item should be developed accordingly to make clear to the licensee that an appropriate safety-related development process must be established before the engineering tool is used to revise platform software.

---

**ANSWER:**

Section 4.1.4.1 a) of the Topical Report describes the two steps of the process involved with the creation of application software using the MELTAC engineering tool. The first step is creating FBDs through the usage of an application specific tool, or Mitsubishi's CAD software called "RAPID". The second step is converting FBDs to GBDs by using the MELTAC engineering tool. The process for the first step (Creation of FBDs) is application specific. MELCO will add this description to Section 4.1.4.1 a) of the Topical Report. Please see Attachment-1.

**Impact on Topical Report**

The answer above will be added to Section 4.1.4.1 of the Topical Report. (see Attachment-1)

#### 4.1.4 MELTAC Engineering Tool

The MELTAC engineering tool provides various functions aimed at steadier and more efficient software management during all system life cycle phases (including design, fabrication, test, adjustment and maintenance).

The MELTAC engineering tool is used to generate safety application software for the MELTAC controller, but the tool itself is non-safety software running on a non-safety personal computer (PC) using the Microsoft Windows Operating System. The MELTAC engineering tool was developed in accordance with the MELCO QAP for non-safety items. Safety application software generated by the MELTAC engineering tool must be qualified by independent V&V. Access is controlled by means of the PC password (BIOS, OS) and the MELTAC engineering tool password.

The application software execution data generated by the MELTAC engineering tool is downloaded to the controller via the Maintenance Network and is stored in the F-ROM of the CPU Module. The functions of the MELTAC engineering tool are described as follows.

##### 4.1.4.1 Function Description

###### a) Creation of Application Software

~~FBDs that are created with a commercial Mitsubishi CAD software package called "RAPID" can be automatically converted to GBDs by the MELTAC engineering tool. (Access to RAPID is also controlled by a password.)~~

~~The MELTAC engineering tool is then used to automatically generate (compile) the application software execution data directly from the GBD.~~

~~This automated process eliminates human translation errors.~~

~~GBDs iscan also be manually created (drawn), based on legacy FBDs provided by the customer, using t~~  
The MELTAC engineering tool's GUI editor can be used to manually create (draw) GBDs, which is then used to automatically generate (compile) the application software executable data directly from the GBD.

~~Regardless of how the GBD is generated (automatically from RAPID or manually drawn with the MELTAC engineering tool's GUI editor), t~~  
 The MELTAC engineering tool is used to configure the assignment of GBDs to controllers, and the assignment of I/O signals. GBDs (whether created automatically or manually) and the application software executable data output from the MELTAC engineering tool are confirmed through manual V&V activities.

The MELTAC engineering tool can also be used to automatically convert FBDs to GBDs if the FBD is created with Mitsubishi's CAD software "RAPID".

The conversion process from FBD to GBD is application specific, regardless of whether the process is automatic or manual. This process should follow the licensee's appropriate safety-related development process for revising application software.

###### b) Download

ToR-4

ToR-4

---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

8/10/2016

**SAFETY SYSTEM DIGITAL PLATFORM  
- MELTAC (MITSUBISHI ELECTRIC TOTAL ADVANCED CONTROLLER) -  
TOPICAL REPORT**

**Mitsubishi Electric Corporation**

**TAC NO.:** MF4228  
**RAI NO.:** #1  
**DATE OF RAI ISSUE:** 6/29/2016

---

**QUESTION NO.:** 5 for JEXU-1041-1008, "Safety System Digital Platform – MELTAC"

With regard to TR Page 55, e) In order to complete its evaluation of the MELCO platform the NRC staff needs to understand the temporary changes to field changeable process value in data table (Data Set). Please provide a description and examples of temporary changes to field changeable process values.

---

**ANSWER:**

[

]



Figure 1 Temporary Change to Data Table

[

]

**Impact on Topical Report**

The answer above will be added to Section 4.1.4.1 of the Topical Report (see Attachment-1).



] The correct download is confirmed by a different MELTAC engineering tool function that checks the F-ROM data as discussed below.

**c) Verifying F-ROM data**

The MELTAC engineering tool provides a manually initiated function which automatically compares the basic software and application software data in the F-ROM of the controller, bit by bit, with the basic software data and application software data stored in the MELTAC engineering tool. This function is used after a new download and during periodic surveillance tests to confirm that the data in F-ROMs is the same as the data in the MELTAC engineering tool, and therefore has not changed. This function can be used for the CPU Module while installed in the on-line Chassis because this does not make any changes to the F-ROM of the CPU Module.

ToR-6

**d) Controller failure diagnosis display**

The MELTAC engineering tool displays the self-diagnosis result of the controllers. It shows which module is in a failed state. This function can be used for the CPU Module while installed in the on-line Chassis because this does not make any changes to the F-ROM of the CPU Module.

ToR-6

**e) Temporary changes to the ~~field change eable process value in~~ data table (Data Set)**

[

ToR-6

ToR-6

ToR-5

ToR-6

]

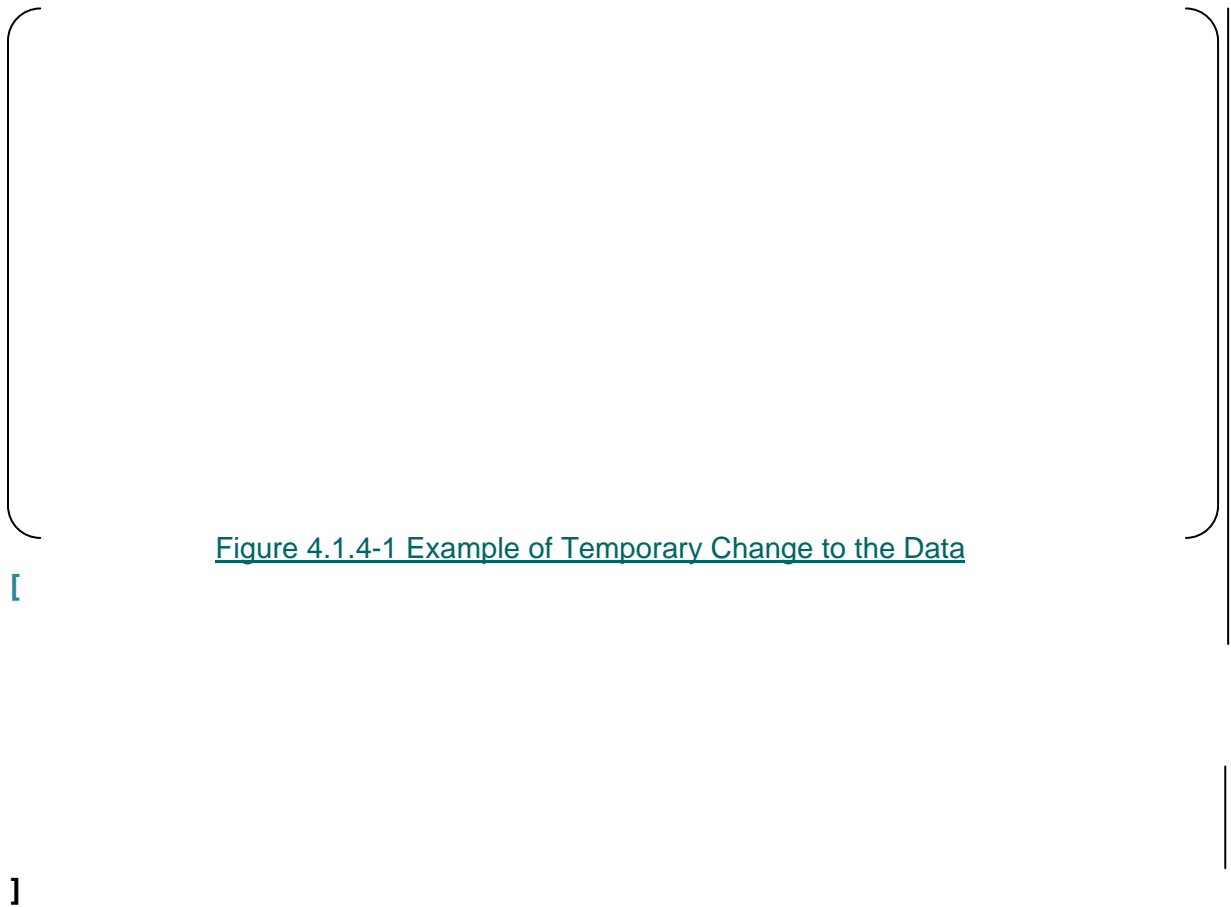


Figure 4.1.4-1 Example of Temporary Change to the Data

---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

8/10/2016

**SAFETY SYSTEM DIGITAL PLATFORM  
- MELTAC (MITSUBISHI ELECTRIC TOTAL ADVANCED CONTROLLER) -  
TOPICAL REPORT**

**Mitsubishi Electric Corporation**

**TAC NO.:** MF4228  
**RAI NO.:** #1  
**DATE OF RAI ISSUE:** 6/29/2016

---

**QUESTION NO.:** 6 for JEXU-1041-1008, "Safety System Digital Platform – MELTAC"

With regard TR Page 54, in Section 4.1.4.1, Function Description, subsection b) states this activity is done with the central processing unit (CPU) Module in the Re-programming Chassis and therefore the controller status is off line; however; subsections c), d), & e) do not include similar statements. Please provide additional information regarding controller status in relation to performing functions described in subsections c), d), & e).

---

**ANSWER:**

[

]

**Impact on Topical Report**

The answer above will be added to Section 4.1.4 of the Topical Report. See Attachment-1.

#### 4.1.4 MELTAC Engineering Tool

The MELTAC engineering tool provides various functions aimed at steadier and more efficient software management during all system life cycle phases (including design, fabrication, test, adjustment and maintenance).

The MELTAC engineering tool is used to generate safety application software for the MELTAC controller, but the tool itself is non-safety software running on a non-safety personal computer (PC) using the Microsoft Windows Operating System. The MELTAC engineering tool was developed in accordance with the MELCO QAP for non-safety items. Safety application software generated by the MELTAC engineering tool must be qualified by independent V&V. Access is controlled by means of the PC password (BIOS, OS) and the MELTAC engineering tool password.

The application software execution data generated by the MELTAC engineering tool is downloaded to the controller via the Maintenance Network and is stored in the F-ROM of the CPU Module. The functions of the MELTAC engineering tool are described as follows. [These functions can be used only when the controller isn't performing a safety function.](#)

ToR-6

##### 4.1.4.1 Function Description

###### a) Creation of Application Software

FBDs that are created with a commercial Mitsubishi CAD software package called "RAPID" can be automatically converted to GBDs by the MELTAC engineering tool. (Access to RAPID is also controlled by a password.)

The MELTAC engineering tool is then used to automatically generate (compile) the application software execution data directly from the GBD.

This automated process eliminates human translation errors.

GBDs can also be manually created (drawn), based on legacy FBDs provided by the customer, using the MELTAC engineering tool's GUI editor.

Regardless of how the GBD is generated (automatically from RAPID or manually drawn with the MELTAC engineering tool's GUI editor), the assignment of GBDs to controllers and the assignment of I/O signals is manually configured using the MELTAC engineering tool.

GBDs (whether created automatically or manually) and the executable data output from the MELTAC engineering tool are confirmed through manual V&V activities.

###### b) Download

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

]  
The correct download is confirmed by a different MELTAC engineering tool function that checks the F-ROM data as discussed below.

**c) Verifying F-ROM data**

The MELTAC engineering tool provides a manually initiated function which automatically compares the basic software and application software data in the F-ROM of the controller, bit by bit, with the basic software data and application software data stored in the MELTAC engineering tool. This function is used after a new download and during periodic surveillance tests to confirm that the data in F-ROMs is the same as the data in the MELTAC engineering tool, and therefore has not changed. This function can be used for the CPU Module while installed in the on-line Chassis because this does not make any changes to the F-ROM of the CPU Module.

ToR-6

**d) Controller failure diagnosis display**

The MELTAC engineering tool displays the self-diagnosis result of the controllers. It shows which module is in a failed state. This function can be used for the CPU Module while installed in the on-line Chassis because this does not make any changes to the F-ROM of the CPU Module.

ToR-6

**e) Temporary changes to the ~~field change eable process value in~~ data table (Data Set)**

[

ToR-6

ToR-6

ToR-5

ToR-6

]



---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

8/10/2016

**SAFETY SYSTEM DIGITAL PLATFORM  
- MELTAC (MITSUBISHI ELECTRIC TOTAL ADVANCED CONTROLLER) -  
TOPICAL REPORT**

**Mitsubishi Electric Corporation**

**TAC NO.:** MF4228  
**RAI NO.:** #1  
**DATE OF RAI ISSUE:** 6/29/2016

---

**QUESTION NO.:** 7 for JEXU-1041-1008, "Safety System Digital Platform – MELTAC"

DI&C-ISG-04, Section 1 Interdivisional Communications, Point 6, states the safety function processor should not accept interrupts from outside its own safety division. Page 56, third paragraph, states; [

] Provide information  
on how the engineering tool is prevented from disrupting the controller safety functions.

---

**ANSWER:**

[

]

**Impact on Topical Report**

The answer above will be added to Section 4.1.4.2 of the Topical Report. See Attachment -1.

#### 4.1.4.2 Network for the MELTAC Engineering Tool

In order to communicate between the MELTAC engineering tool and the controller, the Maintenance Network is used. The MELTAC engineering tool, which runs on a PC, is temporarily connected via the Maintenance Network to the System Management Modules of each controller in the division. This interface allows all functions described in Section 4.1.4.1. The Maintenance Network is temporarily connected to the controllers in the same safety division. There is a separate Maintenance Network for each division. There are no Maintenance Network interconnections between safety divisions. There is also a separate MELTAC engineering tool for each division. The specification of the Maintenance Network is described below.

For the configuration and the isolation of the Maintenance Network, see Section 4.3.4.

(Specification)

Function: Transmission of maintenance data for MELTAC engineering tools

- Transmission protocol: Ethernet (IEEE Std. 802.3; CSMA / CD, UDP/IP)
- Transmission speed: 100 Mbps/10 Mbps
- Communication form: Dialog communication
- Connection form: Bus/Star-type

Transmission media: UTP Category 5 cable  
Optical fiber (Multi mode)

[

ToR-7

1

---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

8/10/2016

**SAFETY SYSTEM DIGITAL PLATFORM  
- MELTAC (MITSUBISHI ELECTRIC TOTAL ADVANCED CONTROLLER) -  
TOPICAL REPORT**

**Mitsubishi Electric Corporation**

**TAC NO.:** MF4228  
**RAI NO.:** #1  
**DATE OF RAI ISSUE:** 6/29/2016

---

**QUESTION NO.:** 8 for JEXU-1041-1008, "Safety System Digital Platform – MELTAC"

P. 76, Section 4.1.7.2, Memory Integrity Check (MIC), describes an activity that is part of the verification program for the MIC software tool. Per ISG-06, Section D.10.4.2.3.2, the information needed for the NRC staff to reach a determination that the software tools are adequate for their intended use should be contained in the documentation for the software tool verification program. Therefore, provide the procedure for the verification of the MIC tool to demonstrate adequacy. In addition, please clarify the following: How far along is the development of the MIC? Is it currently in use by operating plants? Please explain if all of the system memory locations are checked during this activity including data locations and unused memory.

---

**ANSWER:**

ISG-06, Section D.10.4.2.3.2 refers to IEEE 7-4.3.2 which pertains to "software tools used to support software development processes and verification and validation (V&V) processes". [

1

**Impact on Topical Report**

There is no impact on the Topical Report.

---

---

## RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

---

---

8/10/2016

### SAFETY SYSTEM DIGITAL PLATFORM - MELTAC (MITSUBISHI ELECTRIC TOTAL ADVANCED CONTROLLER) - TOPICAL REPORT

Mitsubishi Electric Corporation

**TAC NO.:** MF4228  
**RAI NO.:** #1  
**DATE OF RAI ISSUE:** 6/29/2016

---

**QUESTION NO.:** 9 for JEXU-1041-1008, "Safety System Digital Platform – MELTAC"

Page 214 of the TR discusses the generic redundant parallel controller reliability analysis and a fault tree analysis to support that controller configuration review. The NRC staff needs to review this specific analysis and additional analyses for other controller configurations and modules that are included in the MELCO platform to complete its evaluation in accordance with ISG-06 Section D.9.4.2.1.1. Please provide a description of the criteria used to determine which controller configuration will be used (i.e. single, redundant parallel or redundant standby) as well as documentation to demonstrate compliance of other possible controller configurations to this criteria.

---

**ANSWER:**

ISG-06 Section D.9.4.2.1.1, "Failure Modes and Effects Analysis (FMEA)" does not pertain to reliability, which is the subject of page 214 of the Topical Report (i.e., Controller Reliability Analysis). The FMEA is conducted to demonstrate that there are no single failures that can adversely affect the safety function in multiple safety divisions, and that there are no undetectable failures that could accumulate to result in failure of multiple safety divisions. The FMEA does not consider the frequency of failures. The FMEA method for MELTAC is described in Section 7.3 of the Topical Report.

Section 7.2, "Controller Reliability Analysis" pertains to frequency of failures for the three controller configurations that can be applied with MELTAC. These are single, redundant parallel, and redundant standby (described in Section 4.1.1).

Among these configurations, the configuration that can satisfy the plant specific reliability requirements is applied, with consideration of both actuation assurance and spurious actuation prevention. The actual reliability calculations are in plant specific documentation. The reliability models shown in Section 7.2 are intended to only show the reliability analysis method for each of the three basic controller configurations. The reliability models of these configurations are shown in Figure 1, Figure 2 and Figure 3, respectively.



Each configuration has one input module and one output module as a single I/O module. Redundant I/O modules can also be applied, as described in Section 4.1.1; for simplicity, these reliability models show only single I/O modules.

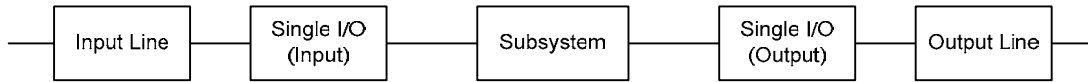


Figure 1 Reliability Model of a Single Controller

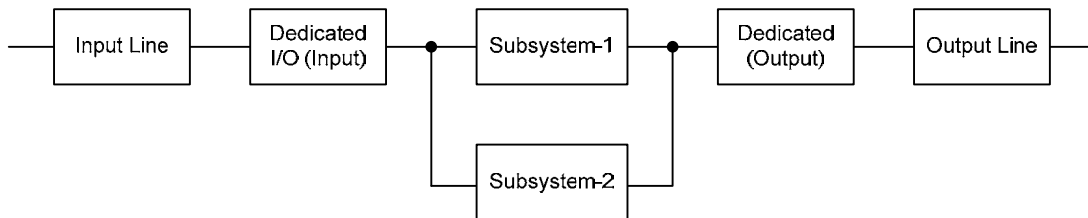


Figure 2 Reliability Model of a Redundant Parallel Controller

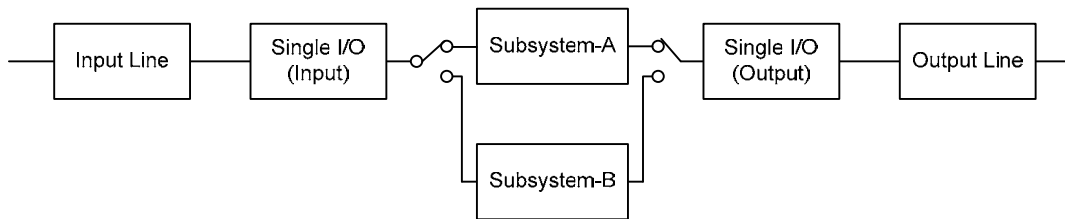


Figure 3 Reliability Model of a Redundant Standby

A comparison of the three controller subsystem configurations is described below. This comparison excludes the reliability of the single I/O modules, which is common to each configuration.

a) Spurious actuation

The continuous self-testing will shut down the single controller for most faults that could result in spurious actuation. Prevention of spurious actuation is not improved through the redundant standby controller configuration, which is equivalent to the single controller configuration. The likelihood of spurious actuation of the redundant parallel configuration is increased by 100% compared to the single and standby redundant configurations if the outputs are in a 1-out-of-2 configuration. However, if those outputs are in a 2-out-of-2 configuration to prevent spurious actuation, then the probability of spurious actuation is 50% of the single controller. And the outputs in a 2-out-of-2 configuration will be better than the single controller configuration because it can prevent spurious actuation caused by all failures in one of the two controllers.

$$F_{(\text{Redundant Parallel (2-out-of-2)})} < F_{(\text{Single})} = F_{(\text{Redundant Standby})} < F_{(\text{Redundant Parallel (1-out-of-2)})}$$

b) Failure to actuate

The redundant standby controller has almost the same reliability as the single controller. The reliability is limited primarily by the coverage of continuous self-testing, which is close to, but not 100%. The probability of failure to actuate of the redundant parallel controller is twice of the single controller when these outputs are 1-out-of-2. However, if those outputs are in a 2-out-of-2 configuration to prevent spurious actuation, then the probability of failure to actuate is 50% of the single controller.

$$U_{(\text{Redundant parallel (1-out-of-2)})} < U_{(\text{Redundant standby})} < U_{(\text{Single})} < U_{(\text{Redundant parallel (2-out-of-2)})}$$

Other configurations of MELTAC controllers are possible for plant specific applications. However, those configurations would be comprised of one or more of the three configurations described above, with the inputs shared and the outputs combined on the field side of the I/O modules using hardwired connections.

The FTAs for each controller configuration will be added to the Topical Report.

**Impact on Topical Report**

The answer above will be added to Section 7.2 of the Topical Report. See Attachment-1.

## 7.2 Controller Reliability Analysis

The failure rate of any safety-related system where MELTAC platform is applied as a whole, depends on the configuration of the entire system. Variations for each application include:

- The number and configuration of redundant divisions
- The number and configuration of controllers within each division
- The redundancy within each controller
- The configuration of I/O modules and Communication Interface Modules and the significance of these interfaces to the safety function (i.e.: the safety function logic design)

~~This section describes a method used to determine the reliability of a generic redundant parallel controller. The method for single controller architecture can be extrapolated from this method.~~

ToR-9

The controller reliability analysis is performed as follows.

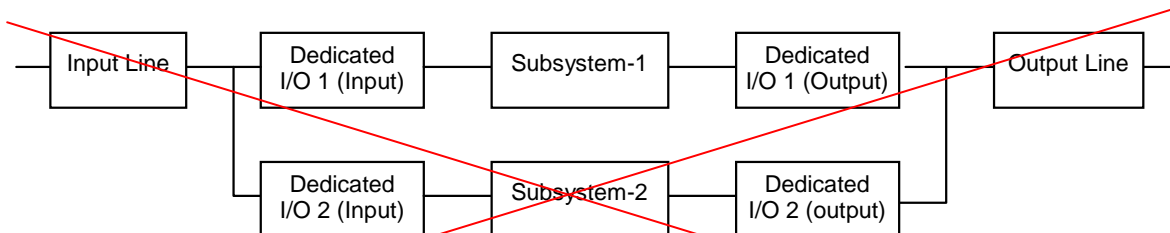
- A reliability model for the system's safety function is generated
- The fault tree analysis (FTA) of this reliability model is performed to determine the frequency of:
  - Spurious actuation of the safety function
  - Failure to actuate the safety function

~~The reliability model of a simple system is shown in Section 7.2.1. As an example of the reliability analysis process, Figure 7.2-2 shows the fault tree for spurious actuation of the safety function. The FTA for spurious actuation is explained below.~~

ToR-9

The three controller configurations that can be applied with MELTAC are described in section 4.1.1. These are single controller, redundant parallel and redundant standby controller. Among those three, the configuration that can satisfy the plant specific reliability requirements is applied, with consideration of both actuation assurance and spurious actuation prevention.

### 7.2.1 Reliability Model

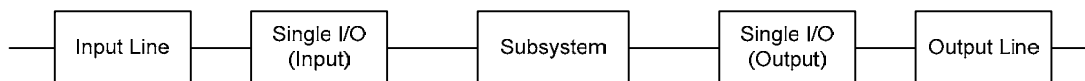


**Figure 7.2-1 Reliability Model**

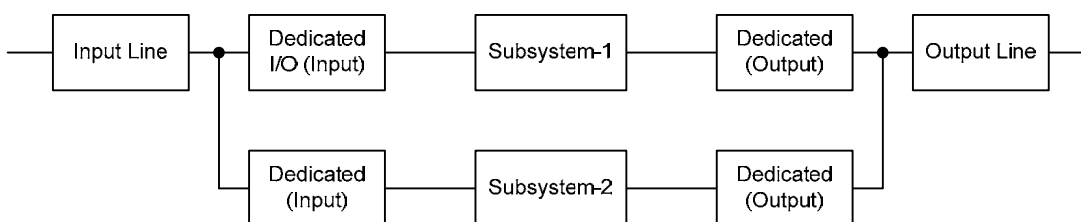
The above figure shows the reliability model of a redundant parallel controller, which contains one input module and one output module in each subsystem.

In the reliability model, the Status Display Module is not contained in the subsystem, because the Status Display Module only displays the current state of the subsystem and its failure does not affect the safety function of the subsystem. The Control Network I/F Module and the Optical Switch Module are not contained in this simplified system. They would be included, depending on how the data from the Control Network is used in the application software. This also applies to the Data Link interface from the Bus Master Modules.

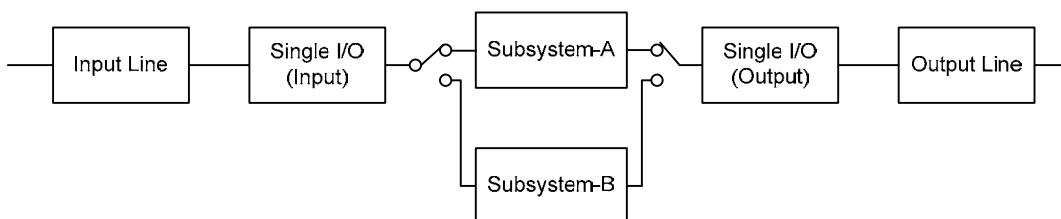
The reliability models of the single controller, redundant parallel and redundant standby controller are shown in Figure 7.2-1, Figure 7.2-2 and Figure 7.2-3 respectively.



**Figure 7.2-1 Reliability Model of a Single controller 3**



**Figure 7.2-2 Reliability Model of a Redundant Parallel**



**Figure 7.2-3 Reliability Model of a Redundant Standby**

A comparison of the three controller subsystem configurations is described below.

a) Spurious actuation

The continuous self-testing will shut down the single controller for most faults that could result in spurious actuation. Prevention of spurious actuation is not improved through the redundant standby controller configuration, which is equivalent to the single controller configuration. The likelihood of spurious actuation of the redundant parallel configuration is increased by 100% compared to the single and standby redundant configurations if the outputs are in a 1-out-of-2 configuration. However, if those outputs are in a 2-out-of-2 configuration to prevent spurious actuation, then the probability of spurious actuation is 50% of the single controller. And the outputs in a 2-out-of-2 configuration will be better than the single controller configuration because it can prevent spurious actuation caused by all failures in one of the two controllers.

$$F_{(\text{Redundant Parallel (2-out-of-2)})} < F_{(\text{Single})} = F_{(\text{Redundant Standby})} \leq F_{(\text{Redundant Parallel (1-out-of-2)})}$$

The FTAs for each controller configuration are shown in the Figure 7.2-4 to Figure 7.2-6.

b) Failure to actuate

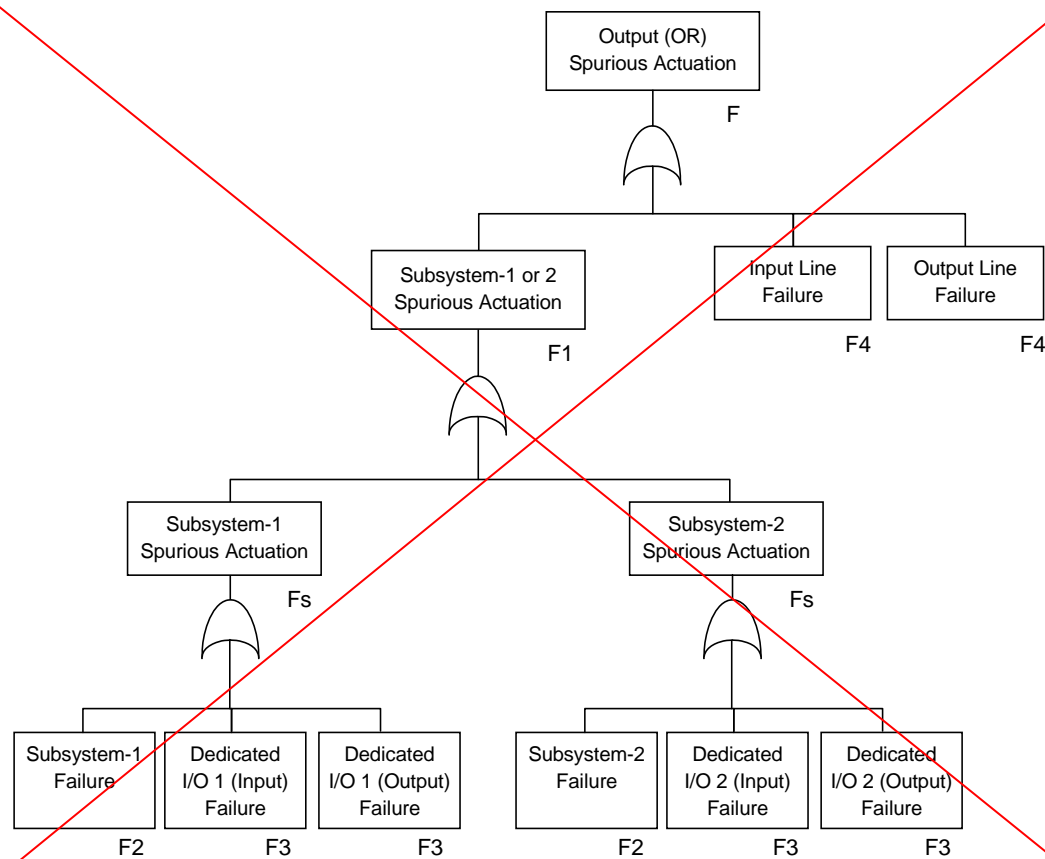
The redundant standby controller has almost the same reliability as the single controller. The reliability is limited primarily by the coverage of continuous self-testing, which is close to, but not 100%. The probability of failure to actuate of the redundant parallel controller is twice of the single controller when these outputs are 1-out-of-2. However, if those outputs are in a 2-out-of-2 configuration to prevent spurious actuation, then the probability of failure to actuate is 50% of the single controller.

$$U_{(\text{Redundant parallel (1-out-of-2)})} < U_{(\text{Redundant standby})} < U_{(\text{Single})} < U_{(\text{Redundant parallel (2-out-of-2)})}$$

The FTAs for each controller configuration are shown in the Figure 7.2-7 to Figure 7.2-9.

Other configurations of MELTAC controllers are possible for plant specific applications. However, those configurations would be comprised of one or more of the three configurations described above, with the inputs shared and the outputs combined on the field side of the I/O modules using hardwired connections.

ToR-9

**7.2.2 FTA of Spurious Actuation of the Safety Function****Figure 7.2-2 Fault Tree for Output Failure Spurious Actuation**

Regarding the cause of spurious actuation, the failure rate is described below.

$$F = F1 + F4 + F4$$

$$F1 = Fs + Fs$$

$$Fs = F2 + F3 + F3$$

Failure rate  $F_i$  ( $i = 1, 2, 3, \dots$ ) causes spurious action of each module or subsystem and is defined below.

$$F_i = \lambda_i \times (1 - P_i)$$

$\lambda_i$  = failure rate

$P_i$  = probability of detecting the failure which affects the safety function through self-diagnosis

Calculations of  $F2$ ,  $F3$  and  $F4$  are described in Sections 7.2.4.1, 7.2.4.2 and 7.2.4.3.

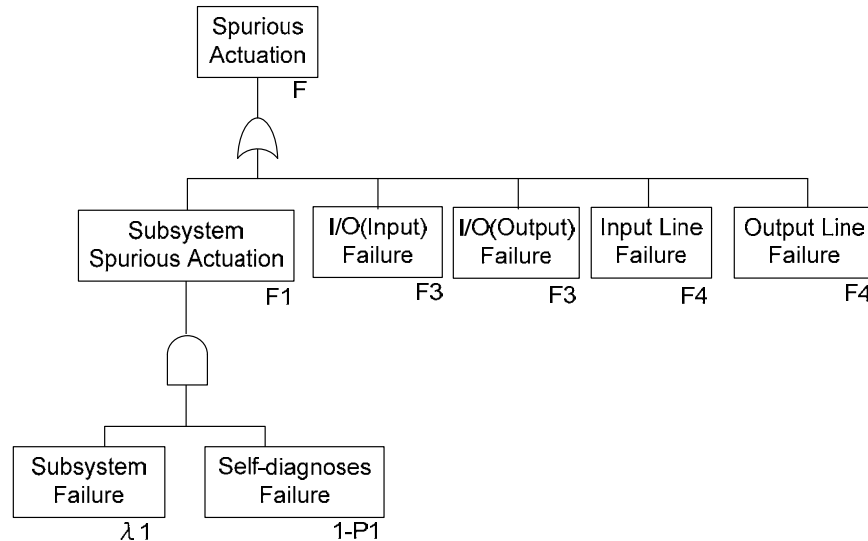
The failure rates of the Input Line and the Output Line are the same, because they consist of the same module and unit.

ToR-9

~~This FTA model assumes this very simple system, in which an input directly affects a system output. Systems with more complex logic may validate inputs (e.g.: voting) within the application logic so that spurious actuation requires multiple input failures.~~

The Figure 7.2-4, Figure 7.2-5, and Figure 7.2-6 show the FTA for spurious actuation of single controller, redundant standby and redundant parallel respectively.

The redundant standby configuration has Status Display and Switch Module. However it is not considered in this analysis because the failure of the Status Display and Switch Module doesn't cause the loss of safety function and subsystem switch function.



**Figure 7.2-4 Fault Tree for Spurious Actuation of Single Controller**

Regarding the cause of spurious actuation of the single controller, the failure rate is described below.

$$F_{(\text{Single})} = F1 + F3 + F3 + F4 + F4$$

Failure rate  $F_i$  ( $i = 1, 2, 3 \dots$ ) causes spurious action of each module or subsystem and is defined below.

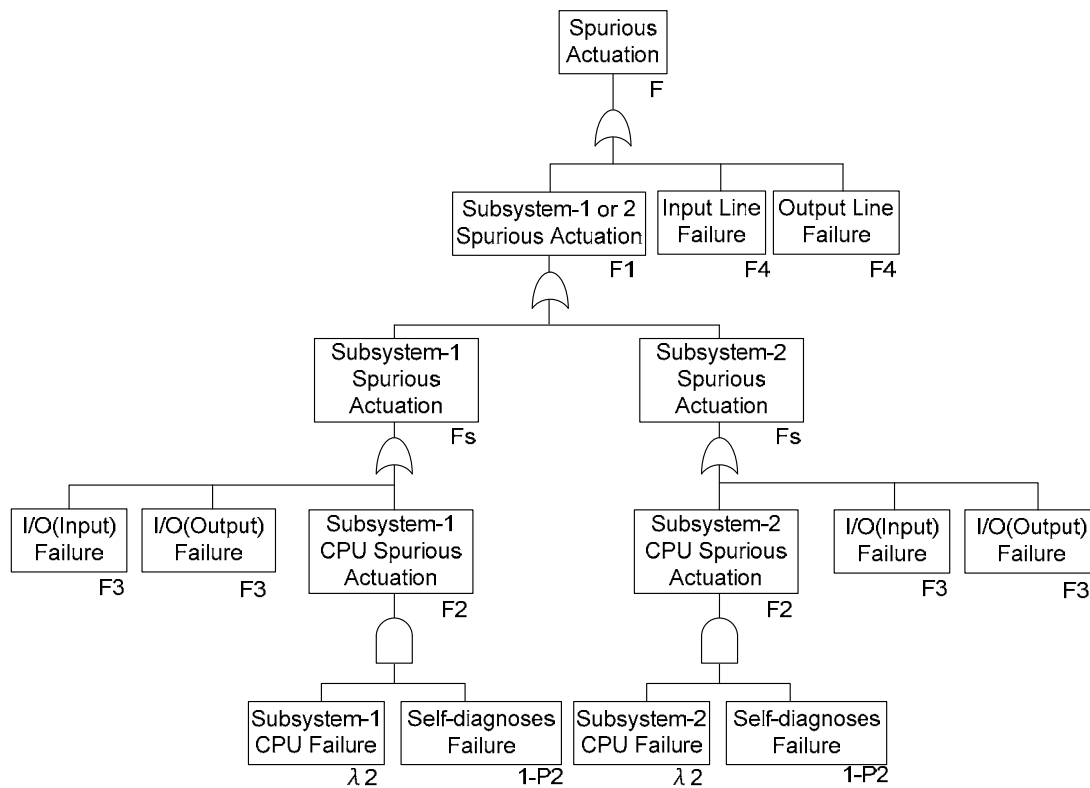
$$F_i = \lambda_i \times (1 - P_i)$$

$\lambda_i$  = failure rate

$P_i$  = probability of detecting the failure which affects the safety function through self-diagnosis

ToR-9





ToR-9

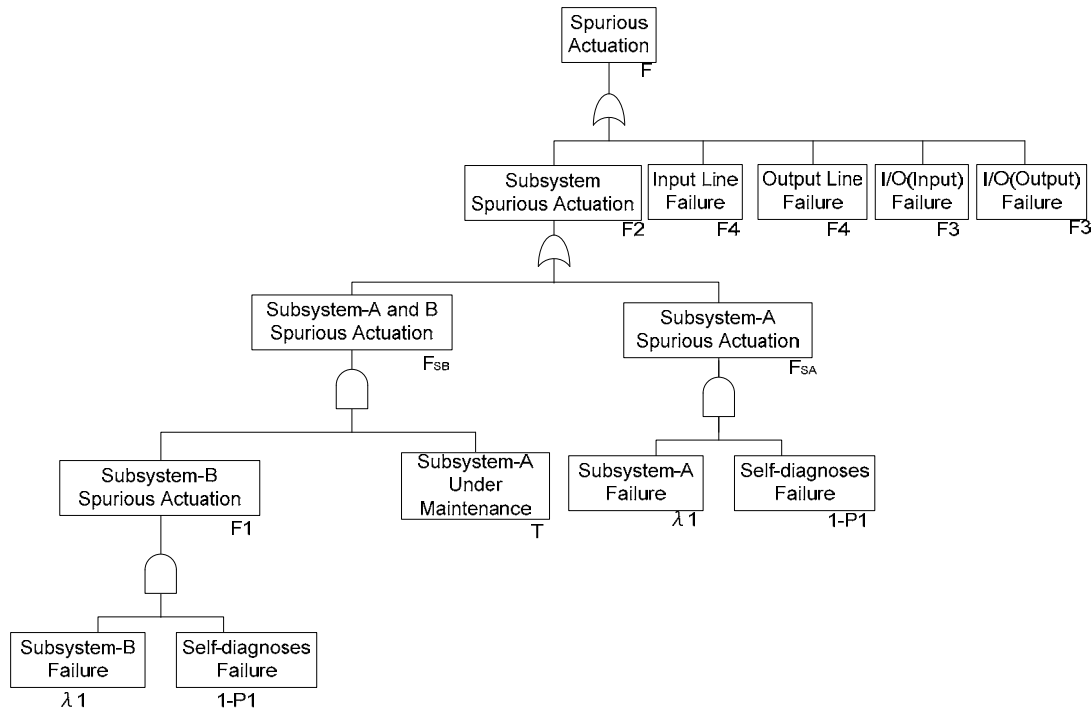
**Figure 7.2-5 Fault Tree for Spurious Actuation of Redundant Parallel**

Regarding the cause of spurious actuation of the redundant parallel whose output is 1 out of 2, the failure rate is described below.

$$F_{\text{(Redundant Parallel)}} = F1 + F4 + F4$$

$$F1 = Fs + Fs$$

$$Fs = F2 + F2 + F3$$



ToR-9

**Figure 7.2-6 Fault Tree for Spurious Actuation of Redundant Standby**

Regarding the cause of spurious actuation of the redundant standby, the failure rate is described below.

$$F_{(\text{Redundant Standby})} = F_2 + F_3 + F_3 + F_4 + F_4$$

$$F_2 = F_{SA} + F_{SB}$$

$$F_{SA} = F_1 (= \lambda_i \times (1-P_i))$$

$$F_{SB} = F_1 \times T$$

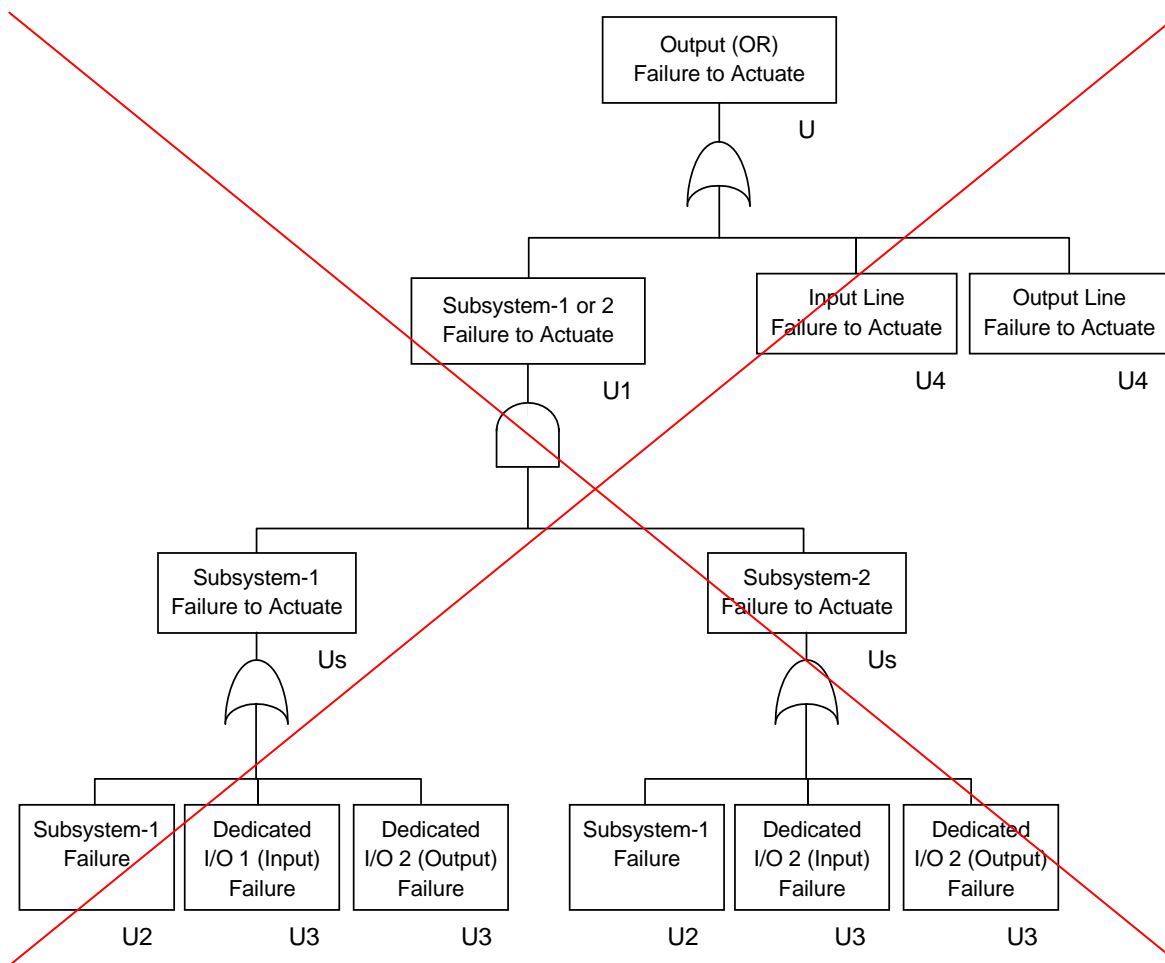
T stands for period of the maintenance of subsystem-A

$$T = \text{MTTR} / (\text{MTBF} + \text{MTTR})$$

Since  $\text{MTTR} \ll \text{MTBF}$ , T can be considered as closely 0.

Therefore, the spurious actuation is provided as follows, because  $F_2 = F_1$ .

$$F_{(\text{Redundant Standby})} = F_1 + F_3 + F_3 + F_4 + F_4$$

**7.2.3 FTA of Failure to Actuate the Safety Function**

ToR-9

**Figure 7.2-3 Fault Tree for Failure to Actuate**

Regarding the cause of failure to actuate, unavailability is described below.

$$U = U1 + U4 + U4$$

$$U1 = Us \times Us$$

$$Us = U2 + U3 + U3$$

$U_i$  is the unavailability of each module or subsystem and is defined below.

$$U_i = 1 - MTBF / (MTBF + (1 - P_i) \times (T_i / 2) + MTTR)$$

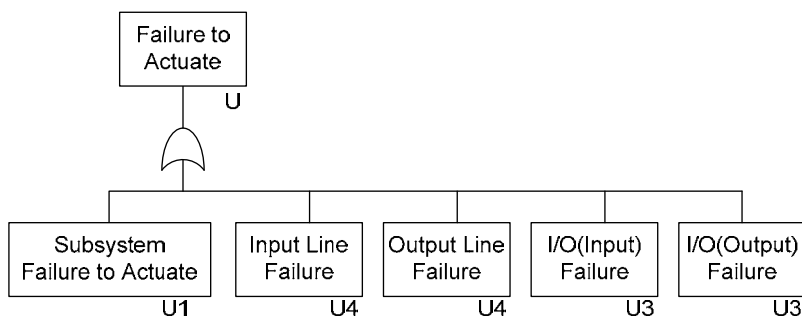
$T_i$  = Manual test interval

$$MTBF = 1 / \lambda_i$$

$T_i$  and Mean Time To Repair (MTTR) are unique to each application.

The Figure 7.2-7, Figure 7.2-8, and Figure 7.2-9 show the FTA for failure to actuate of single controller, redundant standby and redundant parallel respectively.

The failure rate of the Status Display and Switch Module is not considered to this analysis because of the same reason of analysis for spurious actuation.



**Figure 7.2-7 Fault Tree for Failure to Actuate of Single controller**

Regarding the cause of failure to actuate of the single controller, unavailability is described below.

$$U_{(Single)} = U1 + U3 + U3 + U4 + U4$$

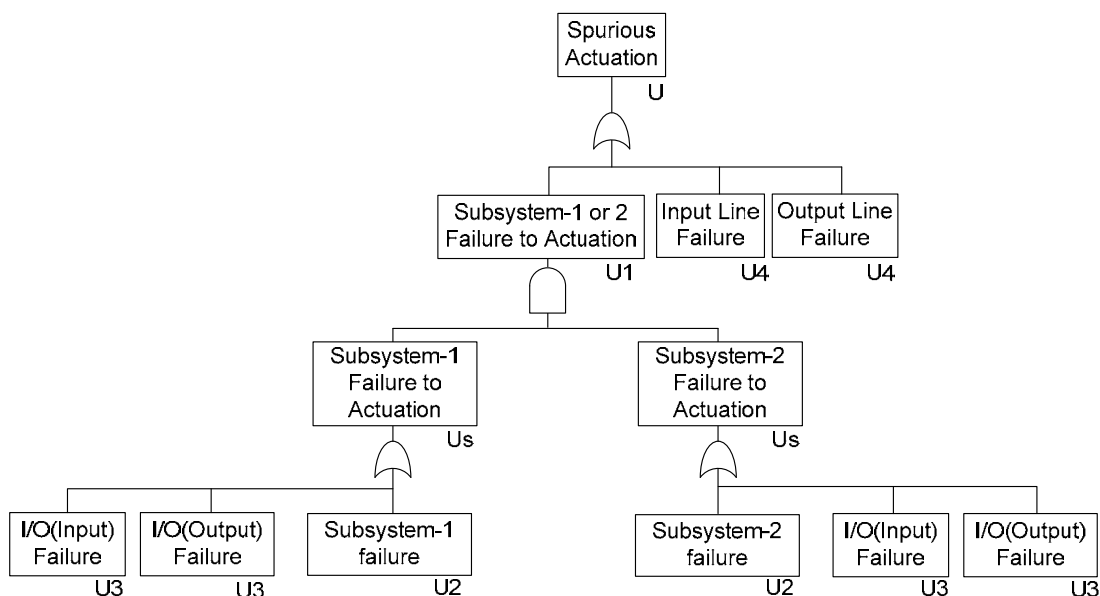
Ui is the unavailability of each module or subsystem and is defined below.

$$U_i = 1 - MTBF / (MTBF + (1 - P_i) \times (T_i / 2) + MTTR)$$

Ti = Manual test interval

$$MTBF = 1 / \lambda_i$$

Ti and Mean Time To Repair (MTTR) are unique to each application.



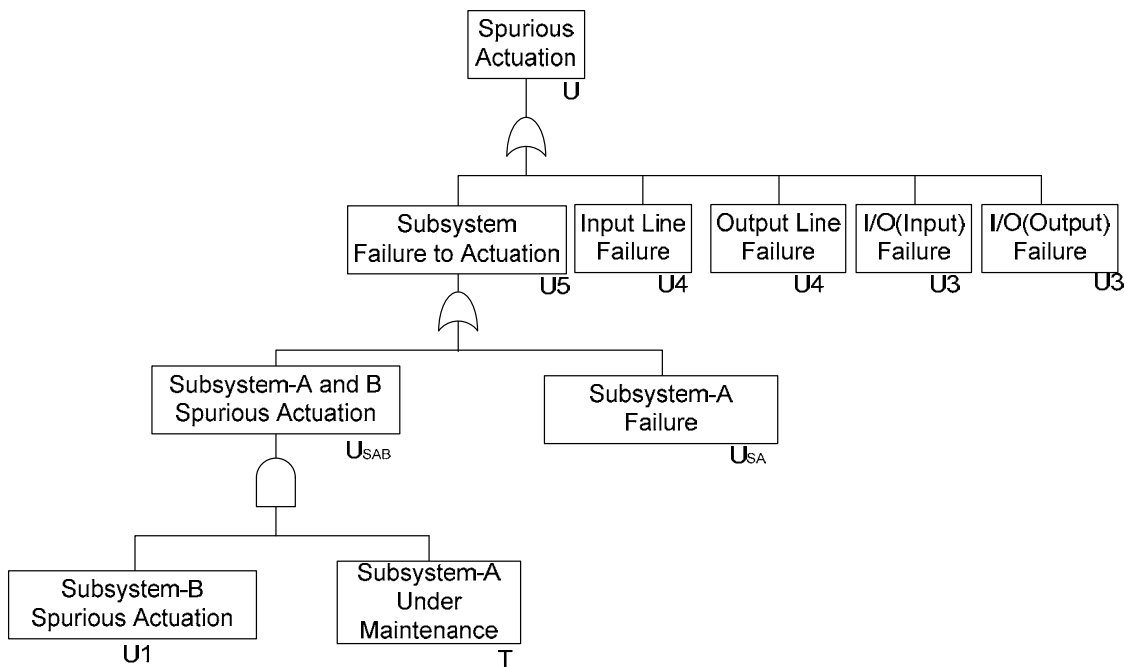
**Figure 7.2-8 Fault Tree for Failure to Actuate of Redundant Parallel**

Regarding the cause of failure to actuate of the redundant parallel controller, unavailability is described below.

$$U(\text{redundant parallel}) = U_1 + U_4 + U_4$$

$$U_2 = U_s + U_s$$

$$U_s = U_2 + U_3 + U_3$$



### 7.2-9 Fault Tree for Failure to Actuate of Redundant Standby

Regarding the cause of failure to actuate of the redundant standby controller, unavailability is described below.

$$U(\text{redundant standby}) = U_5 + U_3 + U_3 + U_4 + U_4$$

$$U_5 = U_{SA} + U_{SAB}$$

$$U_{SA} = 1 - \text{MTBF} / (\text{MTBF} + (1 - P_5) \times (T_5 / 2)) \quad (\text{note})$$

$$U_{SAB} = U_1 \times T$$

T stands for period of the maintenance of subsystem-A

$$T = \text{MTTR} / (\text{MTBF} + \text{MTTR})$$

Since MTTR << MTBF, T can be considered as closely 0.

Therefore, the spurious actuation is provided as follows, because U5=USA.

$$U(\text{redundant standby}) = U_{SA} + U_3 + U_3 + U_4 + U_4 \quad (\text{note})$$

(Note)

USA is the unavailability of the subsystem when the other subsystem is not in failure mode.

USA is provided as above because when the other subsystem is not in failure mode, MTTR can be considered as 0.

ToR-9

---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

8/10/2016

**SAFETY SYSTEM DIGITAL PLATFORM  
- MELTAC (MITSUBISHI ELECTRIC TOTAL ADVANCED CONTROLLER) -  
TOPICAL REPORT**

**Mitsubishi Electric Corporation**

**TAC NO.:** MF4228  
**RAI NO.:** #1  
**DATE OF RAI ISSUE:** 6/29/2016

---

**QUESTION NO.:** 5 for JEXU-1041-1015, "MELTAC Platform ISG-04 Conformance Analysis"

With regard to the response to Staff Position 10, The NRC staff requires the following:

- a. A description of what constitutes a "temporary change"
- b. The NRC staff requests the procedure describing how user configurable constants, such as setpoints, time delays or instrument ranges will be changed with the CPU Module mounted in the dedicated Re-programming Chassis.

---

**ANSWER:**

[

]



Figure 1 Example of Temporary Change

[

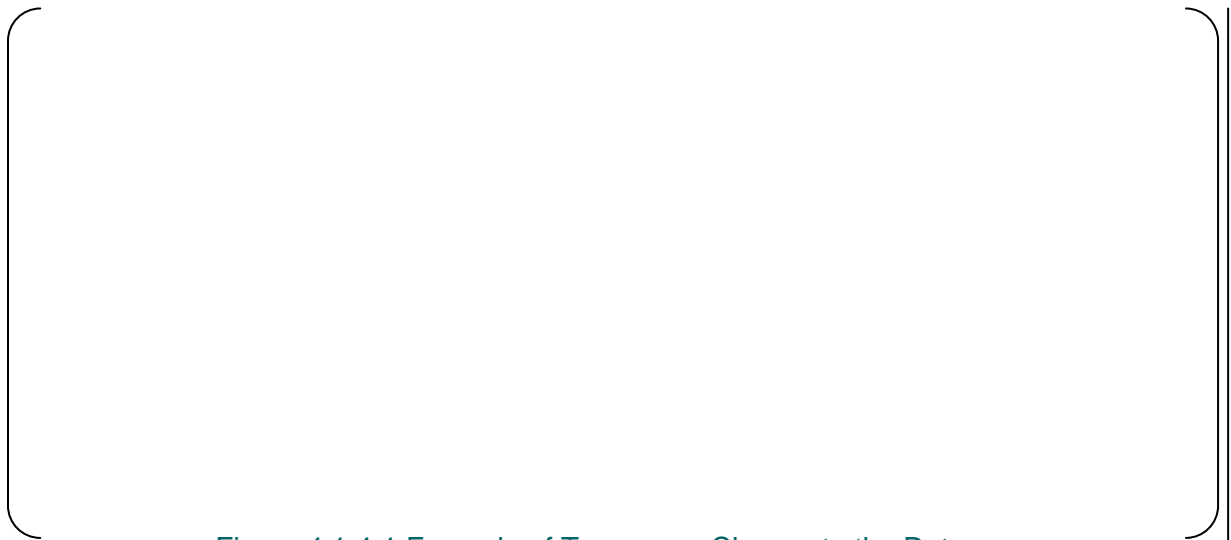
]

**Impact on Technical Report**

The answer above will be added to Section 4.1.4 of the Topical Report. See Attachment-1.

There is no impact on the “MELTAC Platform ISG-04 Conformance Analysis”.





ToR-5,  
ISG04CA-5

Figure 4.1.4-1 Example of Temporary Change to the Data

[

ToR-5

ISG04CA-5

]

## **PART 3-2**

### **Responses to RAI, including:**

Transmittal Letter, dated September 23, 2016

JEXU-1041-2073 R0 (Response to S/W Tools RAI 1)

JEXU-1041-2074 R0 (Response to S/W Tools RAI 2)

JEXU-1041-2075 R0 (Response to S/W Tools RAI 3)

JEXU-1041-2076 R0 (Response to S/W Tools RAI 4)

JEXU-1041-2077 R0 (Response to S/W Tools RAI 5)

JEXU-1041-2078 R0 (Response to IEEE CMs RAI 1)

JEXU-1041-2080 R0 (Response to IEEE CMs RAI 3)

JEXU-1041-2081 R0 (Response to ISG04CA RAI 1)

JEXU-1041-2082 R0 (Response to ISG04CA RAI 2)

JEXU-1041-2084 R0 (Response to ISG04CA RAI 4)

JEXU-1041-2086 R0 (Response to ISG04CA RAI 6)



Sep 23, 2016  
JEXU-1041-8523

Document Control Desk  
U.S. Nuclear Regulatory Commission  
11555 Rockville Pike  
Rockville, MD 20852-2738

Attention: Mr. Joseph Holonich

**SUBJECT: MELCO's responses to MELTAC Topical Report Revision 0 RAI #1 (TAC No.MF4228)  
(Regarding, items No.1 through No.5 for JEXU-1041-1031, "MELTAC Platform  
Software Tools", items No.1 and No.3 for JEXU-1041-1018, "Summary of  
Compliance to the IEEE Std. 603 and IEEE Std. 7-4.3.2", and items No.1, No.2, No.4  
and No.6 for JEXU-1041-1015, "Conformance Analysis to ISG-04")**

With this letter, Mitsubishi Electric Corporation (MELCO) submits the documents listed in the enclosures table below to the U.S. Nuclear Regulatory Commission (NRC).

Enclosed are the documents that make up the response to items No.1 through No.5 for JEXU-1041-1031, "MELTAC Platform Software Tools", items No.1 and No.3 for JEXU-1041-1018, "Summary of Compliance to the IEEE Std. 603 and IEEE Std. 7-4.3.2", and items No.1, No.2, No.4 and No.6 for JEXU-1041-1015, "Conformance Analysis to ISG-04". As indicated in the enclosed materials, these documents contain information that MELCO considers proprietary, and therefore should be withheld from public disclosure pursuant to 10 C.F.R 2.390 (a)(4) as trade secrets and commercial or financial information which is privileged or confidential.

The accompanying affidavit, Enclosure (1) sets forth the basis on which the information identified as proprietary should be withheld from public disclosure.

Sincerely,

Shigeru Sugitani  
Senior Manager, Control & Protection Systems Section  
Nuclear Power Department, Energy Systems Center  
Mitsubishi Electric Corporation

**Enclosures:**

No.	Document Number	Document Title	Date of Issue
1	-	Affidavit of Shigeru Sugitani	09/23/2016
2	JEXU-1041-2073-P	1 for JEXU-1041-1031, "MELTAC Platform Software Tools"	09/23/2016
3	JEXU-1041-2073-NP		
4	JEXU-1041-2074-P	2 for JEXU-1041-1031, "MELTAC Platform Software Tools",	09/23/2016
5	JEXU-1041-2074-NP		
6	JEXU-1041-2075-P	3 for JEXU-1041-1031, "MELTAC Platform Software Tools"	09/23/2016
7	JEXU-1041-2075-NP		
8	JEXU-1041-2076-P	4 for JEXU-1041-1031, "MELTAC Platform Software Tools"	09/23/2016
9	JEXU-1041-2076-NP		
10	JEXU-1041-2077-P	5 for JEXU-1041-1031, "MELTAC Platform Software Tools"	09/23/2016
11	JEXU-1041-2077-NP		
12	JEXU-1041-2078	1 for JEXU-1041-1018, "Summary of Compliance to the IEEE Std. 603 and IEEE Std. 7-4.3.2"	09/23/2016
13	JEXU-1041-2080	3 for JEXU-1041-1018, "Summary of Compliance to the IEEE Std. 603 and IEEE Std. 7-4.3.2"	09/23/2016
14	JEXU-1041-2081-P	1 for JEXU-1041-1015, "Conformance Analysis to ISG-04"	09/23/2016
15	JEXU-1041-2081-NP		
16	JEXU-1041-2082-P	2 for JEXU-1041-1015, "Conformance Analysis to ISG-04"	09/23/2016
17	JEXU-1041-2082-NP		
18	JEXU-1041-2084-P	4 for JEXU-1041-1015, "Conformance Analysis to ISG-04"	09/23/2016
19	JEXU-1041-2084-NP		
20	JEXU-1041-2086-P	6 for JEXU-1041-1015, "Conformance Analysis to ISG-04"	09/23/2016
21	JEXU-1041-2086-NP		

CC: Gilbert W. Remley  
Nuclear Systems Department Manager  
Mitsubishi Electric Power Products, Inc

---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

**9/23/2016**

**SAFETY SYSTEM DIGITAL PLATFORM  
- MELTAC (MITSUBISHI ELECTRIC TOTAL ADVANCED CONTROLLER) -  
TOPICAL REPORT**

**Mitsubishi Electric Corporation**

**TAC NO.: MF4228**  
**RAI NO.: #1**  
**DATE OF RAI ISSUE: 6/29/2016**

---

**QUESTION NO.: 1 for JEXU-1041-1031, "MELTAC Platform Software Tools"**

P. 4, List of Software Tools Category Used in Each Phase:

- a. In order for the NRC staff to evaluate software tools for compliance with IEEE 7-4.3.2 Section 5.3.2, we will need to understand what the tools are used for as well as what functions they perform in relation to the MELCO safety software development processes. The software tools listed in Table 1 are not consistent with names of the software tools provided in Section 5.0, Detailed Description of Processes. Please clarify the specific function of the tools and identify what document describes the function of each tool. The response should include a description of what the rules are for using the tool correctly and what configurations or options are recommended or advised against.
  - i. By further example of what the NRC staff needs to understand is the functions of the Engineering Tool. Section 4.1.4.1, Function Description of the TR, states the functional block diagrams are converted to graphical block diagrams by the MELTAC engineering tool. Section 5.7, MELTAC Engineering Tool, does not describe this function. Please explain.
- b. Please provide an assessment of how each tool conforms to the software tools criteria of IEEE 7-4.3.2 Section 5.3.2 for the tools listed below:
  - i. [            ]
  - ii. [            ]
- c. Identify the lifecycle phases that the MIC will be used in as was done with the other software tools on Table 1.

- d. Clause 5.3.2 of IEEE Std 7-4.3.2 specifies that software tools used to support software development are controlled under a configuration management plan. To evaluate compliance with this requirement, the NRC needs to review plans and procedures for establishment and maintenance of tool configuration control. Please provide documentation to show how tool configurations are controlled and Identify procedures used to maintain tool configuration control.

---

**ANSWER:**

[

]

**Impact on Topical Report**

There is no impact on the Topical Report.

**Impact on Technical Report**

Regarding a), Section 1.0, Table 1 in Section 4.0 and Section 5.0 of JEXU-1041-1031, "MELTAC Platform Software Tools" will be revised. Appendix B will be added to JEXU-1041-1031, "MELTAC Platform Software Tools" (see Attachment 1).

Regarding b), Section 5.10.2 of JEXU-1041-1031, "MELTAC Platform Software Tools" will be revised (see Attachment-2).

Regarding c), Table 1 in Section 4.0 of JEXU-1041-1031, "MELTAC Platform Software Tools" will be revised (see Attachment-3).

Regarding d), There is no impact on the Technical Report.



## 1.0 INTRODUCTION

This document describes the software tools, how their quality has been determined, how they are used and maintained, and verification and the validation (V&V) activities associated with the outputs generated by those software tools for the Mitsubishi Electric Total Advanced Controller (MELTAC) platform (i.e., Method (b) in Clause 5.3.2 of IEEE Std. 7-4.3.2-2003). This document encompasses the software tools used to develop the MELTAC platform basic software, which includes firmware and field programmable gate arrays (FPGAs) on all MELTAC platform modules.

This document supports “Safety System Digital Platform - MELTAC - Topical Report” (JEXU-1041-1008), which references “MELTAC Platform Software Program Manual” (JEXU-1041-1016) and satisfies the commitments made under Table 1 Section 2.17 “Software Tool Analysis Report” of “Mapping of MELTAC Platform Licensing Documents to the DI&C-ISG-06 Guidance” (JEXU-1041-1012).

BTP 7-14, B.3.1.11.2 requires evaluation process for software tools, if tools are purchased as commercial items. Appendix A describes the evaluation procedure for purchased software tools used to develop MELTAC platform basic software.

Tools-2

“Safety System Digital Platform - MELTAC - Topical Report” (JEXU-1041-1008) also describes the MELTAC engineering tool functions associated with application software development. Appendix B of this document further describes these functions: how their quality has been determined, how they are expected to be used and maintained, and the verification and validation (V&V) activities associated with the outputs generated by the MELTAC engineering tool (i.e., Method (b) in Clause 5.3.2 of IEEE Std. 7-4.3.2-2003).

Tools-1a

## 2.0 REFERENCES

Document Name	Document Number	Revision
Safety System Digital Platform - MELTAC - Topical Report	JEXU-1041-1008	Current
Mapping of MELTAC Platform Licensing Documents to the Digital I&C-ISG-06 Guidance”	JEXU-1041-1012	Current
Digital I&C-ISG-06 “Digital Instrumentation & Control Licensing Process”	ML110140103	1
MELTAC Platform Software Program Manual	JEXU-1041-1016	Current
Guidance on Software Reviews for Digital Computer-Based I&C Systems	NUREG 0800 BTP 7-14	2007
Criteria for use of Computer in Safety Systems for Nuclear Power Plants	RG 1.152	3
Criteria for Digital Computers in Safety Systems for Nuclear Power Generating Stations	IEEE Std. 7-4.3.2-2003	2003

4.0 OBJECTIVE AND METHODOLOGY

[ The software life cycle is described in Section 3 of “MELTAC Platform Software Program Manual” (JEXU-1041-1016). ]

[

]

Table 1 - List of Software Tools Category Used in Each Phase


Tools-1a

Tools-1c

5.0 DETAILED DESCRIPTION OF PROCESSES  
[

]

(


[

Tools-1a

[

]


[

Tools-1a

]

[

]


Tools-1a

[

[

]


Tools-1a

[

]


[

Tools-1a

]



[

]


[

Tools-1a

]

[

]


Tools-1a

[

]

[

]


Tools-1a

[

Tools-1a

]

[


Tools-1a

[

]

(

[

]


)

Tools-4

Tools-4

Tools-1a

[

]


[

Tools-1a

Tools-5

Tools-5

**APPENDIX B MELTAC ENGINEERING TOOL FUNCTIONS FOR APPLICATION SOFTWARE DEVELOPMENT**

The functional description of MELTAC engineering tool is described in Section 4.1.4 of “Safety System Digital Platform - MELTAC - Topical Report” (JEXU-1041-1008).

The table below lists the MELTAC engineering tool functions used to develop application software, which are expected to be used during implementation, test, and installation of application software.

This appendix also describes how the functions are used, including verification and validation (V&V) activities associated with the outputs generated by the MELTAC engineering tool.

Table B.1 MELTAC engineering tool functions used to develop application software


Tools-1a



[	
]	

Tools-1a

[

]


[

Tools-1a

Tools-5

Tools-5

]

[

]

4.0 OBJECTIVE AND METHODOLOGY

[ The software life cycle is described in Section 3 of “MELTAC Platform Software Program Manual” (JEXU-1041-1016). ]

]

Table 1 - List of Software Tools Category Used in Each Phase


Tools-1a

Tools-1c

---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

9/23/2016

**SAFETY SYSTEM DIGITAL PLATFORM  
- MELTAC (MITSUBISHI ELECTRIC TOTAL ADVANCED CONTROLLER) -  
TOPICAL REPORT**

**Mitsubishi Electric Corporation**

**TAC NO.: MF4228**  
**RAI NO.: #1**  
**DATE OF RAI ISSUE: 6/29/2016**

---

**QUESTION NO.: 2 for JEXU-1041-1031, "MELTAC Platform Software Tools"**

Page 15, Section 5.0, of this document, "Detailed Description of Processes," does not identify the procedure used to initially select, track and maintain the specific software tool suppliers that are identified in this section. BTP 7-14, B.3.1.11.2, states that the a description of the process used to maintain and track purchased items, such as software tools used to make the final product should be provided. BTP 7-14 goes on to state this qualification procedure should be provided, and a method of tracking tool history, bug lists, and errata sheets should enable tracking which design outputs may be affected. Please provide this qualification procedure on the docket for NRC staff review.

---

**ANSWER:**

[

]

**Impact on Topical Report**

There is no impact on the Topical Report.

**Impact on Technical Report**

Section 1.0 will be revised and Appendix A will be added to JEXU-1024-1031, "MELTAC Platform Software Tools" (see Attachment-1).

## 1.0 INTRODUCTION

This document describes the software tools, how their quality has been determined, how they are used and maintained, and verification and the validation (V&V) activities associated with the outputs generated by those software tools for the Mitsubishi Electric Total Advanced Controller (MELTAC) platform (i.e., Method (b) in Clause 5.3.2 of IEEE Std. 7-4.3.2-2003). This document encompasses the software tools used to develop the MELTAC platform basic software, which includes firmware and field programmable gate arrays (FPGAs) on all MELTAC platform modules.

This document supports “Safety System Digital Platform - MELTAC - Topical Report” (JEXU-1041-1008), which references “MELTAC Platform Software Program Manual” (JEXU-1041-1016) and satisfies the commitments made under Table 1 Section 2.17 “Software Tool Analysis Report” of “Mapping of MELTAC Platform Licensing Documents to the DI&C-ISG-06 Guidance” (JEXU-1041-1012).

BTP 7-14, B.3.1.11.2 requires evaluation process for software tools, if tools are purchased as commercial items. Appendix A describes the evaluation procedure for purchased software tools used to develop MELTAC platform basic software.

Tools-2

“Safety System Digital Platform - MELTAC - Topical Report” (JEXU-1041-1008) also describes the MELTAC engineering tool functions associated with application software development. Appendix B of this document further describes these functions: how their quality has been determined, how they are expected to be used and maintained, and the verification and validation (V&V) activities associated with the outputs generated by the MELTAC engineering tool (i.e., Method (b) in Clause 5.3.2 of IEEE Std. 7-4.3.2-2003).

Tools-1a

## 2.0 REFERENCES

Document Name	Document Number	Revision
Safety System Digital Platform - MELTAC - Topical Report	JEXU-1041-1008	Current
Mapping of MELTAC Platform Licensing Documents to the Digital I&C-ISG-06 Guidance”	JEXU-1041-1012	Current
Digital I&C-ISG-06 “Digital Instrumentation & Control Licensing Process”	ML110140103	1
MELTAC Platform Software Program Manual	JEXU-1041-1016	Current
Guidance on Software Reviews for Digital Computer-Based I&C Systems	NUREG 0800 BTP 7-14	2007
Criteria for use of Computer in Safety Systems for Nuclear Power Plants	RG 1.152	3
Criteria for Digital Computers in Safety Systems for Nuclear Power Generating Stations	IEEE Std. 7-4.3.2-2003	2003

**APPENDIX A EVALUATION PROCEDURE FOR PURCHASED SOFTWARE TOOLS TO DEVELOP MELTAC BASIC SOFTWARE**

[

Tools-2

]

Table A.1 Evaluation Test Applicability




[

Tools-2

]

---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

9/23/2016

**SAFETY SYSTEM DIGITAL PLATFORM  
- MELTAC (MITSUBISHI ELECTRIC TOTAL ADVANCED CONTROLLER) -  
TOPICAL REPORT**

**Mitsubishi Electric Corporation**

**TAC NO.: MF4228**  
**RAI NO.: #1**  
**DATE OF RAI ISSUE: 6/29/2016**

---

**QUESTION NO.: 3 for JEXU-1041-1031, "MELTAC Platform Software Tools"**

3. [ ], Page 23, Section 5.8.2,2 "Verification & Validation (V&V) Method," of this document states the same V&V process applies to the MIC tool as the safety system software per the MELTAC Platform Software Program Manual (SPM). The NRC staff needs to understand the applicability of the SPM to the MIC and the Appendix B process. Therefore, provide the final V&V Report, per Section 3.10.4.8 of the MELTAC Platform Software Program Manual, which was completed for the MIC tool on the docket. Also, please reference and provide the procedure which includes the instructions for completing the V&V report for software tools.
- a. Section 5.8.1 of this description identifies the MIC function of the MELENS software is developed and managed under Appendix B but the previous page and Section 5.7 states the MELENS software is developed as non-safety. The NRC staff requests the description of [ ]. How is separation maintained for development and maintenance purposes? Is there a separate sign-on for access to the MIC function?

---

**ANSWER:**

[

]

**Impact on Topical Report**

There is no impact on the Topical Report.

**Impact on Technical Report**

There is no impact on the Technical Report.

---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

9/23/2016

**SAFETY SYSTEM DIGITAL PLATFORM  
- MELTAC (MITSUBISHI ELECTRIC TOTAL ADVANCED CONTROLLER) -  
TOPICAL REPORT**

**Mitsubishi Electric Corporation**

**TAC NO.: MF4228**  
**RAI NO.: #1**  
**DATE OF RAI ISSUE: 6/29/2016**

---

**QUESTION NO.: 4 for JEXU-1041-1031, “MELTAC Platform Software Tools”**

Criterion V of Appendix B of 10 CFR 50 requires, in part, “Activities affecting quality shall be prescribed by documented instructions,” and this Criterion also states “Instructions shall include appropriate acceptance criteria” (see RAI 2 of JEXU-1041-1008). In this document, Page 24, Section 5.9.2, 2), states: “[

]” Provide the V&V procedure that describes the acceptance criteria used to determine the write operation of the tool is successful by reading the result of the tools listed.

---

**ANSWER:**

[

]

**Impact on Topical Report Report**

There is no impact on Topical Report.

**Impact on Technical Report**

Section 5.9.2 of JEXU-1042-1031, “MELTAC Platform Software Tools” will be revised (see Attachment-1).

]

(

[

]


)

Tools-4

Tools-4

Tools-1a

---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

**9/23/2016**

**SAFETY SYSTEM DIGITAL PLATFORM  
- MELTAC (MITSUBISHI ELECTRIC TOTAL ADVANCED CONTROLLER) -  
TOPICAL REPORT**

**Mitsubishi Electric Corporation**

**TAC NO.: MF4228  
RAI NO.: #1  
DATE OF RAI ISSUE: 6/29/2016**

---

**QUESTION NO.: 5 for JEXU-1041-1031, "MELTAC Platform Software Tools"**

The NRC staff needs a clear understanding of where 10 CFR 50 Appendix B applies and where is it not applicable in order to complete the evaluation. [

]

---

**ANSWER:**

[

]

**Impact on Topical Report**

There is no impact on the Topical Report.

**Impact on Technical Report**

Section 5.10.2 of JEXU-1041-1031, "MELTAC Platform Software Tools" will be revised (see Attachment-1).

[

]


[

Tools-1a

Tools-5

Tools-5

---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

9/23/2016

**SAFETY SYSTEM DIGITAL PLATFORM  
- MELTAC (MITSUBISHI ELECTRIC TOTAL ADVANCED CONTROLLER) -  
TOPICAL REPORT**

**Mitsubishi Electric Corporation**

**TAC NO.:** MF4228  
**RAI NO.:** #1  
**DATE OF RAI ISSUE:** 6/29/2016

---

**QUESTION NO.: 1 for JEXU-1041-1018, "Summary of Compliance to the IEEE Std. 603 and IEEE Std. 7-4.3.2"**

Regarding Page 10, Table 3, of this document, IEEE 603, 5.11, Identification. Does MELCO have an identification system of hardware and software applied during the design and manufacturing of the generic platform? If so this requirement applies and the NRC needs to evaluate how it is implemented. Please provide a description of platform hardware and software identification methods to demonstrate compliance with this requirement.

---

**ANSWER:**

The "Assessment" entry for Section 5.11 in Table 3 will be revised as follows:

Hardware, software and documents of the MELTAC platform are uniquely identified including "nuclear safety related" markings, as described in Section 6.1.7 of JEXU-1041-1008, "Safety System Digital Platform - MELTAC - Topical Report". This identification is controlled in accordance with MELCO's 10 CFR 50 Appendix B QAP.

**Impact on Technical Report**

Table 3 of JEXU-1041-1018, "Summary of Compliance to the IEEE Std. 603 and IEEE Std. 7-4.3.2" will be revised by incorporating the evaluation above (see Attachment-1).



Table 3 IEEE Std. 603 (1991) Compliance Matrix

Section	Title	Assessment	References <Document Number Sections>
5.8.3	Indication of Bypasses	This is an application specific requirement that is dependent on a plant design. Therefore this requirement is not addressed for the MELTAC platform.	None
5.8.4	Location	This is an application specific requirement that is dependent on a plant design. Therefore this requirement is not addressed for the MELTAC platform.	None
5.9	Control of Access	This is an application specific requirement that is dependent on a plant design. Therefore this requirement is not addressed for the MELTAC platform.	None
5.10	Repair	The MELTAC platform has Self-diagnosis functions and engineering tool features to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment.	<u>JEXU-1041-1008</u> 4.1.4, 4.1.5, 4.2.3
5.11	Identification	<del>This is an application specific requirement that is dependent on a plant design. Therefore this requirement is not addressed for the MELTAC platform.</del> <u>Hardware, software and documents of the MELTAC platform are uniquely identified including “nuclear safety related” markings, as described in Section 6.1.7 of JEXU-1041-1008, “Safety System Digital Platform - MELTAC - Topical Report”. This identification is controlled in accordance with MELCO’s 10 CFR 50 Appendix B QAP.</u>	<del>None</del> <u>JEXU-1041-1008</u> <u>6.1.7</u>
5.12	Auxiliary Features	This is an application specific requirement that is dependent on a plant design. Therefore this requirement is not addressed for the MELTAC platform.	None

COMPLIA  
NCE-1

---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

**9/23/2016**

**SAFETY SYSTEM DIGITAL PLATFORM  
- MELTAC (MITSUBISHI ELECTRIC TOTAL ADVANCED CONTROLLER) -  
TOPICAL REPORT**

**Mitsubishi Electric Corporation**

**TAC NO.: MF4228**  
**RAI NO.: #1**  
**DATE OF RAI ISSUE: 6/29/2016**

---

**QUESTION NO.: 3 for JEXU-1041-1018, "Summary of Compliance to the IEEE Std. 603 and IEEE Std. 7-4.3.2"**

Page 12, Table 3, IEEE 603, 6.6 & 6.7, Operating and Maintenance Bypasses. Confirm for the NRC staff that the generic platform has the capability to complete these two requirements. It is understood by the NRC staff that specific operating bypasses are defined on a plant specific basis as well as plant specific Technical Specifications govern the use of the maintenance bypass feature.

---

**ANSWER:**

The "Assessment" entry for Section 6.6 in Table 3 will be revised as follows:

This is an application specific requirement that is dependent on the plant design. The generic MELTAC application program function symbols shown in Appendix B of the JEXU-1041-1008, "Safety System Digital Platform - MELTAC - Topical Report" are suitable for generating operating bypass permissive interlocks and automatic removal of operating bypass by plant condition.

The "Assessment" entry for Section 6.7 in Table 3 will be revised as follows:

This is an application specific requirement that is dependent on the plant design. The MELTAC application program function symbols shown in Appendix B of JEXU-1041-1008, "Safety System Digital Platform - MELTAC - Topical Report" and the inter-division Data Link are suitable for:

- (1) generating a maintenance bypass interlock to prevent multiple bypasses of the same process parameters measured in multiple safety divisions.

- (2) generating a voting logic that ensures that a safety function can be accomplished while a maintenance bypass is in effect.

The MELTAC platform also provides the capability to automatically initiate maintenance bypasses for self-detected failure condition. For example, the MELTAC platform has the capability for detecting communication failures, as described in JEXU-1041-1015, “MELTAC Platform ISG-04 Conformance Analysis”. When any communication error is detected, the affected measurement channel(s) can be bypassed automatically. In addition, the MELTAC platform has the capability for detecting analog input failures, as described in Section 4.1.5.5.1 of JEXU-1041-1008, “Safety System Digital Platform - MELTAC - Topical Report”. When an I/O module failure is detected, the affected measurement channel can be bypassed automatically.

Figure 1 shows the failure detection capability of the MELTAC platform for automatic maintenance bypass in a typical system configuration. Any automatic maintenance bypass is subject to any application interlocks that may prohibit the automatic maintenance bypass if a channel from another division is already bypassed.

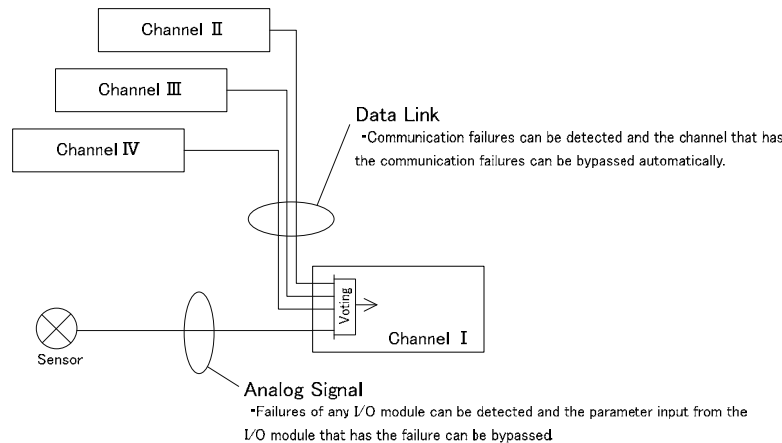


Figure 1 Failure detection capability for maintenance bypass

### Impact on Technical Report

Table 3 of JEXU-1041-2080, “Summary of Compliance to the IEEE Std. 603 and IEEE Std. 7-4.3.2” will be revised by adding the above evaluation (see Attachment-1).

Table 3 IEEE Std. 603 (1991) Compliance Matrix

Section	Title	Assessment	References <Document Number Sections>
6.2	Manual Control	This is an application specific requirement that is dependent on a plant design. Therefore this requirement is not addressed for the MELTAC platform.	None
6.3	Interaction Between the Sense and Command Features and Other Systems	This is an application specific requirement that is dependent on a plant design. Therefore this requirement is not addressed for the MELTAC platform.	None
6.4	Derivation of System Inputs	This is an application specific requirement that is dependent on a plant design. Therefore this requirement is not addressed for the MELTAC platform.	None
6.5	Capability for Testing and Calibration	The MELTAC platform contains Self-diagnosis features to identify failures.  Testing and calibration during system operation can be accomplished by the appropriate MELTAC platform system configuration. This is an application specific item that is dependent on the plant design.	<u>JEXU-1041-1008</u> 4.1.5, 4.2.3, 7.0 <u>JEXU-1041-1030</u> <u>JEXU-1041-1027</u>
6.6	Operating Bypasses	This is an application specific requirement that is dependent on a plant design. <del>Therefore this requirement is not addressed for the MELTAC platform.</del> <u>The MELTAC application program function symbols, shown in Appendix B of JEXU-1041-1008, "Safety System Digital Platform - MELTAC - Topical Report" are suitable for generating operating bypass permissive interlocks and automatic removal of operating bypass by plant condition.</u>	<del>None</del> <u>JEXU-1041-1008</u> <u>Appendix B</u>

COMPLIA  
NCE-3

Table 3 IEEE Std. 603 (1991) Compliance Matrix

Section	Title	Assessment	References <Document Number Sections>
6.7	Maintenance Bypass	<p>This is an application specific requirement that is dependent on a plant design. <del>Therefore this requirement is not addressed for the MELTAC platform.</del> The MELTAC application program function symbols shown in Appendix B of JEXU-1041-1008, "Safety System Digital Platform - MELTAC - Topical Report" and the inter-division Data Link are suitable for:</p> <p>(1) <u>generating a maintenance bypass interlock to prevent multiple bypasses of the same process parameters measured in multiple safety divisions.</u></p> <p>(2) <u>generating a voting logic that ensures that a safety function can be accomplished while a maintenance bypass is in effect.</u></p> <p>The MELTAC platform also provides the capability to <u>automatically initiate maintenance bypasses for self-detected failure condition. For example, the MELTAC platform has the capability for detecting communication failures, as described in JEXU-1041-1015, "MELTAC platform ISG-04 Conformance Analysis". When any communication error is detected, the affected measurement channel(s) can be bypassed automatically. In addition, the MELTAC platform has the capability for detecting analog input failures, as described in Section 4.1.5.5.1 of JEXU-1041-1008, "Safety System Digital Platform - MELTAC - Topical Report". When an I/O module failure is detected, the affected measurement channel can be bypassed automatically.</u></p>	<p><del>None</del></p> <p><u>JEXU-1041-1008</u> <u>4.1.5.5.1, Appendix B</u> <u>JEXU-1041-1015</u></p>

COMPLIA  
NCE-3

---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

**9/23/2016**

**SAFETY SYSTEM DIGITAL PLATFORM  
- MELTAC (MITSUBISHI ELECTRIC TOTAL ADVANCED CONTROLLER) -  
TOPICAL REPORT**

**Mitsubishi Electric Corporation**

**TAC NO.: MF4228  
RAI NO.: #1  
DATE OF RAI ISSUE: 6/29/2016**

---

**QUESTION NO.: 1 for JEXU-1041-1015, "MELTAC Platform ISG-04 Conformance Analysis"**

With regards to the response to Staff Position 2; the last sentence of staff position 2 is not addressed, that is "This protection must be sustained despite any operation, malfunction, design error, communication error, or software error or corruption existing or originating outside the division." Please provide additional information to demonstrate compliance with this position.

---

**ANSWER:**

[

]

**Impact on Technical Report.**

Section 3.1.2 of JEXU-1041-1015, "MELTAC Platform ISG-04 Conformance Analysis" will be revised by adding the above evaluation (see Attachment-1).

### 3.1.2 Staff Position 2

Requirement	The safety function of each safety channel should be protected from adverse influence from outside the division of which that channel is a member. Information and signals originating outside the division must not be able to inhibit or delay the safety function. This protection must be implemented within the affected division (rather than in the sources outside the division), and must not itself be affected by any condition or information from outside the affected division. This protection must be sustained despite any operation, malfunction, design error, communication error, or software error or corruption existing or originating outside the division.
Analysis	

ISG-04-1



---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

9/23/2016

**SAFETY SYSTEM DIGITAL PLATFORM  
- MELTAC (MITSUBISHI ELECTRIC TOTAL ADVANCED CONTROLLER) -  
TOPICAL REPORT**

**Mitsubishi Electric Corporation**

**TAC NO.: MF4228**  
**RAI NO.: #1**  
**DATE OF RAI ISSUE: 6/29/2016**

---

**QUESTION NO.: 2 for JEXU-1041-1015, "MELTAC Platform ISG-04 Conformance Analysis"**

With regards to the response to Staff Position 3; is the "vital communication" division voting logic the only input coming from outside the division (i.e. request for actuation coming from the other divisions)? If not what are the other inputs coming from outside the division that is necessary for the generic platform?

---

**ANSWER:**

[

]

**Impact on Technical Report**

Section 3.1.3 of JEXU-1041-1015, "MELTAC Platform ISG-04 Conformance Analysis" will be revised by adding the above evaluation (see Attachment-1).

### 3.1.3 Staff Position 3

Requirement	<p>A safety channel should not receive any communication from outside its own safety division unless that communication supports or enhances the performance of the safety function. Receipt of information that does not support or enhance the safety function would involve the performance of functions that are not directly related to the safety function. Safety systems should be as simple as possible. Functions that are not necessary for safety, even if they enhance reliability, should be executed outside the safety system. A safety system designed to perform functions not directly related to the safety function would be more complex than a system that performs the same safety function, but is not designed to perform other functions. The more complex system would increase the likelihood of failures and software errors. Such a complex design, therefore, should be avoided within the safety system. For example, comparison of readings from sensors in different divisions may provide useful information concerning the behavior of the sensors (for example, On-Line Monitoring). Such a function executed within a safety system, however, could also result in unacceptable influence of one division over another, or could involve functions not directly related to the safety functions, and should not be executed within the safety system. Receipt of information from outside the division, and the performance of functions not directly related to the safety function, if used, should be justified. It should be demonstrated that the added system/software complexity associated with the performance of functions not directly related to the safety function and with the receipt of information in support of those functions does not significantly increase the likelihood of software specification or coding errors, including errors that would affect more than one division. The applicant should justify the definition of “significantly” used in the demonstration.</p>
Analysis	

ISG-04-2

---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

**9/23/2016**

**SAFETY SYSTEM DIGITAL PLATFORM  
- MELTAC (MITSUBISHI ELECTRIC TOTAL ADVANCED CONTROLLER) -  
TOPICAL REPORT**

**Mitsubishi Electric Corporation**

**TAC NO.: MF4228  
RAI NO.: #1  
DATE OF RAI ISSUE: 6/29/2016**

---

**QUESTION NO.: 4 for JEXU-1041-1015, "MELTAC Platform ISG-04 Conformance Analysis"**

With regards to the response to Staff Position 7, The NRC staff requires additional information on the characteristics of a predefined data set used in MELTAC communication interfaces to support its safety evaluation. This information should include message formatting and protocol, message identification, status information, as well as signal attributes such as point of signal origin and destination. Include a discussion of how unrecognized messages are handled.

---

**ANSWER:**

[

]

**Impact on Topical Report**

There is no impact on the Topical Report.

**Impact on Technical Report**

Section 3.1.7 of JEXU-1041-1015, "MELTAC Platform ISG-04 Conformance Analysis" will be revised by adding the description above.

3.1.7 Staff Position 7

Requirement
Only predefined data sets should be used by the receiving system. Unrecognized messages and data should be identified and dispositioned by the receiving system in accordance with the pre-specified design requirements. Data from unrecognized messages must not be used within the safety logic executed by the safety function processor. Message format and protocol should be pre-determined. Every message should have the same message field structure and sequence, including message identification, status information, data bits, etc. in the same locations in every message. Every datum should be included in every transmit cycle, whether it has changed since the previous transmission or not, to ensure deterministic system behavior.
Analysis

ISG-04-4

---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

9/23/2016

**SAFETY SYSTEM DIGITAL PLATFORM  
- MELTAC (MITSUBISHI ELECTRIC TOTAL ADVANCED CONTROLLER) -  
TOPICAL REPORT**

**Mitsubishi Electric Corporation**

**TAC NO.: MF4228**  
**RAI NO.: #1**  
**DATE OF RAI ISSUE: 6/29/2016**

---

**QUESTION NO.: 6 for JEXU-1041-1015, "MELTAC Platform ISG-04 Conformance Analysis"**

With regard to the response to Staff Position 12, the NRC staff does not have information needed to perform an evaluation of faults 1 through 12 identified in this staff position. Please provide a discussion of how each of these faults as well as any additional identified communications faults will be handled by the MELCO safety platform and identify any application specific features needed to support system response to such faults.

---

**ANSWER:**

[

]

**Impact on Technical Report**

There is no impact on the Technical Report.

## **PART 3-3**

### **Responses to RAI, including:**

Transmittal Letter, dated October 7, 2016

JEXU-1041-2070 R0 (Response to Design RAI 1)

JEXU-1041-2071 R0 (Response to Design RAI 2)

JEXU-1041-2072 R0 (Response to Design RAI 3)

JEXU-1041-2083 R0 (Response to ISG04CA RAI 3)

JEXU-1041-2092 R0 (Response to EQ RAI 4)

JEXU-1041-2079 R0 (Response to IEEE CMs RAI 2)



October 7, 2016  
JEXU-1041-8527

Document Control Desk  
U.S. Nuclear Regulatory Commission  
11555 Rockville Pike  
Rockville, MD 20852-2738

Attention: Mr. Joseph Holonich

**SUBJECT: MELCO's responses to MELTAC Topical Report Revision 0 RAI #1 (TAC No.MF4228)  
(Regarding, items No.1, 2 and 3 for JEXU-1041-2022, "Summary of MELTAC  
Platform Design" and item No.3 for JEXU-1041-1015, "MELTAC Platform ISG-04  
Conformance Analysis", item No.4 for JEXU-1041-1023, "Summary of MELTAC  
Platform Equipment Qualification" and item No.2 for JEXU-1041-1018, "Summary of  
Compliance to the IEEE Std. 603 and IEEE Std. 7-4.3.2") and MELTAC Topical  
Report Supporting Documentation**

With this letter, Mitsubishi Electric Corporation (MELCO) submits the documents listed in the enclosures table below to the U.S. Nuclear Regulatory Commission (NRC).

Enclosed are the documents that make up the response to No.1, 2 and 3 for JEXU-1041-2022, "Summary of MELTAC Platform Design", No.3 for JEXU-1041-1015, "MELTAC Platform ISG-04 Conformance Analysis", No.4 for JEXU-1041-1023, "Summary of MELTAC Platform Equipment Qualification" and No.2 for JEXU-1041-1018, "Summary of Compliance to the IEEE Std. 603 and IEEE Std. 7-4.3.2" and supporting documentation of MELTAC lifecycle document schedule. As indicated in the enclosed materials, these documents contain information that MELCO considers proprietary, and therefore should be withheld from public disclosure pursuant to 10 C.F.R 2.390 (a)(4) as trade secrets and commercial or financial information which is privileged or confidential.

The accompanying affidavit, Enclosure (1) sets forth the basis on which the information identified as proprietary should be withheld from public disclosure.

Sincerely,

Shigeru Sugitani  
Senior Manager, Control & Protection Systems Section  
Nuclear Power Department, Energy Systems Center  
Mitsubishi Electric Corporation



**Enclosures:**

No.	Document Number	Document Title	Date of Issue
1	-	Affidavit of Shigeru Sugitani	10/07/2016
2	JEXU-1041-2051-P JEXU-1041-2051-NP	MELTAC Life Cycle Document Schedule	10/07/2016
3	JEXU-1041-2070-P	1 for JEXU-1041-2022, "Summary of MELTAC Platform Design"	10/07/2016
4	JEXU-1041-2070-NP		
5	JEXU-1041-2071-P	2 for JEXU-1041-2022, "Summary of MELTAC Platform Design"	10/07/2016
6	JEXU-1041-2071-NP		
7	JEXU-1041-2072	3 for JEXU-1041-2022, "Summary of MELTAC Platform Design"	10/07/2016
8	JEXU-1041-2083-P	3 for JEXU-1041-1015, "MELTAC Platform ISG-04 Conformance Analysis"	10/07/2016
9	JEXU-1041-2083-NP		
10	JEXU-1041-2092-P	4 for JEXU-1041-1023, "Summary of MELTAC Platform Equipment Qualification"	10/07/2016
11	JEXU-1041-2092-NP		
12	JEXU-1041-2079	2 for JEXU-1041-1018, "Summary of Compliance to the IEEE Std. 603 and IEEE Std. 7-4.3.2"	10/07/2016

CC: Gilbert W. Remley  
Nuclear Systems Department Manager  
Mitsubishi Electric Power Products, Inc.

---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

10/7/2016

**SAFETY SYSTEM DIGITAL PLATFORM  
- MELTAC (MITSUBISHI ELECTRIC TOTAL ADVANCED CONTROLLER) -  
TOPICAL REPORT**

**Mitsubishi Electric Corporation**

**TAC NO.: MF4228**  
**RAI NO.: #1**  
**DATE OF RAI ISSUE: 6/29/2016**

---

**QUESTION NO.: 1 for JEXU-1041-1022, "Summary of MELTAC Platform Design"**

Software Requirements Specification (SRS) & Software Design Specifications (SDS):

- a. The summary document, JEXU-1041-1022, states the MELCO document which contains the information for a software requirements specification is "MELTAC-Nplus S System Specification." Section 4.1, "System Specification (Platform Specification)." The summary document provides the table of contents of the System Specification but not the specification itself. The NRC requires System Specifications to support its safety evaluation. The NRC staff has endorsed Institute of Electrical and Electronics Engineers (IEEE) Standard 830-1998, "IEEE Recommended Practice for Software Requirements Specifications," by regulatory guide (RG) 1.172. Also, the NRC Standard Review Plan (SRP) Section 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems," Section B.3.3.1 provides acceptance criteria for a SRS. Additional guidance can be found in NUREG/CR-6101 Sections 3.2.1 and 4.2.1. The acceptance criteria using these references is delineated in ISG-06 Section D.4.4.3.1. The summary document points to JEXU-1024-1010, "MELTAC-Nplus S System Specification." Therefore the staff requests this document be submitted on the docket with an analysis of conformance to the acceptance criteria, or any alternatives, to RG 1.172 and the applicable sections of the SRP, Section 7.14, specifically identified.
- b. ISG-06. Section D.4.4.3.3, references the acceptance criteria for the software design specification including the SRP Section BTP 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems," Section B.3.3.3, "Design Activities – Software Design Specification

(SDS).” This guidance provides functional and process characteristics as well as review guidance of SDSs.

Provide an explanation how the following documents, identified in Table 1 and Appendix A, provide the information for the controller CPU module to conform to the Software Design Specification guidance stated above. Also the NRC staff requests these documents be submitted on the docket:

Hardware Requirement Specification, JEXU-1024-1021,  
Hardware Specification, JEXU-1024-1051,  
Software Specification, JSX4L400,  
FPGA Specification, JEXU-1024-1071.

---

**ANSWER:**

[

]

**Impact on Topical Report**

There is no impact on the Topical Report.

**Impact on Technical Report**

Regarding a.), Section 2.0 of "Summary of MELTAC Platform Design" (JEXU-1041-1022) will be revised. Appendix B will be added to "Summary of MELTAC Platform Design" (JEXU-1041-1022) (see Attachment-1).

Regarding b.), Section 2.0 of "Summary of MELTAC Platform Design" (JEXU-1041-1022) will be revised. Appendix C will be added to "Summary of MELTAC Platform Design" (JEXU-1041-1022) (see Attachment-1).

## 1.0 INTRODUCTION

This summary describes the design documents associated with the Mitsubishi Electric Corporation (MELCO) Energy Systems Center (ESC) Mitsubishi Electric Total Advanced Controller (MELTAC) Platform. The MELCO ESC design documents encompass the MELTAC Platform hardware and the basic software, which includes the firmware and Field Programmable Gate Arrays (FPGAs) on all MELTAC Platform modules.

This document supports the “Safety System Digital Platform - MELTAC - Topical Report” (JEXU-1041-1008) and satisfies the commitments made under Table 1 sections 1.12, 1.13, 2.3, 2.9, 3.1, 3.3, 3.7, 3.8, 3.9 and 3.10 of “Mapping of MELTAC Platform Licensing Documents to the DI&C-ISG-06 Guidance” (JEXU-1041-1012).

## 2.0 DOCUMENTATION TREE AND CATEGORIZATION

Figure 1 shows the MELTAC Platform Documentation Tree. These documents are internal documents, which are categorized into three groups according to the following phases: Design Phase, Qualification Phase, and V&V Phase. The scope of this summary is the design documents prepared in the Design Phase.

The Qualification Phase documents are described in “Summary of MELTAC Platform Equipment Qualification” (JEXU-1041-1023), and the V&V Phase documents are described in “Summary of MELTAC Platform V&V” (JEXU-1041-1026).

The MELTAC Platform Design documents corresponding to the information required by DI&C-ISG-06 “Licensing Process” (ISG-06) Enclosure B (Tier 3) are listed in Section 3. Specific document numbers are identified in Appendix A.

The types and summaries of the design documents related to the MELTAC Platform are listed in Section 4.

The conformance of Software Requirements Specification (SRS), regarding NRC Standard Review Plan (SRP) Section 7-14, “Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems,” Section B.3.3.1 acceptance criteria for SRS, is evaluated in Appendix B.

Design-1a

The conformance of Software Design Specification (SDS), regarding NRC Standard Review Plan (SRP) Section 7-14, “Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems,” Section B.3.3.3 acceptance criteria for SDS, is evaluated in Appendix C.

Design-1b

**APPENDIX B CONFORMANCE EVALUATION OF SOFTWARE REQUIREMENT SPECIFICATION**

Table B-1 Conformance of SRP Section BTP 7-14  
Section B.3.3.1.1 Functional Characteristics of SRS


Design-1a


Design-1a


## Design-1a



Table B-2 Conformance of SRP Section BTP 7-14  
Section B.3.3.1.2 Process Characteristics of SRS


Design-1a


Design-1a


## Design-1a


Design-1a

**APPENDIX C CONFORMANCE EVALUATION OF SOFTWARE DESIGN SPECIFICATIONS**

Table C-1 Conformance of SRP Section BTP 7-14  
Section B.3.3.3.1 Functional Characteristics of SDS


Design-1b


Design-1b


Design-1b

Table C-2 Conformance of SRP Section BTP 7-14  
Section B.3.3.3.2 Process Characteristics of SDS


Design-1b



## Design-1b

[illegible]

## Design-1b


Design-1b

---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

10/7/2016

**SAFETY SYSTEM DIGITAL PLATFORM  
- MELTAC (MITSUBISHI ELECTRIC TOTAL ADVANCED CONTROLLER) -  
TOPICAL REPORT**

**Mitsubishi Electric Corporation**

**TAC NO.: MF4228**  
**RAI NO.: #1**  
**DATE OF RAI ISSUE: 6/29/2016**

---

**QUESTION NO.: 2 for JEXU-1041-2022, “Summary of MELTAC Platform Design”**

Thoroughly explain the statement on page 1; “Since the development of the MELTAC Platform is ongoing, only auditable documents are listed in Appendix A”. The staff needs to understand the extent of the ongoing development process and the limitations of document availability. Please identify by specific type what activities, equipment, procedures are not complete and why the changes are taking place including those involved in the MELTAC Reevaluation Program. Also include the schedule to complete the development.

---

**ANSWER:**

[

]

**Impact on Topical Report**

There is no impact on Topical Report.

---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

10/7/2016

**SAFETY SYSTEM DIGITAL PLATFORM  
- MELTAC (MITSUBISHI ELECTRIC TOTAL ADVANCED CONTROLLER) -  
TOPICAL REPORT**

**Mitsubishi Electric Corporation**

**TAC NO.: MF4228**  
**RAI NO.: #1**  
**DATE OF RAI ISSUE: 6/29/2016**

---

**QUESTION NO.: 3 for JEXU-1041-2022, “Summary of MELTAC Platform Design”**

The MELTAC-N plus S Basic Software Update Project was not scheduled to be finished until after the NRC inspection in 2011, therefore the NRC inspection team limited its review to completed supporting documents for the requirement, software design, implementation, and maintenance phases. (Note: this did not include testing or the test plans). Identify when this was completed or identify any activities yet to be completed, by procedure, and identify the schedule for completion.

---

**ANSWER:**

Please see answer to QUESTION NO.: 2 for JEXU-1041-2022, “Summary of MELTAC Platform Design”.

The schedule is described in JEXU-1041-2051.

**Impact on Technical Report**

There is no impact on the Technical Report.

---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

10/7/2016

**SAFETY SYSTEM DIGITAL PLATFORM  
- MELTAC (MITSUBISHI ELECTRIC TOTAL ADVANCED CONTROLLER) -  
TOPICAL REPORT**

**Mitsubishi Electric Corporation**

**TAC NO.: MF4228**  
**RAI NO.: #1**  
**DATE OF RAI ISSUE: 6/29/2016**

---

**QUESTION NO.: 3 for JEXU-1041-1015, "MELTAC platform ISG-04 Conformance Analysis"**

With regards to the response to Staff Position 4; this is the only place the communications processor is a "to be determined" processing technology. Discussion within this section and the topical report, such as section 4.3.3.5.1, "Detailed Data Flow," identifies this as a [ ]. The NRC staff requires the technology of the communications processor to be determined and consistent with the design, process and procedures. If this processor is yet to be determined, or is being changed, the NRC staff needs to be notified of the changes.

---

**ANSWER:**

[

]

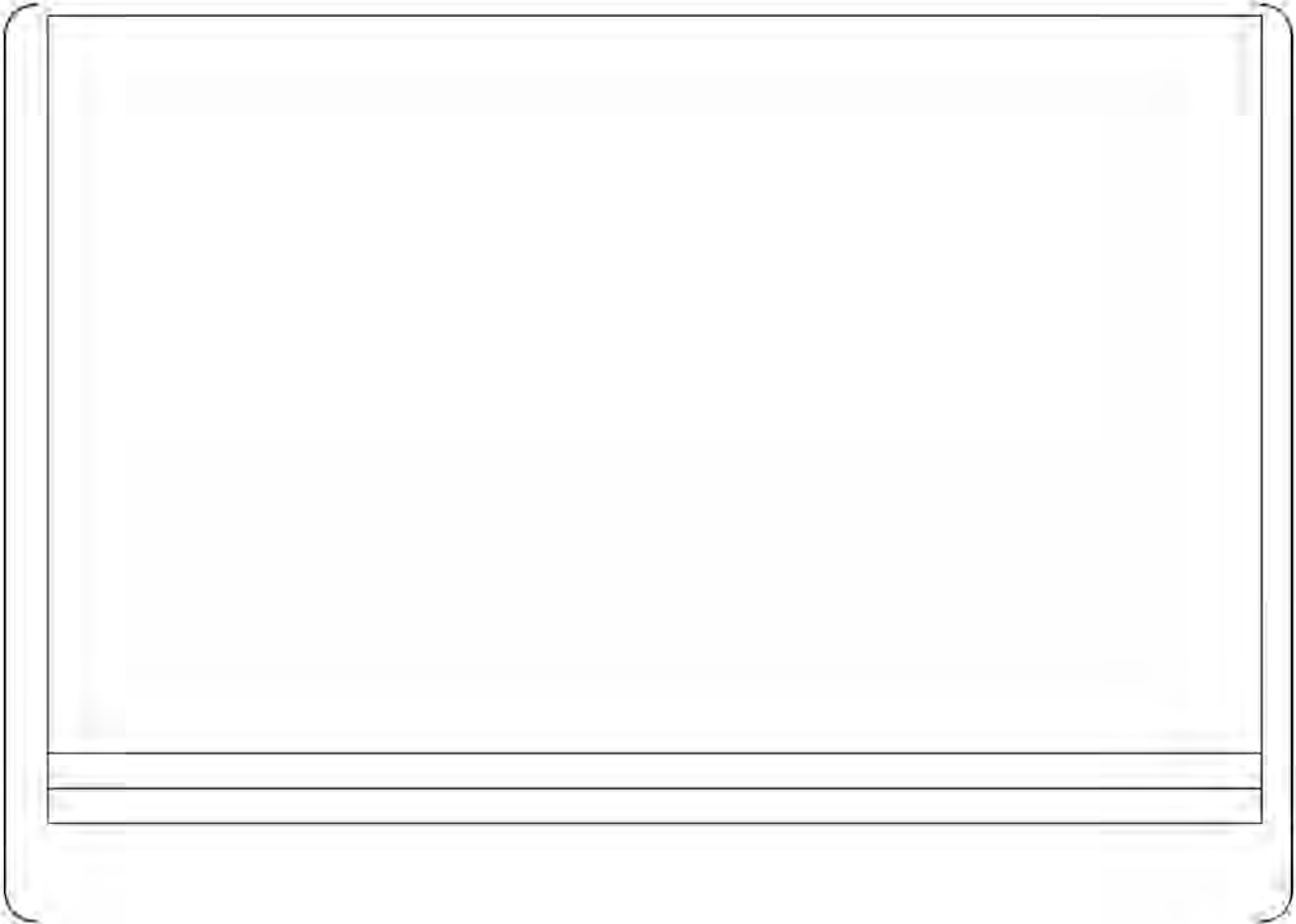
**Impact on Technical Report**

Section 3.1.4 of JEXU-1041-1015, "MELTAC Platform ISG-04 Conformance Analysis" will be revised by adding explanation about technology applied for communication processor and deleting the ambiguous note (see Attachment-1).

3.1.4 Staff Position 4

Requirement
<p>The communication process itself should be carried out by a communications processor<sup>ii</sup> separate from the processor that executes the safety function, so that communications errors and malfunctions will not interfere with the execution of the safety function. The communication and function processors should operate asynchronously, sharing information only by means of dual-ported memory or some other shared memory resource that is dedicated exclusively to this exchange of information. The function processor, the communications processor, and the shared memory, along with all supporting circuits and software, are all considered to be safety-related, and must be designed, qualified, fabricated, etc., in accordance with 10 C.F.R. Part 50, Appendix A and B. Access to the shared memory should be controlled in such a manner that the function processor has priority access to the shared memory to complete the safety function in a deterministic manner.</p> <p>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.</p>
Analysis

ISG-04-3



ISG-04-3



---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

10/7/2016

**SAFETY SYSTEM DIGITAL PLATFORM  
- MELTAC (MITSUBISHI ELECTRIC TOTAL ADVANCED CONTROLLER) -  
TOPICAL REPORT**

**Mitsubishi Electric Corporation**

**TAC NO.:** MF4228  
**RAI NO.:** #1  
**DATE OF RAI ISSUE:** 6/29/2016

---

**QUESTION NO.:** 4 for JEXU-1041-1023, "Summary of MELTAC Platform Equipment Qualification," Rev.2

Per ISG-06, Section D.5.2 "Information to be Provided," states that the Summary of Testing Results should be provided during Phase 2 which requires submittal 12 months prior to requested approval. In light of MELCO's phased redevelopment of modules including redesign and testing, please identify when the test results will be submitted for all modules. Per the lack of information identified in the EQ Summary document as noted in RAI(s) 1 - 3 , the NRC may have to request the actual test procedures and reports to be submitted on the docket for the equipment qualification review.

---

**ANSWER:**

The requested information identified in Question No.1, 2 and 3 for JEXU-1041-1023, "Summary of MELTAC Platform Equipment Qualification," Rev.2 will be added to JEXU-1041-1023, "Summary of MELTAC Platform Equipment Qualification" according to the attached schedule (see Attachment -1).

**Impact on Technical Report**

The above revised schedule will be reflected in JEXU-1041-1012, "Mapping of MELTAC Platform Licensing Documents to the DI&C-ISG-06 Guidance" Rev.2.

## Mapping of MELTAC Platform Licensing Documents to the DI&amp;C-ISG-06 Guidance

JEXU-1041-1012-NP (R42)

Table 2 Submitted MELTAC Documents to be Revised

Document Title	Document Number	Submitted Date and Revision	Planned Submittal Date (Revision Number)				
Summary of MELTAC Platform Design	JEXU-1041-1022-P JEXU-1041-1022-NP	<u>May 2016</u> ≤Rev.1≥ (*1)	<del>May 2016</del> ←Rev.1 Submitted→	Oct. 2016 (Rev.2) (*2)	Feb. 2017 (Rev.3) (*3)	-	
Summary of MELTAC Platform Reliability	JEXU-1041-1027-P JEXU-1041-1027-NP	<u>May 2016</u> ≤Rev.1≥ (*1)	<del>May 2016</del> ←Rev.1 Submitted→	Oct. 2016 (Rev.2) (*2)	Feb. 2017 (Rev.3) (*3)	-	
Summary of MELTAC Platform Equipment Qualification	JEXU-1041-1023-P JEXU-1041-1023-NP	<u>Feb.2016</u> ≤Rev.2≥ (*1)	Oct. 2016 (Rev.3) (*4)	<del>Feb.2017</del> <u>May.2017</u> (Rev.4) (*5)	-	-	
Summary of MELTAC Platform V&V	JEXU-1041-1026-P JEXU-1041-1026-NP	<u>May 2016</u> ≤Rev.2≥ (*1)	<del>May 2016</del> ←Rev.2 Submitted→	Oct. 2016 (Rev.3) (*4)	<del>Feb. 2017</del> <u>Nov.2016</u> (Rev.4) (*2)	<u>Mar.2017</u> (Rev.5) (*3)	

(\*1) This revision scope is indicated in Table 3, No.1.

(\*2) This revision scope is indicated in Table 3, No.2.

(\*3) This revision scope is indicated in Table 3, No.3.

(\*4) This revision is provided to add the detailed explanation regarding the test results for the scope of Table 3, No1.

(\*5) This revision scope is indicated in Table 3, No.2 and No.3. Note there is a possibility that the planned submittal date of this revision will be revised depending on the EQ test progress.

Table 3 ~~Planned~~-Revision Scope for Summary of MELTAC Platform Design / Reliability / Equipment Qualification / V&V


---

---

## RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

---

---

10/7/2016

### SAFETY SYSTEM DIGITAL PLATFORM - MELTAC (MITSUBISHI ELECTRIC TOTAL ADVANCED CONTROLLER) - TOPICAL REPORT

Mitsubishi Electric Corporation

TAC NO.: MF4228  
RAI NO.: #1  
DATE OF RAI ISSUE: 6/29/2016

---

#### QUESTION NO.: 2 for JEXU-1041-1018, "Summary of Compliance to the IEEE Std. 603 and IEEE Std. 7-4.3.2"

Also on Page 10, Table 3, IEEE 603, 5.14, Human Factors. This requirement includes how certain safety system design goals should be met in accordance with IEEE Std 1023. This includes maintenance of the displays (Safety VDUs) which provides assembly/ disassembly, tools required and interchangeability of parts as well as features to prevent incorrect assembly. The staff requests information including an explanation of why such an evaluation would not be required on a generic basis (versus application specific) for the Safety VDUs.

---

#### ANSWER:

The "Assessment" entry for Section 5.14 of "Table 1 IEEE Std. 603 (1991) Compliance Matrix" will be replaced with the following:

Human factors engineering is applied to the MELTAC platform to ensure the human systems interfaces for generic platform maintenance activities meet the safety system design goals. The HFE process is guided by IEEE 1023, with a graded approach that considers that the MELTAC human systems interfaces for maintenance activities are less significant than those of plant operations. Therefore, the MELTAC HFE focus is in two areas:

- Using the MELTAC engineering tool to (1) identify failed components detected by the MELTAC self-diagnostic functions, and (2) conduct periodic surveillance tests that are assigned to maintenance personnel, such as channel calibration and memory integrity check (MIC). MELCO HFE personnel review the MELTAC engineering tool screen designs to ensure they are suitable for these tasks and are not contributors to human performance errors.
- Spare parts replacement of failed MELTAC components, including the safety VDU panel. Spare part replacement does not need any special

tools or any special methods. Instructions for parts replacement, such as the caution to de-energize specific components prior to replacement and configuration settings, are identified in the MELTAC platform technical manual. All replaceable parts are clearly labeled. Replaceable parts also include physical installation guides. These guides prevent parts installation in wrong direction. MELCO HFE personnel review the generic platform design and maintenance documentation to ensure the MELTAC platform has the appropriate measures to prevent incorrect spare parts replacement.

The functions allocated, in whole or in part, to plant operators and the human systems interface design for plant operators, are dependent on a specific plant design. Therefore, the HFE considerations for these functions are not addressed generically for the MELTAC platform.

**Impact on Technical Report**

JEXU-1041-1018 "Summary of Compliance to the IEEE Std. 603 and IEEE Std. 7-4.3.2" will be revised as identified above (see Attachment-1).

Table 3 IEEE Std. 603 (1991) Compliance Matrix

Section	Title	Assessment	References <Document Number Sections>
5.13	Multi-Unit Stations	This is an application specific requirement that is dependent on a plant design. Therefore this requirement is not addressed for the MELTAC platform.	None
5.14	Human Factors Considerations	<p><del>This is an application specific requirement that is dependent on a plant design. Therefore this requirement is not addressed for the MELTAC platform.</del></p> <p>Human factors engineering is applied to the MELTAC platform to ensure the human systems interfaces for generic platform maintenance activities meet the safety system design goals. The HFE process is guided by IEEE 1023, with a graded approach that considers that the MELTAC human systems interfaces for maintenance activities are less significant than those of plant operations. Therefore, the MELTAC HFE focus is in two areas:</p> <ul style="list-style-type: none"> <li>• Using the MELTAC Engineering Tool to (1) identify failed components detected by the MELTAC self-diagnostic functions, and (2) conduct periodic surveillance tests that are assigned to maintenance personnel, such as channel calibration and memory integrity check (MIC). MELCO HFE personnel review the MELTAC Engineering Tool screen designs to ensure they are suitable for these tasks and are not contributors to human performance errors.</li> </ul>	<p>None</p> <p><a href="#">JEXU-1041-1008</a> <a href="#">4.1.4, 4.1.7</a></p>

COMPLIA  
NCE-2

Table 3 IEEE Std. 603 (1991) Compliance Matrix

Section	Title	Assessment	References <Document Number Sections>
		<ul style="list-style-type: none"> <li><u>Spare parts replacement of failed MELTAC components, including the safety VDU panel. Spare part replacement doesn't need any special tools or any special methods. Instructions for parts replacement, such as the caution to de-energize specific components prior to replacement and configuration settings, are identified in the MELTAC platform technical manual. All replaceable parts are clearly labeled. Replaceable parts also include physical installation guides. These guides prevent parts installation in the wrong direction. MELCO HFE personnel review the generic platform design and maintenance documentation to ensure the MELTAC platform has the appropriate measures to prevent incorrect spare parts replacement.</u></li> </ul> <p><u>The functions allocated, in whole or in part, to plant operators and the human systems interface design for plant operators, are dependent on a specific plant design. Therefore, the HFE consideration for these functions is not addressed generically for the MELTAC platform.</u></p>	
5.15	Reliability	<p>This is an application specific item that is dependent on the plant design. The MELTAC platform includes features to minimize the possibility of a single failure affecting the operation of the equipment.</p> <p>The MELTAC platform contains Self-diagnosis features to identify failures.</p> <p>Failure Mode and Effects Analysis (FMEA) and the reliability data for each MELTAC platform module is provided for input to the application level systems analysis.</p>	<p><u>JEXU-1041-1008</u> 4.1.5, 4.2.3, 7.0 <u>JEXU-1041-1030</u> <u>JEXU-1041-1027</u></p>

COMPLIA  
NCE-2

## **PART 3-4**

### **Responses to RAI, including:**

Transmittal Letter, dated October 17

JEXU-1041-2089 R0 (Response to EQ RAI 1)

JEXU-1041-2090 R0 (Response to EQ RAI 2)

JEXU-1041-2091 R0 (Response to EQ RAI 3)

JEXU-1041-2088 R0 (Response to QA RAI 2)





October 17, 2016  
JEXU-1041-8529

Document Control Desk  
U.S. Nuclear Regulatory Commission  
11555 Rockville Pike  
Rockville, MD 20852-2738

Attention: Mr. Joseph Holonich

**SUBJECT: MELCO's responses to MELTAC Topical Report Revision 0 RAI #1 (TAC No.MF4228)  
(Regarding, items No.1 through No.3 for JEXU-1041-1023, "Summary of MELTAC  
Platform Equipment Qualification" and item No.2 for JEXU-1041-1025, "Summary of  
MELTAC Platform QA") and Summary of MELTAC Platform CGD Activity**

With this letter, Mitsubishi Electric Corporation (MELCO) submits the documents listed in the enclosures table below to the U.S. Nuclear Regulatory Commission (NRC).

Enclosed are the documents that make up the response to items No.1 through No.3 for JEXU-1041-1023, "Summary of MELTAC Platform Equipment Qualification" and item No.2 for JEXU-1041-1025, "Summary of MELTAC Platform QA" and the corresponding documents, Summary of MELTAC Platform Equipment Qualification, Summary of MELTAC Platform V&V, Summary of MELTAC Platform CGD Activity. As indicated in the enclosed materials, these documents contain information that MELCO considers proprietary, and therefore should be withheld from public disclosure pursuant to 10 C.F.R 2.390 (a)(4) as trade secrets and commercial or financial information which is privileged or confidential.

The accompanying affidavit, Enclosure (1) sets forth the basis on which the information identified as proprietary should be withheld from public disclosure.

Sincerely,

Shigeru Sugitani  
Senior Manager, Control & Protection Systems Section  
Nuclear Power Department, Energy Systems Center  
Mitsubishi Electric Corporation

**Enclosures:**

No.	Document Number	Document Title	Date of Issue
1	-	Affidavit of Shigeru Sugitani	10/17/2016
2	JEXU-1041-2089-P	1 for JEXU-1041-1023, "Summary of MELTAC Platform Equipment Qualification"	10/15/2016
3	JEXU-1041-2089-NP		
4	JEXU-1041-2090-P	2 for JEXU-1041-1023, "Summary of MELTAC Platform Equipment Qualification",	10/15/2016
5	JEXU-1041-2090-NP		
6	JEXU-1041-2091-P	3 for JEXU-1041-1023, "Summary of MELTAC Platform Equipment Qualification"	10/15/2016
7	JEXU-1041-2091-NP		
8	JEXU-1041-2088-P	2 for JEXU-1041-1025, "Summary of MELTAC Platform QA"	10/15/2016
9	JEXU-1041-2088-NP		
10	JEXU-1041-1023-P	Summary of MELTAC Platform Equipment Qualification	10/15/2016
11	JEXU-1041-1023-NP		
12	JEXU-1041-1026-P	Summary of MELTAC Platform V&V	10/15/2016
13	JEXU-1041-1026-NP		
14	JEXU-1041-1124-P	Summary of MELTAC Platform CGD Activity	10/15/2016
15	JEXU-1041-1124-NP		

CC: Gilbert W. Remley  
Nuclear Systems Department Manager  
Mitsubishi Electric Power Products, Inc

---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

10/15/2016

**SAFETY SYSTEM DIGITAL PLATFORM  
- MELTAC (MITSUBISHI ELECTRIC TOTAL ADVANCED CONTROLLER) -  
TOPICAL REPORT**

**Mitsubishi Electric Corporation**

**TAC NO.:** MF4228  
**RAI NO.:** #1  
**DATE OF RAI ISSUE:** 6/29/2016

---

**QUESTION NO.:** 1 for JEXU-1041-1023, "Summary of MELTAC Platform Equipment Qualification," Rev.2

Results of the testing is identified only as "acceptance criteria was met," or "test results will be added to this section upon test completion." The results should identify any failures occurring during the test as well as the changes and/or modifications that were made to the modules or the testing to complete the test satisfactorily.

---

**ANSWER:**

The explanation of the test results, including any failures has been added to Sections 5.2.1, 5.2.2, 5.2.3, and 5.2.4 of "Summary of MELTAC Platform Equipment Qualification" (JEXU-1041-1023), Rev.3.

[

]

Section 5.0 of "Summary of MELTAC Platform V&V" Rev.3 (JEXU-1041-1026) has been revised and Appendix C has been added with consideration to the same point of view as "Summary of MELTAC Platform Equipment Qualification" (JEXU-1041-1023), Rev.3 to summarize V&V results including findings and corrective actions.

[

]

[

]



**Impact on Technical Report**  
“Summary of MELTAC Platform Equipment Qualification” (JEXU-1041-1023) and  
“Summary of MELTAC Platform V&V” (JEXU-1041-1026) have been revised.

---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

10/15/2016

**SAFETY SYSTEM DIGITAL PLATFORM  
- MELTAC (MITSUBISHI ELECTRIC TOTAL ADVANCED CONTROLLER) -  
TOPICAL REPORT**

**Mitsubishi Electric Corporation**

**TAC NO.:** MF4228  
**RAI NO.:** #1  
**DATE OF RAI ISSUE:** 6/29/2016

---

**QUESTION NO.:** 2 for JEXU-1041-1023, "Summary of MELTAC Platform Equipment Qualification," Rev.2

The NRC staff needs to know the specific modules, by part number and version, included in the Equipment-under-Test (EUT) setup. Descriptions such as "performed with a MELTAC cabinet fully loaded with most, but not all, MELTAC components" and "performed with a MELTAC cabinet fully equipped with a typical configuration of the MELTAC components required for the safety protection system" do not identify the necessary information on the modules, part numbers or revisions that were qualified.

---

**ANSWER:**

The explanation for identifying the specific modules which are included in the EUT for the scope of Phase 1 has been added to Section 5.1.1.3, 5.1.2.3, 5.1.3.3, and 5.1.4.3 of "Summary of MELTAC Platform Equipment Qualification" (JEXU-1041-1023), Rev.3.

[

]

Section 5.0 of "Summary of MELTAC Platform V&V" Rev.3 (JEXU-1041-1026) has been revised and Appendix C has been added with consideration of the same point of view as "Summary of MELTAC Platform Equipment Qualification" (JEXU-1041-1023), Rev.3 to summarize V&V results including findings and corrective actions.

[

]

**Impact on Technical Report**

"Summary of MELTAC Platform Equipment Qualification" (JEXU-1041-1023) and "Summary of MELTAC Platform V&V" (JEXU-1041-1026) have been revised.

---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

10/15/2016

**SAFETY SYSTEM DIGITAL PLATFORM  
- MELTAC (MITSUBISHI ELECTRIC TOTAL ADVANCED CONTROLLER) -  
TOPICAL REPORT**

**Mitsubishi Electric Corporation**

**TAC NO.:** MF4228  
**RAI NO.:** #1  
**DATE OF RAI ISSUE:** 6/29/2016

---

**QUESTION NO.:** 3 for JEXU-1041-1023, "Summary of MELTAC Platform Equipment Qualification," Rev.2

Many of the tests were performed per MIL-STD-461. This standard has two accompanying standards on the information that should be included in a test procedure and a test report (Document numbers: DI-EMCS-80201B and DI-EMCS-80200C, respectively). This could be used as guidance to identify different types of information that could be presented in a summary document.

---

**ANSWER:**

In view of the applicable guidance in DI-EMCS-80201B and DI-EMCS-80200C for the MELTAC Platform, the detailed explanation regarding the equipment qualification test for the scope of Phase 1 has been added to Section 5 of "Summary of MELTAC Platform Equipment Qualification" (JEXU-1041-1023), Rev.3.

[

]

**Impact on Technical Report**

"Summary of MELTAC Platform Equipment Qualification" (JEXU-1041-1023) has been revised.

---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

**10/15/2016**

**SAFETY SYSTEM DIGITAL PLATFORM  
- MELTAC (MITSUBISHI ELECTRIC TOTAL ADVANCED CONTROLLER) -  
TOPICAL REPORT**

**Mitsubishi Electric Corporation**

**TAC NO.: MF4228**  
**RAI NO.: #1**  
**DATE OF RAI ISSUE: 6/29/2016**

---

**QUESTION NO.:** 2 for JEXU-1041-1025, "Summary of MELTAC Platform QA"

Per ISG-06, Section D.2.2, the review of the NRC staff is predicated on an Appendix B compliant organization and therefore, the hardware should be dedicated in accordance with Appendix B compliant processes. This information would be in commercial grade dedication plans and reports. As identified by the NRC inspection report (ADAMS Accession No. ML12013A353), a pilot commercial grade dedication of two modules was performed since MELCO had not fully developed a complete MELTAC platform under its Appendix B program. Due to the critical nature of this one report demonstrating an Appendix B compliant process for recurring commercial grade dedication, the NRC staff requests that pilot dedication documentation JEXU-1030-1001, "S MDOJ-03/04 Commercial Grade Item Technical Evaluation," be submitted on the docket.

---

**ANSWER:**

[

]

**Impact on Technical Report**

There is no impact on the Technical Report. "Summary of MELTAC Platform CGD activity" (JEXU-1041-1124) will be provided.

## **PART 3-5**

### **Responses to RAI, including:**

Transmittal Letter, dated March 17, 2017

JEXU-1041-2067 R1 (Response to TR RAI 7)





Mar 17, 2017  
JEXU-1041-8539

Document Control Desk  
U.S. Nuclear Regulatory Commission  
11555 Rockville Pike  
Rockville, MD 20852-2738

Attention: Mr. Joseph Holonich

**SUBJECT: MELCO's responses to MELTAC Topical Report Revision 2 RAI #1 (TAC No.MF4228)  
(Regarding item No.7 for JEXU-1041-1008, Topical Report,)**

With this letter, Mitsubishi Electric Corporation (MELCO) submits the documents listed in the enclosures table below to the U.S. Nuclear Regulatory Commission (NRC).

Enclosed are the documents that make up the response to item No.7 for JEXU-1041-1008, Topical Report. As indicated in the enclosed materials, these documents contain information that MELCO considers proprietary, and therefore should be withheld from public disclosure pursuant to 10 C.F.R. 2.390 (a)(4) as trade secrets and commercial or financial information which is privileged or confidential.

The accompanying affidavit, Enclosure (1) sets forth the basis on which the information identified as proprietary should be withheld from public disclosure.

Sincerely,

Shigeru Sugitani  
Senior Manager, Control & Protection Systems Section  
Nuclear Power Department, Energy Systems Center  
Mitsubishi Electric Corporation

**Enclosures:**

No.	Document Number	Document Title	Date of Issue
1	JEXU-1041-2067-P(R1)	7 for JEXU-1041-1008, "Safety Digital Platform - MELTAC-"	03/15/2017
2	JEXU-1041-2067-NP(R1)		

CC: Gilbert W. Remley  
Nuclear Systems Department Manager  
Mitsubishi Electric Power Products, Inc

---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

**3/15/2017**

**SAFETY SYSTEM DIGITAL PLATFORM  
- MELTAC (MITSUBISHI ELECTRIC TOTAL ADVANCED CONTROLLER) -  
TOPICAL REPORT**

**Mitsubishi Electric Corporation**

**TAC NO.: MF4228**  
**RAI NO.: #1**  
**DATE OF RAI ISSUE: 6/29/2016**

---

**QUESTION NO.:** 7 for JEXU-1041-1008, "Safety System Digital Platform – MELTAC"

DI&C-ISG-04, Section 1 Interdivisional Communications, Point 6, states the safety function processor should not accept interrupts from outside its own safety division. Page 56, third paragraph, states; [

] Provide information  
on how the engineering tool is prevented from disrupting the controller safety functions.

---

**ANSWER:**

[

]

### **Impact on Topical Report**

The answer above will be added to Section 4.1.4.2 of the Topical Report. See Attachment -1.

#### 4.1.4.2 Network for the MELTAC Engineering Tool

In order to communicate between the MELTAC engineering tool and the controller, the Maintenance Network is used. The MELTAC engineering tool, which runs on a PC, is temporarily connected via the Maintenance Network to the System Management Modules of each controller in the division. This interface allows all functions described in Section 4.1.4.1. The Maintenance Network is temporarily connected to the controllers in the same safety division. There is a separate Maintenance Network for each division. There are no Maintenance Network interconnections between safety divisions. There is also a separate MELTAC engineering tool for each division. The specification of the Maintenance Network is described below.

For the configuration and the isolation of the Maintenance Network, see Section 4.3.4.

(Specification)

Function: Transmission of maintenance data for MELTAC engineering tools

- Transmission protocol: Ethernet (IEEE Std. 802.3; CSMA / CD, UDP/IP)
- Transmission speed: 100 Mbps/10 Mbps
- Communication form: Dialog communication
- Connection form: Bus/Star-type

Transmission media: UTP Category 5 cable  
Optical fiber (Multi mode)

[

ToR-7

1

## **PART 3-6**

### **Responses to RAI, including:**

Transmittal Letter, dated May 31, 2017

JEXU-1041-2073 R1 (Response to S/W Tools RAI 1)



May 31, 2017  
JEXU-1041-8547

Document Control Desk  
U.S. Nuclear Regulatory Commission  
11555 Rockville Pike  
Rockville, MD 20852-2738

Attention: Mr. Joseph Holonich

**SUBJECT: MELCO's responses to MELTAC Topical Report Revision 0 RAI #1 (TAC No.MF4228)  
(Regarding, items No.1 for JEXU-1041-1031, "MELTAC Platform Software Tools")  
and Submittal of MELTAC Topical Report Supporting Documentation**

With this letter, Mitsubishi Electric Corporation (MELCO) submits the documents listed in the enclosures table below to the U.S. Nuclear Regulatory Commission (NRC).

Enclosed are the documents that make up the response to items No.1 for JEXU-1041-1031, "MELTAC Platform Software Tools" and MELTAC Topical Report Supporting Documentation. As indicated in the enclosed materials, these documents contain information that MELCO considers proprietary, and therefore should be withheld from public disclosure pursuant to 10 C.F.R 2.390 (a)(4) as trade secrets and commercial or financial information which is privileged or confidential.

The accompanying affidavit, Enclosure (1) sets forth the basis on which the information identified as proprietary should be withheld from public disclosure.

Sincerely,

Manabu Taniguchi  
Senior Manager, Control & Protection Systems Section  
Nuclear Power Department, Energy Systems Center  
Mitsubishi Electric Corporation



**Enclosures:**

No.	Document Number	Document Title	Date of Issue
1	-	Affidavit of Manabu Taniguchi	05/31/2017
2	JEXU-1041-2073-P	1 for JEXU-1042-1031, "MELTAC Platform Software Tools", Rev.1	05/31/2017
3	JEXU-1041-2073-NP		
4	JEXU-1041-1023-P	Summary of MELTAC Platform Equipment Qualification, Rev.4	05/31/2017
5	JEXU-1041-1023-NP		
6	JEXU-1041-1026-P	Summary of MELTAC Platform V&V, Rev.4	05/31/2017
9	JEXU-1041-1026-NP		

CC: Gilbert W. Remley  
Nuclear Systems Department Manager  
Mitsubishi Electric Power Products, Inc

---

---

**RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION**

---

---

5/31/2017

**SAFETY SYSTEM DIGITAL PLATFORM  
- MELTAC (MITSUBISHI ELECTRIC TOTAL ADVANCED CONTROLLER) -  
TOPICAL REPORT**

**Mitsubishi Electric Corporation**

**TAC NO.: MF4228**  
**RAI NO.: #1**  
**DATE OF RAI ISSUE: 6/29/2016**

---

**QUESTION NO.: 1 for JEXU-10412-1031, "MELTAC Platform Software Tools"**

P. 4, List of Software Tools Category Used in Each Phase:

- a. In order for the NRC staff to evaluate software tools for compliance with IEEE 7-4.3.2 Section 5.3.2, we will need to understand what the tools are used for as well as what functions they perform in relation to the MELCO safety software development processes. The software tools listed in Table 1 are not consistent with names of the software tools provided in Section 5.0, Detailed Description of Processes. Please clarify the specific function of the tools and identify what document describes the function of each tool. The response should include a description of what the rules are for using the tool correctly and what configurations or options are recommended or advised against.
  - i. By further example of what the NRC staff needs to understand is the functions of the Engineering Tool. Section 4.1.4.1, Function Description of the TR, states the functional block diagrams are converted to graphical block diagrams by the MELTAC engineering tool. Section 5.7, MELTAC Engineering Tool, does not describe this function. Please explain.
- b. Please provide an assessment of how each tool conforms to the software tools criteria of IEEE 7-4.3.2 Section 5.3.2 for the tools listed below:
  - i. [                      ]
  - ii. [                      ]
- c. Identify the lifecycle phases that the MIC will be used in as was done with the other software tools on Table 1.

- d. Clause 5.3.2 of IEEE Std 7-4.3.2 specifies that software tools used to support software development are controlled under a configuration management plan. To evaluate compliance with this requirement, the NRC needs to review plans and procedures for establishment and maintenance of tool configuration control. Please provide documentation to show how tool configurations are controlled and Identify procedures used to maintain tool configuration control.

---

**ANSWER:**

[

]

#### **Impact on Topical Report**

There is no impact on the Topical Report.

#### **Impact on Technical Report**

Regarding a), Section 1.0, Table 1 in Section 4.0 and Section 5.0 of JEXU-104~~4~~2-1031, "MELTAC Platform Software Tools" will be revised. Appendix B will be added to JEXU-104~~4~~2-1031, "MELTAC Platform Software Tools" (see Attachment 1).

Regarding b), Section 5.10.2 of JEXU-104~~4~~2-1031, "MELTAC Platform Software Tools" will be revised (see Attachment-2).

Regarding c), Table 1 and Table 2 in Section 4.0 of JEXU-104~~4~~2-1031, "MELTAC Platform Software Tools" will be revised (see Attachment-3).

Regarding d), There is no impact on the Technical Report.

## 1.0 INTRODUCTION

This document describes the software tools, how their quality has been determined, how they are used and maintained, and verification and the validation (V&V) activities associated with the outputs generated by those software tools for the Mitsubishi Electric Total Advanced Controller (MELTAC) platform (i.e., Method (b) in Clause 5.3.2 of IEEE Std. 7-4.3.2-2003). This document encompasses the software tools used to develop the MELTAC platform basic software, which includes firmware and field programmable gate arrays (FPGAs) on all MELTAC platform modules.

This document supports “Safety System Digital Platform - MELTAC - Topical Report” (JEXU-1041-1008), which references “MELTAC Platform Software Program Manual” (JEXU-1041-1016) and satisfies the commitments made under Table 1 Section 2.17 “Software Tool Analysis Report” of “Mapping of MELTAC Platform Licensing Documents to the DI&C-ISG-06 Guidance” (JEXU-1041-1012).

BTP 7-14, B.3.1.11.2 requires an evaluation process for software tools, if tools are purchased as commercial items. Appendix A describes the evaluation procedure for purchased software tools used to develop MELTAC platform basic software.

Tools-2

“Safety System Digital Platform - MELTAC - Topical Report” (JEXU-1041-1008) also describes the MELTAC engineering tool functions associated with application software development. Appendix B of this document further describes these functions: how their quality has been determined, how they are expected to be used and maintained, and the verification and validation (V&V) activities associated with the outputs generated by the MELTAC engineering tool (i.e., Method (b) in Clause 5.3.2 of IEEE Std. 7-4.3.2-2003).

Tools-1a

## 2.0 REFERENCES

Document Name	Document Number	Revision
Safety System Digital Platform - MELTAC - Topical Report	JEXU-1041-1008	Current
Mapping of MELTAC Platform Licensing Documents to the Digital I&C-ISG-06 Guidance”	JEXU-1041-1012	Current
Digital I&C-ISG-06 “Digital Instrumentation & Control Licensing Process”	ML110140103	1
MELTAC Platform Software Program Manual	JEXU-1041-1016	Current
Guidance on Software Reviews for Digital Computer-Based I&C Systems	NUREG 0800 BTP 7-14	2007
Criteria for use of Computer in Safety Systems for Nuclear Power Plants	RG 1.152	3
Criteria for Digital Computers in Safety Systems for Nuclear Power Generating Stations	IEEE Std. 7-4.3.2-2003	2003

4.0 OBJECTIVE AND METHODOLOGY

[ The software life cycle is described in Section 3 of “MELTAC Platform Software Program Manual” (JEXU-1041-1016). ]

[

]

Table 1 - List of Software Tools Category Used in Each Phase


Tools-1a

Tools-1c

5.0 DETAILED DESCRIPTION OF PROCESSES

[

]

(


[

Tools-1a

Tools-1a  
(See the revised RAI response No. JEXU-1041-2073 R1.)

[

]


[

Tools-1a

Tools-1a  
(See the revised RAI response No. JEXU-1041-2073 R1.)

]

Tools-1a  
(See the revised RAI response No. JEXU-1041-2073 R1.)



[

]


[

Tools-1a

Tools-1a  
(See the revised RAI response No. JEXU-1041-2073 R1.)

[

]


[

Tools-1a

Tools-1a  
(See the revised RAI response No. JEXU-1041-2073 R1.)

[

]


[

Tools-1a

Tools-1a  
(See the  
revised RAI  
response No.  
JEXU-1041-  
2073 R1.)

]

[

]


[

Tools-1a

Tools-1a  
(See the revised RAI response No. JEXU-1041-2073 R1.)

]

Tools-1a

[

]


Tools-1a

[

Tools-1a

]

Tools-1a

[

]


Tools-1a

[

Tools-1a

Tools-1a  
(See the revised RAI response No. JEXU-1041-2073 R1.)

]

[

]


[

Tools-1a

Tools-1a

(See the revised RAI response No. JEXU-1041-2073 R1.)

Tools-1a  
(See the revised RAI response No. JEXU-1041-2073 R1.)



[

]


[

Tools-1a

Tools-1a

(See the revised RAI response No. JEXU-1041-2073 R1.)

Tools-1a

(See the revised RAI response No. JEXU-1041-2073 R1 )

Tools-5

Tools-5

## **APPENDIX B MELTAC ENGINEERING TOOL FUNCTIONS FOR APPLICATION SOFTWARE DEVELOPMENT**

The functional description of MELTAC engineering tool is described in Section 4.1.4 of “Safety System Digital Platform - MELTAC - Topical Report” (JEXU-1041-1008).

The table below lists the MELTAC engineering tool functions used to develop application software, which are expected to be used during implementation, test, and installation of application software.

For the functions of the MELTAC engineering tool other than the Memory Integrity Check (MIC) used to develop application software, MELCO has chosen to utilize METHOD b as described in Section 3.0 to ensure the quality of the MELTAC engineering tool and to V&V the outputs to ensure that the outputs generated by it are correct.

The table below ~~This appendix also~~ describes how the functions are used, including verification and validation (V&V) activities associated with the outputs generated by the MELTAC engineering tool.

The description of the conversion function from the functional block diagram (FBD) to graphic block diagram (GBD) described in Section 4.1.4 is not applied in the table below, since it is application specific item.

Table B.1 MELTAC engineering tool functions used to develop application software


Tools-1a

Tools-1a  
(See the revised RAI response No. JEXU-1041-

Tools-1a  
(See the revised RAI response No. JEXU-1041-2073 R1.)

MELTAC Platform Software Tools

JEXU-1042-1031-NP (R01)


[

]

Tools-1a

Tools-1a  
(See the revised RAI response No. JEXU-1041-2073 R1.)

Tools-1a  
(See the revised RAI response No. JEXU-1041-2073 R1.)

[

]


[

Tools-1a

Tools-1a

(See the revised RAI response No. JEXU-1041-2073 R1.)

Tools-1a

(See the revised RAI response No. JEXU-1041-2073 R1 )

Tools-5

Tools-5

Tools-1b

]

[

Tools-1b

]

4.0 OBJECTIVE AND METHODOLOGY

[ The software life cycle is described in Section 3 of “MELTAC Platform Software Program Manual” (JEXU-1041-1016). ]

[

]

Table 1 - List of Software Tools Category Used in Each Phase


Tools-1a

Tools-1c


Tools-1c  
(See the  
revised RAI  
response No.  
JEXU-1041-  
2073 R1.)

## **PART 3-7**

### **Response to RAI, including:**

Transmittal Letter, dated August 31, 2017





August 31, 2017  
JEXU-1041-8550

Document Control Desk  
U.S. Nuclear Regulatory Commission  
11555 Rockville Pike  
Rockville, MD 20852-2738

Attention: Mr. Joseph Holonich

**SUBJECT: MELCO's responses to MELTAC Topical Report Revision 0 RAI #1 (TAC No.MF4228)  
(Regarding, items No.1 for JEXU-1041-1023, "MELTAC Platform Equipment  
Qualification") and Submittal of MELTAC Topical Report Supporting  
Documentation**

With this letter, Mitsubishi Electric Corporation (MELCO) submits the documents listed in the enclosures table below to the U.S. Nuclear Regulatory Commission (NRC).

Enclosed are the documents that make up the response to items No.1 for JEXU-1041-1023, "MELTAC Platform Equipment Qualification" and MELTAC Topical Report Supporting Documentation. As indicated in the enclosed materials, these documents contain information that MELCO considers proprietary, and therefore should be withheld from public disclosure pursuant to 10 C.F.R 2.390 (a)(4) as trade secrets and commercial or financial information which is privileged or confidential.

The accompanying affidavit, Enclosure (1) sets forth the basis on which the information identified as proprietary should be withheld from public disclosure.

Sincerely, 

Manabu Taniguchi  
Senior Manager, Control & Protection Systems Section  
Nuclear Power Department, Energy Systems Center  
Mitsubishi Electric Corporation

**Enclosures:**

No.	Document Number	Document Title	Date of Issue
1	-	Affidavit of Manabu Taniguchi	08/31/2017
2	JEXU-1041-1023-P	Summary of MELTAC Platform Equipment Qualification, Rev.5	08/31/2017
3	JEXU-1041-1023-NP		

CC: Gilbert W. Remley  
Nuclear Systems Department Manager  
Mitsubishi Electric Power Products, Inc

## **PART 4**

**Safety System Digital Platform - MELTAC - Topical Report,**

**JEXU-1041-1008, Revision 1**

# **Safety System Digital Platform - MELTAC - Topical Report**

**Non-Proprietary**

**April 2016**

**© 2016 MITSUBISHI ELECTRIC CORPORATION  
All Rights Reserved**

Prepared: Susumu Okuda Apr. 25, 2016 Kazuhiro Eguchi Apr. 25, 2016  
Susumu Okuda, Engineer Date Kazuhiro Eguchi, Manager  
Control & Protection Systems Section Radiation Monitoring Instrumentation  
Section

Reviewed: Manabu Taniguchi Apr. 25, 2016 Shingo Nakamura Apr. 25, 2016  
Manabu Taniguchi, Manager Date Shingo Nakamura, Manager  
Control & Protection Systems Section Radiation Monitoring Instrumentation  
Section

Approved: Shigeru Sugitani Apr. 25, 2016 Yasuo Uranaka Apr. 25, 2016  
Shigeru Sugitani, Senior Manager Date Yasuo Uranaka, Senior Manager  
Control & Protection Systems Section Radiation Monitoring Instrumentation  
Section

Approved: H. Funakoshi Apr. 25, 2016  
Hisashi Funakoshi, General Manager Date  
Nuclear Power Department

Approved: Hideki Matsui Apr. 26, 2016  
Hideki Matsui, QA Manager Date  
Energy Systems Center

**Signature History**

	Rev.0, April 2014			
Prepared	Hitomi Sasaki			
	Masaki Taguchi			
Reviewed	Manabu Taniguchi			
	Shingo Nakamura			
Approved	Hidetoshi Matsushita			
	Yasuo Uranaka			
	Katsumi Akagi			
	Hirotohi Ohkawa			

## Revision History

Revision	Date	Page (section)	Description
0	April 2014	All	Initial issue
1	April 2016	9 (3)	Corrected item No.24 description. (Remove reference to Appendix C)
		13 (3)	Modified the reference version of IEEE Std. 1028. (1997 -> 2008)
		31,32 (4.1.1.4)	Added "EMC" and "EMS" to Table 4.1.1-2
		34 (4.1.2.1)	Deleted the description of Slide-split CPU Chassis.
		38,39,182, 183 (4.1.2.3, 5.5)	Deleted the description of Binary Isolation Module (KIDJ) including Figure 4.1-2-3, 5.5-3, 5.5-4.
		223 (A.5)	Modified the specification for the MRTJ Module in Table A.5. From "32 to 392°F (0 to 200°C) to 32 to 752 °F (0 to 400 °C)"
		226 (A.5)	Deleted the contact input (external contact power supply) type MDIJ from Table A.7. Deleted the DC24 V type MDIJ Module from Table A.7.

Revision	Date	Page (section)	Description
		227 (A.5)	Deleted the closed contact type MDOJ Module from Table A.8.
		228 (A.6)	Deleted the KIDJ Module from Table A.10.
		229 (A.6)	Deleted the KEXJ Module from Table A.11.
		231 (A.8)	Deleted the DPLJ Module from Table A.13.
		232 (A.9)	Deleted the description of Slide-split CPU Chassis from the PPSJ Module specification of Table A.14.
		239 (A.16)	Deleted the Slide-split Chassis from Table A.21.
		240 (A.17)	Deleted the following from Table A.24. <ul style="list-style-type: none"> <li>• Digital (DI/DO)(Lift/Jumper function)</li> <li>• Digital (With specific cable for power supply)(Lift function)</li> </ul>



© 2016  
**MITSUBISHI ELECTRIC CORPORATION**  
All Rights Reserved

This document has been prepared by Mitsubishi Electric Corporation (MELCO) in connection with MELCO's request to the U.S. Nuclear Regulatory Commission (NRC) for a review of the Mitsubishi Electric Total Advanced Controller (MELTAC) platform. No right to disclose, use or copy any of the information in this document, other than by the NRC and its contractors is authorized without the express written permission of MELCO.

This document contains technology information, trade secrets and intellectual property relating to the MELTAC platform, and it is delivered to the NRC on the express condition that it not be disclosed, copied or reproduced in whole or in part, or used for the benefit of anyone other than MELCO without the express written permission of MELCO, except as set forth in the previous paragraph.

This document is protected by the laws of Japan, U.S. copyright law, international treaties and conventions, and the applicable laws of any country where it is being used.

Mitsubishi Electric Corporation  
7-3, Marunouchi 2-chome, Chiyoda-ku  
Tokyo 100-8310 Japan

---

## Abstract

This Topical 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 can be used for safety and non-safety Instrumentation and Control (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 operating experience in various non-safety system applications such as the reactor and turbine control systems in PWR nuclear power plants operating in Japan. Based on its excellent performance in numerous non-safety applications, the MELTAC platform has now been applied to almost all non-safety and safety systems throughout Japanese PWR nuclear power plants. The MELTAC platform has also been applied for plant-wide digital upgrades in several Japanese PWR nuclear power plants that have been completed and those currently in progress.

The goal of this report is to seek a favorable Safety Evaluation from the U.S. Nuclear Regulatory Commission (NRC) for the use of the MELTAC platform for nuclear safety systems in operating plants and new plants.

For applications in the US, this report demonstrates conformance of the MELTAC platform 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 detailed description of the hardware and software of the MELTAC platform, including digital processing, human systems interfaces (HSI) and digital communication interfaces and the detailed description of the MELTAC application development tools
- The equipment qualification of the MELTAC platform and its conformance to the corresponding U.S. standards
- The life cycle and the Quality Assurance Program (QAP) of the MELTAC platform and conformance to U.S. regulatory criteria
- The equipment reliability of the MELTAC platform and how that reliability is used to determine the reliability of any MELTAC safety application

MELTAC was developed under a Japanese QAP, and has undergone a one-time commercial grade dedication (CGD) by MELCO for use in US safety related applications. The details of that CGD program are provided in this report by reference. MELTAC is now maintained and manufactured under MELCO's 10 CFR 50 Appendix B QAP.

Prior to implementing the MELTAC commercial grade dedication program, MELCO developed and adopted a nuclear QAP in compliance with 10 CFR 50 Appendix B and 10 CFR 21. MELCO has undergone an inspection by NRC to verify the implementation of an adequate QAP in compliance with the requirements of 10 CFR 50 Appendix B and 10 CFR 21 in support of digital I&C development activities. The results of this NRC inspection are documented in NRC Inspection Report NO. 99901410/2011-202 (ADAMS Accession number ML12013A353). In NRC Inspection Report NO. 99901410/2011-202, the NRC inspection team concluded that MELCO is effective in implementing its QA and 10 CFR Part 21 programs in support of the MELTAC platform development. The Inspection Report stated that the NRC inspectors determined that MELCO's commercial grade dedication process adequately identified and verified the critical characteristics of the MELTAC platform that provide assurance that the platform will perform its safety function satisfactorily. The Inspection Report also stated that the NRC inspectors determined that the process implemented by MELCO is consistent with regulatory requirements associated with software development. The nonconformance identified in the Inspection Report has been corrected.

MELCO also underwent a successful audit by the NRC Office of New Reactors (NRO). This NRO audit focused on reviewing the design details related to the MELTAC platform to assist in making the determination that the specifications for the digital platform to be used for the implementation of the safety I&C systems, which reflect the MELTAC platform, meet the regulatory requirements. The results of the NRO audit are documented in the "Digital Instrumentation and Controls Design Audit Report" (ADAMS Accession number ML12291A673).

The information in this Topical Report 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 future licensing submittals. 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 Topical Report.

## **Table of Contents**

List of Tables .....	0-11
List of Figures .....	0-13
List of Acronyms .....	0-15
1.0 PURPOSE .....	1
2.0 SCOPE .....	1
3.0 APPLICABLE CODE, STANDARDS AND REGULATORY GUIDANCE .....	2
4.0 MELTAC PLATFORM DESCRIPTION .....	15
4.1 Controller .....	18
4.1.1 Hardware Configuration .....	18
4.1.2 Hardware Descriptions .....	33
4.1.3 Software .....	47
4.1.4 MELTAC Engineering Tool .....	53
4.1.5 Self-Diagnosis .....	56
4.1.6 Bus Inside the Controller .....	72
4.1.7 Manual Test .....	72
4.1.8 Defense-in-Depth and Diversity (DAS) Interface .....	78
4.2 Safety VDU Panel and Processor .....	79
4.2.1 Hardware .....	79
4.2.2 Software .....	84
4.2.3 Self-Diagnosis .....	91
4.2.4 Manual Test .....	92
4.3 Communication System .....	93
4.3.1 General Description .....	93
4.3.2 Control Network .....	93
4.3.3 Data Link .....	123
4.3.4 Maintenance Network .....	141
4.4 Response Time .....	150
4.4.1 Processing Time of MELTAC Fundamental Cycle .....	150
4.4.2 Processing Time of MELTAC Application .....	151
4.4.3 Examples of Response Time Calculations .....	155
4.5 Control of Access .....	157
4.5.1 Control of Access for Hardware .....	157
4.5.2 Control of Access for Software .....	157
4.5.3 Control of Access for Temporary Changes to Process Values .....	157
5.0 ENVIRONMENTAL, SEISMIC, ELECTROMAGNETIC AND ISOLATION QUALIFICATION .....	159
5.1 Environmental Qualification Testing .....	161
5.1.1 Environmental Specification and Outline of Test .....	161
5.1.2 Contents of Environmental Test .....	162
5.2 Seismic Qualification Testing .....	166
5.2.1 Overview .....	166
5.2.2 Seismic Resistance Test .....	166
5.3 Electromagnetic Compatibility and Radio Frequency Interference Qualification Testing .....	172
5.3.1 Test Configuration .....	173
5.3.2 Description of Tests .....	174
5.4 Electrostatic Discharge Qualification Testing .....	180

---

5.5 Isolation Qualification Testing .....	182
6.0 QUALITY ASSURANCE AND LIFE CYCLE .....	184
6.1 MELTAC Platform Life Cycle Plans and Activities .....	184
6.1.1 Overview of the MELTAC Quality Assurance Program .....	184
6.1.2 Secure Development Environment Management .....	193
6.1.3 Operations .....	198
6.1.4 Training .....	199
6.1.5 Maintenance .....	201
6.1.6 Obsolescence Management .....	203
6.1.7 Identification .....	204
6.1.8 Reliability Database .....	205
6.2 MELTAC Re-evaluation Program (MRP) .....	206
6.3 MELTAC Engineering Tool Life Cycle .....	206
7.0 EQUIPMENT RELIABILITY .....	207
7.1 Mean Time between Failures (MTBF) Analysis .....	208
7.2 Controller Reliability Analysis .....	211
7.2.1 Reliability Model .....	212
7.2.2 FTA of Spurious Actuation of the Safety Function .....	213
7.2.3 FTA of Failure to Actuate the Safety Function .....	214
7.2.4 Detailed Controller Reliability Analysis .....	215
7.3 Failure Mode and Effect Analysis (FMEA) .....	218
7.4 Equipment (Parts) that Require Periodic Replacement to Maintain Reliability .....	219
APPENDIX A HARDWARE SPECIFICATION .....	221
A.1 CPU Module Specification .....	221
A.2 System Management Module Specification .....	221
A.3 Bus Master Module Specification .....	222
A.4 Control Network I/F Module Specification .....	222
A.5 I/O Module Specification .....	223
A.6 Isolation Module and Distribution Module Specification .....	228
A.7 E/O Converter Module Specification .....	230
A.8 Power Interface Module Specification .....	231
A.9 Power Supply Module Specification .....	232
A.10 Safety VDU Panel Specification .....	233
A.11 FMU Module Specification .....	233
A.12 NI Module Specification.....	234
A.13 RM Module Specification.....	238
A.14 Status Display and Switch Module Specification .....	238
A.15 Repeater Module Specification .....	238
A.16 Module Chassis Specification .....	239
A.17 Other Modules Specification .....	240
APPENDIX B FUNCTIONAL SYMBOL SOFTWARE SPECIFICATIONS .....	241
APPENDIX C DEFINITION .....	250
APPENDIX D REGULATORY REQUIREMENTS AND GUIDANCE APPLICABILITY MATRIX .....	255

---

## **List of Tables**

Table 4.1.1-1 Scale and Capacity .....	30
Table 4.1.1-2 Environmental Specifications .....	31
Table 4.1.2-1 Module in the CPU Chassis .....	33
Table 4.1.2-2 CPU Chassis.....	34
Table 4.1.2-3 MELTAC Cabinet Specifications .....	44
Table 4.1.5-1 WDT Timeout Process.....	69
Table 4.1.6-1 Bus Inside the Controller .....	72
Table 4.1.6-2 I/O Bus Specification .....	72
Table 4.2-1 Screen Descriptions .....	87
Table 4.2-2 Data Details .....	89
Table 4.3-1 Configuration of Control Network .....	94
Table 4.3-2 Control Network Specification .....	100
Table 4.3-3 Self-Diagnosis Functions of Control Network .....	106
Table 4.3-4 Data Link Communication Specification .....	125
Table 4.3-5 The Maintenance Network Communication Specification .....	148
Table 4.4-1 Description of Processing in Each Component (Maximum/Minimum Values).....	153
Table 5.0-1 Regulatory Requirements and Reference to Acceptance Criteria for Each Qualification Test .....	160
Table 5.0-2 Test Reports .....	161
Table 6.1-1 MELTAC Life Cycle Plan/Activity Summary .....	185
Table 6.1-2 Security Measures of the Software Development/Storage Environment ....	195
Table 6.1-3 Security Measures in the Software Development Process .....	196
Table 6.1-4 Information Provided in the MELTAC Maintenance Manuals .....	199
Table 6.1-5 Hardware Maintenance .....	201
Table 6.1-6 Software Maintenance .....	202
Table 7.1-1 Failure Rate of Modules .....	209
Table 7.4-1 List of Parts that Require Periodic Replacement .....	220
Table A.1 CPU Module Specification .....	221
Table A.2 System Management Module Specification.....	221
Table A.3 Bus Master Module Specification .....	222
Table A.4 Control Network I/F Module Specification .....	222
Table A.5 Analog Input Module Specification .....	223
Table A.6 Analog Output Module Specification .....	225
Table A.7 Digital Input Module Specification .....	226
Table A.8 Digital Output Module Specification .....	227
Table A.9 Pulse Input Module Specification .....	227
Table A.10 Isolation Module Specification .....	228
Table A.11 Distribution Module Specification .....	229
Table A.12 E/O Converter Module and Device Specification .....	230
Table A.13 Power Interface Module Specification .....	231
Table A.14 Power Supply Module Specification .....	232
Table A.15 Safety VDU Panel Specification .....	233
Table A.16 FMU Module Specification .....	233
Table A.17 NI Module Specification .....	234
Table A.18 RM Module Specification .....	238
Table A.19 Status Display and Switch Module Specification .....	238

---

Table A.20 Repeater Module Specification .....	238
Table A.21 CPU Module Chassis Specification .....	239
Table A.22 I/O Module Chassis Specification .....	239
Table A.23 Fan Modules Specification.....	240
Table A.24 Terminal Unit Specification .....	240
Table A.25 Optical Switch Specification .....	240
Table B.1 List of Function Symbols for Discrete Control Processes .....	241
Table B.2 List of Function Symbols for Analog Control Processes .....	244
Table B.3 List of Function Symbols for Input and Output Process .....	247
Table B.4 List of Function Symbols for Obtaining and Setting Status Values .....	249

## **List of Figures**

Figure 4.0-1 MELTAC Platform Typical PSS Configuration .....	16
Figure 4.1.1-1 Single Controller Configuration .....	19
Figure 4.1.1-2 Redundant Parallel Controller Configuration .....	21
Figure 4.1.1-3 Redundant Standby Controller Configuration .....	23
Figure 4.1.1-4 Picture of Modules in a CPU Chassis for a Redundant Standby Controller Configuration .....	24
Figure 4.1.1-5 Mode Management of Single Controller and Redundant Parallel .....	26
Figure 4.1.1-6 Mode Management of Redundant Standby Controller.....	28
Figure 4.1.2-1 Location of Isolation Modules .....	38
Figure 4.1.2-2 The Internal Configuration Diagram of the Analog Isolation Modules .....	39
Figure 4.1.2-3 The Internal Configuration Diagram of the Pulse Input Isolation Module ..	39
Figure 4.1.2-4 Sample Internal Configuration Diagram of the PIF Module .....	41
Figure 4.1.2-5 Cabinet External Dimensions and Rack Up, Typical Sample A.....	45
Figure 4.1.2-6 Cabinet External Dimensions and Rack Up, Typical Sample B .....	46
Figure 4.1.2-7 Configuration of Power Supply for Controller Cabinet .....	47
Figure 4.1.3-1 Basic Software Processes and Execution Order .....	48
Figure 4.1.3-2 Remaining Time Diagnosis .....	51
Figure 4.1.5-1 Coverage of Self-Diagnosis Function of the Controller .....	58
Figure 4.1.5-2 WDT Mechanism (CPU Module) .....	66
Figure 4.1.5-3 WDTs Mounted in MELTAC Platform .....	68
Figure 4.1.7-1 Manual Test for Process Input and Output .....	74
Figure 4.2-1 Configuration of Safety VDU Processor .....	81
Figure 4.2-2 Configuration of Power Supply for Safety VDU .....	83
Figure 4.2-3 Software Structure of Safety VDU Processor .....	84
Figure 4.2-4 Screen Transition of the Safety VDU Processor .....	86
Figure 4.2-5 A Sample of Operation Switch Pictogram on the Safety VDU Panel.....	88
Figure 4.2-6 Explanation of the Safety VDU Processor Operation .....	90
Figure 4.3-1 Configuration of Control Network .....	95
Figure 4.3-2 Explanation of Optical Switch Bypass Operation .....	97
Figure 4.3-3 Explanation of Optical Switch Failure .....	98
Figure 4.3-4 Protocol Stack of Control Network .....	100
Figure 4.3-5 Separation in Communication of Control Network .....	105
Figure 4.3-6 Operation Signal Flow from S-VDU .....	108
Figure 4.3-7 Process Signal Flow from Controller to Safety Bus .....	109
Figure 4.3-8 Detail Signal Flow in Controller (Receiving Process) .....	110
Figure 4.3-9 Detail Signal Flow in Controller (Sending Process of the Process Signal)	111
Figure 4.3-10 Processing by the Control Network I/F Module in the Receiving Process	113
Figure 4.3-11 Processing by the CPU Module in the Control Network Receiving Process.....	115
Figure 4.3-12 Processing by the CPU Module in the Control Network Sending Process	118
Figure 4.3-13 Processing by the Control Network I/F Module in the Sending Process ..	120
Figure 4.3-14 Example of Connection Configuration of Data Link Configuration .....	123
Figure 4.3-15 Separation in Communication of Data Link .....	128
Figure 4.3-16 Partial Trip Signal Flow between RPPs .....	130
Figure 4.3-17 Detail Signal Flow in RPP (Receiving Process) .....	131
Figure 4.3-18 Detail Signal Flow in RPP (Sending Process of the Trip Signal) .....	132
Figure 4.3-19 Processing by the Bus Master Module .....	133



---

Figure 4.3-20 Processing by the CPU Module in the Data Link Receiving Process .....	134
Figure 4.3-21 Processing by the CPU Module in the Data Link Sending Process .....	136
Figure 4.3-22 Processing by the Bus Master Module in the Data Link Sending Process .....	138
Figure 4.3-23 Maintenance Network Configuration .....	141
Figure 4.3-24 Separation in Communication of the Maintenance Network .....	144
Figure 4.3-25 Dedicated Re-programming Chassis for Writing to the F-ROM .....	145
Figure 4.4-1 The Time Chart of Fundamental Process in Cyclic .....	150
Figure 4.4-2 Internal Process Divisions of the MELTAC Platform to Perform Response Time Calculations .....	152
Figure 5.5-1 Isolation Test Configuration of KILJ for Transverse Mode Faults .....	183
Figure 5.5-2 Isolation Test Configuration of KILJ for Common Mode Faults .....	183
Figure 6.1-1 Security Measures of the Software Development/Storage Environment ...	194
Figure 7.2-1 Reliability Model .....	212
Figure 7.2-2 Fault Tree for Output Failure Spurious Actuation .....	213
Figure 7.2-3 Fault Tree for Failure to Actuate .....	214
Figure 7.2-4 Reliability Model of Subsystem .....	215
Figure 7.2-5 Fault Tree of Subsystem .....	215
Figure 7.2-6 Reliability Model of Dedicated I/O .....	216
Figure 7.2-7 Fault Tree of Dedicated I/O .....	216
Figure 7.2-8 Input/Output Line .....	217
Figure 7.2-9 Fault Tree of Input/Output Line .....	217

## **List of Acronyms**

AI	Analog Input
ANSI	American National Standards Institute
AO	Analog Output
ASME	American Society of Mechanical Engineers
BTP	Branch Technical Position
CCF	Common Cause Failure
CCP	Component Control Processor
CEAS	Corporate Electronic Archive System
CFR	Code of Federal Regulations
COTS	Commercial Off-The-Shelf
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
DAS	Diverse Actuation System
DI	Digital Input
DO	Digital Output
DSP	Digital Signal Processor
ECC	Error Correcting Code
EEPROM	Electrically Erasable Programmable Read Only Memory
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EMS	Electromagnetic Susceptibility
ESD	Electrostatic Discharge
ESF	Engineered Safety Features
EUT	Equipment under Test
E/O	Electrical/Optical
FBD	Functional Block Diagram
FIT	Failure Rate
FMEA	Failure Mode and Effect Analysis
FMU	Frame Memory Unit
FPGA	Field Programmable Gate Array
F-ROM	Flash Read Only Memory
F/W	Firmware
GBD	Graphical Block Diagram
GDC	General Design Criteria
GUI	Graphical User Interface
HFE	Human Factor Engineering
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	Inspections, Tests, Analyses, and Acceptance Criteria
I/O	Input/Output
I&C	Instrumentation and Control

---

JEC	Japanese Electrotechnical Committee
JIS	Japanese Industrial Standards
JEIDA	Japan Electronic Industry Development Association
LCO	Limiting Conditions for Operation
LED	Light Emitting Diode
MCB	Main Control Board
MCR	Main Control Room
MELCO	Mitsubishi Electric Corporation
MELTAC	Mitsubishi Electric Total Advanced Controller
MEPPI	Mitsubishi Electric Power Products Inc.
MIC	Memory Integrity Check
MRP	MELTAC Re-evaluation Program
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair
NC	Normally Closed
NI	Nuclear Instrumentation
NO	Normally Open
NRC	Nuclear Regulatory Commission
OBE	Operating Basis Earthquake
PIF	Power Interface
POL	Problem Oriented Language
QA	Quality Assurance
QAP	Quality Assurance Program
PCS	Plant Control System
PSS	Plant Safety System
RAM	Random Access Memory
RCP	Reactor Coolant Pump
RFI	Radio Frequency Interference
RG	Regulatory Guide
RGB	Red/Green/Blue
RM	Radiation Monitoring
ROM	Read-Only Memory
RPR	Resilient Packet Ring
RPP	Reactor Protection Processor
RTD	Resistance Temperature Detector
SCMP	Software Configuration Management Plan
SDOE	Secure Development and Operational Environment
SDP	Software Development Plan
SIntP	Software Integration Plan
SInstP	Software Installation Plan
SMC	Self-diagnosis Memory Check
SMP	Software Management Plan
SPM	Software Program Manual
SQAP	Software Quality Assurance Plan
SSE	Safe Shutdown Earthquake
SSP	Software Safety Plan
STP	Software Test Plan
S-VDU	Safety VDU
SVVP	Software Verification and Validation
VDU	Visual Display Unit
V&V	Verification and Validation

---

---

UDP/IP	User Datagram Protocol Internet Protocol
UTP	Unshielded Twist Pair Cable
WDT	Watchdog Timer

## 1.0 PURPOSE

The purpose of this Topical Report is to describe 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 can be used for safety and non-safety I&C systems. The modular structure of the platform allows it to be applied to solve most utility needs for safety applications, including new systems, component replacements and complete system replacements.

The MELTAC platform can be applied to nuclear safety systems such as the reactor protection system, engineered safety features actuation system, safety-related HSI system, and any other safety system. In addition, the MELTAC platform can be applied to non-safety systems. The MELTAC equipment applied for non-safety applications is the same design as the equipment for safety applications. However, there are software and hardware components that are unique to non-safety applications. These components have differences in Quality Assurance methods for software design and other software life cycle processes.

Therefore, MELTAC components that are applicable to either safety or non-safety applications are identified as "MELTAC Nplus S"; components that are only applicable to non-safety applications are identified as "MELTAC Nplus". These identifier distinctions apply to all aspects of MELTAC, including hardware, software, documentation and engineering tools.

The following terminology is used in this section and throughout this document:

Application Licensing Documentation – This refers to application specific documentation for 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 Topical Report. "Equipment" includes the MELCO safety-related digital I&C platform. "Equipment" does not include the MELCO non-safety digital I&C or HSI platforms, unless specifically identified.

## 2.0 SCOPE

The scope of this report includes the hardware and software associated with the MELTAC Nplus S platform. Components unique to the MELTAC Nplus platform for non-safety applications are not discussed, except to the extent of their interface with MELTAC Nplus S components in safety systems. The MELTAC platform described herein encompasses design, qualification, and reliability.

### 3.0 APPLICABLE CODE, STANDARDS AND REGULATORY GUIDANCE

This section identifies conformance to applicable codes, standards, and regulatory guidance required by NUREG-0800 and ISG-06. Unless specifically noted, the latest version issued on the date of this Topical Report is applicable.

Appendix D shows the compliance matrix of codes, standards, and regulatory guidance required by NUREG-0800 and ISG-06. Also, Appendix D points to the corresponding location within this Topical Report that describes design information related to the applicable codes, standards, and regulatory guidance of the MELTAC platform.

#### Code of Federal Regulations

1. 10 CFR Part 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 that meets all requirements of 10 CFR Part 50 Appendix B is described in Section 6. This is referred to as the App.B-based quality assurance program (QAP).

MELTAC was developed under a Japanese QA program and has undergone a one-time commercial grade dedication (CGD) by MELCO for use in US safety - related applications. The details of that CGD program are provided in this report by reference. MELTAC is now maintained and manufactured under MELCO's 10 CFR 50 Appendix B QAP.

##### GDC 2: Design Bases for Protection against Natural Phenomena

This Equipment is seismically qualified. The Equipment must be located within building structures that provide protection against other natural phenomena. Specific buildings and Equipment locations are described in Application Licensing Documentation.

##### GDC 4: Environmental and Dynamic Effects Design Bases

This Equipment is qualified for use in a mild environment that is not adversely affected by plant accidents as described in Section 5.

##### GDC 21: Protection System Reliability and Testability

This Equipment includes automated testing with a high degree of coverage, and additional overlapping manual test features for the areas that are not covered by automated tests. All manual tests may be conducted with the plant on line, with consideration of plant specific accessibility, and with the Equipment bypassed or out of service. Depending on the system design for a specific plant, the Equipment is configured with N or N+1 redundancy, where N is the number of divisions needed for single failure compliance and to meet the plant reliability goals. For systems with N+1 redundancy, this GDC is met with one division continuously bypassed or out of service. The redundancy configuration for each plant system is described in Application Licensing Documentation.

#### GDC 22: Protection System Independence

Redundant divisions are physically and electrically isolated to ensure that failures that originate in one division cannot propagate to other divisions. Physical isolation is discussed in Application Licensing Documentation. Platform features to accommodate electrical isolation are discussed in this Topical Report.

All Equipment is qualified to ensure that the Equipment is unaffected by adverse conditions that may concurrently affect multiple divisions. The qualification limits of this equipment are described in this Topical Report. Application Licensing Documentation describes the specific analysis for each plant.

Interlocks between redundant divisions and administrative controls ensure maintenance is performed on one division at a time. Interlocks and administrative controls are described in Application Licensing Documentation.

#### GDC 23: Protection System Failure Modes

Signals are generated for all detected failures. These signals can be configured at the application level to generate alarms. Functions can be designed to fail to an actuated trip state on loss of all power, on failures that are not automatically detected, or on failures that are automatically detected and would prevent proper execution of the function. Functions can also be designed to fail to an unactuated state. The unactuated state may be desirable to avoid spurious plant transients. Compliance for reactor trip and engineered safety features actuation functions are application specific and described in Application Licensing Documentation.

#### GDC 24: Separation of Protection and Control Systems

The separation of protection and control systems is an application specific design characteristic. Redundant divisions of the protection systems are physically and electrically isolated from the non-safety control systems. Where safety sensors are shared between control and protection systems, signal selection logic is typically used in the control system to prevent erroneous control actions due to single sensor failures. Eliminating these erroneous control actions prevents challenges to the protection system while it is degraded due to the same sensor failure. Where non-safety signals control safety systems or components, logic in the safety systems is typically used to ensure prioritization of safety functions. The details regarding the separation of protection and control systems are described in Application Licensing Documentation.

## 2. 10 CFR Part 50.55a

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

Section 6 describes the App.B-based QAP, which is fully compliant to 10 CFR 50 Appendix B.

MELCO has undergone an inspection by NRC to verify the implementation of an adequate QAP.

---

(h) Invokes IEEE Std. 603-1991

See conformance to IEEE Std. 603-1991

### **NRC Regulatory Guides**

3. RG 1.22 Periodic Testing of Protection System Actuation Functions (Rev. 0, February 1972)  
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.
4. RG 1.29 Seismic Design Classification (Rev. 4, March 2007)  
The Equipment is designated Seismic Category I.
5. RG 1.53 Application of the Single-Failure Criterion to Safety Systems (Rev. 2, November 2003)  
endorses IEEE Std. 379-2000  
See conformance to GDC 21 and 24. This Equipment can be configured at the application level so that safety functions are designed with N or N+1 divisions. Each safety division can be independent from the other safety divisions and from non-safety divisions. Independence ensures that credible single failures cannot propagate between divisions within the system and therefore cannot prevent proper protective action at the system level. Single failures considered in the divisions are described in the Failure Mode and Effect Analysis (FMEA) for each system. The FMEA method for the components of this Equipment is provided in this Topical Report. The MELTAC module level FMEA report is incorporated by reference. The module level FMEA provides input to the system level FMEA for each application. The system level FMEA is described in Application Licensing Documentation.
6. RG 1.75 Criteria for Independence of Electrical Safety Systems (Rev. 3, February 2005)  
endorses IEEE Std. 384-1992  
The MELTAC platform contains features to ensure that redundant safety divisions are physically and electrically independent of each other and physically and electrically independent of any non-safety divisions. Physical independence is maintained either by the required distance or by barriers which prevent propagation of fire or electrical faults. Electrical independence is maintained by fiber optic cable communication interfaces or conventional isolators, such as opto-couplers, relays or transformers. Conventional isolators include fault interrupting devices such as fuses or circuit breakers. Fiber optic cable communication interfaces are described in Section 4.3.2 (Control Network), 4.3.3 (Data Link) and 4.3.4 (Maintenance Network). Specifications and qualification of conventional isolators are discussed in Section 4.1.2 and 5.5 of this Topical Report, respectively.



- 
7. RG 1.89 Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants (Rev. 1, June 1984)

endorses IEEE Std. 323-1974

The environmental qualification of this Equipment is by an appropriate combination of type testing and analysis. This Equipment is qualified for use in a mild environment that is not adversely affected by plant accidents. Qualification for temperature and humidity is by type test. The generic MELTAC temperature and humidity qualification is demonstrated to envelope actual plant conditions by analysis of room ambient conditions and heat rise calculations for the installed configuration. Seismic qualification is by type testing. The generic MELTAC seismic qualification is demonstrated to envelope actual plant conditions by analysis of floor response spectrum at the installed location. Electromagnetic Interference (EMI) qualification is by type testing. MELTAC is generically qualified to the EMI envelope and acceptance criteria that are identified by regulatory guidance as enveloping US nuclear plant installations; therefore there is no additional site specific EMI qualification.

This Equipment has no known aging mechanisms, except as noted in Section 7.4 and accommodated by periodic replacement; random failures will be detected through self-diagnoses and periodic surveillance testing. Type testing for conformance to RG 1.89 is described through the aggregate of all qualification reports – Environmental, Seismic and Electromagnetic Compatibility (EMC), see Section 5.

8. RG 1.100 Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants (Rev. 3, September 2009)

This Equipment is designated Seismic Category I. It is designed and qualified to withstand the cumulative effects of a minimum of 5 Operating Basis Earthquakes (OBEs) and one Safe Shutdown Earthquake (SSE) without loss of safety function or physical integrity. The input spectrum is selected to envelope all anticipated applications. Conformance to this envelope for specific applications is discussed in Application Licensing Documentation.

9. RG 1.105 Setpoints for Safety-Related Instrumentation (Rev. 3, December 1999)

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

The uncertainties associated with the Equipment are described in this Topical Report. Appendix A.5 defines I/O module 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 Application Licensing Documentation. The plant specific uncertainty/setpoint analysis is described in Application Licensing Documentation.

- 
10. RG 1.118 Periodic Testing of Electric Power and Protection Systems (Rev. 3, April 1995)  
endorses IEEE Std. 338-1987  
See conformance to GDC 21, 10 CFR 50.36 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.
11. RG 1.152 Criteria for Use of Computers in Safety Systems of Nuclear Power Plants (Rev. 3, July 2011)  
endorses IEEE Std. 7-4.3.2-2003  
The methods used for specifying, designing, verifying, validating and maintaining software for this Equipment conforms to these requirements, including requirements for a secure development environment and MELTAC features that facilitate a secure operational environment. The life cycle process for the MELTAC platform is described in "MELTAC Platform Software Program Manual" (JEXU-1041-1016).  
  
MELCO has undergone an inspection by NRC to verify the implementation of an adequate QAP.  
  
The life cycle process for the system application software is described in the Application Licensing Documentation.  
  
The methods used for ensuring a secure development and operational environment throughout the life cycle are described in these documents.
12. RG 1.153 Criteria for Safety Systems (Rev. 1, June 1996)  
endorses IEEE Std. 603-1991  
Compliance with the General Design Criterion identified in this Regulatory Guide is discussed above. Compliance with IEEE Std. 603-1991 is discussed below.
13. RG 1.168 Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants (Rev. 2, July 2013)  
endorses IEEE Std. 1012-2004 and IEEE Std. 1028-2008  
This Equipment uses processes for verification, validation, reviews and audits that conform to this Regulatory Guide. The software life cycle process for the MELTAC platform is described in "MELTAC Platform Software Program Manual" (JEXU-1041-1016). MELCO has undergone an inspection by NRC to verify the implementation of an adequate QAP.  
  
The life cycle process for the system application software is described in the Application Licensing Documentation.
14. RG 1.169 Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants (Rev. 1, July 2013)  
endorses IEEE Std. 828-2005 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 MELTAC platform is described in "MELTAC Platform Software Program Manual" (JEXU-1041-1016). MELCO has undergone an inspection by NRC to verify the implementation of an adequate QAP.

The Configuration Management for the system application software is described in the Application Licensing Documentation.

15. RG 1.170 Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants (Rev. 1, July 2013)

endorses IEEE Std. 829-2008

The test documentation for this Equipment conforms to this Regulatory Guide. The test process and corresponding documentation for the MELTAC platform are described in "MELTAC Platform Software Program Manual" (JEXU-1041-1016). MELCO has undergone an inspection by NRC to verify the implementation of an adequate QAP.

The test documentation for the system application software is described in the Application Licensing Documentation.

16. RG 1.171 Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants (Rev. 1, July 2013)

endorses IEEE Std. 1008-1987

Unit testing for this Equipment conforms to this Regulatory Guide. The unit testing for the MELTAC platform is described in "MELTAC Platform Software Program Manual" (JEXU-1041-1016). MELCO has undergone an inspection by NRC to verify the implementation of an adequate QAP.

Unit testing for the system application software is described in the Application Licensing Documentation.

17. RG 1.172 Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants (Rev. 1, July 2013)

endorses IEEE Std. 830-1998

The Software Requirements Specifications for this Equipment conforms to this Regulatory Guide. The Software Requirements Specifications for the MELTAC platform are described in in Section 6.1 of this Topical Report. MELCO has undergone an inspection by NRC to verify the implementation of an adequate QAP.

The Software Requirements Specifications for the system application software are described in the Application Licensing Documentation.

- 
18. RG 1.173 Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants (Rev. 1, July 2013)  
endorses IEEE Std. 1074-2006
- The Software Life Cycle Process for this Equipment conforms to this Regulatory Guide. The Software Life Cycle Processes for the MELTAC platform are described in "MELTAC Platform Software Program Manual" (JEXU-1041-1016). MELCO has undergone an inspection by NRC to verify the implementation of an adequate QAP.
- The Software Life Cycle Processes for the system application software are described in the Application Licensing Documentation.
19. RG 1.180 Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related Instrumentation and Control Systems (Rev. 1, October 2003)  
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 (Radio Frequency Interference) requirements of this standard. Qualification testing for the digital platform is described in this Topical Report.
20. RG 1.204 Guidelines for Lightning Protection of Nuclear Power Plants (Rev. 0, November 2005)
- The platform has been designed with surge resistance. Surge qualification testing has been performed using ANSI Std. 62.41, ANSI Std. 62.45, and IEEE Std. 472, see Section 5.3.
21. RG 1.209 Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants (Rev. 0, March 2007)  
endorses IEEE Std. 323-2003
- This Equipment is tested and analyzed to satisfy the mild environment qualification requirements.

### **NRC Branch Technical Positions**

22. BTP 7-8 Guidance for Application of Regulatory Guide 1.22
- The Equipment includes extensive self-diagnosis tests which run continuously. The LCO related to bypassed or out of service conditions for a single division are dependent upon the extent of redundancy and the extent of automated self-testing for the equipment that remains in service to perform the safety function. The Equipment can be configured at the application level with additional manual test features to test the portions of the system that are not tested automatically. These manual test features can be configured so that all

---

functions of the protection system are testable at power. Self-diagnosis tests are described in Section 4.1.5 of this Topical Report. Manual test features are described in Section 4.1.7 and 4.2.4 of this Topical Report, and also in Application Licensing Documentation.

23. BTP 7-11 Guidance on Application and Qualifications of Isolation Devices  
endorses IEEE Std. 472, ANSI Std. C62.36, ANSI Std. C62.41, ANSI Std. C62.45  
See conformance to RG 1.75. Isolation devices are qualified in conformance to these standards.
24. BTP 7-14 Guidance on Software Reviews for Digital Computer-Based I&C Systems  
See conformance to RG 1.168 through 1.173.
25. BTP 7-17 Guidance on Self-Test and Surveillance Test Provisions  
See conformance to GDC 21, 10 CFR 50.36, RG 1.22 and RG 1.118.  
Surveillance testing taken together with automatic self-testing provides a mechanism for detecting all failures. The methods used for testing are described in Application Licensing Documentation.
26. BTP 7-21 Guidance on Digital Computer Real-Time Performance  
The real-time performance for this Equipment conforms to this BTP. The response time performance for digital platform components is described in Section 4.4 of this Topical Report. Requirements for system response time for conformance with the plant design basis and the response time of actual plant systems is described in Application Licensing Documentation.

#### **NUREG-Series Publications (NRC Reports)**

27. NUREG-0737, Supplement 1 Clarification of TMI Action Plan Requirements  
This Equipment can be configured at the application level for conformance to the following TMI Action Plan Requirements:
- Plant Safety Parameter Display – This Equipment can provide safety-related data to the non-safety HSI system which can provide this display for the control room and for emergency support facilities.
  - Indication and Control for Safety Components (e.g.: relief valves, pressurizer heaters, containment isolation valves), Inadequate Core Cooling Monitoring and Instrumentation for Accident Monitoring - This Equipment can provide safety-related controls and monitoring for safety-related instruments to generate safety-related displays. Alarms and non-safety displays can be generated by the non-safety HSI system.

- 
28. NUREG-0800 Chapter 7 of the USNRC Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, Section 7.1 Rev.5  
This Equipment fulfills all safety-related requirements of this NUREG for monitoring safety-related plant instrumentation and controlling safety-related plant components. Descriptions of specific plant systems are described in Application Licensing Documentation.
  29. NUREG/CR-6303 Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems  
The design of this Equipment is described in this Topical Report. Functional diversity within the safety and non-safety I&C systems is described by the Application Licensing and design documentation.
  30. NUREG/CR-6421 A Proposed Acceptance Process For Commercial-Off-The-Shelf (COTS) Software in Reactor Applications  
This NUREG is not applicable to this Equipment since there is no COTS software. All software has been designed for nuclear applications.

#### **Digital Instrumentation and Controls (DI&C) Interim Staff Guidance (ISG)**

31. DI&C-ISG-04 Highly-Integrated Control Rooms – Communications Issues (Rev 1, March 2009)  
A detailed discussion of the MELTAC platform communication systems and compliance with the requirements given in DI&C-ISG-04 is provided in Section 4.3 and “MELTAC Platform ISG-04 Conformance Analysis” (JEXU-1041-1015 Rev.0).
32. DI&C-ISG-06 Licensing Process (Rev 1, January 2011)  
DI&C-ISG-06 is intended for plant-specific licensing amendment requests (LARs) and lists the documents expected for a plant-specific review of a digital safety system. Some interpretation is required to identify the subset of documentation that applies to a generic review of a safety system digital platform. This interpretation and summary of DI&C-ISG-06 compliance is given in "Mapping of MELTAC Platform Licensing Documents to the DI&C-ISG-06 Guidance" (JEXU-1041-1012 Rev0).

#### **IEEE Standards**

33. IEEE Std. 7-4.3.2-2003 Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations  
This Equipment conforms to all requirements of this standard, as augmented by RG 1.152.

- 
34. IEEE Std. 323-2003 Qualifying Class 1E Equipment for Nuclear Power Generating Systems  
This Equipment is qualified in conformance to this standard, as augmented by RG 1.89. See conformance to RG1.89.
35. IEEE Std. 338-1987 Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems  
The self-diagnosis that is usable for Periodic Surveillance Testing are described throughout this document. RG1.22 and Std. IEEE 338 test features that are configured at the system level or within the application software are described by the Application Licensing and design documentation.
36. IEEE Std. 344-2004 Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations  
This Equipment conforms to this standard as augmented by RG 1.100. Conformance is described in the Section 5 of this Topical Report.
37. IEEE Std. 379-2000 Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems  
As described in RG1.53 item 13, compliance to the Single-Failure Criterion is achieved through the configuration of this Equipment at the system level.
38. IEEE Std. 383-2003 Type Test of Class 1E Electric Cables, Field Splices, and Connections for Nuclear Power Generating Stations  
The cable and electrical connections used within MELTAC cabinets conform to this standard, including requirements for flame retarding qualification. Cables for interfaces between MELTAC cabinets and interfaces to/from MELTAC cabinets to other I&C systems and components are discussed in Application Licensing Documentation.
39. IEEE Std. 384-1992 Criteria for Independence of Class 1E Equipment and Circuits  
This Equipment supports conformance to this standard as augmented by RG 1.75. All safety functions implemented within multiple divisions can have physical separation and electrical independence between redundant safety divisions and between safety and non-safety divisions. Electrical independence between divisions is accomplished through the use of fiber optic cables or conventional qualified isolators. Digital data communication using fiber optic cables also facilitates physical independence between divisions. MELTAC components for electrical isolation are described in Section 4 (4.3.2.3) of this Topical Report.
40. IEEE Std. 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 Topical Report. Equipment is clearly marked to
-

---

identify safety-related designations, as described in Section 6.1.8 Identification of Equipment. Other enclosures, including any deviations from this standard, are described in Application Licensing Documentation.

41. IEEE Std. 472 IEEE Guide for Surge Withstand Capability (SWC) Tests  
Power supplies and Input/Output modules used within this Equipment conform to this standard. Conformance to surge withstand requirements is described in the EMC Qualification Report.
42. IEEE Std. 497-2002 Accident Monitoring Instrumentation for Nuclear Power Generating Stations  
See conformance for RG 1.97.
43. IEEE Std. 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
- Specifications corresponding to the key requirements above are described in Sections 4 through 7.
44. IEEE Std. 730-1989 Software Quality Assurance Plans  
The Software Quality Assurance Plans are described in Section 6 and "MELTAC Platform Software Program Manual" (JEXU-1041-1016).
45. IEEE Std. 828-2005 IEEE Standard for Software Configuration Management Plans  
The Software Configuration Management Plan is described in Section 6 and "MELTAC Platform Software Program Manual" (JEXU-1041-1016).  
As the Standard of Configuration Management, ISG-06 refers to IEEE Std. 828-1990 and IEEE Std. 828-1998.  
IEEE Std. 828-1998 contains the contents of IEEE Std. 828-1990. Therefore, this Topical Report refers IEEE Std. 828-1998 as the applicable standard.
46. IEEE Std. 829-2008 Software Test Documentation



- 
47. The software test documentation is described in "MELTAC Platform Software Program Manual" (JEXU-1041-1016).  
IEEE Std. 830-1998 IEEE Recommended Practice for Software Requirements Specifications  
The software requirements are documented in the Platform specification as an output of Requirement Phase, which is described in Section 6.1.
48. IEEE Std. 1008-1987 IEEE Standard for Software Unit Testing  
Software unit testing is described in "MELTAC Platform Software Program Manual" (JEXU-1041-1016).
49. IEEE Std. 1012-2004 IEEE Standard for Software Verification and Validation Plans  
Software V&V is described in "MELTAC Platform Software Program Manual" (JEXU-1041-1016).
50. IEEE Std. 1016-1987 IEEE Recommended Practice for Software Design Descriptions  
The software design description is documented in the Software Specifications as outputs of Design Phase which is described in Section 6.1.
51. IEEE Std. 1028-2008 IEEE Standard for Software Reviews and Audits  
Software reviews and audits are described in "MELTAC Platform Software Program Manual" (JEXU-1041-1016).
52. IEEE Std. 1042-1987 IEEE Guide To Software Configuration Management  
Configuration management is described in "MELTAC Platform Software Program Manual" (JEXU-1041-1016).
53. IEEE Std. 1074-2006 IEEE Standard for Developing Software Life Cycle Processes  
The software life cycle process is described in Section 6 and in "MELTAC Platform Software Program Manual" (JEXU-1041-1016).
54. IEEE Std. 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

55. 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.
56. 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.

## 57. 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.

## 58. ISA-S67.04-1994 Setpoints For Nuclear Safety Related Instrumentation Used in Nuclear Power Plants

See conformance to RG 1.105. The methodology used to develop setpoints is described in Application Licensing and Design Documentation.

## 59. 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.

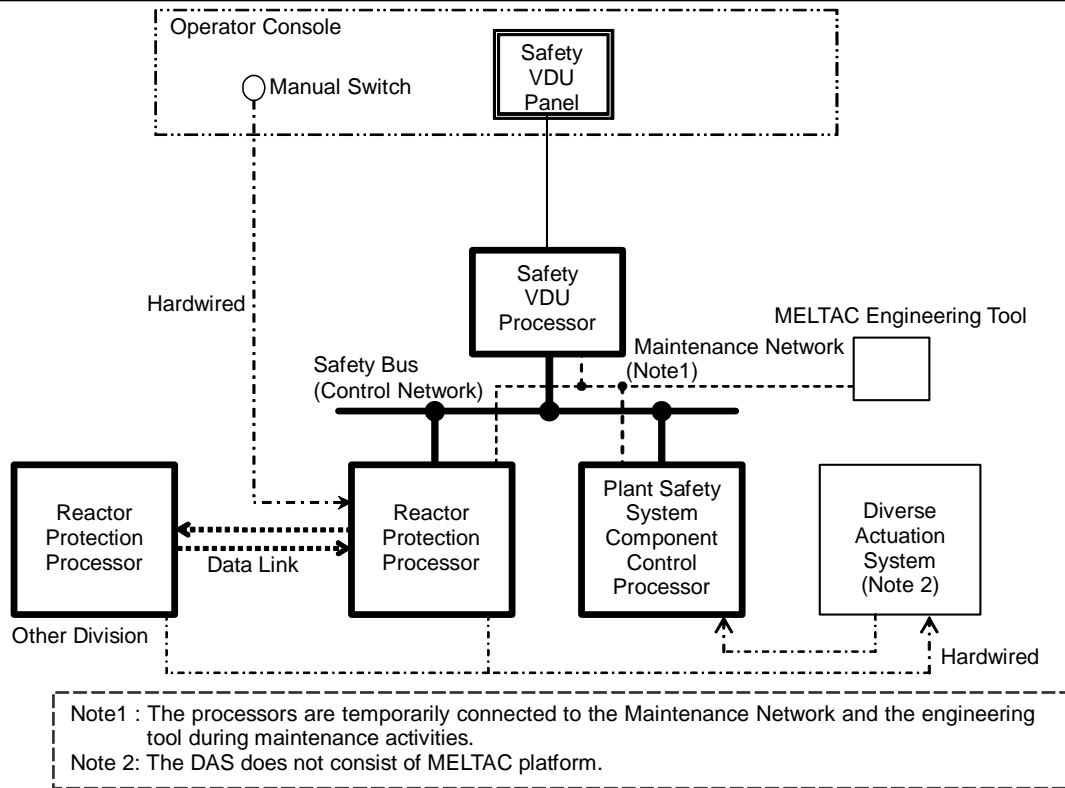
## 4.0 MELTAC PLATFORM DESCRIPTION

The MELTAC platform is based on using qualified building blocks that can be used for many safety system applications. The building blocks are the following items.

- Controller
- Safety VDU (Visual Display Unit) panel and processor
- Control Network
- Data Link

The MELTAC platform can take a single controller configuration, redundant standby controller configuration, or redundant parallel controller configuration, depending on the system requirements. The I/O modules can also take a redundant configuration. The MELTAC platform includes a large variety of I/O modules that can interface with various plant components (See Section 4.1). Also, the MELTAC platform includes a safety VDU which consists of a safety VDU panel and processor (See Section 4.2). The Control Network is used to communicate safety-related data between multiple controllers, and between controllers and the safety VDU processor(s) in the same division. The Data Link is used to transmit process signals between the controllers in different safety divisions or trains (See Section 4.3).

A typical configuration of the MELTAC platform for a safety system is shown in Figure 4.0-1. It shows a single division of a Plant Safety System (PSS) with an interface to a different division via Data Link. It also shows Controllers, which are the main component of the MELTAC platform, as the Reactor Protection Processor (RPP) and the Plant Safety System Component Control Processor (PSS-CCP).



**Figure 4.0-1 MELTAC Platform Typical PSS Configuration**

The PSS provides monitoring and displays for safety-related plant instrumentation, and automated actuation and manual control of safety-related plant components. It consists of multiple independent safety divisions.

The PSS consists of the following items described in a) to g).

- a) Each PSS division typically contains one Reactor Protection Processor (RPP). The RPP is a MELTAC controller with associated I/O modules. The RPP performs the following key functions:
  - Execute reactor trip (RT) functions and Engineered Safety Features (ESF) functions
  - Receive RT and ESF initiation signals from the RPPs of other divisions via inbound inter-division Data Links, and transmit those same signals from its own division to the other divisions via an outbound inter-division Data Link
  - Direct actuation of RT Breakers (RTB)
  - Transmit Interlock and ESF initiation signals via the intra-division Control Network to PSS Component Control Processors (PSS-CCPs)
  - Receive manually initiated control commands from the safety Visual Display Unit (VDU) processors via the intra-division Control Network
  - Transmit the monitored plant sensor data and status to the safety VDU processors via the intra-division Control Network
- b) The number of PSS-CCPs per division is application specific. Each PSS-CCP is a MELTAC controller with associated I/O modules. The PSS-CCPs perform the following key functions:

- 
- Control and drive the plant components and equipment by ESF actuation signal from the RPP
  - Receive ESF actuation signals from the RPP via the intra-division Control Network
  - Receive manual component control commands from the safety VDU processors via the intra-division Control Network
  - Receive diverse component control signals from the Diverse Actuation System (DAS), and combine the signals with the control signals from the PSS-CCPs within the hardware based Interposing Logic (IPL) of the Power Interface (PIF) Module to determine the final control command relayed to each plant component
  - Transmit the monitored status of interlocks and components to the safety VDU processors via the intra-division Control Network
- c) Each PSS division typically contains at least one safety VDU processor and safety VDU panel. The safety VDU processor and safety VDU panel consist of a special purpose MELTAC controller, peripherals, and an LCD touch screen. The safety VDU processor and safety VDU panel perform the following key functions:
- Transmit the operation signals to the RPP and PSS-CCPs via the intra-division Control Network, and can be configured to provide the human-machine interface
  - Receive plant sensor data, RT and ESF initiation, and actuation status from the RPP via the intra-division Control Network
  - Receive interlock and component status data from the PSS-CCPs via the intra-division Control Network
  - Receive touch commands from safety VDU panel
- d) There is one MELTAC engineering tool connected via Maintenance Network in each PSS division used exclusively for the following functions within that one division:
- To display self-test diagnostics reported from all PSS processors within the division
  - To store copies of software for all processors within the division, and to conduct the manually initiated Memory Integrity Check (MIC) using that stored software
  - To control the updating of software for any processor within the division, utilized only when a processor is taken out-of-service and declared inoperable by plant Technical Specifications and the processor CPU Module is removed and transferred to the dedicated Re-programming Chassis
  - To control simulated input values for troubleshooting any processors within the division, only when a processor is taken out-of-service and declared inoperable by plant Technical Specification
- e) There is one Control Network in each PSS division used for the following key intra-division communication functions:
- Interlock and ESF initiation signals from the RPP to the PSS-CCPs
  - Manual control commands from the safety VDU processor to the RPP and the PSS-CCPs
  - Monitored plant sensor data, RT and ESF initiation, and actuation status from the RPP to the safety VDU processor
  - Monitored plant sensor data, interlock and component status data from the PSS-CCPs to the safety VDU processor
- f) There is one Data Link in each PSS division used for broadcasting RT and ESF initiation signals from one PSS division to each of the other divisions.
-

- 
- g) Each PSS division typically contains Manual Switches. Manual Switches manually initiate the same RT and ESF functions that are automatically initiated by the RPP. The switch for each function interfaces with the RPP using conventional hardwired interfaces.

## **4.1 Controller**

### **4.1.1 Hardware Configuration**

The controller for the MELTAC platform consists of the following parts.

- a) 1 CPU Chassis including 1 or 2 subsystems, 1 Switch Panel, 1 or 2 Status Display (and Switch) Modules, and 1 Fan Unit. Each subsystem consists of 1 or 2 Power Supply Modules, a CPU Module, 1 or more Control Network I/F Modules, a System Management Module, and 1 or more Bus Master Modules. Each subsystem communicates with the Control Network via its own Optical Switch.
- b) Multiple I/O Chassis, each with multiple I/O modules

#### **4.1.1.1 Configuration Concept**

The MELTAC platform is capable of operating in any of the 3 following configurations:

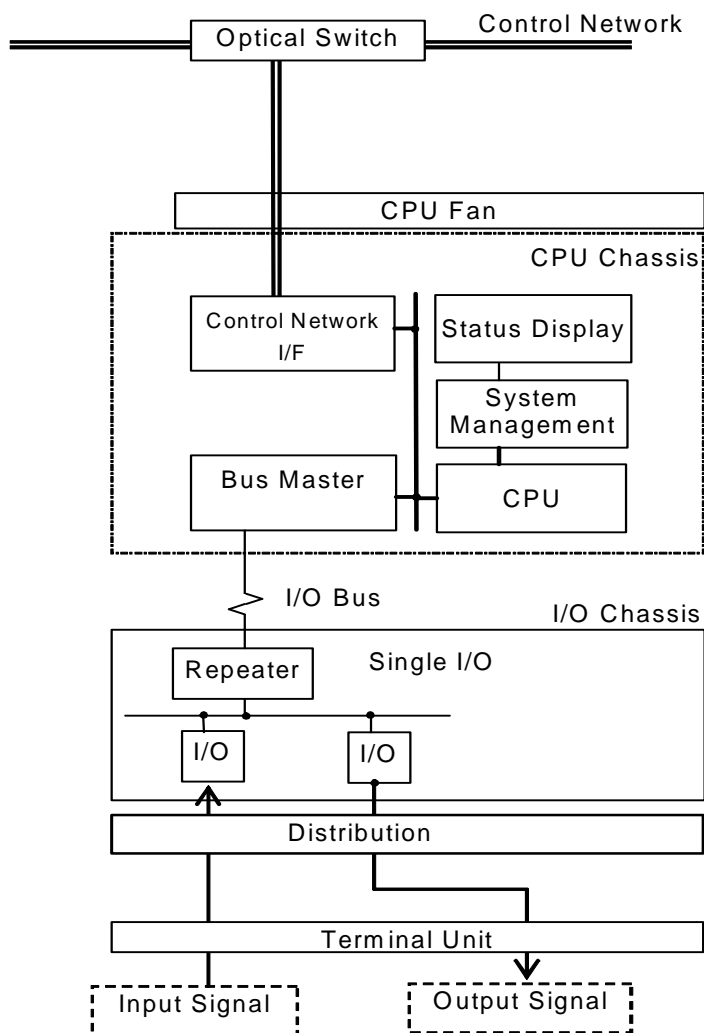
- a) **Single Controller Configuration**  
The controller includes 1 subsystem. The subsystem operates in Control Mode. (Control Mode means the subsystem controls the outputs to plant components.)
- b) **Redundant Parallel Controller Configuration**  
The controller includes 2 subsystems. Each subsystem operates in Control Mode.
- c) **Redundant Standby Controller Configuration**  
The controller includes 2 subsystems. 1 subsystem operates in Control Mode while the other subsystem operates in Standby Mode. Standby Mode means the subsystem is closely monitoring the operation of the subsystem in Control Mode, including memory states. If that subsystem fails, the subsystem operating in Standby Mode will automatically switch to Control Mode, with no bump in the control outputs.

The configuration to be applied is determined based on the application system requirements. Any of the 3 configurations may be applied to safety systems.

For redundant configurations, the internally redundant subsystems are only for reliability enhancement. This redundancy is not credited for single failure compliance. Single failure compliance is achieved through multiple controllers located in physically separate and independent safety divisions.

#### 4.1.1.1.1 Single Controller Configuration

The single controller configuration is shown in Figure 4.1.1-1.



**Figure 4.1.1-1 Single Controller Configuration**

The single controller consists of the following:

**a) CPU Chassis**

The CPU Chassis includes 1 subsystem and a CPU Fan. A subsystem consists of a CPU Module, System Management Module, Status Display Module, Control Network I/F Module, and Bus Master Module. A subsystem communicates with the Control Network via its own Optical Switch. A subsystem is capable of driving a number of Control Network I/F Modules and Bus Master Modules depending on the scale of the application.

**b) I/O Chassis**

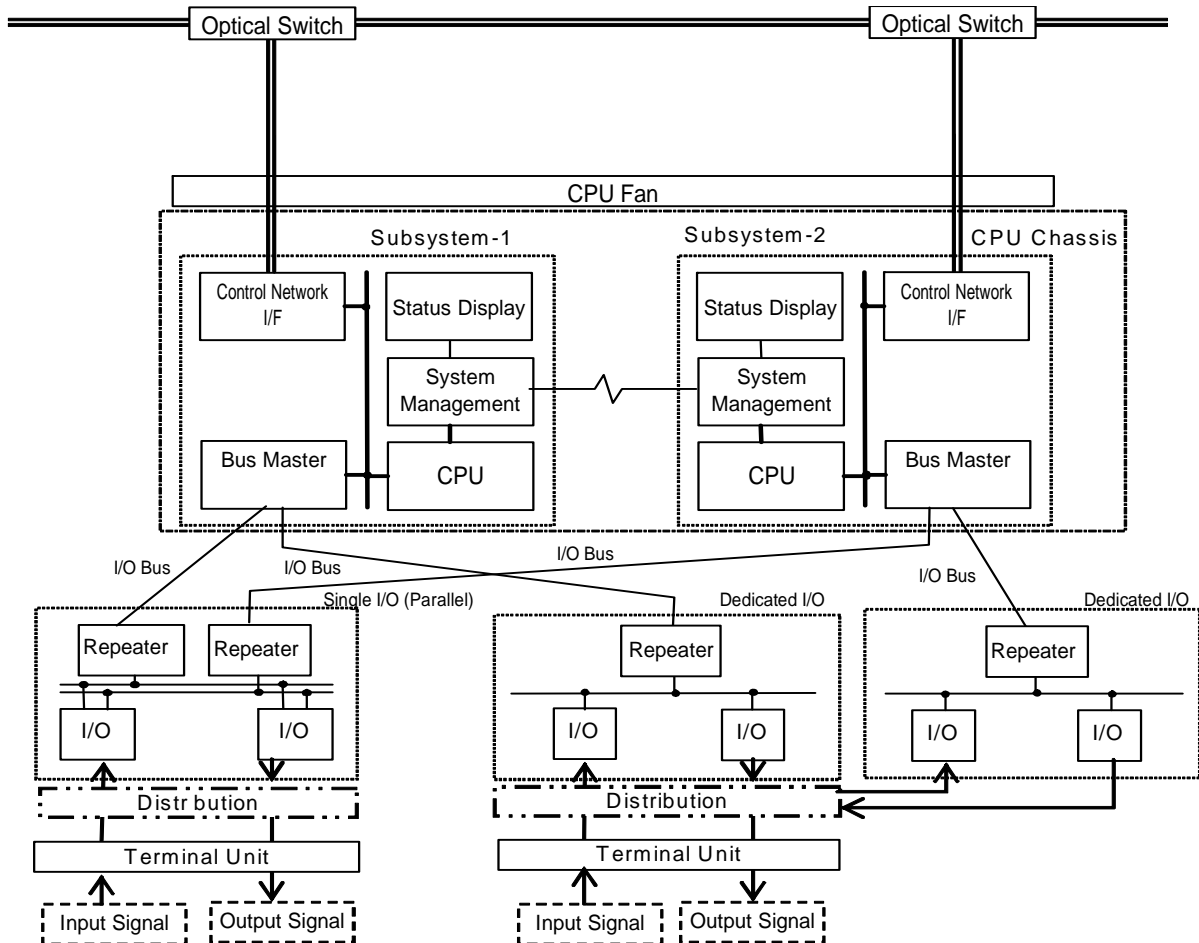
The I/O Chassis includes only single I/O. Single I/O consists of a Repeater Module and multiple I/O modules. Each I/O module communicates with the Bus Master Module in the subsystem via the Repeater Module and the I/O bus.

The I/O modules receive signals from sensors and send control outputs to components via the Terminal Unit and Distribution Module. For single I/O, the Distribution Module works as a surge absorber between the I/O modules and the Terminal Unit which connects external cables.



#### 4.1.1.1.2 Redundant Parallel Controller Configuration

The redundant parallel controller configuration is shown in Figure 4.1.1-2. This configuration can only be used within the same division (i.e.: the redundant subsystems cannot be in different divisions), because there is no electrical or functional independence between subsystems.



**Figure 4.1.1-2 Redundant Parallel Controller Configuration**

The redundant parallel controller consists of the following:

##### a) CPU Chassis

The CPU Chassis includes Subsystem-1, Subsystem-2, and a CPU Fan. Both subsystems have the same configuration. Each subsystem consists of a CPU Module, System Management Module, Status Display Module, Control Network I/F Module, and Bus Master Module. Each subsystem communicates with the Control Network via its own Optical Switch. The subsystem is capable of driving a number of Control Network I/F Modules and Bus Master Modules depending on the scale of the application.

In the redundant parallel controller configuration, both subsystems operate in Control Mode. Each subsystem operates independently. However, when a subsystem initially starts, the Data

Link between the System Management Modules allows all state based logic to be updated, if the other subsystem is already in Control Mode. Since both systems operate in Control Mode, there is no subsystem changeover to accommodate a subsystem failure as in the redundant standby configuration.

The Status Display Module displays the mode and alarms of the subsystem.

#### **b) I/O Chassis**

The redundant parallel controller can be configured with either redundant I/O (called dedicated I/O) and/or non-redundant I/O (called single I/O).

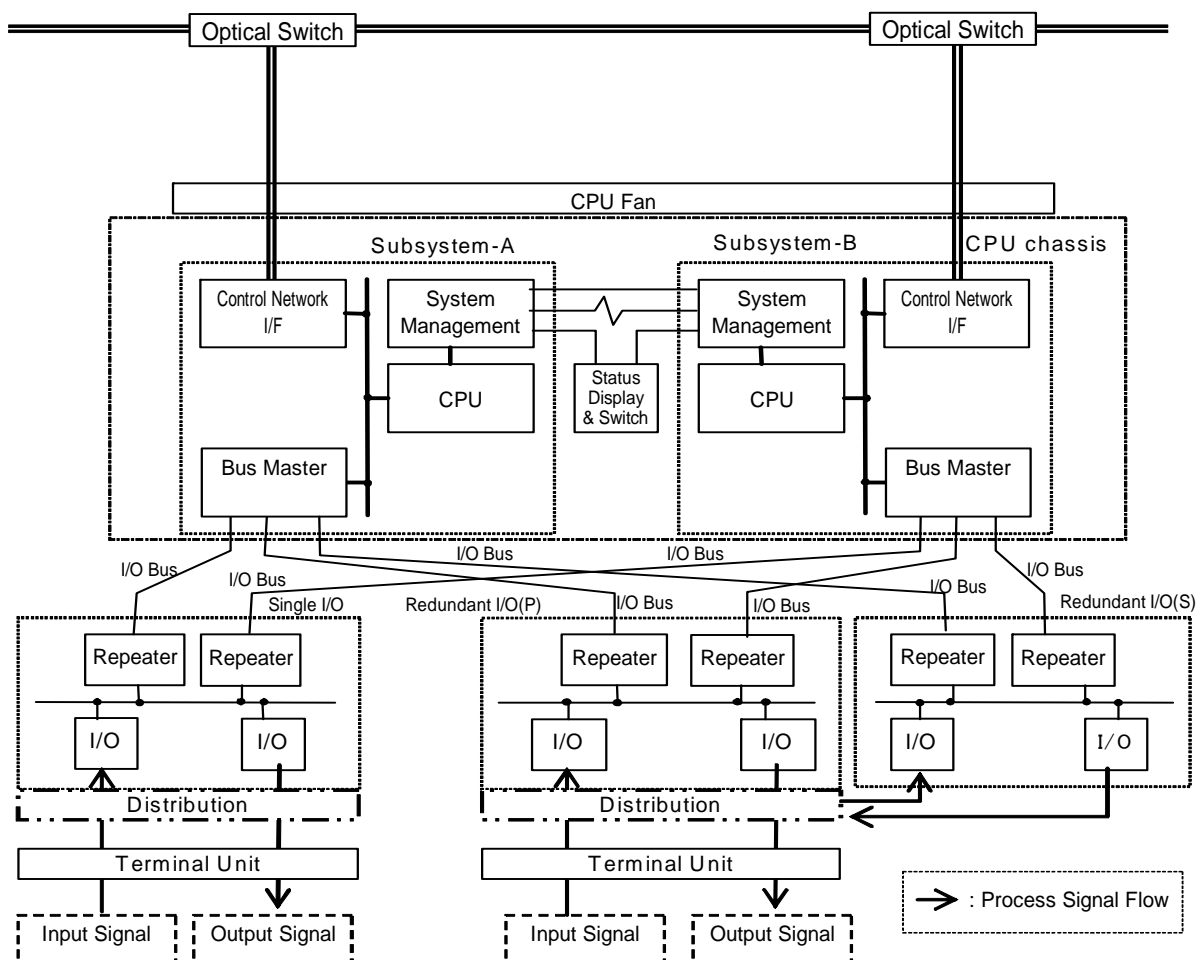
For single I/O, each non-redundant I/O module communicates with the Bus Master Modules in Subsystem-1 and Subsystem-2 via separate Repeater Modules and the redundant I/O bus. The single I/O, redundant Repeater Modules, and redundant I/O bus are all contained within the same I/O Chassis. The data from each non-redundant input module is communicated to both subsystems. The output control signals from each subsystem are logically combined within the non-redundant output modules. Each output can be individually configured using 1-out-2 or 2-out-of-2 voting logic, as needed for the specific application. The single I/O for a redundant parallel controller is referred to as single I/O (Parallel) to distinguish it from the single I/O for a single controller. Single I/O (Parallel) provides interfaces for the redundant I/O bus and the redundant subsystems.

To enhance I/O reliability, a redundant parallel controller can also be configured with redundant dedicated I/O. Dedicated I/O is distributed in 2 separate I/O Chassis. Each chassis consists of a Repeater Module and multiple dedicated I/O modules. Each dedicated I/O module communicates with the Bus Master Module in only 1 subsystem via the Repeater module and the I/O bus within the chassis. Therefore, each dedicated I/O module is subordinate to Subsystem-1 or Subsystem-2. The same input signals are distributed to each dedicated I/O module via the Distribution Module. And output signals from each dedicated I/O module are combined in the Distribution Module by using wired OR logic.

The Terminal Units for dedicated I/O are the same as for single I/O.

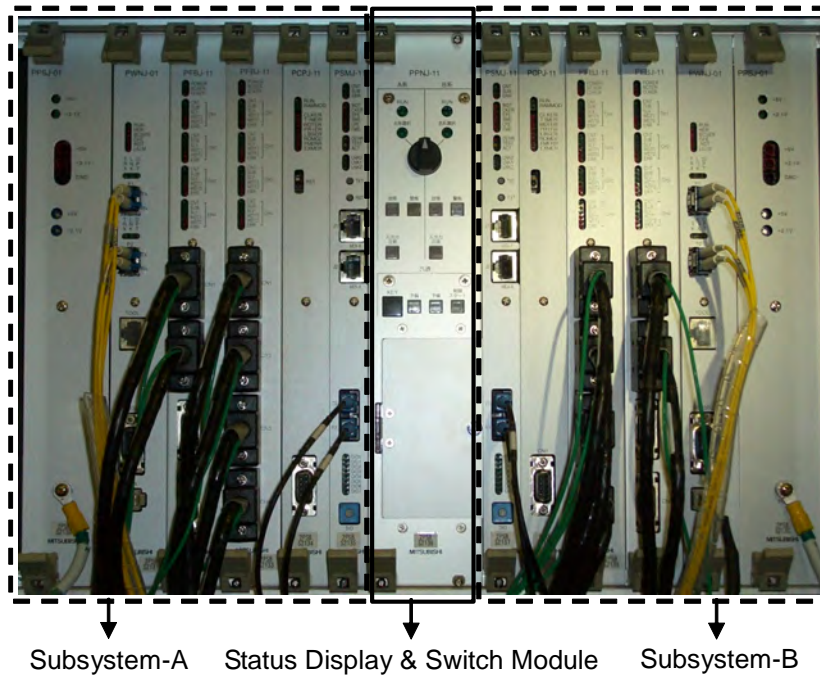
#### 4.1.1.1.3 Redundant Standby Controller Configuration

The redundant standby controller configuration is shown in Figure 4.1.1-3.



**Figure 4.1.1-3 Redundant Standby Controller Configuration**

A photograph of the MELTAC redundant standby controller configuration is shown in Figure 4.1.1-4.



**Figure 4.1.1-4 Picture of Modules in a CPU Chassis for a Redundant Standby Controller Configuration**

The redundant standby controller consists of the following.

**a) CPU Chassis**

The CPU Chassis includes Subsystem-A, Subsystem-B, a Status Display & Switch Module, and a CPU Fan. Both subsystems have the same configuration. Each subsystem consists of a CPU Module, System Management Module, Control Network I/F Module, and Bus Master Module. Each subsystem communicates with the Control Network via its own Optical Switch. The subsystem is capable of driving a number of Control Network I/F Modules and Bus Master Modules depending on the scale of the application.

In a redundant standby controller configuration one subsystem is in Control Mode while the other one is in Standby Mode. Each subsystem operates independently.

When the subsystem in Control Mode stops operating due to a self-detected fault, the subsystem in Standby Mode will automatically switch to the Control Mode, with no manual intervention. When in the Control Mode the subsystem takes over all control functions with no bump in the control process. The switchover is controlled by the System Management Modules. The subsystems can also be switched manually from the Status Display & Switch Module.

**b) I/O Chassis**

The redundant standby controller includes either redundant I/O and/or single I/O.

The single I/O consists of 2 Repeater Modules, a non-redundant I/O Bus and multiple I/O modules. Each I/O module communicates with the Bus Master Module for the subsystem in Control Mode. When the subsystems switch modes, communication with the I/O modules also switches. Process input signals and output signals are connected to the single I/O via the Distribution Module and Terminal Unit.

To enhance I/O reliability, a redundant standby controller can also be configured with redundant I/O. The redundant I/O consists of redundant I/O primary (P) and redundant I/O secondary (S). 2 I/O modules (primary and secondary) are utilized to interface with one field signal via the Distribution Module and Terminal Unit. However, like the subsystems, one I/O module is in Control Mode and the other is in Standby Mode. Only the I/O module in Control Mode generates output signals.

The subsystem in Control Mode decides which I/O module is in Control Mode based on communication self-diagnosis. Each I/O module communicates only with the subsystem in Control Mode via the I/O bus, Repeater Module, and Bus Master Module.

#### 4.1.1.2 Mode Management

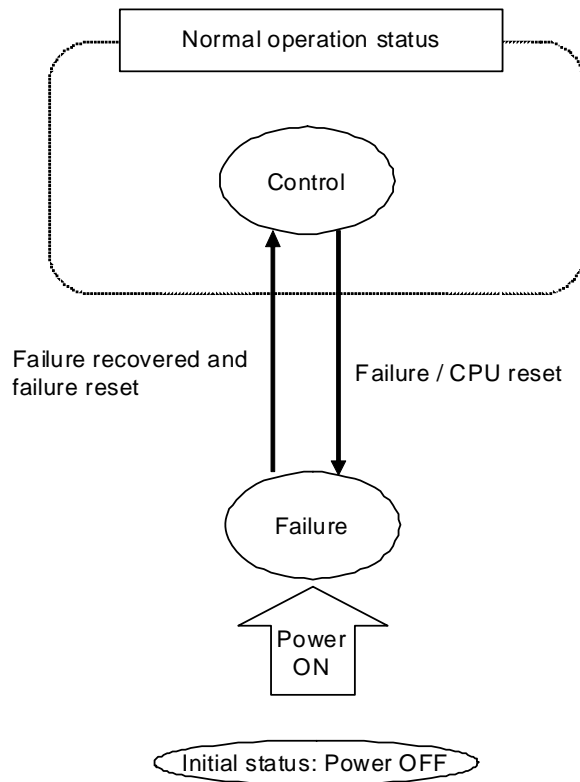
There are 2 types of mode management depending on the controller.

##### 4.1.1.2.1 Mode Management of Single Controller and Redundant Parallel Controller

In the single controller and the redundant parallel controller, there are 2 modes: Control Mode and Failure Mode.

The Mode Management of the subsystem in a single controller configuration is the same as the Mode Management of each subsystem in a redundant parallel controller configuration.

Mode Management of these controllers is shown in Figure 4.1.1-5.



**Figure 4.1.1-5 Mode Management of Single Controller and Redundant Parallel**

The subsystem has the following 2 modes.

**Control Mode:** A state in which the subsystem performs input, operation, output processing, and Self-diagnosis. When the subsystem detects its own failure (through self-diagnosis), it automatically changes from Control Mode to Failure Mode. A

---

failure signal, which can be used for external alarming, is generated for this transition.

**Failure Mode:** The subsystem initializes to Failure Mode after initial power activation. The subsystem also shifts to this mode automatically after it detects its own failure or there is a loss of power longer than 20 ms. A subsystem shifts from Failure Mode to Control Mode only when the Reset button on the Status Display Module is pushed.

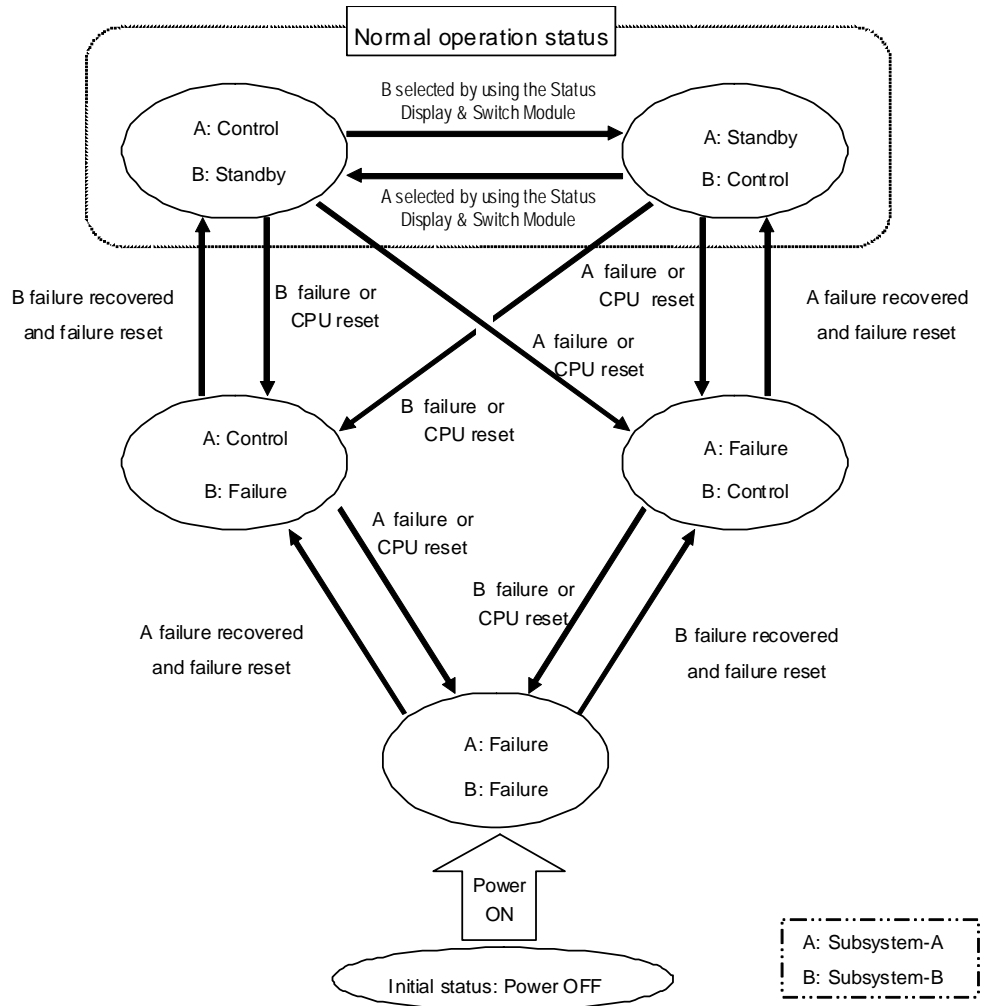
In the redundant parallel controller configuration, Subsystem-A and Subsystem-B operate independently with the Mode Management described above, including failure detection, loss of power detection, and manual reset.

Analog and digital outputs can be held in their preset initial mode, after the subsystem shifts to Control Mode, until the Output Start button on the Status Display Module is pushed. After pushing the output start button, output updating by the controller is enabled. For the redundant parallel controller configuration there are separate Output Start buttons for each controller. Pushing either button will enable output updating for the respective controller.

The output holding function can be disabled or enabled in the application program configuration. If this function is disabled, the outputs are enabled immediately after the subsystem shifts to the Control Mode, without the need for pushing the Output Start button. This function is enabled if it is required to confirm that the status of application software outputs matches the status of actual output devices before enabling output updating.

#### 4.1.1.2.2 Mode Management of Redundant Standby Controller

In a redundant standby controller, there are 3 modes: Control Mode, Standby Mode, and Failure Mode. The system transitions between these modes according to the events that occur. An example of the status transitions of a redundant standby controller configuration is shown in Figure 4.1.1-6.



**Figure 4.1.1-6 Mode Management of Redundant Standby Controller**

**Control Mode:** A state in which the subsystem performs input, operation, output processing, and Self-diagnosis. When the subsystem detects its own failure (through self-diagnosis), it automatically changes from Control Mode to Failure Mode.

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



---

**Failure Mode:** The subsystem is initialized to Failure Mode after initial power activation. The subsystem also shifts to this mode automatically after it detects its own failure. A subsystem shifts from Failure Mode to Control Mode or Standby Mode only when the Reset button on the Status Display & Switch Module is pushed. If there is no subsystem in Control Mode, the subsystem switches to Control Mode when the Reset button is pushed. If a subsystem is already in Control Mode, the subsystem switches to Standby Mode when the Reset button is pushed.

Analog and digital outputs can be held in their preset initial mode, after the subsystem shifts to Control Mode, until the Output Start button on the Status Display & Switch Module is pushed. After pushing the Output Start button, output updating by the controller is enabled. For the redundant standby controller configuration there is one common Output Start button. Pushing the button will enable output updating for the redundant standby controller.

The output holding function can be disabled or enabled in the application program configuration which is the same as the Mode Management of single and redundant parallel controllers described in Section 4.1.1.2.1.

#### 4.1.1.3 Scale and Capacity

The scale and capacity of the MELTAC platform controller is described in Table 4.1.1-1.

**Table 4.1.1-1 Scale and Capacity**

Item	Scale/Capacity
Input/Output	Maximum 3072 I/O modules per controller
Software	Cycle time: 20 ms to 1 s The value between 20 ms to 1 s is set in the application software F-ROM. This value is determined based on the application requirements. During the design phase, the system response time is determined through analysis, as described in Section 4.4. This analysis confirms the ability of the system to execute all functions within the allowed software cycle time. In the Integration Test phase, the system response time is confirmed by measurement.

**4.1.1.4 Environmental Specifications**

The MELTAC controller is designed to operate within the environmental conditions described in Table 4.1.1-2. Also see Section 5.

**Table 4.1.1-2 Environmental Specifications**

Item	Specifications	
Room Ambient temperature	Recommended	68 to 78.8 °F (20 to 26 °C) This temperature range is expected within a heated/air-conditioned instrumentation and control room of the nuclear power plant. The controller should be mounted in a cabinet with no more than 18 °F (10 °C) heat rise. Operating within this range will maximize the life of the equipment.
	Operation guarantee	32 to 122 °F (0 to 50 °C) The controller should be mounted in a cabinet with no more than 18 °F (10 °C) heat rise.
Relative humidity	10 to 95%Rh (No condensation)	
Withstand voltage	AC power input line	AC power input line: 5 MΩ or more (500 VDC megger) (input - ground, input - DC output) Analog I/O line: 5 MΩ or more (500 VDC megger) (I/O - ground, input - output) Digital I/O line: 5 MΩ or more (500 VDC megger) (I/O - ground, input - output) Applicable standard: JIS-C0704-1995 (IEC664/947)
	I/O line	Analog I/O line: 1 KV AC (1 minute) (I/O - ground, input - output) Digital I/O line: 2 KV AC (1 minute) (I/O - ground, input - output) Applicable standard: JIS-C0704-1995 (IEC664/947)
Electro-magnetic Compatibility (EMC)	Electromagnetic Interference (EMI)	Complies with MIL-STD-461E for emissions: 1. Conducted emissions Conducted emissions from the power line (field discharge) CE101: Low-frequency, 30 Hz to 10 kHz CE102: High-frequency, 10 kHz to 2 MHz 2. Radiated emission RE101: Magnetic field, 30 Hz to 100 kHz RE102: Electric field, 2 MHz to 10 GHz

Item	Specifications	
	Electromagnetic Susceptibility (EMS)	<p>Complies with MIL-STD-461E for susceptibility:</p> <ol style="list-style-type: none"> <li>Conducted susceptibility           <ul style="list-style-type: none"> <li>CS101: Low-frequency, 30 Hz to 150 kHz</li> <li>CS114: High-frequency, 10 kHz to 30 MHz</li> <li>CS115: bulk cable injection, impulse excitation</li> <li>CS116: damped sinusoidal transients, 10 kHz to 100 MHz</li> </ul> </li> <li>Radiated susceptibility           <ul style="list-style-type: none"> <li>RS103: Electric field, 30 MHz to 10 GHz</li> </ul> </li> <li>Surge to the power line           <ul style="list-style-type: none"> <li>IEEE Std. 472</li> <li>IEC61000-4:               <ul style="list-style-type: none"> <li>IEC61000-4-12: Ring wave</li> <li>IEC61000-4-5: Surge (Switching, lightning)</li> <li>IEC61000-4-4: Electrically Fast</li> </ul> </li> </ul> </li> </ol> <p>Transients/bursts</p> <ol style="list-style-type: none"> <li>Electrostatic noise resistance           <ul style="list-style-type: none"> <li>IEC61000-4-2-1999 Level 2</li> </ul> </li> <li>Lightning impulse resistance           <ul style="list-style-type: none"> <li>AC power source line: Applied voltage 4 kV, waveform 1.2/50 <math>\mu</math>s</li> <li>Digital I/O signal line: 4 kV, waveform 1.2/50 <math>\mu</math>s</li> <li>Applicable standard: JEC-210-1981 (Japanese Standard) Circuit category: 6</li> </ul> </li> </ol>
Seismic resistance	MELTAC Cabinet (at floor mounting)	Horizontal: 2.5 G (X- and Y-directions) Vertical: 1 G
	MELTAC modules (at chassis mounting)	Horizontal: 10 G (X- and Y-directions) Vertical: 2 G
Radiation resistance	Environment in which radiation is negligible.	
Dust	$1.87 \times 10^{-8}$ lb/ft <sup>3</sup> (0.3 mg/m <sup>3</sup> ) Reference standard: JEIDA-63-2000 Class B (Japanese Standard).	
Corrosive gas	Environment where no corrosive gas is detected.	

## 4.1.2 Hardware Descriptions

### 4.1.2.1 CPU Chassis

The modules that reside in the CPU Chassis are described in Table 4.1.2-1.

**Table 4.1.2-1 Module in the CPU Chassis**

	Name	Module Type	Function
Basic Function Module	CPU Module	PCPJ	<ul style="list-style-type: none"> <li>Executes basic software</li> <li>Executes application software, including control computation processing</li> </ul>
	System Management Module	PSMJ	<ul style="list-style-type: none"> <li>Communication between the redundant subsystems</li> <li>Communication with the MELTAC engineering tool.</li> <li>Auxiliary DI and DO functions</li> </ul>
Communication Module	Control Network I/F Module	PWNJ	Communication with the Control Network.
	Bus Master Module	PFBJ	<ul style="list-style-type: none"> <li>Communication with I/O</li> <li>Data Link communication with other controllers</li> </ul> This module has 4 communication channels.
Power Supply Module	CPU Power Supply Module	PPSJ	Supplies power to the modules within the CPU Chassis.
Display & Switch Module	Status Display & Switch Module	PPNJ	<ul style="list-style-type: none"> <li>Mode display LED</li> <li>Subsystem Mode switch</li> <li>Output Start button (described below)</li> </ul> This module is only used in the redundant standby controller configuration.
	Status Display Module		<ul style="list-style-type: none"> <li>Mode display LED</li> <li>Output Start button (described below)</li> </ul> This module is used for the single controller configuration or the redundant parallel controller configuration.

MELTAC has 2 types of CPU Chassis as shown in Table 4.1.2-2.

**Table 4.1.2-2 CPU Chassis**

Type	Use
Mirror-split CPU Chassis	- For redundant standby controller configuration
Non-split CPU Chassis	- For redundant standby controller configuration
	- For redundant parallel controller configuration
	- For single controller configuration

The CPU Chassis is selected from these 2 types to match the scale and configuration of the controller. For example, if each subsystem in redundant standby controller configuration has less than 5 modules, then a Mirror-split CPU Chassis is used. If each subsystem in redundant parallel controller configuration or single controller configuration has less than 5 modules, then a Non-split CPU Chassis is used. If each subsystem in redundant standby controller configuration or a redundant parallel controller configuration has more than 5 modules, 2 Non-split CPU Chassis are used. If the subsystem in single controller configuration has more than 5 modules, one Non-split CPU Chassis is used.

#### **4.1.2.1.1 CPU Module (PCPJ)**

The CPU Module utilizes a 32-bit microprocessor. This processor module is IEEE Std. 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 Read Only Memory) for storing both the basic software and the application software (such as function block interconnections, setpoints and constants). Specifications of the CPU Module are in Appendix A, Section A.1.

#### **4.1.2.1.2 System Management Module (PSMJ)**

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 4.1.1-3. In addition, this module has a 2-port memory Data Link for communicating operation data between the Standby Mode subsystem and the Control Mode subsystem.

Specifications of the System Management Module are in Appendix A, Section A.2.

#### **4.1.2.1.3 Bus Master Module (PFBJ)**

The Bus Master Module has 4 communication interface channels. Either of the following 2 functions can be defined for each channel.

- Communication with I/O modules  
This module is IEEE standard Futurebus+ compliant. It has a 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 modules, enabling control of a maximum of 384 I/O modules per Bus Master Module.
- Data Link communication  
This module implements serial Data Link communication between controllers in separate safety divisions. It has a 2-port memory to ensure that 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, Section A.3.

**4.1.2.1.4 Control Network I/F Module (PWNJ)**

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

The Control Network is redundant using optical fiber as the communication medium. An optical switch unit enables optical bypass for node maintenance. This module employs a 2-port memory to ensure that communication functions do not disrupt deterministic CPU Module operation.

The description of the Control Network, including the Control Network I/F Module is shown in Section 4.3.2.

Specifications of the Control Network I/F Module are in Appendix A, Section A.4.

**4.1.2.1.5 Status Display & Switch Module and Status Display Module (PPNJ)**

The Status Display & Switch Module and the Status Display Module are mounted in the CPU Chassis. The Status Display & Switch Module is used with the redundant standby controller configuration and the Status Display Module is used with the redundant parallel controller or single controller configurations. Both of these modules display the mode and alarms of the subsystem. The Status Display & Switch Module also provides a manual Mode Change Over Switch.

Specifications of the Status Display & Switch Module and Status Display Module are in Appendix A, Section A.14.



#### **4.1.2.2 I/O Modules**

The I/O modules in the MELTAC platform provide the input/output functions and the signal conditioner function, including signal conversion and noise reduction. The MELTAC platform includes several types of analog and digital modules to accommodate various input/output signal interfaces.

The I/O modules are mounted in dedicated I/O Chassis. One I/O Chassis can accommodate 16 modules. The modules mounted in the chassis are connected to the Bus Master Modules in the CPU Chassis via Repeater Modules that can shape and amplify data communication signals. Data transfer is achieved via the I/O bus.

There is 1 analog input or output per analog I/O module and there are 4 digital inputs or outputs per digital I/O module.

Dedicated I/O modules are applied for nuclear instrumentation (NI) and radiation monitoring (RM). These modules provide unique signal processing for neutron monitoring and RM detectors. These I/O modules are mounted in the dedicated chassis installed in the dedicated cabinets for NI and RM, respectively. NI and RM I/O modules are connected to MELTAC Bus Master Modules in the CPU Chassis, the same as described above.

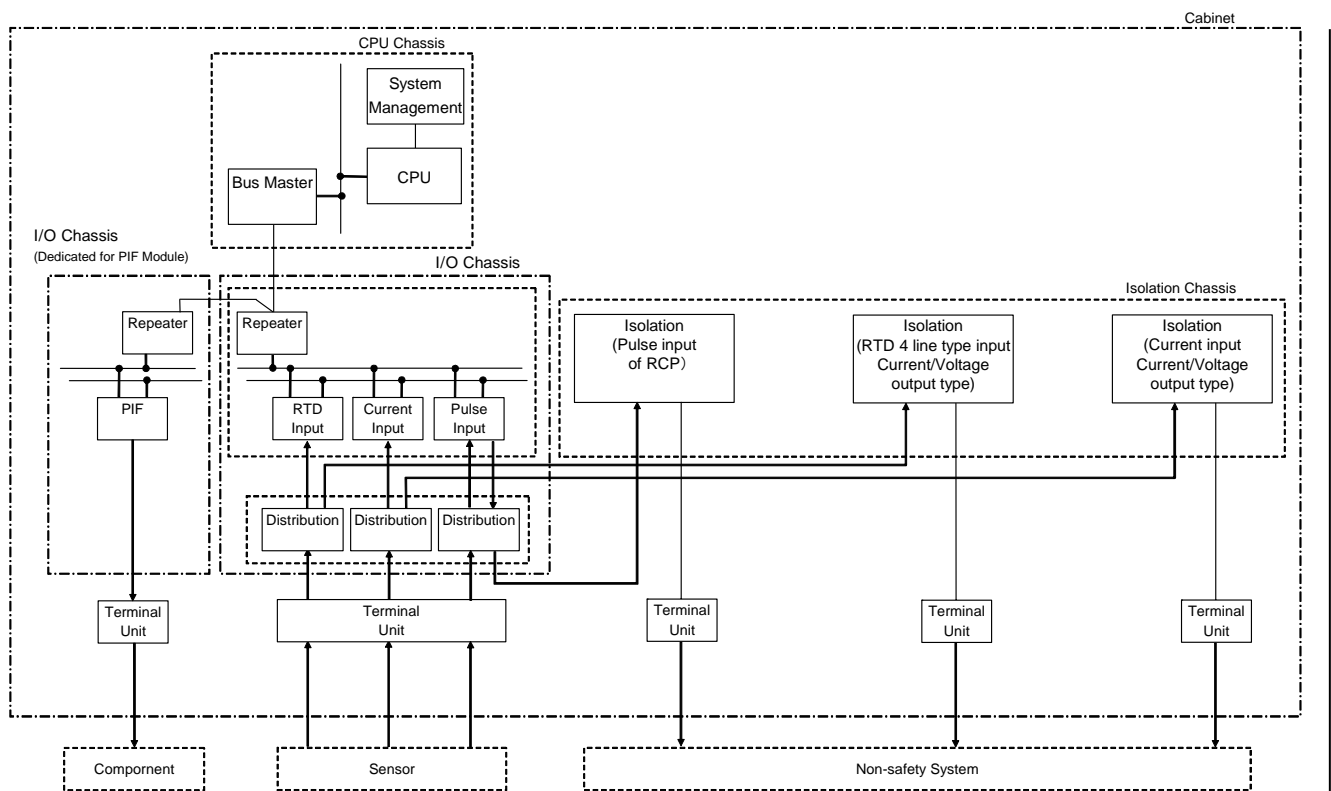
Specifications of I/O modules are in Appendix A, Section A.5, A.12 and A.13.

#### 4.1.2.3 Isolation Module and Distribution Module

Isolation Modules provide electrical isolation between equipment in different divisions or fire zones. Analog Isolation Modules receive current input signal, Resistance Temperature Detector (RTD) input signals, or pulse input signals and transmit corresponding analog output signals without any software processing.

Electrical isolation is provided between the input and output signals inside the Isolation Module. The Isolation Modules are mounted in dedicated Isolation Chassis. A single Isolation Chassis can accommodate 14 Isolation Modules. Analog Isolation Modules process 1 signal.

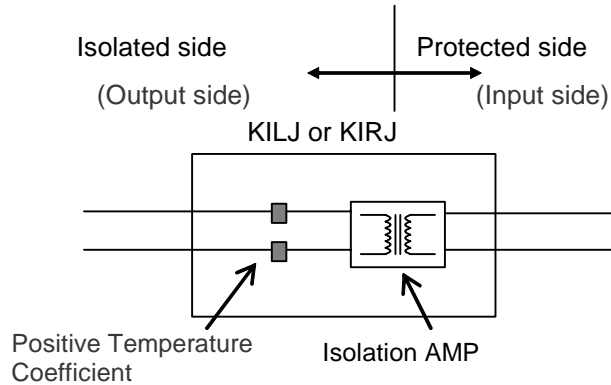
The location of Isolation Modules is shown in Figure 4.1.2-1.



**Figure 4.1.2-1 Location of Isolation Modules**

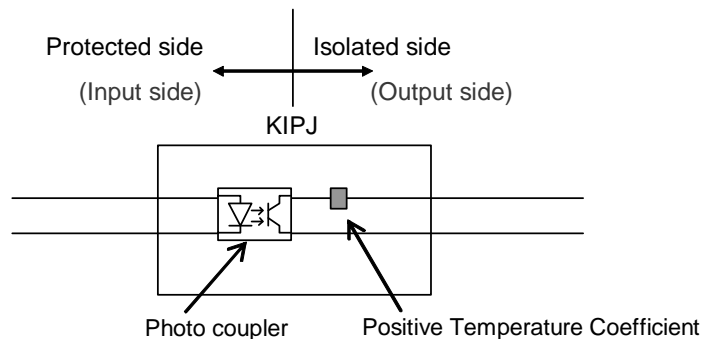
Specifications of Isolation Modules are in Appendix A, Section A.6.

Figure 4.1.2-2 shows the internal configuration diagram of the Analog Isolation Modules KILJ and KIRJ. For common mode faults, the input and output are electrically isolated by the isolation amplifier. The positive temperature coefficient device (e.g.: PolySwitch™) 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.



**Figure 4.1.2-2 The Internal Configuration Diagram of the Analog Isolation Modules**

Figure 4.1.2-3 shows the internal configuration diagram of pulse input Isolation Module KIPJ. The input and output are electrically isolated by a photo coupler. The positive temperature coefficient device (e.g.: PolySwitch™) is used to limit overcurrent.



**Figure 4.1.2-3 The Internal Configuration Diagram of the Pulse Input Isolation Module**

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 4.1.1-1, Figure 4.1.1-2, and inputs from sensors are input to the Distribution Module via the Terminal Unit. The Distribution Module distributes input signals to redundant I/O modules. Output signals are also output via the Distribution Module. The Distribution Module is used in accordance with the type of I/O modules. Appendix A.6 shows the list of I/O modules applicable to each Distribution Module.

#### 4.1.2.4 Power Interface Module

The Power Interface (PIF) Modules have the same I/O bus interfaces as with the I/O modules. 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.

The PIF Modules also receive inputs from external contacts (the status contacts of the components) and transmit component status signals to the subsystem. The PIF 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 (e.g.: switchgears, solenoid valves, etc.). Each PIF Module is configured with the appropriate IPL sub-board for the component being controlled. The IPL is realized by discrete logic Integrated Circuits.

[

]

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. New IPL sub-boards will maintain the same design process, qualification process, hardware technology and quality program as current IPL sub-boards.

The entire PIF Module, including the Communication Interface part is considered safety-related. Therefore, the life cycle process for the development and maintenance of the firmware within the Communication 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.

Unlike electro-mechanical relays, the power semiconductor output of the PIF Module does not degrade mechanically or electrically and can be treated the same as any other general semiconductor device. Thus, the PIF Modules have no known aging limitations in their expected service life. Therefore, the PIF Module is not included in the list of MELTAC platform components that have a limited service life as identified in Section 7.4 Periodic Replacement Equipment (Parts) to Keep Reliability.



**Figure 4.1.2-4 Sample Internal Configuration Diagram of the PIF Module**

Specifications of the PIF Module are in Appendix A, Section A.8.

#### **4.1.2.5 Electrical/Optical Converter Module**

Electrical/Optical (E/O) Converter Modules for Data Link communication convert electrical signals to optical signals or optical signals to electrical signals. They are mounted in dedicated E/O Chassis. Up to 14 modules can be installed per chassis, with 1 communication link per module.

The specifications for the E/O Converter Module are in Appendix A, Section A.7.

#### **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.

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 de-energized if there is a power loss to the fan. Therefore, fan failure can be detected.

##### **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 (described above) 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). It is equipped with a fan stop detection circuit (described above) which provides a contact signal to the System Management Module.

#### 4.1.2.8 Power Supply Module

The Power Supply Module convert the AC power supplied to the chassis to DC power voltages suitable for the individual modules and units. Redundant Power Supply Modules with power from 2 separate AC sources are typically provided.

There are 2 types of Power Supply Modules. The CPU Power Supply (PS and PPSJ) provides multiple outputs of +2.1 VDC and +5 VDC for the CPU Chassis. The I/O Power Supply (PS) provides +24 VDC for I/O modules, Isolation Modules, PIF Modules, E/O Converter Modules and Fan Units.

PPSJ's are mounted in the CPU Chassis. PS's are mounted outside of the chassis. PS's are mounted on the panel cut parts that are set right and left of the cabinet chassis as shown in Figure 4.1.2-5 and Figure 4.1.2-6. This mounting location was selected, rather than mounting them within the chassis for 3 reasons (1) this leaves space in the chassis for additional modules, (2) external mounting allows DC power to be supplied to the chassis from 2 redundant Power Supply Modules, and (3) this location keeps the heat from the power supplies away from the modules, thereby improving module reliability.

Both types of Power Supply Modules are equipped with overvoltage protection that de-energizes 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 shutdown 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 generates an "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.

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

#### 4.1.2.9 Controller Cabinet

##### a) Overview

The controller cabinet stores the following:

- CPU Chassis
- I/O Chassis
- E/O Chassis
- Isolation Chassis
- Power Interface Chassis
- CPU Power Supply Module
- I/O Power Supply Module
- CPU Fan
- Power Supply Fan
- Door Fan
- Terminal Unit
- Optical Switch

The inside layout of the cabinet is as follows:

- Each module can be changed from the front side of the cabinet and each status display can be monitored from the front side of the cabinet. Therefore, maintenance personnel can easily identify the status of the module and repair the module without pulling it out of the chassis.
- The modules within the I/O Chassis can be replaced at power. The modules in the CPU Chassis cannot be replaced at power. For redundant subsystem configurations power down of the CPU Chassis for module replacement has no effect on the system operation, since the other subsystem remains operable.
- Field cables enter through the rear side of the cabinet (through top and/or bottom entry) and are connected to the Terminal Unit.

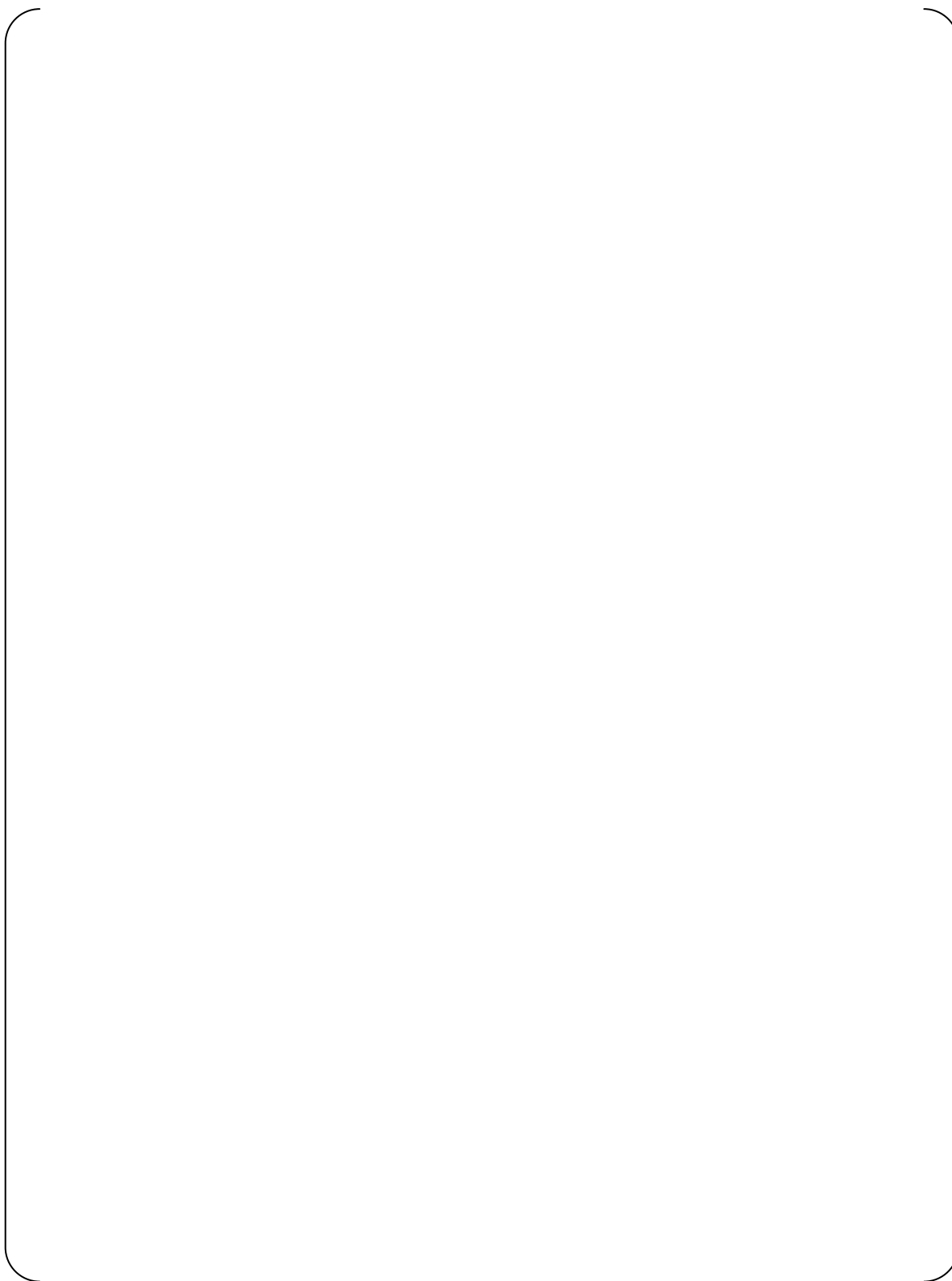
##### b) Controller Cabinet Specifications

The MELTAC cabinet is described in Table 4.1.2-3. Typical configurations of MELTAC cabinets are shown in Figure 4.1.2-5 and Figure 4.1.2-6.

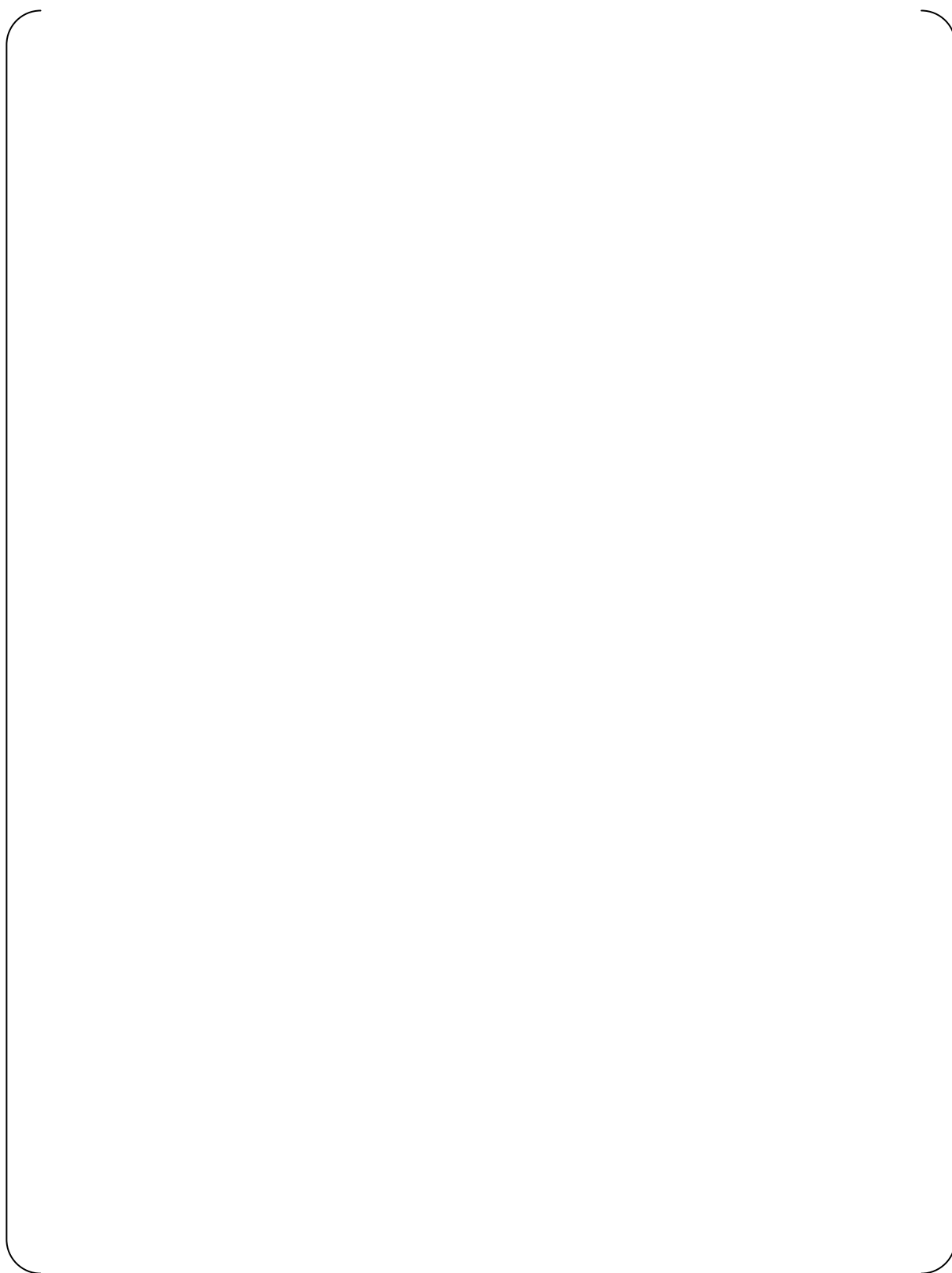
**Table 4.1.2-3 MELTAC Cabinet Specifications**

Item	Specifications
Typical External dimensions	2.62 (W) x 2.95 (D) X 7.55 (H) ft (800 (W) x 900 (D) x 2300 (H) mm) per cabinet
Weight	Approximately 1600 lb (750 kg) per cabinet including inside modules and units. Weight will vary with the number of chassis and modules.
Door specifications	Front and rear doors include handles, locks and seismic support bolts.
Cooling	The cabinet has forced air-cooling. An exhaust fan is mounted in the upper part of the cabinet's rear side. The doors are provided with filtered ventilation ports. Exhaust fans are mounted above each CPU Chassis and adjacent to I/O power supplies. The I/O Chassis are convection-cooled with no forced ventilation.





**Figure 4.1.2-5 Cabinet External Dimensions and Rack Up, Typical Sample A**



**Figure 4.1.2-6 Cabinet External Dimensions and Rack Up, Typical Sample B**

#### 4.1.2.10 Power Supply Configuration

Redundant AC power from 2 separate sources may be supplied to the MELTAC cabinet to avoid loss of function due to a single failure in the power supply or power source, as shown in Figure 4.1.2-7.

The source of AC power is described in system Application Licensing Document. The AC power is filtered and converted to DC voltage by the Power Supply Modules. DC power from both sources is diode auctioneered, then distributed to each component in the cabinet. For some components diode auctioneering is separate for each component.

[

]



**Figure 4.1.2-7 Configuration of Power Supply for Controller Cabinet**

#### 4.1.3 Software

The MELTAC platform consists of basic software and application software. Each software function is described below.

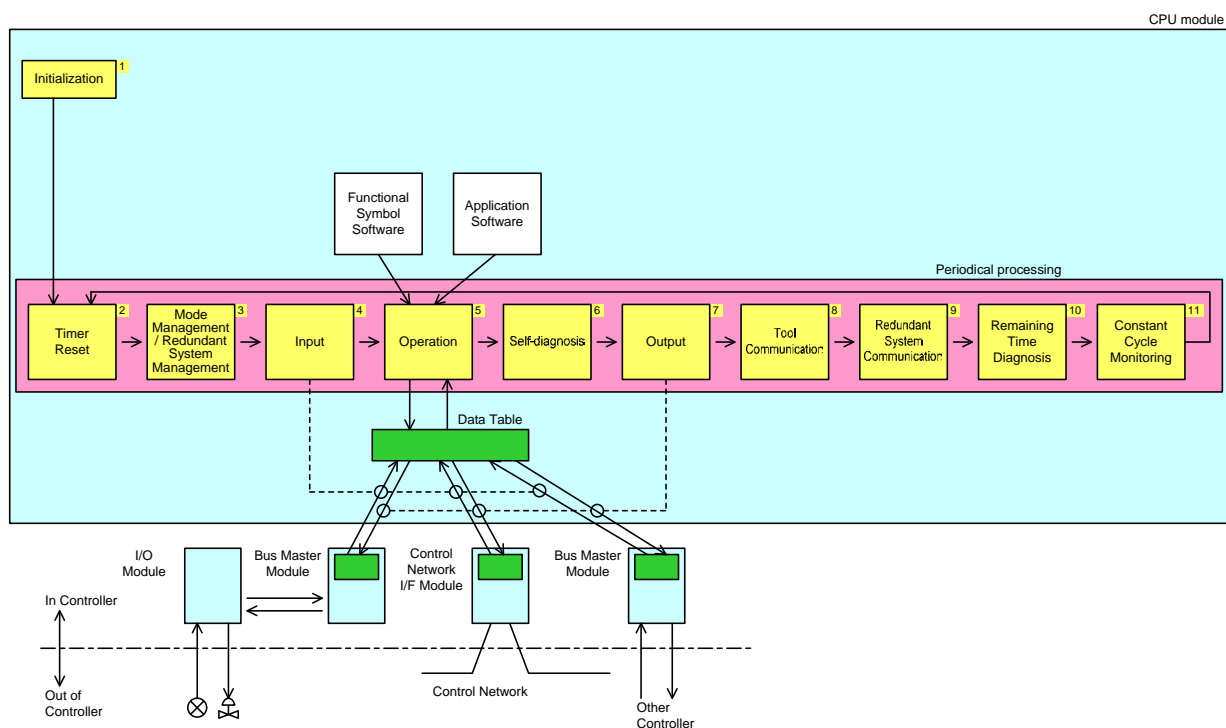
#### 4.1.3.1 Basic Software

In order to achieve deterministic processing, the basic software of the MELTAC platform adheres to the following design principles.

- a) There is only single task processing
- b) [

]

The processes within the basic software and the order of their execution are shown in Figure 4.1.3-1.



**Figure 4.1.3-1 Basic Software Processes and Execution Order**

The processing time from No.2 to No.8 is based on the application logic and the input/output signal quantity of each system. Since the controller operates cyclically, the processing time from No.2 to No.11 can be 100% of the application requirement (i.e.: there is no application margin required for the system). However, to allow future system expansion and to allow reasonable time for Remaining Time Diagnostics (discussed below), during the system design phase, the approximate processing time from No.2 to No.8 is calculated as described in Section 4.4. If the processing time exceeds about 80% of the processing cycle required for the system, the application is divided into 2 or more controllers, as necessary. In the test phase, the system response time is confirmed by measurement.

The processes of the MELTAC basic software are described below.

[

]



**Figure 4.1.3-2 Remaining Time Diagnosis**

[

]

#### 4.1.3.2 Application Software

The application software of the MELTAC platform is designed using the MELTAC engineering tool. Application software for functional algorithms is designed by combining simple graphical function blocks such as “And”, “Or”, and “Not” using the Graphical User Interface (GUI) of the MELTAC engineering tool. A GUI is used to reduce the potential for design errors in building or modifying the application software. It also makes it easier for the independent verifier to ensure that the application software Graphical Block Diagram (GBD)s, which are created by the I&C system designer are consistent with the Functional Block Diagram (FBD)s, which are created by the process system designer.

This GUI-based programming language used in both FBDs and GBDs is called POL (Problem Oriented Language). POL allows application software to be developed by graphically interconnecting conventional function blocks as noted above.

Using the MELTAC engineering tool, the application software GBD is automatically converted into execution data that is executed directly by the Operation process of the basic software. The Operation process of the basic software executes the Functional Symbol Software sequentially according to the execution data.

Application software execution data is stored in the F-ROM of the CPU Module.

[

]

The POL Functional Symbols are listed in Appendix B.



#### **4.1.4 MELTAC Engineering Tool**

The MELTAC engineering tool provides various functions aimed at steadier and more efficient software management during all system life cycle phases (including design, fabrication, test, adjustment and maintenance).

The MELTAC engineering tool is used to generate safety application software for the MELTAC controller, but the tool itself is non-safety software running on a non-safety personal computer (PC) using the Microsoft Windows Operating System. The MELTAC engineering tool was developed in accordance with the MELCO QAP for non-safety items. Safety application software generated by the MELTAC engineering tool must be qualified by independent V&V. Access is controlled by means of the PC password (BIOS, OS) and the MELTAC engineering tool password.

The application software execution data generated by the MELTAC engineering tool is downloaded to the controller via the Maintenance Network and is stored in the F-ROM of the CPU Module. The functions of the MELTAC engineering tool are described as follows.

##### **4.1.4.1 Function Description**

###### **a) Creation of Application Software**

FBDs that are created with a commercial Mitsubishi CAD software package called "RAPID" can be automatically converted to GBDs by the MELTAC engineering tool. (Access to RAPID is also controlled by a password.)

The MELTAC engineering tool is then used to automatically generate (compile) the application software execution data directly from the GBD.

This automated process eliminates human translation errors.

GBDs can also be manually created (drawn), based on legacy FBDs provided by the customer, using the MELTAC engineering tool's GUI editor.

Regardless of how the GBD is generated (automatically from RAPID or manually drawn with the MELTAC engineering tool's GUI editor), the assignment of GBDs to controllers and the assignment of I/O signals is manually configured using the MELTAC engineering tool.

GBDs (whether created automatically or manually) and the executable data output from the MELTAC engineering tool are confirmed through manual V&V activities.

###### **b) Download**

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

]

---

The correct download is confirmed by a different MELTAC engineering tool function that checks the F-ROM data as discussed below.

**c) Verifying F-ROM data**

The MELTAC engineering tool provides a manually initiated function which automatically compares the basic software and application software data in the F-ROM of the controller, bit by bit, with the basic software data and application software data stored in the MELTAC engineering tool. This function is used after a new download and during periodic surveillance tests to confirm that the data in F-ROMs is the same as the data in the MELTAC engineering tool, and therefore has not changed.

**d) Controller failure diagnosis display**

The MELTAC engineering tool displays the self-diagnosis result of the controllers. It shows which module is in a failed state.

**e) Temporary changes to field changeable process value in data table (Data Set)**

[

]

#### 4.1.4.2 Network for the MELTAC Engineering Tool

In order to communicate between the MELTAC engineering tool and the controller, the Maintenance Network is used. The MELTAC engineering tool, which runs on a PC, is temporarily connected via the Maintenance Network to the System Management Modules of each controller in the division. This interface allows all functions described in Section 4.1.4.1. The Maintenance Network is temporarily connected to the controllers in the same safety division. There is a separate Maintenance Network for each division. There are no Maintenance Network interconnections between safety divisions. There is also a separate MELTAC engineering tool for each division. The specification of the Maintenance Network is described below.

For the configuration and the isolation of the Maintenance Network, see Section 4.3.4.

(Specification)

Function: Transmission of maintenance data for MELTAC engineering tools

- Transmission protocol: Ethernet (IEEE Std. 802.3; CSMA / CD, UDP/IP)
- Transmission speed: 100 Mbps/10 Mbps
- Communication form: Dialog communication
- Connection form: Bus/Star-type

Transmission media: UTP Category 5 cable  
Optical fiber (Multi mode)

[

]

### **4.1.5 Self-Diagnosis**

The MELTAC platform controller is equipped with 3 types of self-diagnosis features: a hardware based detection process, a software based detection process, and a combination thereof. When an error is detected, an alarm is generated. When the error is severe, the controller makes a transition from the Control or Standby Mode to the Failure Mode.

Detailed error descriptions are provided in Sections 4.1.5.2 through 4.1.5.6. The categorization of each error is shown in parenthesis, for example "Clock check (Failure)".

All errors in Sections 4.1.5.2 and 4.1.5.3 are severe and categorized as "Failure". These errors stop the main CPU operation, and generate signals that can be used for alarms. All other errors (those identified in Sections 4.1.5.4 and 4.1.5.5) generate signals that can be used for alarms, but do not stop the main CPU operation. All error signals are identified on the MELTAC engineering tool. The specific grouping of error signals into operator alarms is application specific. Since most applications have redundant CPUs, typically all error signals are grouped to a single operator alarm and then the MELTAC engineering tool is used for diagnosis of specific error conditions.

Failure notice may be provided to the plant monitoring system for the 3 types of errors, "Failure", "Alarm", and "I/O Alarm". These error signals are typically grouped into system trouble alarms, however the method used to present this information to the operator from the plant monitoring system is application dependent and not within the scope of the MELTAC platform.

Detailed information for diagnosis of all error conditions is provided on the MELTAC engineering tool.

#### **a) Hardware based detection process**

With this feature, self-diagnosis is implemented by special diagnostic circuitry on the CPU Module. The feature involves a WDT, parity error, timeout, analog input check, etc.

#### **b) Software based detection process**

With this feature, self-diagnosis is implemented using software. The feature involves CPU health check, F-ROM check, RAM check, etc.

#### **c) Software/hardware combination**

With this feature, circuitry that supports self-diagnosis is added to the controller and self-diagnosis is performed using software-based read/write operations. This feature involves a digital input check, digital/analog output read-back check, etc.

The controller is monitored based on the above self-diagnosis processes at every execution cycle. The individual error items can be identified by viewing the LED display on the front of each module and the representative alarm display (Failure, Alarm, I/O Alarm) on the Status Display & Switch Module and by using the MELTAC engineering tool connected via the Maintenance Network.

Each detected error is categorized into 3 types (Failure, Alarm and I/O Alarm) as below.

**1) Failure**

Fatal abnormalities by which the subsystem cannot continue its functions are categorized as Failure.

When the subsystem detects this type of error, it transitions to the Failure Mode.

[

]

In the Failure Mode, the processing of input/output and operation are stopped, although the process of sending status data related to the Failure Mode is continued.

[

]

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

When there is no subsystem which communicates with the controller's Output Module, the Output Module transitions to the Failure Mode which is "as-is mode" or "off mode". This mode is preset at the application level.

**2) Alarm**

Minor abnormalities with which the subsystem can continue its functions are categorized as Alarm.

When the subsystem detects this type of error, it does not change its mode and only warns of the alarm. This abnormality is communicated to other systems for alarming via Data Link or Control Network, as configured at the application level.

**3) I/O Alarm**

Abnormalities of I/O are categorized as I/O Alarm.

When the subsystem detects this type of error, it does not change its mode and only warns of the alarm. This abnormality is communicated to other systems for alarming via Data Link or Control Network, as configured at the application level.

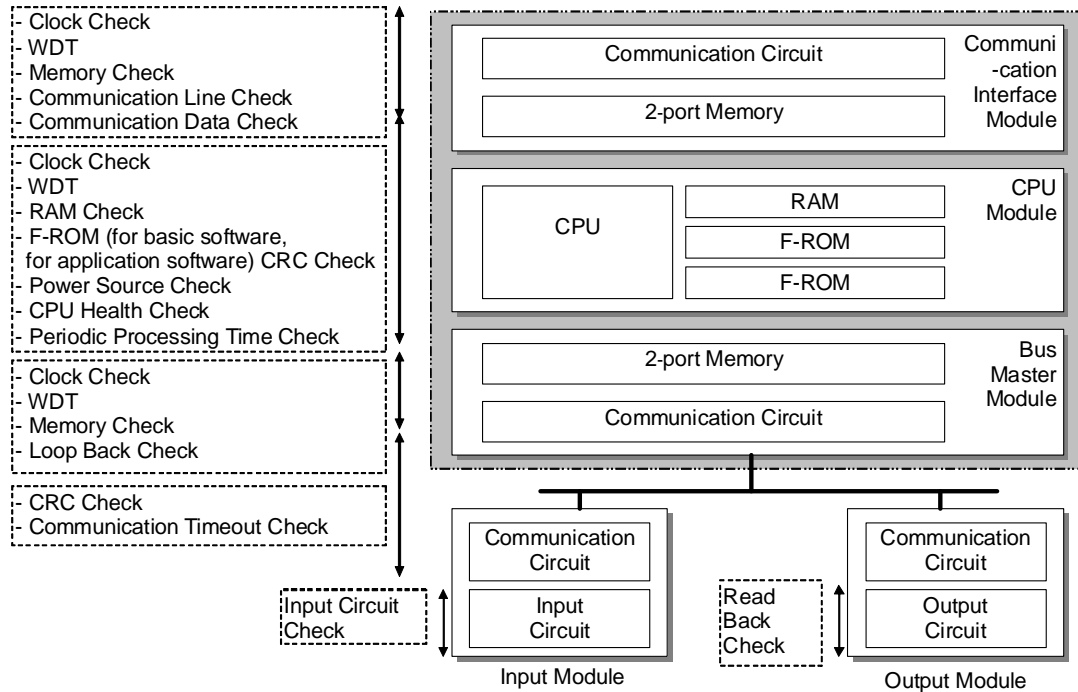
In the case of redundant standby controller configuration, when the I/O Alarm occurs in the Redundant I/O in the Control Mode, the subsystem stops to use this I/O, switches the other I/O from the Standby Mode to the Control Mode, and continues the processing of input/output.

When the I/O Alarm occurs in the Single Input Module, the last good input values are retained and the application software is informed of the abnormal state of the input signals. For digital inputs, the input values are kept at the last value (1 or 0) before the error occurred. For analog inputs, the input values are kept at the last engineering value before the error occurred.

Based on the error flag, the application software can be programmed for a predetermined control action.

#### 4.1.5.1 Coverage of Self-Diagnosis

The controller's self-diagnosis coverage is shown in Figure 4.1.5-1.



**Figure 4.1.5-1 Coverage of Self-Diagnosis Function of the Controller**

#### 4.1.5.2 Self-Diagnosis of the Controller

The self-diagnosis of the processor modules is described below.

Each diagnosis item is shown with the timing of diagnosis classified as follows:

- Initialization: At the time of initialization
- Self-diagnosis: Once per cycle in the constant cycle operation
- Remaining Time Diagnosis: Periodically in the remaining time of constant cycle operation, but not every cycle.
- Constant: On a constant basis by hardware

##### 4.1.5.2.1 CPU Module

[

]

[

]

#### **4.1.5.2.2 Bus Master Module**

[



]

#### **4.1.5.2.3 Control Network I/F Module**

[

]

**4.1.5.3 Self-Diagnosis of Power Supply Modules in the CPU Chassis**

[

]

**4.1.5.4 Self-Diagnosis of the Communication System**

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

**4.1.5.5 Self-Diagnosis of I/O Modules**

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

**4.1.5.5.1 Input Module**

[

]

#### **4.1.5.5.2 Output Module**

[

]

#### **4.1.5.5.3 Controller Cabinet**

[

]

**4.1.5.6 Operations When the Hardware and Software Do Not Match**

Mismatch of the module configuration in the CPU Chassis:

The CPU Module detects the error and the subsystem switches to Failure Mode.

Mismatch of the module configuration in the I/O Chassis:

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

#### 4.1.5.7 Watchdog Timer (WDT)

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

]

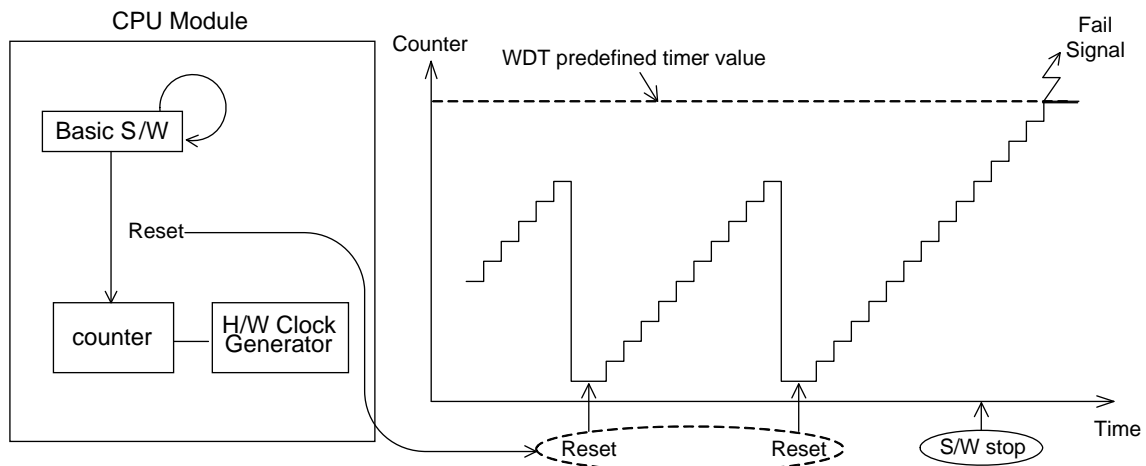
##### 4.1.5.7.1 Architecture of the WDT

The following describes the detailed WDT mechanism. Figure 4.1.5-2 shows the WDT mechanism, taking the CPU Module as an example. The left-side of the figure represents the elements related to the WDT in the CPU Module. The right-side of the figure shows the WDT behavior, regarding count-up, counter reset, and timeout when the counter value reaches a predefined value.

The flow of the WDT operations and controls is as follows:

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

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



**Figure 4.1.5-2 WDT Mechanism (CPU Module)**

**4.1.5.7.2 WDT Timeout Process (per Module)**

[

]



**Figure 4.1.5-3 WDTs Mounted in MELTAC Platform**





[illegible]

[illegible]

#### 4.1.6 Bus Inside the Controller

Table 4.1.6-1 shows the busses used inside the controller. Table 4.1.6-2 shows the I/O bus specification.

**Table 4.1.6-1 Bus Inside the Controller**

Item	Application
Futurebus+	Backplane bus in the CPU Chassis. It is used to connect modules in CPU Chassis and transfers other module data in the CPU Chassis.
I/O bus	A bus that connects the CPU Chassis and the I/O module. See Table 4.1.6-2 for details.

**Table 4.1.6-2 I/O Bus Specification**

Item	Specification
Protocol	1:N master polling
Configuration	Maximum 96 I/O modules can be connected to 1 I/O bus. (Up to 16 I/O modules can be mounted on 1 I/O Chassis and up to 6 Chassis can be connected to 1 I/O bus.). There are 4 I/O busses on each Bus Master Module and each controller can have 8 Bus Master Modules.
Interface	RS-485 transformer isolation.
Baud rate	1Mbps
Error detection method	CRC check
Operation	The Bus Master Module and the I/O modules are connected to the I/O bus. The Bus Master Module sends output data and input data requests to the I/O module, and the I/O module responds to that. This communication method is common to all I/O modules, including the PIF Module.

#### 4.1.7 Manual Test

Manual test refers to conducting periodic surveillance testing of all functions that are not automatically tested through self-diagnosis, and conforming to the guidelines of BTP 7-17 "Surveillance Testing".

(1) Input and Output Function

The integrity of the input and output function of the I/O module hardware circuits is confirmed during periodic testing. The integrity can be tested by the method described in Section 4.1.7.1.

(2) Memory

The memory integrity is checked during periodic testing. The integrity can be tested by the method described in Section 4.1.7.2.

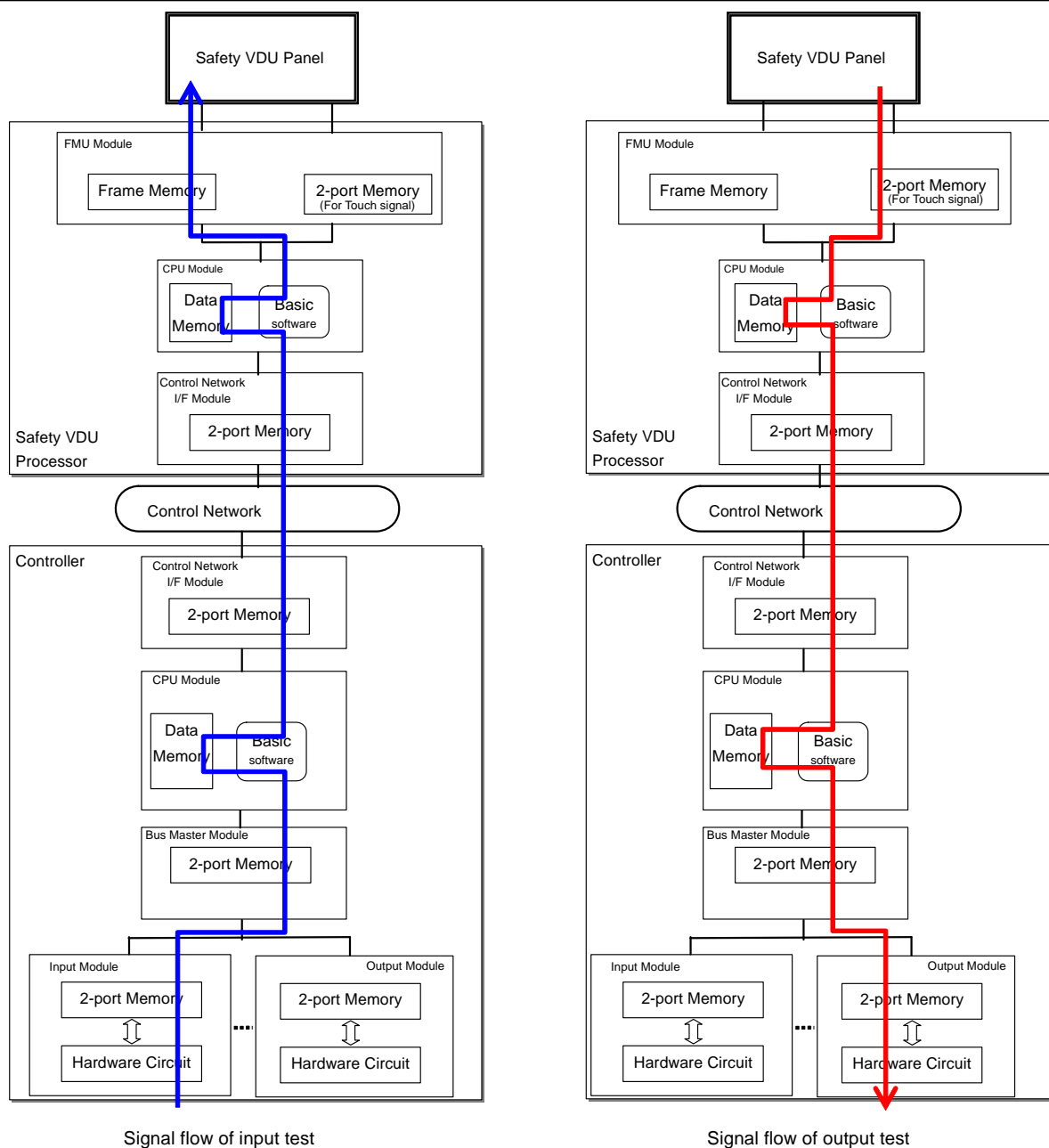
(3) Safety VDU Panel

The consistency between the actual screen display and the coordinates of the S-VDU panel is confirmed during periodic testing. The consistency can be tested by the method described in Section 4.2.4.

#### **4.1.7.1 Process Input and Output**

Figure 4.1.7-1 shows the signal flow of manual test for process input and output. The input function is tested by manipulating the process to stimulate a state change. Correct functionality is confirmed by monitoring the state of signals on the safety VDU. The output function is tested by operation from the safety VDU.

It is noted that these tests are intended to confirm functionality of the system's process input and output signal paths, since these cannot be fully tested by self-diagnosis. Therefore, the process input and output tests can be conducted using the safety VDU that obtains its data from the Control Network. A separate manual test for the safety VDU is described in Section 4.2.4.



**Figure 4.1.7-1 Manual Test for Process Input and Output**

#### 4.1.7.2 Memory Integrity Check

The MELTAC engineering tool includes a manually initiated Memory Integrity Check (MIC) function which compares the software memory in the controller, bit by bit, with a controlled copy of the software stored off-line in the MELTAC engineering tool.

This function is used to provide confirmation that the software in the controller is the same as the off-line version, and therefore has not changed or failed. This test confirms the functional integrity of both the basic software and application software residing in the controller. The MIC is conducted periodically for every controller in the system.

By confirming the basic software, the MIC confirms the CPU instructions stored in F-ROM for all MELTAC functions described throughout this document, including the self-diagnosis functions. By confirming the application software, the MIC also confirms the CPU instructions stored in F-ROM for all functional logic required for the safety functions of the application.

The following table summarizes the differences between the MIC which is conducted periodically, and Self-diagnosis Memory Check (SMC) (see Section 4.1.5.2.1) which is conducted continuously on-line, including the effectiveness of these 2 functions.

[

]

Table 4.1.7-1 MIC vs. SMC


[

]

The versions of the application software and the basic software are controlled through software configuration management. The application software is described in the Application Licensing Document. The basic software is controlled and maintained in accordance with the App.B-based QAP and “MELTAC Platform Software Program Manual” (JEXU-1041-1016).

The following table summarizes the software differences that can be detected by the MIC and SMC.



Table 4.1.7-2 Detectable Errors by the MIC and SMC



[

]

The periodic manual tests (the process input and output test, and the safety VDU test) ensure that the CPU is capable of executing instructions from both F-ROM for basic software and F-ROM for application software. This encompasses the instructions that control continuous self-diagnosis, and the instructions that control the safety functions of monitoring process

---

measurements and actuating plant components. Therefore, through the aggregate of periodic manual tests and continuous self-diagnosis tests, the complete functionality of the safety system is confirmed.

#### **4.1.8 Defense-in-Depth and Diversity (DAS) Interface**

Nuclear power plants that implement digital platforms (e.g.: the MELTAC platform) in plant safety systems may be required to implement a Diverse Actuation System (DAS). The DAS is typically a non-safety system consisting of conventional equipment that is totally diverse and independent from the MELTAC platform. The DAS would provide monitoring and control of safety-related and non-safety plant systems to cope with abnormal plant conditions concurrent with a CCF that disables all functions of the plant safety systems.

Sensors would typically be interfaced from within the MELTAC Distribution Modules. These Distribution Modules would utilize Isolation Modules to connect the input signals to the DAS prior to any digital processing. Therefore, a software CCF within the plant safety system will not affect the DAS function.

The DAS typically controls selected plant components independent of the output from the plant safety system. Outputs from the DAS are typically interfaced to plant components via MELTAC platform PIF Modules. The PIF Modules combine the signals received from the DAS with signals received from the plant safety system (MELTAC controllers) to generate a single power interface to the plant component. The DAS output to the PIF Modules is typically isolated to prevent propagation of DAS faults to the plant safety systems. The combination logic and power interface within these PIF Modules is simple and fully testable so any additional potential for CCF that may be introduced is negligible. The PIF Module design and examples of typical plant safety system and DAS inputs is provided in Section 4.1.2.4.

## **4.2 Safety VDU Panel and Processor**

The MELTAC platform includes a safety VDU which consists of a safety VDU panel, and a safety VDU processor. There is one safety VDU processor for each safety VDU panel.

The number of safety VDUs is defined by specific plant design. Each safety VDU can be configured to provide the HSI for only one safety division.

### **4.2.1 Hardware**

The CPU Chassis, Control Network Optical Switch, fans, cabinet power supplies and the cabinet are the same as previously described in Sections 4.1.2.1, 4.1.2.6, 4.1.2.7, 4.1.2.8 and 4.1.2.9, respectively. Unique components of the Safety HSI are described below.

All unique components of the safety VDU panel and safety VDU processor comply with the same environmental specifications and are qualified to the same levels as described for the MELTAC controller in Section 4.1.1.4.

#### **4.2.1.1 Safety VDU Panel**

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

- Display function:  
Displays operational screens by receiving RGB analog video signals from the safety VDU processor.
- Control function:  
Inputs by operator on the touch screen are transmitted to the safety VDU processor in the form of x-y coordinate data using an RS-232C data link.

Specifications of the safety VDU panel are in Appendix A.10.

#### **4.2.1.2 Safety VDU Processor**

##### **4.2.1.2.1 Configuration of the Safety VDU Processor**

The safety VDU processor has a single subsystem architecture as shown in Figure 4.2-1. Except for the Frame Memory Unit (FMU) Module, the hardware modules are the same as those of the MELTAC platform. The software structure is based on the same design as that of the MELTAC basic software.

##### **a) Information Display Function**

The safety VDU processor stores the static data for each pre-configured display screen. The safety VDU processor gathers live plant data from safety controllers via the Control Network. The safety VDU processor organizes the static data of the pre-configured screen with the live plant data and then displays those combined images on the safety VDU panel by means of the RGB interface. The RGB interface is generated by the FMU Module.

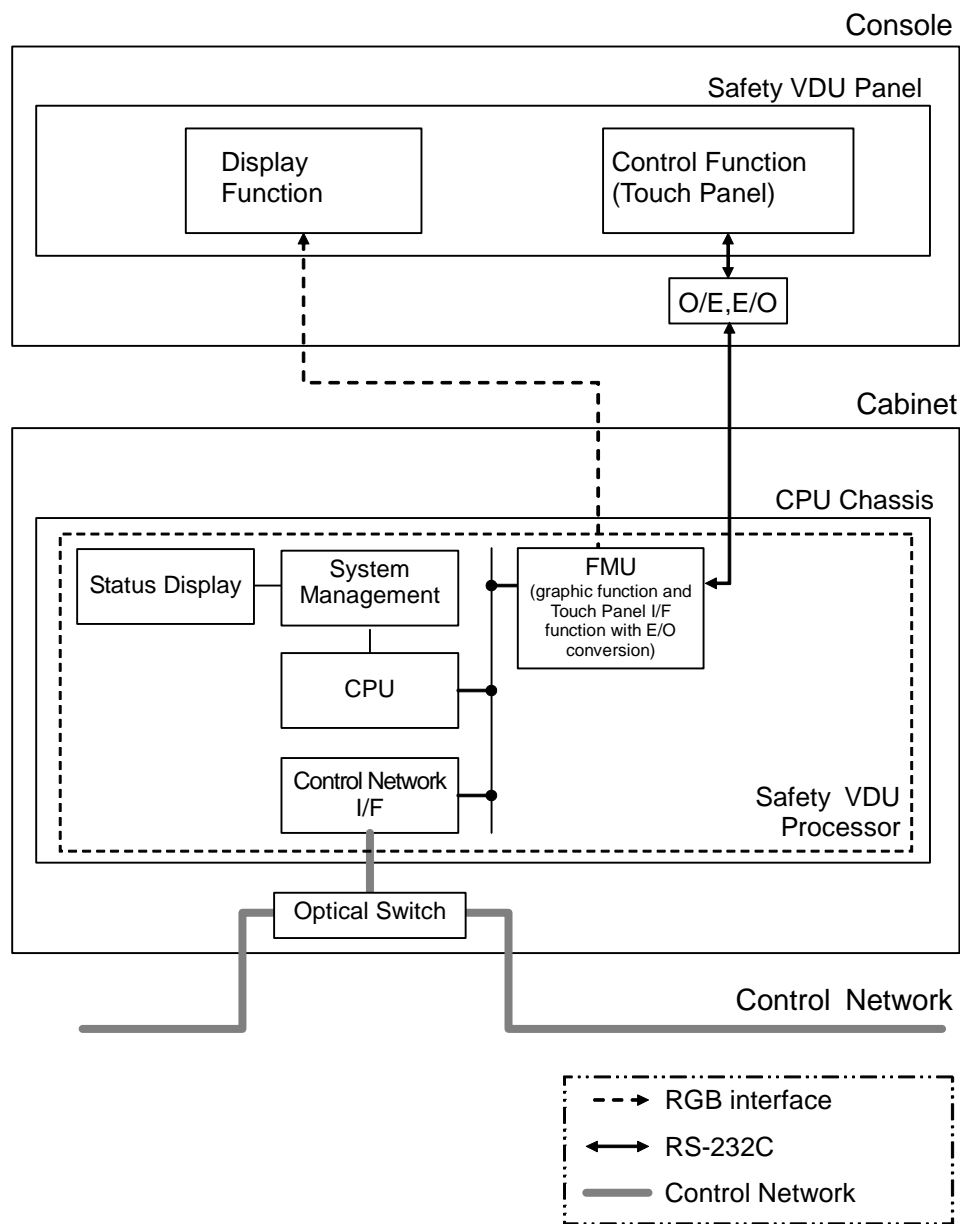
##### **b) Control Function**

Operators take manual control actions by touching an operation switch image displayed on the safety VDU panel. A sample picture of the operation switch image is shown in Figure 4.2-5. The results of a touch screen operation are sent in the form of x-y coordinate data from the safety VDU panel to the safety VDU processor via the FMU Module. This is an RS-232C Data Link, which is converted from electrical to optical, to increase the transmission distance. The safety VDU processor converts the x-y coordinate data received from the safety VDU panel to plant control data (i.e.: component ID and operational command), and then sends the data to the controllers via the Control Network.

##### **c) Control Network Interface**

The Control Network interface receives live plant data from the controllers, and sends the plant control data to the controllers via the Control Network.

The Control Network and safety VDU are both intra-divisional.



**Figure 4.2-1 Configuration of Safety VDU Processor**

#### 4.2.1.2.2 Module Specifications of Safety VDU Processor

The safety VDU processor is comprised of the following modules:

- CPU Module
- System Management Module
- Control Network I/F Module
- Frame Memory Unit (FMU) Module
- Status Display Module

The FMU Module is specific to the safety VDU processor. The other modules are the same hardware as the modules of the controller. The following sections describe the modules that are specific to the safety VDU processor.

##### a) FMU Module

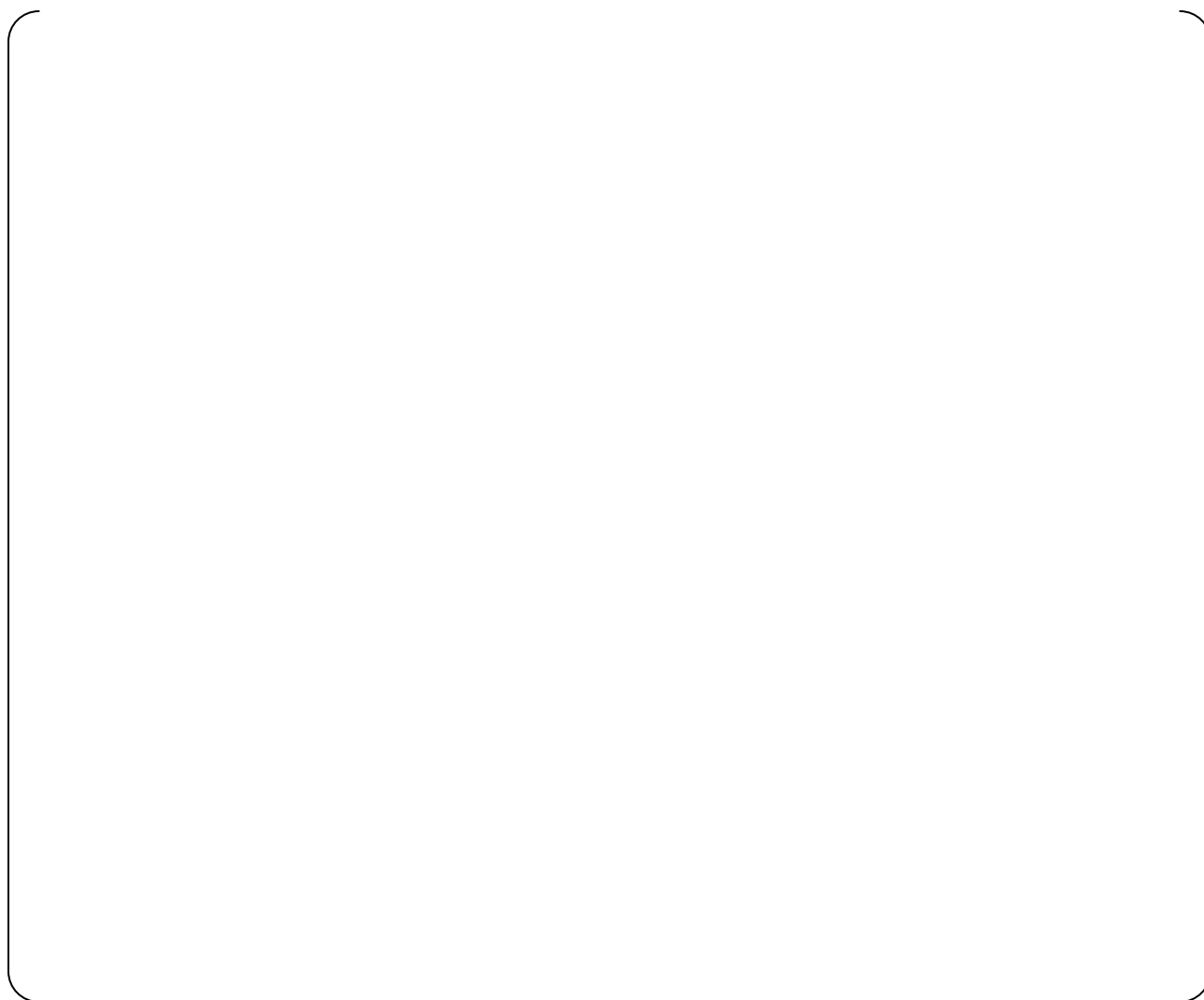
The FMU Module provides the analog RGB signal for the graphic images to the safety VDU panel. The FMU Module also provides the RS-232C touch panel interface signal from the safety VDU panel to the safety VDU processor. The FMU Module communicates with the CPU Module inside the chassis by means of the Futurebus+ backplane.

Specifications of the FMU Module are in Appendix A.11.

#### 4.2.1.3 Power Supply

AC power can be supplied to the safety VDU with a single power supply configuration or a redundant configuration. The redundant configuration avoids loss of function due to a single failure in the power supply or the AC power source, as shown in Figure 4.2-2.

The AC power is converted to DC voltage by the Power Supply Modules. The power supplies for the safety VDU are the same as for the controller CPU Chassis. The power supplies for the safety VDU panel are unique to accommodate mounting within typical main control boards or operator consoles. For a redundant power supply configuration, the DC power from both sources is diode auctioneered for each component of the safety VDU.



**Figure 4.2-2 Configuration of Power Supply for Safety VDU**

#### **4.2.1.4 Safety VDU Panel Optical to Electrical Converter Modules**

Electrical/Optical (E/O) Converter Modules for the safety VDU panel convert the operator touch signals to optical signals. Specifications of the E/O Converter Module is in Appendix A.7

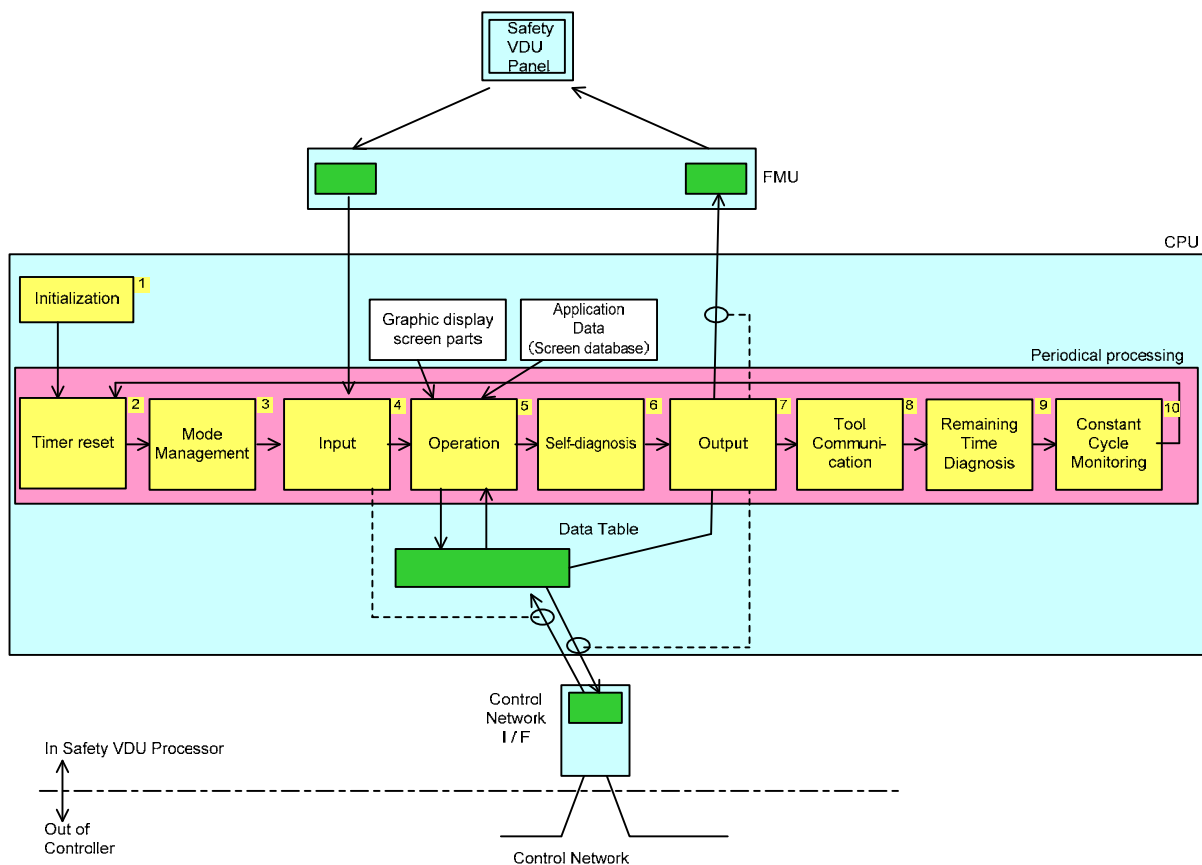
### 4.2.2 Software

The safety VDU processor software consists of basic software and application software. Each software function is described below.

#### 4.2.2.1 Basic Software

The safety VDU basic software is designed to the same safety critical software integrity level as all other MELTAC basic software.

The safety VDU processor software structure is shown in Figure 4.2-3 . The software structure ensures reliable deterministic operation and is based on the same design as that of the controller basic software. With fixed cycle control and no external interrupts (except processing of self-diagnosis errors detected by the hardware within the CPU Module and the Power Supply Module and categorized as “Failure” (see Section 4.1.5)), the basic software provides high reliability, and deterministic processing.



**Figure 4.2-3 Software Structure of Safety VDU Processor**



Details of the processing executed in each process are described below.

[

]

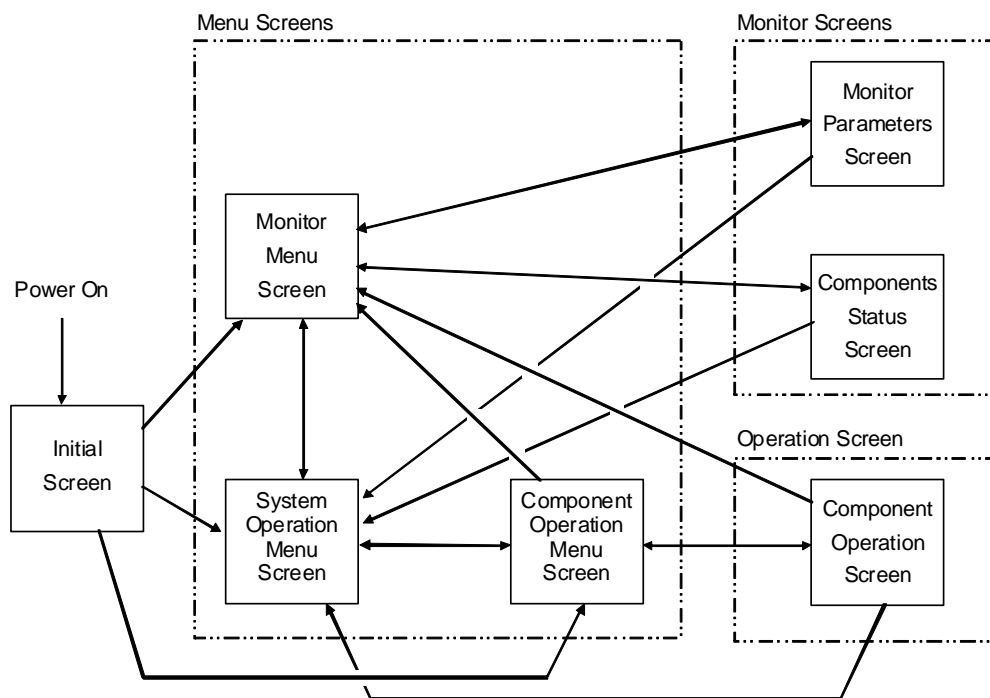
#### 4.2.2.1.1 Screen Selection on the Safety VDU Processor

One operation within basic software process No.5 is Screen Selection. Screen Selection is described in this section.

Figure 4.2-4 shows the types of screens displayed by the safety VDU processor and the available screen transitions. The Initial Screen is the screen shown-after the power is turned on. The types of information displayed on the Menu Screen, the Monitor Screen, and Operation Screen are shown in Table 4.2-1. The actual information displayed on these screens is configured uniquely for each application.

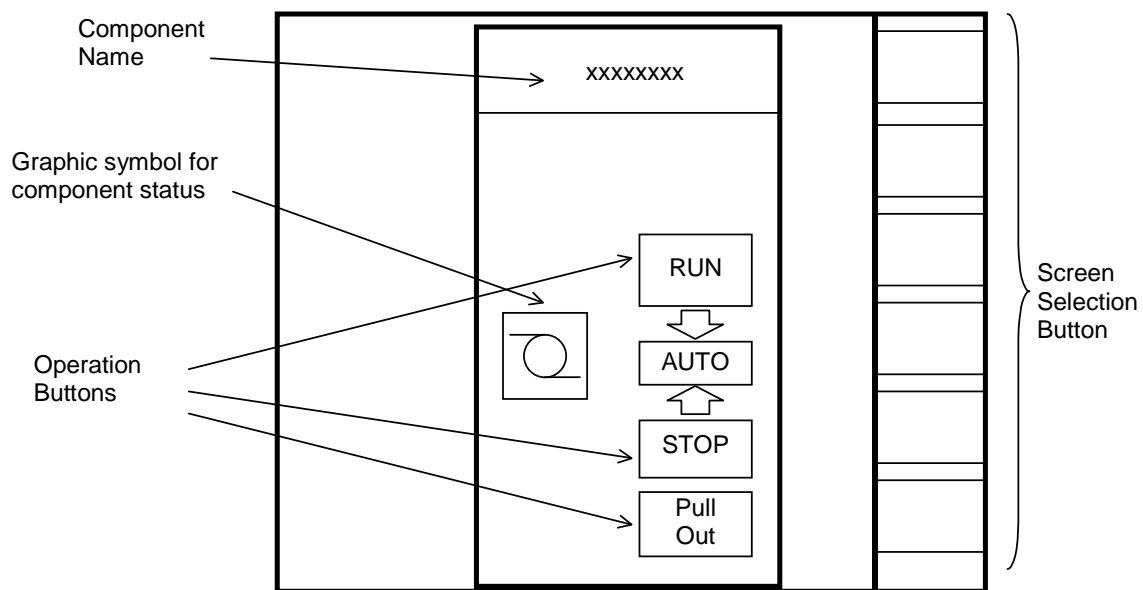
A sample of the operation switch image on the safety VDU panel is shown in Figure 4.2-5.

The screens described in this section are generic screens included in the generic basic software of the MELTAC platform. Other types of screens can be developed on a plant specific basis. The actual screens for any safety application are described in Application Licensing Document.



**Figure 4.2-4 Screen Transition of the Safety VDU Processor**

Table 4.2-1 Screen Descriptions

**Figure 4.2-5 A Sample of Operation Switch Pictogram on the Safety VDU Panel**

4.2.2.1.2 Detailed Explanation of Screen Display and Demand Processing

Basic software process No.5 also includes Screen Display Processing and Screen Demand Processing. These Operation processes and their relationship to other Operation processes are shown in Figure 4.2-6.  
The table below shows the data used to create screen displays and the data used to generate output operation signals.

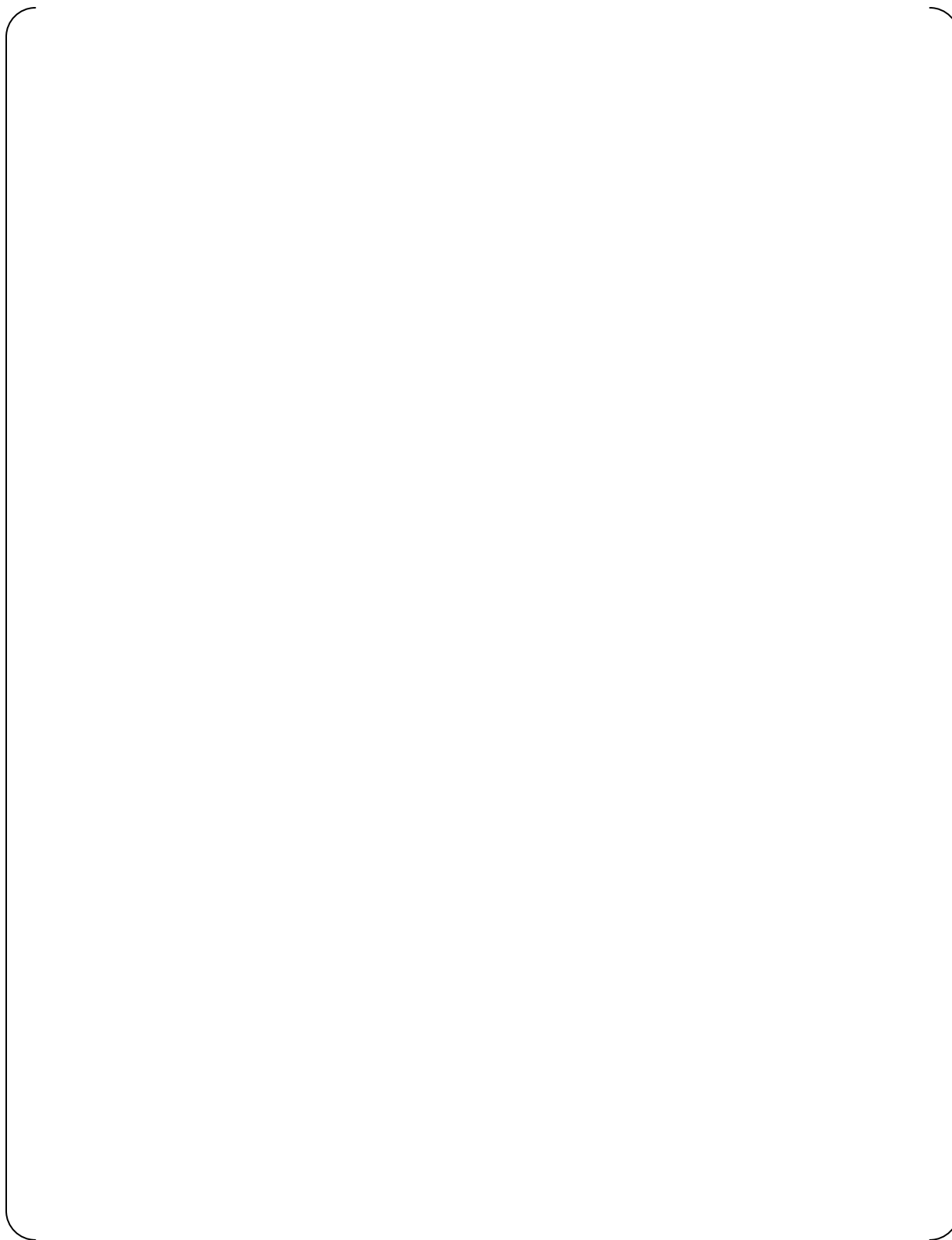
Table 4.2-2 Data Details


a) Screen Display Processing  
[

]

b) Operation Demand Processing  
[

]



**Figure 4.2-6 Explanation of the Safety VDU Processor Operation**

**4.2.2.2 Application Software and MELTAC Engineering Tools**

[

]

**4.2.3 Self-Diagnosis**

[

]

#### **4.2.4 Manual Test**

The safety VDU panel is tested by manually touching screen targets and confirming correct safety VDU processor response.

This test is conducted using a special test display screen that does not initiate any manual control actions.

Many soft buttons are displayed throughout the special test display screen. When a button is touched, the safety VDU panel sends an Operation Touch Signal to the safety VDU processor. The safety VDU processor responds by changing the color of the touched button after receiving the signal.

During this test, the safety VDU processor does not send any touch command control signals to the Control Network.

These test response are generated by the safety VDU processor, so there is an overlap between the manual test and the platform self-diagnosis performed within the safety VDU processor.



### **4.3 Communication System**

#### **4.3.1 General Description**

The key design bases of the Control Network, Data Link and Maintenance Network are provided below. These are applicable to both the controller and the safety VDU processor.

a) Maintenance Network, Control Network and Data Link:

- Asynchronous communication is used. The CPU Module and the communication controller execute their tasks asynchronously. This is facilitated through shared 2-port memory, which allows data to be communicated between the two digital components with no synchronization.
- The CPU Module performs no communication handshaking that could disrupt deterministic logic processing. The digital components that execute the safety functions are separate from the digital components that execute the communications.
- Predefined data size and structure ensure deterministic communication.
- Electrical faults or communication processing faults in one electrical division (or controller) cannot adversely affect performance of the safety function in other divisions (or controllers).

b) Maintenance Network:

- Hardwired interlocks in the CPU Module ensure changes to basic software or application software cannot be made through the data communication interface while the controller or the safety VDU processor are operating, or while the CPU Module is installed in the on-line chassis.

#### **4.3.2 Control Network**

The Control Network communicates plant process data and control signal data with a deterministic periodic cycle.

Inter-divisional communication for safety-related functions is not implemented in the Control Network. For this application only Data Link communication is used, see Section 4.3.3.

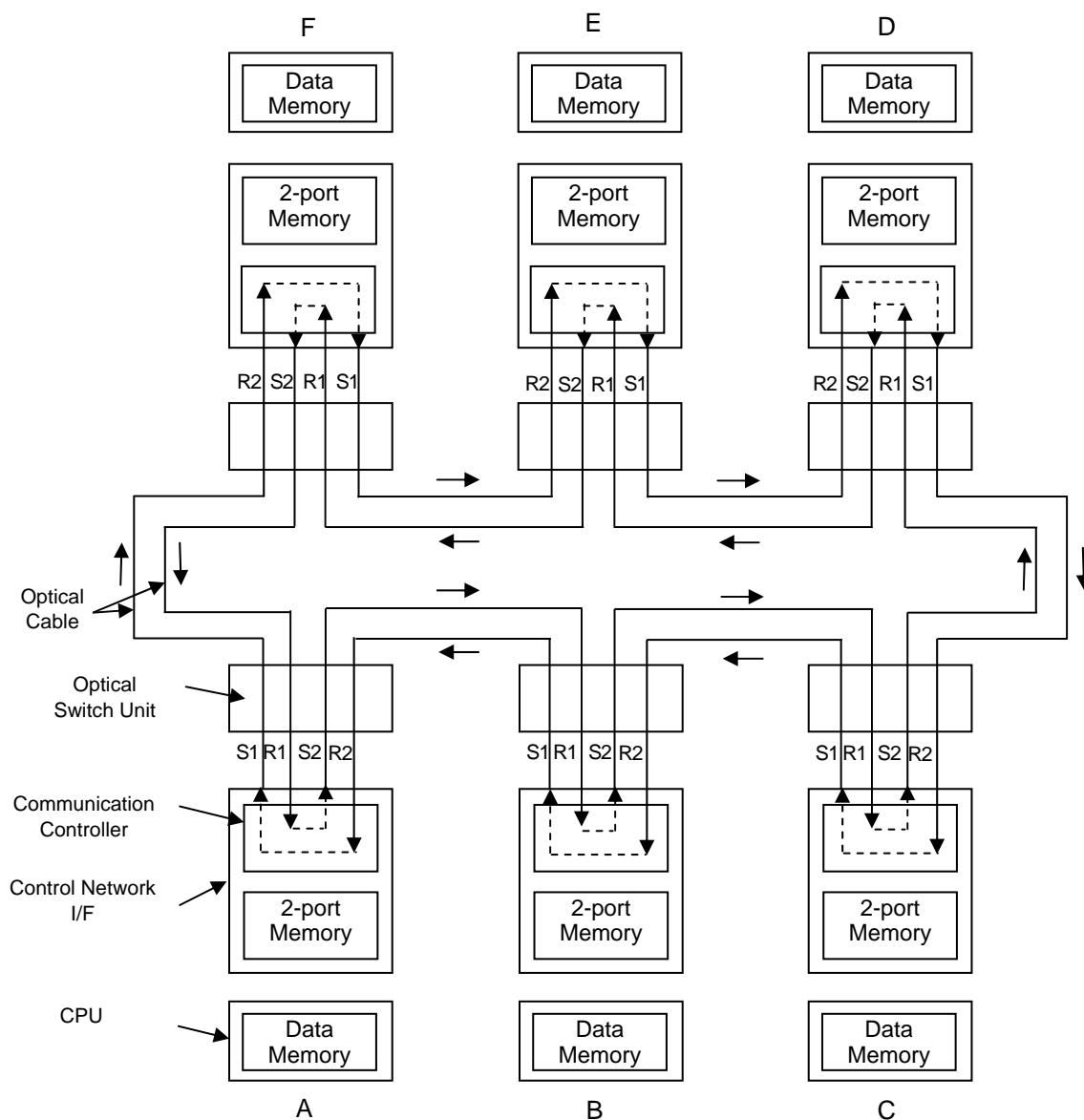
4.3.2.1 Configurations

The Control Network has two types of periodic cycles, normal and high-speed. The desired type is selected during the application design process.

The configuration of the Control Network is as shown in Table 4.3-1.

Table 4.3-1 Configuration of Control Network


A typical configuration of the Control Network for 6 controllers is shown in Figure 4.3-1.

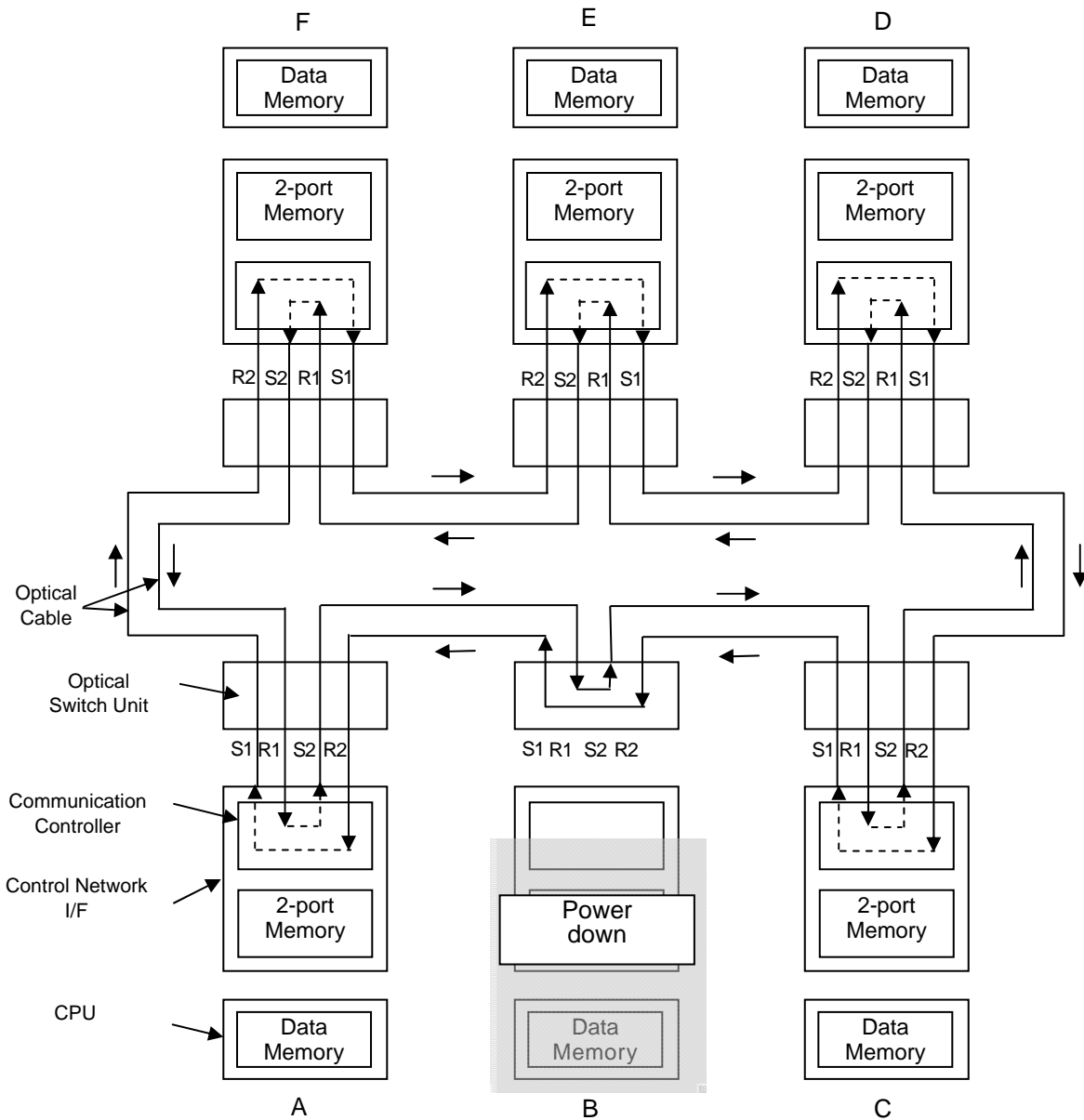


**Figure 4.3-1 Configuration of Control Network**

The Control Network I/F Modules are interconnected in a ring configuration. Each module communicates through an optical switch using 4 independent optical cables: S1 and S2 for transmission and R1 and R2 for reception as shown in Figure 4.3-1, in both clockwise and counterclockwise directions. The optical switch allows any subsystem on the Control Network that is halted or disconnected for maintenance or for failure, to be bypassed so the network ring topology is always maintained. Figure 4.3-2 shows the case where subsystem (B) is halted. In this case, the optical switch bypasses subsystem (B) and directly connects subsystem (A) and (C).

These are the key technical aspects of the Control Network:

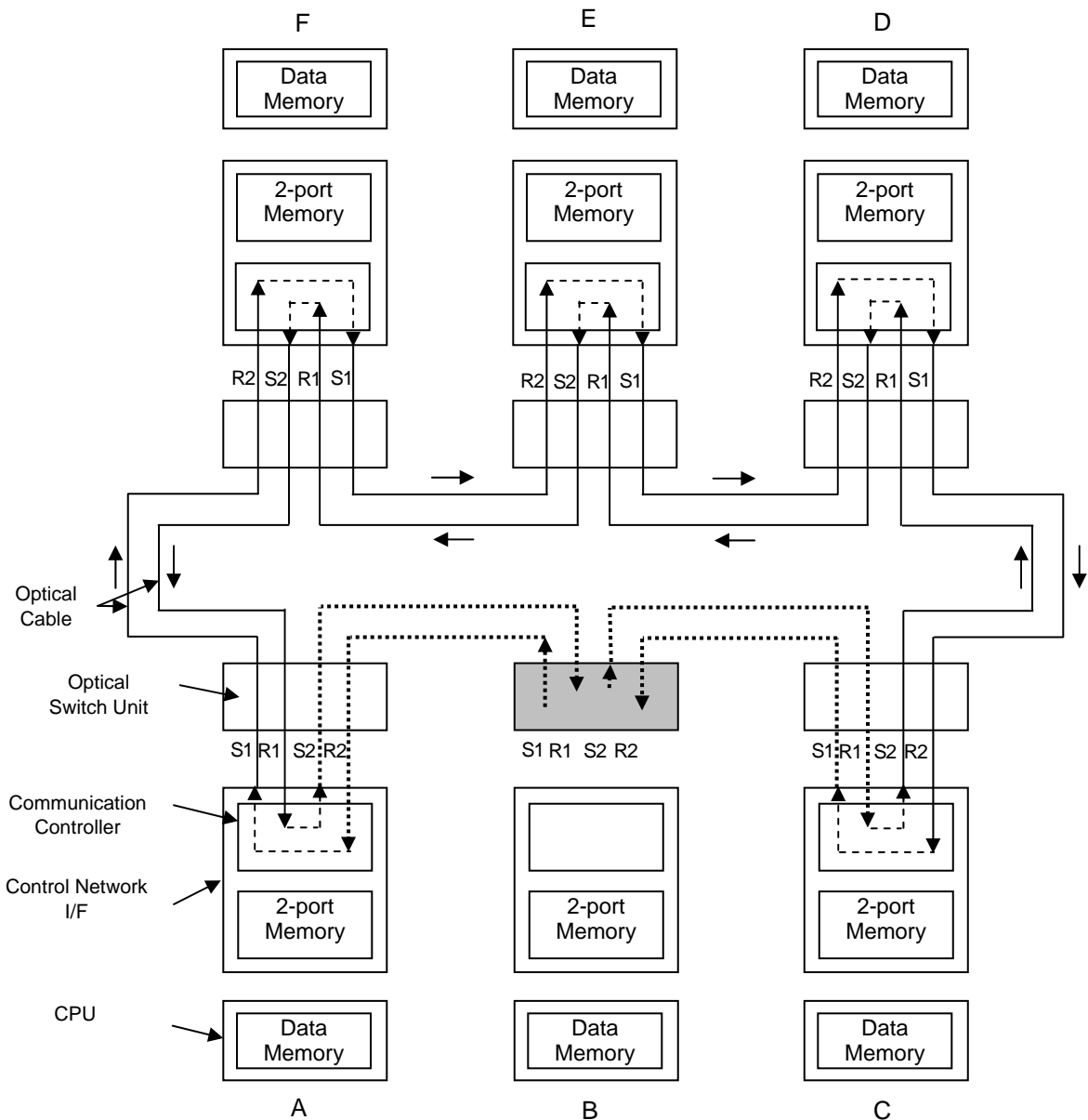
- Each Control Network I/F Module includes 2 receive ports and 2 transmit ports for dual ring redundancy.
- All received data is relayed to the adjacent nodes (in both directions) by the communication controller within the Control Network I/F Module, until the data has been relayed to all nodes. [
- ]
- The communication controller also places the received data in 2-port memory for processing by the CPU Module in its node.
- The 2-port memory contains designated memory locations for the complete data package sent from each node on the Network. [
- ]
- [
- ]
- During its own deterministic cycle, the CPU Module reads data only from the memory locations in 2-port memory that correspond to the network nodes that send data that is relevant to its application software. [
- ]
- If the CPU Module only sends data to the Control Network (unidirectional data flow), as defined in [
- ], the CPU Module does not read any data locations in 2-port memory.
- The CPU Module places data to be transmitted on the Control Network in its designated area of 2-port memory, during its own deterministic cycle. The updated data overwrites the data written by the CPU Module in the previous cycle. If the data has not changed, the same data is rewritten again. This process repeats for every deterministic cycle of the CPU Module.
- The data from the CPU Module, that is stored within its designated location within 2-port memory, is then transmitted to the Control Network by the communication controller during its next deterministic relay/transmit cycle, along with the complete data package sent from each node on the network.
- The deterministic cycles of the communication controller and CPU Module are completely independent.



**Figure 4.3-2 Explanation of Optical Switch Bypass Operation**

The optical switch is powered by the power feeding cable from its associated Control Network I/F Module. If the node's CPU Module fails, or its Control Network I/F Module fails, or the power feeding cable is disconnected, the power is removed from the optical switch causing it to revert to Bypass Mode for that node. When failures are detected by a node's self-diagnosis, the Control Network I/F Module voluntarily removes the power from the optical switch.

A Control Network can bypass a minimum of one failed node. Additional nodes can be bypassed depending on the distance between nodes, as described in Table 4.3-2.



**Figure 4.3-3 Explanation of Optical Switch Failure**

Figure 4.3-3 shows the configuration of the network for failure of an optical switch. If the optical switch for subsystem (B) is in failure status, the communication path is disconnected between the optical switch and the Control Network I/F Module in subsystem (B), and between subsystems (A) and (C), as shown in the figure.

With the failure described above, the optical signal of subsystem (B)'s S1 and S2 port will be cut off. This will be detected by subsystem (A)'s R2 port and subsystem (C)'s R1 port, respectively. Thus the communication path that goes through subsystem (B) is determined to be unusable.

A communication path between subsystems (A) and (C) will then be established automatically via subsystems (D), (E), and (F). The same applies for communication from the other nodes that normally communicate through subsystem (B). Therefore, the only node that can no longer send or receive communication is subsystem (B). The send and receive communication between all other nodes remains fully operable.

The reconfiguration of the communication paths described above causes a momentary disruption of data communication on the Control Network [ ]. However, since the optical switch has been qualified, failure of an optical switch is a random hardware failure that can adversely affect the safety function of only one train; this momentary disruption is not considered in the normal Control Network response time. If the CPU Module reads the data in the Control Network I/F Module 2-port memory during this network reconfiguration disruption interval, the CPU Module will continue to use the data from the previous communication cycle. The CPU Module will alarm the network as failed if the data does not get updated after a predefined time.

4.3.2.2 Specifications

4.3.2.2.1 Infrastructure

The protocol stack of the Control Network is described in Figure 4.3-4.  
The optical Gbit Ethernet is used for the physical layer.  
The Resilient Packet Ring (RPR) based on IEEE Std. 802.17 is applied to the Data Link Layer protocol.

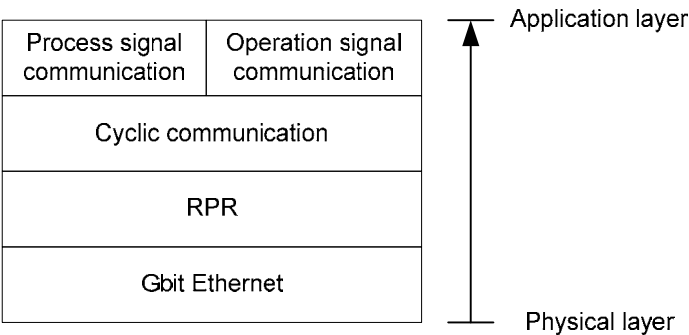


Figure 4.3-4 Protocol Stack of Control Network

The specifications of the Control Network are described in Table 4.3-2.

Table 4.3-2 Control Network Specification


Fiber cable, including outer and inner jackets and any strengthening components, is constructed using only non-conducting materials to ensure inherent isolation to prevent electrical fault propagation.



#### **4.3.2.2.2 Communication Method**

The data communication method of the Control Network is as follows.

[

]

The data is delivered to the destination Control Network I/F Module within the guaranteed data update cycle time, shown in Table 4.3-1.

**4.3.2.2.3 Communication Controller**

[

1

#### **4.3.2.3 Isolation**

The MELTAC platform maintains electrical isolation and communication isolation for the interface between controllers in separate safety trains and for the interface between safety controllers and any non-safety train. The methodology to ensure this isolation is described below.

##### **a) 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 4.3-5

##### **b) Communication Isolation**

[

]

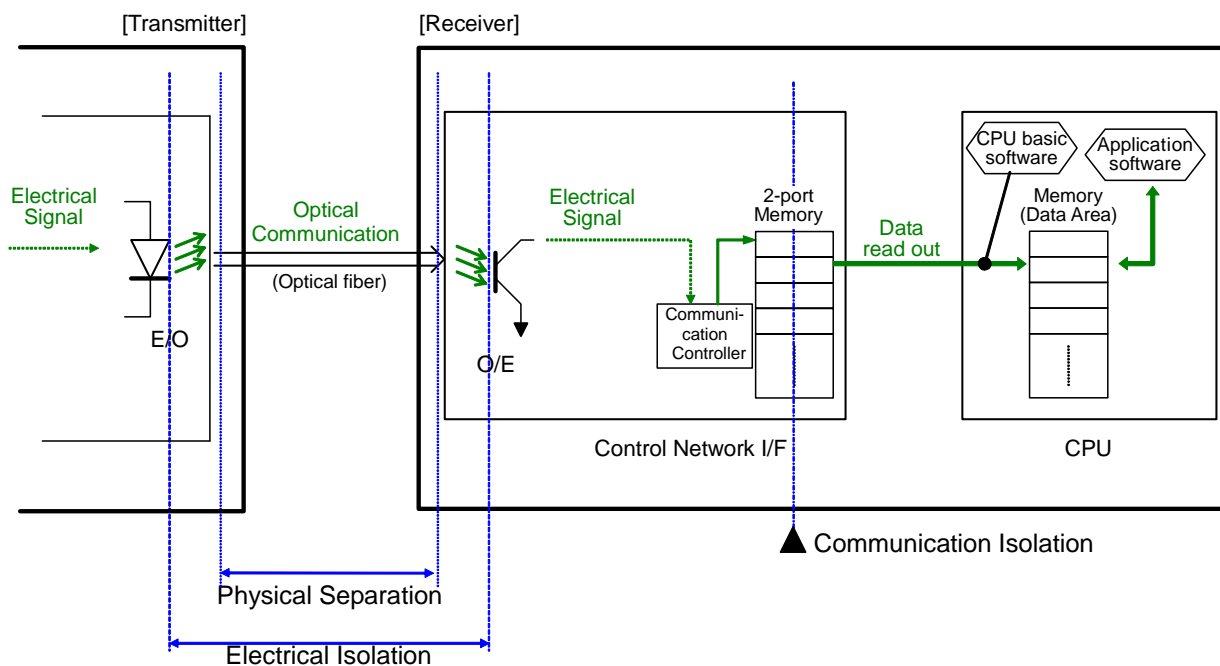


Figure 4.3-5 Separation in Communication of Control Network

4.3.2.4 Self-Diagnosis

The self-diagnosis functions of the Control Network are described below.  
In MELTAC, a fatal error is defined as “Failure” and a tolerable error is defined as “Alarm” (see Section 4.1.5.). For Failure conditions, the CPU Module stops operation; the CPU Module continues operating for Alarm conditions. The application software determines the response to Alarm conditions. For loss of input data, options include using predefined values or the last good values. The categorization of self-diagnosis errors detected for the Control Network I/F Module, as defined in Table 4.3-3, is described below:

Table 4.3-3 Self-Diagnosis Functions of Control Network


#### 4.3.2.5 Communication process

This section provides details for communication process, which is described in Section 4.3.2.3. To exemplify this communication process, this section describes the operational signal interface from the safety VDU (S-VDU) to the safety controller via the intra-division Control Network (referred to as the Safety Bus), and the monitoring signal interface from the safety controller to the S-VDU via the Safety Bus, as applied in a typical application. Figure 4.3-6 is an example to show the receiving process from the S-VDU to the safety controller and Figure 4.3-7 is an example to show the sending process from the safety controller to S-VDU.

[

]



**Figure 4.3-6 Operation Signal Flow from S-VDU**





**Figure 4.3-7 Process Signal Flow from Controller to Safety Bus**

#### 4.3.2.5.1 Detailed Data Flow

This section describes the detailed data flow between the Control Network I/F Module and the CPU Module in the safety controller.

[

]



**Figure 4.3-8 Detail Signal Flow in Controller (Receiving Process)**

[

]

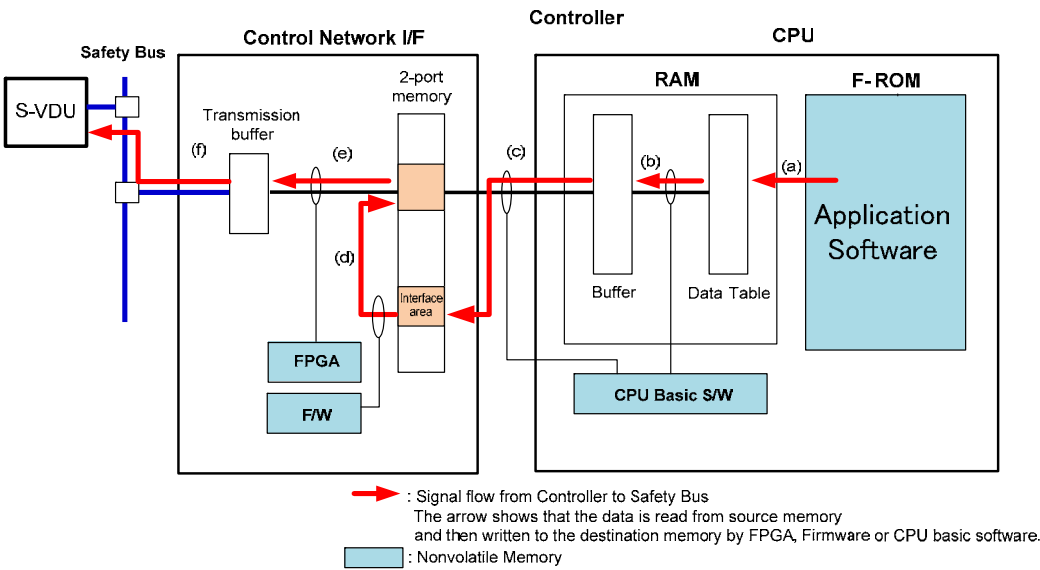


Figure 4.3-9 Detail Signal Flow in Controller (Sending Process of the Process Signal)

[

]

(1) Receiving process

(1-1) Processing by the Control Network I/F Module

This paragraph discusses the processing in the Control Network I/F Module.

Figure 4.3-10 provides details of Figure 4.3-8.



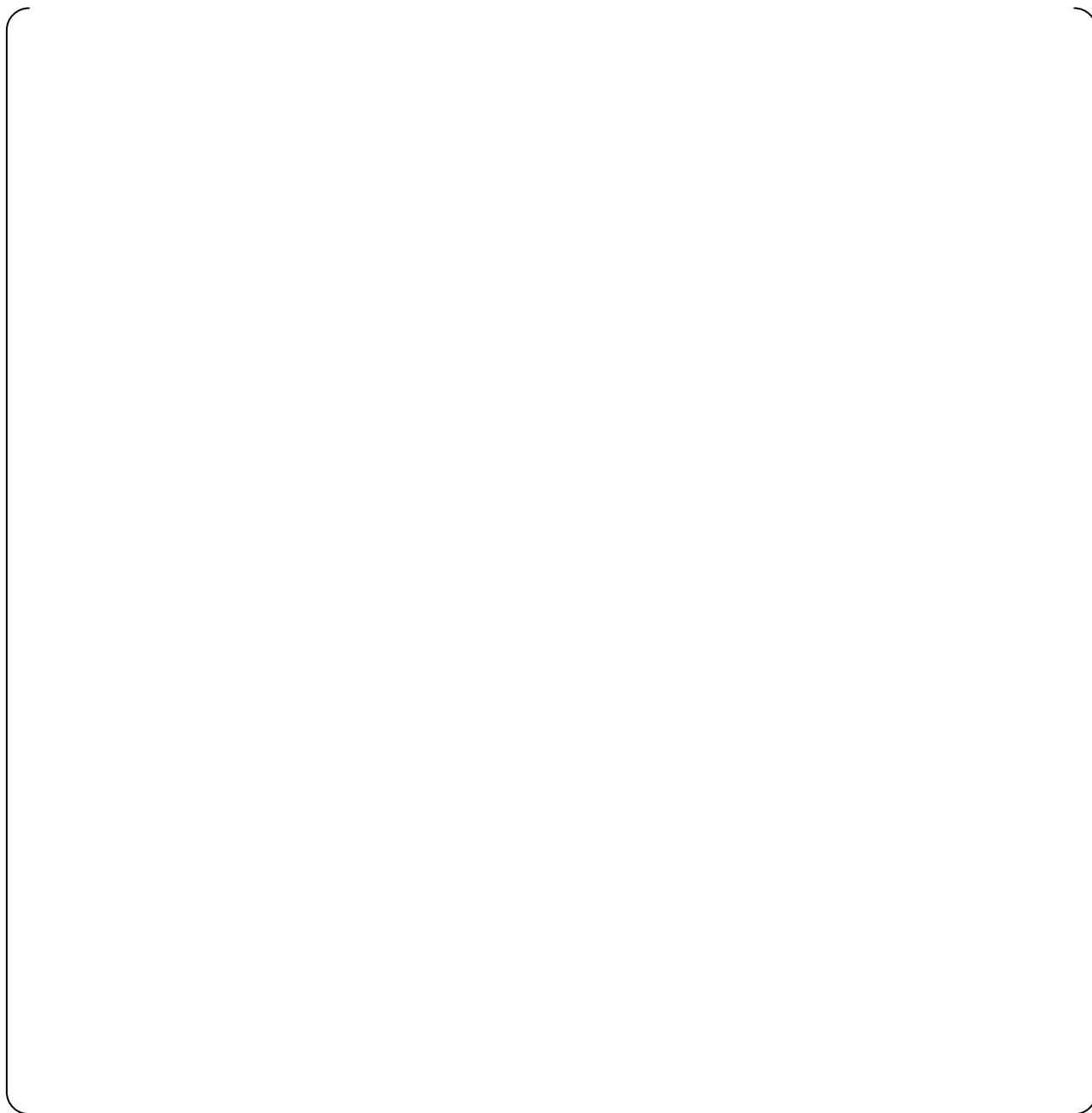
**Figure 4.3-10 Processing by the Control Network I/F Module in the Receiving Process**

[

]

(1-2) Processing by the CPU Module

This paragraph explains the processing of the data by the CPU Module.  
Figure 4.3-11 provides details of Figure 4.3-8.



**Figure 4.3-11 Processing by the CPU Module in the Control Network Receiving Process**

[

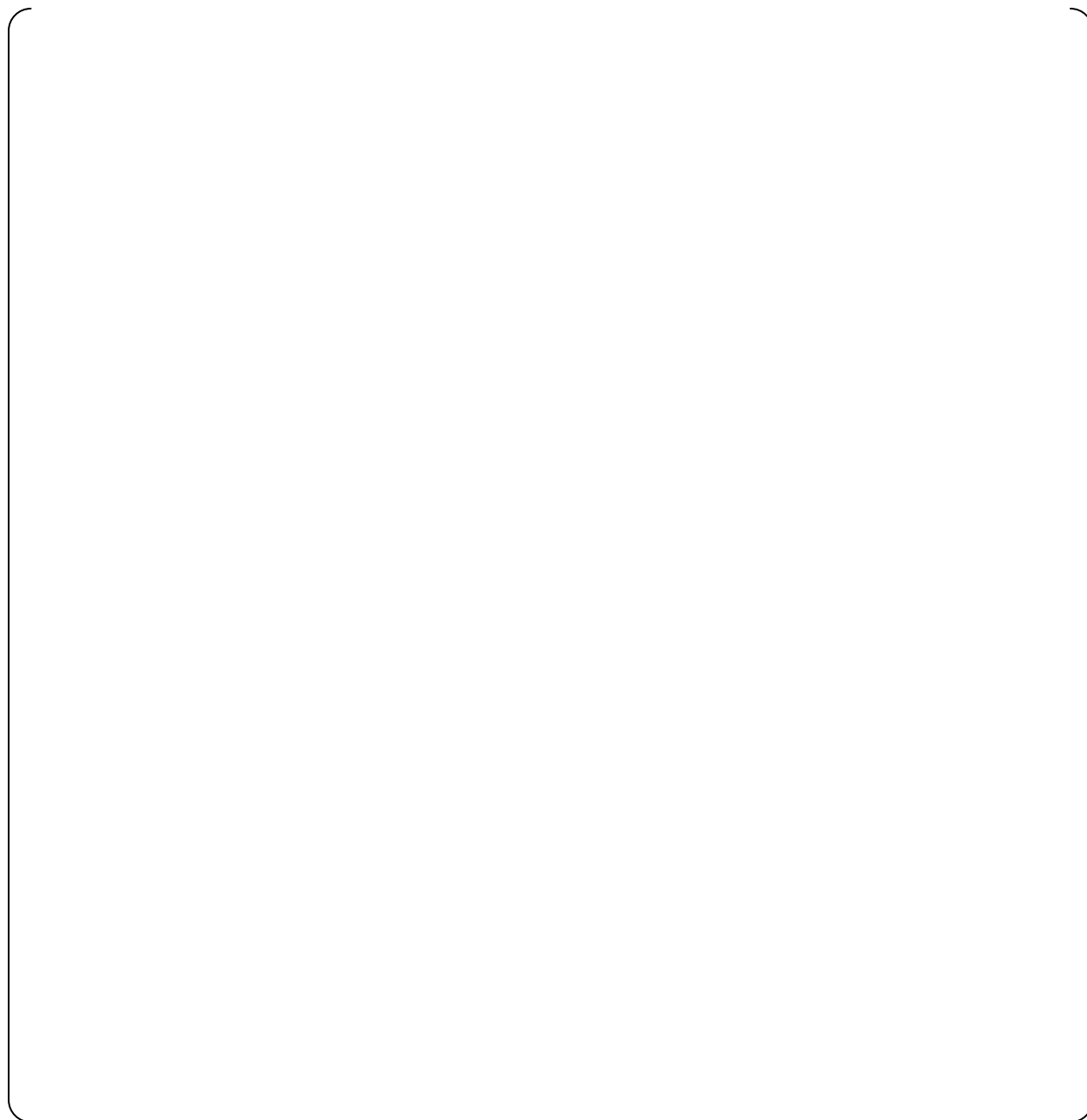


]

(2) Sending Process

(2-1) Processing by the CPU Module

Figure 4.3-12 provides details of Figure 4.3-9.



**Figure 4.3-12 Processing by the CPU Module in the Control Network Sending Process**

[

]

(2-2) Processing by the Control Network I/F Module  
Figure 4.3-13 provides details of Figure 4.3-9.



**Figure 4.3-13 Processing by the Control Network I/F Module in the Sending Process**

[

]

**4.3.2.5.2 Summary of Design Features for the Control Network Communications**

The receiving process in the data flow from the S-VDU to the safety controller will be discussed in this section.

Following are design policies and network check methods for the Control Network interface.

[

]

[

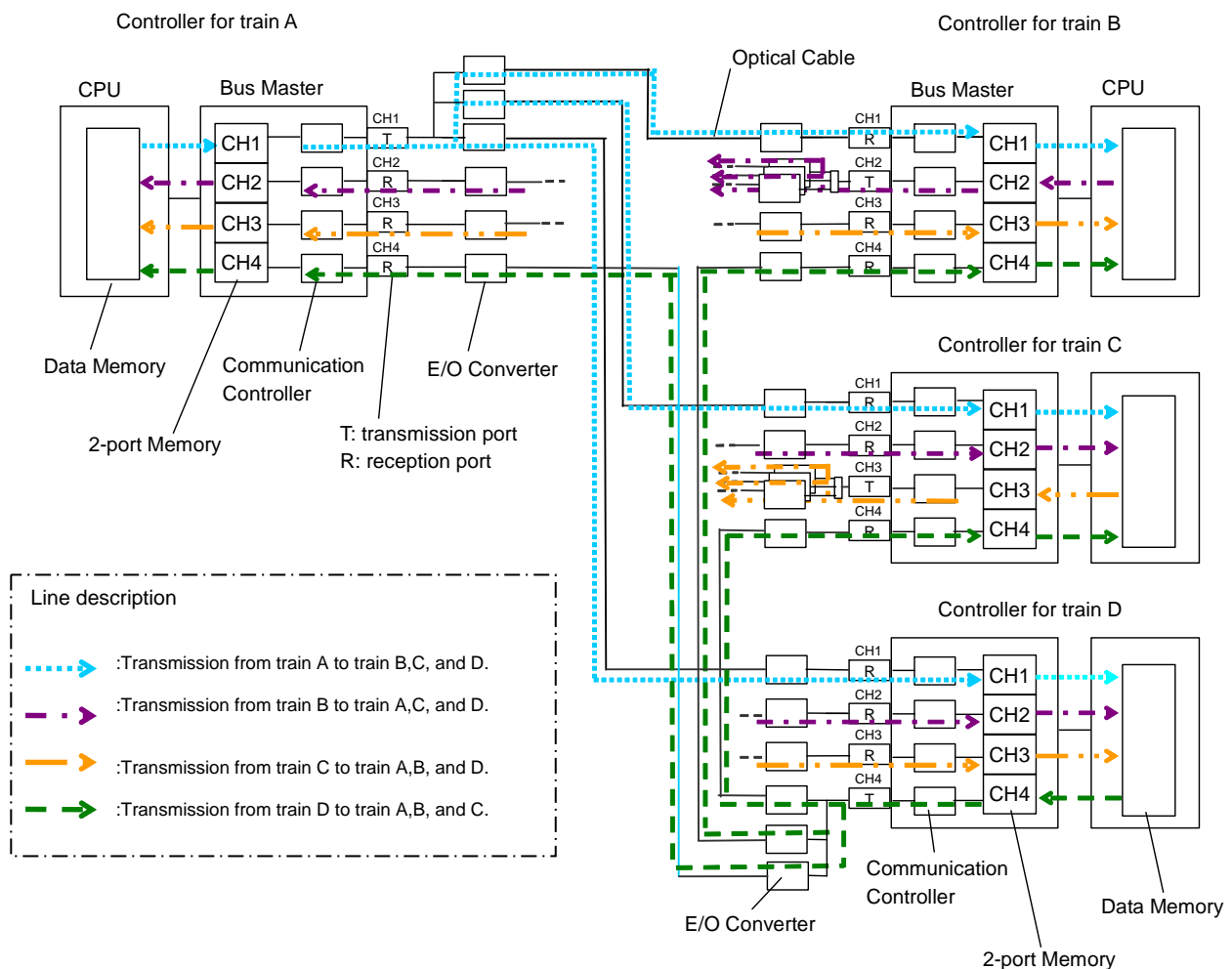
]

### 4.3.3 Data Link

#### 4.3.3.1 Configuration

Data Link communication is used to transmit process signals between the controllers in different safety trains. The Data Link uses a broadcast protocol with a 1 Mbps throughput, with no communication handshaking.

Figure 4.3-14 provides a graphical representation of typical Data Link connections between redundant safety trains. This figure shows all the Data Link components and an example of a connection configuration when CH1 of the controller for train A is the transmission port (T), CH1 of controllers for other trains is the reception port (R), CH4 of controller for train D is the transmission port (T), and CH4 of controllers for other trains is the reception port (R).



**Figure 4.3-14 Example of Connection Configuration of Data Link Configuration**

The Data Link is interfaced through Bus Master Modules. The Bus Master Module provides 4 communication ports (also referred to as channels). [

]

Each port is set either as a transmission port or a reception port. The Bus Master Module produces an electrical output. The output is divided into 3 signal lines; then each output is converted into an optical signal by the E/O Converter Module. The transmission port of the E/O Converter Module is connected by the optical cable to the reception port of the E/O Converter Module in another train.

[

]



4.3.3.2 Specifications

4.3.3.2.1 Infrastructure

The specifications of the Data Link communications are described in Table 4.3-4.

Table 4.3-4 Data Link Communication Specification


Fiber cable, including outer and inner jackets and any strengthening components, is constructed using only non-conducting materials to ensure inherent isolation to prevent electrical fault propagation.

4.3.3.2.2 Communication Method

[

]

**4.3.3.2.3 Communication Controller**

[

]

#### 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 Figure 4.3-14, are described below.

a) Physical Separation

The E/O Converter Module of the Data Link allows for a distance of up to 1 km between sending and receiving controllers. This allows the controllers to be geographically separated into separate areas of the plant.

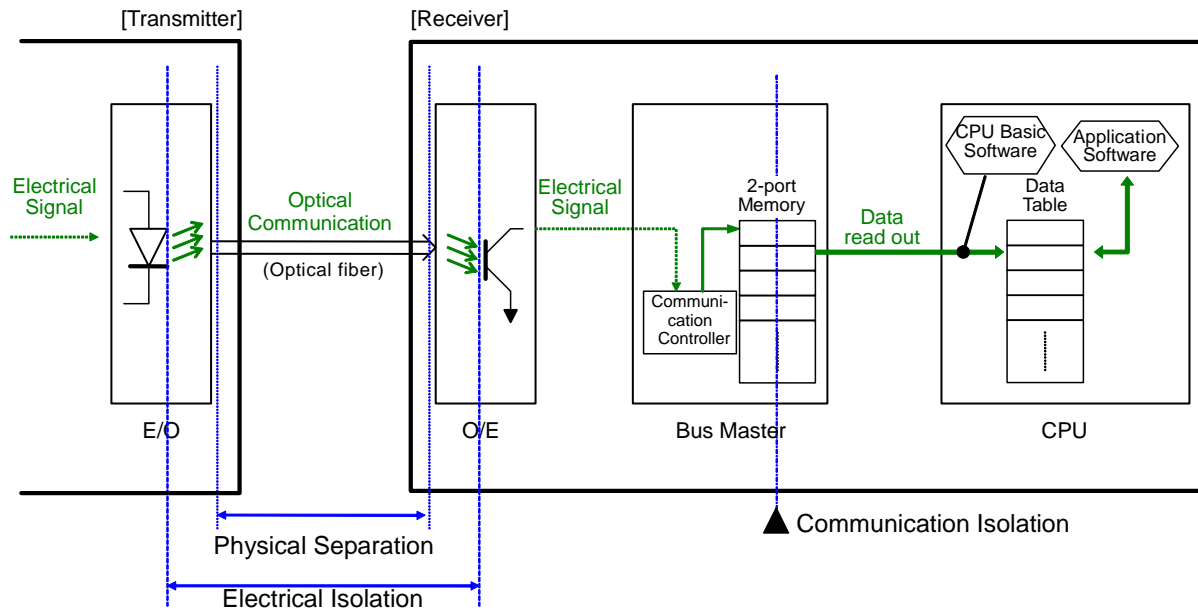
b) Electrical Isolation

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

c) Communication Isolation

[

]



**Figure 4.3-15 Separation in Communication of Data Link**

#### **4.3.3.4 Self-Diagnosis**

The self-diagnosis functions of the Data Link are described below.

[

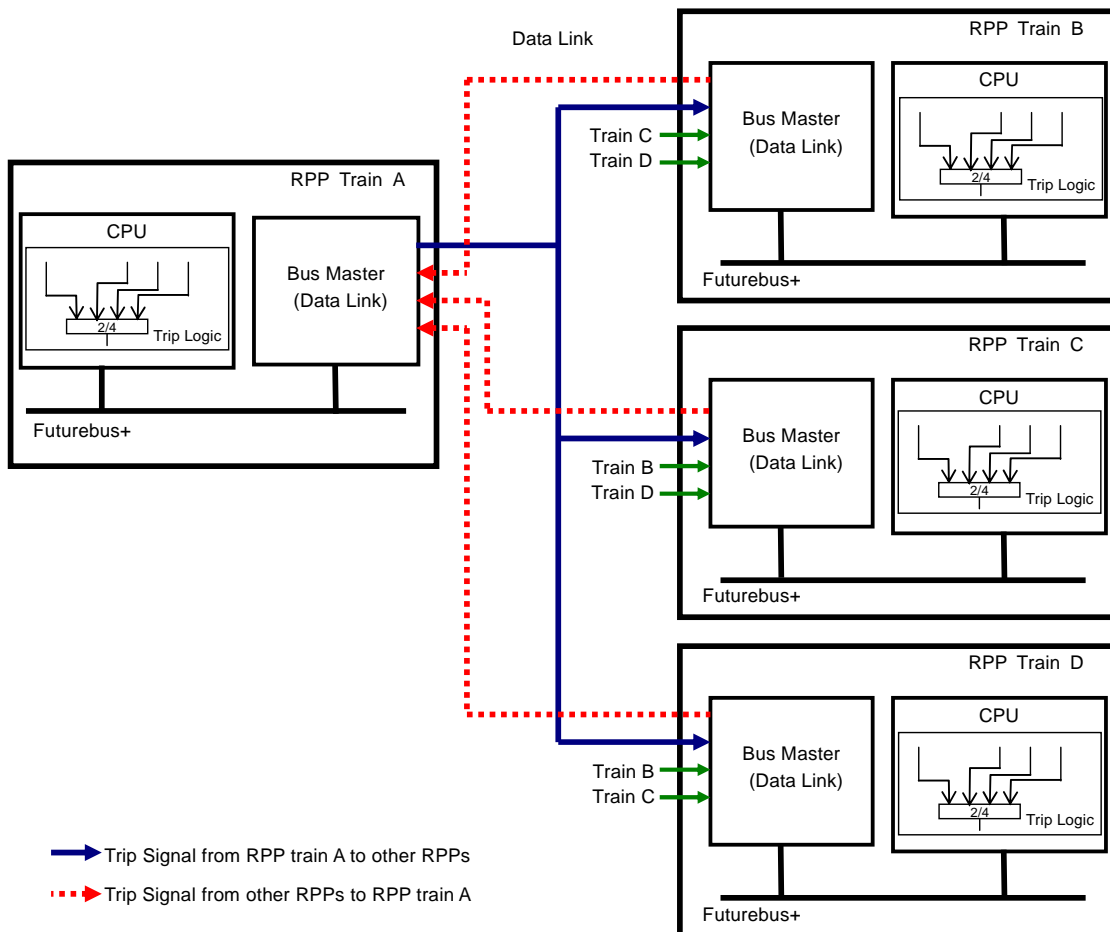
]

#### 4.3.3.5 Communication Independence

This section describes how communication independence is maintained when the Data Link is applied to data communication between controllers in other trains. This section provides details on communication isolation, which is described in Section 4.3.3.3. To exemplify this independence, this section describes the Reactor Protection Processor (RPP) interface to controllers in other trains, as applied in a typical system. Figure 4.3-16 shows the configuration of a part of a typical 4 train RPP that is relevant to the partial trip signal to each of the other 3 RPP trains.

[

]



**Figure 4.3-16 Partial Trip Signal Flow between RPPs**

#### 4.3.3.5.1 Detailed Data Flow

This section describes the detailed data flow between the Bus Master Module and the CPU Module in the RPP.

[

]



**Figure 4.3-17 Detail Signal Flow in RPP (Receiving Process)**

[

]

[

]

**Figure 4.3-18 Detail Signal Flow in RPP (Sending Process of the Trip Signal)**

[

]



(1) Receiving Process

(1-1) Processing by the Bus Master Module

Figure 4.3-19 provides details of Figure 4.3-17.

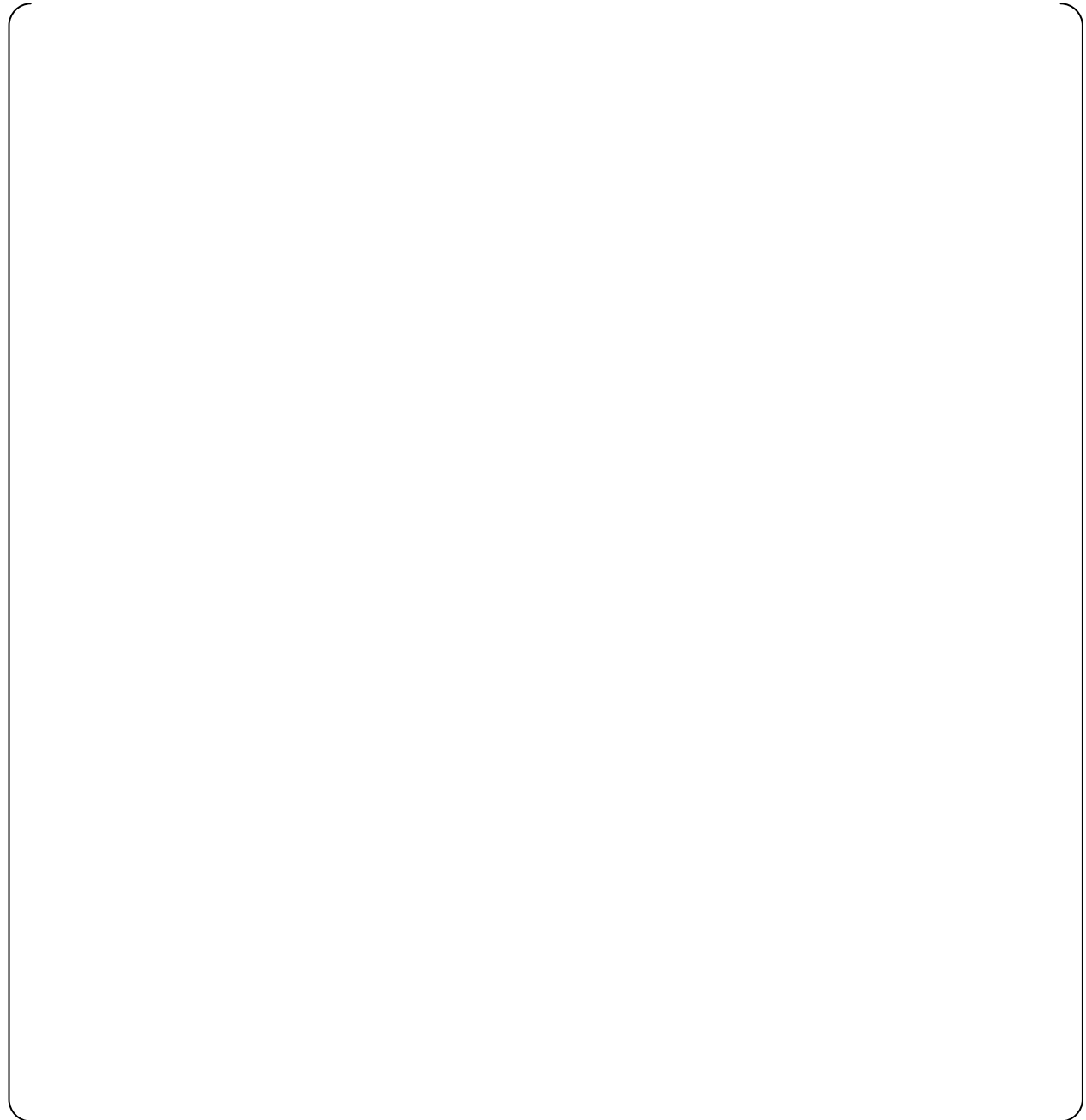


**Figure 4.3-19 Processing by the Bus Master Module**

[

]

(1-2) Processing by the CPU Module  
Figure 4.3-20 provides details of Figure 4.3-17.



**Figure 4.3-20 Processing by the CPU Module in the Data Link Receiving Process**

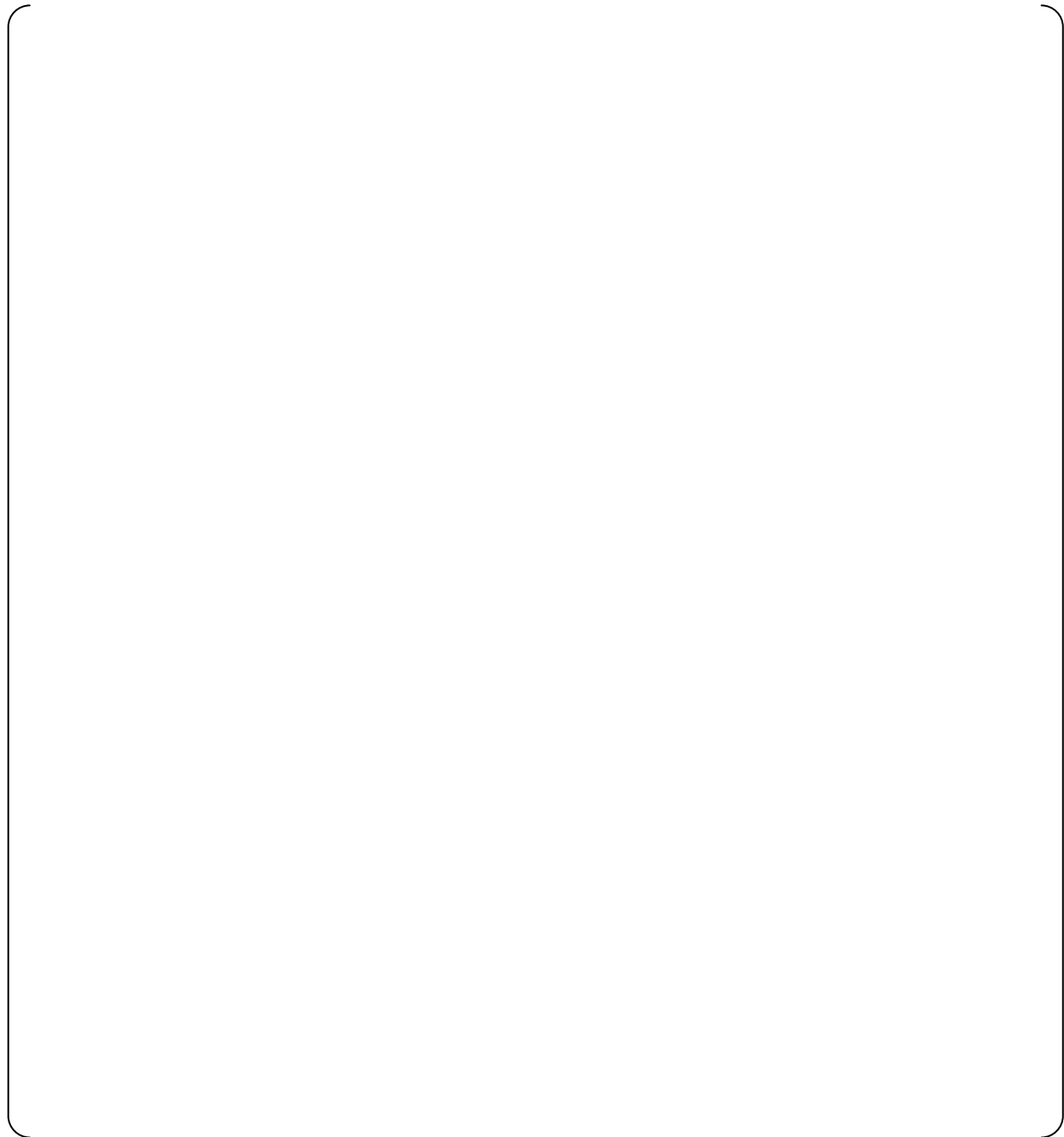
[

1

(2) Sending Process

(2-1) Processing by the CPU Module

Figure 4.3-21 provides details of Figure 4.3-18.



**Figure 4.3-21 Processing by the CPU Module in the Data Link Sending Process**

[

]

(2-2) Processing by the Bus Master Module  
Figure 4.3-22 provides details of Figure 4.3-18.



**Figure 4.3-22 Processing by the Bus Master Module in the Data Link Sending Process**

[

]

**4.3.3.5.2 Summary of Design Features for Data Link Communication**

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

[

]

(3) Conformance to ISG-04

The conformance of ISG-04 is shown in MELTAC platform ISG-04 Conformance Analysis (JEXU-1041-1015).



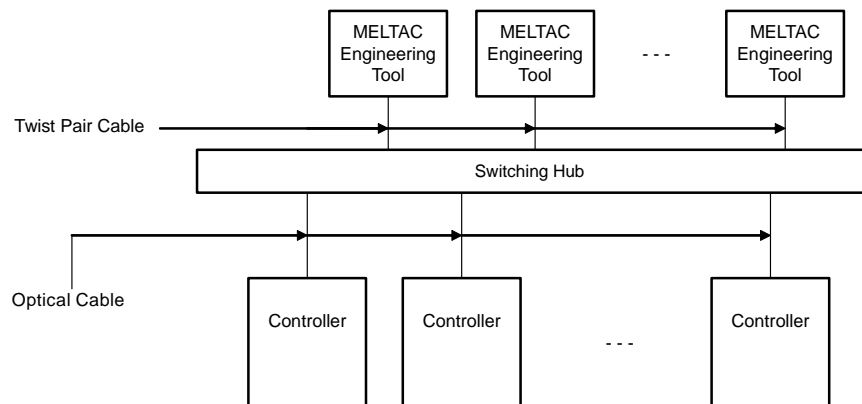
### 4.3.4 Maintenance Network

#### 4.3.4.1 Configuration

The Maintenance Network is used to communicate between the controllers or safety VDU processor and the MELTAC engineering tool, to download new application software to the CPU Module (when installed in the dedicated Re-programming Chassis), or to read/write inside the Data Table of the controller. There may be up to 3 MELTAC engineering tools connected to one controller at any one time. The number of engineering tools actually connected to the Maintenance Network is application dependent.

The description of the controller's processing of data for the MELTAC engineering tool is described in Section 4.1.4.2.

Figure 4.3-23 shows the Maintenance Network configuration for one division. In this figure the Maintenance Network is connected to the controllers. The controllers are normally disconnected at the controller end during normal operation. The controllers are connected periodically for equipment maintenance. A connection signal may be configured in the application software to generate an alarm in the Main Control Room (MCR) when the engineering tool is connected.



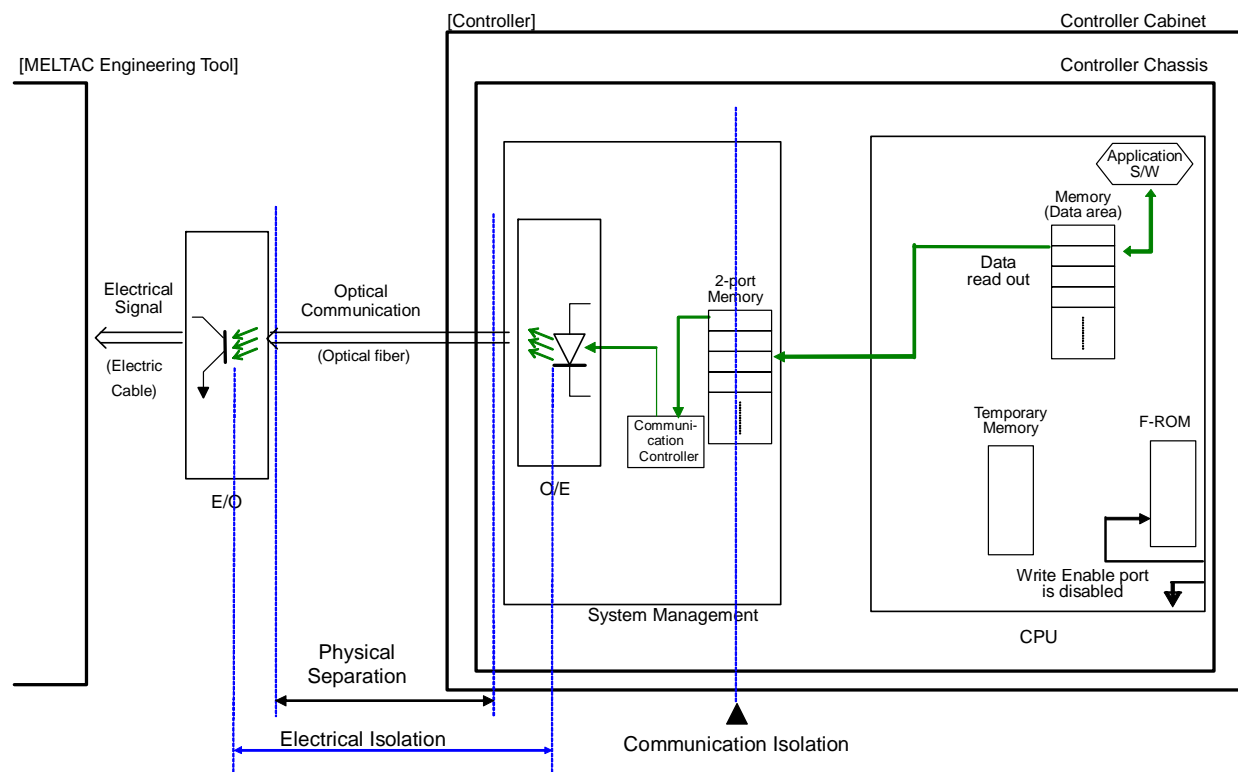
**Figure 4.3-23 Maintenance Network Configuration**

**4.3.4.2 Isolation**

[

|

]



**Figure 4.3-24 Separation in Communication of the Maintenance Network**



**Figure 4.3-25 Dedicated Re-programming Chassis for Writing to the F-ROM**

The MELTAC engineering tool and Switching Hub are connected to the controller based on the following design features:

- The non-safety MELTAC engineering tool and Switching Hub are electrically isolated from the safety components through qualified fiber optic isolators with E/O Converters of System Management Module.
- The communication interface for each controller uses a separate System Management Module with 2-port memory to ensure the communication process and safety function process execute asynchronously.

The controller is normally disconnected from the Maintenance Network, so there is no communication with the MELTAC engineering tool. However, when the controller is connected to the Maintenance Network, the following applies:

- When the controllers are in service (i.e.: with the CPU Module in its normal configuration in the controller cabinet and with the write enable port of the F-ROM disabled) they provide only outbound communication to the MELTAC engineering tool (i.e.: there is no ability for the MELTAC engineering tool to write information to the controller's memory), based on data requests from the MELTAC engineering tool.

[

]

**4.3.4.3 Design Basis of Connection to Maintenance Network**

[

]

#### 4.3.4.4 Specifications

##### 4.3.4.4.1 Infrastructure

The specifications of the Maintenance Network communication are described in Table 4.3-5.

**Table 4.3-5 The Maintenance Network Communication Specification**


Fiber cable, including outer and inner jackets and any strengthening components, is constructed using only non-conducting materials to ensure inherent isolation to prevent electrical fault propagation.

##### 4.3.4.4.2 Communication Method

[



]

#### **4.3.4.4.3 Communication Controller**

[

]

## 4.4 Response Time

The response time depends on the configuration of the controller for a specific application. The worst case response time is determined by combining the response time of individual control processes. This section describes the concepts behind the processing time of each control process. It also describes the calculation method to determine the total response time of an application for a typical hardware configuration. All self-diagnosis are considered in the response time calculation method.

As described in the following sections, the worst case response time is deterministic. Therefore, the response time conforms to BTP 7-21.

### 4.4.1 Processing Time of MELTAC Fundamental Cycle

[

]

**Figure 4.4-1 The Time Chart of Fundamental Process in Cyclic**

[

]

#### 4.4.2 Processing Time of MELTAC Application

The MELTAC platform is composed of the CPU Module, Bus Master Module, various types of I/O module, Control Network I/F Module and safety VDU panel. An external input is processed by each of these components before the control result is output to external terminal(s).

Figure 4.4-2 is an example of a typical MELTAC hardware configuration, including communication between 2 controllers. As shown in Figure 4.4-2, the same process applies to many components of a typical application. Table 4.4-1 shows the method to calculate the minimum and maximum response time for each process (T1 – T7). Each process executes asynchronously. Therefore, the minimum time reflects a theoretical situation where each consecutive process is completed prior to the initiation of the next process. Similarly, the maximum time reflects a theoretical situation where each consecutive process is completed just after the initiation of the next process; therefore each process requires an additional cycle.

Response times for safety critical applications, such as reactor trip and ESF actuation, are based on the maximum time.



**Figure 4.4-2 Internal Process Divisions of the MELTAC Platform to Perform Response Time Calculations**

Table 4.4-1 Description of Processing in Each Component (Maximum/Minimum Values)



**4.4.3 Examples of Response Time Calculations**  
[

1



**4.5 Control of Access**

[

]

**4.5.1 Control of Access for Hardware**

[

]

**4.5.2 Control of Access for Software**

[

]

**4.5.3 Control of Access for Temporary Changes to Process Values**

[

]

## **5.0 ENVIRONMENTAL, SEISMIC, ELECTROMAGNETIC AND ISOLATION QUALIFICATION**

This section describes the environmental, seismic, electromagnetic, surge withstand capability, electrostatic discharge and isolation qualifications of the MELTAC platform. The method and the result of the qualification testing are described. If any module is updated, and it is determined that qualification re-testing is required by the evaluations conducted in accordance with Section 6.1.7, the module will be tested with the same method and acceptance criteria. The same method and acceptance criteria will also be used for any new MELTAC modules.

Table 5.0-1 shows the regulatory requirements and acceptance criteria for each test.

**Table 5.0-1 Regulatory Requirements and Reference to Acceptance Criteria for Each Qualification Test**

Test Item	Regulatory Requirement	Reference to Acceptance Criteria
Environmental Test	RG 1.89 (IEEE Std. 323-1974)	System Level Test: 5.1.2.1 Module Level Test: 5.1.2.2
Seismic Test	RG 1.100 (IEEE Std. 344-2004)	Cabinet Test: 5.2.2.1 Module Level Test: 5.2.2.2
Electromagnetic Test	RG 1.180	Conducted Emissions, Low Frequency (CE101) Test: 5.3 Conducted Emissions, High Frequency (CE102) Test: 5.3.2.1 Radiated Emissions, Magnetic Field (RE101) Test: 5.3.2.2 Radiated Emissions, 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	RG 1.180 (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	RG 1.75 (IEEE Std. 384-1992)	5.5

The overview of the qualification tests, test methods, acceptance criteria and any deviations from the acceptance criteria for the MELTAC modules are provided in Sections 5.1 through 5.5. These qualification tests demonstrate that the MELTAC platform is in accordance with the regulatory requirements in Table 5.0-1.

The test items and results are presented in the following test reports. The test reports reference the test procedures.

**Table 5.0-2 Test Reports**

Test Item	Test Report
Environmental Test	MELTAC-Nplus S Environmental Test Report (JEXU-1041-1044)
Seismic Test	MELTAC-Nplus S Seismic Test Report (JEXU-1041-1045)
Electromagnetic Test, Surge Withstand Test, Electrostatic Discharge Test	MELTAC-Nplus S EMC/ESD Test Report (JEXU-1041-1046)
Isolation Test	MELTAC-Nplus S Isolation Test Report (JEXU-1041-1047)

## **5.1 Environmental Qualification Testing**

### **5.1.1 Environmental Specification and Outline of Test**

The environmental specifications of the MELTAC platform are shown in Section 4.1.1.4. The tests are performed to demonstrate that the MELTAC platform will continue to operate without loss of functions under the identified abnormal environmental conditions (temperature, humidity).

The MELTAC platform System Environmental Testing is performed in a cabinet equipped with representative components of the platform.

The MELTAC platform System Environmental Testing is in accordance with RG 1.89 which endorses IEEE Std. 323-1974.

## **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 selected as those that are deemed necessary to confirm the safety function of a typical reactor protection system, including the bi-stable operation and the trip signal output.

#### **(1) Method**

For the System Environmental Tests, a cabinet equipped with the MELTAC modules interconnected and powered in a test configuration is placed inside a thermostatic chamber. The test configuration produces the worst case expected temperature rise across the module chassis and across the cabinet. Before, during, and after each test, it is confirmed that there are no equipment failures or abnormal functions such as erroneous bi-stable operation or erroneous trip signal output, etc. To determine whether any functional abnormalities occurred, the output signals are recorded on a chart recorder to capture any erroneous output during the test. In addition, the test confirms that the self-diagnosis function of the MELTAC platform detects no abnormalities during the test. The test also confirms that the self-diagnosis function is still operating at the end of the test.

#### **(2) Acceptance Criteria**

For the System Environmental Test, the correct performance of the system is confirmed during the following tests.

[

]

### **5.1.2.2 Module Environmental Test**

The MELTAC modules for the Module Environmental Test are shown in Appendix A. For module types with similar circuit electronics whose differences will have no impact on environmental test results, such as NO vs. NC contacts or differences in their input ranges, one typical module type is selected.

[



1

## **5.2 Seismic Qualification Testing**

### **5.2.1 Overview**

The seismic qualification testing confirms that the MELTAC platform maintains structural integrity and correct functional operation during and after a design basis earthquake. Seismic testing is part of the overall system seismic qualification which ensures there is no negative effect on the safety protection function of the equipment in case an earthquake occurs during plant operation.

The Cabinet Seismic Resistance Test is performed with a MELTAC cabinet fully loaded with most, but not all, MELTAC components. For the Cabinet Seismic Resistance Test, a test specimen is prepared for a typical safety protection system application. The tests are conducted using a 3-Direction large shaker table. The test specimen is vibration-excited on the tri-axial shaker table. During the test, the physical integrity and vibration characteristics of the cabinet are confirmed. All system functions are also confirmed before, during and after the excitation. The input acceleration used for the Cabinet Seismic Resistance Test is set high enough to cover the floor response spectrum range of power plants in the U.S.

In addition, the Module Seismic Resistance Tests are performed for mechanically different MELTAC-Nplus S components. For modules that have similar structures and positions of parts, one typical module type is tested because the module differences, such as input ranges, will have no impact on their seismic capability. Other mechanically comparable modules are qualified by similarity to the tested module. The similarity analysis for any untested modules is documented in the Seismic Qualification Report. The modules are mounted in a chassis for the Module Seismic Resistance Test.

In the seismic test, the acceleration ratio applied to the modules mounted in the cabinet with respect to the input acceleration of the cabinet increases with the position of the height within the cabinet. Hereafter, this acceleration ratio is called “response ratio”. For the Module Seismic Resistance Tests, the cabinet maximum response ratio is analyzed from the Cabinet Seismic Resistance Test. The input acceleration for the Cabinet Seismic Resistance Test is multiplied by the maximum response ratio, and additional margin is added to the worst case input acceleration for the chassis.

A chassis loaded with the MELTAC modules is vibration-excited with this worst case input acceleration. During and after this testing, the physical integrity and correct functional operation of the modules are confirmed.

The seismic testing methods for the MELTAC platform comply with RG 1.100, which endorses IEEE 344-2004.

### **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 is prepared. The loading configuration represents the worst case

expected stress on internal mounting hardware. The MELTAC modules for the Cabinet Seismic Resistance Test are shown in Appendix A.

For module types with similar circuit electronics whose differences will have no impact on environmental test results, such as NO vs. NC contacts or differences in input ranges, one typical module type is selected.

[

]

[

]

**5.2.2.2 Module Seismic Resistance Test**

For the Module Seismic Resistance Test, physical and functional integrity are confirmed by testing individual modules or chassis loaded with multiple modules. The MELTAC modules for the Module Seismic Resistance Test are shown in Appendix A.

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

[

]

### 5.3 Electromagnetic Compatibility and Radio Frequency Interference Qualification Testing

The EMI/RFI emission and susceptibility tests are performed for the MELTAC platform based on the methods and acceptance criteria of RG 1.180. The EMC qualification to RG 1.180 is confirmed for the MELTAC platform. The tests are performed with a MELTAC cabinet fully equipped with a typical configuration of the MELTAC components required for the safety protection system.

[

]

The specific test methods used for the EMI/RFI emission and susceptibility tests are described below as specified by MIL-STD-461E.

- Conducted emissions, low frequency, 120 Hz to 10 kHz (CE101)
- Conducted emissions, high frequency, 10 kHz to 2 MHz (CE102)
- Radiated emissions, magnetic field, 30 Hz to 100 kHz (RE101)
- Radiate emissions, electric field, 2 MHz to 1 GHz, 1 GHz to 10 GHz (RE102)
- Conducted susceptibility, low frequency, 120 Hz to 150 kHz (CS101)
- Conducted susceptibility, high frequency, 10 kHz to 30 MHz (CS114)
- Conducted susceptibility, bulk cable injection, impulse excitation (CS115)
- Conducted susceptibility, damped sinusoidal transients, 10 kHz to 100 MHz (CS116)
- Radiated susceptibility, electric field, 30 MHz to 1 GHz, 1 GHz to 10 GHz (RS103)

For the Power Line Surge Withstand Capability Test, the following tests are performed with the same configuration as that for the EMI/RFI Test. The specific test methods used for these tests are described below as specified by IEC 61000-4.

- Surge Withstand Capability, Ring Wave (IEC 61000-4-12)
- Surge Withstand Capability, Combination Wave (IEC 61000-4-5)
- Surge Withstand Capability, Electrically Fast Transients/Bursts (IEC 61000-4-4)

An Oscillatory Wave Test related to surge withstand capability is performed based on IEEE Std. 472 for the MELTAC modules. The following test parameters are applied: a frequency range of 1 MHz, first peak voltage range of more than 2.5 kV and repetitive rate of more than 50 tests per second for a period of more than 2 seconds.

For all Susceptibility and Surge Withstand Capability Tests the following acceptance criteria are applied:

- There is no equipment damage
- Processors continue to function
- Data communications are not disrupted
- Discrete I/O does not change state
- Analog I/O levels do not vary by more than 3%
- There is no VDU image disturbance



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 occurrences of any system function abnormality, data communication abnormality, and equipment failure are confirmed by referring to the results of the self-diagnosis function of the MELTAC platform. It is verified that the self-diagnosis function is still operating at the end of the test.

Sections 5.3.1 and 5.3.2 describe the test configuration, the test method, and acceptance criteria.

### **5.3.1 Test Configuration**

The EUT is comprised of 2 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 cabinet layout, the 2 cabinets are placed side by side with no space in between, thus acquiring the integral configuration. The cabinets are 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 2 cabinets.

The power to the safety VDU panel is supplied from the CPU cabinet and connected with the power cable and the signal cable. The EUT includes the module types required for safety protection system applications, as shown in Appendix A.

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

The AC power to the EUT is supplied from 2 systems: main and standby. Since both power sources with the EUT have the same configuration, the tests for AC input power line of CE102, CS101, CS114 and IEC 61000-4 are performed for one AC power cable.

### 5.3.2 Description of Tests

#### 5.3.2.1 Conducted Emissions, Low Frequency (CE101) Test

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

a) Method

The conducted emissions from the input power lead cable of the EUT are measured to confirm that the electromagnetic conducted emissions from the EUT do not exceed the specified value.

b) Test Subject

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

[

]

#### 5.3.2.2 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 emissions from the input power lead cable of the EUT are measured to confirm that the electromagnetic conducted emissions from the EUT do not exceed the specified value.

b) Test Subject

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

[

]

#### 5.3.2.3 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 confirm that the

magnetic field radiated emissions from the EUT do 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 4 surfaces are scanned for 360 degrees with the loop sensor positioned at the center of the location (height) where the module is mounted.

[

]

#### **5.3.2.4 Radiated Emissions, 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 emissions from the EUT do not exceed the specified value.

b) Test Subject

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

[

]

#### **5.3.2.5 Conducted Susceptibility, Low Frequency (CS101) Test for Power Leads**

According to Section 4 of RG 1.180, the CS101 test is mentioned as the MIL-STD-461E test method that can be applied for testing the conducted EMI/RFI susceptibility of 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 the AC input power lead to the EUT.

[

]

#### **5.3.2.6 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 RG 1.180.

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 cables and the control cables (input and output cables of the Digital I/O Modules and Power Interface Module) to the EUT.

[

]

#### **5.3.2.7 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 RG 1.180.

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 of each of the signal cables (input and output cables of the Analog I/O Modules, the Isolation Modules and the RGB cables) to the EUT.

[

]

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

According to Section 4.2 of RG 1.180, 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 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 of each of the signal cables (input and output cables of the Analog I/O Modules, the Digital I/O Modules, the PIF Module, the Isolation Modules and the RGB cables) to the EUT.

[

]

**5.3.2.9 Conducted Susceptibility, Damped Sinusoidal Transients (CS116) Test**

According to Section 4.2 of RG 1.180, the CS116 test is stated as the MIL-STD-461E test method that can be applied as the conducted EMI/RFI susceptibility test along the signal 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 Modules, the Digital I/O Modules, the PIF Module, the Isolation Modules and the RGB cables) to the EUT.

[

]

**5.3.2.10 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, all interface cables and the safety VDU panel.

The EUT enclosure is placed above the floor as in actual plant conditions to make its height 7.55 ft (2300 mm). Then the emission of the radiated electric field to the EUT enclosure comes from 4 horizontal directions because the top and the bottom parts are not likely to be affected by the electric field.

[

]

**5.3.2.11 Surge Withstand Capability, Ring Wave Test**

The test is performed according to the method set forth in IEC 61000-4-12 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 (RG 1.180 Table 22), 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.

[

]

**5.3.2.12 Surge Withstand Capability, Combination Wave Test**

The test is performed according to the method set forth in IEC 61000-4-5 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 (RG 1.180 Table 22), and the according surge level is 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.

[

]

**5.3.2.13 Surge Withstand Capability, Electrically Fast Transients/bursts Test**

The test is performed according to the method set forth in IEC 61000-4-4 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 (RG 1.180 Table 22), and the corresponding surge voltage level is 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.

[

]

## 5.4 Electrostatic Discharge Qualification Testing

For the MELTAC platform, the electrostatic discharge (ESD) test is performed based on IEC 61000-4-2 with test level-2, in accordance with Annex A (maximum charge voltage is 8 kV, 15 kV). This maximum charge voltage is based on the MELTAC cabinet being installed on the floor using antistatic materials or concrete.

To avoid any special ESD maintenance precautions for US applications, an additional ESD test is also performed to level-4. This section describes the test and acceptance criteria.

The test is performed with the MELTAC cabinet fully equipped with a typical configuration of the MELTAC components required for a safety protection system.

The MELTAC modules for the ESD test are shown in Appendix A

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

The following acceptance criteria are applied for equipment that can be accessed during operation:

- There is no equipment damage
- Processors continue to function
- Data communications are not disrupted
- Discrete I/O does not change state
- Analog I/O levels do not vary by more than 3%
- There is no VDU image disturbance

This is the same acceptance criteria as for the EMI/RFI susceptibility test.

For equipment that can be accessed only during maintenance, the only acceptance criterion is to ensure no equipment damage.

The ESD test is performed according to the method set forth in IEC 61000-4-2 as follows:

### a) Method

Confirm that the EUT can withstand the ESD, where personnel can contact, such as the human-machine interface, during normal operation and when the equipment is out of service during maintenance.

### b) Test Subject

The following equipment areas are likely to be accessible by personnel during normal operation.

- The touch panel of the safety VDU panel and the surrounding area
- The front/rear door handles of the cabinet and the surrounding area
- The switches of the Status Display Module, and the surrounding area
- The switches and fuses of the fans, and the surrounding area
- The front panel of the Power Supply Modules and Analog Output Modules

Other human-machine interface areas of the equipment are expected to be accessed only during maintenance.



[

]

## 5.5 Isolation Qualification Testing

[

|

|

]



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



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

[

]

## 6.0 QUALITY ASSURANCE AND LIFE CYCLE

The MELCO quality assurance program (QAP) complies with 10 CFR 50 Appendix B (complies with ASME NQA-1-1994). This is referred to as the App.B-based QAP.

The MELTAC platform was originally developed under the Japanese nuclear quality program that encompasses most of 10 CFR 50 Appendix B requirements. MELCO performed a re-evaluation of the MELTAC platform design and the design process based on the commercial grade dedication process in accordance with 10 CFR 21. This re-evaluation was performed by an independent MELCO organization that was not involved in the original MELCO development to ensure that the MELTAC platform has the technical characteristics and quality equivalent to a product originally developed under a 10 CFR 50 Appendix B program. This is referred to as the MELTAC Re-evaluation Program (MRP) (See Section 6.2). The App.B-based QAP governed the re-evaluation of the previous MELTAC platform development, and governs all new MELTAC platform development or revisions that occur after this re-evaluation. The MRP (i.e.: one-time commercial grade dedication) established a baseline to demonstrate that the MELTAC platform has suitable technical characteristics and quality for nuclear safety applications in the U.S. MELTAC is now maintained as a 10 CFR Appendix B product.

MELCO has undergone an inspection by NRC to verify the implementation of an adequate QA program in compliance with the requirements of 10 CFR 50 Appendix B and 10 CFR 21 in support of digital I&C development activities. The results of this NRC inspection are documented in NRC Inspection Report NO. 99901410/2011-202 (ADAMS Accession number ML12013A353). In this Inspection Report, the NRC inspection team concluded that MELCO is generally effective in implementing its QA and 10 CFR 21 programs in support of the MELTAC platform development. It states that “the NRC inspectors determined that MELCO’s commercial grade dedication process adequately identified and verified the critical characteristics of the MELTAC platform that provide assurance that the platform will perform its safety function satisfactorily”. In addition, it states that “the NRC inspectors determined that the process implemented by MELCO is consistent with regulatory requirements associated with software development”.

### 6.1 MELTAC Platform Life Cycle Plans and Activities

This section describes key elements of the life cycle process for the basic components (software and hardware) of the MELTAC platform, based on the App.B-based QAP.

#### 6.1.1 Overview of the MELTAC Quality Assurance Program

The MELCO procedures applicable to software encompass the basic software, which includes the firmware and FPGAs on all MELTAC modules.

The MELCO procedures, processes and software life cycle for nuclear safety-related activities (hardware and software) comply with the applicable requirements given in Section 3 of this Topical Report, the “MELTAC Platform Software Program Manual” (JEXU-1041-1016), referred to here as SPM, 10 CFR 50 Appendix B, and ASME NQA-1-1994.

The SPM provides the generic plans that are followed under MELCO’s App.B-based QAP for all activities related to the basic software life cycle conducted after the MRP. The SPM complies with the guidance of BTP 7-14 “Guidance on Software Reviews for Digital Computer-

based Instrumentation and Control Systems”. A summary of the basic software life cycle plans and activities is given in Table 6.1-1.

The QAP and software life cycle for plant specific nuclear safety-related system implementation (hardware and application software) is not described in this report.

**Table 6.1-1 MELTAC Life Cycle Plan/Activity Summary**


Note:

MELTAC uses FPGAs only for dedicated functions, such as communication controllers. These FPGAs are not programmable for application dependent functions. Therefore, the same FPGAs are applied to all MELTAC applications.

Consistent with the practices defined in NUREG/CR-7006, MELCO does not view FPGA development as hardware, but rather applies a complete life cycle development process equivalent to software development, to achieve readable, traceable and verifiable FPGA components. Details are described in the SPM.

[illegible]








### **6.1.2 Secure Development Environment Management**

The Secure Development Environment Management Program for the basic software complies with RG 1.152 as described in the SPM. The overall Secure Development Environment Management Program ensures:

- 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.  
This is described in further detail in Section 6.1.2.3.

These processes are applicable to the basic software and related documentations. The compliance assessment for the MELTAC platform and its life cycle development process, relative to RG 1.152, is provided in the SPM.

The security measures in the development process of the application software are described in the Application Licensing Document.

#### **6.1.2.1 Development/Storage Security Measures of the basic software**

[

]



**Figure 6.1-1 Security Measures of the Software Development/Storage Environment**

[

]

Table 6.1-2 Security Measures of the Software Development/Storage Environment


[

]

6.1.2.2 Security Measures in Each Phase of Development Process

The security measures shown in Table 6.1-3 ensure that no unintended code can be introduced during the development process.

Table 6.1-3 Security Measures in the Software Development Process





**6.1.2.3 Secure Development Environment Measures During System Operation**

[

]

**6.1.3 Operations**

[

]

**Table 6.1-4 Information Provided in the MELTAC Maintenance Manuals**


Licensees may supplement the instructions in the MELTAC Maintenance Manuals with plant specific procedures and instructions

**6.1.4 Training**

MELCO supports training that assists customers in understanding the operation and proper use of the MELTAC platform.

This training is comprised of lecture classes and hands-on training using actual MELTAC equipment. The typical training course contents are shown below:

[

1  
Additional application specific training is described in application specific documentation.

6.1.5 Maintenance

6.1.5.1 Hardware

The following hardware measurements and adjustments (as needed) are recommended on a periodic basis, once every operating cycle or every 24 months, whichever is shorter.

Table 6.1-5 Hardware Maintenance


6.1.5.2 Software

This section describes the upgrade process for the basic software. Upgrades or changes to application software are described in application level documentation

Table 6.1-6 Software Maintenance



### 6.1.6 Obsolescence Management

This section describes the obsolescence management program for the MELTAC platform. MELCO uses hardware parts which have excellent production continuity. Regardless, the product service life for nuclear applications covers 20 to 30 years, so it is inevitable that many parts will become unavailable. The following sections summarize the process used to determine the availability of parts and the process used to evaluate and utilize different parts for substitution. All changes to the MELTAC platform are done under the MELCO App.B-based QAP

The parts substitution method described in this section is primarily applicable to the obsolescence management. However, MELCO will also use the same method of parts substitution to ensure adequate parts supply from multiple sources to accommodate supply management issues or production peaks.

#### 6.1.6.1 Obtaining Information on Part Availability

[

]

#### 6.1.6.2 Selecting Replacement Parts

[

]

#### **6.1.6.3 Verification after Replacement**

[

]

#### **6.1.7 Identification**

[



]

#### **6.1.8 Reliability Database**

[

]

**6.2 MELTAC Re-evaluation Program (MRP)**

[

]

**6.3 MELTAC Engineering Tool Life Cycle**

The MELTAC engineering tool was developed and is managed under the MELCO QAP for non-safety items (Complies with ISO 9001). This is acceptable because the MELTAC engineering tool is not credited for any safety-related functions..

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.

## 7.0 EQUIPMENT RELIABILITY

The following sections describe methods and conditions to assess the reliability of each MELTAC module, which are required to assess the reliability of any safety-related system where MELTAC platform is applied.

Mean Time Between Failures (MTBF) values and failure rates of MELTAC modules are also described in the following sections (see Table 7.1-1). These values are more conservative than the actual failure records in Japanese nuclear plants. An example is shown below.

Regarding the CPU Module and peripheral modules, a typical subsystem failure rate, which is composed of many modules, is more than 15,000 Failure In Time (FIT) based on Table 7.1-1 . However, the FIT for similar configuration of safety-related controllers and safety VDUs in Japanese nuclear plants is about 100. The calculated result predicts that a failure should occur at least once a month. However, the operating subsystems have failed less than once a year.

## 7.1 Mean Time between Failures (MTBF) Analysis

MTBF shown in Table 7.1-1 is calculated for each MELTAC module based on MIL-HDBK-217F NOTICE 2. These values are used to assess the reliability of the entire MELTAC platform for each system, as explained in Section 7.2.

MTBF is calculated from the sum of the failure rates of the components which make up each module, and the reciprocal of the module's failure rate is thus obtained. In MIL-HDBK-217F, the failure rate is defined for each type of component with consideration given to operating conditions and reliability factors. Therefore, it represents a generic reliability assessment technique. The following environmental conditions were used in the calculation.

[

]

The MTBF of each module is shown Table 7.1-1.

Table 7.1-1 provides the calculated FIT and MTBF for each MELTAC module. If a module is updated, the FIT and MTBF will be calculated using the same method and reliability will be demonstrated. The same method of calculating the FIT and MTBF will also be used for any new modules. The impact on the reliability of the entire controller due to the introduction of any new modules is evaluated as describe in Section 7.2.

Table 7.1-1 Failure Rate of Modules



Note:  
FIT (Failure In Time) rate is used to indicate the failure rate. 1 FIT = 1X10<sup>-9</sup>(/hour).

## 7.2 Controller Reliability Analysis

The failure rate of any safety-related system where MELTAC platform is applied as a whole, depends on the configuration of the entire system. Variations for each application include:

- The number and configuration of redundant divisions
- The number and configuration of controllers within each division
- The redundancy within each controller
- The configuration of I/O modules and Communication Interface Modules and the significance of these interfaces to the safety function (i.e.: the safety function logic design)

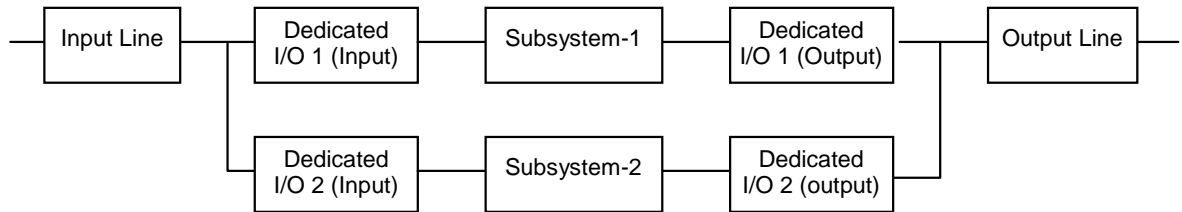
This section describes a method used to determine the reliability of a generic redundant parallel controller. The method for single controller architecture can be extrapolated from this method.

The controller reliability analysis is performed as follows.

- A reliability model for the system's safety function is generated
- The fault tree analysis (FTA) of this reliability model is performed to determine the frequency of:
  - Spurious actuation of the safety function
  - Failure to actuate the safety function

The reliability model of a simple system is shown in Section 7.2.1. As an example of the reliability analysis process, Figure 7.2-2 shows the fault tree for spurious actuation of the safety function. The FTA for spurious actuation is explained below.

### 7.2.1 Reliability Model



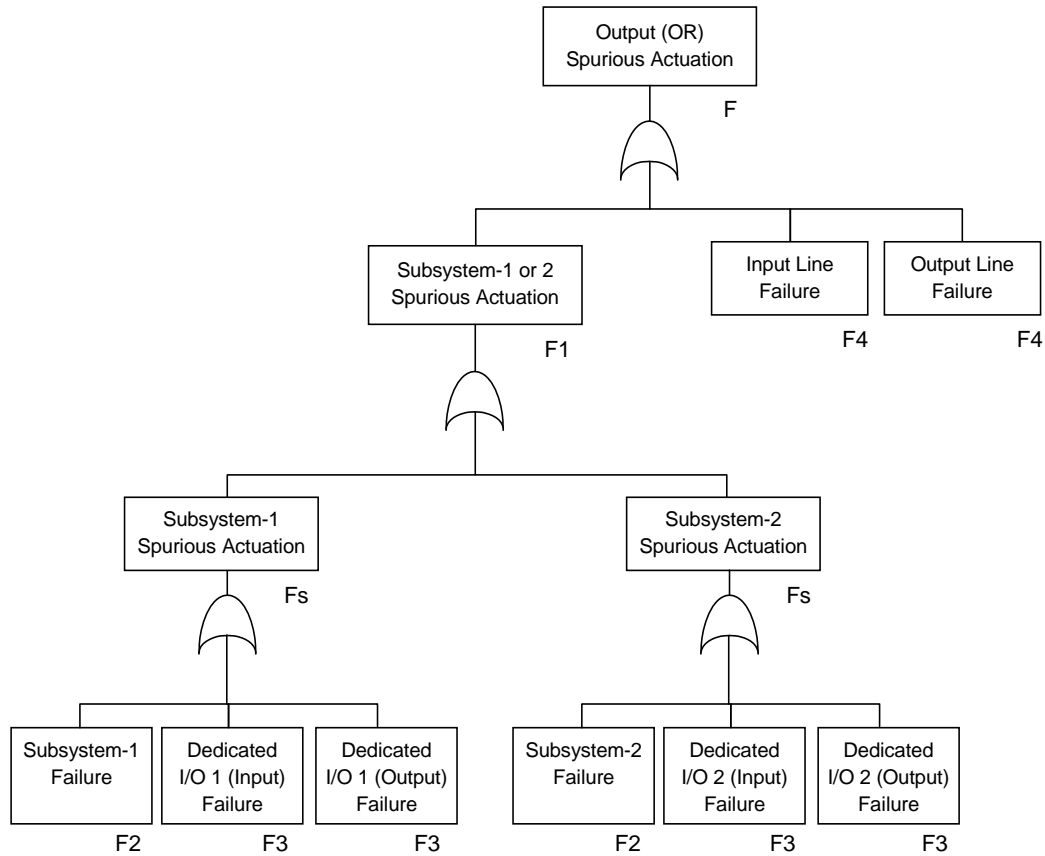
**Figure 7.2-1 Reliability Model**

The above figure shows the reliability model of a redundant parallel controller, which contains one input module and one output module in each subsystem.

In the reliability model, the Status Display Module is not contained in the subsystem, because the Status Display Module only displays the current state of the subsystem and its failure does not affect the safety function of the subsystem. The Control Network I/F Module and the Optical Switch Module are not contained in this simplified system. They would be included, depending on how the data from the Control Network is used in the application software. This also applies to the Data Link interface from the Bus Master Modules.



### 7.2.2 FTA of Spurious Actuation of the Safety Function



**Figure 7.2-2 Fault Tree for Output Failure Spurious Actuation**

Regarding the cause of spurious actuation, the failure rate is described below.

$$F = F1 + F4 + F4$$

$$F1 = Fs + Fs$$

$$Fs = F2 + F3 + F3$$

Failure rate  $F_i$  ( $i = 1, 2, 3 \dots$ ) causes spurious action of each module or subsystem and is defined below.

$$F_i = \lambda_i \times (1 - P_i)$$

$\lambda_i$  = failure rate

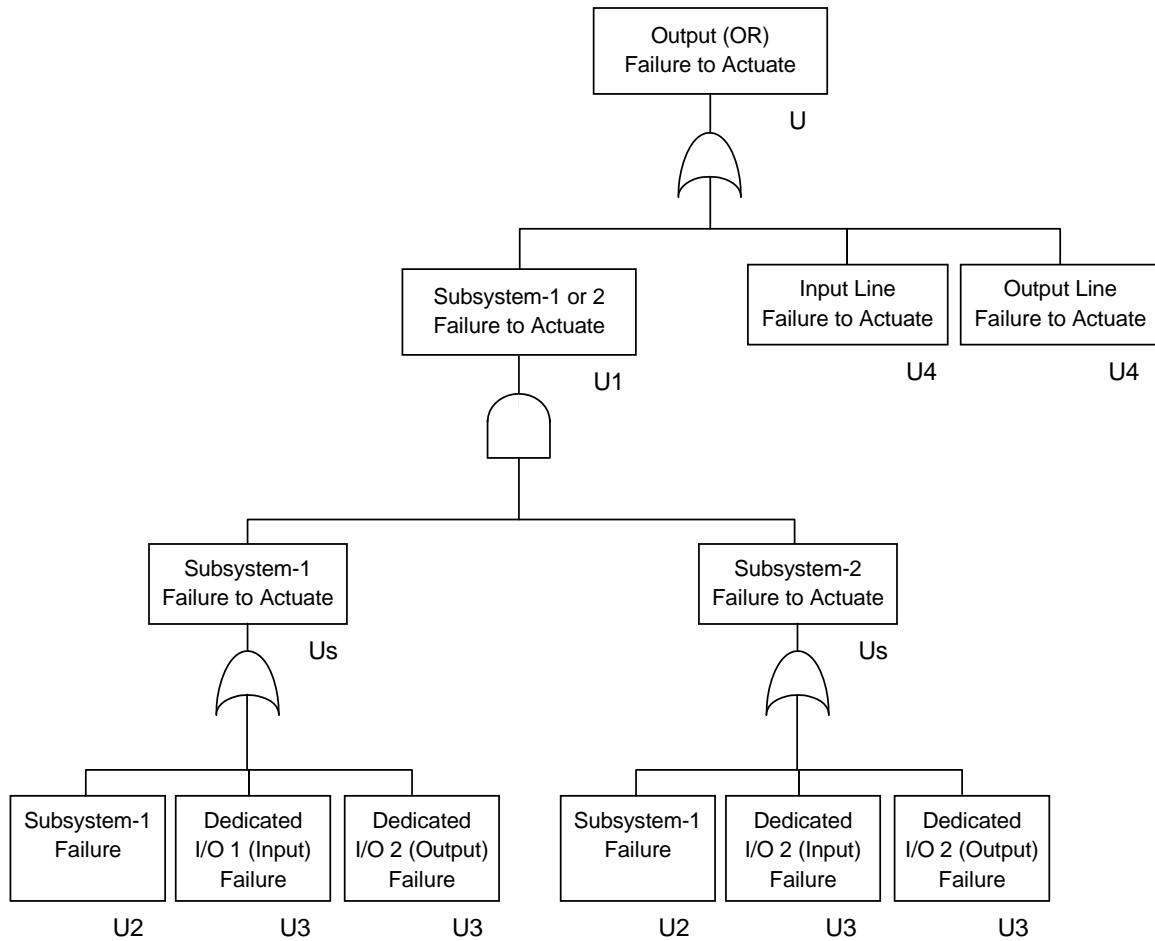
$P_i$  = probability of detecting the failure which affects the safety function through self-diagnosis

Calculations of  $F2$ ,  $F3$  and  $F4$  are described in Sections 7.2.4.1, 7.2.4.2 and 7.2.4.3.

The failure rates of the Input Line and the Output Line are the same, because they consist of the same module and unit.

This FTA model assumes this very simple system, in which an input directly affects a system output. Systems with more complex logic may validate inputs (e.g.: voting) within the application logic so that spurious actuation requires multiple input failures.

### 7.2.3 FTA of Failure to Actuate the Safety Function



**Figure 7.2-3 Fault Tree for Failure to Actuate**

Regarding the cause of failure to actuate, unavailability is described below.

$$U = U1 + U4 + U4$$

$$U1 = Us \times Us$$

$$Us = U2 + U3 + U3$$

$U_i$  is the unavailability of each module or subsystem and is defined below.

$$U_i = 1 - \text{MTBF} / (\text{MTBF} + (1 - P_i) \times (T_i / 2) + \text{MTTR})$$

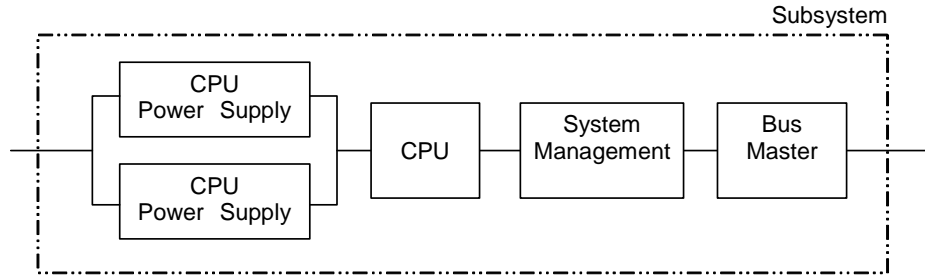
$T_i$  = Manual test interval

$$\text{MTBF} = 1 / \lambda_i$$

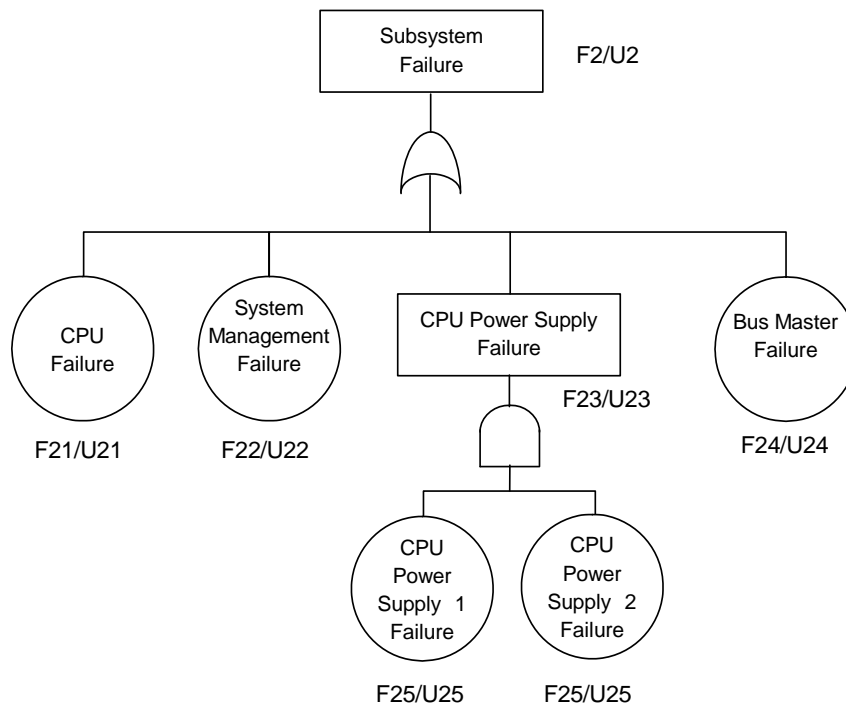
$T_i$  and Mean Time To Repair (MTTR) are unique to each application.

## 7.2.4 Detailed Controller Reliability Analysis

### 7.2.4.1 Subsystem



**Figure 7.2-4 Reliability Model of Subsystem**



**Figure 7.2-5 Fault Tree of Subsystem**

The failure rate of the subsystem (F2) is defined as follows.

$$F2 = F21 + F22 + F23 + F24$$

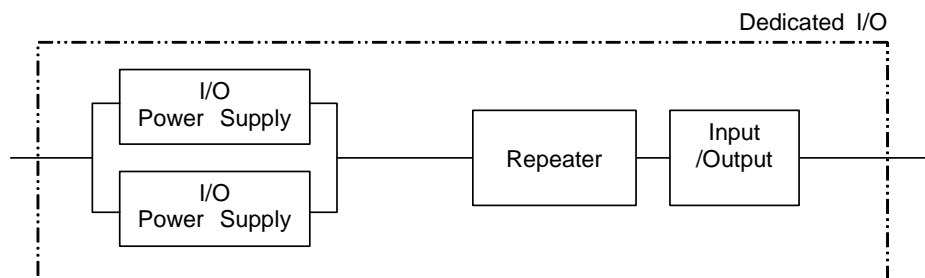
$$F23 = F25 \times F25 \times \text{MTTR} \times 2$$

The unavailability of subsystem (U2) is defined as follows.

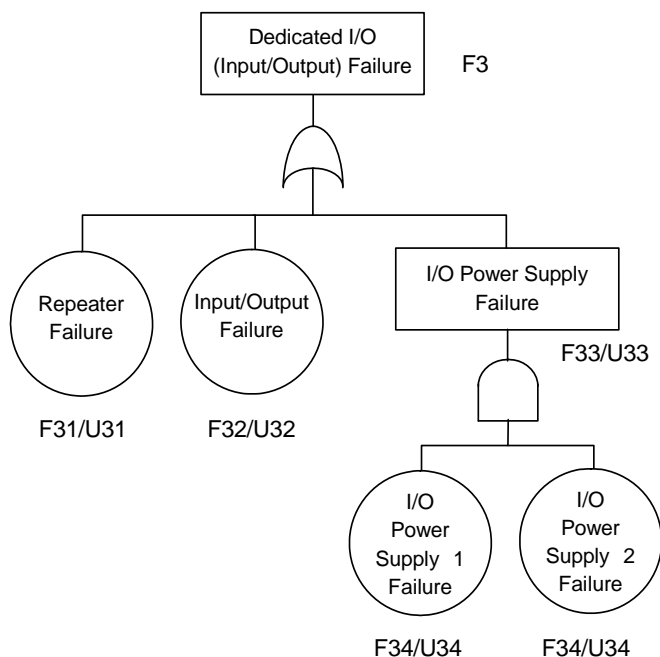
$$U2 = U21 + U22 + U23 + U24$$

$$U23 = U25 \times U25$$

### 7.2.4.2 Dedicated I/O (Input/Output)



**Figure 7.2-6 Reliability Model of Dedicated I/O**



**Figure 7.2-7 Fault Tree of Dedicated I/O**

The failure rate of the subsystem (F3) is defined as follows.

$$F3 = F31 + F32 + F33$$

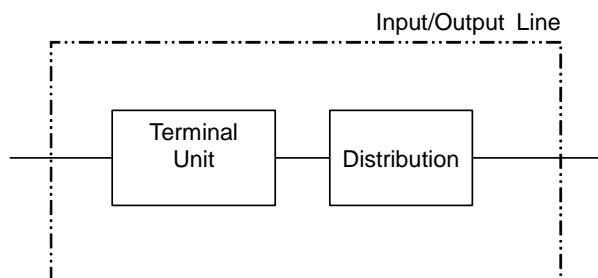
$$F33 = F34 \times F34 \times \text{MTTR} \times 2$$

The unavailability of the subsystem (U3) is defined as follows.

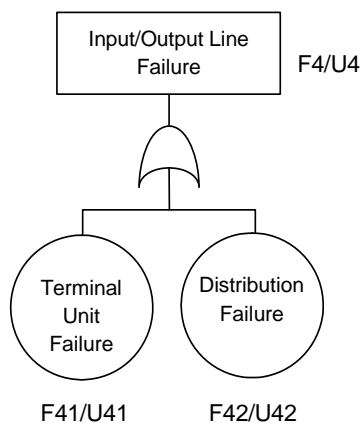
$$U3 = U31 + U32 + U33$$

$$U33 = U34 \times U34$$

### 7.2.4.3 Input/Output Line



**Figure 7.2-8 Input/Output Line**



**Figure 7.2-9 Fault Tree of Input/Output Line**

The failure rate of the subsystem (F4) is defined as follows.

$$F4 = F41 + F42$$

The unavailability of the subsystem (U4) is defined as follows.

$$U4 = U41 + U42$$

### 7.3 Failure Mode and Effect Analysis (FMEA)

This section describes the process of conducting the FMEA, which is a method of determining the failure mode for each type of MELTAC module and the resulting effects to the controller.

The steps for conducting the FMEA are as follows:

- Divide module circuits into function blocks
- Determine failure modes of the function blocks
- Determine the state(s) of the module output(s) caused by the failure mode(s) of the function blocks
- Determine the effects to the controller based on the states of the module output failures

For a module acceptable for use in the CPU Chassis, failures in the function blocks that may affect the control function must be detected either by the self-diagnosis function inside the module or through a combination of modules.

Parts which do not affect the safety function, such as the RS-232C communication port which is used only for CPU Module debugging, are identified through the FMEA.

For a module acceptable for use in the I/O Chassis, failures in the parts that may affect the control function must be detected either by the self-diagnosis function of the CPU Module or by the application software. For instance, if the Relay Output Module's relay contact suffers a seizure failure, it cannot be detected by the self-diagnosis function of the controller. However, this failure can be detected by the application software when the component is actuated either automatically or manually.

The FMEA method and acceptance criteria described in this section apply to all MELTAC modules.

#### **7.4 Equipment (Parts) that Require Periodic Replacement to Maintain Reliability**

The failure rates of each MELTAC module are shown in Section 7.1 (see Table 7.1-1). However, the following 3 components of the MELTAC modules have limited service life and need to be replaced periodically to maintain the reliability of MELTAC.

- a) Capacitor within power supplies
- b) Fan fuses
- c) Liquid crystal display within safety VDU panel

For item a), the entire power supply module need to be replaced. For item b), the fuses inside the Fan Unit need to be replaced but it is not necessary replace the entire Fan Unit. For item c), the entire safety VDU panel needs to be replaced. Parts may be replaced at any time while the equipment is energized or de-energized. Restrictions on on-line replacement are governed only by specific plant applications.

The parts that require periodic replacement are listed in Table 7.4-1. When components are updated or new components are added, the requirements for periodic parts replacement will be re-evaluated.

**Table 7.4-1 List of Parts that Require Periodic Replacement**


For the power supplies, the estimated service life of the internal electrolytic capacitor is calculated based on the Arrhenius equation. For fuses used in the fan assemblies, the estimated service life is determined based on the condition under which the fuses are actually used.

The replacement intervals for the components listed above are determined based on the estimated life of subparts. The estimated life of the subparts is shorter than the life that is provided in the catalog, in order to reinforce the reliability of the safety-related system where MELTAC platform is applied.

The components listed above have failure mechanisms related to aging. However, these aging mechanisms do not significantly affect the equipment's susceptibility to failure during the equipment qualification tests described in Section 5. Therefore, there is no age-related preconditioning prior to the qualification tests.

Other components used in the MELTAC platform do not have any known age-related failure mechanisms. Therefore, replacement only takes place when a failure occurs.



## APPENDIX A HARDWARE SPECIFICATION

The modules described here are used for safety systems.

Module types and specifications in this appendix represent current MELTAC modules at the time of this document revision. Module types and specifications will change as the product life cycle progresses. New modules will retain the functional features, performance specifications and reliability of current modules.

### A.1 CPU Module Specification

**Table A.1 CPU Module Specification**

Item	Specification
Module Type	PCPJ
Memory	DDR-SDRAM: 128 Mbytes SRAM: 512 kbytes F-ROM for application software: 64 Mbytes F-ROM for basic software: 32 Mbytes
External dimensions	11.4×10.4×0.98 inch (290×265×25 mm)
Hot-swapping	Power supply must be disabled when unplugging the module.

### A.2 System Management Module Specification

**Table A.2 System Management Module Specification**

Item	Specification
Module Type	PSMJ
Communication between redundant subsystems	Optical module transmission speed: 100 Mbps
System DI	Number of inputs: 32 Rated voltage: 24 V (30 V, maximum) external supply Contact current: 3 mA Dielectric voltage: AC 500 V
System DO	Number of outputs: 8 Rated voltage: 24 V (30 V, maximum) external supply Rated current: 50 mA (100 mA, maximum) Dielectric voltage: AC 500 V
Onboard memory	2-port memory: 1 Mbyte Dedicated transmission memory: 1 Mbyte Dedicated receiving memory: 1 Mbyte DDR-SDRAM: 128 Mbytes F-ROM for Firmware: 32 Mbytes
Firmware	Firmware is mounted on the F-ROM. It executes Maintenance Network communication function.
Ethernet Interface	Module Chassis, rear side: 10 Mbps, 1ch Module front side: 100 Mbps/10 Mbps (Speed: Automatically switched), 2 channels (UTP cable) Module front side: 100 Mbps, 1 channel (optical fiber)
External dimension	11.4×10.4×0.79 inch (290×265×20 mm)
Hot-swapping	Power supply must be disabled when unplugging the module.

**A.3 Bus Master Module Specification****Table A.3 Bus Master Module Specification**

Item	Specification
Module Type	PFBJ
Protocol	1:N master polling (Case of Communication with I/O) One way communication (Case of Data Link communication)
Configuration	Number of channels: 4 channels/module (I/O or serial Data Link communication can be defined for each channel.)
Interface	RS-485 transformer insulation.
Baud rate	1 Mbps
Error detection	CRC method
Transmission capacity	1 kbyte/channel, maximum (Case of Communication with I/O) 3 kbyte/channel, maximum (Case of Data Link communication)
Onboard memory	Dedicated transmission memory: 1 Mbyte (256 kbyte/channel)
External dimension	11.4 x10.4 x1.18 inch (290x265x30 mm)
Hot-swapping	Power supply must be disabled when unplugging the module.

**A.4 Control Network I/F Module Specification****Table A.4 Control Network I/F Module Specification**

Item	Specification
Module Type	PWNJ
Protocol	Communication method: Cyclic Multiplexing method: RPR (Resilient Packet Ring) IEEE Std. 802.17
Configuration	Loop (redundant)
Medium	Optical fiber
Speed	Transmission rate: 1 Gbps
Capacity	Transmission capacity: <ul style="list-style-type: none"> <li>- 256 kbytes, maximum for normal speed communication</li> <li>- 128 kbytes, maximum for high speed communication</li> </ul> Number of connected stations: <ul style="list-style-type: none"> <li>- 126 stations, maximum for normal speed communication</li> <li>- 32 stations, maximum for high speed communication</li> </ul> Distance between stations: <ul style="list-style-type: none"> <li>- 2 km, maximum</li> </ul>
Firmware	Firmware is mounted on the F-ROM. It executes Control Network communication function.
External dimension	11.4 x10.4 x1.18 inch (290x265x30 mm)
Error detection	CRC method
Hot-swapping	Power supply must be disabled when unplugging the module.

**A.5 I/O Module Specification****Table A.5 Analog Input Module Specification**

Module Type	Description	Specification
MLPJ	Current input	AI: 1 input/module 4 to 20 mA (Transmitter power supply is provided.) Input impedance: 10 M $\Omega$ or greater Accuracy*: $\pm 0.25$ %FS Temperature coefficient: $\pm 50$ ppm/ $^{\circ}$ C Firmware: mounted on the F-ROM.
MAIJ	Voltage input	AI: 1 input/module 0 to 10 V Input impedance: 10 M $\Omega$ or greater Accuracy*: $\pm 0.25$ %FS Temperature coefficient: $\pm 50$ ppm/ $^{\circ}$ C Firmware: same as MLPJ
MRTJ	RTD 4 line type	AI: 1 input/module 4-line Pt200 $\Omega$ , 32 to 752 $^{\circ}$ F (0 to 400 $^{\circ}$ C) Input impedance: 10 M $\Omega$ or greater Accuracy*: $\pm 0.25$ %FS Temperature coefficient: $\pm 50$ ppm/ $^{\circ}$ C Firmware: same as MLPJ
		AI: 1 input/module 4-line Pt200 $\Omega$ , 500 to 662 $^{\circ}$ F (260 to 350 $^{\circ}$ C) Input impedance: 10 M $\Omega$ or greater Accuracy*: $\pm 0.25$ %FS Temperature coefficient: $\pm 50$ ppm/ $^{\circ}$ C Firmware: same as MLPJ

**Table A.5 Analog Input Module Specification**

Module Type	Description	Specification
MRTJ	RTD 4 line type	AI: 1 input/module 4-line Pt100 $\Omega$ , 32 to 212 °F (0 to 100 °C) Input impedance: 10 M $\Omega$ or greater Accuracy*: $\pm 0.25$ %FS Temperature coefficient: $\pm 50$ ppm/°C Firmware: same as MLPJ
		AI: 1 input/module 4-line Pt100 $\Omega$ , 32 to 392 °F (0 to 200 °C) Input impedance: 10 M $\Omega$ or greater Accuracy*: $\pm 0.25$ %FS Temperature coefficient: $\pm 50$ ppm/°C Firmware: same as MLPJ
MTCJ	Thermocouple K type	AI: 1 input/module 32 to 2372 °F (0 to 1300 °C) Input impedance: 10 M $\Omega$ or greater Accuracy*: $\pm 0.5$ %FS Temperature coefficient: $\pm 350$ ppm/°C Firmware: same as MLPJ
		AI: 1 input/module 32 to 752 °F (0 to 400 °C) Input impedance: 10 M $\Omega$ or greater Accuracy*: $\pm 0.25$ %FS Temperature coefficient: $\pm 350$ ppm/°C Firmware: same as MLPJ

\* A 16 bit successive approximation type A/D converter is applied to the Analog Input Module. The rounding error of 16 bit sampling is approximately 1E-3 %FS. This is negligible compared to the accuracy of the input device of the Analog Input Module which is 0.25 %FS, as described in the table above.

Consideration of cumulative error, which is a problem when integrating type A/D converters, is not necessary.

**Table A.6 Analog Output Module Specification**

Module Type	Description	Specification
MAOJ	Current output	AO: 1 output/module Maximum load: 600 $\Omega$ Accuracy: $\pm 0.25$ %FS Firmware: mounted on the F-ROM.
MVOJ	Voltage output	AO: 1 output/module Minimum load: 500 $\Omega$ Accuracy: $\pm 0.25$ %FS Firmware: same as MAOJ

**Table A.7 Digital Input Module Specification**

Module Type	Description	Specification
MDIJ	Contact input (built-in contact power supply)	DI: 4 inputs/module Contact impressed voltage: DC 48 V Contact current: 10 mA

**Table A.8 Digital Output Module Specification**

Module Type	Description	Specification
MDOJ	Relay contact output	DO: 4 outputs/module, normally open contact Rated load (resistive load) : AC 220 V 0.5 A, AC 110 V 0.5 A DC 110 V 0.1 A, DC 125 V 0.1 A
	Semiconductor output (open collector)	DO: 2 outputs/module (power DO) Maximum impressed voltage: AC110 V/DC125 V Output current: 1 A (continuous) 6 A (100 ms) 10 A (20 ms)

**Table A.9 Pulse Input Module Specification**

Module Type	Description	Specification
MPIJ	Pulse input (for RCP rotation speed input)	Input: 1 input/module Pulse amplitude: $\pm 0.5$ to $\pm 60$ V Measurement range: 100 to 1500 rpm

**A.6 Isolation Module and Distribution Module Specification****Table A.10 Isolation Module Specification**

Module Type	Description	Specification
KILJ	Current input, Current/Voltage output	AI: 1 input/module 4 to 20 mA Input impedance: 10 M $\Omega$ or greater Accuracy: $\pm 0.5$ %FS Temperature coefficient: $\pm 100$ ppm/ $^{\circ}$ C AO: 1 output/module 4 to 20 mA / DC 0 to 10 V (selectable)
KIRJ	RTD 4 line type input Current/Voltage output	AI: 1 input/module 4-line Pt100 $\Omega$ , 32 to 302 $^{\circ}$ F (0 to 150 $^{\circ}$ C) 4-line Pt100 $\Omega$ , 32 to 392 $^{\circ}$ F (0 to 200 $^{\circ}$ C) 4-line Pt200 $\Omega$ , 32 to 752 $^{\circ}$ F (0 to 400 $^{\circ}$ C) Input impedance: 10 M $\Omega$ or greater Accuracy: $\pm 0.5$ %FS Temperature coefficient: $\pm 100$ ppm/ $^{\circ}$ C AO: 1 output/module 4 to 20 mA / DC 0 to 10 V (selectable)
KIPJ	Pulse signal input (for RCP)	Input: 1 (Pulse signal) Output: 2 (Pulse signal) Output pulse width: about 10 ms Output voltage: 10 V $\pm$ 1 V or output of open collector



**Table A.11 Distribution Module Specification**

Module Type	Description	Applicable I/O Modules
KIOJ	For Digital I/O	MDIJ MDOJ
KLPJ	For Current input (Active)	MLPJ
	For Current input (Passive)	MLPJ
KRTJ	For RTD input (4 wire)	MRTJ
KTCJ	For Thermocouple input	MTCJ
KAIJ	For Voltage input	MAIJ
KAQJ	For Current output	MAQJ
KVOJ	For Voltage output	MVOJ
KAIJ	For Pulse signal input (for RCP)	MPIJ

**A.7 E/O Converter Module Specification****Table A.12 E/O Converter Module and Device Specification**

Module Type	Description	Specification
MEOJ	Electrical/Optical conversion	Electrical to Optical: 1 channel Optical to Electrical: 1 channel Electrical interface: RS-485 Optical signal: Multi mode optical fiber
		Electrical to Optical: 1 channel Optical to Electrical: 1 channel Electrical interface: RS-232C Optical signal: Multi mode optical fiber

**A.8 Power Interface Module Specification****Table A.13 Power Interface Module Specification**

Module Type	Description	Specification
DPOJ	Semiconductor output (open collector)  Contact input (built-in contact power supply)	DO: 2 outputs/module (power DO) Rated voltage: AC 120 V/DC 125 V Output current: DC 1.5 A (continuous) AC 2.0 A <sub>rms</sub> (continuous) 16 A <sub>0-P</sub> (100 ms) 2.5 A <sub>0-P</sub> (1 s) DI: 8 inputs/module Contact impressed voltage: DC 48 V Contact current: 10 mA

**A.9 Power Supply Module Specification****Table A.14 Power Supply Module Specification**

Module Type	Description	Specification
PS	CPU Power Supply	Input voltage: AC 85 to 140 V Frequency: 47 Hz to 63 Hz Output voltage: DC 5 V (50 A), DC 2.1 V (11 A)
	I/O Power Supply	Input voltage: AC 85 to 140 V Frequency: 47 Hz to 63 Hz Output voltage: DC 24 V (12 A)
PPSJ	CPU Power Supply (Small capacity type)	Input voltage: AC 85 to 140 V Frequency: 47 Hz to 63 Hz Output voltage: DC 5 V (30A), DC 2.1 V (11 A) Mounted inside Mirror-split Chassis
	CPU Power Supply (Large capacity type)	Input voltage: AC 85 to 140 V Frequency: 47 to 63 Hz Output voltage: DC 5 V (60 A), DC 2.1 V (11 A) Mounted inside Non-split CPU Chassis

**A.10 Safety VDU Panel Specification****Table A.15 Safety VDU Panel Specification**

Item	Specification
Module Type	T10DH
Type	Thin Film Transistor Liquid Crystal Display (TFT LCD) module
Operator Interface	Touch interface (non-pressure-sensitive type)
Communication Interface	<ul style="list-style-type: none"> <li>- Safety VDU processor to panel Display signal : RGB, Horizontal Sync (HSYNC), Vertical Sync (VSYNC)</li> <li>- Safety VDU panel to processor RS-232C electrical or optical fiber with E/O,O/E converters</li> </ul>

**A.11 FMU Module Specification****Table A.16 FMU Module Specification**

Item		Specification
Module Type		PFDJ
Graphic	Picture Size	SVGA (800*600) (Case of Analog signal)
	Interface	D-SUB type (Case of Analog signal) DVI type (Case of Digital signal)
	Memory	64 Mbytes
Touch Panel Interface	Configuration	1:1 serial interface
	Interface	RS-232C (With optical conversion function, Transmission distance: Less than 2 km)
	Baud rate	76.8 kbps, maximum
	Capacity	Transmission capacity : 2 kbytes (Number of channels : 1)
Hot-swapping		Power supply must be disabled when unplugging the module.

**A.12 NI Module Specification****Table A.17 NI Module Specification**

Module Type	Description	Specification
NFAN	Pre Amplifier	Input: Current pulse signal (1 input/module) Pulse amplitude: 40 dB Output: Voltage pulse signal (1 output/module) For SR <sup>*1</sup> Unit outside of NI cabinet
		Input: Current pulse signal (1 input/module) Pulse amplitude: 40 dB Output: Voltage pulse signal (1 output/module) For WR <sup>*4</sup> Unit outside of NI cabinet
NHBN	Pulse Amplifier	Input: Voltage pulse signal (1 input/module) Pulse amplitude: 40 dB Output: Voltage pulse signal (1 output/module) For SR <sup>*1</sup>
		Input: Voltage pulse signal (1 input/module) Pulse amplitude: 40 dB Output: Voltage pulse signal (1 output/module) For WR <sup>*4</sup>
NHCN	Discrimination	Input: Voltage pulse signal (1 input/module) Discrimination level: Settable within the range of DC 0 to 5 V Output: Voltage pulse signal (1 output/module), DC 10 <sup>-10</sup> to 10 <sup>-4</sup> A (1 output/module) For SR <sup>*1</sup> , WR <sup>*4</sup>
NHDN	Logarithmic Amplifier	Input: DC 10 <sup>-10</sup> to 10 <sup>-4</sup> A (1 input/module) Output: DC 0 to 10 V (1 output/module) For SR <sup>*1</sup>
		Input: DC 10 <sup>-10</sup> to 10 <sup>-4</sup> A (1 input/module) Output: DC 0 to 6.667 V (1 output/module) For WR <sup>*4</sup>
NDAN	Signal Processing	Input: DC 0 to 10 V (1 input/module), DC 0 to 500 $\mu$ A (1 input/module) Contact impressed voltage: DC 24 V (2 input/module) Communication interface: RS-485 transformer insulation (6 channels/module) Firmware: mounted on the F-ROM. It executes analog/digital conversion and communication function. For SR <sup>*1</sup>
		Input: DC 0 to 10 V (1 input/module), DC 0 to 500 $\mu$ A (1 input/module), DC 0 to -500 $\mu$ A (1 input/module) Contact impressed voltage: DC 24 V (2 inputs/module) Communication interface: RS-485 transformer insulation (6 channels/module) Firmware: mounted on the F-ROM. It executes analog/digital conversion and communication function. For IR <sup>*2</sup>

**Table A.17 NI Module Specification**

Module Type	Description	Specification
NDAN	Signal Processing	Input: DC 0 to 10 V (2 inputs/module), DC 0 to 500 $\mu$ A (1 input/module) Contact impressed voltage: DC 24 V (2 inputs/module) Communication interface: RS-485 transformer insulation (6 channels/module) Firmware: mounted on the F-ROM. It executes analog/digital conversion and communication function. For PR <sup>*3</sup>
NDCN	Operation Panel	Communication interface: RS-485 transformer insulation (1 channel/module) Output: DC 0 to -12 V (for Log Amp test signal), DC 0/24 V (for Pre Amp test and Pulse Amp test signal) For SR <sup>*1</sup>
		Communication interface: RS-485 transformer insulation (1 channel/module) Output: DC 0 to 24 V (for Log Amp test signal, 8 outputs/module), DC 0/24 V (for test signal range select, 5 outputs/module) For IR <sup>*2</sup>
		Communication interface: RS-485 transformer insulation (1 channel/module) Output: DC 1 to 5 V (for I/E Converter test signal, 2 outputs/module), DC 0/24 V (for test signal range select, 16 outputs/module) For PR <sup>*3</sup>
NHEN	High Voltage Cut Off Circuit Card	Contact impressed voltage: DC 24 V (4 inputs/module) Input voltage: AC 103.5 to 126.5 V Output voltage: AC 103.5 to 126.5 V For SR <sup>*1</sup>
NFTN	Test Signal Generator	Input: DC 0/24 V (4 inputs/module) Output: Voltage pulse signal (Output either 60, 10 <sup>3</sup> , 10 <sup>5</sup> or 10 <sup>6</sup> cps) For SR <sup>*1</sup>
		Output: Voltage pulse signal (Output either 10 <sup>5</sup> , 10 <sup>7</sup> or 10 <sup>9</sup> cps for Campbell circuit test), Voltage pulse signal (Output either 10, 10 <sup>3</sup> , 10 <sup>5</sup> or 10 <sup>6</sup> cps for Pulse circuit test) For WR <sup>*4</sup>
NHFN	Logarithmic Amplifier	Input: DC 10 <sup>-11</sup> to 5 $\times$ 10 <sup>-3</sup> A (1 input/module) Output: DC 0 to 10 V (1 output/module) For IR <sup>*2</sup>
		Input: DC 10 <sup>-7</sup> to 10 <sup>-3</sup> A (1 input/module) Output: DC 5.555 to 10 V (1 output/module) For WR <sup>*4</sup>
NHMN	Test Signal Generator	Input: DC 0 to 24 V (for Log Amp test signal, 8 inputs/module), DC 0/24 V (for test signal range select, 5 inputs/module) Output: DC 10 <sup>-11</sup> to 5 $\times$ 10 <sup>-3</sup> A (1 output/module) For IR <sup>*2</sup>

**Table A.17 NI Module Specification**

Module Type	Description	Specification
NLPN	Isolation Card	Input: DC 0 to 10 V (1 input/module) Output: DC 0 to 10 V (1 output/module) For IR <sup>*2</sup>
NDBN	I/E Converter	Input: DC 0 to 9 mA (max) Gain: Variable Output: DC 0 to 10 V For PR <sup>*3</sup>
NHVN	Detector Current Indicator	Input: DC 0 to 10 V (1 input/module) Display: Display 5 digits current value For PR <sup>*3</sup>
	Reactor Power Level Indicator	Input: DC 0 to 10 V (1 input/module) Display: Display 4 digits reactor power level value For PR <sup>*3</sup>
NHNN	Test Signal Generator	Input: DC 1 to 5 V (for I/E Converter test signal, 2 inputs/module), DC 0/24 V (for test signal range select, 8 inputs/module) Output: DC 0 to 10 mA, maximum (2 outputs/module) For PR <sup>*3</sup>
NFFN	Root Mean Square Converter	Input: Voltage pulse signal (1 input/module) Output: DC $10^{-7}$ to $10^{-3}$ A (1 output/module) For WR <sup>*4</sup>
NFHN	Mode Switching Card	Input: DC 0 to 6.667 V (1 input/module), DC 5.555 to 10 V (1 input/module) Output: Select one of above 2 points to output. For WR <sup>*4</sup>
NJAN	Power Supply for SR Detector	Input voltage: AC 103.5 to 126.5 V Frequency: 47 to 63 Hz Output voltage: DC 0 to 2500 V For SR <sup>*1</sup>
NJBN	Power Supply for IR Detector	Input voltage: AC 103.5 to 126.5 V Frequency: 47 to 63 Hz Output voltage: DC 0 to 1000 V For IR <sup>*2</sup>
	Power Supply for WR Detector	Input voltage: AC 103.5 to 126.5 V Frequency: 47 to 63 Hz Output voltage: DC 0 to 1000 V For WR <sup>*4</sup>
NHGN	Power Supply for IR Detector	Input voltage: AC 103.5 to 126.5 V Frequency: 47 to 63 Hz Output voltage: DC 0 to -200V For IR <sup>*2</sup>
NJCN	Power Supply for PR Detector	Input voltage: AC 103.5 to 126.5 V Frequency: 47 Hz to 63 Hz Output voltage: DC 0 to 1000 V For PR <sup>*3</sup>
501AJ0UN	Power Supply (NIS)	Input voltage: AC 103.5 to 126.5 V Frequency: 47 to 63 Hz Output voltage: DC 24.5 V (1 A)



**Table A.17 NI Module Specification**

Module Type	Description	Specification
NALN	Signal Comparator	Input: DC 0 to 10 V (1 input/module) Output: DC 0/24 V (1 output/module)
NHTN	Trip Bypass Switch	Operation switch: 3 switches for bypass operation Output: DC 0/24 V (Normal / Bypass) For SR <sup>*3</sup> and IR <sup>*2</sup>
NDHN	Summing Amplifier	Input: DC 0 to 6 mA (2 detector current inputs/module) DC 0 to 5 mA (2 test current signal inputs/module) Output: DC 0 to 10 V (as upper neutron flux level) DC 0 to 10 V (as lower neutron flux level) DC 0 to 10 V (as reactor power level) DC 0 to 10 V (as over power level) For PR <sup>*3</sup>
NHJN	Flux Level Change Rate Detection Circuit	Input: DC 0 to 10 V (as reactor power level) Output: DC -10 to +10 V (differential waveform) For PR <sup>*3</sup>
NHKN	Self-Holding Circuit	Operation switch: Close (for trip reset operation) Input: Open/DC 5 V (Trip signal) Close (for trip reset operation) Output: DC Over 20 V/Under 0.7 V (Normal/Holding) For PR <sup>*3</sup>
NBYN	Bypass Control Circuit	Input: Bypass permission Output: Bypass demand For PR <sup>*3</sup>
NOIN	E/O Converter	Electrical to Optical: 1 channel Optical to Electrical: 1 channel Electrical interface: RS-422 Optical signal: Multi mode optical fiber For PR <sup>*3</sup>

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

**A.13 RM Module Specification****Table A.18 RM Module Specification**

Module Type	Description	Specification
MUBN	Signal Converter (Analog)	Pulse to RS-485 converter Range: $10^7$ cpm, maximum
	Signal Converter (Pulse)	RS-485 to RS-485 protocol converter
MURN2	Repeater Card	RS-485 to O/E, E/O Converter
501AJOUR	Power Supply (RM)	Input voltage: AC 98 to 132 V Frequency: 47 to 63 Hz Output voltage: DC 12 V, DC $\pm 15$ V, DC 24 V

**A.14 Status Display and Switch Module Specification****Table A.19 Status Display and Switch Module Specification**

Module Type	Applicable System Configurations	Description
PPNJ	Single	Status Display: Displays the operation mode and status of representative alarm
	Redundant Parallel	
	Redundant Standby	Status Display: Displays the operation mode of Subsystem A/ B. Displays the status of representative alarm.  Subsystem Switching: Select which Subsystem, A or B, should be controlled in the Control Mode or Standby Mode.

**A.15 Repeater Module Specification****Table A.20 Repeater Module Specification**

Module Type	Function	Specification
MRPJ	Repeater	For Subsystem-A
	Repeater	For Subsystem-B
	Repeater	For Subsystem-A/B Double Size

**A.16 Module Chassis Specification****Table A.21 CPU Module Chassis Specification**

Module Type	Chassis Type	Applicable System Configuration	Number of Implementable Extension Modules <sup>*1</sup>
ZCAJS	Mirror-split	Redundant Standby	3
	Non-split	Redundant Parallel	9
		Single	9

\*1 :Bus Master Module, Control Network I/F Module, FMU Module

**Table A.22 I/O Module Chassis Specification**

Module Type	Applicable I/O Modules	Maximum Number of Modules
ZIOJS	Digital Input Module Digital Output Module Analog Output Module Analog Input Module	16 (and 2 Repeater Modules)
ZEHJS	PIF Module	16 (and 2 Repeater Modules)
ZISJS	Isolation Module	14
ZMEJS	Optical Conversion Module	14

**A.17 Other Modules Specification****Table A.23 Fan Modules Specification**

Module Type	Application	Number of fans per unit	Remarks
KFNJ	CPU Fan	4	Alarm detection circuit is prepared
	PS Fan	1	Alarm detection circuit is prepared
	Door Fan	3	Alarm detection circuit is prepared

**Table A.24 Terminal Unit Specification**

Module Type	Application	Number of terminals	Rated Voltage	Switching Function
PSND	Analog (AI/AO)	32	AC 115 V/ DC 125 V	Test Terminal Switching Function
	Digital (DI/DO)	64	AC 115 V/ DC 125 V	Lift Function









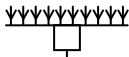
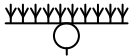
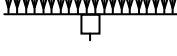
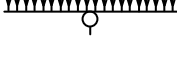
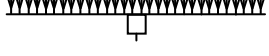
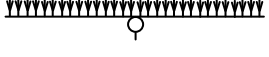
**Table A.25 Optical Switch Specification**

Item	Specification
Module Type	RJMA
Power Supply	5 V $\pm$ 5 %
Optical Switch ON/OFF Interface	Wire to board (4 pins) connector
Optical Fiber Interface	Interface for the Control Network I/F Module: Optical fiber cable with LC connector x 4
	Interface for the external cable: LC connector x 4









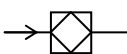
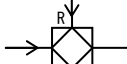
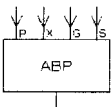
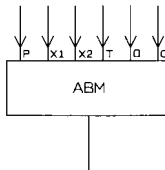
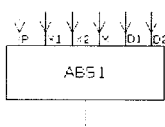
**APPENDIX B FUNCTIONAL SYMBOL SOFTWARE SPECIFICATIONS**

The function symbols listed below are for safety applications.

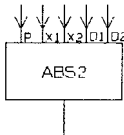
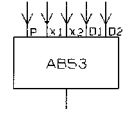
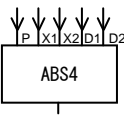


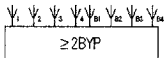
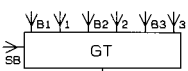
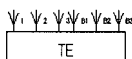
**Table B.1 List of Function Symbols for Discrete Control Processes**

No	Symbol	Name	Function
1		AND	Defines the output signal (Y) with respect to the input signals ( $X_1, X_2$ ) as follows: $Y = X_1 \text{ and } X_2$
2		OR	Defines the output signal (Y) with respect to the input signals ( $X_1, X_2$ ) as follows: $Y = X_1 \text{ or } X_2$
3		AND3	Defines the output signal (Y) with respect to the input signals ( $X_1, X_2, X_3$ ) as follows: $Y = X_1 \text{ and } X_2 \text{ and } X_3$
4		OR3	Defines the output signal (Y) with respect to the input signals ( $X_1, X_2, X_3$ ) as follows: $Y = X_1 \text{ or } X_2 \text{ or } X_3$
5		AND4	Defines the output signal (Y) with respect to the input signals ( $X_1, X_2, X_3, X_4$ ) as follows: $Y = X_1 \text{ and } X_2 \text{ and } X_3 \text{ and } X_4$
6		OR4	Defines the output signal (Y) with respect to the input signals ( $X_1, X_2, X_3, X_4$ ) as follows: $Y = X_1 \text{ or } X_2 \text{ or } X_3 \text{ or } X_4$
7		AND5	Defines the output signal (Y) with respect to the input signals ( $X_1, X_2, X_3, X_4, X_5$ ) as follows: $Y = X_1 \text{ and } X_2 \text{ and } X_3 \text{ and } X_4 \text{ and } X_5$
8		OR5	Defines the output signal (Y) with respect to the input signals ( $X_1, X_2, X_3, X_4, X_5$ ) as follows: $Y = X_1 \text{ or } X_2 \text{ or } X_3 \text{ or } X_4 \text{ or } X_5$
9		AND10	Defines the output signal (Y) with respect to the input signals ( $X_1, X_2, \dots, X_{10}$ ) as follows: $Y = X_1 \text{ and } X_2 \text{ and } \dots \text{ and } X_{10}$
10		OR10	Defines the output signal (Y) with respect to the input signals ( $X_1, X_2, \dots, X_{10}$ ) as follows: $Y = X_1 \text{ or } X_2 \text{ or } \dots \text{ or } X_{10}$
11		AND20	Defines the output signal (Y) with respect to the input signals ( $X_1, X_2, \dots, X_{20}$ ) as follows: $Y = X_1 \text{ and } X_2 \text{ and } \dots \text{ and } X_{20}$
12		OR20	Defines the output signal (Y) with respect to the input signals ( $X_1, X_2, \dots, X_{20}$ ) as follows: $Y = X_1 \text{ or } X_2 \text{ or } \dots \text{ or } X_{20}$
13		AND30	Defines the output signal (Y) with respect to the input signals ( $X_1, X_2, \dots, X_{30}$ ) as follows: $Y = X_1 \text{ and } X_2 \text{ and } \dots \text{ and } X_{30}$
14		OR30	Defines the output signal (Y) with respect to the input signals ( $X_1, X_2, \dots, X_{30}$ ) as follows: $Y = X_1 \text{ or } X_2 \text{ or } \dots \text{ or } X_{30}$

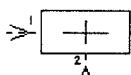
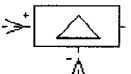
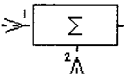
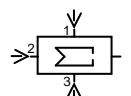
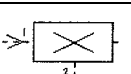

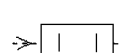

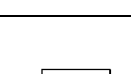
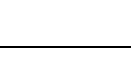
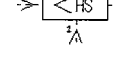
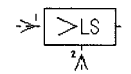
**Table B.1 List of Function Symbols for Discrete Control Processes**

No	Symbol	Name	Function
15		NOT	Defines the output signal (Y) with respect to the input signals (X) as follows: $Y = \bar{X}$
16		ON DELAY TIMER	Turns the output signal ON after the delay time when the input signal changes from OFF to ON.
17		OFF DELAY TIMER	Turns the output signal OFF after the delay time when the input signal changes from ON to OFF.
18		ONE SHOT TIMER	Turns the output signal ON only for a set time span when the input signal changes from OFF to ON.
19		FLIP-FLOP	Latches output signal ON with the Set signal input, and clears the output signal with the Reset signal input.
20		2-out-of-3	Outputs a signal if 2 or more inputs out of 3 inputs are ON.
21		2-out-of-4	Outputs a signal if 2 or more inputs out of 4 inputs are ON.
22		3-out-of-4	Output a signal if 3 or more inputs out of 4 inputs are ON.
23		1-INPUT FLIP-FLOP	Inverts the output signal every time the input signal changes OFF (0) -> ON (1).
24		1-INPUT FLIP-FLOP WITH RESET	Performs the same function as 1-INPUT FLIP-FLOP when reset-signal is OFF.
25		ANSWER BACK FOR AUX. UNIT (INCL. TIME MEASURING FUNCTION)	Performs the aux. unit answer back error judgment logic computation and outputs the results of the computation.
26		ANSWER BACK FOR POWER VALVE (INCL. TIME MEASURING FUNCTION)	Performs the power valve answer back error judgment logic computation and outputs the results of the computation.
27		ANSWER BACK 1 FOR PNEUMATIC VALVE (INCL. TIME MEASURING FUNCTION)	Performs the pneumatic valve answer back error judgment logic computation and outputs the results of the computation.

**Table B.1 List of Function Symbols for Discrete Control Processes**

No	Symbol	NAME	Function
28		ANSWER BACK 2 FOR PNEUMATIC VALVE (INCL. TIME MEASURING FUNCTION)	Performs the pneumatic valve answer back error judgment logic computation and outputs the results of the computation.
29		ANSWER BACK 3 FOR PNEUMATIC VALVE (INCL. TIME MEASURING FUNCTION)	Performs the pneumatic valve answer back error judgment logic computation and outputs the results of the computation.
30		ANSWER BACK 4 FOR PNEUMATIC VALVE (INCL. TIME MEASURING FUNCTION)	Performs the pneumatic valve answer back error judgment logic computation and outputs the results of the computation.
31		ON FIXED OUTPUT	Outputs an "ON" signal. (Logic value = 1)
32		OFF FIXED OUTPUT	Outputs an "OFF" signal. (Logic value = 0)
33		2/4-LOGIC WITH BYPASS FUNCTION	Outputs if 2 (or more) out of 4 inputs are ON. Provided with the bypass function for the input signal. Outputs status to the multi-bypass-input tag.
34		GLOBAL TRIP LOGIC	Outputs if 2 (or more) out of 3 inputs are ON. Provided with the bypass function for the input signal.
35		TRIP ENABLE LOGIC	Outputs if 1 (or more) out of 3 inputs are ON. Provided with the bypass function for the input signal.

**Table B.2 List of Function Symbols for Analog Control Processes**

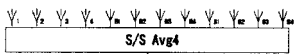

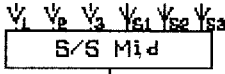

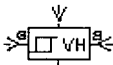

No.	Symbol	Name	Function
1		ADDER	Defines the output signal (Y) with respect to the input signals ( $X_1, X_2$ ) as follows: $Y = X_1 + X_2$
2		SUBTRACTER	Defines the output signal (Y) with respect to the input signals ( $X_1, X_2$ ) as follows: $Y = X_1 - X_2$
3		ADDER-SUBTRACTOR	Defines the output signal (Y) with respect to the input signals ( $X_1, X_2$ ) as follows: $Y = G_1 \cdot X_1 + G_2 \cdot X_2$
4		3-INPUT ADDER-SUBTRACTOR	Defines the output signal (Y) with respect to the input signals ( $X_1, X_2, X_3$ ) as follows: $Y = G_1 \cdot X_1 + G_2 \cdot X_2 + G_3 \cdot X_3$ ( $G_1, G_2, G_3$ :GAIN)
5		MULTIPLIER	Defines the output signal (Y) with respect to the input signals ( $X_1, X_2$ ) as follows: $Y = X_1 \times X_2$
6		DIVIDER	Defines the output signal (Y) with respect to the input signals ( $X_1, X_2$ ) as follows: $Y = X_1 \div X_2$
7		ABSOLUTE VALUE	Defines the output signal (Y) with respect to the input signals (X) as follows: $Y =  X $
8		SQUARE ROOT	Defines the output signal (Y) with respect to the input signals (X) as follows: $Y = G \cdot \sqrt{X}$
9		DEAD ZONE	Defines the output signal (Y) with respect to the input signals (X) as follows: $d_1 < X, d_2 > X \quad Y = X$ $d_2 \leq X \leq d_1 \quad Y = (d_1 + d_2)/2$
10		HIGH SIGNAL SELECTOR / LOWER LIMIT CONTROLLER	Defines the output signal (Y) with respect to the input signals ( $X_1, X_2$ ) as follows: $X_1 < X_2 \quad Y = X_2, \quad X_1 = X_2 \text{ or } X_1 > X_2 \quad Y = X_1$
11		LOW SIGNAL SELECTOR / UPPER LIMIT CONTROLLER	Defines the output signal (Y) with respect to the input signals ( $X_1, X_2$ ) as follows: $X_1 = X_2 \text{ or } X_1 < X_2 \quad Y = X_1, \quad X_1 > X_2 \quad Y = X_2$
12		UPPER LIMIT MONITOR	Outputs a signal when the input signal is equal or greater than a set value. At the time the system is reset, the input signal is below the gap with respect to the set value.

















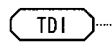
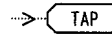
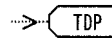


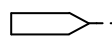
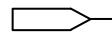
**Table B.2 List of Function Symbols for Analog Control Processes**

No.	Symbol	Name	Function
13		LOWER LIMIT MONITOR	Outputs a signal when the input signal is equal or less than a set value. At the time the system is reset, the input signal is below the gap with respect to the set value.
14		PROPORTIONAL	Outputs a signal with a proportional constant in response to the input signal.
15		INTEGRAL	Outputs an integrated output signal in response to the input signal.
16		DIFFERENTIATION	Outputs a differentiated output signal in response to the input signal.
17		LAG	Outputs the lag operation result as the output signal in response to the input signal.
18		LEAD/LAG	Outputs the lead/lag operation result as the output signal in response to the input signal.
19		SIGNAL SWITCH	Switches the digital input signal (SW) in response to the input signals ( $X_1$ , $X_2$ ) and outputs the output signal ( $Y$ ). $SW=1 \quad Y= X_1, \quad SW=0 \quad Y= X_2$
20		DEAD TIME	Outputs a signal in response to the input signal after delaying the output for a specified period of time.
21		ANALOG MEMORY	Gets parameters externally and, considering the digital input signal a trigger, outputs an output signal in proportion to the change rate set externally.
22		SIGNAL GENERATOR	Outputs a defined set value
23		LOGISTICS CONVERSION	Outputs the results of logistics output computation to the input signal.
24		SATURATION TEMPERATURE OPERATION	Outputs the operation result $Y$ as indicated below with respect to the input signal $X$ . $Y=a \cdot (X+b)^c$ (a:Coefficient, b: Bias, c: Power)
25		4-CH 2ND-HI SIGNAL SELECTOR	Selects and outputs second highest value with respect to the input values (1-4).
26		4-CH MEAN VALUE SIGNAL SELECTOR 3	Calculates and outputs the average value of normal channels for a 3-loop plant with respect to the input values (1 to 4).

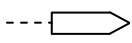
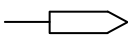
**Table B.2 List of Function Symbols for Analog Control Processes**

No.	Symbol	NAME	Function
27		4-CH MEAN VALUE SIGNAL SELECTOR 4	Calculates and outputs the average value of normal channels for a 4-loop plant with respect to the input values (1 to 4).
28		20-POLYGONAL LINE FUNCTION	Outputs the polygonal function of up to 20 points to the input signal.
29		3-CH INTERMEDIATE VALUE SIGNAL SELECTOR	Outputs the intermediate value with respect to the input values (1 to 3). The channels are compared and if the deviation is larger than the deviation upper limit setting value (A), the larger deviation status output flag is set ON after T seconds.
30		UPPER/LOWER LIMIT LIMITER	Outputs a signal within the set range of the output upper/lower limit to the input signal.
31		VARIABLE UPPER LIMIT MONITOR	Outputs a signal when the input signal reaches the set value. The input signal should be below the gap value in relation to the set value. (The gap value can be changed by using the input signal.)
32		ANALOG SIGNAL BCD CONVERSION	Converts the analog signal to BCD code.





**Table B.3 List of Function Symbols for Input and Output Process**

No	Symbol	Name
1		ANALOG INPUT
2		ANALOG OUTPUT
3		DIGITAL INPUT
4		DIGITAL OUTPUT
5		POWER INTERFACE DIGITAL INPUT
6		POWER INTERFACE DIGITAL OUTPUT
7		COMMUNICATION ANALOG INPUT
8		COMMUNICATION ANALOG OUTPUT
9		COMMUNICATION DIGITAL INPUT
10		COMMUNICATION DIGITAL OUTPUT
11		STATUS COMMUNICATION DIGITAL INPUT
12		STATUS COMMUNICATION DIGITAL OUTPUT
13		OPERATION ANALOG INPUT
14		OPERATION DIGITAL INPUT
15		TEST DIGITAL INPUT
16		TEST ANALOG OUTPUT
17		TEST DIGITAL OUTPUT
18		APPLICATION DIAGNOSIS ERROR OUTPUT
19		ANSWER BACK ERROR DIAGNOSIS OUTPUT
20		CROSS REFERENCE ANALOG INPUT
21		CROSS REFERENCE DIGITAL INPUT

**Table B.3 List of Function Symbols for Input and Output Process**

No	Symbol	NAME
22		CROSS REFERENCE ANALOG OUTPUT
23		CROSS REFERENCE DIGITAL OUTPUT

**Table B.4 List of Function Symbols for Obtaining and Setting Status Values**

No	Symbol	Name
1		ANALOG STATUS RESET
2		DIGITAL STATUS RESET
3		ANALOG ATTACHMENT BIT TAKEOUT
4		DIGITAL ATTACHMENT BIT TAKEOUT

## APPENDIX C DEFINITION

### **Alarm**

A minor abnormality with which the subsystem can continue its functions. When the subsystem detects this type of error, it does not change its mode and only warns of the error.

### **Application Software**

Software which provides or supports user specific functions. This software resides on a CPU Module with the basic software.

### **Basic Software**

System software that operates the controller (or hardware) and peripheral modules. This software consists of initialization code, device drivers, communication layers, function blocks, diagnostics, etc. for the MELTAC platform including firmware and FPGA.

### **Bus Master Module**

A module that has 4 communication interface channels to use for communication with I/O modules or Data Link communications. This module resides in the CPU Chassis.

### **Control Mode**

A state in which the subsystem performs input, operation, output processing, and self-diagnosis for the purpose of controlling plant systems.

### **Control Network**

A MELTAC dedicated ring topology network which continuously communicates plant process data and control signal data within a deterministic periodic cycle.

### **Control Network I/F Module**

A module that connects the controller to the Control Network. This module resides in the CPU Chassis .

### **CPU Chassis**

A chassis which can accommodate various modules such as the Power Supply Module, CPU Module, Control Network I/F Module, System Management Module and Bus Master Module.

### **CPU Fan**

A fan installed on top of the CPU Chassis to cool the modules within the CPU Chassis.

### **CPU Module**

A module that utilizes a microprocessor and performs internal operations and data transmission with other modules (i.e.: Bus Master Module, Control Network I/F Module and System Management Module).

This module utilizes F-ROM for storing both the basic software and the application software. This module resides in the CPU Chassis

### **Data Link**

A communication type used to transmit process signals between controllers of different safety divisions. This communication is unidirectional.

### **Dedicated Re-programming Chassis**

The CPU Module F-ROM can be updated only when the CPU Module is placed in this chassis after removing it from the on-line controller chassis.

**Distribution Module**

A module that interfaces with field signals. This module distributes the field signal to input modules on the rear side of the I/O Chassis. Similarly, the output signal is sent out through this module. This module resides in the I/O Chassis.

**Door Fan Unit**

A Fan Unit installed at the top rear of the cabinet to cool internal cabinet components.

**EEPROM**

Electrically Erasable Programmable Read Only Memory.

This memory can be erased and reprogrammed repeatedly through the application of higher than normal electrical voltage.

**Electrical/Optical (E/O) Converter Module**

A module for Data Link communication, which converts electrical signals to optical signals or optical signals to electrical signals.

**Electrical/Optical Converter Chassis**

A chassis which can accommodate up to 14 E/O converter modules.

**Failure**

A fatal abnormality with which the subsystem cannot continue its functions. When the subsystem detects this type of error, it transitions to Failure Mode. In Failure Mode, the processing of I/O and operation is stopped.

**Failure Mode**

The subsystem initializes in this mode after initial power activation. The subsystem also shifts to this mode automatically after it detects its own failure or there is a loss of power greater than 20 ms. A subsystem can shift from this mode to the Control Mode only by pushing the reset button on the Status Display Module.

**FPGA**

Field Programmable Gate Array.

FPGA has many internal logical blocks consisting of logic gates and arithmetic circuits. Internal logical blocks are located on a matrix. Required circuit configurations are implemented by connecting these internal logical blocks.

**Frame Memory Unit (FMU) Module**

A module that provides the analog RGB signal for the graphic images to the safety VDU panel. This module also provides the touch panel interface signal from the safety VDU panel to the safety VDU processor by means of an RS-232C data link. This module resides in the CPU Chassis.

**F-ROM**

Flash Read Only Memory. Also called flash memory.

One of the nonvolatile semiconductor memory type in which data does not disappear even after a device is turned off.

**I/O Alarm**

This alarm indicates I/O abnormality. When the subsystem detects this type of abnormality, it does not change its mode and only warns of the alarm.

**I/O Bus**

A communication line between the Bus Master Module and the I/O Chassis. This bus is used for transmission of data, such as process inputs from the I/O module to the CPU Module and outputs commands from the CPU Module to the I/O module.

**Input/Output Chassis**

A chassis which can accommodate up to 16 I/O modules.

**Input/Output(I/O) Modules**

Modules that interface with process signals. These modules provide process input/output functions and signal conditioner functions, including signal conversion and noise reduction.

**Isolation Module**

A module which provides electrical isolation between safety systems and non-safety systems.

**Maintenance Network**

The network used to communicate between the controllers / safety VDU processors and the MELTAC engineering tools.

**MELTAC Controller**

Mitsubishi Electric Total Advanced Controller.

MELCO's safety system digital platform for nuclear power plants.

**MELTAC engineering tool**

A tool that generates applications which operate on the MELTAC platform. The tool downloads generated applications to the MELTAC controllers, and displays failure and status information of the MELTAC platform (see Section 4.1.4.1 for details). This tool consists of (Windows-based) non-safety PC and software called "MELENS".

**NI Chassis**

A chassis which can accommodate NI modules.

**NI modules**

Modules that interface to neutron detector or other modules. These modules provide signal conditioner functions.

**Optical Switch**

A switch which 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 controllers.

**Power Interface Module (PIF Module)**

A module that receives output commands as a result of subsystem operation, and controls the power that drives the switchgears, solenoid valves, etc. for plant components. This module resides in the I/O Chassis dedicated for PIF Module.

**Power Supply Fan Unit**

Fan Units 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**

A module that converts the AC power into DC power voltages suitable for the individual modules and units. This module resides in the CPU Chassis and I/O Chassis.



**Redundant Parallel Controller**

In the "Redundant Parallel" configuration, the controller includes 2 subsystems. Each subsystem operates in Control Mode.

Even if one of the subsystems fail, this configuration allows a system to maintain its safety function without a subsystem changeover.

**Redundant Standby Controller**

In the "Redundant Standby" configuration, the controller includes 2 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 an 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 Module**

A module that is used to shape and amplify data communication signals between I/O modules and the Bus Master Module. This module resides in the I/O Chassis.

**ROM writing tool**

A tool used to write binary code to nonvolatile devices (ROM).

**Safety VDU Panel**

An HSI device which provides a color graphic display with an integral touch screen.

**Safety VDU Processor**

A processor which transfers operation signals received from the safety VDU panel to the safety systems and displays information from the safety systems on the safety 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 only one subsystem. This subsystem operates in Control Mode.

**Standby Mode**

In this mode, the subsystem tracks the data from the subsystem in the Control Mode so that 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-diagnosis), it automatically changes from the Standby Mode to the Failure Mode.

**Status Display & Switch Module**

A module that displays the mode and alarms of 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**

A module that displays the mode and alarms of single subsystem.

This module is used in a CPU Chassis configured for a Redundant Parallel Controller or a Single Controller.

**System Management Module**

A module that 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 MELTAC engineering tool. This module resides in the CPU Chassis.

**V&V**

Verification and Validation.

The process of determining whether:

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

**APPENDIX D REGULATORY REQUIREMENTS AND GUIDANCE APPLICABILITY MATRIX**

Appendix D shows the compliance matrix of applicable codes, standards, and regulatory guidance required by NUREG-0800 and ISG-06. Also, Appendix D points to the corresponding location within this Topical Report that describes design information related to the applicable codes, standards, and regulatory guidance of the MELTAC platform.

**10 CFR 50, 10 CFR 52, AND 10 CFR 73**

Criteria <sup>(1)</sup>	Title	Applicability	Design Information <sup>(2)</sup>
50.55a(a)(1)	Quality Standards for Systems Important to Safety	X	<u>JEXU-1041-1008</u> 6.0
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	Described in Application Licensing Document.
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	N/A	
52.80(a)	ITAAC for Combined Licensee Applications	N/A	
73.54	Protection of digital computer and communication systems and networks	N/A	

- (1) The applicable criteria in NUREG-0800 Standard Review Plan (SRP) Sec. 7.1 Rev. 5, ISG-06, and each clause of IEEE Std. 603-1991 and IEEE Std. 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.
- (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.

**GDC 10 CFR 50 APPENDIX A**

Criteria <sup>(1)</sup>	Title	Applicability	Design Information <sup>(2)</sup>
GDC 1	Quality Standards and Records	X	<u>JEXU-1041-1008</u> 6.0
GDC 2	Design Bases for Protection Against Natural Phenomena	X	<u>JEXU-1041-1008</u> 5.0
GDC 4	Environmental and Dynamic Effects Design Bases	X	<u>JEXU-1041-1008</u> 5.0
GDC 10	Reactor Design	N/A	Described in Application Licensing Document.
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	<u>JEXU-1041-1008</u> 4.1.5, 4.1.7, 4.2.3, 4.2.4, 7.0
GDC 22	Protection System Independence	X	<u>JEXU-1041-1008</u> 4.1.2.3, 4.1.2.5, 4.3, 5.5, Appendix A.3, A.4, A.6, A.7
GDC 23	Protection System Failure Modes	X	<u>JEXU-1041-1008</u> 4.1.5, 4.2.3
GDC 24	Separation of Protection and Control Systems	X	<u>JEXU-1041-1008</u> Appendix B (Signal Selection [S/S] Function)
GDC 25	Protection System Requirements for Reactivity Control Malfunctions	N/A	Described in Application Licensing Document.
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**

Criteria <sup>(1)</sup>	Title	Applicability	Design Information <sup>(2)</sup>
SRM to SECY 93087 II.Q	Defense Against Common-Mode Failures in Digital I&C Systems	N/A	Described in Application Licensing Document.
SRM to SECY 93087 II.T	Control Room Annunciator (Alarm) Reliability	N/A	

**REGULATORY GUIDE**

Criteria <sup>(1)</sup>	Title	Applicability	Design Information <sup>(2)</sup>
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	Described in Application Licensing Document.
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	Described in Application Licensing Document.
RG 1.75	Independence of Electrical Safety Systems	X	See applicability to GDC 22.
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	Described in Application Licensing Document.
RG 1.105	Setpoints for Safety-related Instrumentation	X	JEXU-1041-1008 Appendix A.5, A.6, A.9
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	Described in Application Licensing Document.
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	JEXU-1041-1008 4.1.3, 4.2.2, 6.0
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		
RG 1.174	An Approach for Using PRA in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis	N/A	Described in Application Licensing Document.
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	JEXU-1041-1008 5.3, 5.4
RG 1.189	Fire Protection for Operating Nuclear Power Plants	N/A	Described in Application Licensing Document.
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	JEXU-1041-1008 5.3
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.
RG 1.32	Criteria for Power Systems for Nuclear Power Plants	N/A	Described in Application Licensing Document.
RG 1.89	Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants	X	JEXU-1041-1008 5.1

**BRANCH TECHINICAL POSITION**

Criteria <sup>(1)</sup>	Title	Applicability	Design Information <sup>(2)</sup>
BTP 7-1	Guidance on Isolation of Low-Pressure Systems from the High-Pressure RCS	N/A	Described in Application Licensing Document.
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	
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	N/A
BTP 7-8	Guidance on Application of RG 1.22	X	See applicability to RG 1.22 and GDC 21.
BTP 7-9	Guidance on Requirements for RPS Anticipatory Trips	N/A	Described in Application Licensing Document.
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 GDC 22.
BTP 7-12	Guidance on Establishing and Maintaining Instrument Setpoints	N/A	Described in Application Licensing Document.
BTP 7-13	Guidance on Cross-Calibration of Protection System Resistance	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	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 GDC 21.
BTP 7-18	Guidance on Use of Programmable Logic Controllers in Digital Computer-Based I&C Systems	N/A	Described in Application Licensing Document.
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	N/A
BTP 7-21	Guidance on Digital Computer Real-Time Performance	X	JEXU-1041-1008 4.1.3, 4.2.2, 4.4

**IEEE STD. 603-1991**

Criteria <sup>(1)</sup>	Title	Applicability	Design Information <sup>(2)</sup>
1.	Scope	N/A	Described in Application Licensing Document.
2.	Definitions	N/A	
3.	References	N/A	
4	Safety System Designation	No Request	N/A
4.1	Design Basis Events	N/A	Described in Application Licensing Document.
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	<u>JEXU-1041-1008</u> 4.1.5, 4.2.3, 7.0
4.10	The Critical Points in Time or the Plant Conditions	X	<u>JEXU-1041-1008</u> 4.1.3, 4.2.2, 4.4
4.11	Equipment Protective Provisions	X	<u>JEXU-1041-1008</u> 4.1.5, 4.2.3
4.12	Other Special Design Basis	No Request	N/A
5	Safety System Criteria	No Request	N/A
5.1	Single Failure Criterion	N/A	Described in Application Licensing Document.
5.2	Completion of Protective Action	N/A	
5.3	Quality	X	<u>JEXU-1041-1008</u> 6.0
5.4	Equipment Qualification	X	<u>JEXU-1041-1008</u> 5.0
5.5	System Integrity	N/A	Described in Application Licensing Document.
5.6	Independence	X	<u>JEXU-1041-1008</u> 4.1.2.3, 4.1.2.5, 4.3, 5.5, Appendix A.3, A.4, A.6, A.7
5.6.1	Between Redundant Portions of a Safety System		
5.6.2	Between Safety Systems and Effects of a Design Basis		
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		

Criteria <sup>(1)</sup>	Title	Applicability	Design Information <sup>(2)</sup>
5.7	Capability for Test and Calibration	X	<u>JEXU-1041-1008</u> 4.1.5, 4.2.3, 7.0
5.8	Information Displays	No Request	N/A
5.8.1	Displays for Manually Controlled Actions	N/A	Described in Application Licensing Document.
5.8.2	System Status Indication	N/A	
5.8.3	Indication of Bypasses	N/A	
5.8.4	Location of Displays	N/A	
5.9	Control of Access	X	<u>JEXU-1041-1008</u> 4.5
5.10	Repair	X	<u>JEXU-1041-1008</u> 4.1.4, 4.1.5, 4.2.3
5.11	Identification	N/A	Described in Application Licensing Document.
5.12	Auxiliary Features	N/A	
5.13	Multi-Unit Stations	N/A	
5.14	Human Factors	N/A	
5.15	Reliability	X	<u>JEXU-1041-1008</u> 7.0
5.16	Common Cause Failure (IEEE 603-1998)	X	<u>JEXU-1041-1008</u> 4.1.3, 4.2.2, 5.0, 6.0
6	Sense and Command Features - Functional and Design Requirements.	N/A	Described in Application Licensing Document.
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	<u>JEXU-1041-1008</u> Appendix B (S/S Function)
6.4	Derivation of System Inputs	N/A	Described in Application Licensing Document.
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 Request	N/A
6.8.1	Setpoint Uncertainties	N/A	Described in Application Licensing Document.
6.8.2	Multiple Setpoints	N/A	
7	Executive Features - Functional and Design Requirements	N/A	
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**

Criteria <sup>(1)</sup>	Title	Applicability	Design Information <sup>(2)</sup>
1.	Scope	N/A	Described in Application Licensing Document.
2.	References	N/A	
3.	Definitions and Abbreviations	N/A	
4	Safety System Designation	No Request	N/A
5	Safety System Criteria	No Request	
5.1	Single Failure Criterion	No Request	
5.2	Completion of Protective Action	No Request	
5.3	Quality	X	<u>JEXU-1041-1008</u> 4.1.3, 4.2.2, 6.0
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	<u>JEXU-1041-1008</u> 4.1.5, 4.3, 5.0, 6.0
5.4.1	Computer System Testing		
5.4.2.	Qualification of Existing Commercial Computers	N/A	Described in Application Licensing Document.
5.5.	System Integrity	X	<u>JEXU-1041-1008</u> 4.1.3, 4.2.2, 6.0
5.5.1	Design for computer integrity		
5.5.2	Design for test and calibration	X	<u>JEXU-1041-1008</u> 4.1.5, 4.2.3, 7.0
5.5.3	Fault detection and self-diagnostics		
5.6	Independence	X	<u>JEXU-1041-1008</u> 4.1.2.3, 4.1.2.5, 4.3, 5.5, Appendix A.3, A.4, A.6, A.7
5.7	Capability for Test and Calibration	No Request	N/A
5.8	Information Displays	No Request	
5.9	Control of Access	No Request	
5.10	Repair	No Request	
5.11	Identification	X	<u>JEXU-1041-1008</u> 6.1.8
5.12	Auxiliary Features	No Request	N/A
5.13	Multi-Unit Stations	No Request	
5.14	Human Factors	No Request	
5.15	Reliability	X	<u>JEXU-1041-1008</u> 7.0
6	Sense and Command Features - Functional and Design	No Request	N/A
7	Executive Features - Functional and Design Requirements	No Request	
8	Power Source Requirements	No Request	