RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

8/10/2016

SAFETY SYSTEM DIGITAL PLATFORM
- MELTAC (MITSUBISHI ELECTRIC TOTAL ADVANCED CONTROLLER) -
TOPICAL REPORT

Mitsubishi Electric Corporation

TAC NO.:	**MF4228**
RAI NO.:	**#1**
DATE OF RAI ISSUE:	**6/29/2016**

QUESTION NO.: 1 for JEXU-1041-1008, "Safety System Digital Platform – MELTAC"

Title 10 of the *Code of Federal Regulations* (10 CFR) Part 50, "Domestic Licensing of Production Utilization Facilities, establishes fundamental regulatory requirements. Specifically, Appendix B, "Quality Assurance Criteria," Criterion II, "Quality Assurance Program," states, in part; "This program shall be documented by written policies, procedures, or instructions." Page 0-6 of the TR states "the information provided in this report covers the life cycle and the Quality Assurance Program (QAP) of the MELTAC platform." In other inferences throughout the document, there are references to "10 CFR Part 50 Appendix B QAP" or just "QAP" or "MELCO QAP." The U.S. Nuclear Regulatory Commission (NRC) staff notes there is also a separate QAP for non-safety items. It is therefore unclear to the NRC staff how this requirement for specific written policies, procedures, or instructions is met and thus the staff is unable to make a regulatory compliance determination. Please provide information to identify each QAP by title, number, date and revision which is proposed to meet the requirements (or not) as stated by 10 CFR 50 Appendix B, Criterion II.

ANSWER:
The quality assurance programs mentioned in the ToR are the following two programs:

- "MELCO's 10 CFR 50 Appendix B QAP"
  This program is fully compliant with 10 CFR 50 Appendix B. The life cycle process of the MELTAC platform for use in US safety related applications is managed under this program. This program is also compliant with 10 CFR 21.

[

]

- "MELCO's ISO9001 QAP"
  This program manages the life cycle process of the MELTAC platform for use in non-safety

applications and the life cycle process of the MELTAC engineering tool. This program is not proposed to meet the requirements stated in 10 CFR 50 Appendix B.

[

]

MELCO will revise Abstract, Section 1.0, Section 4.1 and Section 6 of ToR to reflect the clarification above, as shown in Attachment-1.

Impact on Technical Report

The answer above will be added to MELTAC Platform Software Program Manual (see Attachment-2).
The answer above will be added to MELTAC Platform ISG-04 Conformance Analysis.(see Attachment-3).

Abstract

This Topical Report describes the design of the Mitsubishi Electric Total Advanced Controller (MELTAC) platform and its conformance to the U.S. Nuclear Regulatory requirements for nuclear safety systems. The MELTAC platform can be used for safety and non-safety Instrumentation and Control (I&C) systems.

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

The MELTAC platform has accumulated many years of positive operating experience in various non-safety system applications such as the reactor and turbine control systems in PWR nuclear power plants operating in Japan. Based on its excellent performance in numerous non-safety applications, the MELTAC platform has now been applied to almost all non-safety and safety systems throughout Japanese PWR nuclear power plants. The MELTAC platform has also been applied for plant-wide digital upgrades in several Japanese PWR nuclear power plants that have been completed and those currently in progress.

The goal of this report is to seek a favorable Safety Evaluation from the U.S. Nuclear Regulatory Commission (NRC) for the use of the MELTAC platform for nuclear safety systems in operating plants and new plants.

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

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

The information provided in this report covers the following topics to fully understand the MELTAC platform for nuclear safety systems: ToR-1

- The detailed description of the hardware and software of the MELTAC platform, including digital processing, human systems interfaces (HSI) and digital communication interfaces and the detailed description of the MELTAC application development tools
- The equipment qualification of the MELTAC platform and its conformance to the corresponding U.S. standards
- The life cycle process and the ~~Q~~quality ~~A~~assurance ~~P~~program ~~(QAP)~~ of the MELTAC platform and conformance to U.S. regulatory criteria ToR-1
- The equipment reliability of the MELTAC platform and how that reliability is used to determine the reliability of any MELTAC safety application

The MELTAC platform was developed under a Japanese ~~QAP~~quality assurance program compliant with ISO9001, and has undergone a one-time commercial grade dedication (CGD) by MELCO for use in US safety related applications. The details of that CGD program are provided in this report by reference. The MELTAC platform is now maintained and manufactured under MELCO's quality assurance program compliant with 10 CFR 50 Appendix B ("MELCO's 10 CFR 50 Appendix B QAP"), and 10 CFR 21. ToR-1 ToR-1

Prior to implementing the MELTAC commercial grade dedication program, MELCO developed and adopted the MELCO's 10 CFR 50 Appendix B QAP~~a nuclear QAP in compliance with 10 CFR 50 Appendix B and 10 CFR 21~~. MELCO has undergone an inspection by NRC to verify the implementation of an adequate quality assurance program ~~QAP~~ in compliance with the requirements of 10 CFR 50 Appendix B and 10 CFR 21 in support of digital I&C development activities. The results of this NRC inspection are documented in NRC Inspection Report NO. 99901410/2011-202 (ADAMS Accession number ML12013A353). In NRC Inspection Report NO. 99901410/2011-202, the NRC inspection team concluded that MELCO is effective in implementing its ~~QA~~10 CFR 50 Appendix B program and 10 CFR ~~Part~~ 21 programs in support of the MELTAC platform development. The Inspection Report stated that the NRC inspectors determined that MELCO's commercial grade dedication process adequately identified and verified the critical characteristics of the MELTAC platform that provide assurance that the platform will perform its safety function satisfactorily. The Inspection Report also stated that the NRC inspectors determined that the process implemented by MELCO is consistent with regulatory requirements associated with software development. The nonconformance identified in the Inspection Report has been corrected. ToR-1 ToR-1

MELCO also underwent a successful audit by the NRC Office of New Reactors (NRO). This NRO audit focused on reviewing the design details related to the MELTAC platform to assist in making the determination that the specifications for the digital platform to be used for the implementation of the safety I&C systems, which reflect the MELTAC platform, meet the regulatory requirements. The results of the NRO audit are documented in the "Digital Instrumentation and Controls Design Audit Report" (ADAMS Accession number ML12291A673).

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

3.0 APPLICABLE CODE, STANDARDS AND REGULATORY GUIDANCE

This section identifies conformance to applicable codes, standards, and regulatory guidance required by NUREG-0800 and ISG-06. Unless specifically noted, the latest version issued on the date of this Topical Report is applicable.

Appendix D shows the compliance matrix of codes, standards, and regulatory guidance required by NUREG-0800 and ISG-06. Also, Appendix D points to the corresponding location within this Topical Report that describes design information related to the applicable codes, standards, and regulatory guidance of the MELTAC platform.

Code of Federal Regulations

1. 10 CFR ~~Part~~ 50 Appendix A: General Design Criteria for Nuclear Power Plants ToR-1

GDC 1: Quality Standards and Records

The lifecycle process for the Basic components of the MELTAC platform that meets all requirements of 10 CFR ~~Part~~ 50 Appendix B and 10 CFR 21 is described in Section 6. This is referred to as ~~the~~ MELCO's quality assurance program compliant with 10 CFR 50 Appendix B and 10 CFR 21 (MELCO's 10 CFR 50 Appendix B QAP), which is also described in "Quality Manual based on U.S. Nuclear Regulations" (ESC Procedure N-G000-P)~~App.B based quality assurance program (QAP)~~. ToR-1

The MELTAC platform was developed under a Japanese quality assurance~~QA~~ program compliant with ISO9001 (MELCO's ISO9001 QAP) and has undergone a one-time commercial grade dedication (CGD) by MELCO for use in US safety -related applications. The details of that CGD program are provided in this report by reference. MELTAC is now maintained and manufactured under MELCO's 10 CFR 50 Appendix B QAP. ToR-1

GDC 2: Design Bases for Protection against Natural Phenomena

This Equipment is seismically qualified. The Equipment must be located within building structures that provide protection against other natural phenomena. Specific buildings and Equipment locations are described in Application Licensing Documentation.

GDC 4: Environmental and Dynamic Effects Design Bases

This Equipment is qualified for use in a mild environment that is not adversely affected by plant accidents as described in Section 5.

GDC 21: Protection System Reliability and Testability

This Equipment includes automated testing with a high degree of coverage, and additional overlapping manual test features for the areas that are not covered by automated tests. All manual tests may be conducted with the plant on line, with consideration of plant specific accessibility, and with the Equipment bypassed or out of service. Depending on the system design for a specific plant, the

Section 6 describes ~~the~~ MELCO's 10 CFR 50 Appendix B QAP~~App.B based QAP~~, which is fully compliant to 10 CFR 50 Appendix B. ToR-1

MELCO has undergone an inspection by NRC to verify the implementation of an adequate QAP.

(h) Invokes IEEE Std. 603-1991

See conformance to IEEE Std. 603-1991

NRC Regulatory Guides

3. RG 1.22 Periodic Testing of Protection System Actuation Functions (Rev. 0, February 1972)

   See GDC 21 conformance. The functions controlled by this Equipment can be configured at the application level to be completely testable through a combination of overlapping automatic and manual tests.

4. RG 1.29 Seismic Design Classification (Rev. 4, March 2007)

   The Equipment is designated Seismic Category I.

5. RG 1.53 Application of the Single-Failure Criterion to Safety Systems (Rev. 2, November 2003)

   endorses IEEE Std. 379-2000

   See conformance to GDC 21 and 24. This Equipment can be configured at the application level so that safety functions are designed with N or N+1 divisions. Each safety division can be independent from the other safety divisions and from non-safety divisions. Independence ensures that credible single failures cannot propagate between divisions within the system and therefore cannot prevent proper protective action at the system level. Single failures considered in the divisions are described in the Failure Mode and Effect Analysis (FMEA) for each system. The FMEA method for the components of this Equipment is provided in this Topical Report. The MELTAC module level FMEA report is incorporated by reference. The module level FMEA provides input to the system level FMEA for each application. The system level FMEA is described in Application Licensing Documentation.

6. RG 1.75 Criteria for Independence of Electrical Safety Systems (Rev. 3, February 2005)

   endorses IEEE Std. 384-1992

   The MELTAC platform contains features to ensure that redundant safety divisions are physically and electrically independent of each other and physically and electrically independent of any non-safety divisions. Physical independence is maintained either by the required distance or by barriers which prevent propagation of fire or electrical faults. Electrical independence is maintained by fiber optic cable communication interfaces or conventional isolators, such as opto-couplers, relays or transformers. Conventional isolators include fault

4.1.4 MELTAC Engineering Tool

The MELTAC engineering tool provides various functions aimed at steadier and more efficient software management during all system life cycle phases (including design, fabrication, test, adjustment and maintenance).

The MELTAC engineering tool is used to generate safety application software for the MELTAC controller, but the tool itself is non-safety software running on a non-safety personal computer (PC) using the Microsoft Windows Operating System. The MELTAC engineering tool was developed in accordance with MELCO's QAP compliant with ISO9001 (MELCO's ISO9001 QAP)~~the MELCO QAP~~ for non-safety items. Safety application software generated by the MELTAC engineering tool must be qualified by independent V&V. Access is controlled by means of the PC password (BIOS, OS) and the MELTAC engineering tool password. ToR-1

The application software execution data generated by the MELTAC engineering tool is downloaded to the controller via the Maintenance Network and is stored in the F-ROM of the CPU Module. The functions of the MELTAC engineering tool are described as follows.

4.1.4.1 Function Description

a) Creation of Application Software

FBDs that are created with a commercial Mitsubishi CAD software package called "RAPID" can be automatically converted to GBDs by the MELTAC engineering tool. (Access to RAPID is also controlled by a password.)
The MELTAC engineering tool is then used to automatically generate (compile) the application software execution data directly from the GBD.
This automated process eliminates human translation errors.
GBDs can also be manually created (drawn), based on legacy FBDs provided by the customer, using the MELTAC engineering tool's GUI editor.
Regardless of how the GBD is generated (automatically from RAPID or manually drawn with the MELTAC engineering tool's GUI editor), the assignment of GBDs to controllers and the assignment of I/O signals is manually configured using the MELTAC engineering tool.

GBDs (whether created automatically or manually) and the executable data output from the MELTAC engineering tool are confirmed through manual V&V activities.

b) Download

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

]

Table 4.1.7-1 MIC vs. SMC

[

]

The versions of the application software and the basic software are controlled through software configuration management. The application software is described in the Application Licensing Document. The basic software is controlled and maintained in accordance with ~~the~~ MELCO's 10 CFR 50 Appendix B QAP ~~App.B based QAP~~ and "MELTAC Platform Software Program Manual" (JEXU-1041-1016). ToR-1

The following table summarizes the software differences that can be detected by the MIC and SMC.

Table 4.1.7-2 Detectable Errors by the MIC and SMC

[

ToR-1

]

The periodic manual tests (the process input and output test, and the safety VDU test) ensure that the CPU is capable of executing instructions from both F-ROM for basic software and F-ROM for application software. This encompasses the instructions that control continuous self-diagnosis, and the instructions that control the safety functions of monitoring process

6.0 QUALITY ASSURANCE AND LIFE CYCLE

The MELCO quality assurance program ~~(QAP)~~ complies with 10 CFR 50 Appendix B (complies with ASME NQA-1-1994) and 10 CFR 21. This is referred to as ~~the~~ MELCO's 10 CFR 50 Appendix B QAP~~App.B based QAP~~. ToR-1

The MELTAC platform was originally developed under the Japanese nuclear quality program that encompasses most of 10 CFR 50 Appendix B requirements. MELCO performed a re-evaluation of the MELTAC platform design and the design process based on the commercial grade dedication process in accordance with 10 CFR 21. This re-evaluation was performed by an independent MELCO organization that was not involved in the original MELCO development to ensure that the MELTAC platform has the technical characteristics and quality equivalent to a product originally developed under a 10 CFR 50 Appendix B program. This is referred to as the MELTAC Re-evaluation Program (MRP) (See Section 6.2). ~~The~~ MELCO's 10 CFR 50 Appendix B QAP~~App.B based QAP~~ governed the re-evaluation of the previous MELTAC platform development, and governs all new MELTAC platform development or revisions that occur after this re-evaluation. The MRP (i.e.: one-time commercial grade dedication) established a baseline to demonstrate that the MELTAC platform has suitable technical characteristics and quality for nuclear safety applications in the U.S. MELTAC is now maintained as a 10 CFR Appendix B product. ToR-1

MELCO has undergone an inspection by NRC to verify the implementation of an adequate quality assurance~~QA~~ program in compliance with the requirements of 10 CFR 50 Appendix B and 10 CFR 21 in support of digital I&C development activities. The results of this NRC inspection are documented in NRC Inspection Report NO. 99901410/2011-202 (ADAMS Accession number ML12013A353). In this Inspection Report, the NRC inspection team concluded that MELCO is generally effective in implementing its 10 CFR 50 Appendix B program~~QA~~ and 10 CFR 21 programs in support of the MELTAC platform development. It states that "the NRC inspectors determined that MELCO's commercial grade dedication process adequately identified and verified the critical characteristics of the MELTAC platform that provide assurance that the platform will perform its safety function satisfactorily". In addition, it states that "the NRC inspectors determined that the process implemented by MELCO is consistent with regulatory requirements associated with software development". ToR-1 ToR-1

6.1 MELTAC Platform Life Cycle Plans and Activities

This section describes key elements of the life cycle process for the basic components (software and hardware) of the MELTAC platform, based on ~~the~~ MELCO's 10 CFR 50 Appendix B QAP~~App.B based QAP~~. ToR-1

6.1.1 Overview of the MELTAC Quality Assurance Program

The MELCO procedures applicable to software encompass the basic software, which includes the firmware and FPGAs on all MELTAC modules.

The MELCO procedures, processes and software life cycle for nuclear safety-related activities (hardware and software) comply with the applicable requirements given in Section 3 of this Topical Report, the "MELTAC Platform Software Program Manual" (JEXU-1041-1016), referred to here as SPM, 10 CFR 50 Appendix B, and ASME NQA-1-1994.

The SPM provides the generic plans that are followed under MELCO's 10 CFR 50 Appendix B QAP~~MELCO's App.B based QAP~~ for all activities related to the basic software life cycle conducted after the MRP. The SPM complies with the guidance of BTP 7-14 "Guidance on Software Reviews for Digital Computer-based Instrumentation and Control Systems". A summary of the basic software life cycle plans and activities is given in Table 6.1-1. ToR-1

The QAP and software life cycle for plant specific nuclear safety-related system implementation (hardware and application software) is not described in this report.

Table 6.1-1 MELTAC Life Cycle Plan/Activity Summary

ToR-1

ToR-1

6.1.2 Secure Development Environment Management

The Secure Development Environment Management Program for the basic software complies with RG 1.152 as described in the SPM. The overall Secure Development Environment Management Program ensures:

a) There is no unintended code included in the software during the process of software development.
b) Unintended changes to the software installed in the system are prevented and detected. This is described in further detail in Section 6.1.2.3.

These processes are applicable to the basic software and related documentations.
The compliance assessment for the MELTAC platform and its life cycle development process, relative to RG 1.152, is provided in the SPM.

The security measures in the development process of the application software are described in the Application Licensing Document.

6.1.2.1 Development/Storage Security Measures of the basic software

[

ToR-1

]

6.1.6 Obsolescence Management

This section describes the obsolescence management program for the MELTAC platform. MELCO uses hardware parts which have excellent production continuity. Regardless, the product service life for nuclear applications covers 20 to 30 years, so it is inevitable that many parts will become unavailable. The following sections summarize the process used to determine the availability of parts and the process used to evaluate and utilize different parts for substitution. All changes to the MELTAC platform are done under ~~the~~ MELCO's 10 CFR 50 Appendix B QAP.~~MELCO App.B based QAP~~ ToR-1

The parts substitution method described in this section is primarily applicable to the obsolescence management. However, MELCO will also use the same method of parts substitution to ensure adequate parts supply from multiple sources to accommodate supply management issues or production peaks.

6.1.6.1 Obtaining Information on Part Availability

[

]

6.1.6.2 Selecting Replacement Parts

[

]

6.1.6.3 Verification after Replacement

[

]

6.1.7 Identification

[

ToR-1

ToR-1

ToR-1

]

6.1.8 Reliability Database

[

ToR-1

]

6.2 MELTAC Re-evaluation Program (MRP)

[

ToR-1

ToR-1

]

6.3 MELTAC Engineering Tool Life Cycle

The MELTAC engineering tool was developed and is managed under ~~the~~ MELCO's QAP compliant with ISO 9001 (MELCO's ISO9001 QAP)~~MELCO QAP~~ for non-safety items ~~(Complies with ISO 9001)~~. This is acceptable because the MELTAC engineering tool is not credited for any safety-related functions..

ToR-1

The MELTAC engineering tool will continue to be managed under ~~the~~ MELCO's ISO9001 QAP ~~MELCO QAP~~ for non-safety items, and the output of the tool will continue to be manually verified. Since the tool is used to develop application software, the application development and verification process is defined in application level documentation and managed under the applicable application level QAP.

ToR-1

Design, Implementation, Test, and Operation and Maintenance). A Project Plan and a Master Test Plan are prepared before starting any project activities. A Project Plan may encompass multiple software changes and activities across multiple life cycle phases. A Master Test Plan summarizes the test activities to be performed in a project and their schedules.

3.1.2 Organization / Responsibilities

The basic software is developed through a combined effort of several technical sections within MELCO.

The ultimate responsibility for the development of the basic software lies with the “Design Section,” which is responsible for assuring that it is structured, staffed, and qualified to meet the rigorous and technical demands for developing and maintaining the basic software.

Development of the basic software is performed by the Design Section in conjunction with the “QA Section", "V&V Team" and “Manufacturing Department”.

The QA Section is responsible for assuring all activities conducted by MELCO throughout the MELTAC product life cycle (including activities of the Design Section, V&V Team and Manufacturing Department) follow the required regulations, standards, this SPM, and internal MELCO policies and procedures. QA audits are conducted independently from any activities or assessments of the Design Section, V&V Team or Manufacturing Department. MELCO maintains a 10 CFR 50 Appendix B ~~Q~~quality ~~A~~assurance program~~Plan~~ (MELCO’s 10 CFR 50 Appendix B QAP) which is MELCO’s quality assurance program compliant with 10 CFR 50 Appendix B and 10 CFR 21~~that is implemented via NQA-1~~. ToR-1

The V&V Team executes independent V&V activities in accordance with the SVVP. The V&V Team is responsible for confirming the correctness of the basic software, including the portions of the software that are critical to safety functions.

The Manufacturing Department manufactures the MELTAC platform hardware modules and performs installation of the basic software on each hardware module during the production process.

The organization chart relating to MELTAC platform development and maintenance is described in Figure 3.1-1.

ToR-1

ToR-1

]

ToR-1

ToR-1

3.3 Software Quality Assurance Plan

3.3.1 Purpose and Scope

The purpose of the Software Quality Assurance Plan (SQAP) is to describe the quality assurance requirements and methods used to assure high quality of the basic software throughout the basic software life cycle process.

The requirements of this SQAP as well as this entire SPM shall be implemented by procedures controlled in accordance with MELCO's 10 CFR 50 Appendix B Quality Assurance Program (MELCO's 10 CFR 50 Appendix B QAP). All responsible groups that are assigned activities described in this SPM shall follow these implementing procedures. ToR-1

The quality of the following basic software life cycle process documents outputs shall be assured through the methods and processes described in this SQAP:

- Project Plan as described in the SMP
- Design documentation (Platform Specification, Software Specification, Program Specification, and FPGA Specification)
- Source code (for processor software and for FPGA)
- Test Descriptions, Test Specifications, and Test Reports (as described in the SVVP and the STP)

3.3.2 Organization / Responsibilities

The organization of the groups responsible for basic software quality is described in Section 3.1.2.

The QA Section and the V&V Team shall be independent from Design Section and Manufacturing Department members. V&V Team independence is described in detail in the SVVP.

The class of the QA Manager within the overall MELCO organization hierarchy is equivalent or higher than the classes of all managers of any other organization.

The Design Section Manager is responsible for ensuring that all basic software design activities are performed as described in accordance with the SDP.

The Design Section shall generate and maintain the design outputs throughout the basic software life cycle as described in the SDP and shall also assure their correctness through reviews by Design Review Engineers.

The Design Section is responsible for performing the software safety analysis activities described in the SSP.

The V&V Team Manager is responsible for ensuring that all the V&V activities are executed independently by the V&V Team, including software safety analysis V&V activities, as described in the SVVP.

The QA Manager is responsible for assuring that the planned software development and V&V activities are appropriately conducted by these sections in accordance with this SPM and

3.1.4 Staff Position 4

Requirement
The communication process itself should be carried out by a communications processor[ii] separate from the processor that executes the safety function, so that communications errors and malfunctions will not interfere with the execution of the safety function. The communication and function processors should operate asynchronously, sharing information only by means of dual-ported memory or some other shared memory resource that is dedicated exclusively to this exchange of information. The function processor, the communications processor, and the shared memory, along with all supporting circuits and software, are all considered to be safety-related, and must be designed, qualified, fabricated, etc., in accordance with 10 C.F.R. Part 50, Appendix A and B. Access to the shared memory should be controlled in such a manner that the function processor has priority access to the shared memory to complete the safety function in a deterministic manner. For example, if the communication processor is accessing the shared memory at a time when the function processor needs to access it, the function processor should gain access within a timeframe that does not impact the loop cycle time assumed in the plant safety analyses. If the shared memory cannot support unrestricted simultaneous access by both processors, then the access controls should be configured such that the function processor always has precedence. The safety function circuits and program logic should ensure that the safety function will be performed within the timeframe established in the safety analysis, and will be completed successfully without data from the shared memory in the event that the function processor is unable to gain access to the shared memory.
Analysis

ToR-1

3.3 Analysis of Command Prioritization (Section 2 of ISG-04)

This section provides an analysis of the MELTAC platform command prioritization features. The Staff Positions in ISG-04 Section 2 are used as criteria for this analysis.

The MELTAC platform includes a Power Interface (PIF) Module to implement priority logic. The PIF Module employs state-based priority logic to ensure that either the primary system (e.g. the safety system) or backup system (e.g. the Diverse Actuation System) can place the component in its preferred safety state. This state-based priority logic is implemented on an Interposing Logic (IPL) sub-board mounted on the PIF Module that controls the component in direct response to external contact inputs, independent of the MELTAC controller output commands. There are several types of IPL sub-boards for different types of plant components (e.g.: switchgears, solenoid valves, etc.). Each PIF Module is configured with the appropriate IPL sub-board for the component being controlled. The IPL is realized by discrete logic Integrated Circuits.

3.3.1 Staff Position 1

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

ToR-1

3.3.7 Staff Position 7

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

ToR-1