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.

Sincerely,

***/RA/***

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

Docket No.: 99902039

Enclosure:
Final Safety Evaluation

SUBJECT: FINAL PROPRIETARY SAFETY EVALUATION FOR "SAFETY SYSTEM DIGITAL PLATFORM – MELTAC," (CAC NO. MF4228; EPID L-2014-TOP-0006) DATED NOVEMBER 5, 2018

DISTRIBUTION:

| | | |
|---|---|---|
| PUBLIC Letter | NON-PUBLIC SE | RidsNroOd RidsNrrDlp |
| RidsNrrDlpPlpb | JHolonich, NRR | SDarbali, NRR |
| RidsNrrLADHarrison | RidsOgcMailCenter | RidsACRS_MailCTR |
| RidsNrrDeEicb | RidsResOd | RStattel, NRR |
| MWaters, NRR | DMorey, NRR | DRaneja, NRO |

**ADAMS Accession No.: ML18257A014** ***via e-mail** **NRR-106**

| OFFICE | NRR/DLP/PLPB/PM | NRR/DLP/PLPB/LA* | NRR/DE/EICB/BC* |
|---|---|---|---|
| NAME | JHolonich | DHarrison | MWaters |
| DATE | 11/05/2018 | 10/31/2018 | 11/02/2018 |
| OFFICE | NRR/DE/EICA/BC* | NRR/DLP/PLPB/BC | |
| NAME | NSalgado | DMorey | |
| DATE | 11/05/2018 | 11/05/2018 | |

**OFFICIAL RECORD COPY**

# 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


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

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

## 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

| Supplement | Date | Reference |
|---|---|---|
| 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. 603-1991incorporation 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 (IS0)-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.

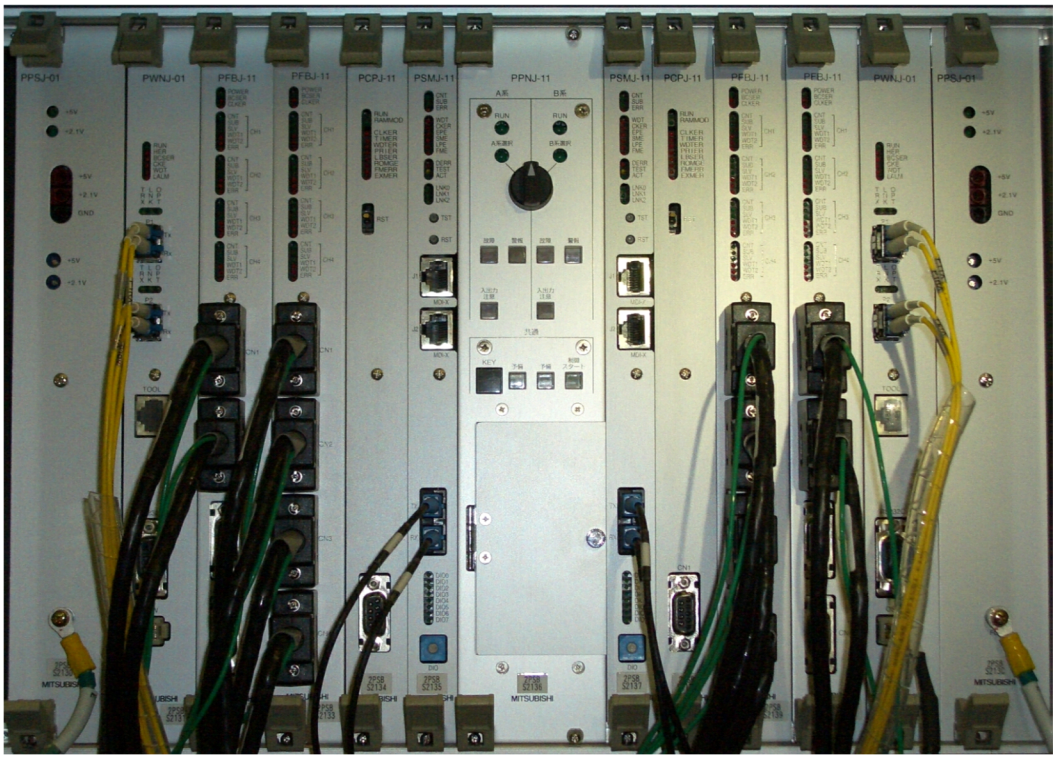


**Figure 3.1-1: MELTAC platform modules in CPU chassis**

(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.

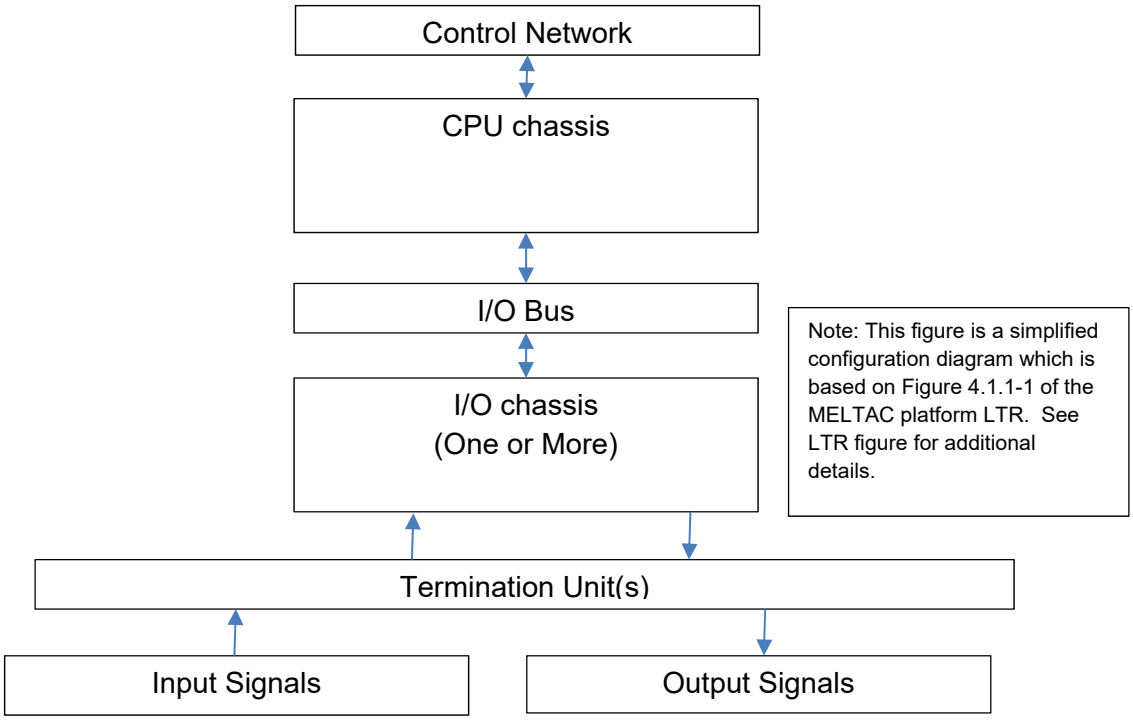


**Figure 3.2.2-1: MELTAC Subsystem Architecture Configuration**

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 staffs 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 can 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**

| Document Title | MELCO Document Identification | Reference Number |
|---|---|---|
| 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 Sagamihara 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.

<u>Data Link:</u>

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, liveliness, and real-time properties essential to the safety application should be verified in the protocol. Liveliness, 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 (IS0)-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 Section5.2.3).

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 3.11.1of 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) and 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".<br>NOTE: The LTR uses the term "Safety Visual Display" only. | Agreed. Term changed. |