Safety System Digital Platform - MELTAC - Topical Report

Non-Proprietary

April 2016

Prepared:	Susumu Okuda Susumu Okuda, Engineer Control & Protection Systems Section	Apr. 25, 2016 Date	Kazuhiro Eguchi Kazuhiro Eguchi, Manager Radiation Monitoring Instrumentation Section	Apr. 25. 2016 Date	
Reviewed:	Manabu Taniguchi Manabu Taniguchi, Manager Control & Protection Systems Section	Apr. 25. 2016 Date	Shingo Nakamura Shingo Nakamura, Manager Radiation Monitoring Instrumentation Section	Apr. 25, 2016 Date	
Approved:	Shigeru Sugitani Shigeru Sugitani, Senior Manager Control & Protection Systems Section	Apr. 25. 2016 Date	Yasuo Uranaka Yasuo Uranaka, Senior Manager Radiation Monitoring Instrumentation Section	Apr. 25, 2016 Date	

Approved:	H. Funakoshi Hisashi Funakoshi, General Manager Nuclear Power Department	Apr. 25. 2016 Date
Approved:	Hideki Matsui Hideki Matsui, QA Manager Energy Systems Center	Apr. 26. 2016 Date

Signature History

	Rev.0, April 2014			
Prepared	Hitomi Sasaki			
	Masaki Taguchi			
Reviewed	Manabu Taniguchi			
	Shingo Nakamura			
Approved	Hidetoshi Matsushita			
	Yasuo Uranaka			
	Katsumi Akagi			
	Hirotoshi Ohkawa			

Revision History

Revision	Date	Page (section)	Description
0	April 2014	All	Initial issue
1	April 2016	9 (3)	Corrected item No.24 description. (Remove reference to Appendix C)
		13 (3)	Modified the reference version of IEEE Std. 1028. (1997 -> 2008)
		31,32 (4.1.1.4)	Added “EMC” and “EMS” to Table4.1.1-2
		34 (4.1.2.1)	Deleted the description of Slide-split CPU Chassis.
		38,39,182, 183 (4.1.2.3, 5.5)	Deleted the description of Binary Isolation Module (KIDJ) including Figure 4.1-2-3, 5.5-3, 5.5-4.
		223 (A.5)	Modified the specification for the MRTJ Module in Table A.5. From “32 to 392°F (0 to 200°C) to 32 to 752 °F (0 to 400 °C)”
		226 (A.5)	Deleted the contact input (external contact power supply) type MDIJ from Table A.7. Deleted the DC24 V type MDIJ Module from Table A.7.

Revision	Date	Page (section)	Description
		227 (A.5)	Deleted the closed contact type MDOJ Module from Table A.8.
		228 (A.6)	Deleted the KIDJ Module from Table A.10.
		229 (A.6)	Deleted the KEXJ Module from Table A.11.
		231 (A.8)	Deleted the DPLJ Module from Table A.13.
		232 (A.9)	Deleted the description of Slide-split CPU Chassis from the PPSJ Module specification of Table A.14.
		239 (A.16)	Deleted the Slide-split Chassis from Table A.21.
		240 (A.17)	Deleted the following from Table A.24. • Digital (DI/DO)(Lift/Jumper function) • Digital (With specific cable for power supply)(Lift function)

Mitsubishi Electric Corporation
7-3, Marunouchi 2-chome, Chiyoda-ku
Tokyo 100-8310 Japan

Abstract

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

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

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

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

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

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

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

- The detailed description of the hardware and software of the MELTAC platform, including digital processing, human systems interfaces (HSI) and digital communication interfaces and the detailed description of the MELTAC application development tools
- The equipment qualification of the MELTAC platform and its conformance to the corresponding U.S. standards
- The life cycle and the Quality Assurance Program (QAP) of the MELTAC platform and conformance to U.S. regulatory criteria
- The equipment reliability of the MELTAC platform and how that reliability is used to determine the reliability of any MELTAC safety application

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

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

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

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

Table of Contents

List of Tables

List of Figures

List of Acronyms

AI	Analog Input
ANSI	American National Standards Institute
AO	Analog Output
ASME	American Society of Mechanical Engineers
BTP	Branch Technical Position
CCF	Common Cause Failure
CCP	Component Control Processor
CEAS	Corporate Electronic Archive System
CFR	Code of Federal Regulations
COTS	Commercial Off-The-Shelf
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
DAS	Diverse Actuation System
DI	Digital Input
DO	Digital Output
DSP	Digital Signal Processor
ECC	Error Correcting Code
EEPROM	Electronically Erasable Programmable Read Only Memory
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EMS	Electromagnetic Susceptibility
ESD	Electrostatic Discharge
ESF	Engineered Safety Features
EUT	Equipment under Test
E/O	Electrical/Optical
FBD	Functional Block Diagram
FIT	Failure Rate
FMEA	Failure Mode and Effect Analysis
FMU	Frame Memory Unit
FPGA	Field Programmable Gate Array
F-ROM	Flash Read Only Memory
F/W	Firmware
GBD	Graphical Block Diagram
GDC	General Design Criteria
GUI	Graphical User Interface
HFE	Human Factor Engineering
HSI	Human System Interface
ID	Identification
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IPL	Interposing Logic
ISO	International Standardization Organization
IT	Information Technology
ITAAC	Inspections, Tests, Analyses, and Acceptance Criteria
I/O	Input/Output
I&C	Instrumentation and Control

JEC	Japanese Electrotechnical Committee
JIS	Japanese Industrial Standards
JEIDA	Japan Electronic Industry Development Association
LCO	Limiting Conditions for Operation
LED	Light Emitting Diode
MCB	Main Control Board
MCR	Main Control Room
MELCO	Mitsubishi Electric Corporation
MELTAC	Mitsubishi Electric Total Advanced Controller
MEPPI	Mitsubishi Electric Power Products Inc.
MIC	Memory Integrity Check
MRP	MELTAC Re-evaluation Program
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair
NC	Normally Closed
NI	Nuclear Instrumentation
NO	Normally Open
NRC	Nuclear Regulatory Commission
OBE	Operating Basis Earthquake
PIF	Power Interface
POL	Problem Oriented Language
QA	Quality Assurance
QAP	Quality Assurance Program
PCS	Plant Control System
PSS	Plant Safety System
RAM	Random Access Memory
RCP	Reactor Coolant Pump
RFI	Radio Frequency Interference
RG	Regulatory Guide
RGB	Red/Green/Blue
RM	Radiation Monitoring
ROM	Read-Only Memory
RPR	Resilient Packet Ring
RPP	Reactor Protection Processor
RTD	Resistance Temperature Detector
SCMP	Software Configuration Management Plan
SDOE	Secure Development and Operational Environment
SDP	Software Development Plan
SIntP	Software Integration Plan
SInstP	Software Installation Plan
SMC	Self-diagnosis Memory Check
SMP	Software Management Plan
SPM	Software Program Manual
SQAP	Software Quality Assurance Plan
SSE	Safe Shutdown Earthquake
SSP	Software Safety Plan
STP	Software Test Plan
S-VDU	Safety VDU
SVVP	Software Verification and Validation
VDU	Visual Display Unit
V&V	Verification and Validation

UDP/IP	User Datagram Protocol Internet Protocol
UTP	Unshielded Twist Pair Cable
WDT	Watchdog Timer

1.0 PURPOSE

The purpose of this Topical Report is to describe the Mitsubishi Electric Total Advanced Controller (MELTAC) platform and its conformance to the U.S. Nuclear Regulatory requirements for nuclear safety systems. The MELTAC platform can be used for safety and non-safety I&C systems. The modular structure of the platform allows it to be applied to solve most utility needs for safety applications, including new systems, component replacements and complete system replacements.

The MELTAC platform can be applied to nuclear safety systems such as the reactor protection system, engineered safety features actuation system, safety-related HSI system, and any other safety system. In addition, the MELTAC platform can be applied to non-safety systems. The MELTAC equipment applied for non-safety applications is the same design as the equipment for safety applications. However, there are software and hardware components that are unique to non-safety applications. These components have differences in Quality Assurance methods for software design and other software life cycle processes.

Therefore, MELTAC components that are applicable to either safety or non-safety applications are identified as “MELTAC Nplus S”; components that are only applicable to non-safety applications are identified as “MELTAC Nplus”. These identifier distinctions apply to all aspects of MELTAC, including hardware, software, documentation and engineering tools.

The following terminology is used in this section and throughout this document:

> Application Licensing Documentation – This refers to application specific documentation for a group of plants or a single plant, such as the Design Certification Document, Combined Operating Licensing Application, Final Safety Analysis Report, or License Amendment Request.
>
> Equipment - This refers to the components that are the subject of this Topical Report. “Equipment” includes the MELCO safety-related digital I&C platform. “Equipment” does not include the MELCO non-safety digital I&C or HSI platforms, unless specifically identified.

2.0 SCOPE

The scope of this report includes the hardware and software associated with the MELTAC Nplus S platform. Components unique to the MELTAC Nplus platform for non-safety applications are not discussed, except to the extent of their interface with MELTAC Nplus S components in safety systems. The MELTAC platform described herein encompasses design, qualification, and reliability.

3.0 APPLICABLE CODE, STANDARDS AND REGULATORY GUIDANCE

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

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

Code of Federal Regulations

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

GDC 1: Quality Standards and Records

The lifecycle process for the Basic components of the MELTAC platform that meets all requirements of 10 CFR Part 50 Appendix B is described in Section 6. This is referred to as the App.B-based quality assurance program (QAP).

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

GDC 2: Design Bases for Protection against Natural Phenomena

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

GDC 4: Environmental and Dynamic Effects Design Bases

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

GDC 21: Protection System Reliability and Testability

This Equipment includes automated testing with a high degree of coverage, and additional overlapping manual test features for the areas that are not covered by automated tests. All manual tests may be conducted with the plant on line, with consideration of plant specific accessibility, and with the Equipment bypassed or out of service. Depending on the system design for a specific plant, the Equipment is configured with N or N+1 redundancy, where N is the number of divisions needed for single failure compliance and to meet the plant reliability goals. For systems with N+1 redundancy, this GDC is met with one division continuously bypassed or out of service. The redundancy configuration for each plant system is described in Application Licensing Documentation.

GDC 22: Protection System Independence

Redundant divisions are physically and electrically isolated to ensure that failures that originate in one division cannot propagate to other divisions. Physical isolation is discussed in Application Licensing Documentation. Platform features to accommodate electrical isolation are discussed in this Topical Report.

All Equipment is qualified to ensure that the Equipment is unaffected by adverse conditions that may concurrently affect multiple divisions. The qualification limits of this equipment are described in this Topical Report. Application Licensing Documentation describes the specific analysis for each plant.

Interlocks between redundant divisions and administrative controls ensure maintenance is performed on one division at a time. Interlocks and administrative controls are described in Application Licensing Documentation.

GDC 23: Protection System Failure Modes

Signals are generated for all detected failures. These signals can be configured at the application level to generate alarms. Functions can be designed to fail to an actuated trip state on loss of all power, on failures that are not automatically detected, or on failures that are automatically detected and would prevent proper execution of the function. Functions can also be designed to fail to an unactuated state. The unactuated state may be desirable to avoid spurious plant transients. Compliance for reactor trip and engineered safety features actuation functions are application specific and described in Application Licensing Documentation.

GDC 24: Separation of Protection and Control Systems

The separation of protection and control systems is an application specific design characteristic. Redundant divisions of the protection systems are physically and electrically isolated from the non-safety control systems. Where safety sensors are shared between control and protection systems, signal selection logic is typically used in the control system to prevent erroneous control actions due to single sensor failures. Eliminating these erroneous control actions prevents challenges to the protection system while it is degraded due to the same sensor failure. Where non-safety signals control safety systems or components, logic in the safety systems is typically used to ensure prioritization of safety functions. The details regarding the separation of protection and control systems are described in Application Licensing Documentation.

2. 10 CFR Part 50.55a

(a)(1) Quality Standards for Systems Important to Safety
Section 6 describes the App.B-based QAP, which is fully compliant to 10 CFR 50 Appendix B.

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

(h) Invokes IEEE Std. 603-1991

See conformance to IEEE Std. 603-1991

NRC Regulatory Guides

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

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

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

   The Equipment is designated Seismic Category I.

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

   endorses IEEE Std. 379-2000

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

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

   endorses IEEE Std. 384-1992

   The MELTAC platform contains features to ensure that redundant safety divisions are physically and electrically independent of each other and physically and electrically independent of any non-safety divisions. Physical independence is maintained either by the required distance or by barriers which prevent propagation of fire or electrical faults. Electrical independence is maintained by fiber optic cable communication interfaces or conventional isolators, such as opto-couplers, relays or transformers. Conventional isolators include fault interrupting devices such as fuses or circuit breakers. Fiber optic cable communication interfaces are described in Section 4.3.2 (Control Network), 4.3.3 (Data Link) and 4.3.4 (Maintenance Network). Specifications and qualification of conventional isolators are discussed in Section 4.1.2 and 5.5 of this Topical Report, respectively.

7. RG 1.89 Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants (Rev. 1, June 1984)

endorses IEEE Std. 323-1974

The environmental qualification of this Equipment is by an appropriate combination of type testing and analysis. This Equipment is qualified for use in a mild environment that is not adversely affected by plant accidents. Qualification for temperature and humidity is by type test. The generic MELTAC temperature and humidity qualification is demonstrated to envelope actual plant conditions by analysis of room ambient conditions and heat rise calculations for the installed configuration. Seismic qualification is by type testing. The generic MELTAC seismic qualification is demonstrated to envelope actual plant conditions by analysis of floor response spectrum at the installed location. Electromagnetic Interference (EMI) qualification is by type testing. MELTAC is generically qualified to the EMI envelope and acceptance criteria that are identified by regulatory guidance as enveloping US nuclear plant installations; therefore there is no additional site specific EMI qualification.

This Equipment has no known aging mechanisms, except as noted in Section 7.4 and accommodated by periodic replacement; random failures will be detected through self-diagnoses and periodic surveillance testing. Type testing for conformance to RG 1.89 is described through the aggregate of all qualification reports – Environmental, Seismic and Electromagnetic Compatibility (EMC), see Section 5.

8. RG 1.100 Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants (Rev. 3, September 2009)

This Equipment is designated Seismic Category I. It is designed and qualified to withstand the cumulative effects of a minimum of 5 Operating Basis Earthquakes (OBEs) and one Safe Shutdown Earthquake (SSE) without loss of safety function or physical integrity. The input spectrum is selected to envelope all anticipated applications. Conformance to this envelope for specific applications is discussed in Application Licensing Documentation.

9. RG 1.105 Setpoints for Safety-Related Instrumentation (Rev. 3, December 1999)

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

The uncertainties associated with the Equipment are described in this Topical Report. Appendix A.5 defines I/O module accuracies. Appendix A.6 defines Isolation Module accuracies. Appendix A.9 defines accuracy of I/O power supplies. This includes uncertainties for signal conditioning modules, signal splitters, instrument loop power suppliers and analog to digital converters. The uncertainties associated with specific process instrumentation and the resulting safety-related setpoints are described in Application Licensing Documentation. The plant specific uncertainty/setpoint analysis is described in Application Licensing Documentation.

10. RG 1.118 Periodic Testing of Electric Power and Protection Systems (Rev. 3, April 1995)

endorses IEEE Std. 338-1987

See conformance to GDC 21, 10 CFR 50.36 and RG 1.22. The Equipment can be configured so that all safety functions are tested either automatically or manually, and so that manual tests do not require any system reconfiguration, such as jumpers or fuse removal.

11. RG 1.152 Criteria for Use of Computers in Safety Systems of Nuclear Power Plants (Rev. 3, July 2011)

endorses IEEE Std. 7-4.3.2-2003

The methods used for specifying, designing, verifying, validating and maintaining software for this Equipment conforms to these requirements, including requirements for a secure development environment and MELTAC features that facilitate a secure operational environment. The life cycle process for the MELTAC platform is described in “MELTAC Platform Software Program Manual” (JEXU-1041-1016).

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

The life cycle process for the system application software is described in the Application Licensing Documentation.

The methods used for ensuring a secure development and operational environment throughout the life cycle are described in these documents.

12. RG 1.153 Criteria for Safety Systems (Rev. 1, June 1996)

endorses IEEE Std. 603-1991

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

13. RG 1.168 Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants (Rev. 2, July 2013)

endorses IEEE Std. 1012-2004 and IEEE Std. 1028-2008

This Equipment uses processes for verification, validation, reviews and audits that conform to this Regulatory Guide. The software life cycle process for the MELTAC platform is described in “MELTAC Platform Software Program Manual” (JEXU-1041-1016). MELCO has undergone an inspection by NRC to verify the implementation of an adequate QAP.

The life cycle process for the system application software is described in the Application Licensing Documentation.

14. RG 1.169 Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants (Rev. 1, July 2013)

endorses IEEE Std. 828-2005 and IEEE Std. 1042-1987

This Equipment is designed and maintained using a Configuration Management process that conforms to this Regulatory Guide. The Configuration Management process for the MELTAC platform is described in “MELTAC Platform Software Program Manual” (JEXU-1041-1016). MELCO has undergone an inspection by NRC to verify the implementation of an adequate QAP.

The Configuration Management for the system application software is described in the Application Licensing Documentation.

15. RG 1.170 Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants (Rev. 1, July 2013)

endorses IEEE Std. 829-2008

The test documentation for this Equipment conforms to this Regulatory Guide. The test process and corresponding documentation for the MELTAC platform are described in “MELTAC Platform Software Program Manual” (JEXU-1041-1016). MELCO has undergone an inspection by NRC to verify the implementation of an adequate QAP.

The test documentation for the system application software is described in the Application Licensing Documentation.

16. RG 1.171 Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants (Rev. 1, July 2013)

endorses IEEE Std. 1008-1987

Unit testing for this Equipment conforms to this Regulatory Guide. The unit testing for the MELTAC platform is described in “MELTAC Platform Software Program Manual” (JEXU-1041-1016). MELCO has undergone an inspection by NRC to verify the implementation of an adequate QAP.

Unit testing for the system application software is described in the Application Licensing Documentation.

17. RG 1.172 Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants (Rev. 1, July 2013)

endorses IEEE Std. 830-1998

The Software Requirements Specifications for this Equipment conforms to this Regulatory Guide. The Software Requirements Specifications for the MELTAC platform are described in in Section 6.1 of this Topical Report. MELCO has undergone an inspection by NRC to verify the implementation of an adequate QAP.

The Software Requirements Specifications for the system application software are described in the Application Licensing Documentation.

18. RG 1.173 Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants (Rev. 1, July 2013)

endorses IEEE Std. 1074-2006

The Software Life Cycle Process for this Equipment conforms to this Regulatory Guide. The Software Life Cycle Processes for the MELTAC platform are described in “MELTAC Platform Software Program Manual” (JEXU-1041-1016). MELCO has undergone an inspection by NRC to verify the implementation of an adequate QAP.

The Software Life Cycle Processes for the system application software are described in the Application Licensing Documentation.

19. RG 1.180 Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related Instrumentation and Control Systems (Rev. 1, October 2003)

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

This Equipment conforms to the EMI/RFI (Radio Frequency Interference) requirements of this standard. Qualification testing for the digital platform is described in this Topical Report.

20. RG 1.204 Guidelines for Lightning Protection of Nuclear Power Plants (Rev. 0, November 2005)

The platform has been designed with surge resistance. Surge qualification testing has been performed using ANSI Std. 62.41, ANSI Std. 62.45, and IEEE Std. 472, see Section 5.3.

21. RG 1.209 Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants (Rev. 0, March 2007)

endorses IEEE Std. 323-2003

This Equipment is tested and analyzed to satisfy the mild environment qualification requirements.

NRC Branch Technical Positions

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

The Equipment includes extensive self-diagnosis tests which run continuously. The LCO related to bypassed or out of service conditions for a single division are dependent upon the extent of redundancy and the extent of automated self-testing for the equipment that remains in service to perform the safety function. The Equipment can be configured at the application level with additional manual test features to test the portions of the system that are not tested automatically. These manual test features can be configured so that all

functions of the protection system are testable at power. Self-diagnosis tests are described in Section 4.1.5 of this Topical Report. Manual test features are described in Section 4.1.7 and 4.2.4 of this Topical Report, and also in Application Licensing Documentation.

23. BTP 7-11 Guidance on Application and Qualifications of Isolation Devices

endorses IEEE Std. 472, ANSI Std. C62.36, ANSI Std. C62.41, ANSI Std. C62.45

See conformance to RG 1.75. Isolation devices are qualified in conformance to these standards.

24. BTP 7-14 Guidance on Software Reviews for Digital Computer-Based I&C Systems

See conformance to RG 1.168 through 1.173.

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

See conformance to GDC 21, 10 CFR 50.36, RG 1.22 and RG 1.118. Surveillance testing taken together with automatic self-testing provides a mechanism for detecting all failures. The methods used for testing are described in Application Licensing Documentation.

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

The real-time performance for this Equipment conforms to this BTP. The response time performance for digital platform components is described in Section 4.4 of this Topical Report. Requirements for system response time for conformance with the plant design basis and the response time of actual plant systems is described in Application Licensing Documentation.

NUREG-Series Publications (NRC Reports)

27. NUREG-0737, Supplement 1 Clarification of TMI Action Plan Requirements

This Equipment can be configured at the application level for conformance to the following TMI Action Plan Requirements:

- Plant Safety Parameter Display – This Equipment can provide safety-related data to the non-safety HSI system which can provide this display for the control room and for emergency support facilities.
- Indication and Control for Safety Components (e.g.: relief valves, pressurizer heaters, containment isolation valves), Inadequate Core Cooling Monitoring and Instrumentation for Accident Monitoring - This Equipment can provide safety-related controls and monitoring for safety-related instruments to generate safety-related displays. Alarms and non-safety displays can be generated by the non-safety HSI system.

28. NUREG-0800 Chapter 7 of the USNRC Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, Section 7.1 Rev.5

    This Equipment fulfills all safety-related requirements of this NUREG for monitoring safety-related plant instrumentation and controlling safety-related plant components. Descriptions of specific plant systems are described in Application Licensing Documentation.

29. NUREG/CR-6303 Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems

    The design of this Equipment is described in this Topical Report. Functional diversity within the safety and non-safety I&C systems is described by the Application Licensing and design documentation.

30. NUREG/CR-6421 A Proposed Acceptance Process For Commercial-Off-The-Shelf (COTS) Software in Reactor Applications

    This NUREG is not applicable to this Equipment since there is no COTS software. All software has been designed for nuclear applications.

Digital Instrumentation and Controls (DI&C) Interim Staff Guidance (ISG)

31. DI&C-ISG-04 Highly-Integrated Control Rooms – Communications Issues (Rev 1,March 2009)
    A detailed discussion of the MELTAC platform communication systems and compliance with the requirements given in DI&C-ISG-04 is provided in Section 4.3 and “MELTAC Platform ISG-04 Conformance Analysis” (JEXU-1041-1015 Rev.0).

32. DI&C-ISG-06 Licensing Process (Rev 1, January 2011)
    DI&C-ISG-06 is intended for plant-specific licensing amendment requests (LARs) and lists the documents expected for a plant-specific review of a digital safety system. Some interpretation is required to identify the subset of documentation that applies to a generic review of a safety system digital platform. This interpretation and summary of DI&C-ISG-06 compliance is given in "Mapping of MELTAC Platform Licensing Documents to the DI&C-ISG-06 Guidance" (JEXU-1041-1012 Rev0).

IEEE Standards

33. IEEE Std. 7-4.3.2-2003 Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations

    This Equipment conforms to all requirements of this standard, as augmented by RG 1.152.

34. IEEE Std. 323-2003 Qualifying Class 1E Equipment for Nuclear Power Generating Systems

This Equipment is qualified in conformance to this standard, as augmented by RG 1.89. See conformance to RG1.89.

35. IEEE Std. 338-1987 Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems

The self-diagnosis that is usable for Periodic Surveillance Testing are described throughout this document. RG1.22 and Std. IEEE 338 test features that are configured at the system level or within the application software are described by the Application Licensing and design documentation.

36. IEEE Std. 344-2004 Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations

This Equipment conforms to this standard as augmented by RG 1.100. Conformance is described in the Section 5 of this Topical Report.

37. IEEE Std. 379-2000 Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems

As described in RG1.53 item 13, compliance to the Single-Failure Criterion is achieved through the configuration of this Equipment at the system level.

38. IEEE Std. 383-2003 Type Test of Class 1E Electric Cables, Field Splices, and Connections for Nuclear Power Generating Stations

The cable and electrical connections used within MELTAC cabinets conform to this standard, including requirements for flame retarding qualification. Cables for interfaces between MELTAC cabinets and interfaces to/from MELTAC cabinets to other I&C systems and components are discussed in Application Licensing Documentation.

39. IEEE Std. 384-1992 Criteria for Independence of Class 1E Equipment and Circuits

This Equipment supports conformance to this standard as augmented by RG 1.75. All safety functions implemented within multiple divisions can have physical separation and electrical independence between redundant safety divisions and between safety and non-safety divisions. Electrical independence between divisions is accomplished through the use of fiber optic cables or conventional qualified isolators. Digital data communication using fiber optic cables also facilitates physical independence between divisions. MELTAC components for electrical isolation are described in Section 4 (4.3.2.3) of this Topical Report.

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

Standard enclosures for this Equipment conform to this standard. These enclosures are described in this Topical Report. Equipment is clearly marked to

identify safety-related designations, as described in Section 6.1.8 Identification of Equipment. Other enclosures, including any deviations from this standard, are described in Application Licensing Documentation.

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

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

42. IEEE Std. 497-2002 Accident Monitoring Instrumentation for Nuclear Power Generating Stations

See conformance for RG 1.97.

43. IEEE Std. 603-1991 Safety Systems for Nuclear Power Generating Stations

1998 version is currently not endorsed by NRC

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

- Single failures
- Completion of Protective Action
- Quality
- Qualification
- Independence
- Testability
- Monitoring and Information
- Bypasses

Specifications corresponding to the key requirements above are described in Sections 4 through 7.

44. IEEE Std. 730-1989 Software Quality Assurance Plans

The Software Quality Assurance Plans are described in Section 6 and “MELTAC Platform Software Program Manual” (JEXU-1041-1016).

45. IEEE Std. 828-2005 IEEE Standard for Software Configuration Management Plans

The Software Configuration Management Plan is described in Section 6 and “MELTAC Platform Software Program Manual” (JEXU-1041-1016).

As the Standard of Configuration Management, ISG-06 refers to IEEE Std. 828-1990 and IEEE Std. 828-1998.

IEEE Std. 828-1998 contains the contents of IEEE Std. 828-1990.Therefore, this Topical Report refers IEEE Std. 828-1998 as the applicable standard.

46. IEEE Std. 829-2008 Software Test Documentation

The software test documentation is described in “MELTAC Platform Software Program Manual” (JEXU-1041-1016).

47. IEEE Std. 830-1998 IEEE Recommended Practice for Software Requirements Specifications

    The software requirements are documented in the Platform specification as an output of Requirement Phase, which is described in Section 6.1.

48. IEEE Std. 1008-1987 IEEE Standard for Software Unit Testing

    Software unit testing is described in “MELTAC Platform Software Program Manual” (JEXU-1041-1016).

49. IEEE Std. 1012-2004 IEEE Standard for Software Verification and Validation Plans

    Software V&V is described in “MELTAC Platform Software Program Manual” (JEXU-1041-1016).

50. IEEE Std. 1016-1987 IEEE Recommended Practice for Software Design Descriptions

    The software design description is documented in the Software Specifications as outputs of Design Phase which is described in Section 6.1.

51. IEEE Std. 1028-2008 IEEE Standard for Software Reviews and Audits

    Software reviews and audits are described in “MELTAC Platform Software Program Manual” (JEXU-1041-1016).

52. IEEE Std. 1042-1987 IEEE Guide To Software Configuration Management

    Configuration management is described in “MELTAC Platform Software Program Manual” (JEXU-1041-1016).

53. IEEE Std. 1074-2006 IEEE Standard for Developing Software Life Cycle Processes

    The software life cycle process is described in Section 6 and in “MELTAC Platform Software Program Manual” (JEXU-1041-1016).

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

    The communication between modules in the same subsystem of the MELTAC platform conforms to this standard.

Other Industry Standards

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

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

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

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

57. IEC 61000 Electromagnetic compatibility (Basic EMC publication)

This Equipment conforms to the following sections of this standard:

- IEC 61000-4-2: Testing and measurement techniques - Electrostatic discharge immunity tests. Basic EMC publication
- IEC 61000-4-4: Testing and measurement techniques - Electrical fast transient/burst immunity test. Basic EMC publication
- IEC 61000-4-5: Testing and measurement techniques - Surge immunity test
- IEC 61000-4-12: Testing and measurement techniques - Oscillatory waves immunity test.

58. ISA-S67.04-1994 Setpoints For Nuclear Safety Related Instrumentation Used in Nuclear Power Plants

See conformance to RG 1.105. The methodology used to develop setpoints is described in Application Licensing and Design Documentation.

59. MIL-STD-461E Requirements for the Control of Electromagnetic Interference Characteristics of subsystems and equipment

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

4.0 MELTAC PLATFORM DESCRIPTION

The MELTAC platform is based on using qualified building blocks that can be used for many safety system applications. The building blocks are the following items.

- Controller
- Safety VDU (Visual Display Unit) panel and processor
- Control Network
- Data Link

The MELTAC platform can take a single controller configuration, redundant standby controller configuration, or redundant parallel controller configuration, depending on the system requirements. The I/O modules can also take a redundant configuration. The MELTAC platform includes a large variety of I/O modules that can interface with various plant components (See Section 4.1). Also, the MELTAC platform includes a safety VDU which consists of a safety VDU panel and processor (See Section 4.2). The Control Network is used to communicate safety-related data between multiple controllers, and between controllers and the safety VDU processor(s) in the same division. The Data Link is used to transmit process signals between the controllers in different safety divisions or trains (See Section 4.3).

A typical configuration of the MELTAC platform for a safety system is shown in Figure 4.0-1. It shows a single division of a Plant Safety System (PSS) with an interface to a different division via Data Link. It also shows Controllers, which are the main component of the MELTAC platform, as the Reactor Protection Processor (RPP) and the Plant Safety System Component Control Processor (PSS-CCP).

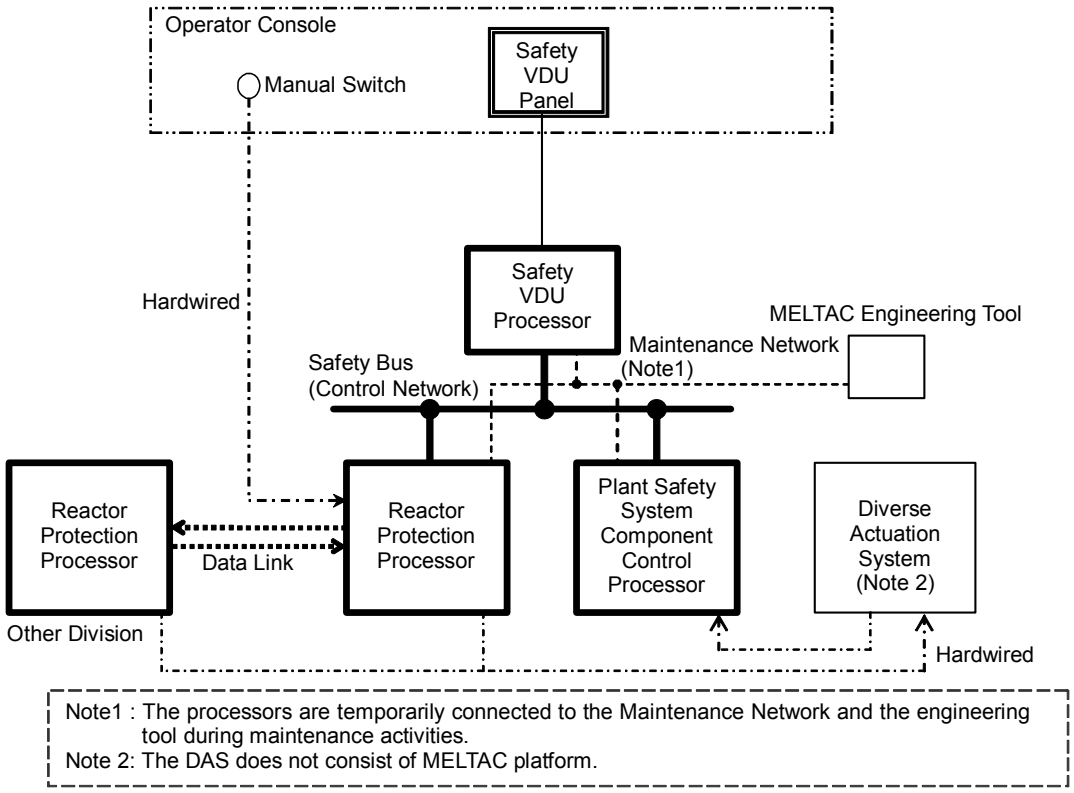


Figure 4.0-1 MELTAC Platform Typical PSS Configuration

The PSS provides monitoring and displays for safety-related plant instrumentation, and automated actuation and manual control of safety-related plant components. It consists of multiple independent safety divisions.

The PSS consists of the following items described in a) to g).

a) Each PSS division typically contains one Reactor Protection Processor (RPP). The RPP is a MELTAC controller with associated I/O modules. The RPP performs the following key functions:
   - Execute reactor trip (RT) functions and Engineered Safety Features (ESF) functions
   - Receive RT and ESF initiation signals from the RPPs of other divisions via inbound inter-division Data Links, and transmit those same signals from its own division to the other divisions via an outbound inter-division Data Link
   - Direct actuation of RT Breakers (RTB)
   - Transmit Interlock and ESF initiation signals via the intra-division Control Network to PSS Component Control Processors (PSS-CCPs)
   - Receive manually initiated control commands from the safety Visual Display Unit (VDU) processors via the intra-division Control Network
   - Transmit the monitored plant sensor data and status to the safety VDU processors via the intra-division Control Network

b) The number of PSS-CCPs per division is application specific. Each PSS-CCP is a MELTAC controller with associated I/O modules. The PSS-CCPs perform the following key functions:

- Control and drive the plant components and equipment by ESF actuation signal from the RPP
- Receive ESF actuation signals from the RPP via the intra-division Control Network
- Receive manual component control commands from the safety VDU processors via the intra-division Control Network
- Receive diverse component control signals from the Diverse Actuation System (DAS), and combine the signals with the control signals from the PSS-CCPs within the hardware based Interposing Logic (IPL) of the Power Interface (PIF) Module to determine the final control command relayed to each plant component
- Transmit the monitored status of interlocks and components to the safety VDU processors via the intra-division Control Network

c) Each PSS division typically contains at least one safety VDU processor and safety VDU panel. The safety VDU processor and safety VDU panel consist of a special purpose MELTAC controller, peripherals, and an LCD touch screen. The safety VDU processor and safety VDU panel perform the following key functions:
   - Transmit the operation signals to the RPP and PSS-CCPs via the intra-division Control Network, and can be configured to provide the human-machine interface
   - Receive plant sensor data, RT and ESF initiation, and actuation status from the RPP via the intra-division Control Network
   - Receive interlock and component status data from the PSS-CCPs via the intra-division Control Network
   - Receive touch commands from safety VDU panel

d) There is one MELTAC engineering tool connected via Maintenance Network in each PSS division used exclusively for the following functions within that one division:
   - To display self-test diagnostics reported from all PSS processors within the division
   - To store copies of software for all processors within the division, and to conduct the manually initiated Memory Integrity Check (MIC) using that stored software
   - To control the updating of software for any processor within the division, utilized only when a processor is taken out-of-service and declared inoperable by plant Technical Specifications and the processor CPU Module is removed and transferred to the dedicated Re-programming Chassis
   - To control simulated input values for troubleshooting any processors within the division, only when a processor is taken out-of-service and declared inoperable by plant Technical Specification

e) There is one Control Network in each PSS division used for the following key intra-division communication functions:
   - Interlock and ESF initiation signals from the RPP to the PSS-CCPs
   - Manual control commands from the safety VDU processor to the RPP and the PSS-CCPs
   - Monitored plant sensor data, RT and ESF initiation, and actuation status from the RPP to the safety VDU processor
   - Monitored plant sensor data, interlock and component status data from the PSS-CCPs to the safety VDU processor

f) There is one Data Link in each PSS division used for broadcasting RT and ESF initiation signals from one PSS division to each of the other divisions.

g) Each PSS division typically contains Manual Switches. Manual Switches manually initiate the same RT and ESF functions that are automatically initiated by the RPP. The switch for each function interfaces with the RPP using conventional hardwired interfaces.

4.1 Controller

4.1.1 Hardware Configuration

The controller for the MELTAC platform consists of the following parts.

a) 1 CPU Chassis including 1 or 2 subsystems, 1 Switch Panel, 1 or 2 Status Display (and Switch) Modules, and 1 Fan Unit. Each subsystem consists of 1 or 2 Power Supply Modules, a CPU Module, 1 or more Control Network I/F Modules, a System Management Module, and 1 or more Bus Master Modules. Each subsystem communicates with the Control Network via its own Optical Switch.
b) Multiple I/O Chassis, each with multiple I/O modules

4.1.1.1 Configuration Concept

The MELTAC platform is capable of operating in any of the 3 following configurations:

a) Single Controller Configuration
The controller includes 1 subsystem. The subsystem operates in Control Mode. (Control Mode means the subsystem controls the outputs to plant components.)
b) Redundant Parallel Controller Configuration
The controller includes 2 subsystems. Each subsystem operates in Control Mode.
c) Redundant Standby Controller Configuration
The controller includes 2 subsystems. 1 subsystem operates in Control Mode while the other subsystem operates in Standby Mode. Standby Mode means the subsystem is closely monitoring the operation of the subsystem in Control Mode, including memory states. If that subsystem fails, the subsystem operating in Standby Mode will automatically switch to Control Mode, with no bump in the control outputs.

The configuration to be applied is determined based on the application system requirements. Any of the 3 configurations may be applied to safety systems.

For redundant configurations, the internally redundant subsystems are only for reliability enhancement. This redundancy is not credited for single failure compliance. Single failure compliance is achieved through multiple controllers located in physically separate and independent safety divisions.

4.1.1.1.1 Single Controller Configuration

The single controller configuration is shown in Figure 4.1.1-1.

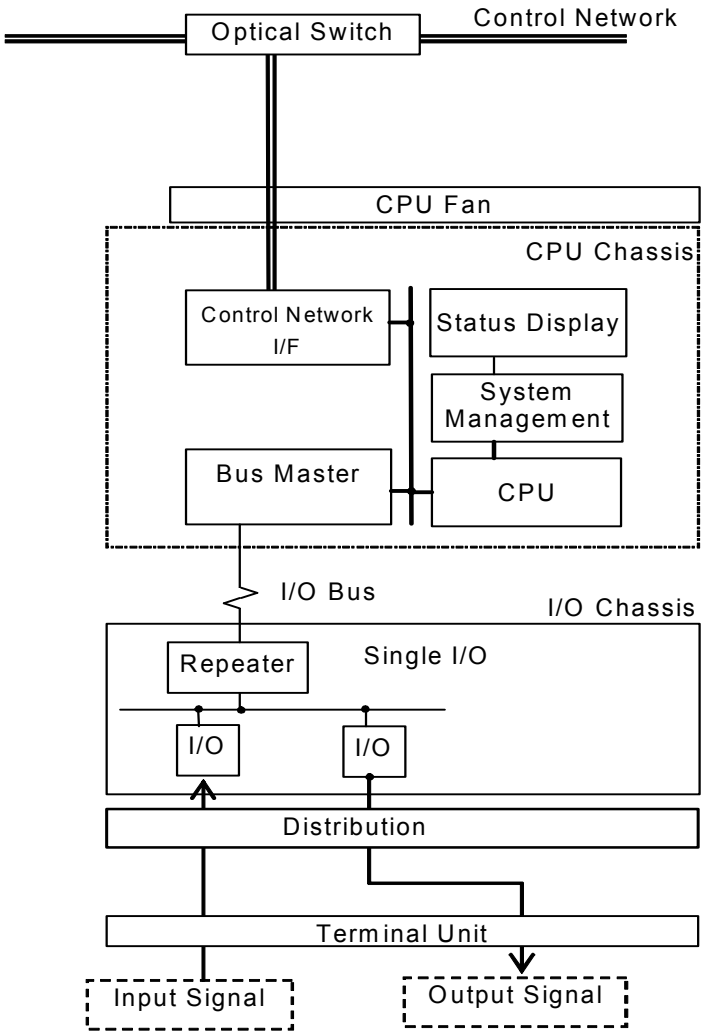


Figure 4.1.1-1 Single Controller Configuration

The single controller consists of the following:

a) CPU Chassis

The CPU Chassis includes 1 subsystem and a CPU Fan. A subsystem consists of a CPU Module, System Management Module, Status Display Module, Control Network I/F Module, and Bus Master Module. A subsystem communicates with the Control Network via its own Optical Switch. A subsystem is capable of driving a number of Control Network I/F Modules and Bus Master Modules depending on the scale of the application.

b) I/O Chassis

The I/O Chassis includes only single I/O. Single I/O consists of a Repeater Module and multiple I/O modules. Each I/O module communicates with the Bus Master Module in the subsystem via the Repeater Module and the I/O bus.

The I/O modules receive signals from sensors and send control outputs to components via the Terminal Unit and Distribution Module. For single I/O, the Distribution Module works as a surge absorber between the I/O modules and the Terminal Unit which connects external cables.

4.1.1.1.2 Redundant Parallel Controller Configuration

The redundant parallel controller configuration is shown in Figure 4.1.1-2. This configuration can only be used within the same division (i.e.: the redundant subsystems cannot be in different divisions), because there is no electrical or functional independence between subsystems.

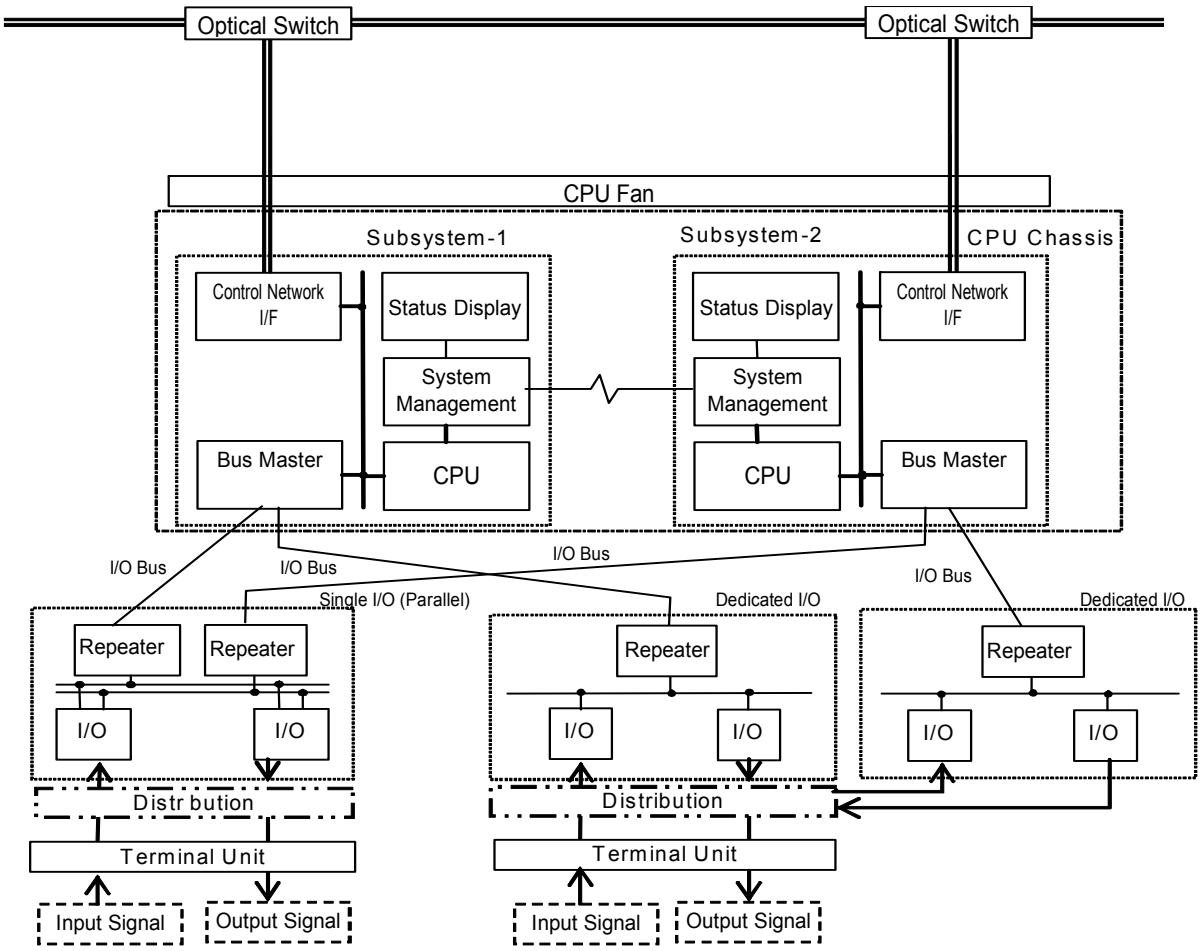


Figure 4.1.1-2 Redundant Parallel Controller Configuration

The redundant parallel controller consists of the following:

a) CPU Chassis

The CPU Chassis includes Subsystem-1, Subsystem-2, and a CPU Fan. Both subsystems have the same configuration. Each subsystem consists of a CPU Module, System Management Module, Status Display Module, Control Network I/F Module, and Bus Master Module. Each subsystem communicates with the Control Network via its own Optical Switch. The subsystem is capable of driving a number of Control Network I/F Modules and Bus Master Modules depending on the scale of the application.

In the redundant parallel controller configuration, both subsystems operate in Control Mode. Each subsystem operates independently. However, when a subsystem initially starts, the Data

Link between the System Management Modules allows all state based logic to be updated, if the other subsystem is already in Control Mode. Since both systems operate in Control Mode, there is no subsystem changeover to accommodate a subsystem failure as in the redundant standby configuration.

The Status Display Module displays the mode and alarms of the subsystem.

b) I/O Chassis

The redundant parallel controller can be configured with either redundant I/O (called dedicated I/O) and/or non-redundant I/O (called single I/O).

For single I/O, each non-redundant I/O module communicates with the Bus Master Modules in Subsystem-1 and Subsystem-2 via separate Repeater Modules and the redundant I/O bus. The single I/O, redundant Repeater Modules, and redundant I/O bus are all contained within the same I/O Chassis. The data from each non-redundant input module is communicated to both subsystems. The output control signals from each subsystem are logically combined within the non-redundant output modules. Each output can be individually configured using 1-out-2 or 2-out-of-2 voting logic, as needed for the specific application. The single I/O for a redundant parallel controller is referred to as single I/O (Parallel) to distinguish it from the single I/O for a single controller. Single I/O (Parallel) provides interfaces for the redundant I/O bus and the redundant subsystems.

To enhance I/O reliability, a redundant parallel controller can also be configured with redundant dedicated I/O. Dedicated I/O is distributed in 2 separate I/O Chassis. Each chassis consists of a Repeater Module and multiple dedicated I/O modules. Each dedicated I/O module communicates with the Bus Master Module in only 1 subsystem via the Repeater module and the I/O bus within the chassis. Therefore, each dedicated I/O module is subordinate to Subsystem-1 or Subsystem-2. The same input signals are distributed to each dedicated I/O module via the Distribution Module. And output signals from each dedicated I/O module are combined in the Distribution Module by using wired OR logic.

The Terminal Units for dedicated I/O are the same as for single I/O.

4.1.1.1.3 Redundant Standby Controller Configuration

The redundant standby controller configuration is shown in Figure 4.1.1-3.

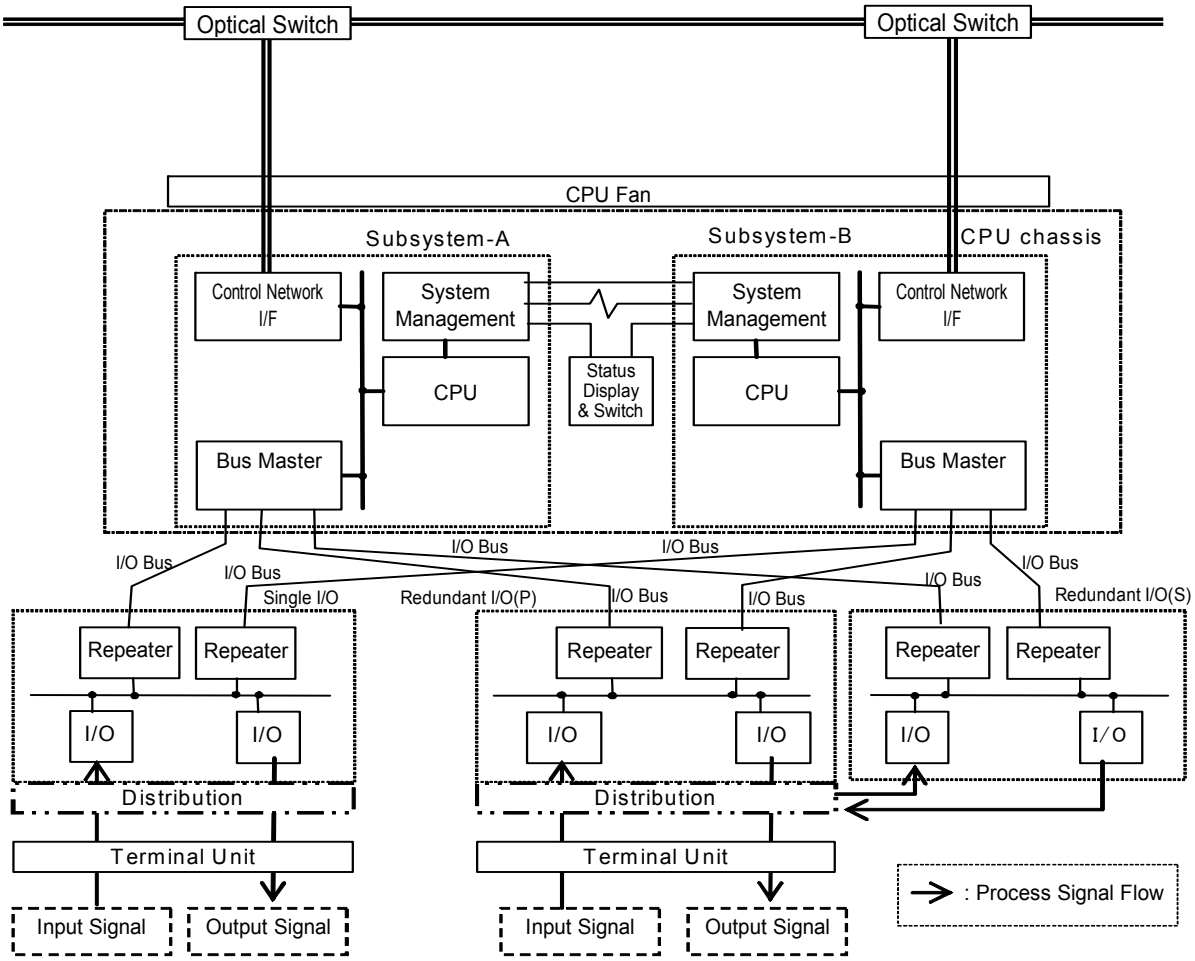


Figure 4.1.1-3 Redundant Standby Controller Configuration

A photograph of the MELTAC redundant standby controller configuration is shown in Figure 4.1.1-4.

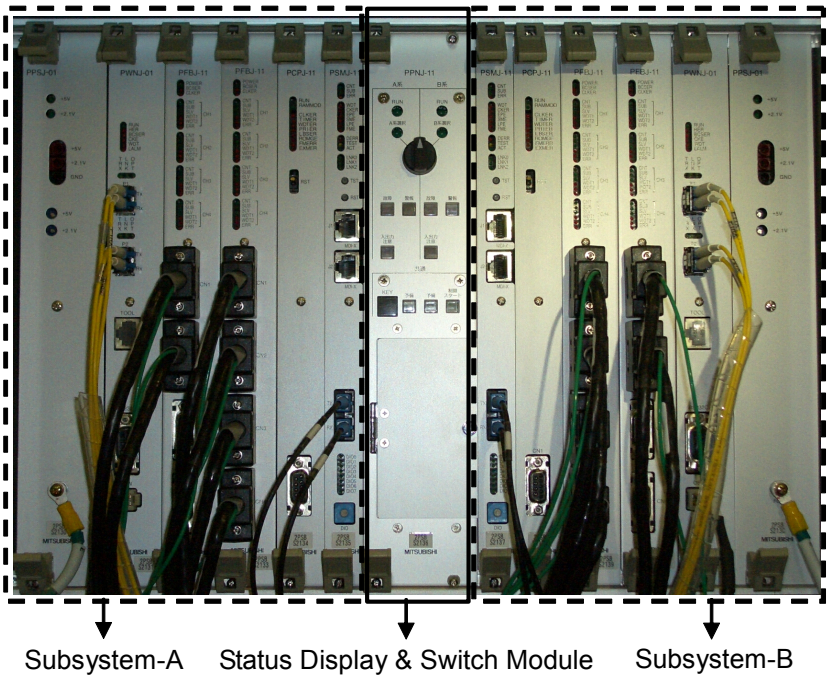


Figure 4.1.1-4 Picture of Modules in a CPU Chassis for a Redundant Standby Controller Configuration

The redundant standby controller consists of the following.

a) CPU Chassis

The CPU Chassis includes Subsystem-A, Subsystem-B, a Status Display & Switch Module, and a CPU Fan. Both subsystems have the same configuration. Each subsystem consists of a CPU Module, System Management Module, Control Network I/F Module, and Bus Master Module. Each subsystem communicates with the Control Network via its own Optical Switch. The subsystem is capable of driving a number of Control Network I/F Modules and Bus Master Modules depending on the scale of the application.

In a redundant standby controller configuration one subsystem is in Control Mode while the other one is in Standby Mode. Each subsystem operates independently.

When the subsystem in Control Mode stops operating due to a self-detected fault, the subsystem in Standby Mode will automatically switch to the Control Mode, with no manual intervention. When in the Control Mode the subsystem takes over all control functions with no bump in the control process. The switchover is controlled by the System Management Modules. The subsystems can also be switched manually from the Status Display & Switch Module.

b) I/O Chassis

The redundant standby controller includes either redundant I/O and/or single I/O.

The single I/O consists of 2 Repeater Modules, a non-redundant I/O Bus and multiple I/O modules. Each I/O module communicates with the Bus Master Module for the subsystem in Control Mode. When the subsystems switch modes, communication with the I/O modules also switches. Process input signals and output signals are connected to the single I/O via the Distribution Module and Terminal Unit.

To enhance I/O reliability, a redundant standby controller can also be configured with redundant I/O. The redundant I/O consists of redundant I/O primary (P) and redundant I/O secondary (S). 2 I/O modules (primary and secondary) are utilized to interface with one field signal via the Distribution Module and Terminal Unit. However, like the subsystems, one I/O module is in Control Mode and the other is in Standby Mode. Only the I/O module in Control Mode generates output signals.

The subsystem in Control Mode decides which I/O module is in Control Mode based on communication self-diagnosis. Each I/O module communicates only with the subsystem in Control Mode via the I/O bus, Repeater Module, and Bus Master Module.

4.1.1.2 Mode Management

There are 2 types of mode management depending on the controller.

4.1.1.2.1 Mode Management of Single Controller and Redundant Parallel Controller

In the single controller and the redundant parallel controller, there are 2 modes: Control Mode and Failure Mode.

The Mode Management of the subsystem in a single controller configuration is the same as the Mode Management of each subsystem in a redundant parallel controller configuration.

Mode Management of these controllers is shown in Figure 4.1.1-5.

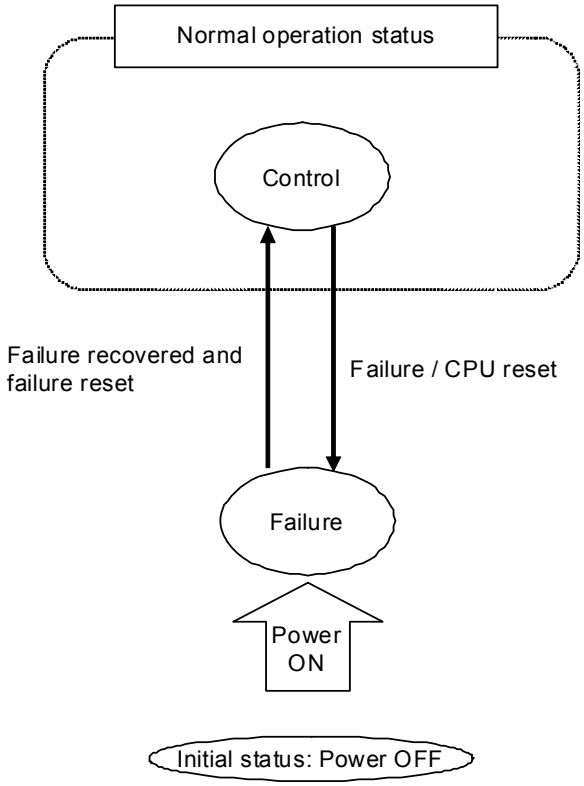


Figure 4.1.1-5 Mode Management of Single Controller and Redundant Parallel

The subsystem has the following 2 modes.

Control Mode: A state in which the subsystem performs input, operation, output processing, and Self-diagnosis. When the subsystem detects its own failure (through self-diagnosis), it automatically changes from Control Mode to Failure Mode. A

failure signal, which can be used for external alarming, is generated for this transition.

Failure Mode: The subsystem initializes to Failure Mode after initial power activation. The subsystem also shifts to this mode automatically after it detects its own failure or there is a loss of power longer than 20 ms. A subsystem shifts from Failure Mode to Control Mode only when the Reset button on the Status Display Module is pushed.

In the redundant parallel controller configuration, Subsystem-A and Subsystem-B operate independently with the Mode Management described above, including failure detection, loss of power detection, and manual reset.

Analog and digital outputs can be held in their preset initial mode, after the subsystem shifts to Control Mode, until the Output Start button on the Status Display Module is pushed. After pushing the output start button, output updating by the controller is enabled. For the redundant parallel controller configuration there are separate Output Start buttons for each controller. Pushing either button will enable output updating for the respective controller.

The output holding function can be disabled or enabled in the application program configuration. If this function is disabled, the outputs are enabled immediately after the subsystem shifts to the Control Mode, without the need for pushing the Output Start button. This function is enabled if it is required to confirm that the status of application software outputs matches the status of actual output devices before enabling output updating.

4.1.1.2.2 Mode Management of Redundant Standby Controller

In a redundant standby controller, there are 3 modes: Control Mode, Standby Mode, and Failure Mode. The system transitions between these modes according to the events that occur. An example of the status transitions of a redundant standby controller configuration is shown in Figure 4.1.1-6.

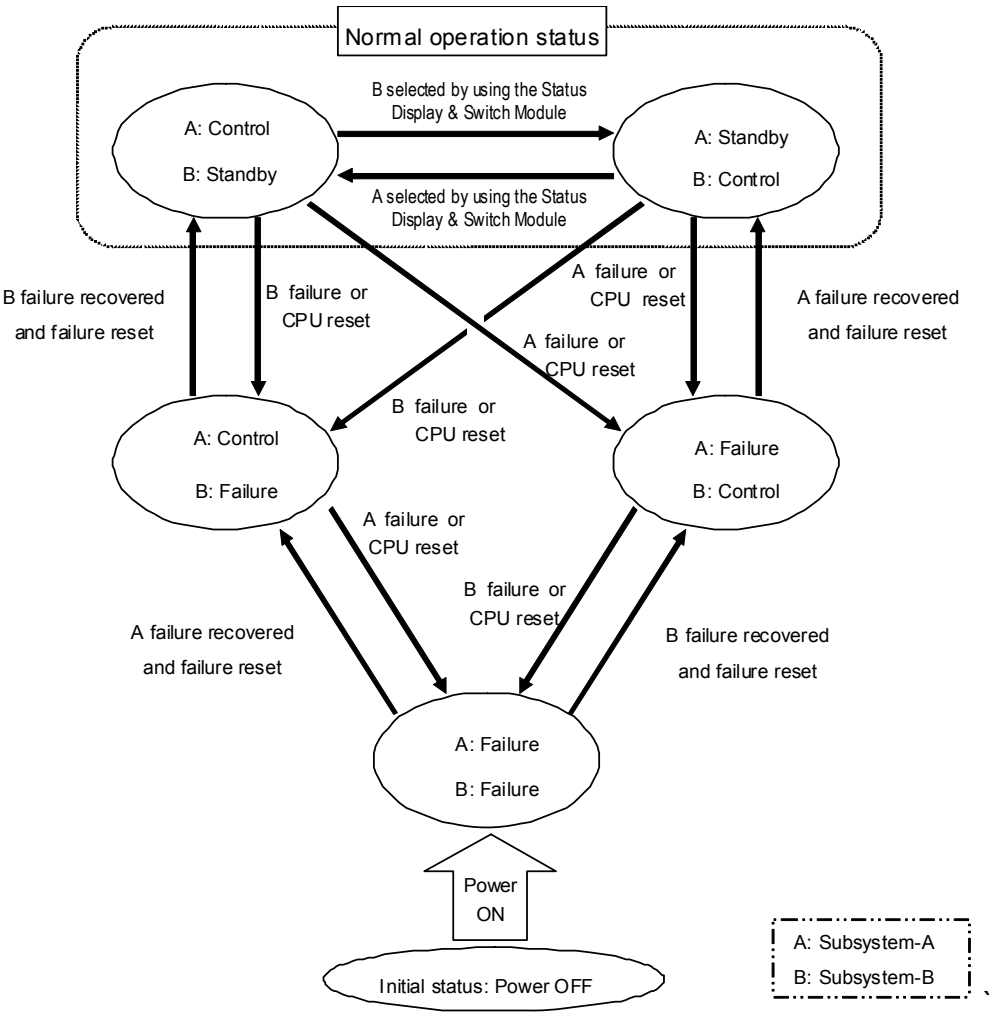


Figure 4.1.1-6 Mode Management of Redundant Standby Controller

Control Mode: A state in which the subsystem performs input, operation, output processing, and Self-diagnosis. When the subsystem detects its own failure (through self-diagnosis), it automatically changes from Control Mode to Failure Mode.

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

Failure Mode: The subsystem is initialized to Failure Mode after initial power activation. The subsystem also shifts to this mode automatically after it detects its own failure. A subsystem shifts from Failure Mode to Control Mode or Standby Mode only when the Reset button on the Status Display & Switch Module is pushed. If there is no subsystem in Control Mode, the subsystem switches to Control Mode when the Reset button is pushed. If a subsystem is already in Control Mode, the subsystem switches to Standby Mode when the Reset button is pushed.

Analog and digital outputs can be held in their preset initial mode, after the subsystem shifts to Control Mode, until the Output Start button on the Status Display & Switch Module is pushed. After pushing the Output Start button, output updating by the controller is enabled. For the redundant standby controller configuration there is one common Output Start button. Pushing the button will enable output updating for the redundant standby controller.

The output holding function can be disabled or enabled in the application program configuration which is the same as the Mode Management of single and redundant parallel controllers described in Section 4.1.1.2.1.

4.1.1.3 Scale and Capacity

The scale and capacity of the MELTAC platform controller is described in Table 4.1.1-1.

Table 4.1.1-1 Scale and Capacity

Item	Scale/Capacity
Input/Output	Maximum 3072 I/O modules per controller
Software	Cycle time: 20 ms to 1 s The value between 20 ms to 1 s is set in the application software F-ROM. This value is determined based on the application requirements. During the design phase, the system response time is determined through analysis, as described in Section 4.4. This analysis confirms the ability of the system to execute all functions within the allowed software cycle time. In the Integration Test phase, the system response time is confirmed by measurement.

4.1.1.4 Environmental Specifications

The MELTAC controller is designed to operate within the environmental conditions described in Table 4.1.1-2. Also see Section 5.

Table 4.1.1-2 Environmental Specifications

Item	Specifications	
Room Ambient temperature	Recommended	68 to 78.8 °F (20 to 26 °C) This temperature range is expected within a heated/ air-conditioned instrumentation and control room of the nuclear power plant. The controller should be mounted in a cabinet with no more than 18 °F (10 °C) heat rise. Operating within this range will maximize the life of the equipment.
	Operation guarantee	32 to 122 °F (0 to 50 °C) The controller should be mounted in a cabinet with no more than 18 °F (10 °C) heat rise.
Relative humidity	10 to 95%Rh (No condensation)	
Withstand voltage	AC power input line	AC power input line: 5 MΩ or more (500 VDC megger) (input - ground, input - DC output) Analog I/O line: 5 MΩ or more (500 VDC megger) (I/O - ground, input - output) Digital I/O line: 5 MΩ or more (500 VDC megger) (I/O - ground, input - output) Applicable standard: JIS-C0704-1995 (IEC664/947)
	I/O line	Analog I/O line: 1 KV AC (1 minute) (I/O - ground, input - output) Digital I/O line: 2 KV AC (1 minute) (I/O - ground, input - output) Applicable standard: JIS-C0704-1995 (IEC664/947)
Electro-magnetic Compatibility (EMC)	Electromagnetic Interference (EMI)	Complies with MIL-STD-461E for emissions: 1.Conducted emissions Conducted emissions from the power line (field discharge) CE101: Low-frequency, 30 Hz to 10 kHz CE102: High-frequency, 10 kHz to 2 MHz 2.Radiated emission RE101: Magnetic field, 30 Hz to 100 kHz RE102: Electric field, 2 MHz to 10 GHz

Item	Specifications	
	Electromagnetic Susceptibility (EMS)	Complies with MIL-STD-461E for susceptibility: 1. Conducted susceptibility CS101: Low-frequency, 30 Hz to 150 kHz CS114: High-frequency, 10 kHz to 30 MHz CS115: bulk cable injection, impulse excitation CS116: damped sinusoidal transients, 10 kHz to 100 MHz 2. Radiated susceptibility RS103: Electric field, 30 MHz to 10 GHz 3. Surge to the power line • IEEE Std. 472 • IEC61000-4: - IEC61000-4-12: Ring wave - IEC61000-4-5: Surge (Switching, lightning) - IEC61000-4-4: Electrically Fast Transients/bursts 4. Electrostatic noise resistance IEC61000-4-2-1999 Level 2 5. Lightning impulse resistance AC power source line: Applied voltage 4 kV, waveform 1.2/50 μs Digital I/O signal line: 4 kV, waveform 1.2/50 μs Applicable standard: JEC-210-1981 (Japanese Standard) Circuit category: 6
Seismic resistance	MELTAC Cabinet (at floor mounting)	Horizontal: 2.5 G (X- and Y-directions) Vertical: 1 G
	MELTAC modules (at chassis mounting)	Horizontal: 10 G (X- and Y-directions) Vertical: 2 G
Radiation resistance	Environment in which radiation is negligible.	
Dust	1.87×10^{-8} lb/ft^3 (0.3 mg/m^3) Reference standard: JEIDA-63-2000 Class B (Japanese Standard).	
Corrosive gas	Environment where no corrosive gas is detected.	

4.1.2 Hardware Descriptions

4.1.2.1 CPU Chassis

The modules that reside in the CPU Chassis are described in Table 4.1.2-1.

Table 4.1.2-1 Module in the CPU Chassis

	Name	Module Type	Function
Basic Function Module	CPU Module	PCPJ	• Executes basic software • Executes application software, including control computation processing
	System Management Module	PSMJ	• Communication between the redundant subsystems • Communication with the MELTAC engineering tool. • Auxiliary DI and DO functions
Communication Module	Control Network I/F Module	PWNJ	Communication with the Control Network.
	Bus Master Module	PFBJ	• Communication with I/O • Data Link communication with other controllers This module has 4 communication channels.
Power Supply Module	CPU Power Supply Module	PPSJ	Supplies power to the modules within the CPU Chassis.
Display & Switch Module	Status Display & Switch Module	PPNJ	• Mode display LED • Subsystem Mode switch • Output Start button (described below) This module is only used in the redundant standby controller configuration.
	Status Display Module		• Mode display LED • Output Start button (described below) This module is used for the single controller configuration or the redundant parallel controller configuration.

MELTAC has 2 types of CPU Chassis as shown in Table 4.1.2-2.

Table 4.1.2-2 CPU Chassis

Type	Use
Mirror-split CPU Chassis	- For redundant standby controller configuration
Non-split CPU Chassis	- For redundant standby controller configuration - For redundant parallel controller configuration - For single controller configuration

The CPU Chassis is selected from these 2 types to match the scale and configuration of the controller. For example, if each subsystem in redundant standby controller configuration has less than 5 modules, then a Mirror-split CPU Chassis is used. If each subsystem in redundant parallel controller configuration or single controller configuration has less than 5 modules, then a Non-split CPU Chassis is used. If each subsystem in redundant standby controller configuration or a redundant parallel controller configuration has more than 5 modules, 2 Non-split CPU Chassis are used. If the subsystem in single controller configuration has more than 5 modules, one Non-split CPU Chassis is used.

4.1.2.1.1 CPU Module (PCPJ)

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

This module utilizes F-ROM (Flash Read Only Memory) for storing both the basic software and the application software (such as function block interconnections, setpoints and constants).
Specifications of the CPU Module are in Appendix A, Section A.1.

4.1.2.1.2 System Management Module (PSMJ)

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

This module has the following functions:

- Auxiliary DI/DO for generating alarms such as Fan failure.
- Ethernet interface for communicating with the MELTAC engineering tool.
- Transmits and receives the changeover signal for redundant subsystem configurations via a dedicated backplane bus, as shown in Figure 4.1.1-3. In addition, this module has a 2-port memory Data Link for communicating operation data between the Standby Mode subsystem and the Control Mode subsystem.

Specifications of the System Management Module are in Appendix A, Section A.2.

4.1.2.1.3 Bus Master Module (PFBJ)

The Bus Master Module has 4 communication interface channels. Either of the following 2 functions can be defined for each channel.

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

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

4.1.2.1.4 Control Network I/F Module (PWNJ)

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

The Control Network is redundant using optical fiber as the communication medium. An optical switch unit enables optical bypass for node maintenance. This module employs a 2-port memory to ensure that communication functions do not disrupt deterministic CPU Module operation.
The description of the Control Network, including the Control Network I/F Module is shown in Section 4.3.2.
Specifications of the Control Network I/F Module are in Appendix A, Section A.4.

4.1.2.1.5 Status Display & Switch Module and Status Display Module (PPNJ)

The Status Display & Switch Module and the Status Display Module are mounted in the CPU Chassis. The Status Display & Switch Module is used with the redundant standby controller configuration and the Status Display Module is used with the redundant parallel controller or single controller configurations. Both of these modules display the mode and alarms of the subsystem. The Status Display & Switch Module also provides a manual Mode Change Over Switch.
Specifications of the Status Display & Switch Module and Status Display Module are in Appendix A, Section A.14.

4.1.2.2 I/O Modules

The I/O modules in the MELTAC platform provide the input/output functions and the signal conditioner function, including signal conversion and noise reduction. The MELTAC platform includes several types of analog and digital modules to accommodate various input/output signal interfaces.

The I/O modules are mounted in dedicated I/O Chassis. One I/O Chassis can accommodate 16 modules. The modules mounted in the chassis are connected to the Bus Master Modules in the CPU Chassis via Repeater Modules that can shape and amplify data communication signals. Data transfer is achieved via the I/O bus.

There is 1 analog input or output per analog I/O module and there are 4 digital inputs or outputs per digital I/O module.

Dedicated I/O modules are applied for nuclear instrumentation (NI) and radiation monitoring (RM). These modules provide unique signal processing for neutron monitoring and RM detectors. These I/O modules are mounted in the dedicated chassis installed in the dedicated cabinets for NI and RM, respectively. NI and RM I/O modules are connected to MELTAC Bus Master Modules in the CPU Chassis, the same as described above.

Specifications of I/O modules are in Appendix A, Section A.5, A.12 and A.13.

4.1.2.3 Isolation Module and Distribution Module

Isolation Modules provide electrical isolation between equipment in different divisions or fire zones. Analog Isolation Modules receive current input signal, Resistance Temperature Detector (RTD) input signals, or pulse input signals and transmit corresponding analog output signals without any software processing.
Electrical isolation is provided between the input and output signals inside the Isolation Module. The Isolation Modules are mounted in dedicated Isolation Chassis. A single Isolation Chassis can accommodate 14 Isolation Modules. Analog Isolation Modules process 1 signal.

The location of Isolation Modules is shown in Figure 4.1.2-1.

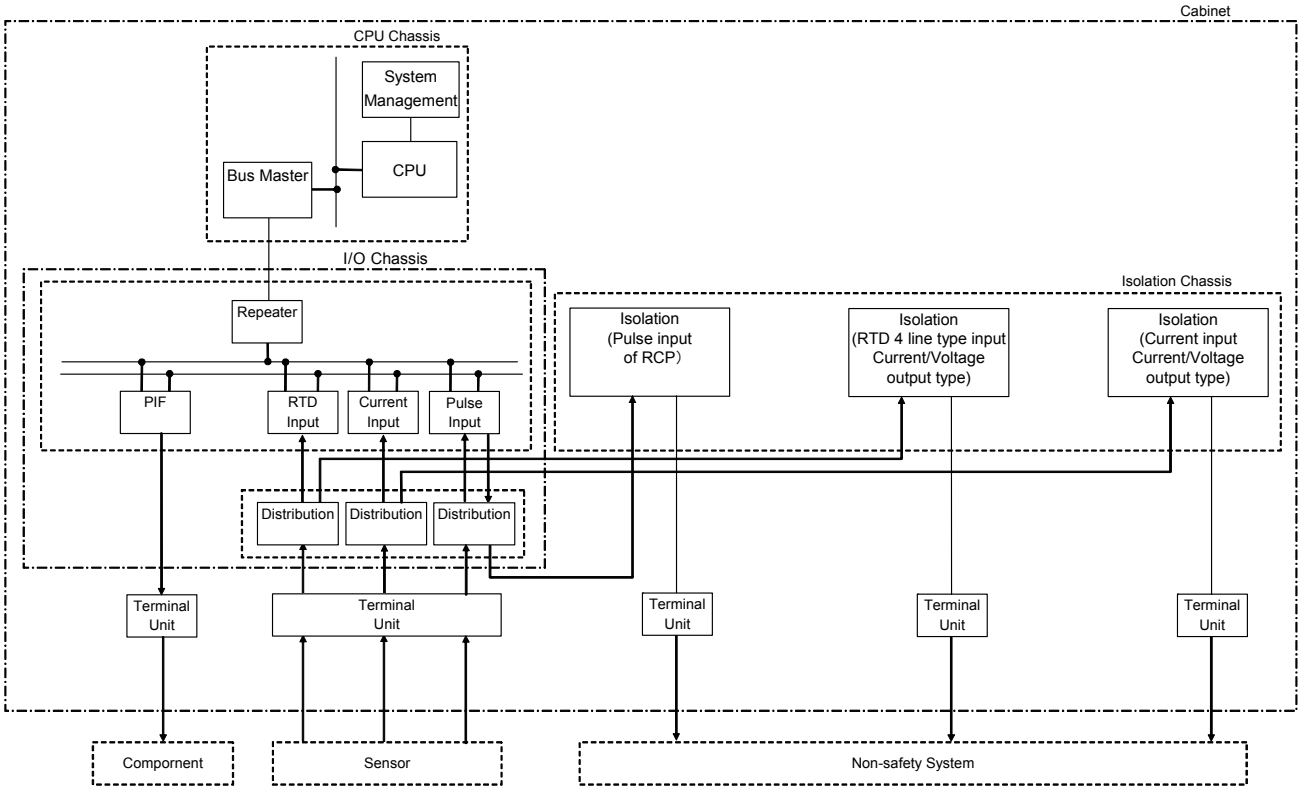


Figure 4.1.2-1 Location of Isolation Modules

Specifications of Isolation Modules are in Appendix A, Section A.6.

Figure 4.1.2-2 shows the internal configuration diagram of the Analog Isolation Modules KILJ and KIRJ. For common mode faults, the input and output are electrically isolated by the isolation amplifier. The positive temperature coefficient device (e.g.: PolySwitch TM) is used to limit overcurrent conditions for transverse mode faults. The positive temperature coefficient device raises its resistance value when it is heated by sustained overcurrent conditions.

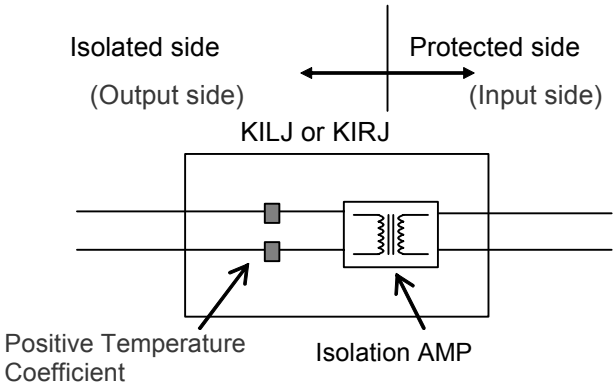


Figure 4.1.2-2 The Internal Configuration Diagram of the Analog Isolation Modules

Figure 4.1.2-3 shows the internal configuration diagram of pulse input Isolation Module KIPJ. The input and output are electrically isolated by a photo coupler. The positive temperature coefficient device (e.g.: PolySwitch TM) is used to limit overcurrent.

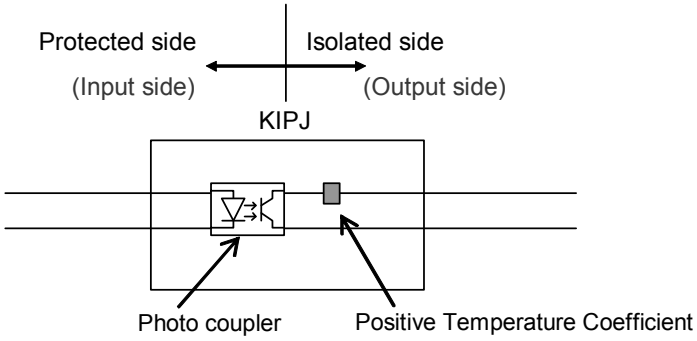


Figure 4.1.2-3 The Internal Configuration Diagram of the Pulse Input Isolation Module

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

As shown in Figure 4.1.1-1, Figure 4.1.1-2, and inputs from sensors are input to the Distribution Module via the Terminal Unit. The Distribution Module distributes input signals to redundant I/O modules. Output signals are also output via the Distribution Module.
The Distribution Module is used in accordance with the type of I/O modules. Appendix A.6 shows the list of I/O modules applicable to each Distribution Module.

4.1.2.4 Power Interface Module

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

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

[

]

New IPL sub-boards may be required for US applications, due to changes in plant process components, changes in DAS interfaces and changes in priority logic. New IPL sub-boards will maintain the same design process, qualification process, hardware technology and quality program as current IPL sub-boards.

The entire PIF Module, including the Communication Interface part is considered safety-related. Therefore, the life cycle process for the development and maintenance of the firmware within the Communication Interface part is the same as the firmware for all other MELTAC modules. During manufacturing and production, the PIF Modules are all tested to confirm the soundness of communication operation, IPL logic operation, and output operation.

Unlike electro-mechanical relays, the power semiconductor output of the PIF Module does not degrade mechanically or electrically and can be treated the same as any other general semiconductor device. Thus, the PIF Modules have no known aging limitations in their expected service life. Therefore, the PIF Module is not included in the list of MELTAC platform components that have a limited service life as identified in Section 7.4 Periodic Replacement Equipment (Parts) to Keep Reliability.

Figure 4.1.2-4 Sample Internal Configuration Diagram of the PIF Module

Specifications of the PIF Module are in Appendix A, Section A.8.

4.1.2.5 Electrical/Optical Converter Module

Electrical/Optical (E/O) Converter Modules for Data Link communication convert electrical signals to optical signals or optical signals to electrical signals. They are mounted in dedicated E/O Chassis. Up to 14 modules can be installed per chassis, with 1 communication link per module.

The specifications for the E/O Converter Module are in Appendix A, Section A.7.

4.1.2.6 Optical Switch

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

4.1.2.7 Fan Units

4.1.2.7.1 CPU Fan

The CPU Fan is installed on the top of the CPU Chassis to cool the modules within the CPU Chassis. It is equipped with a fan stop detection circuit which provides a contact signal to the System Management Module.
The fan stop detection circuit detects the decrease of fan rotation frequency by converting fan rotation frequency into a voltage pulse and monitoring the pulse length. If the pulse length reaches the length equivalent to the detected rotation frequency limit, the fan stop detection circuit de-energizes a relay, which generates a contact closing signal. Also, the same relay is de-energized if there is a power loss to the fan. Therefore, fan failure can be detected.

4.1.2.7.2 Door Fan Unit

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

4.1.2.7.3 Power Supply Fan Units

The Power Supply Fan Units are installed at the bottom and the midsection on both the left- and right-hand sides of the cabinet to cool the power supplies (PS). It is equipped with a fan stop detection circuit (described above) which provides a contact signal to the System Management Module.

4.1.2.8 Power Supply Module

The Power Supply Module convert the AC power supplied to the chassis to DC power voltages suitable for the individual modules and units. Redundant Power Supply Modules with power from 2 separate AC sources are typically provided.

There are 2 types of Power Supply Modules. The CPU Power Supply (PS and PPSJ) provides multiple outputs of +2.1 VDC and +5 VDC for the CPU Chassis. The I/O Power Supply (PS) provides +24 VDC for I/O modules, Isolation Modules, PIF Modules, E/O Converter Modules and Fan Units.

PPSJs are mounted in the CPU Chassis. PSs are mounted outside of the chassis. PSs are mounted on the panel cut parts that are set right and left of the cabinet chassis as shown in Figure 4.1.2-5 and Figure 4.1.2-6. This mounting location was selected, rather than mounting them within the chassis for 3 reasons (1) this leaves space in the chassis for additional modules, (2) external mounting allows DC power to be supplied to the chassis from 2 redundant Power Supply Modules, and (3) this location keeps the heat from the power supplies away from the modules, thereby improving module reliability.

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

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

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

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

4.1.2.9 Controller Cabinet

a) Overview

The controller cabinet stores the following:

- CPU Chassis
- I/O Chassis
- E/O Chassis
- Isolation Chassis
- Power Interface Chassis
- CPU Power Supply Module
- I/O Power Supply Module
- CPU Fan
- Power Supply Fan
- Door Fan
- Terminal Unit
- Optical Switch

The inside layout of the cabinet is as follows:

- Each module can be changed from the front side of the cabinet and each status display can be monitored from the front side of the cabinet. Therefore, maintenance personnel can easily identify the status of the module and repair the module without pulling it out of the chassis.
- The modules within the I/O Chassis can be replaced at power. The modules in the CPU Chassis cannot be replaced at power. For redundant subsystem configurations power down of the CPU Chassis for module replacement has no effect on the system operation, since the other subsystem remains operable.
- Field cables enter through the rear side of the cabinet (through top and/or bottom entry) and are connected to the Terminal Unit.

b) Controller Cabinet Specifications

The MELTAC cabinet is described in Table 4.1.2-3. Typical configurations of MELTAC cabinets are shown in Figure 4.1.2-5 and Figure 4.1.2-6.

Table 4.1.2-3 MELTAC Cabinet Specifications

Item	Specifications
Typical External dimensions	2.62 (W) x 2.95 (D) X 7.55 (H) ft (800 (W) x 900 (D) x 2300 (H) mm) per cabinet
Weight	Approximately 1600 lb (750 kg) per cabinet including inside modules and units. Weight will vary with the number of chassis and modules.
Door specifications	Front and rear doors include handles, locks and seismic support bolts.
Cooling	The cabinet has forced air-cooling. An exhaust fan is mounted in the upper part of the cabinet's rear side. The doors are provided with filtered ventilation ports. Exhaust fans are mounted above each CPU Chassis and adjacent to I/O power supplies. The I/O Chassis are convection-cooled with no forced ventilation.

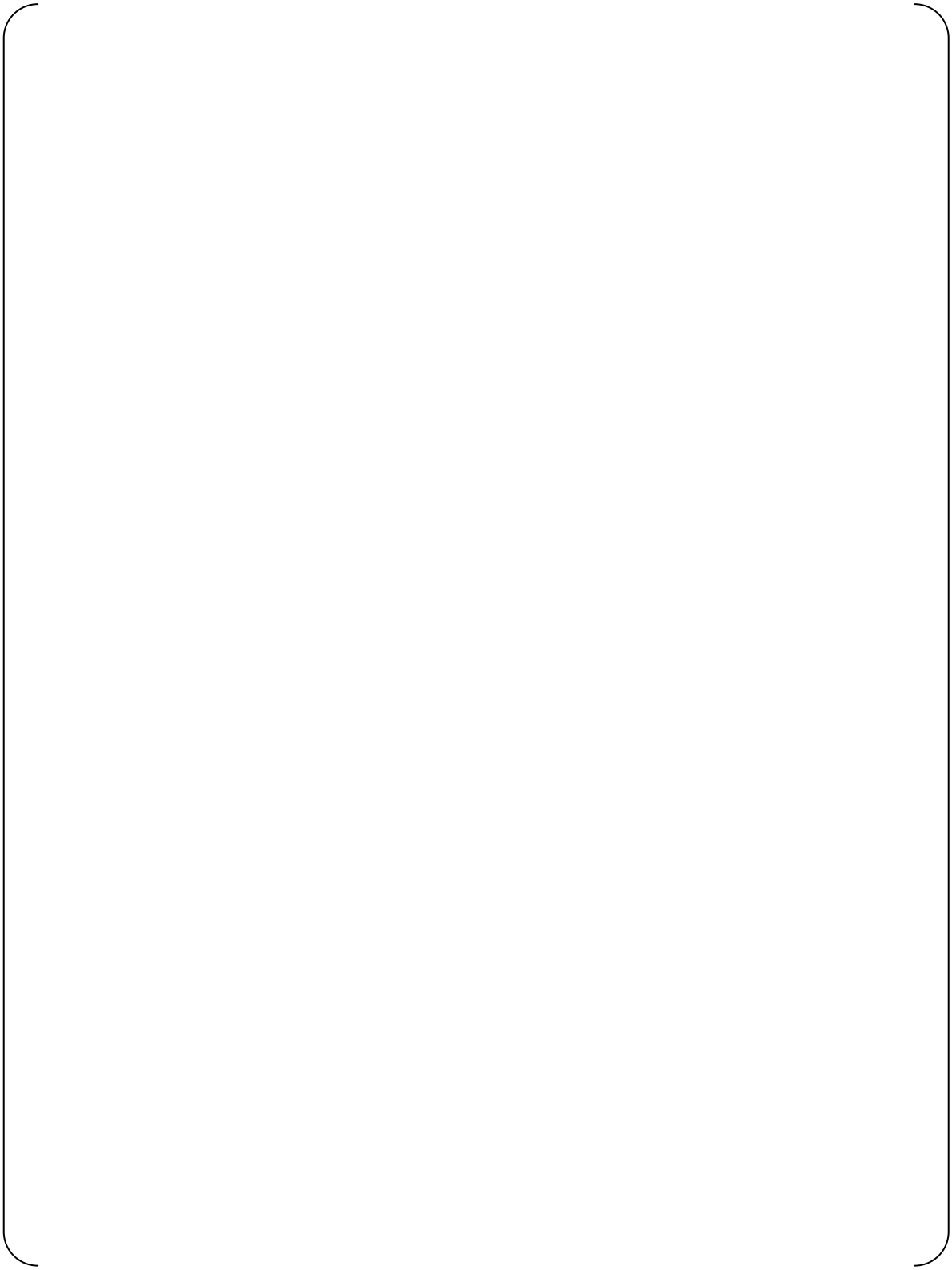


Figure 4.1.2-5 Cabinet External Dimensions and Rack Up, Typical Sample A

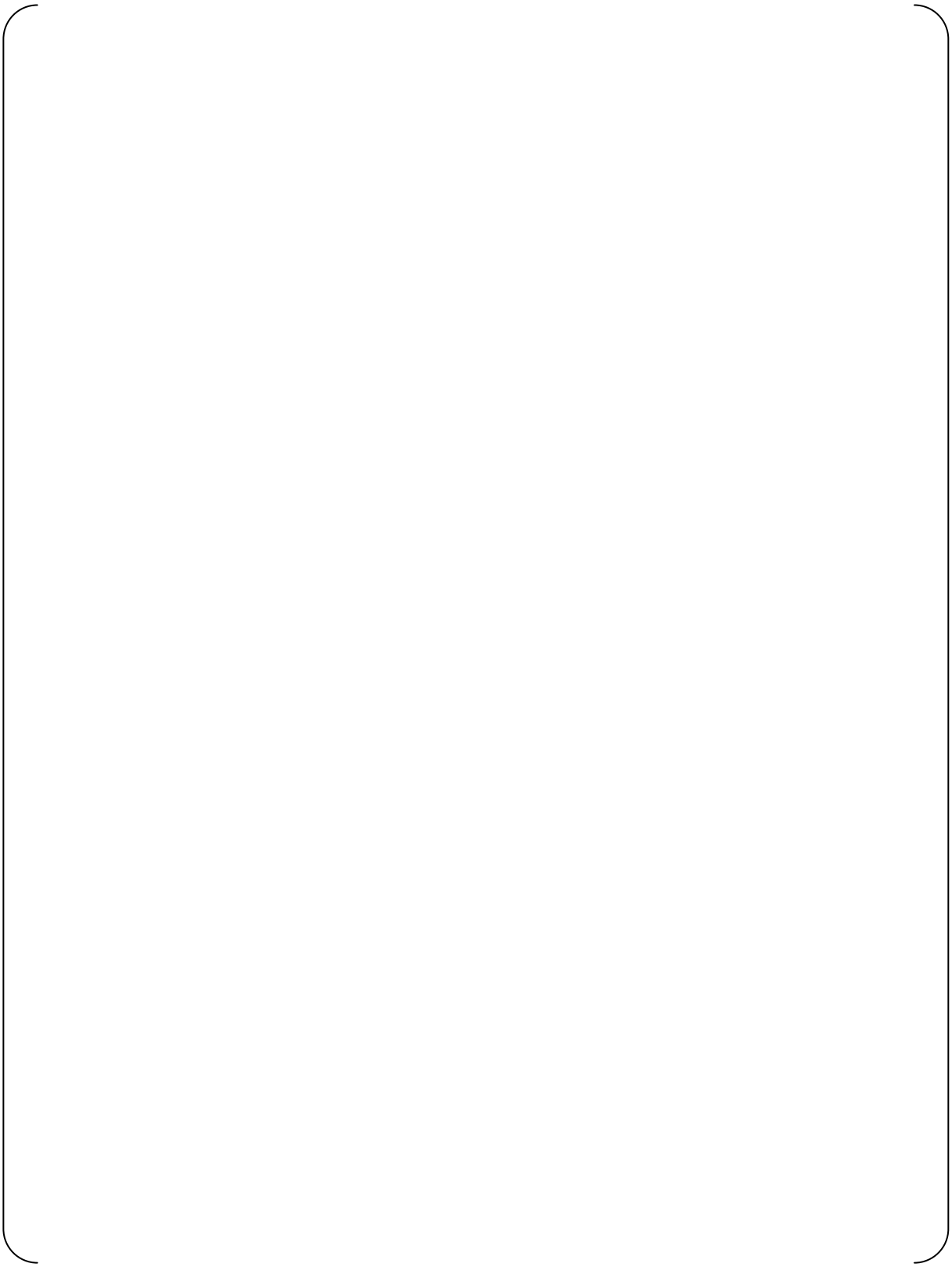


Figure 4.1.2-6 Cabinet External Dimensions and Rack Up, Typical Sample B

4.1.2.10 Power Supply Configuration

Redundant AC power from 2 separate sources may be supplied to the MELTAC cabinet to avoid loss of function due to a single failure in the power supply or power source, as shown in Figure 4.1.2-7.

The source of AC power is described in system Application Licensing Document. The AC power is filtered and converted to DC voltage by the Power Supply Modules. DC power from both sources is diode auctioneered, then distributed to each component in the cabinet. For some components diode auctioneering is separate for each component.

[

]

Figure 4.1.2-7 Configuration of Power Supply for Controller Cabinet

4.1.3 Software

The MELTAC platform consists of basic software and application software. Each software function is described below.

4.1.3.1 Basic Software

In order to achieve deterministic processing, the basic software of the MELTAC platform adheres to the following design principles.
a) There is only single task processing
b) **[**

]

The processes within the basic software and the order of their execution are shown in Figure 4.1.3-1.

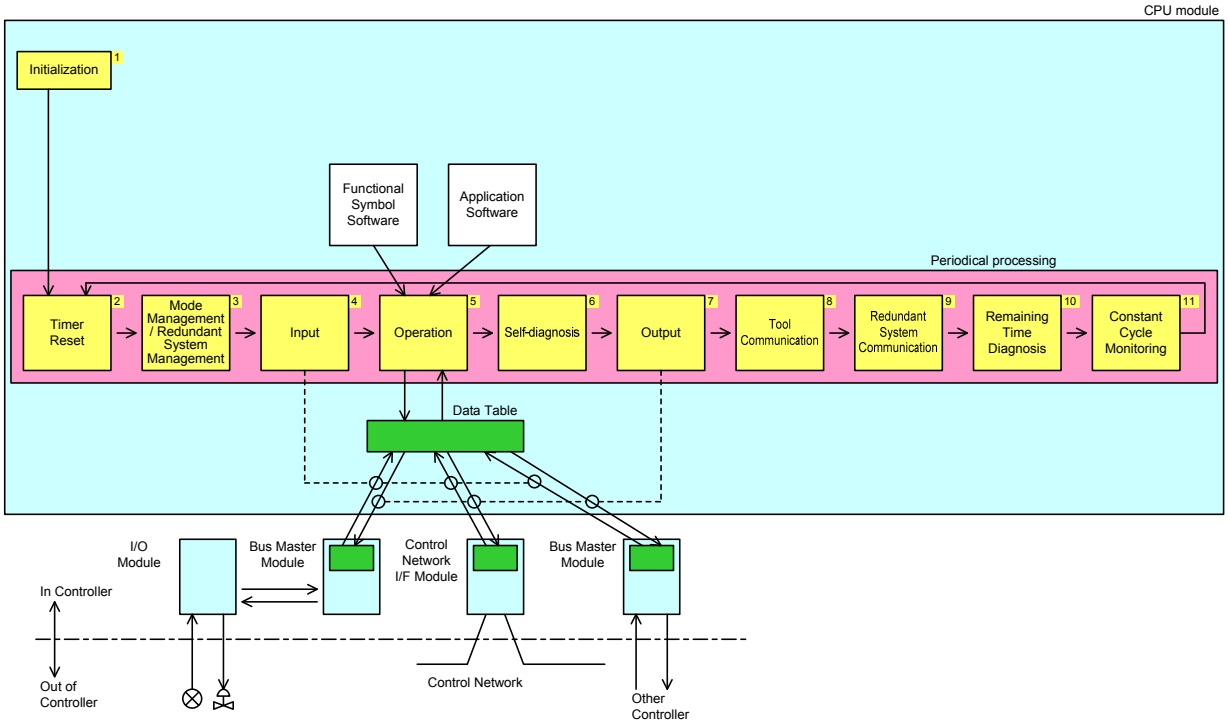


Figure 4.1.3-1 Basic Software Processes and Execution Order

The processing time from No.2 to No.8 is based on the application logic and the input/output signal quantity of each system. Since the controller operates cyclically, the processing time from No.2 to No.11 can be 100% of the application requirement (i.e.: there is no application margin required for the system). However, to allow future system expansion and to allow reasonable time for Remaining Time Diagnostics (discussed below), during the system design phase, the approximate processing time from No.2 to No.8 is calculated as described in Section 4.4. If the processing time exceeds about 80% of the processing cycle required for the system, the application is divided into 2 or more controllers, as necessary. In the test phase, the system response time is confirmed by measurement.

The processes of the MELTAC basic software are described below.
[

]

Figure 4.1.3-2 Remaining Time Diagnosis

[

]

4.1.3.2 Application Software

The application software of the MELTAC platform is designed using the MELTAC engineering tool. Application software for functional algorithms is designed by combining simple graphical function blocks such as “And”, “Or”, and ”Not” using the Graphical User Interface (GUI) of the MELTAC engineering tool. A GUI is used to reduce the potential for design errors in building or modifying the application software. It also makes it easier for the independent verifier to ensure that the application software Graphical Block Diagram (GBD)s, which are created by the I&C system designer are consistent with the Functional Block Diagram (FBD)s, which are created by the process system designer.

This GUI-based programming language used in both FBDs and GBDs is called POL (Problem Oriented Language). POL allows application software to be developed by graphically interconnecting conventional function blocks as noted above.

Using the MELTAC engineering tool, the application software GBD is automatically converted into execution data that is executed directly by the Operation process of the basic software. The Operation process of the basic software executes the Functional Symbol Software sequentially according to the execution data.

Application software execution data is stored in the F-ROM of the CPU Module.
[

]
The POL Functional Symbols are listed in Appendix B.

4.1.4 MELTAC Engineering Tool

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

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

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

4.1.4.1 Function Description

a) Creation of Application Software

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

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

b) Download

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

]

The correct download is confirmed by a different MELTAC engineering tool function that checks the F-ROM data as discussed below.

c) Verifying F-ROM data

The MELTAC engineering tool provides a manually initiated function which automatically compares the basic software and application software data in the F-ROM of the controller, bit by bit, with the basic software data and application software data stored in the MELTAC engineering tool. This function is used after a new download and during periodic surveillance tests to confirm that the data in F-ROMs is the same as the data in the MELTAC engineering tool, and therefore has not changed.

d) Controller failure diagnosis display

The MELTAC engineering tool displays the self-diagnosis result of the controllers. It shows which module is in a failed state.

e) Temporary changes to field changeable process value in data table (Data Set)

[

]

4.1.4.2 Network for the MELTAC Engineering Tool

In order to communicate between the MELTAC engineering tool and the controller, the Maintenance Network is used. The MELTAC engineering tool, which runs on a PC, is temporarily connected via the Maintenance Network to the System Management Modules of each controller in the division. This interface allows all functions described in Section 4.1.4.1. The Maintenance Network is temporarily connected to the controllers in the same safety division. There is a separate Maintenance Network for each division. There are no Maintenance Network interconnections between safety divisions. There is also a separate MELTAC engineering tool for each division. The specification of the Maintenance Network is described below.
For the configuration and the isolation of the Maintenance Network, see Section 4.3.4.

(Specification)
Function: Transmission of maintenance data for MELTAC engineering tools

- Transmission protocol: Ethernet (IEEE Std. 802.3; CSMA / CD, UDP/IP)
- Transmission speed: 100 Mbps/10 Mbps
- Communication form: Dialog communication
- Connection form: Bus/Star-type

Transmission media: UTP Category 5 cable
Optical fiber (Multi mode)

[

]

4.1.5 Self-Diagnosis

The MELTAC platform controller is equipped with 3 types of self-diagnosis features: a hardware based detection process, a software based detection process, and a combination thereof. When an error is detected, an alarm is generated. When the error is severe, the controller makes a transition from the Control or Standby Mode to the Failure Mode.

Detailed error descriptions are provided in Sections 4.1.5.2 through 4.1.5.6. The categorization of each error is shown in parenthesis, for example “Clock check (Failure)”.
All errors in Sections 4.1.5.2 and 4.1.5.3 are severe and categorized as “Failure”. These errors stop the main CPU operation, and generate signals that can be used for alarms. All other errors (those identified in Sections 4.1.5.4 and 4.1.5.5) generate signals that can be used for alarms, but do not stop the main CPU operation. All error signals are identified on the MELTAC engineering tool. The specific grouping of error signals into operator alarms is application specific. Since most applications have redundant CPUs, typically all error signals are grouped to a single operator alarm and then the MELTAC engineering tool is used for diagnosis of specific error conditions.

Failure notice may be provided to the plant monitoring system for the 3 types of errors, ”Failure”, “Alarm”, and “I/O Alarm”. These error signals are typically grouped into system trouble alarms, however the method used to present this information to the operator from the plant monitoring system is application dependent and not within the scope of the MELTAC platform.
Detailed information for diagnosis of all error conditions is provided on the MELTAC engineering tool.

a) Hardware based detection process

With this feature, self-diagnosis is implemented by special diagnostic circuitry on the CPU Module. The feature involves a WDT, parity error, timeout, analog input check, etc.

b) Software based detection process

With this feature, self-diagnosis is implemented using software. The feature involves CPU health check, F-ROM check, RAM check, etc.

c) Software/hardware combination

With this feature, circuitry that supports self-diagnosis is added to the controller and self-diagnosis is performed using software-based read/write operations. This feature involves a digital input check, digital/analog output read-back check, etc.

The controller is monitored based on the above self-diagnosis processes at every execution cycle. The individual error items can be identified by viewing the LED display on the front of each module and the representative alarm display (Failure, Alarm, I/O Alarm) on the Status Display & Switch Module and by using the MELTAC engineering tool connected via the Maintenance Network.

Each detected error is categorized into 3 types (Failure, Alarm and I/O Alarm) as below.

1) Failure
Fatal abnormalities by which the subsystem cannot continue its functions are categorized as Failure.
When the subsystem detects this type of error, it transitions to the Failure Mode.
[

]
In the Failure Mode, the processing of input/output and operation are stopped, although the process of sending status data related to the Failure Mode is continued.
[

]
In the case of the redundant standby controller configuration, when the subsystem in the Control Mode changes to the Failure Mode, the subsystem in the Standby Mode changes to the Control Mode and the control function continues uninterrupted.

When there is no subsystem which communicates with the controller's Output Module, the Output Module transitions to the Failure Mode which is "as-is mode" or "off mode". This mode is preset at the application level.

2) Alarm
Minor abnormalities with which the subsystem can continue its functions are categorized as Alarm.
When the subsystem detects this type of error, it does not change its mode and only warns of the alarm. This abnormality is communicated to other systems for alarming via Data Link or Control Network, as configured at the application level.

3) I/O Alarm
Abnormalities of I/O are categorized as I/O Alarm.
When the subsystem detects this type of error, it does not change its mode and only warns of the alarm. This abnormality is communicated to other systems for alarming via Data Link or Control Network, as configured at the application level.
In the case of redundant standby controller configuration, when the I/O Alarm occurs in the Redundant I/O in the Control Mode, the subsystem stops to use this I/O, switches the other I/O from the Standby Mode to the Control Mode, and continues the processing of input/output.
When the I/O Alarm occurs in the Single Input Module, the last good input values are retained and the application software is informed of the abnormal state of the input signals. For digital inputs, the input values are kept at the last value (1 or 0) before the error occurred. For analog inputs, the input values are kept at the last engineering value before the error occurred. Based on the error flag, the application software can be programmed for a predetermined control action.

4.1.5.1 Coverage of Self-Diagnosis

The controller's self-diagnosis coverage is shown in Figure 4.1.5-1.

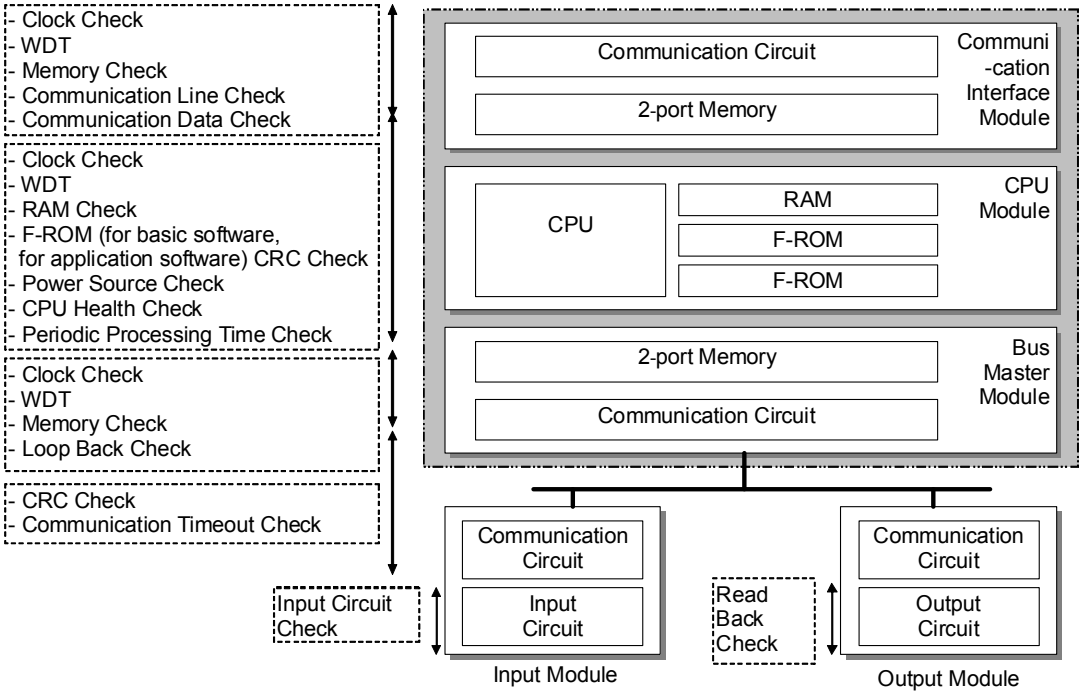


Figure 4.1.5-1 Coverage of Self-Diagnosis Function of the Controller

4.1.5.2 Self-Diagnosis of the Controller

The self-diagnosis of the processor modules is described below.
Each diagnosis item is shown with the timing of diagnosis classified as follows:
- Initialization: At the time of initialization
- Self-diagnosis: Once per cycle in the constant cycle operation
- Remaining Time Diagnosis: Periodically in the remaining time of constant cycle operation, but not every cycle.
- Constant: On a constant basis by hardware

4.1.5.2.1 CPU Module

[

]

[

]

4.1.5.2.2 Bus Master Module

[

]

4.1.5.2.3 Control Network I/F Module

[

]

4.1.5.3 Self-Diagnosis of Power Supply Modules in the CPU Chassis

[

]

4.1.5.4 Self-Diagnosis of the Communication System

See Sections 4.3.2.4 and 4.3.3.4. Communication System errors are categorized as “Failure” or “Alarm”, depending on the redundancy configuration of the controller.

4.1.5.5 Self-Diagnosis of I/O Modules

The self-diagnosis of the I/O modules is described below.

4.1.5.5.1 Input Module

[

]

4.1.5.5.2 Output Module

[

]

4.1.5.5.3 Controller Cabinet

[

]

4.1.5.6 Operations When the Hardware and Software Do Not Match

Mismatch of the module configuration in the CPU Chassis:
The CPU Module detects the error and the subsystem switches to Failure Mode.

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

4.1.5.7 Watchdog Timer (WDT)

This section provides a description of the WDT architecture and how WDT timeout errors are processed in the MELTAC modules. **[**

]

4.1.5.7.1 Architecture of the WDT

The following describes the detailed WDT mechanism. Figure 4.1.5-2 shows the WDT mechanism, taking the CPU Module as an example. The left-side of the figure represents the elements related to the WDT in the CPU Module. The right-side of the figure shows the WDT behavior, regarding count-up, counter reset, and timeout when the counter value reaches a predefined value.
The flow of the WDT operations and controls is as follows:

(1) The WDT consists of a counter with a hardware clock generator, and predefined timer value (for WDT timeout).
(2) After initialization, the timer starts to count up.
(3) The basic software resets the timer to zero at regular intervals (i.e.: for each operation cycle).
(4) If the basic software does not reset the WDT within a predefined timer value, then the WDT times out and the controller transitions to a Failure Mode (see Section 4.1.5) with an alarm indication.

The WDT mechanism of other modules is the same as that of the CPU Module.

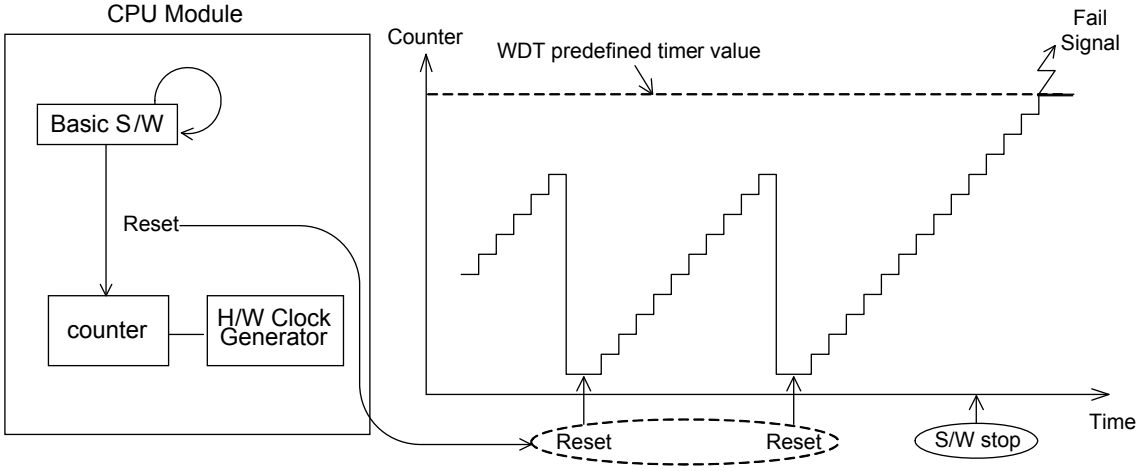


Figure 4.1.5-2 WDT Mechanism (CPU Module)

4.1.5.7.2 WDT Timeout Process (per Module)

[

]

Figure 4.1.5-3 WDTs Mounted in MELTAC Platform

Table 4.1.5-1 WDT Timeout Process

4.1.6 Bus Inside the Controller

Table 4.1.6-1 shows the busses used inside the controller. Table 4.1.6-2 shows the I/O bus specification.

Table 4.1.6-1 Bus Inside the Controller

Item	Application
Futurebus+	Backplane bus in the CPU Chassis. It is used to connect modules in CPU Chassis and transfers other module data in the CPU Chassis.
I/O bus	A bus that connects the CPU Chassis and the I/O module. See Table 4.1.6-2 for details.

Table 4.1.6-2 I/O Bus Specification

Item	Specification
Protocol	1:N master polling
Configuration	Maximum 96 I/O modules can be connected to 1 I/O bus. (Up to 16 I/O modules can be mounted on 1 I/O Chassis and up to 6 Chassis can be connected to 1 I/O bus.). There are 4 I/O busses on each Bus Master Module and each controller can have 8 Bus Master Modules.
Interface	RS-485 transformer isolation.
Baud rate	1Mbps
Error detection method	CRC check
Operation	The Bus Master Module and the I/O modules are connected to the I/O bus. The Bus Master Module sends output data and input data requests to the I/O module, and the I/O module responds to that. This communication method is common to all I/O modules, including the PIF Module.

4.1.7 Manual Test

Manual test refers to conducting periodic surveillance testing of all functions that are not automatically tested through self-diagnosis, and conforming to the guidelines of BTP 7-17 “Surveillance Testing”.

(1) Input and Output Function
The integrity of the input and output function of the I/O module hardware circuits is confirmed during periodic testing. The integrity can be tested by the method described in Section 4.1.7.1.

(2) Memory
The memory integrity is checked during periodic testing. The integrity can be tested by the method described in Section 4.1.7.2.

(3) Safety VDU Panel
The consistency between the actual screen display and the coordinates of the S-VDU panel is confirmed during periodic testing. The consistency can be tested by the method described in Section 4.2.4.

4.1.7.1 Process Input and Output

Figure 4.1.7-1 shows the signal flow of manual test for process input and output.
The input function is tested by manipulating the process to stimulate a state change. Correct functionality is confirmed by monitoring the state of signals on the safety VDU.
The output function is tested by operation from the safety VDU.

It is noted that these tests are intended to confirm functionality of the system's process input and output signal paths, since these cannot be fully tested by self-diagnosis. Therefore, the process input and output tests can be conducted using the safety VDU that obtains its data from the Control Network. A separate manual test for the safety VDU is described in Section 4.2.4.

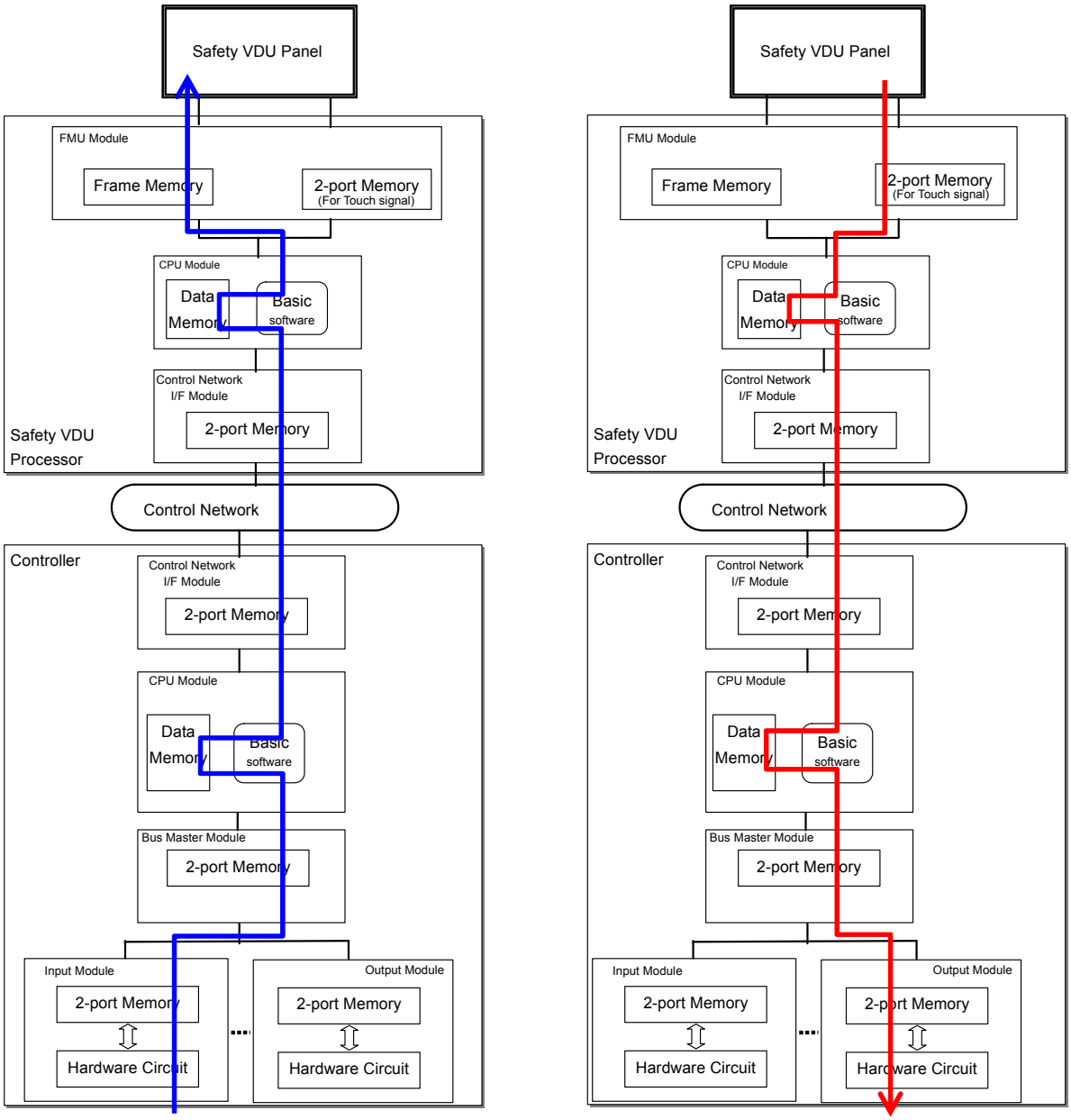


Figure 4.1.7-1 Manual Test for Process Input and Output

4.1.7.2 Memory Integrity Check

The MELTAC engineering tool includes a manually initiated Memory Integrity Check (MIC) function which compares the software memory in the controller, bit by bit, with a controlled copy of the software stored off-line in the MELTAC engineering tool.

This function is used to provide confirmation that the software in the controller is the same as the off-line version, and therefore has not changed or failed. This test confirms the functional integrity of both the basic software and application software residing in the controller. The MIC is conducted periodically for every controller in the system.

By confirming the basic software, the MIC confirms the CPU instructions stored in F-ROM for all MELTAC functions described throughout this document, including the self-diagnosis functions. By confirming the application software, the MIC also confirms the CPU instructions stored in F-ROM for all functional logic required for the safety functions of the application.

The following table summarizes the differences between the MIC which is conducted periodically, and Self-diagnosis Memory Check (SMC) (see Section 4.1.5.2.1) which is conducted continuously on-line, including the effectiveness of these 2 functions.
[

]

Table 4.1.7-1 MIC vs. SMC

[

]

The versions of the application software and the basic software are controlled through software configuration management. The application software is described in the Application Licensing Document. The basic software is controlled and maintained in accordance with the App.B-based QAP and “MELTAC Platform Software Program Manual” (JEXU-1041-1016).

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

Table 4.1.7-2 Detectable Errors by the MIC and SMC

[

]

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

measurements and actuating plant components. Therefore, through the aggregate of periodic manual tests and continuous self-diagnosis tests, the complete functionality of the safety system is confirmed.

4.1.8 Defense-in-Depth and Diversity (DAS) Interface

Nuclear power plants that implement digital platforms (e.g.: the MELTAC platform) in plant safety systems may be required to implement a Diverse Actuation System (DAS). The DAS is typically a non-safety system consisting of conventional equipment that is totally diverse and independent from the MELTAC platform. The DAS would provide monitoring and control of safety-related and non-safety plant systems to cope with abnormal plant conditions concurrent with a CCF that disables all functions of the plant safety systems.

Sensors would typically be interfaced from within the MELTAC Distribution Modules. These Distribution Modules would utilize Isolation Modules to connect the input signals to the DAS prior to any digital processing. Therefore, a software CCF within the plant safety system will not affect the DAS function.

The DAS typically controls selected plant components independent of the output from the plant safety system. Outputs from the DAS are typically interfaced to plant components via MELTAC platform PIF Modules. The PIF Modules combine the signals received from the DAS with signals received from the plant safety system (MELTAC controllers) to generate a single power interface to the plant component. The DAS output to the PIF Modules is typically isolated to prevent propagation of DAS faults to the plant safety systems. The combination logic and power interface within these PIF Modules is simple and fully testable so any additional potential for CCF that may be introduced is negligible. The PIF Module design and examples of typical plant safety system and DAS inputs is provided in Section 4.1.2.4.

4.2 Safety VDU Panel and Processor

The MELTAC platform includes a safety VDU which consists of a safety VDU panel, and a safety VDU processor. There is one safety VDU processor for each safety VDU panel.

The number of safety VDUs is defined by specific plant design. Each safety VDU can be configured to provide the HSI for only one safety division.

4.2.1 Hardware

The CPU Chassis, Control Network Optical Switch, fans, cabinet power supplies and the cabinet are the same as previously described in Sections 4.1.2.1, 4.1.2.6, 4.1.2.7, 4.1.2.8 and 4.1.2.9, respectively. Unique components of the Safety HSI are described below.

All unique components of the safety VDU panel and safety VDU processor comply with the same environmental specifications and are qualified to the same levels as described for the MELTAC controller in Section 4.1.1.4.

4.2.1.1 Safety VDU Panel

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

- Display function:
  Displays operational screens by receiving RGB analog video signals from the safety VDU processor.

- Control function:
  Inputs by operator on the touch screen are transmitted to the safety VDU processor in the form of x-y coordinate data using an RS-232C data link.

Specifications of the safety VDU panel are in Appendix A.10.

4.2.1.2 Safety VDU Processor

4.2.1.2.1 Configuration of the Safety VDU Processor

The safety VDU processor has a single subsystem architecture as shown in Figure 4.2-1. Except for the Frame Memory Unit (FMU) Module, the hardware modules are the same as those of the MELTAC platform. The software structure is based on the same design as that of the MELTAC basic software.

a) Information Display Function

The safety VDU processor stores the static data for each pre-configured display screen. The safety VDU processor gathers live plant data from safety controllers via the Control Network. The safety VDU processor organizes the static data of the pre-configured screen with the live plant data and then displays those combined images on the safety VDU panel by means of the RGB interface. The RGB interface is generated by the FMU Module.

b) Control Function

Operators take manual control actions by touching an operation switch image displayed on the safety VDU panel. A sample picture of the operation switch image is shown in Figure 4.2-5. The results of a touch screen operation are sent in the form of x-y coordinate data from the safety VDU panel to the safety VDU processor via the FMU Module. This is an RS-232C Data Link, which is converted from electrical to optical, to increase the transmission distance. The safety VDU processor converts the x-y coordinate data received from the safety VDU panel to plant control data (i.e.: component ID and operational command), and then sends the data to the controllers via the Control Network.

c) Control Network Interface

The Control Network interface receives live plant data from the controllers, and sends the plant control data to the controllers via the Control Network.

The Control Network and safety VDU are both intra-divisional.

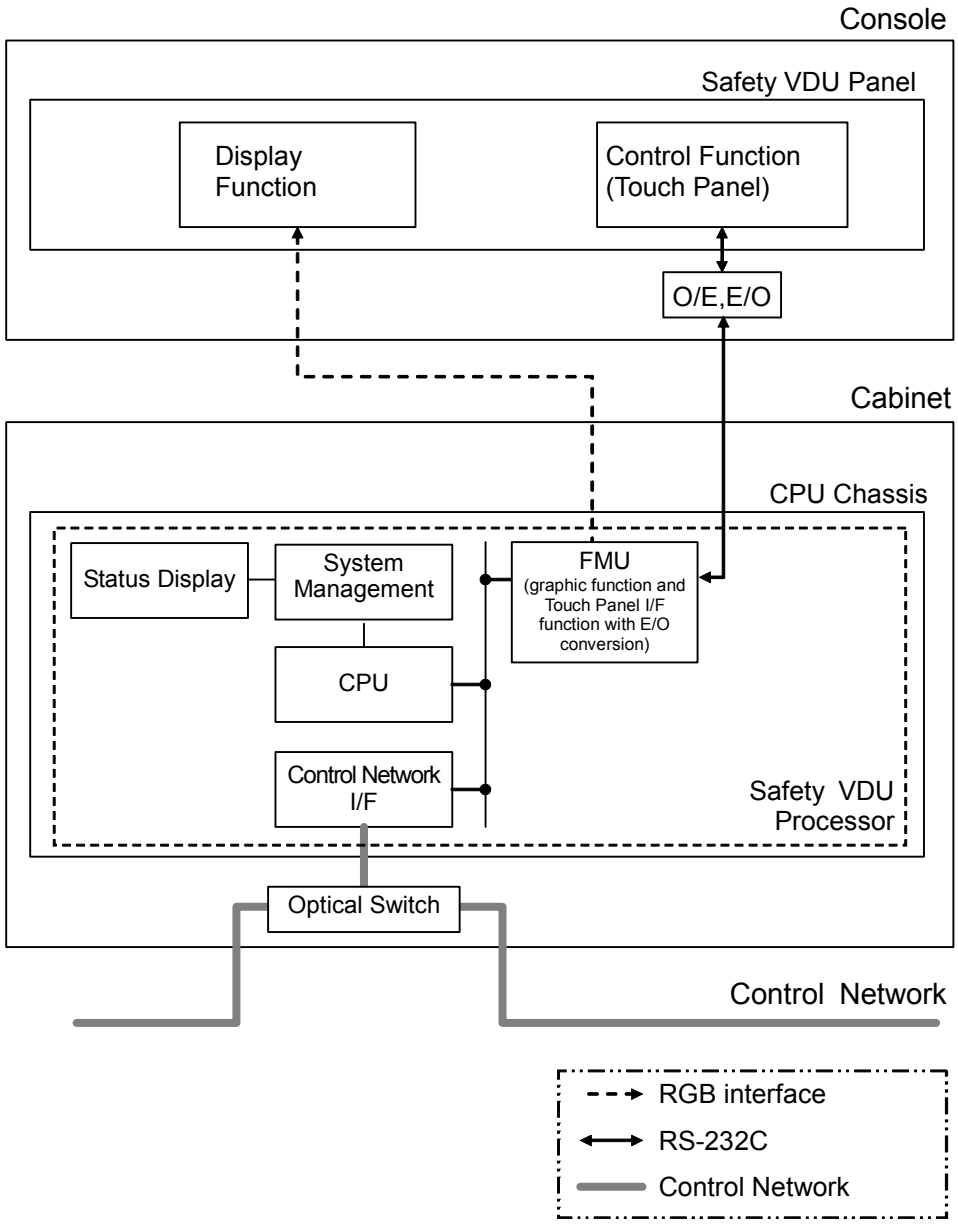


Figure 4.2-1 Configuration of Safety VDU Processor

4.2.1.2.2 Module Specifications of Safety VDU Processor

The safety VDU processor is comprised of the following modules:

- CPU Module
- System Management Module
- Control Network I/F Module
- Frame Memory Unit (FMU) Module
- Status Display Module

The FMU Module is specific to the safety VDU processor. The other modules are the same hardware as the modules of the controller. The following sections describe the modules that are specific to the safety VDU processor.

a) FMU Module

The FMU Module provides the analog RGB signal for the graphic images to the safety VDU panel. The FMU Module also provides the RS-232C touch panel interface signal from the safety VDU panel to the safety VDU processor. The FMU Module communicates with the CPU Module inside the chassis by means of the Futurebus+ backplane.

Specifications of the FMU Module are in Appendix A.11.

4.2.1.3 Power Supply

AC power can be supplied to the safety VDU with a single power supply configuration or a redundant configuration. The redundant configuration avoids loss of function due to a single failure in the power supply or the AC power source, as shown in Figure 4.2-2.

The AC power is converted to DC voltage by the Power Supply Modules. The power supplies for the safety VDU are the same as for the controller CPU Chassis. The power supplies for the safety VDU panel are unique to accommodate mounting within typical main control boards or operator consoles. For a redundant power supply configuration, the DC power from both sources is diode auctioneered for each component of the safety VDU.

Figure 4.2-2 Configuration of Power Supply for Safety VDU

4.2.1.4 Safety VDU Panel Optical to Electrical Converter Modules

Electrical/Optical (E/O) Converter Modules for the safety VDU panel convert the operator touch signals to optical signals. Specifications of the E/O Converter Module is in Appendix A.7

4.2.2 Software

The safety VDU processor software consists of basic software and application software. Each software function is described below.

4.2.2.1 Basic Software

The safety VDU basic software is designed to the same safety critical software integrity level as all other MELTAC basic software.

The safety VDU processor software structure is shown in Figure 4.2-3 . The software structure ensures reliable deterministic operation and is based on the same design as that of the controller basic software. With fixed cycle control and no external interrupts (except processing of self-diagnosis errors detected by the hardware within the CPU Module and the Power Supply Module and categorized as “Failure” (see Section 4.1.5)), the basic software provides high reliability, and deterministic processing.

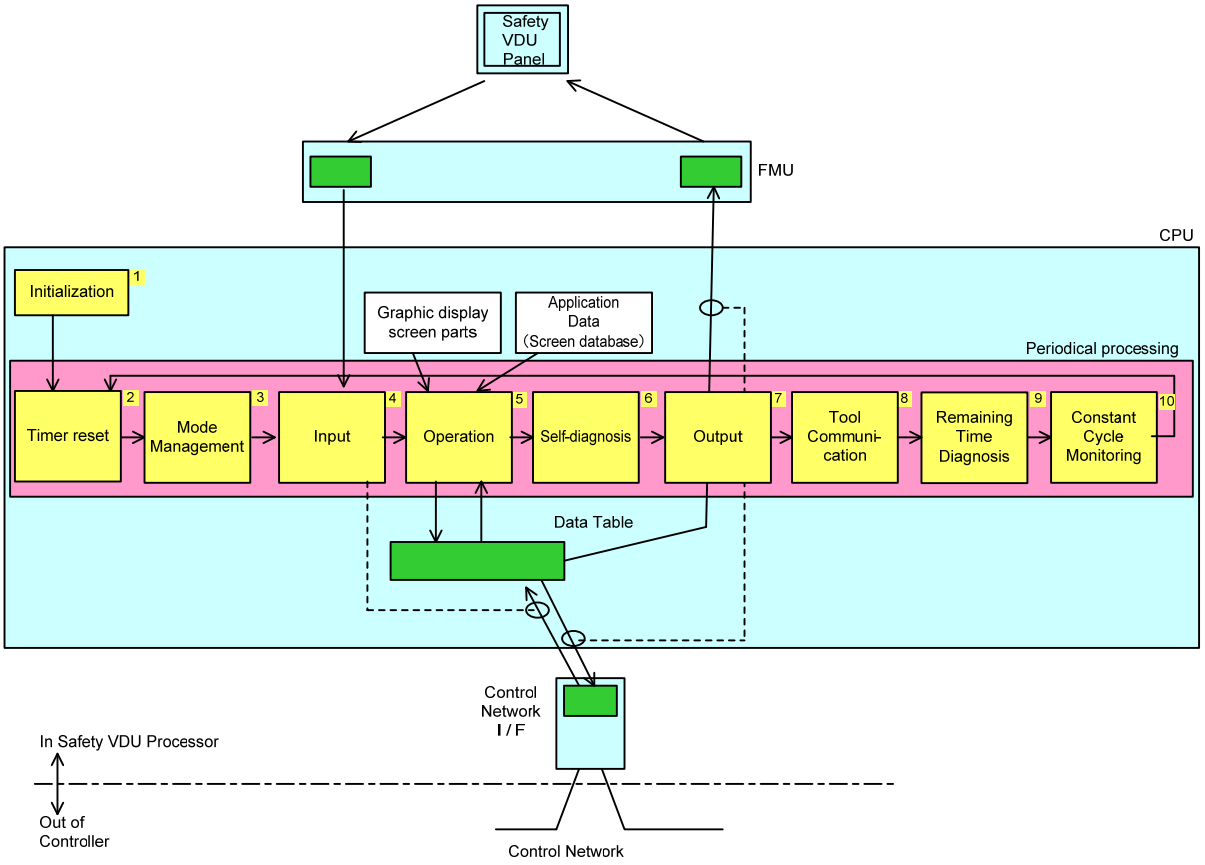


Figure 4.2-3 Software Structure of Safety VDU Processor

Details of the processing executed in each process are described below.
[

]

4.2.2.1.1 Screen Selection on the Safety VDU Processor

One operation within basic software process No.5 is Screen Selection. Screen Selection is described in this section.

Figure 4.2-4 shows the types of screens displayed by the safety VDU processor and the available screen transitions. The Initial Screen is the screen shown after the power is turned on. The types of information displayed on the Menu Screen, the Monitor Screen, and Operation Screen are shown in Table 4.2-1. The actual information displayed on these screens is configured uniquely for each application.

A sample of the operation switch image on the safety VDU panel is shown in Figure 4.2-5.

The screens described in this section are generic screens included in the generic basic software of the MELTAC platform. Other types of screens can be developed on a plant specific basis. The actual screens for any safety application are described in Application Licensing Document.

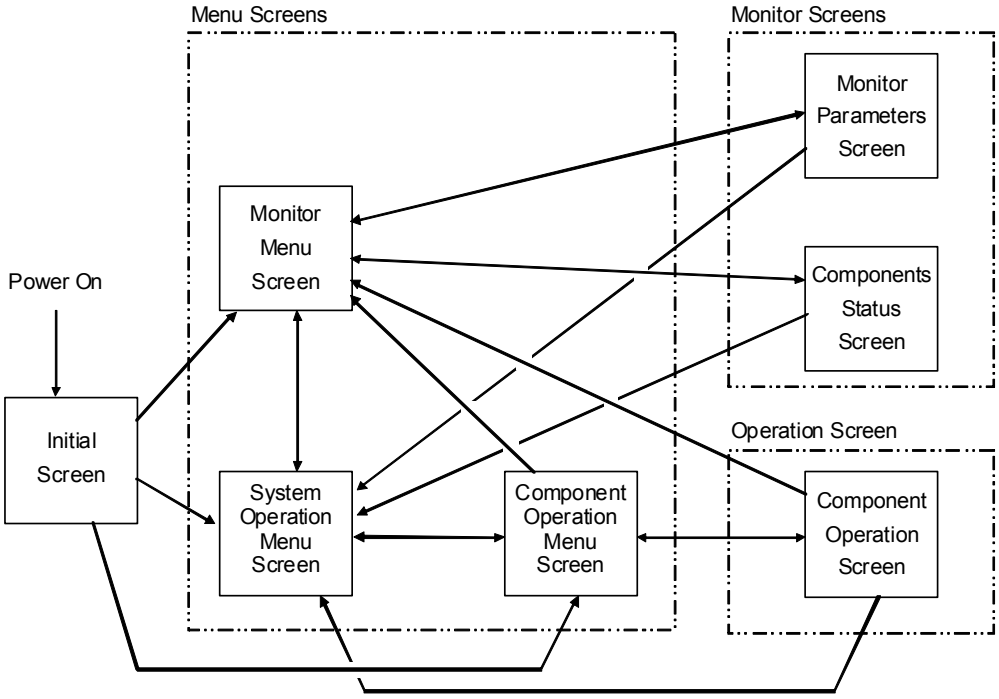


Figure 4.2-4 Screen Transition of the Safety VDU Processor

Table 4.2-1 Screen Descriptions

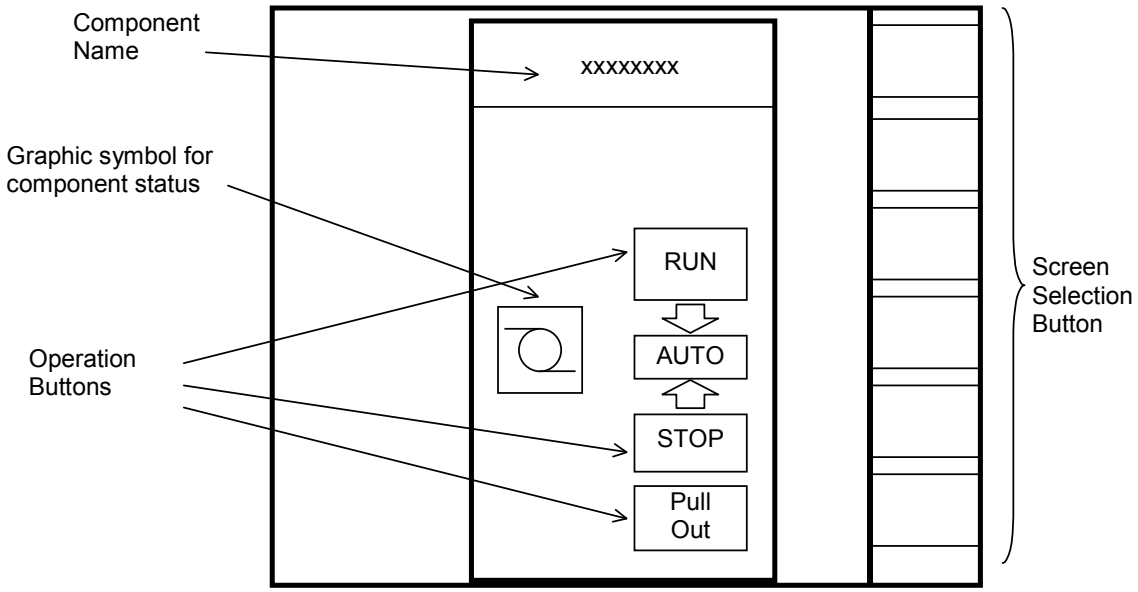


Figure 4.2-5 A Sample of Operation Switch Pictogram on the Safety VDU Panel

4.2.2.1.2 Detailed Explanation of Screen Display and Demand Processing

Basic software process No.5 also includes Screen Display Processing and Screen Demand Processing. These Operation processes and their relationship to other Operation processes are shown in Figure 4.2-6.
The table below shows the data used to create screen displays and the data used to generate output operation signals.

Table 4.2-2 Data Details

a) Screen Display Processing
[

]

b) Operation Demand Processing
[

]

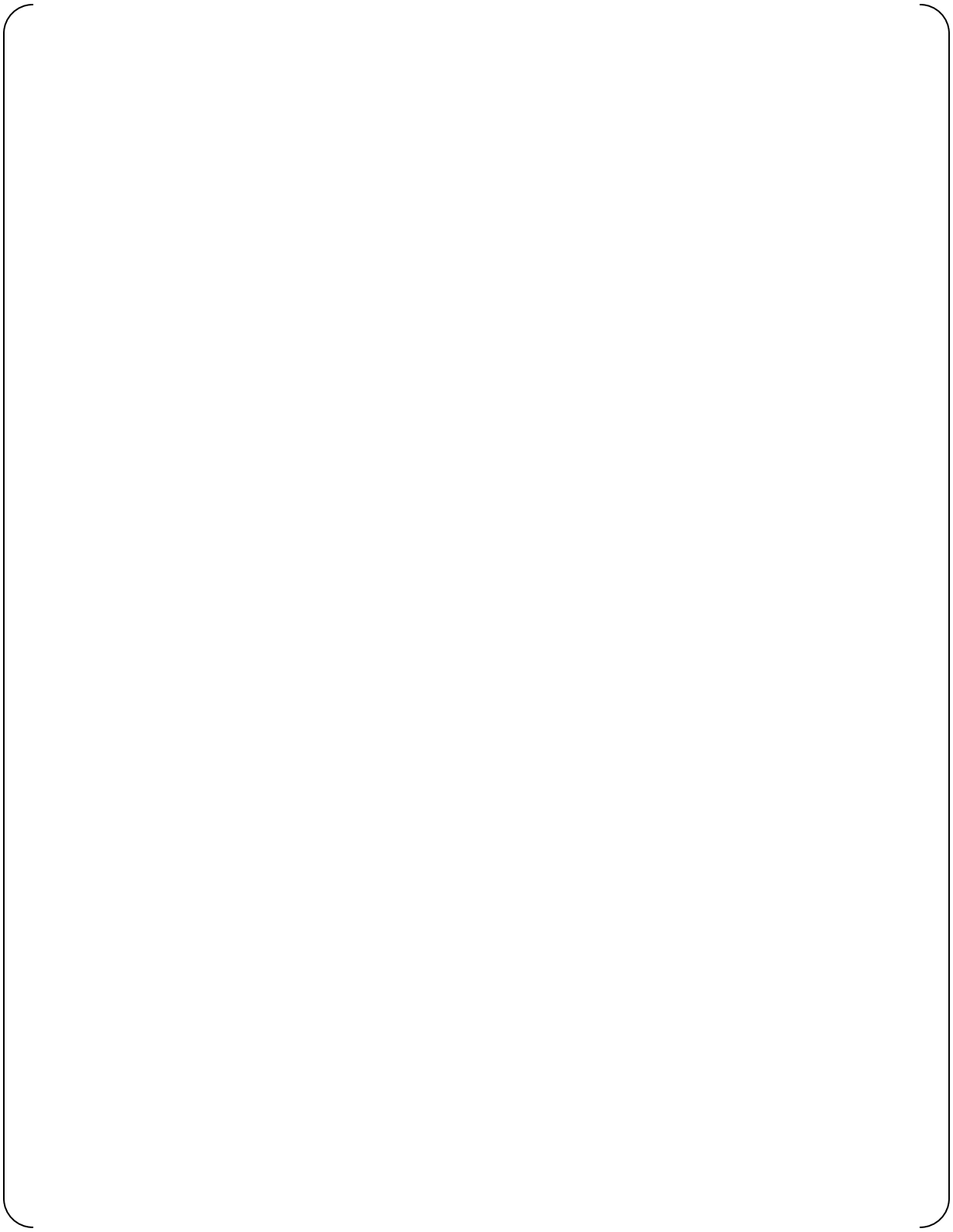


Figure 4.2-6 Explanation of the Safety VDU Processor Operation

4.2.2.2 Application Software and MELTAC Engineering Tools

[

]

4.2.3 Self-Diagnosis

[

]

4.2.4 Manual Test

The safety VDU panel is tested by manually touching screen targets and confirming correct safety VDU processor response.
This test is conducted using a special test display screen that does not initiate any manual control actions.

Many soft buttons are displayed throughout the special test display screen. When a button is touched, the safety VDU panel sends an Operation Touch Signal to the safety VDU processor. The safety VDU processor responds by changing the color of the touched button after receiving the signal.
During this test, the safety VDU processor does not send any touch command control signals to the Control Network.

These test response are generated by the safety VDU processor, so there is an overlap between the manual test and the platform self-diagnosis performed within the safety VDU processor.

4.3 Communication System

4.3.1 General Description

The key design bases of the Control Network, Data Link and Maintenance Network are provided below. These are applicable to both the controller and the safety VDU processor.

a) Maintenance Network, Control Network and Data Link:

- Asynchronous communication is used. The CPU Module and the communication controller execute their tasks asynchronously. This is facilitated through shared 2-port memory, which allows data to be communicated between the two digital components with no synchronization.
- The CPU Module performs no communication handshaking that could disrupt deterministic logic processing. The digital components that execute the safety functions are separate from the digital components that execute the communications.
- Predefined data size and structure ensure deterministic communication.
- Electrical faults or communication processing faults in one electrical division (or controller) cannot adversely affect performance of the safety function in other divisions (or controllers).

b) Maintenance Network:

- Hardwired interlocks in the CPU Module ensure changes to basic software or application software cannot be made through the data communication interface while the controller or the safety VDU processor are operating, or while the CPU Module is installed in the on-line chassis.

4.3.2 Control Network

The Control Network communicates plant process data and control signal data with a deterministic periodic cycle.

Inter-divisional communication for safety-related functions is not implemented in the Control Network. For this application only Data Link communication is used, see Section 4.3.3.

4.3.2.1 Configurations

The Control Network has two types of periodic cycles, normal and high-speed. The desired type is selected during the application design process.

The configuration of the Control Network is as shown in Table 4.3-1.

Table 4.3-1 Configuration of Control Network

A typical configuration of the Control Network for 6 controllers is shown in Figure 4.3-1.

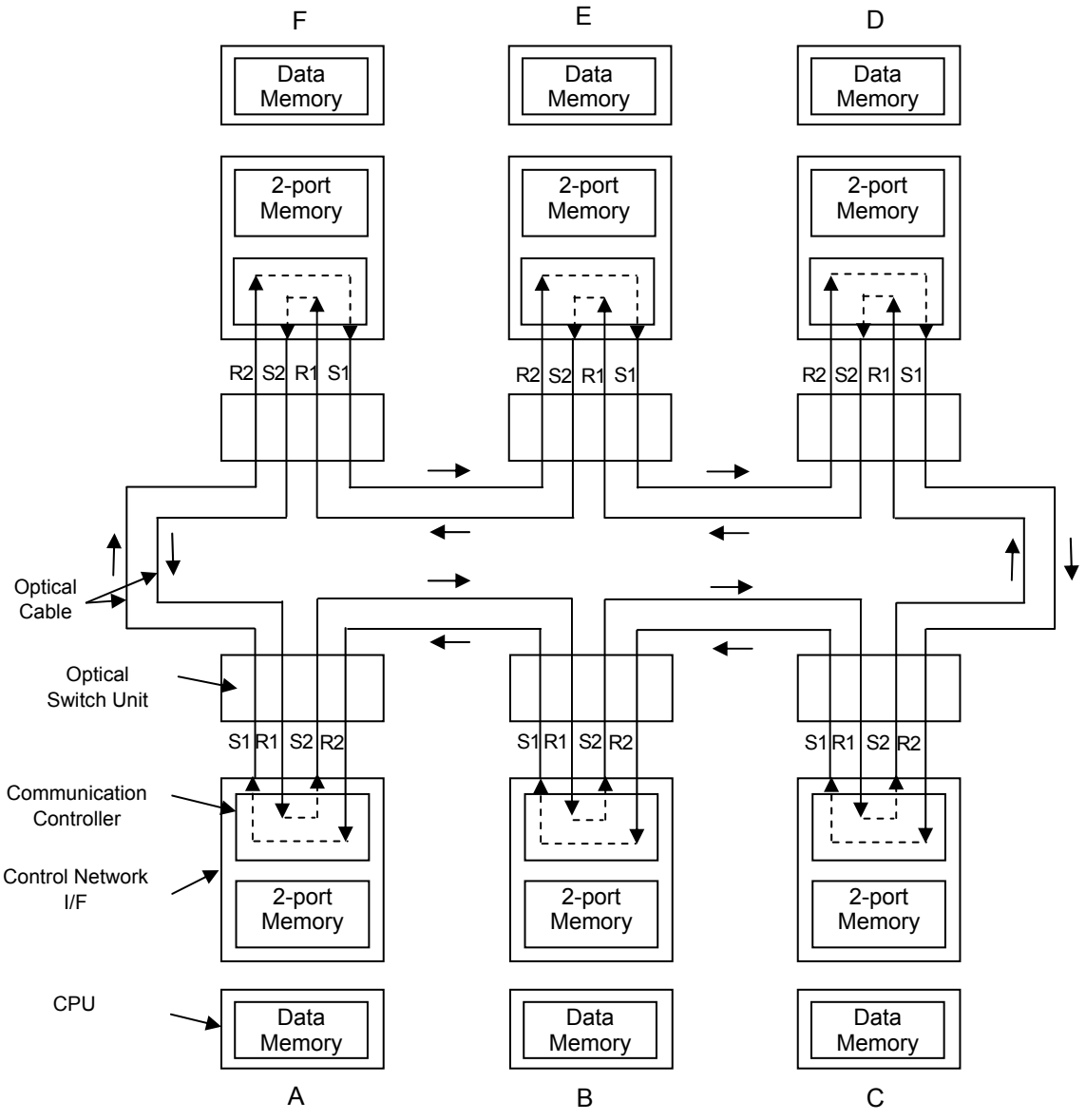


Figure 4.3-1 Configuration of Control Network

The Control Network I/F Modules are interconnected in a ring configuration. Each module communicates through an optical switch using 4 independent optical cables: S1 and S2 for transmission and R1 and R2 for reception as shown in Figure 4.3-1, in both clockwise and counterclockwise directions. The optical switch allows any subsystem on the Control Network that is halted or disconnected for maintenance or for failure, to be bypassed so the network ring topology is always maintained. Figure 4.3-2 shows the case where subsystem (B) is halted. In this case, the optical switch bypasses subsystem (B) and directly connects subsystem (A) and (C).

These are the key technical aspects of the Control Network:

- Each Control Network I/F Module includes 2 receive ports and 2 transmit ports for dual ring redundancy.
- All received data is relayed to the adjacent nodes (in both directions) by the communication controller within the Control Network I/F Module, until the data has been relayed to all nodes. **[**

  ]
- The communication controller also places the received data in 2-port memory for processing by the CPU Module in its node.
- The 2-port memory contains designated memory locations for the complete data package sent from each node on the Network. **[**

  ]
- **[**

  ]
- During its own deterministic cycle, the CPU Module reads data only from the memory locations in 2-port memory that correspond to the network nodes that send data that is relevant to its application software. **[**

  ]
- If the CPU Module only sends data to the Control Network (unidirectional data flow), as defined in **[ ]**, the CPU Module does not read any data locations in 2-port memory.
- The CPU Module places data to be transmitted on the Control Network in its designated area of 2-port memory, during its own deterministic cycle. The updated data overwrites the data written by the CPU Module in the previous cycle. If the data has not changed, the same data is rewritten again. This process repeats for every deterministic cycle of the CPU Module.
- The data from the CPU Module, that is stored within its designated location within 2-port memory, is then transmitted to the Control Network by the communication controller during its next deterministic relay/transmit cycle, along with the complete data package sent from each node on the network.
- The deterministic cycles of the communication controller and CPU Module are completely independent.

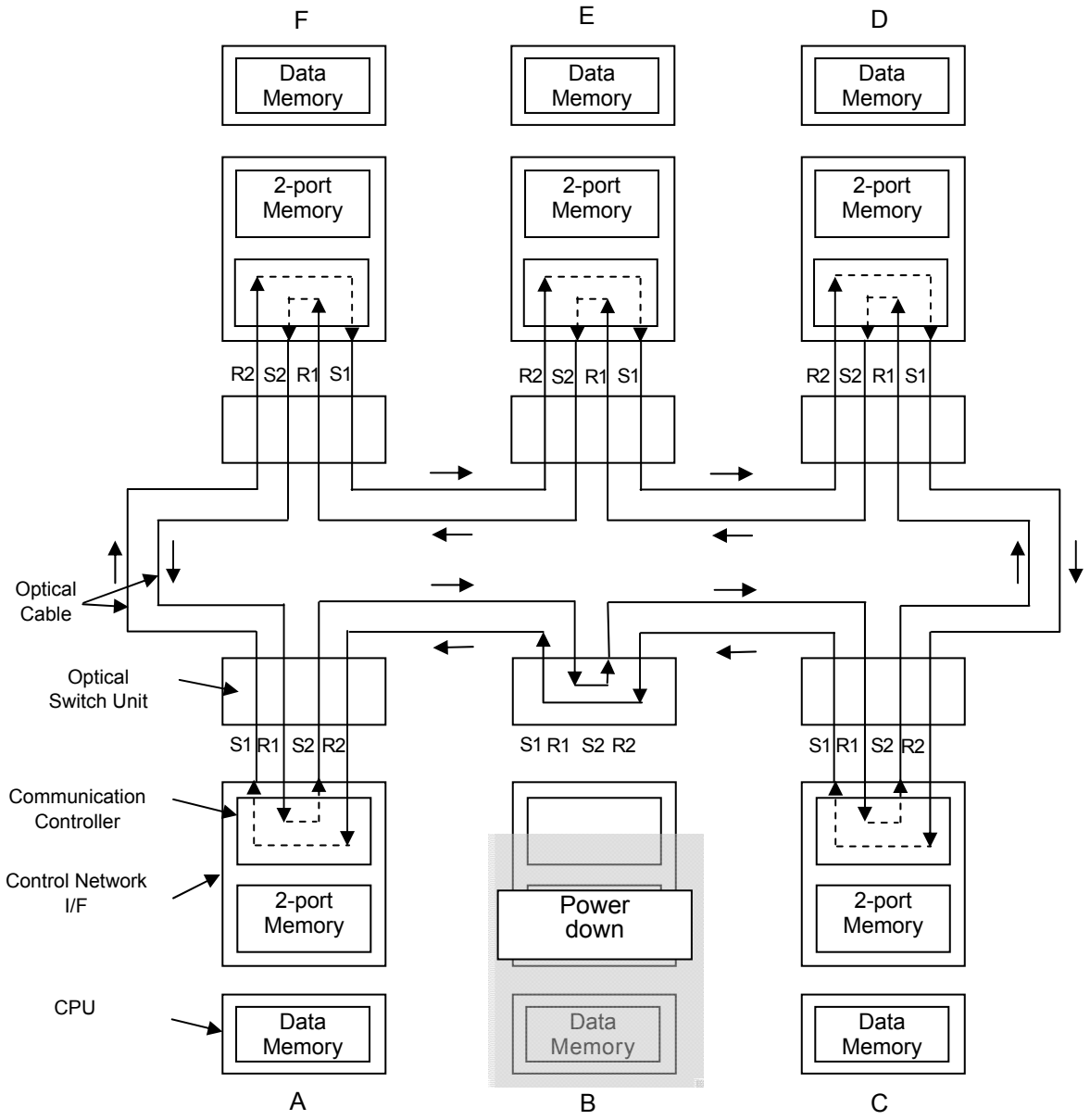


Figure 4.3-2 Explanation of Optical Switch Bypass Operation

The optical switch is powered by the power feeding cable from its associated Control Network I/F Module. If the node's CPU Module fails, or its Control Network I/F Module fails, or the power feeding cable is disconnected, the power is removed from the optical switch causing it to revert to Bypass Mode for that node. When failures are detected by a node's self-diagnosis, the Control Network I/F Module voluntarily removes the power from the optical switch.

A Control Network can bypass a minimum of one failed node. Additional nodes can be bypassed depending on the distance between nodes, as described in Table 4.3-2.

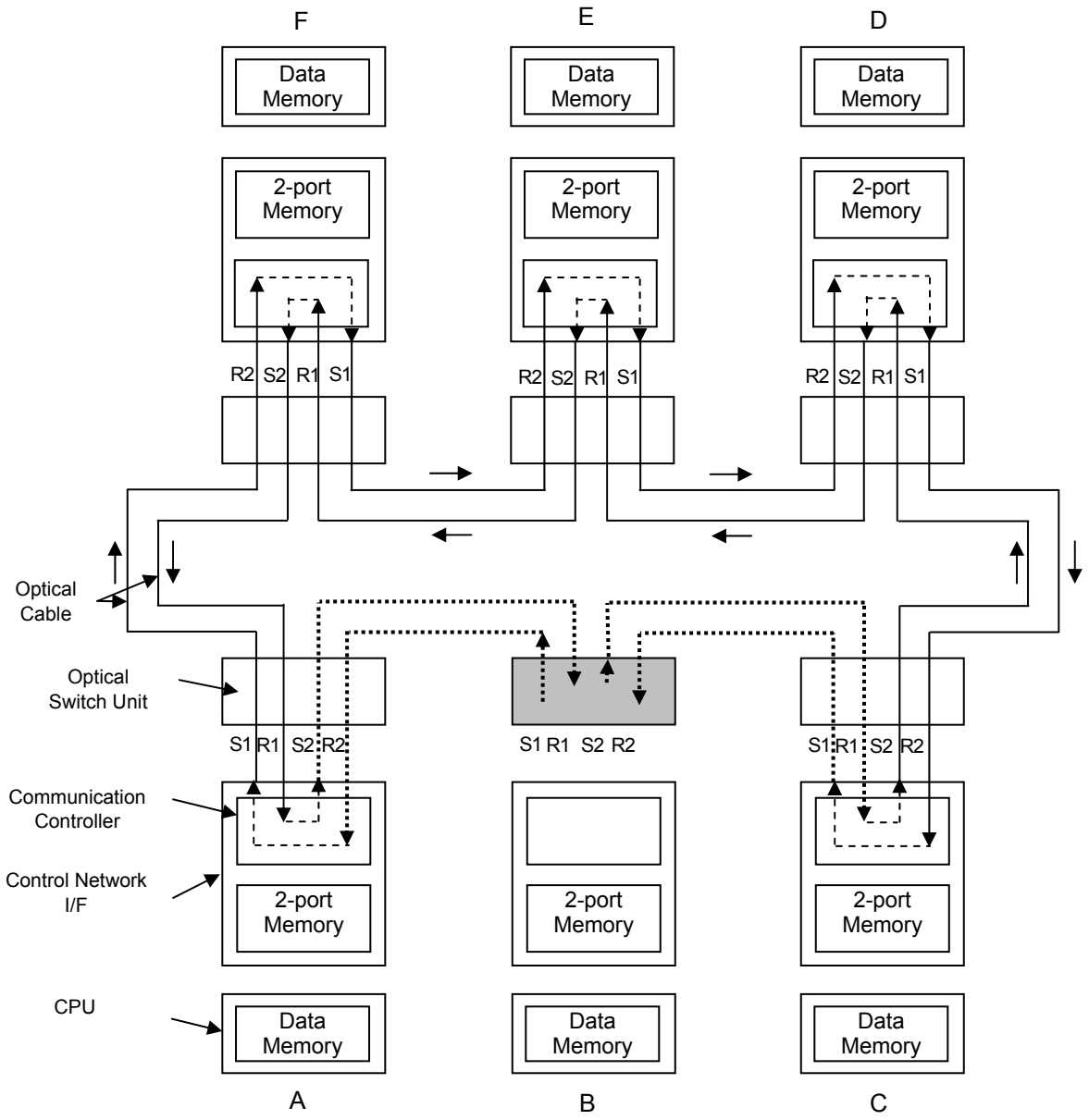


Figure 4.3-3 Explanation of Optical Switch Failure

Figure 4.3-3 shows the configuration of the network for failure of an optical switch. If the optical switch for subsystem (B) is in failure status, the communication path is disconnected between the optical switch and the Control Network I/F Module in subsystem (B), and between subsystems (A) and (C), as shown in the figure.

With the failure described above, the optical signal of subsystem (B)'s S1 and S2 port will be cut off. This will be detected by subsystem (A)'s R2 port and subsystem (C)'s R1 port, respectively. Thus the communication path that goes through subsystem (B) is determined to be unusable.

A communication path between subsystems (A) and (C) will then be established automatically via subsystems (D), (E), and (F). The same applies for communication from the other nodes that normally communicate through subsystem (B). Therefore, the only node that can no longer send or receive communication is subsystem (B). The send and receive communication between all other nodes remains fully operable.

The reconfiguration of the communication paths described above causes a momentary disruption of data communication on the Control Network **[ ]**. However, since the optical switch has been qualified, failure of an optical switch is a random hardware failure that can adversely affect the safety function of only one train; this momentary disruption is not considered in the normal Control Network response time. If the CPU Module reads the data in the Control Network I/F Module 2-port memory during this network reconfiguration disruption interval, the CPU Module will continue to use the data from the previous communication cycle. The CPU Module will alarm the network as failed if the data does not get updated after a predefined time.

4.3.2.2 Specifications

4.3.2.2.1 Infrastructure

The protocol stack of the Control Network is described in Figure 4.3-4.
The optical Gbit Ethernet is used for the physical layer.
The Resilient Packet Ring (RPR) based on IEEE Std. 802.17 is applied to the Data Link Layer protocol.

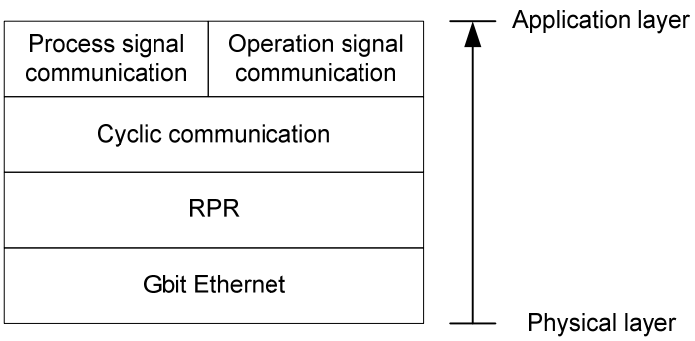


Figure 4.3-4 Protocol Stack of Control Network

The specifications of the Control Network are described in Table 4.3-2.

Table 4.3-2 Control Network Specification

Fiber cable, including outer and inner jackets and any strengthening components, is constructed using only non-conducting materials to ensure inherent isolation to prevent electrical fault propagation.

4.3.2.2.2 Communication Method

The data communication method of the Control Network is as follows.
[

]
The data is delivered to the destination Control Network I/F Module within the guaranteed data update cycle time, shown in Table 4.3-1.

4.3.2.2.3 Communication Controller

[

]

4.3.2.3 Isolation

The MELTAC platform maintains electrical isolation and communication isolation for the interface between controllers in separate safety trains and for the interface between safety controllers and any non-safety train. The methodology to ensure this isolation is described below.

a) Electrical Isolation

The MELTAC platform uses fiber optics and optical to electrical converters (E/O Converter) to ensure electric isolation. The optical communication circuit is shown in Figure 4.3-5

b) Communication Isolation
[

]

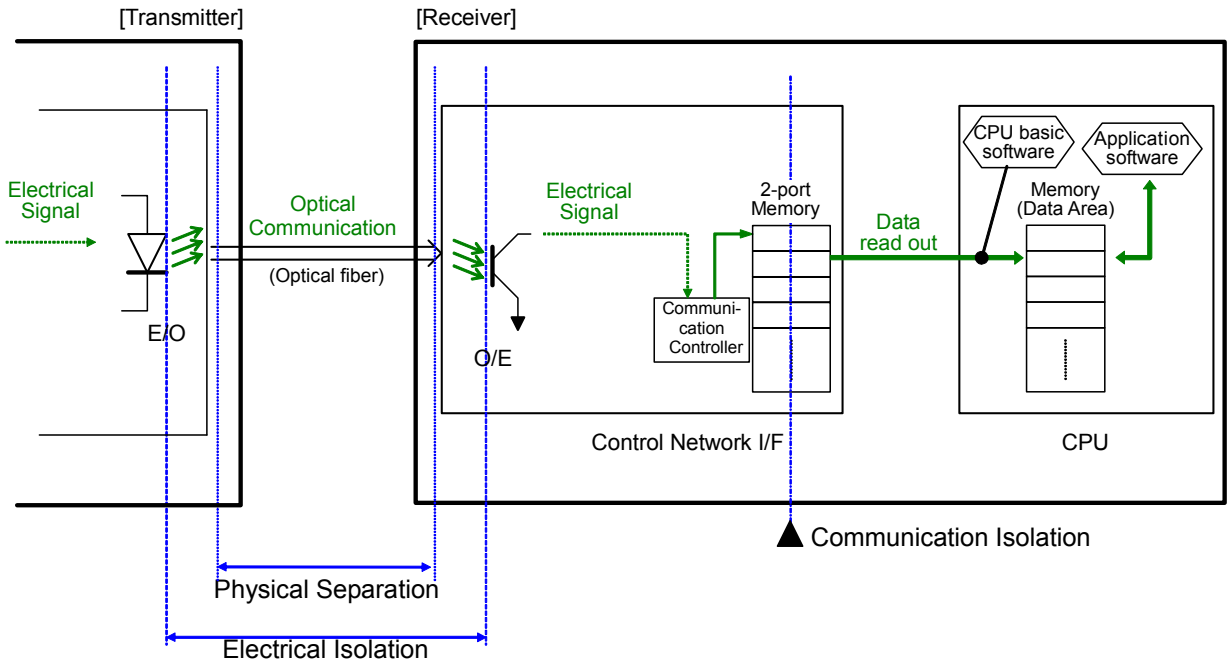


Figure 4.3-5 Separation in Communication of Control Network

4.3.2.4 Self-Diagnosis

The self-diagnosis functions of the Control Network are described below.
In MELTAC, a fatal error is defined as “Failure” and a tolerable error is defined as “Alarm” (see Section 4.1.5.). For Failure conditions, the CPU Module stops operation; the CPU Module continues operating for Alarm conditions. The application software determines the response to Alarm conditions. For loss of input data, options include using predefined values or the last good values. The categorization of self-diagnosis errors detected for the Control Network I/F Module, as defined in Table 4.3-3, is described below:

Table 4.3-3 Self-Diagnosis Functions of Control Network

4.3.2.5 Communication process

This section provides details for communication process, which is described in Section 4.3.2.3. To exemplify this communication process, this section describes the operational signal interface from the safety VDU (S-VDU) to the safety controller via the intra-division Control Network (referred to as the Safety Bus), and the monitoring signal interface from the safety controller to the S-VDU via the Safety Bus, as applied in a typical application.
Figure 4.3-6 is an example to show the receiving process from the S-VDU to the safety controller and Figure 4.3-7 is an example to show the sending process from the safety controller to S-VDU.

[

]

Figure 4.3-6 Operation Signal Flow from S-VDU

Figure 4.3-7 Process Signal Flow from Controller to Safety Bus

4.3.2.5.1 Detailed Data Flow

This section describes the detailed data flow between the Control Network I/F Module and the CPU Module in the safety controller.

[

]

Figure 4.3-8 Detail Signal Flow in Controller (Receiving Process)

[

]

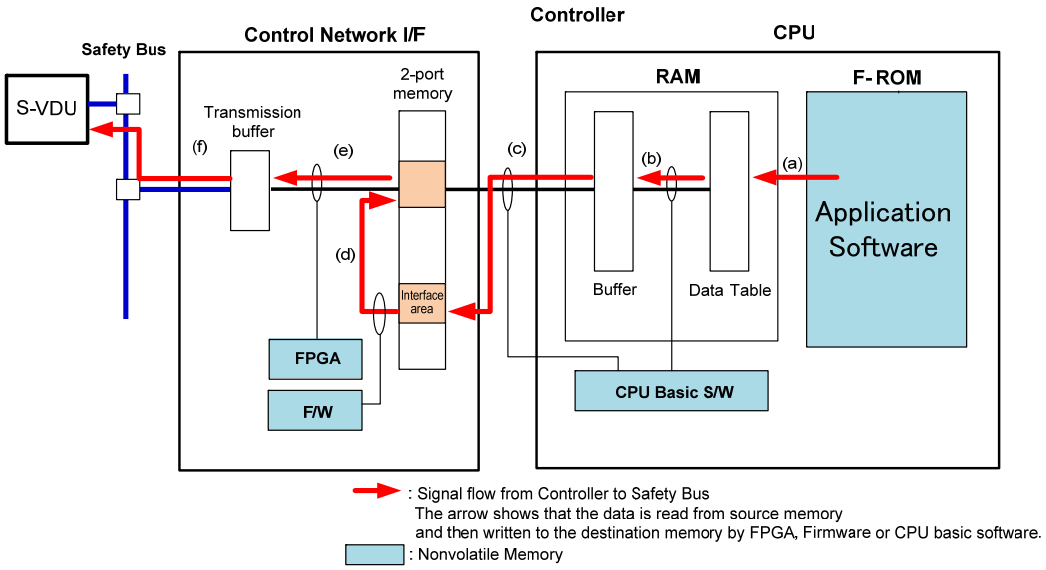


Figure 4.3-9 Detail Signal Flow in Controller (Sending Process of the Process Signal)

[

]

(1) Receiving process
(1-1) Processing by the Control Network I/F Module
This paragraph discusses the processing in the Control Network I/F Module.
Figure 4.3-10 provides details of Figure 4.3-8.

Figure 4.3-10 Processing by the Control Network I/F Module in the Receiving Process

[

]

(1-2) Processing by the CPU Module
This paragraph explains the processing of the data by the CPU Module.
Figure 4.3-11 provides details of Figure 4.3-8.

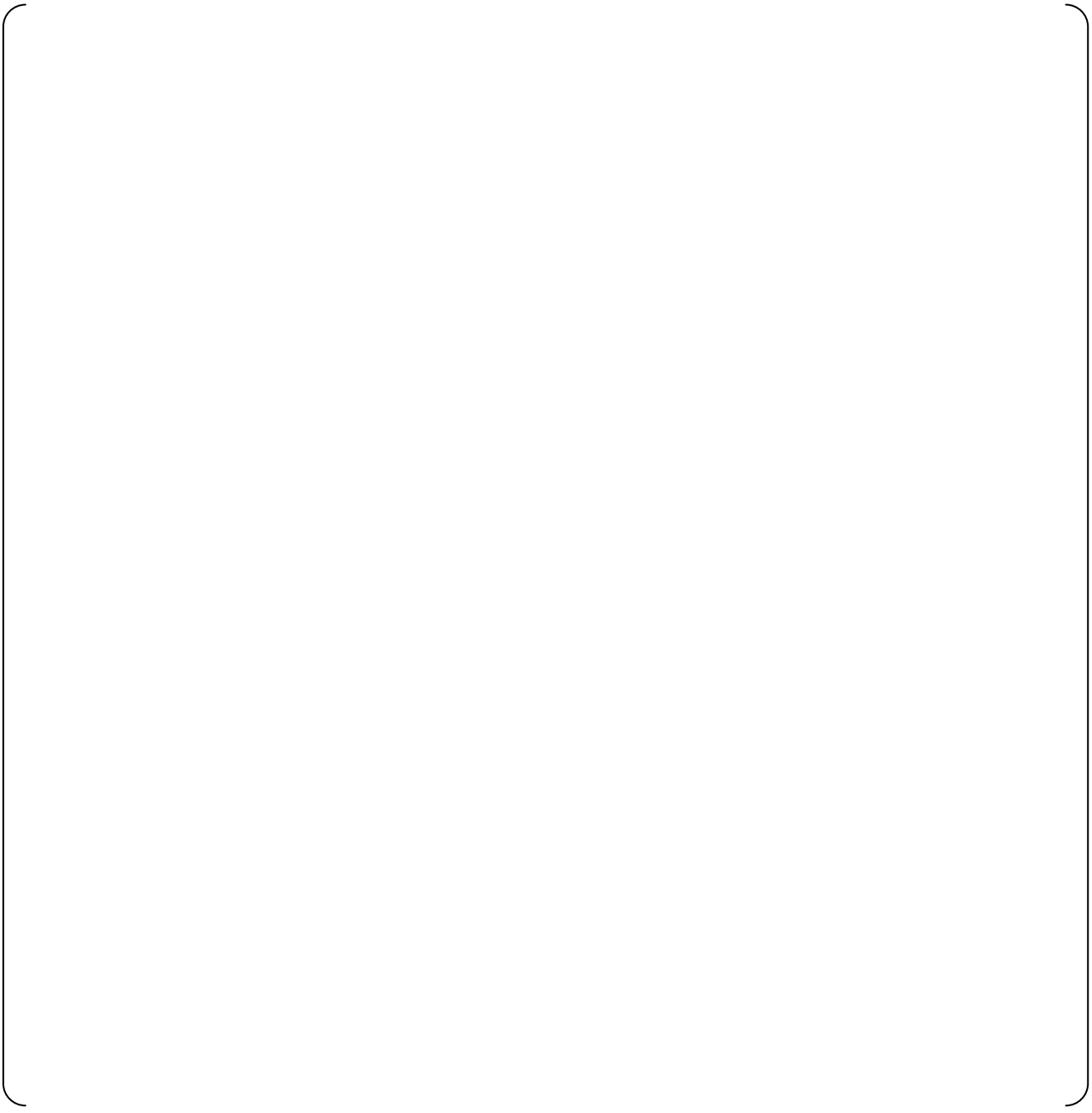


Figure 4.3-11 Processing by the CPU Module in the Control Network Receiving Process

[

]

(2) Sending Process
(2-1) Processing by the CPU Module
Figure 4.3-12 provides details of Figure 4.3-9.

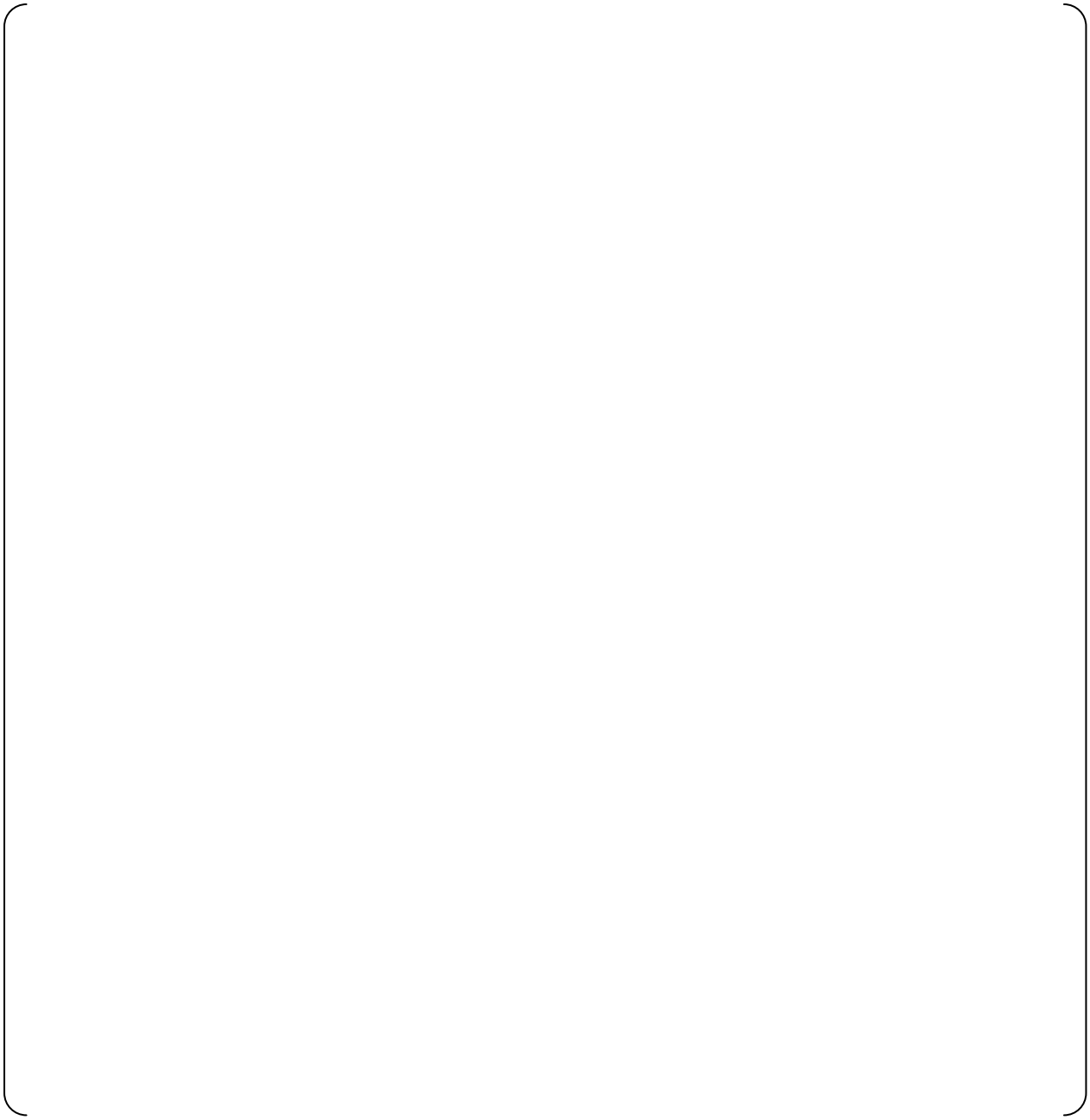


Figure 4.3-12 Processing by the CPU Module in the Control Network Sending Process

[

]

(2-2) Processing by the Control Network I/F Module
Figure 4.3-13 provides details of Figure 4.3-9.

Figure 4.3-13 Processing by the Control Network I/F Module in the Sending Process

[

]

4.3.2.5.2 Summary of Design Features for the Control Network Communications

The receiving process in the data flow from the S-VDU to the safety controller will be discussed in this section.
Following are design policies and network check methods for the Control Network interface.
[

]

[

]

4.3.3 Data Link

4.3.3.1 Configuration

Data Link communication is used to transmit process signals between the controllers in different safety trains. The Data Link uses a broadcast protocol with a 1 Mbps throughput, with no communication handshaking.

Figure 4.3-14 provides a graphical representation of typical Data Link connections between redundant safety trains. This figure shows all the Data Link components and an example of a connection configuration when CH1 of the controller for train A is the transmission port (T), CH1 of controllers for other trains is the reception port (R), CH4 of controller for train D is the transmission port (T), and CH4 of controllers for other trains is the reception port (R).

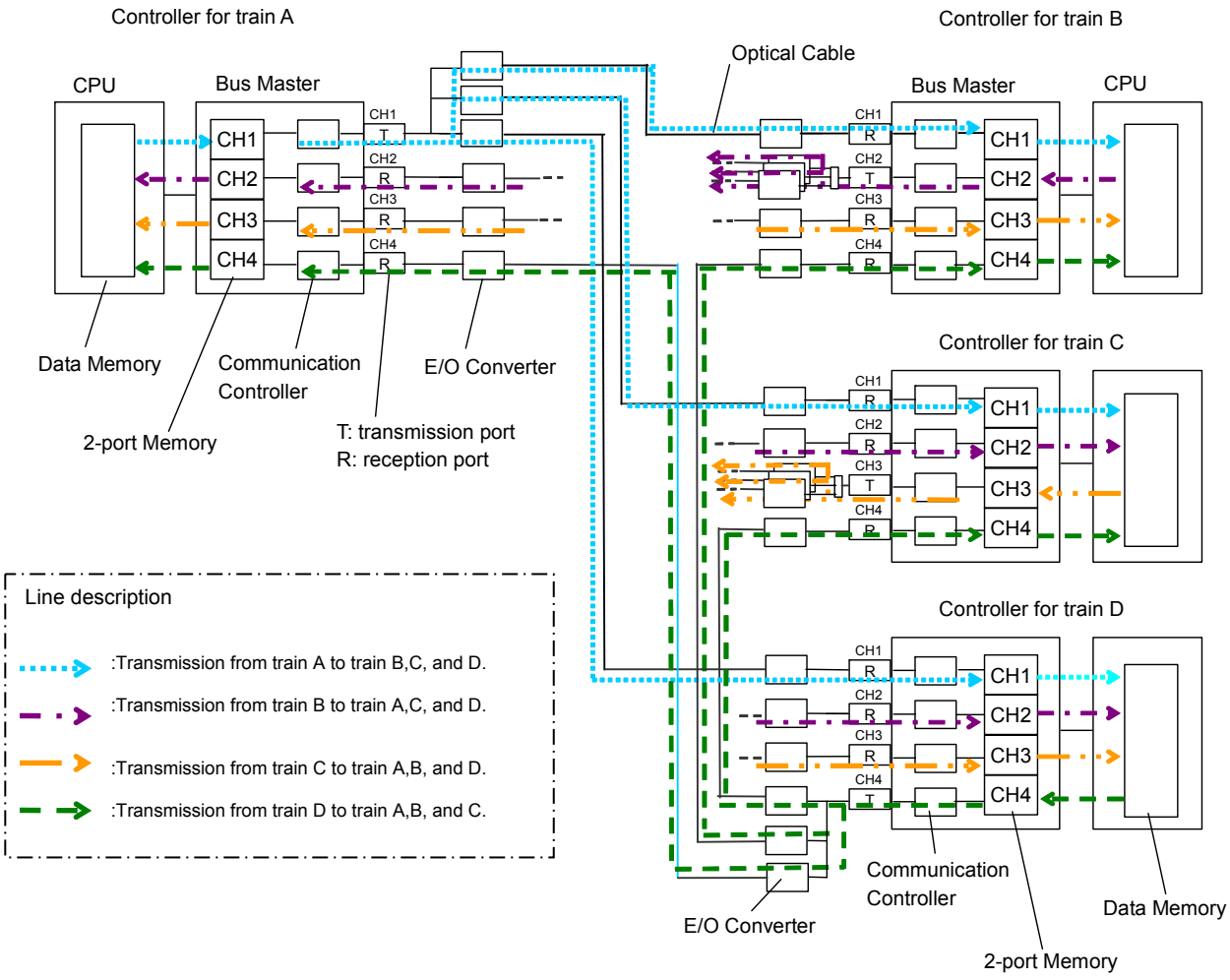


Figure 4.3-14 Example of Connection Configuration of Data Link Configuration

The Data Link is interfaced through Bus Master Modules. The Bus Master Module provides 4 communication ports (also referred to as channels). **[**

]

Each port is set either as a transmission port or a reception port. The Bus Master Module produces an electrical output. The output is divided into 3 signal lines; then each output is converted into an optical signal by the E/O Converter Module. The transmission port of the E/O Converter Module is connected by the optical cable to the reception port of the E/O Converter Module in another train.

[

]

4.3.3.2 Specifications

4.3.3.2.1 Infrastructure

The specifications of the Data Link communications are described in Table 4.3-4.

Table 4.3-4 Data Link Communication Specification

Fiber cable, including outer and inner jackets and any strengthening components, is constructed using only non-conducting materials to ensure inherent isolation to prevent electrical fault propagation.

4.3.3.2.2 Communication Method

[

]

4.3.3.2.3 Communication Controller

[

]

4.3.3.3 Isolation

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

The physical, electrical, and functional isolation, based on Figure 4.3-14, are described below.

a) Physical Separation
The E/O Converter Module of the Data Link allows for a distance of up to 1 km between sending and receiving controllers. This allows the controllers to be geographically separated into separate areas of the plant.

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

c) Communication Isolation
[

]

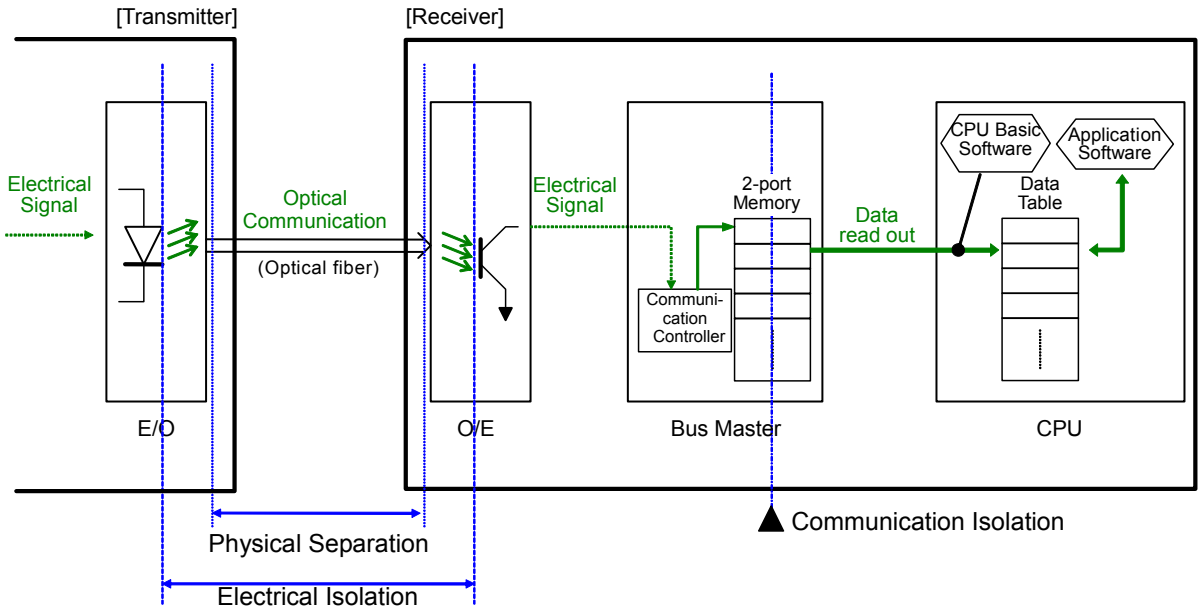


Figure 4.3-15 Separation in Communication of Data Link

4.3.3.4 Self-Diagnosis

The self-diagnosis functions of the Data Link are described below.
[

]

4.3.3.5 Communication Independence

This section describes how communication independence is maintained when the Data Link is applied to data communication between controllers in other trains. This section provides details on communication isolation, which is described in Section 4.3.3.3. To exemplify this independence, this section describes the Reactor Protection Processor (RPP) interface to controllers in other trains, as applied in a typical system. Figure 4.3-16 shows the configuration of a part of a typical 4 train RPP that is relevant to the partial trip signal to each of the other 3 RPP trains.

[

]

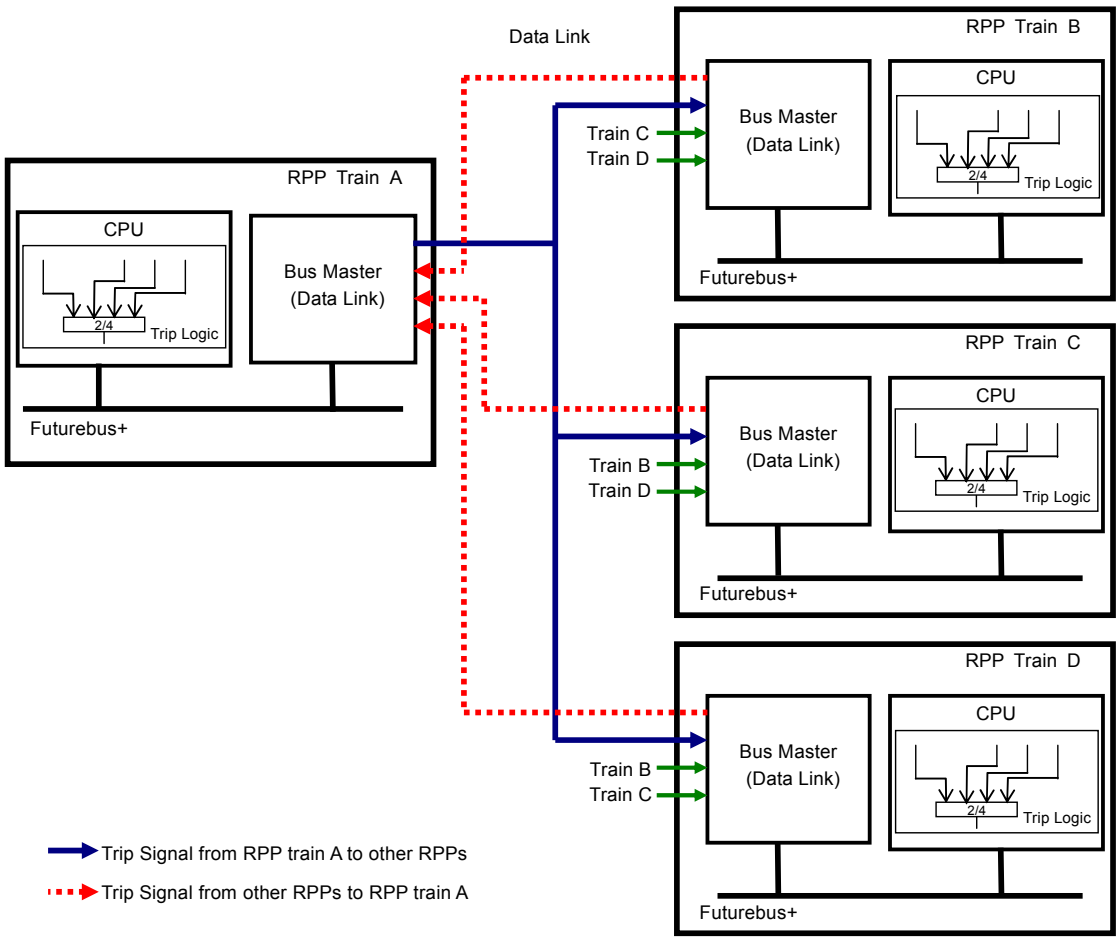


Figure 4.3-16 Partial Trip Signal Flow between RPPs

4.3.3.5.1 Detailed Data Flow

This section describes the detailed data flow between the Bus Master Module and the CPU Module in the RPP.

[

]

Figure 4.3-17 Detail Signal Flow in RPP (Receiving Process)

[

]

Figure 4.3-18 Detail Signal Flow in RPP (Sending Process of the Trip Signal)

[

]

(1) Receiving Process
(1-1) Processing by the Bus Master Module
Figure 4.3-19 provides details of Figure 4.3-17.

Figure 4.3-19 Processing by the Bus Master Module

[

]

(1-2) Processing by the CPU Module

Figure 4.3-20 provides details of Figure 4.3-17.

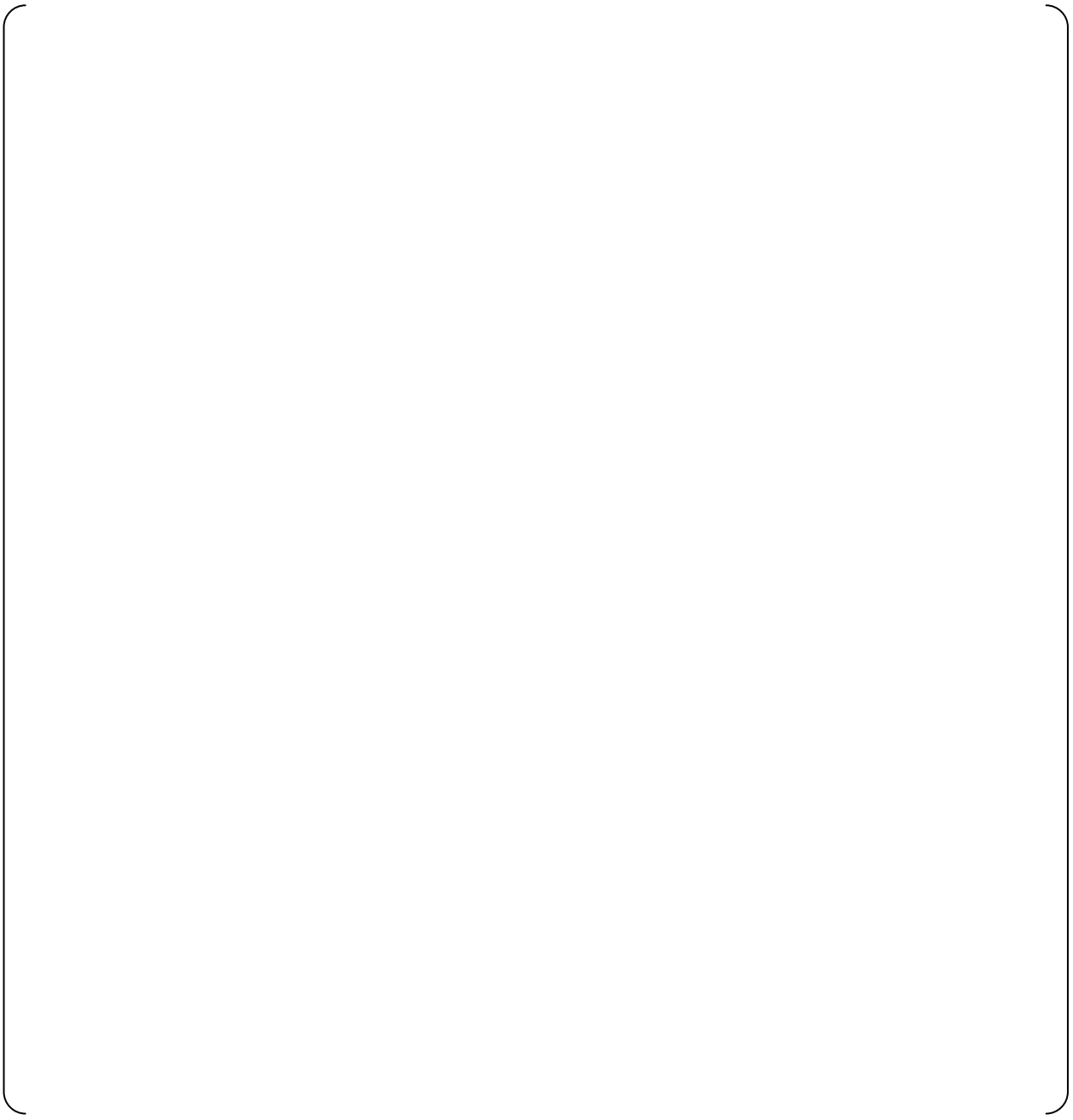


Figure 4.3-20 Processing by the CPU Module in the Data Link Receiving Process

[

]

(2) Sending Process
(2-1) Processing by the CPU Module
Figure 4.3-21 provides details of Figure 4.3-18.

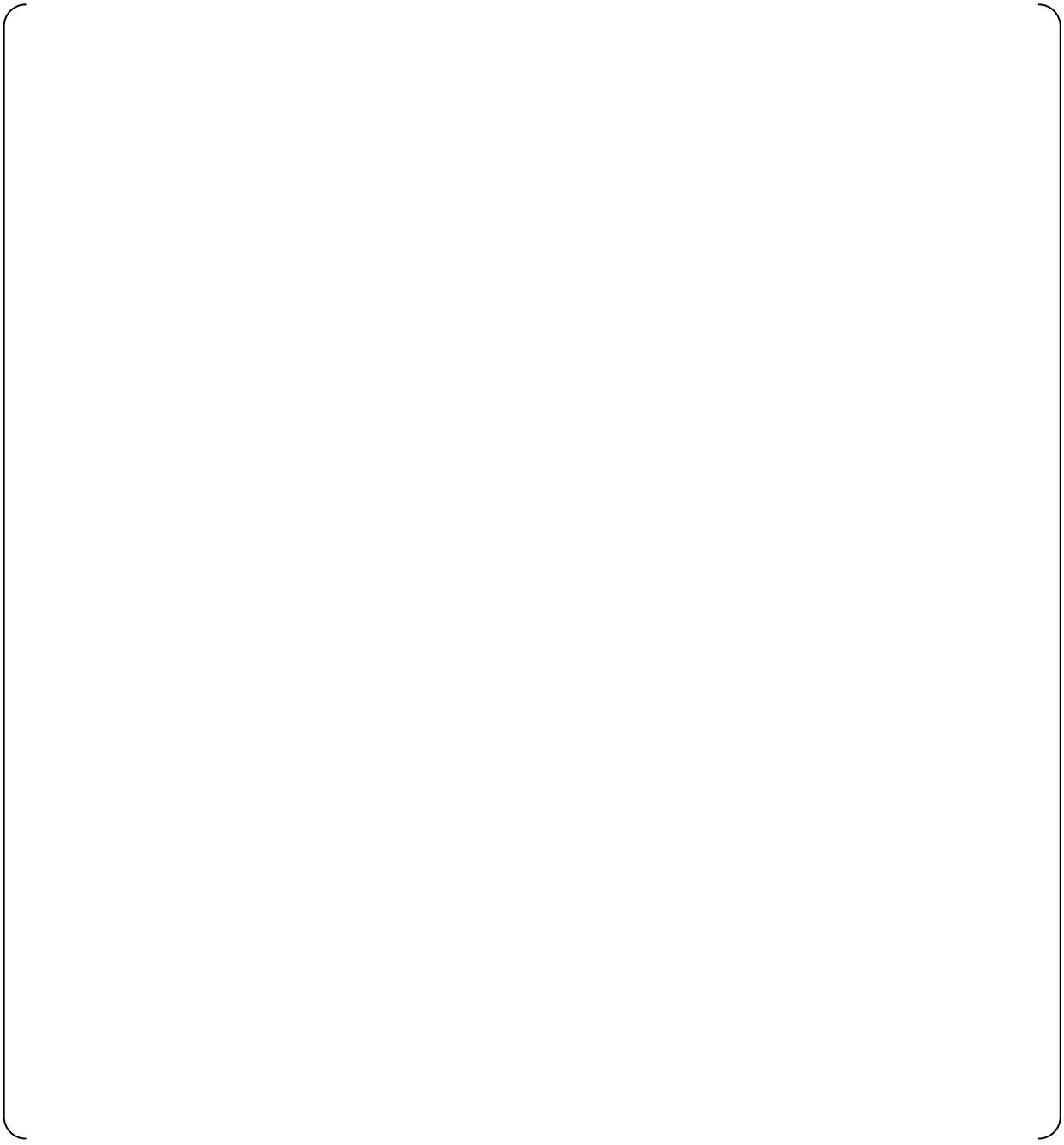


Figure 4.3-21 Processing by the CPU Module in the Data Link Sending Process

[

]

(2-2) Processing by the Bus Master Module
Figure 4.3-22 provides details of Figure 4.3-18.

Figure 4.3-22 Processing by the Bus Master Module in the Data Link Sending Process

[

]

4.3.3.5.2 Summary of Design Features for Data Link Communication

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

[

]

(3) Conformance to ISG-04
The conformance of ISG-04 is shown in MELTAC platform ISG-04 Conformance Analysis (JEXU-1041-1015).

4.3.4 Maintenance Network

4.3.4.1 Configuration

The Maintenance Network is used to communicate between the controllers or safety VDU processor and the MELTAC engineering tool, to download new application software to the CPU Module (when installed in the dedicated Re-programming Chassis), or to read/write inside the Data Table of the controller. There may be up to 3 MELTAC engineering tools connected to one controller at any one time. The number of engineering tools actually connected to the Maintenance Network is application dependent.
The description of the controller's processing of data for the MELTAC engineering tool is described in Section 4.1.4.2.
Figure 4.3-23 shows the Maintenance Network configuration for one division. In this figure the Maintenance Network is connected to the controllers. The controllers are normally disconnected at the controller end during normal operation. The controllers are connected periodically for equipment maintenance. A connection signal may be configured in the application software to generate an alarm in the Main Control Room (MCR) when the engineering tool is connected.

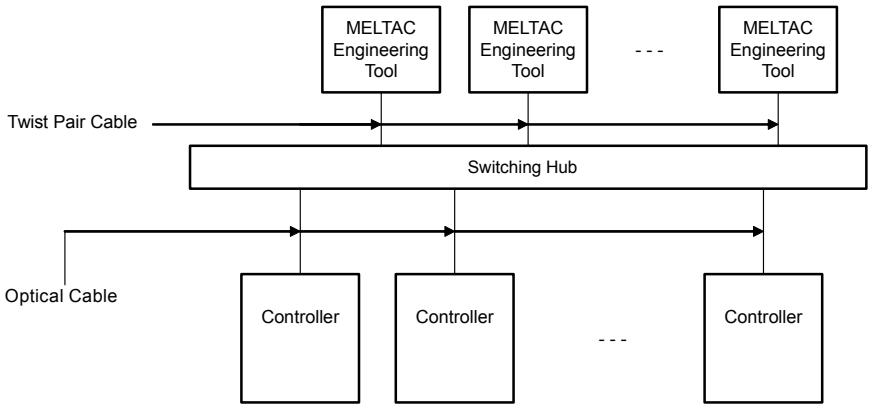


Figure 4.3-23 Maintenance Network Configuration

4.3.4.2 Isolation

[

]

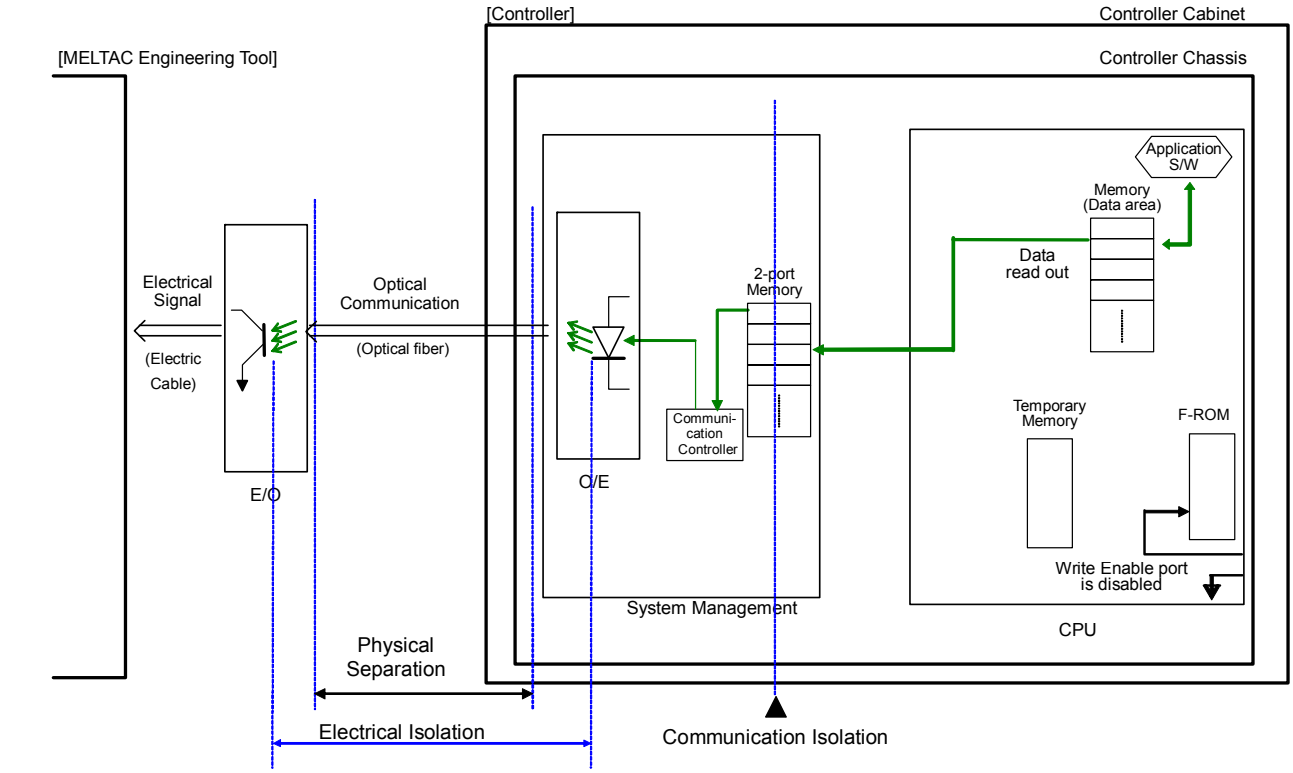


Figure 4.3-24 Separation in Communication of the Maintenance Network

Figure 4.3-25 Dedicated Re-programming Chassis for Writing to the F-ROM

The MELTAC engineering tool and Switching Hub are connected to the controller based on the following design features:

- The non-safety MELTAC engineering tool and Switching Hub are electrically isolated from the safety components through qualified fiber optic isolators with E/O Converters of System Management Module.
- The communication interface for each controller uses a separate System Management Module with 2-port memory to ensure the communication process and safety function process execute asynchronously.

The controller is normally disconnected from the Maintenance Network, so there is no communication with the MELTAC engineering tool. However, when the controller is connected to the Maintenance Network, the following applies:

- When the controllers are in service (i.e.: with the CPU Module in its normal configuration in the controller cabinet and with the write enable port of the F-ROM disabled) they provide only outbound communication to the MELTAC engineering tool (i.e.: there is no ability for the MELTAC engineering tool to write information to the controller's memory), based on data requests from the MELTAC engineering tool.

[

]

4.3.4.3 Design Basis of Connection to Maintenance Network

[

]

4.3.4.4 Specifications

4.3.4.4.1 Infrastructure

The specifications of the Maintenance Network communication are described in Table 4.3-5.

Table 4.3-5 The Maintenance Network Communication Specification

Fiber cable, including outer and inner jackets and any strengthening components, is constructed using only non-conducting materials to ensure inherent isolation to prevent electrical fault propagation.

4.3.4.4.2 Communication Method

[

]

4.3.4.4.3 Communication Controller
[

]

4.4 Response Time

The response time depends on the configuration of the controller for a specific application. The worst case response time is determined by combining the response time of individual control processes. This section describes the concepts behind the processing time of each control process. It also describes the calculation method to determine the total response time of an application for a typical hardware configuration. All self-diagnosis are considered in the response time calculation method.

As described in the following sections, the worst case response time is deterministic. Therefore, the response time conforms to BTP 7-21.

4.4.1 Processing Time of MELTAC Fundamental Cycle

[

]

Figure 4.4-1 The Time Chart of Fundamental Process in Cyclic

[

]

4.4.2 Processing Time of MELTAC Application

The MELTAC platform is composed of the CPU Module, Bus Master Module, various types of I/O module, Control Network I/F Module and safety VDU panel. An external input is processed by each of these components before the control result is output to external terminal(s). Figure 4.4-2 is an example of a typical MELTAC hardware configuration, including communication between 2 controllers. As shown in Figure 4.4-2, the same process applies to many components of a typical application. Table 4.4-1 shows the method to calculate the minimum and maximum response time for each process (T1 – T7). Each process executes asynchronously. Therefore, the minimum time reflects a theoretical situation where each consecutive process is completed prior to the initiation of the next process. Similarly, the maximum time reflects a theoretical situation where each consecutive process is completed just after the initiation of the next process; therefore each process requires an additional cycle.

Response times for safety critical applications, such as reactor trip and ESF actuation, are based on the maximum time.

Figure 4.4-2 Internal Process Divisions of the MELTAC Platform to Perform Response Time Calculations

Table 4.4-1 Description of Processing in Each Component (Maximum/Minimum Values)

4.4.3 Examples of Response Time Calculations

[

]

4.5 Control of Access

[

]

4.5.1 Control of Access for Hardware

[

]

4.5.2 Control of Access for Software

[

]

4.5.3 Control of Access for Temporary Changes to Process Values

[

]

5.0 ENVIRONMENTAL, SEISMIC, ELECTROMAGNETIC AND ISOLATION QUALIFICATION

This section describes the environmental, seismic, electromagnetic, surge withstand capability, electrostatic discharge and isolation qualifications of the MELTAC platform. The method and the result of the qualification testing are described. If any module is updated, and it is determined that qualification re-testing is required by the evaluations conducted in accordance with Section 6.1.7, the module will be tested with the same method and acceptance criteria. The same method and acceptance criteria will also be used for any new MELTAC modules.

Table 5.0-1 shows the regulatory requirements and acceptance criteria for each test.

Table 5.0-1 Regulatory Requirements and Reference to Acceptance Criteria for Each Qualification Test

Test Item	Regulatory Requirement	Reference to Acceptance Criteria
Environmental Test	RG 1.89 (IEEE Std. 323-1974)	System Level Test: 5.1.2.1 Module Level Test: 5.1.2.2
Seismic Test	RG 1.100 (IEEE Std. 344-2004)	Cabinet Test: 5.2.2.1 Module Level Test: 5.2.2.2
Electromagnetic Test	RG 1.180	Conducted Emissions, Low Frequency (CE101) Test: 5.3 Conducted Emissions, High Frequency (CE102) Test: 5.3.2.1 Radiated Emissions, Magnetic Field (RE101) Test: 5.3.2.2 Radiated Emissions, Electric Field (RE102) Test: 5.3.2.3 Conducted Susceptibility, Low Frequency (CS101) Test for Power Leads: 5.3.2.4 Conducted Susceptibility, High Frequency (CS114) Test for Power Leads: 5.3.2.5 Conducted Susceptibility, High Frequency (CS114) Test for Signal Leads: 5.3.2.6 Conducted Susceptibility, Bulk Cable Injection, Impulse Excitation (CS115) Test: 5.3.2.7 Conducted Susceptibility, Damped Sinusoidal Transients (CS116) Test: 5.3.2.8 Radiated Susceptibility, Electric Field (RS103) Test: 5.3.2.9
Surge Withstand Capability Test	RG 1.180 (IEC 61000-4-12, IEC 61000-4-5, IEC 61000-4-4)	5.3.2.10 Surge Withstand Capability, Ring Wave Test 5.3.2.11 Surge Withstand Capability, Combination Wave Test 5.3.2.12 Surge Withstand Capability, Electrically Fast Transients/Bursts Test
Electrostatic Discharge Test	IEC 61000-4-2	5.4
Isolation Test	RG 1.75 (IEEE Std. 384-1992)	5.5

The overview of the qualification tests, test methods, acceptance criteria and any deviations from the acceptance criteria for the MELTAC modules are provided in Sections 5.1 through 5.5. These qualification tests demonstrate that the MELTAC platform is in accordance with the regulatory requirements in Table 5.0-1.
The test items and results are presented in the following test reports. The test reports reference the test procedures.

Table 5.0-2 Test Reports

Test Item	Test Report
Environmental Test	MELTAC-Nplus S Environmental Test Report (JEXU-1041-1044)
Seismic Test	MELTAC-Nplus S Seismic Test Report (JEXU-1041-1045)
Electromagnetic Test, Surge Withstand Test, Electrostatic Discharge Test	MELTAC-Nplus S EMC/ESD Test Report (JEXU-1041-1046)
Isolation Test	MELTAC-Nplus S Isolation Test Report (JEXU-1041-1047)

5.1 Environmental Qualification Testing

5.1.1 Environmental Specification and Outline of Test

The environmental specifications of the MELTAC platform are shown in Section 4.1.1.4.
The tests are performed to demonstrate that the MELTAC platform will continue to operate without loss of functions under the identified abnormal environmental conditions (temperature, humidity).

The MELTAC platform System Environmental Testing is performed in a cabinet equipped with representative components of the platform.

The MELTAC platform System Environmental Testing is in accordance with RG 1.89 which endorses IEEE Std. 323-1974.

5.1.2 Contents of Environmental Test

5.1.2.1 System Level Environmental Test

The MELTAC modules mounted inside the cabinet for the System Environmental Tests are selected as those that are deemed necessary to confirm the safety function of a typical reactor protection system, including the bi-stable operation and the trip signal output.

(1) Method
For the System Environmental Tests, a cabinet equipped with the MELTAC modules interconnected and powered in a test configuration is placed inside a thermostatic chamber. The test configuration produces the worst case expected temperature rise across the module chassis and across the cabinet. Before, during, and after each test, it is confirmed that there are no equipment failures or abnormal functions such as erroneous bi-stable operation or erroneous trip signal output, etc. To determine whether any functional abnormalities occurred, the output signals are recorded on a chart recorder to capture any erroneous output during the test. In addition, the test confirms that the self-diagnosis function of the MELTAC platform detects no abnormalities during the test. The test also confirms that the self-diagnosis function is still operating at the end of the test.

(2) Acceptance Criteria
For the System Environmental Test, the correct performance of the system is confirmed during the following tests.
[

]

5.1.2.2 Module Environmental Test

The MELTAC modules for the Module Environmental Test are shown in Appendix A.
For module types with similar circuit electronics whose differences will have no impact on environmental test results, such as NO vs. NC contacts or differences in their input ranges, one typical module type is selected.

[

]

5.2 Seismic Qualification Testing

5.2.1 Overview

The seismic qualification testing confirms that the MELTAC platform maintains structural integrity and correct functional operation during and after a design basis earthquake. Seismic testing is part of the overall system seismic qualification which ensures there is no negative effect on the safety protection function of the equipment in case an earthquake occurs during plant operation.

The Cabinet Seismic Resistance Test is performed with a MELTAC cabinet fully loaded with most, but not all, MELTAC components. For the Cabinet Seismic Resistance Test, a test specimen is prepared for a typical safety protection system application. The tests are conducted using a 3-Direction large shaker table. The test specimen is vibration-excited on the tri-axial shaker table. During the test, the physical integrity and vibration characteristics of the cabinet are confirmed. All system functions are also confirmed before, during and after the excitation. The input acceleration used for the Cabinet Seismic Resistance Test is set high enough to cover the floor response spectrum range of power plants in the U.S.

In addition, the Module Seismic Resistance Tests are performed for mechanically different MELTAC-Nplus S components. For modules that have similar structures and positions of parts, one typical module type is tested because the module differences, such as input ranges, will have no impact on their seismic capability. Other mechanically comparable modules are qualified by similarity to the tested module. The similarity analysis for any untested modules is documented in the Seismic Qualification Report. The modules are mounted in a chassis for the Module Seismic Resistance Test.

In the seismic test, the acceleration ratio applied to the modules mounted in the cabinet with respect to the input acceleration of the cabinet increases with the position of the height within the cabinet. Hereafter, this acceleration ratio is called “response ratio”. For the Module Seismic Resistance Tests, the cabinet maximum response ratio is analyzed from the Cabinet Seismic Resistance Test. The input acceleration for the Cabinet Seismic Resistance Test is multiplied by the maximum response ratio, and additional margin is added to the worst case input acceleration for the chassis.

A chassis loaded with the MELTAC modules is vibration-excited with this worst case input acceleration. During and after this testing, the physical integrity and correct functional operation of the modules are confirmed.

The seismic testing methods for the MELTAC platform comply with RG 1.100, which endorses IEEE 344-2004.

5.2.2 Seismic Resistance Test

5.2.2.1 Cabinet Seismic Resistance Test

For the Cabinet Seismic Resistance Test, a specimen that simulates a fully loaded safety protection system cabinet is prepared. The loading configuration represents the worst case

expected stress on internal mounting hardware. The MELTAC modules for the Cabinet Seismic Resistance Test are shown in Appendix A.
For module types with similar circuit electronics whose differences will have no impact on environmental test results, such as NO vs. NC contacts or differences in input ranges, one typical module type is selected.

[

]

[

]

5.2.2.2 Module Seismic Resistance Test

For the Module Seismic Resistance Test, physical and functional integrity are confirmed by testing individual modules or chassis loaded with multiple modules. The MELTAC modules for the Module Seismic Resistance Test are shown in Appendix A.
For module types whose differences will have no impact on environmental test results, such as NO vs. NC contacts or differences in input ranges, one typical module type is selected.

[

]

5.3 Electromagnetic Compatibility and Radio Frequency Interference Qualification Testing

The EMI/RFI emission and susceptibility tests are performed for the MELTAC platform based on the methods and acceptance criteria of RG 1.180. The EMC qualification to RG 1.180 is confirmed for the MELTAC platform. The tests are performed with a MELTAC cabinet fully equipped with a typical configuration of the MELTAC components required for the safety protection system.
[

]
The specific test methods used for the EMI/RFI emission and susceptibility tests are described below as specified by MIL-STD-461E.

- Conducted emissions, low frequency, 120 Hz to 10 kHz (CE101)
- Conducted emissions, high frequency, 10 kHz to 2 MHz (CE102)
- Radiated emissions, magnetic field, 30 Hz to 100 kHz (RE101)
- Radiate emissions, electric field, 2 MHz to 1 GHz, 1 GHz to 10 GHz (RE102)
- Conducted susceptibility, low frequency, 120 Hz to 150 kHz (CS101)
- Conducted susceptibility, high frequency, 10 kHz to 30 MHz (CS114)
- Conducted susceptibility, bulk cable injection, impulse excitation (CS115)
- Conducted susceptibility, damped sinusoidal transients, 10 kHz to 100 MHz (CS116)
- Radiated susceptibility, electric field, 30 MHz to 1 GHz, 1 GHz to 10 GHz (RS103)

For the Power Line Surge Withstand Capability Test, the following tests are performed with the same configuration as that for the EMI/RFI Test. The specific test methods used for these tests are described below as specified by IEC 61000-4.

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

An Oscillatory Wave Test related to surge withstand capability is performed based on IEEE Std. 472 for the MELTAC modules. The following test parameters are applied: a frequency range of 1 MHz, first peak voltage range of more than 2.5 kV and repetitive rate of more than 50 tests per second for a period of more than 2 seconds.

For all Susceptibility and Surge Withstand Capability Tests the following acceptance criteria are applied:

- There is no equipment damage
- Processors continue to function
- Data communications are not disrupted
- Discrete I/O does not change state
- Analog I/O levels do not vary by more than 3%
- There is no VDU image disturbance

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

The occurrences of any system function abnormality, data communication abnormality, and equipment failure are confirmed by referring to the results of the self-diagnosis function of the MELTAC platform. It is verified that the self-diagnosis function is still operating at the end of the test.

Sections 5.3.1and 5.3.2 describe the test configuration, the test method, and acceptance criteria.

5.3.1 Test Configuration

The EUT is comprised of 2 cabinets: the CPU cabinet fitted with the CPU Chassis, E/O Converter Chassis, Optical Switch and Power Supply Modules, and the I/O cabinet fitted with the I/O Chassis, Power Interface Chassis, Isolation Chassis and Power Supply Modules. In order to attain the cabinet layout similar to the actual cabinet layout, the 2 cabinets are placed side by side with no space in between, thus acquiring the integral configuration. The cabinets are tested with the doors open to duplicate worst case conditions expected during testing and maintenance. The EUT also includes the safety VDU panel that is placed separately from the 2 cabinets.
The power to the safety VDU panel is supplied from the CPU cabinet and connected with the power cable and the signal cable. The EUT includes the module types required for safety protection system applications, as shown in Appendix A.

For module types whose differences will have no impact on EMC test results, such as NO vs. NC contacts or differences in input ranges, one typical module type is selected.
The AC power to the EUT is supplied from 2 systems: main and standby. Since both power sources with the EUT have the same configuration, the tests for AC input power line of CE102, CS101, CS114 and IEC 61000-4 are performed for one AC power cable.

5.3.2 Description of Tests

5.3.2.1 Conducted Emissions, Low Frequency (CE101) Test

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

a) Method
The conducted emissions from the input power lead cable of the EUT are measured to confirm that the electromagnetic conducted emissions from the EUT do not exceed the specified value.

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

[

]

5.3.2.2 Conducted Emissions, High Frequency (CE102) Test

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

a) Method
The conducted emissions from the input power lead cable of the EUT are measured to confirm that the electromagnetic conducted emissions from the EUT do not exceed the specified value.

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

[

]

5.3.2.3 Radiated Emissions, Magnetic Field (RE101) Test

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

a) Method
A loop sensor is placed on the surface of the object EUT to measure and confirm that the

magnetic field radiated emissions from the EUT do not exceed the specified value.

b) Test Subject
The test subjects are the EUT enclosure, the electrical cable interface and the safety VDU panel. The 4 surfaces are scanned for 360 degrees with the loop sensor positioned at the center of the location (height) where the module is mounted.

[

]

5.3.2.4 Radiated Emissions, Electric Field (RE102) Test

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

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

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

[

]

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

According to Section 4 of RG 1.180, the CS101 test is mentioned as the MIL-STD-461E test method that can be applied for testing the conducted EMI/RFI susceptibility of power leads. This test method is not applied to the signal lead.

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

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

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

[

]

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

The CS114 test is applicable to all interconnecting leads including the power leads of the EUT. This section describes the CS114 test that is applied to the power and control lines described in Section 4.1.2 of RG 1.180.
The test is performed according to the method set forth in MIL-STD-461E, as follows:

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

b) Test Subject
One each of the AC input power cables and the control cables (input and output cables of the Digital I/O Modules and Power Interface Module) to the EUT.

[

]

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

The CS114 test is applicable to all interconnecting leads including the power leads of the EUT. This section describes the CS114 test that is applied to the signal line described in Section 4.2 of RG 1.180.

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

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

b) Test Subject
One of each of the signal cables (input and output cables of the Analog I/O Modules, the Isolation Modules and the RGB cables) to the EUT.

[

]

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

According to Section 4.2 of RG 1.180, the CS115 test is mentioned as the MIL-STD-461E test method that can be applied as the conducted EMI/RFI susceptibility test along the signal leads. This test method is not applied to the power lead.

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

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

b) Test Subject
One of each of the signal cables (input and output cables of the Analog I/O Modules, the Digital I/O Modules, the PIF Module, the Isolation Modules and the RGB cables) to the EUT.

[

]

5.3.2.9 Conducted Susceptibility, Damped Sinusoidal Transients (CS116) Test

According to Section 4.2 of RG 1.180, the CS116 test is stated as the MIL-STD-461E test method that can be applied as the conducted EMI/RFI susceptibility test along the signal cables. This test method is not applied to the power lead.

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

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

b) Test Subject
One each of the signal cables (input and output cables of the Analog I/O Modules, the Digital I/O Modules, the PIF Module, the Isolation Modules and the RGB cables) to the EUT.

[

]

5.3.2.10 Radiated Susceptibility, Electric Field (RS103) Test

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

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

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

The EUT enclosure is placed above the floor as in actual plant conditions to make its height 7.55 ft (2300 mm). Then the emission of the radiated electric field to the EUT enclosure comes from 4 horizontal directions because the top and the bottom parts are not likely to be affected by the electric field.

[

]

5.3.2.11 Surge Withstand Capability, Ring Wave Test

The test is performed according to the method set forth in IEC 61000-4-12 as follows. For the withstand voltage of the test, the B Medium Exposure is selected out of the location categories described in IEEE Std. C62.41-1991 (RG 1.180 Table 22), and the corresponding surge voltage level is applied.

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

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

[

]

5.3.2.12 Surge Withstand Capability, Combination Wave Test

The test is performed according to the method set forth in IEC 61000-4-5 as follows. For the withstand voltage of the test, the B Medium Exposure is selected out of the location categories described in IEEE Std. C62.41-1991 (RG 1.180 Table 22), and the according surge level is applied.

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

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

]

5.3.2.13 Surge Withstand Capability, Electrically Fast Transients/bursts Test

The test is performed according to the method set forth in IEC 61000-4-4 as follows. For the withstand voltage of the test, the B Medium Exposure is selected out of the location categories described in IEEE Std. C62.41-1991 (RG 1.180 Table 22), and the corresponding surge voltage level is applied.

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

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

]

5.4 Electrostatic Discharge Qualification Testing

For the MELTAC platform, the electrostatic discharge (ESD) test is performed based on IEC 61000-4-2 with test level-2, in accordance with Annex A (maximum charge voltage is 8 kV, 15 kV). This maximum charge voltage is based on the MELTAC cabinet being installed on the floor using antistatic materials or concrete.

To avoid any special ESD maintenance precautions for US applications, an additional ESD test is also performed to level-4. This section describes the test and acceptance criteria.

The test is performed with the MELTAC cabinet fully equipped with a typical configuration of the MELTAC components required for a safety protection system.

The MELTAC modules for the ESD test are shown in Appendix A
For module types where differences will have no impact on environmental test results, such as NO vs. NC contacts or differences in input ranges, one typical module type is selected.

The following acceptance criteria are applied for equipment that can be accessed during operation:

- There is no equipment damage
- Processors continue to function
- Data communications are not disrupted
- Discrete I/O does not change state
- Analog I/O levels do not vary by more than 3%
- There is no VDU image disturbance

This is the same acceptance criteria as for the EMI/RFI susceptibility test.

For equipment that can be accessed only during maintenance, the only acceptance criterion is to ensure no equipment damage.

The ESD test is performed according to the method set forth in IEC 61000-4-2 as follows:

a) Method
Confirm that the EUT can withstand the ESD, where personnel can contact, such as the human-machine interface, during normal operation and when the equipment is out of service during maintenance.

b) Test Subject
The following equipment areas are likely to be accessible by personnel during normal operation.

- The touch panel of the safety VDU panel and the surrounding area
- The front/rear door handles of the cabinet and the surrounding area
- The switches of the Status Display Module, and the surrounding area
- The switches and fuses of the fans, and the surrounding area
- The front panel of the Power Supply Modules and Analog Output Modules

Other human-machine interface areas of the equipment are expected to be accessed only during maintenance.

[

]

5.5 Isolation Qualification Testing

[

]

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

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

[

]

6.0 QUALITY ASSURANCE AND LIFE CYCLE

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

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

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

6.1 MELTAC Platform Life Cycle Plans and Activities

This section describes key elements of the life cycle process for the basic components (software and hardware) of the MELTAC platform, based on the App.B-based QAP.

6.1.1 Overview of the MELTAC Quality Assurance Program

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

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

The SPM provides the generic plans that are followed under MELCO’s App.B-based QAP for all activities related to the basic software life cycle conducted after the MRP. The SPM complies with the guidance of BTP 7-14 “Guidance on Software Reviews for Digital Computer-

based Instrumentation and Control Systems". A summary of the basic software life cycle plans and activities is given in Table 6.1-1.

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

Table 6.1-1 MELTAC Life Cycle Plan/Activity Summary

Note:
MELTAC uses FPGAs only for dedicated functions, such as communication controllers. These FPGAs are not programmable for application dependent functions. Therefore, the same FPGAs are applied to all MELTAC applications.

Consistent with the practices defined in NUREG/CR-7006, MELCO does not view FPGA development as hardware, but rather applies a complete life cycle development process equivalent to software development, to achieve readable, traceable and verifiable FPGA components. Details are described in the SPM.

6.1.2 Secure Development Environment Management

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

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

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

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

6.1.2.1 Development/Storage Security Measures of the basic software

[

]

Figure 6.1-1 Security Measures of the Software Development/Storage Environment

[

]

Table 6.1-2 Security Measures of the Software Development/Storage Environment

[

]

6.1.2.2 Security Measures in Each Phase of Development Process

The security measures shown in Table 6.1-3 ensure that no unintended code can be introduced during the development process.

Table 6.1-3 Security Measures in the Software Development Process

6.1.2.3 Secure Development Environment Measures During System Operation

[

]

6.1.3 Operations

[

]

Table 6.1-4 Information Provided in the MELTAC Maintenance Manuals

Licensees may supplement the instructions in the MELTAC Maintenance Manuals with plant specific procedures and instructions

6.1.4 Training

MELCO supports training that assists customers in understanding the operation and proper use of the MELTAC platform.

This training is comprised of lecture classes and hands-on training using actual MELTAC equipment. The typical training course contents are shown below:

[

]
Additional application specific training is described in application specific documentation.

6.1.5 Maintenance

6.1.5.1 Hardware

The following hardware measurements and adjustments (as needed) are recommended on a periodic basis, once every operating cycle or every 24 months, whichever is shorted.

Table 6.1-5 Hardware Maintenance

6.1.5.2 Software

This section describes the upgrade process for the basic software. Upgrades or changes to application software are described in application level documentation

Table 6.1-6 Software Maintenance

6.1.6 Obsolescence Management

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

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

6.1.6.1 Obtaining Information on Part Availability

[

]

6.1.6.2 Selecting Replacement Parts

[

]

6.1.6.3 Verification after Replacement

[

]

6.1.7 Identification

[

]

6.1.8 Reliability Database

[

]

6.2 MELTAC Re-evaluation Program (MRP)

[

]

6.3 MELTAC Engineering Tool Life Cycle

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

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

7.0 EQUIPMENT RELIABILITY

The following sections describe methods and conditions to assess the reliability of each MELTAC module, which are required to assess the reliability of any safety-related system where MELTAC platform is applied.

Mean Time Between Failures (MTBF) values and failure rates of MELTAC modules are also described in the following sections (see Table 7.1-1). These values are more conservative than the actual failure records in Japanese nuclear plants. An example is shown below.

Regarding the CPU Module and peripheral modules, a typical subsystem failure rate, which is composed of many modules, is more than 15,000 Failure In Time (FIT) based on Table 7.1-1 . However, the FIT for similar configuration of safety-related controllers and safety VDUs in Japanese nuclear plants is about 100. The calculated result predicts that a failure should occur at least once a month. However, the operating subsystems have failed less than once a year.

7.1 Mean Time between Failures (MTBF) Analysis

MTBF shown in Table 7.1-1 is calculated for each MELTAC module based on MIL-HDBK-217F NOTICE 2. These values are used to assess the reliability of the entire MELTAC platform for each system, as explained in Section 7.2.

MTBF is calculated from the sum of the failure rates of the components which make up each module, and the reciprocal of the module's failure rate is thus obtained. In MIL-HDBK-217F, the failure rate is defined for each type of component with consideration given to operating conditions and reliability factors. Therefore, it represents a generic reliability assessment technique. The following environmental conditions were used in the calculation.
[

]
The MTBF of each module is shown Table 7.1-1.
Table 7.1-1 provides the calculated FIT and MTBF for each MELTAC module. If a module is updated, the FIT and MTBF will be calculated using the same method and reliability will be demonstrated. The same method of calculating the FIT and MTBF will also be used for any new modules. The impact on the reliability of the entire controller due to the introduction of any new modules is evaluated as describe in Section 7.2.

Table 7.1-1 Failure Rate of Modules

Note:
FIT (Failure In Time) rate is used to indicate the failure rate. 1 FIT = $1X10^{-9}$(/hour).

7.2 Controller Reliability Analysis

The failure rate of any safety-related system where MELTAC platform is applied as a whole, depends on the configuration of the entire system. Variations for each application include:

- The number and configuration of redundant divisions
- The number and configuration of controllers within each division
- The redundancy within each controller
- The configuration of I/O modules and Communication Interface Modules and the significance of these interfaces to the safety function (i.e.: the safety function logic design)

This section describes a method used to determine the reliability of a generic redundant parallel controller. The method for single controller architecture can be extrapolated from this method.

The controller reliability analysis is performed as follows.

- A reliability model for the system's safety function is generated
- The fault tree analysis (FTA) of this reliability model is performed to determine the frequency of:
  - Spurious actuation of the safety function
  - Failure to actuate the safety function

The reliability model of a simple system is shown in Section 7.2.1. As an example of the reliability analysis process, Figure 7.2-2 shows the fault tree for spurious actuation of the safety function. The FTA for spurious actuation is explained below.

7.2.1 Reliability Model

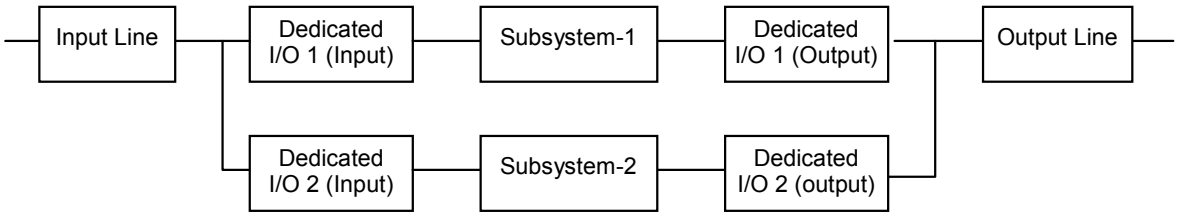


Figure 7.2-1 Reliability Model

The above figure shows the reliability model of a redundant parallel controller, which contains one input module and one output module in each subsystem.
In the reliability model, the Status Display Module is not contained in the subsystem, because the Status Display Module only displays the current state of the subsystem and its failure does not affect the safety function of the subsystem. The Control Network I/F Module and the Optical Switch Module are not contained in this simplified system. They would be included, depending on how the data from the Control Network is used in the application software. This also applies to the Data Link interface from the Bus Master Modules.

7.2.2 FTA of Spurious Actuation of the Safety Function

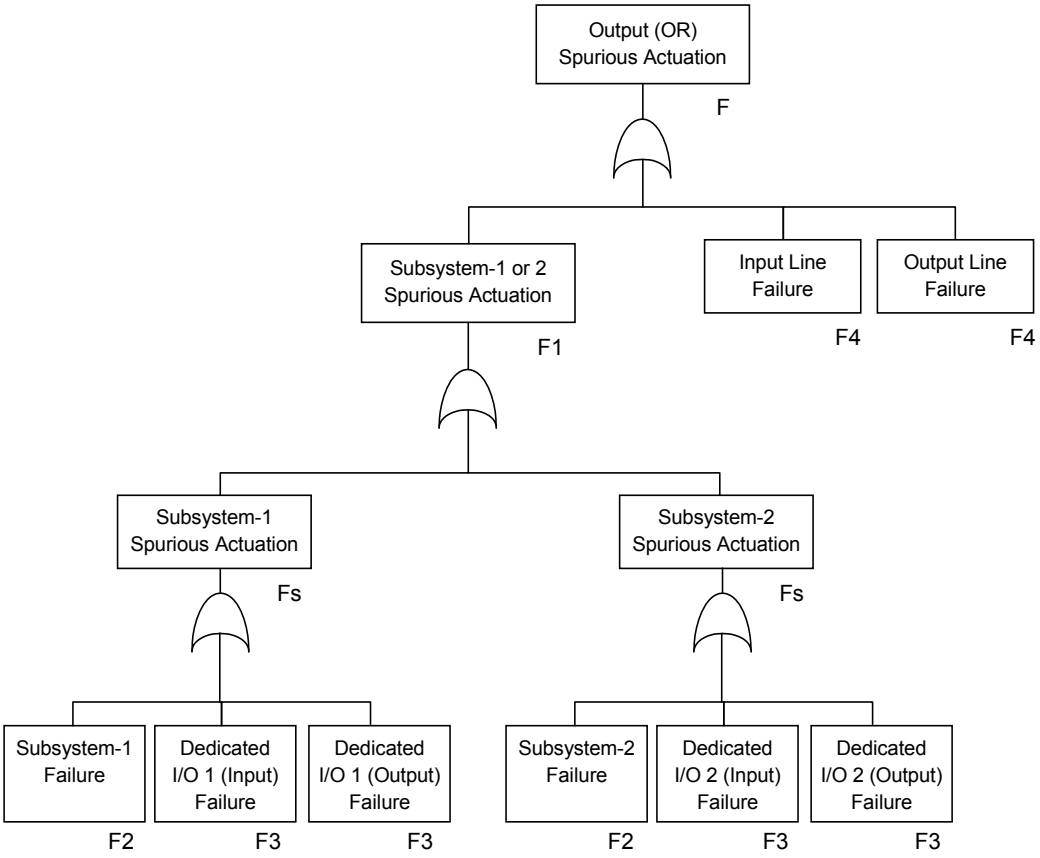


Figure 7.2-2 Fault Tree for Output Failure Spurious Actuation

Regarding the cause of spurious actuation, the failure rate is described below.

F = F1 + F4 + F4
F1 = Fs + Fs
Fs = F2 + F3 + F3

Failure rate Fi (i = 1,2,3⋯) causes spurious action of each module or subsystem and is defined below.

Fi = λ i x (1-Pi)
λ i = failure rate
Pi = probability of detecting the failure which affects the safety function through self-diagnosis

Calculations of F2, F3 and F4 are described in Sections 7.2.4.1, 7.2.4.2 and 7.2.4.3.
The failure rates of the Input Line and the Output Line are the same, because they consist of the same module and unit.

This FTA model assumes this very simple system, in which an input directly affects a system output. Systems with more complex logic may validate inputs (e.g.: voting) within the application logic so that spurious actuation requires multiple input failures.

7.2.3 FTA of Failure to Actuate the Safety Function

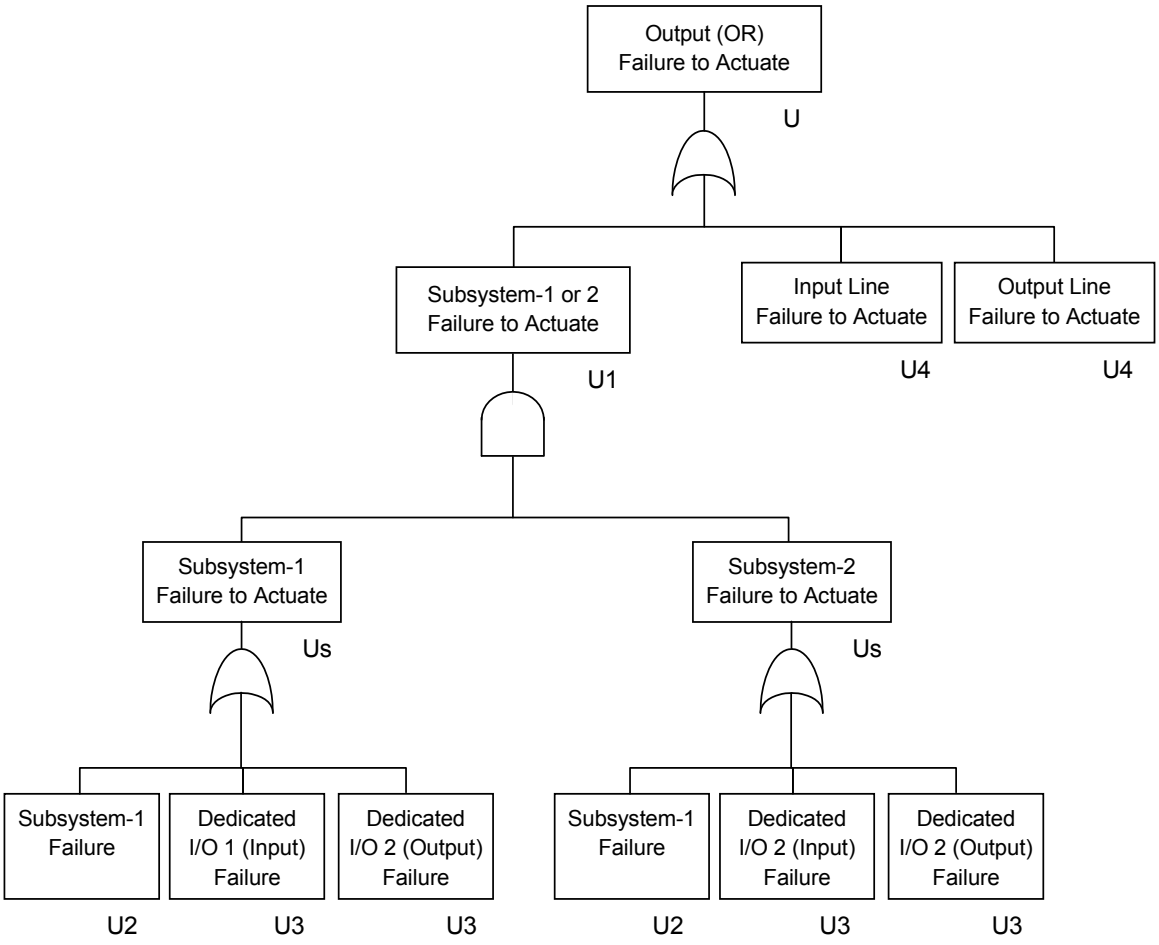


Figure 7.2-3 Fault Tree for Failure to Actuate

Regarding the cause of failure to actuate, unavailability is described below.

U = U1 + U4 + U4
U1 = Us x Us
Us = U2 + U3 + U3

Ui is the unavailability of each module or subsystem and is defined below.

Ui = 1 - MTBF / (MTBF + (1 - Pi) x (Ti /2) + MTTR)
Ti = Manual test interval
MTBF = 1 / λ i

Ti and Mean Time To Repair (MTTR) are unique to each application.

7.2.4 Detailed Controller Reliability Analysis

7.2.4.1 Subsystem

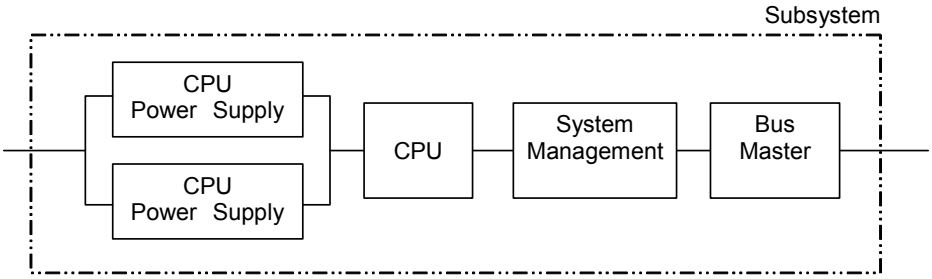


Figure 7.2-4 Reliability Model of Subsystem

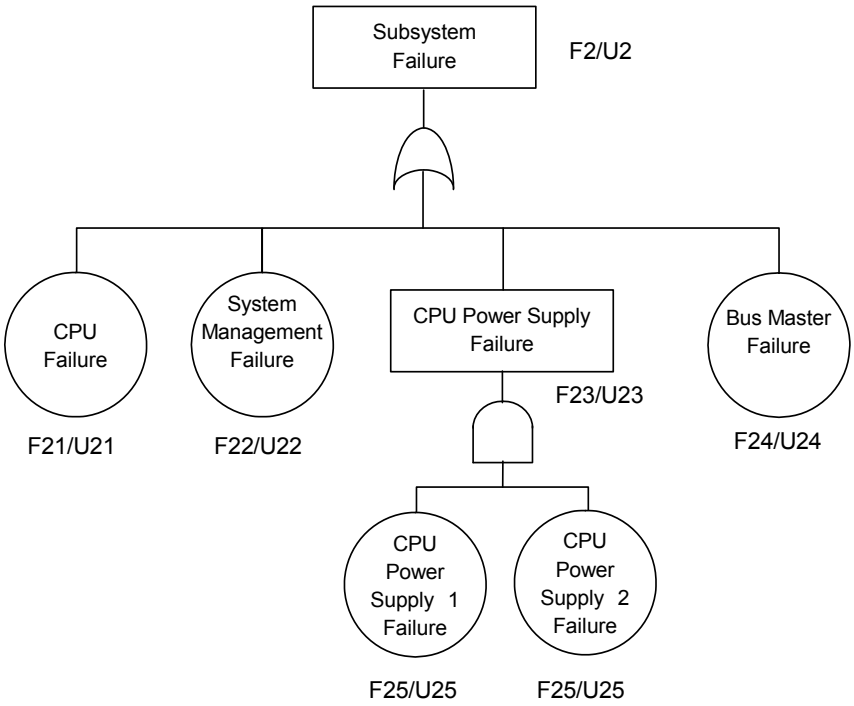


Figure 7.2-5 Fault Tree of Subsystem

The failure rate of the subsystem (F2) is defined as follows.

F2 = F21 + F22 + F23 + F24
F23 = F25 x F25 x MTTR x 2

The unavailability of subsystem (U2) is defined as follows.

U2 = U21 + U22 + U23 +U24
U23 = U25 x U25

7.2.4.2 Dedicated I/O (Input/Output)

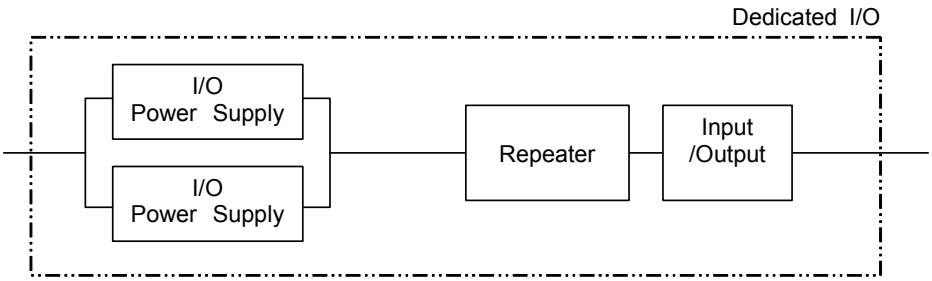


Figure 7.2-6 Reliability Model of Dedicated I/O

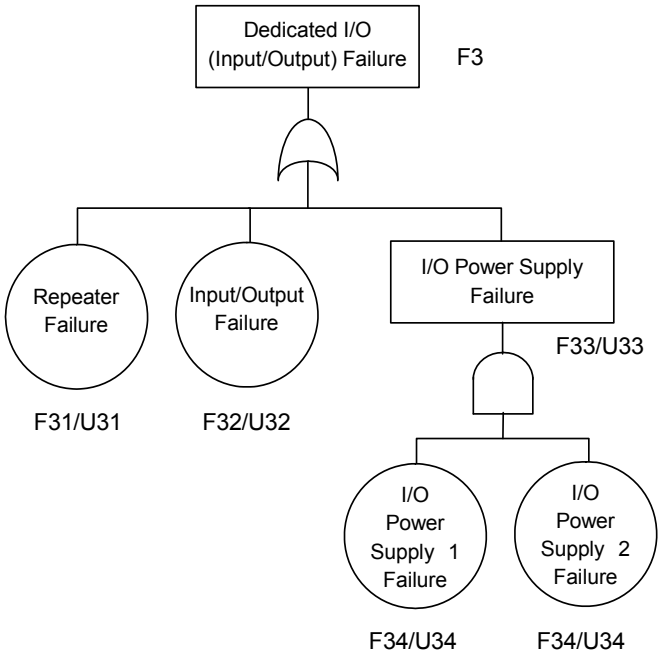


Figure 7.2-7 Fault Tree of Dedicated I/O

The failure rate of the subsystem (F3) is defined as follows.

F3 = F31 + F32 + F33
F33 = F34 x F34 x MTTR x 2

The unavailability of the subsystem (U3) is defined as follows.

U3 = U31 + U32 + U33
U33 = U34 x U34

7.2.4.3 Input/Output Line

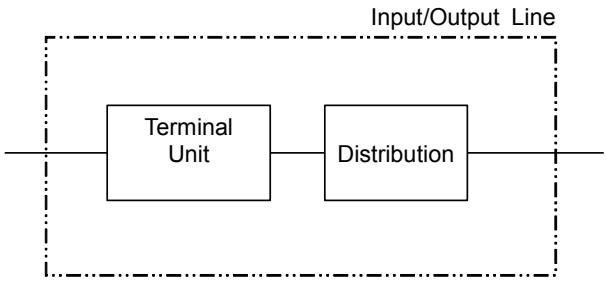


Figure 7.2-8 Input/Output Line

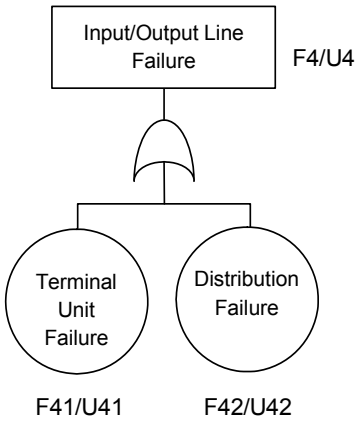


Figure 7.2-9 Fault Tree of Input/Output Line

The failure rate of the subsystem (F4) is defined as follows.

$$F4 = F41 + F42$$

The unavailability of the subsystem (U4) is defined as follows.

$$U4 = U41 + U42$$

7.3 Failure Mode and Effect Analysis (FMEA)

This section describes the process of conducting the FMEA, which is a method of determining the failure mode for each type of MELTAC module and the resulting effects to the controller.

The steps for conducting the FMEA are as follows:

- Divide module circuits into function blocks
- Determine failure modes of the function blocks
- Determine the state(s) of the module output(s) caused by the failure mode(s) of the function blocks
- Determine the effects to the controller based on the states of the module output failures

For a module acceptable for use in the CPU Chassis, failures in the function blocks that may affect the control function must be detected either by the self-diagnosis function inside the module or through a combination of modules.

Parts which do not affect the safety function, such as the RS-232C communication port which is used only for CPU Module debugging, are identified through the FMEA.

For a module acceptable for use in the I/O Chassis, failures in the parts that may affect the control function must be detected either by the self-diagnosis function of the CPU Module or by the application software. For instance, if the Relay Output Module's relay contact suffers a seizure failure, it cannot be detected by the self-diagnosis function of the controller. However, this failure can be detected by the application software when the component is actuated either automatically or manually.

The FMEA method and acceptance criteria described in this section apply to all MELTAC modules.

7.4 Equipment (Parts) that Require Periodic Replacement to Maintain Reliability

The failure rates of each MELTAC module are shown in Section 7.1 (see Table 7.1-1). However, the following 3 components of the MELTAC modules have limited service life and need to be replaced periodically to maintain the reliability of MELTAC.

a) Capacitor within power supplies
b) Fan fuses
c) Liquid crystal display within safety VDU panel

For item a), the entire power supply module need to be replaced. For item b), the fuses inside the Fan Unit need to be replaced but it is not necessary replace the entire Fan Unit. For item c), the entire safety VDU panel needs to be replaced. Parts may be replaced at any time while the equipment is energized or de-energized. Restrictions on on-line replacement are governed only by specific plant applications.

The parts that require periodic replacement are listed in Table 7.4-1.
When components are updated or new components are added, the requirements for periodic parts replacement will be re-evaluated.

Table 7.4-1 List of Parts that Require Periodic Replacement

For the power supplies, the estimated service life of the internal electrolytic capacitor is calculated based on the Arrhenius equation. For fuses used in the fan assemblies, the estimated service life is determined based on the condition under which the fuses are actually used.
The replacement intervals for the components listed above are determined based on the estimated life of subparts. The estimated life of the subparts is shorter than the life that is provided in the catalog, in order to reinforce the reliability of the safety-related system where MELTAC platform is applied.

The components listed above have failure mechanisms related to aging. However, these aging mechanisms do not significantly affect the equipment's susceptibility to failure during the equipment qualification tests described in Section 5. Therefore, there is no age-related preconditioning prior to the qualification tests.

Other components used in the MELTAC platform do not have any known age-related failure mechanisms. Therefore, replacement only takes place when a failure occurs.

APPENDIX A HARDWARE SPECIFICATION

The modules described here are used for safety systems.
Module types and specifications in this appendix represent current MELTAC modules at the time of this document revision. Module types and specifications will change as the product life cycle progresses. New modules will retain the functional features, performance specifications and reliability of current modules.

A.1 CPU Module Specification

Table A.1 CPU Module Specification

Item	Specification
Module Type	PCPJ
Memory	DDR-SDRAM: 128 Mbytes SRAM: 512 kbytes F-ROM for application software: 64 Mbytes F-ROM for basic software: 32 Mbytes
External dimensions	11.4×10.4×0.98 inch (290×265×25 mm)
Hot-swapping	Power supply must be disabled when unplugging the module.

A.2 System Management Module Specification

Table A.2 System Management Module Specification

Item	Specification
Module Type	PSMJ
Communication between redundant subsystems	Optical module transmission speed: 100 Mbps
System DI	Number of inputs: 32 Rated voltage: 24 V (30 V, maximum) external supply Contact current: 3 mA Dielectric voltage: AC 500 V
System DO	Number of outputs: 8 Rated voltage: 24 V (30 V, maximum) external supply Rated current: 50 mA (100 mA, maximum) Dielectric voltage: AC 500 V
Onboard memory	2-port memory: 1 Mbyte Dedicated transmission memory: 1 Mbyte Dedicated receiving memory: 1 Mbyte DDR-SDRAM: 128 Mbytes F-ROM for Firmware: 32 Mbytes
Firmware	Firmware is mounted on the F-ROM. It executes Maintenance Network communication function.
Ethernet Interface	Module Chassis, rear side: 10 Mbps, 1ch Module front side: 100 Mbps/10 Mbps (Speed: Automatically switched), 2 channels (UTP cable) Module front side: 100 Mbps, 1 channel (optical fiber)
External dimension	11.4×10.4×0.79 inch (290×265×20 mm)
Hot-swapping	Power supply must be disabled when unplugging the module.

A.3 Bus Master Module Specification

Table A.3 Bus Master Module Specification

Item	Specification
Module Type	PFBJ
Protocol	1:N master polling (Case of Communication with I/O) One way communication (Case of Data Link communication)
Configuration	Number of channels: 4 channels/module (I/O or serial Data Link communication can be defined for each channel.)
Interface	RS-485 transformer insulation.
Baud rate	1 Mbps
Error detection	CRC method
Transmission capacity	1 kbyte/channel, maximum (Case of Communication with I/O) 3 kbyte/channel, maximum (Case of Data Link communication)
Onboard memory	Dedicated transmission memory: 1 Mbyte (256 kbyte/channel)
External dimension	11.4 x10.4 x1.18 inch (290x265x30 mm)
Hot-swapping	Power supply must be disabled when unplugging the module.

A.4 Control Network I/F Module Specification

Table A.4 Control Network I/F Module Specification

Item	Specification
Module Type	PWNJ
Protocol	Communication method: Cyclic Multiplexing method: RPR (Resilient Packet Ring) IEEE Std. 802.17
Configuration	Loop (redundant)
Medium	Optical fiber
Speed	Transmission rate: 1 Gbps
Capacity	Transmission capacity: - 256 kbytes, maximum for normal speed communication - 128 kbytes, maximum for high speed communication Number of connected stations: - 126 stations, maximum for normal speed communication - 32 stations, maximum for high speed communication Distance between stations: - 2 km, maximum
Firmware	Firmware is mounted on the F-ROM. It executes Control Network communication function.
External dimension	11.4 x10.4 x1.18 inch (290×265×30 mm)
Error detection	CRC method
Hot-swapping	Power supply must be disabled when unplugging the module.

A.5 I/O Module Specification

Table A.5 Analog Input Module Specification

Module Type	Description	Specification
MLPJ	Current input	AI: 1 input/module 4 to 20 mA (Transmitter power supply is provided.) Input impedance: 10 MΩ or greater Accuracy*: ±0.25 %FS Temperature coefficient: ±50 ppm/°C Firmware: mounted on the F-ROM.
MAIJ	Voltage input	AI: 1 input/module 0 to 10 V Input impedance: 10 MΩ or greater Accuracy*: ±0.25 %FS Temperature coefficient: ±50 ppm/°C Firmware: same as MLPJ
MRTJ	RTD 4 line type	AI: 1 input/module 4-line Pt200 Ω, 32 to 752 °F (0 to 400 °C) Input impedance: 10 MΩ or greater Accuracy*: ±0.25 %FS Temperature coefficient: ±50 ppm/°C Firmware: same as MLPJ
		AI: 1 input/module 4-line Pt200 Ω, 500 to 662 °F (260 to 350 °C) Input impedance: 10 MΩ or greater Accuracy*: ±0.25 %FS Temperature coefficient: ±50 ppm/°C Firmware: same as MLPJ

Table A.5 Analog Input Module Specification

Module Type	Description	Specification
MRTJ	RTD 4 line type	AI: 1 input/module 4-line Pt100 Ω, 32 to 212 °F (0 to 100 °C) Input impedance: 10 MΩ or greater Accuracy*: ±0.25 %FS Temperature coefficient: ±50 ppm/°C Firmware: same as MLPJ
		AI: 1 input/module 4-line Pt100 Ω, 32 to 392 °F (0 to 200 °C) Input impedance: 10 MΩ or greater Accuracy*: ±0.25 %FS Temperature coefficient: ±50 ppm/°C Firmware: same as MLPJ
MTCJ	Thermocouple K type	AI: 1 input/module 32 to 2372 °F (0 to 1300 °C) Input impedance: 10 MΩ or greater Accuracy*: ±0.5 %FS Temperature coefficient: ±350 ppm/°C Firmware: same as MLPJ
		AI: 1 input/module 32 to 752 °F (0 to 400 °C) Input impedance: 10 MΩ or greater Accuracy*: ±0.25 %FS Temperature coefficient: ±350 ppm/°C Firmware: same as MLPJ

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

Table A.6 Analog Output Module Specification

Module Type	Description	Specification
MAOJ	Current output	AO: 1 output/module Maximum load: 600 Ω Accuracy: ±0.25 %FS Firmware: mounted on the F-ROM.
MVOJ	Voltage output	AO: 1 output/module Minimum load: 500 Ω Accuracy: ±0.25 %FS Firmware: same as MAOJ

Table A.7 Digital Input Module Specification

Module Type	Description	Specification
MDIJ	Contact input (built-in contact power supply)	DI: 4 inputs/module Contact impressed voltage: DC 48 V Contact current: 10 mA

Table A.8 Digital Output Module Specification

Module Type	Description	Specification
MDOJ	Relay contact output	DO: 4 outputs/module, normally open contact Rated load (resistive load) : AC 220 V 0.5 A, AC 110 V 0.5 A DC 110 V 0.1 A, DC 125 V 0.1 A
	Semiconductor output (open collector)	DO: 2 outputs/module (power DO) Maximum impressed voltage: AC110 V/DC125 V Output current: 1 A (continuous) 6 A (100 ms) 10 A (20 ms)

Table A.9 Pulse Input Module Specification

Module Type	Description	Specification
MPIJ	Pulse input (for RCP rotation speed input)	Input: 1 input/module Pulse amplitude: ±0.5 to ±60 V Measurement range: 100 to 1500 rpm

A.6 Isolation Module and Distribution Module Specification

Table A.10 Isolation Module Specification

Module Type	Description	Specification
KILJ	Current input, Current/Voltage output	AI: 1 input/module 4 to 20 mA Input impedance: 10 MΩ or greater Accuracy: ±0.5 %FS Temperature coefficient: ±100 ppm/°C AO: 1 output/module 4 to 20 mA / DC 0 to 10 V (selectable)
KIRJ	RTD 4 line type input Current/Voltage output	AI: 1 input/module 4-line Pt100 Ω, 32 to 302 °F (0 to 150 °C) 4-line Pt100 Ω, 32 to 392 °F (0 to 200 °C) 4-line Pt200 Ω, 32 to 752 °F (0 to 400 °C) Input impedance: 10 MΩ or greater Accuracy: ±0.5 %FS Temperature coefficient: ±100 ppm/°C AO: 1output/module 4 to 20 mA / DC 0 to 10 V (selectable)
KIPJ	Pulse signal input (for RCP)	Input: 1 (Pulse signal) Output: 2 (Pulse signal) Output pulse width: about 10 ms Output voltage:10 V±1 V or output of open collector

Table A.11 Distribution Module Specification

Module Type	Description	Applicable I/O Modules
KIOJ	For Digital I/O	MDIJ MDOJ
KLPJ	For Current input (Active)	MLPJ
	For Current input (Passive)	MLPJ
KRTJ	For RTD input (4 wire)	MRTJ
KTCJ	For Thermocouple input	MTCJ
KAIJ	For Voltage input	MAIJ
KAOJ	For Current output	MAOJ
KVOJ	For Voltage output	MVOJ
KAIJ	For Pulse signal input (for RCP)	MPIJ

A.7 E/O Converter Module Specification

Table A.12 E/O Converter Module and Device Specification

Module Type	Description	Specification
MEOJ	Electrical/Optical conversion	Electrical to Optical: 1 channel Optical to Electrical: 1 channel Electrical interface: RS-485 Optical signal: Multi mode optical fiber
		Electrical to Optical: 1 channel Optical to Electrical: 1 channel Electrical interface: RS-232C Optical signal: Multi mode optical fiber

A.8 Power Interface Module Specification

Table A.13 Power Interface Module Specification

Module Type	Description	Specification
DPOJ	Semiconductor output (open collector) Contact input (built-in contact power supply)	DO: 2 outputs/module (power DO) Rated voltage: AC 120 V/DC 125 V Output current: DC 1.5 A (continuous) AC 2.0 A_{rms} (continuous) 16 A_{0-P} (100 ms) 2.5 A_{0-P} (1 s) DI: 8 inputs/module Contact impressed voltage: DC 48 V Contact current: 10 mA

A.9 Power Supply Module Specification

Table A.14 Power Supply Module Specification

Module Type	Description	Specification
PS	CPU Power Supply	Input voltage: AC 85 to 140 V Frequency: 47 Hz to 63 Hz Output voltage: DC 5 V (50 A), DC 2.1 V (11 A)
	I/O Power Supply	Input voltage: AC 85 to 140 V Frequency: 47 Hz to 63 Hz Output voltage: DC 24 V (12 A)
PPSJ	CPU Power Supply (Small capacity type)	Input voltage: AC 85 to 140 V Frequency: 47 Hz to 63 Hz Output voltage: DC 5 V (30A), DC 2.1 V (11 A) Mounted inside Mirror-split Chassis
	CPU Power Supply (Large capacity type)	Input voltage: AC 85 to 140 V Frequency: 47 to 63 Hz Output voltage: DC 5 V (60 A), DC 2.1 V (11 A) Mounted inside Non-split CPU Chassis

A.10 Safety VDU Panel Specification

Table A.15 Safety VDU Panel Specification

Item	Specification
Module Type	T10DH
Type	Thin Film Transistor Liquid Crystal Display (TFT LCD) module
Operator Interface	Touch interface (non-pressure-sensitive type)
Communication Interface	- Safety VDU processor to panel Display signal : RGB, Horizontal Sync (HSYNC), Vertical Sync (VSYNC) - Safety VDU panel to processor RS-232C electrical or optical fiber with E/O,O/E converters

A.11 FMU Module Specification

Table A.16 FMU Module Specification

Item		Specification
Module Type		PFDJ
Graphic	Picture Size	SVGA (800*600) (Case of Analog signal)
	Interface	D-SUB type (Case of Analog signal) DVI type (Case of Digital signal)
	Memory	64 Mbytes
Touch Panel Interface	Configuration	1:1 serial interface
	Interface	RS-232C (With optical conversion function, Transmission distance: Less than 2 km)
	Baud rate	76.8 kbps, maximum
	Capacity	Transmission capacity : 2 kbytes (Number of channels : 1)
Hot-swapping		Power supply must be disabled when unplugging the module.

A.12 NI Module Specification

Table A.17 NI Module Specification

Module Type	Description	Specification
NFAN	Pre Amplifier	Input: Current pulse signal (1 input/module) Pulse amplitude: 40 dB Output: Voltage pulse signal (1 output/module) For SR[*1] Unit outside of NI cabinet
		Input: Current pulse signal (1 input/module) Pulse amplitude: 40 dB Output: Voltage pulse signal (1 output/module) For WR[*4] Unit outside of NI cabinet
NHBN	Pulse Amplifier	Input: Voltage pulse signal (1 input/module) Pulse amplitude: 40 dB Output: Voltage pulse signal (1 output/module) For SR[*1]
		Input: Voltage pulse signal (1 input/module) Pulse amplitude: 40 dB Output: Voltage pulse signal (1 output/module) For WR[*4]
NHCN	Discrimination	Input: Voltage pulse signal (1 input/module) Discrimination level: Settable within the range of DC 0 to 5 V Output: Voltage pulse signal (1 output/module), DC 10^{-10} to 10^{-4} A (1 output/module) For SR[*1], WR[*4]
NHDN	Logarithmic Amplifier	Input: DC 10^{-10} to 10^{-4} A (1 input/module) Output: DC 0 to 10 V (1 output/module) For SR[*1]
		Input: DC 10^{-10} to 10^{-4} A (1 input/module) Output: DC 0 to 6.667 V (1 output/module) For WR[*4]
NDAN	Signal Processing	Input: DC 0 to 10 V (1 input/module), DC 0 to 500 μA (1 input/module) Contact impressed voltage: DC 24 V (2 input/module) Communication interface: RS-485 transformer insulation (6 channels/module) Firmware: mounted on the F-ROM. It executes analog/digital conversion and communication function. For SR[*1]
		Input: DC 0 to 10 V (1 input/module), DC 0 to 500 μA (1 input/module), DC 0 to -500 μA (1 input/module) Contact impressed voltage: DC 24 V (2 inputs/module) Communication interface: RS-485 transformer insulation (6 channels/module) Firmware: mounted on the F-ROM. It executes analog/digital conversion and communication function. For IR[*2]

Table A.17 NI Module Specification

Module Type	Description	Specification
NDAN	Signal Processing	Input: DC 0 to 10 V (2 inputs/module), DC 0 to 500 μA (1 input/module) Contact impressed voltage: DC 24 V (2 inputs/module) Communication interface: RS-485 transformer insulation (6 channels/module) Firmware: mounted on the F-ROM. It executes analog/digital conversion and communication function. For PR[*3]
NDCN	Operation Panel	Communication interface: RS-485 transformer insulation (1 channel/module) Output: DC 0 to -12 V (for Log Amp test signal), DC 0/24 V (for Pre Amp test and Pulse Amp test signal) For SR[*1]
		Communication interface: RS-485 transformer insulation (1 channel/module) Output: DC 0 to 24 V (for Log Amp test signal, 8 outputs/module), DC 0/24 V (for test signal range select, 5 outputs/module) For IR[*2]
		Communication interface: RS-485 transformer insulation (1 channel/module) Output: DC 1 to 5 V (for I/E Converter test signal, 2 outputs/module), DC 0/24 V (for test signal range select, 16 outputs/module) For PR[*3]
NHEN	High Voltage Cut Off Circuit Card	Contact impressed voltage: DC 24 V (4 inputs/module) Input voltage: AC 103.5 to 126.5 V Output voltage: AC 103.5 to 126.5 V For SR[*1]
NFTN	Test Signal Generator	Input: DC 0/24 V (4 inputs/module) Output: Voltage pulse signal (Output either 60,10^3,10^5 or 10^6 cps) For SR[*1]
		Output: Voltage pulse signal (Output either 10^5, 10^7 or 10^9 cps for Campbell circuit test), Voltage pulse signal (Output either 10,10^3,10^5 or 10^6 cps for Pulse circuit test) For WR[*4]
NHFN	Logarithmic Amplifier	Input: DC 10^{-11} to 5×10^{-3} A (1 input/module) Output: DC 0 to 10 V (1 output/module) For IR[*2]
		Input: DC 10^{-7} to 10^{-3} A (1 input/module) Output: DC 5.555 to 10 V (1 output/module) For WR[*4]
NHMN	Test Signal Generator	Input: DC 0 to 24 V (for Log Amp test signal, 8 inputs/module), DC 0/24 V (for test signal range select, 5 inputs/module) Output: DC 10^{-11} to 5×10^{-3} A (1 output/module) For IR[*2]

Table A.17 NI Module Specification

Module Type	Description	Specification
NLPN	Isolation Card	Input: DC 0 to 10 V (1 input/module) Output: DC 0 to 10 V (1 output/module) For IR[*2]
NDBN	I/E Converter	Input: DC 0 to 9 mA (max) Gain: Variable Output: DC 0 to 10 V For PR[*3]
NHVN	Detector Current Indicator	Input: DC 0 to 10 V (1 input/module) Display: Display 5 digits current value For PR[*3]
	Reactor Power Level Indicator	Input: DC0 to 10 V (1 input/module) Display: Display 4 digits reactor power level value For PR[*3]
NHNN	Test Signal Generator	Input: DC 1 to 5 V (for I/E Converter test signal, 2 inputs/module), DC 0/24 V (for test signal range select, 8 inputs/module) Output: DC 0 to 10 mA, maximum (2 outputs/module) For PR[*3]
NFFN	Root Mean Square Converter	Input: Voltage pulse signal (1 input/module) Output: DC 10^{-7} to 10^{-3} A (1 output/module) For WR[*4]
NFHN	Mode Switching Card	Input: DC 0 to 6.667 V (1 input/module), DC 5.555 to 10 V (1 input/module) Output: Select one of above 2 points to output. For WR[*4]
NJAN	Power Supply for SR Detector	Input voltage: AC 103.5 to 126.5 V Frequency: 47 to 63 Hz Output voltage: DC 0 to 2500 V For SR[*1]
NJBN	Power Supply for IR Detector	Input voltage: AC 103.5 to 126.5 V Frequency: 47 to 63 Hz Output voltage: DC 0 to 1000 V For IR[*2]
	Power Supply for WR Detector	Input voltage: AC 103.5 to 126.5 V Frequency: 47 to 63 Hz Output voltage: DC 0 to 1000 V For WR[*4]
NHGN	Power Supply for IR Detector	Input voltage: AC 103.5 to 126.5 V Frequency: 47 to 63 Hz Output voltage: DC 0 to -200V For IR[*2]
NJCN	Power Supply for PR Detector	Input voltage: AC 103.5 to 126.5 V Frequency: 47 Hz to 63 Hz Output voltage: DC 0 to 1000 V For PR[*3]
501AJ0UN	Power Supply (NIS)	Input voltage: AC 103.5 to 126.5 V Frequency: 47 to 63 Hz Output voltage: DC 24.5 V (1 A)

Table A.17 NI Module Specification

Module Type	Description	Specification
NALN	Signal Comparator	Input: DC 0 to 10 V (1 input/module) Output: DC 0/24 V (1 output/module)
NHTN	Trip Bypass Switch	Operation switch: 3 switches for bypass operation Output: DC 0/24 V (Normal / Bypass) For SR[*3] and IR[*2]
NDHN	Summing Amplifier	Input: DC 0 to 6 mA (2 detector current inputs/module) DC 0 to 5 mA (2 test current signal inputs/module) Output: DC 0 to 10 V (as upper neutron flux level) DC 0 to 10 V (as lower neutron flux level) DC 0 to 10 V (as reactor power level) DC 0 to 10 V (as over power level) For PR[*3]
NHJN	Flux Level Change Rate Detection Circuit	Input: DC 0 to 10 V (as reactor power level) Output: DC -10 to +10 V (differential waveform) For PR[*3]
NHKN	Self-Holding Circuit	Operation switch: Close (for trip reset operation) Input: Open/DC 5 V (Trip signal) Close (for trip reset operation) Output: DC Over 20 V/Under 0.7 V (Normal/Holding) For PR[*3]
NBYN	Bypass Control Circuit	Input: Bypass permission Output: Bypass demand For PR[*3]
NOIN	E/O Converter	Electrical to Optical: 1 channel Optical to Electrical: 1 channel Electrical interface: RS-422 Optical signal: Multi mode optical fiber For PR[*3]

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

A.13 RM Module Specification

Table A.18 RM Module Specification

Module Type	Description	Specification
MUBN	Signal Converter (Analog)	Pulse to RS-485 converter Range: 10^7 cpm, maximum
	Signal Converter (Pulse)	RS-485 to RS-485 protocol converter
MURN2	Repeater Card	RS-485 to O/E, E/O Converter
501AJ0UR	Power Supply (RM)	Input voltage: AC 98 to 132 V Frequency: 47 to 63 Hz Output voltage: DC 12 V, DC ±15 V, DC 24 V

A.14 Status Display and Switch Module Specification

Table A.19 Status Display and Switch Module Specification

Module Type	Applicable System Configurations	Description
PPNJ	Single Redundant Parallel	Status Display: Displays the operation mode and status of representative alarm
	Redundant Standby	Status Display: Displays the operation mode of Subsystem A/ B. Displays the status of representative alarm. Subsystem Switching: Select which Subsystem, A or B, should be controlled in the Control Mode or Standby Mode.

A.15 Repeater Module Specification

Table A.20 Repeater Module Specification

Module Type	Function	Specification
MRPJ	Repeater	For Subsystem-A
	Repeater	For Subsystem-B
	Repeater	For Subsystem-A/B Double Size

A.16 Module Chassis Specification

Table A.21 CPU Module Chassis Specification

Module Type	Chassis Type	Applicable System Configuration	Number of Implementable Extension Modules *1
ZCAJS	Mirror-split	Redundant Standby	3
	Non-split	Redundant Parallel	9
		Single	9

*1 :Bus Master Module, Control Network I/F Module, FMU Module

Table A.22 I/O Module Chassis Specification

Module Type	Applicable I/O Modules	Maximum Number of Modules
ZIOJS	Digital Input Module Digital Output Module Analog Output Module Analog Input Module	16 (and 2 Repeater Modules)
ZEHJS	PIF Module	16 (and 2 Repeater Modules)
ZISJS	Isolation Module	14
ZMEJS	Optical Conversion Module	14

A.17 Other Modules Specification

Table A.23 Fan Modules Specification

Module Type	Application	Number of fans per unit	Remarks
KFNJ	CPU Fan	4	Alarm detection circuit is prepared
	PS Fan	1	Alarm detection circuit is prepared
	Door Fan	3	Alarm detection circuit is prepared

Table A.24 Terminal Unit Specification

Module Type	Application	Number of terminals	Rated Voltage	Switching Function
PSND	Analog (AI/AO)	32	AC 115 V/ DC 125 V	Test Terminal Switching Function
	Digital (DI/DO)	64	AC 115 V/ DC 125 V	Lift Function

Table A.25 Optical Switch Specification

Item	Specification
Module Type	RJMA
Power Supply	5 V± 5 %
Optical Switch ON/OFF Interface	Wire to board (4 pins) connector
Optical Fiber Interface	Interface for the Control Network I/F Module: Optical fiber cable with LC connector x 4
	Interface for the external cable: LC connector x 4

APPENDIX B FUNCTIONAL SYMBOL SOFTWARE SPECIFICATIONS

The function symbols listed below are for safety applications.

Table B.1 List of Function Symbols for Discrete Control Processes

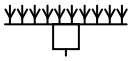
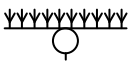
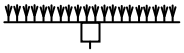
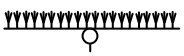
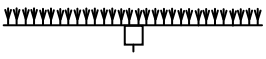
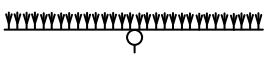
No	Symbol	Name	Function
1		AND	Defines the output signal (Y) with respect to the input signals (X_1, X_2) as follows: Y= X_1 and X_2
2		OR	Defines the output signal (Y) with respect to the input signals (X_1, X_2) as follows: Y= X_1 or X_2
3		AND3	Defines the output signal (Y) with respect to the input signals (X_1, X_2, X_3) as follows: Y= X_1 and X_2 and X_3
4		OR3	Defines the output signal (Y) with respect to the input signals (X_1, X_2, X_3) as follows: Y= X_1 or X_2 or X_3
5		AND4	Defines the output signal (Y) with respect to the input signals (X_1, X_2, X_3, X_4) as follows: Y= X_1 and X_2 and X_3 and X_4
6		OR4	Defines the output signal (Y) with respect to the input signals (X_1, X_2, X_3, X_4) as follows: Y= X_1 or X_2 or X_3 or X_4
7		AND5	Defines the output signal (Y) with respect to the input signals (X_1, X_2, X_3, X_4, X_5) as follows: Y= X_1 and X_2 and X_3 and X_4 and X_5
8		OR5	Defines the output signal (Y) with respect to the input signals (X_1, X_2, X_3, X_4, X_5) as follows: Y= X_1 or X_2 or X_3 or X_4 or X_5
9		AND10	Defines the output signal (Y) with respect to the input signals (X_1, X_2, …X_{10}) as follows: Y= X_1 and X_2 and ⋯ and X_{10}
10		OR10	Defines the output signal (Y) with respect to the input signals (X_1, X_2, …X_{10}) as follows: Y= X_1 or X_2 or ⋯ or X_{10}
11		AND20	Defines the output signal (Y) with respect to the input signals (X_1, X_2, …X_{20}) as follows: Y= X_1 and X_2 and ⋯ and X_{20}
12		OR20	Defines the output signal (Y) with respect to the input signals (X_1, X_2, …X_{20}) as follows: Y= X_1 or X_2 or ⋯ or X_{20}
13		AND30	Defines the output signal (Y) with respect to the input signals (X_1, X_2, …X_{30}) as follows: Y= X_1 and X_2 and ⋯ and X_{30}
14		OR30	Defines the output signal (Y) with respect to the input signals (X_1, X_2, …X_{10}) as follows: Y= X_1 or X_2 or ⋯ or X_{30}

Table B.1 List of Function Symbols for Discrete Control Processes

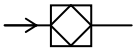
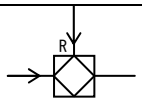
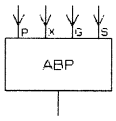
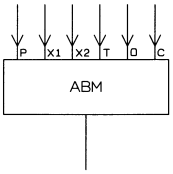
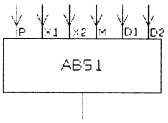
No	Symbol	Name	Function
15		NOT	Defines the output signal (Y) with respect to the input signals (X) as follows: Y= $\overline{X}$
16		ON DELAY TIMER	Turns the output signal ON after the delay time when the input signal changes from OFF to ON.
17		OFF DELAY TIMER	Turns the output signal OFF after the delay time when the input signal changes from ON to OFF.
18		ONE SHOT TIMER	Turns the output signal ON only for a set time span when the input signal changes from OFF to ON.
19		FLIP-FLOP	Latches output signal ON with the Set signal input, and clears the output signal with the Reset signal input.
20		2-out-of-3	Outputs a signal if 2 or more inputs out of 3 inputs are ON.
21		2-out-of-4	Outputs a signal if 2 or more inputs out of 4 inputs are ON.
22		3-out-of-4	Output a signal if 3 or more inputs out of 4 inputs are ON.
23		1-INPUT FLIP-FLOP	Inverts the output signal every time the input signal changes OFF (0) -> ON (1).
24		1-INPUT FLIP-FLOP WITH RESET	Performs the same function as 1-INPUT FLIP-FLOP when reset-signal is OFF.
25		ANSWER BACK FOR AUX. UNIT (INCL. TIME MEASURING FUNCTION)	Performs the aux. unit answer back error judgment logic computation and outputs the results of the computation.
26		ANSWER BACK FOR POWER VALVE (INCL. TIME MEASURING FUNCTION)	Performs the power valve answer back error judgment logic computation and outputs the results of the computation.
27		ANSWER BACK 1 FOR PNEUMATIC VALVE (INCL. TIME MEASURING FUNCTION)	Performs the pneumatic valve answer back error judgment logic computation and outputs the results of the computation.

Table B.1 List of Function Symbols for Discrete Control Processes

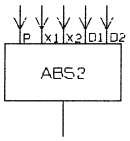
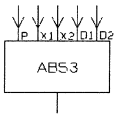
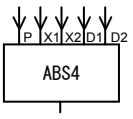
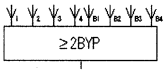
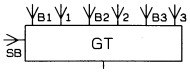
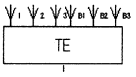
No	Symbol	NAME	Function
28		ANSWER BACK 2 FOR PNEUMATIC VALVE (INCL. TIME MEASURING FUNCTION)	Performs the pneumatic valve answer back error judgment logic computation and outputs the results of the computation.
29		ANSWER BACK 3 FOR PNEUMATIC VALVE (INCL. TIME MEASURING FUNCTION)	Performs the pneumatic valve answer back error judgment logic computation and outputs the results of the computation.
30		ANSWER BACK 4 FOR PNEUMATIC VALVE (INCL. TIME MEASURING FUNCTION)	Performs the pneumatic valve answer back error judgment logic computation and outputs the results of the computation.
31		ON FIXED OUTPUT	Outputs an “ON” signal. (Logic value = 1)
32		OFF FIXED OUTPUT	Outputs an “OFF” signal. (Logic value = 0)
33		2/4-LOGIC WITH BYPASS FUNCTION	Outputs if 2 (or more) out of 4 inputs are ON. Provided with the bypass function for the input signal. Outputs status to the multi-bypass-input tag.
34		GLOBAL TRIP LOGIC	Outputs if 2 (or more) out of 3 inputs are ON. Provided with the bypass function for the input signal.
35		TRIP ENABLE LOGIC	Outputs if 1 (or more) out of 3 inputs are ON. Provided with the bypass function for the input signal.

Table B.2 List of Function Symbols for Analog Control Processes

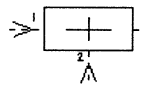
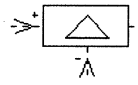
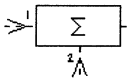
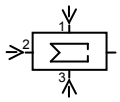
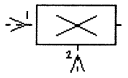
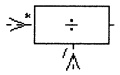
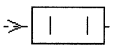
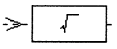
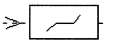
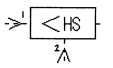
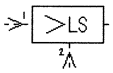
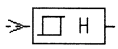
No.	Symbol	Name	Function
1		ADDER	Defines the output signal (Y) with respect to the input signals (X_1, X_2) as follows: $Y= X_1+X_2$
2		SUBTRACTER	Defines the output signal (Y) with respect to the input signals (X_1, X_2) as follows: $Y= X_1-X_2$
3		ADDER-SUBTRACTOR	Defines the output signal (Y) with respect to the input signals (X_1, X_2) as follows: $Y= G_1 \cdot X_1+G_2 \cdot X_2$
4		3-INPUT ADDER-SUBTRACTOR	Defines the output signal (Y) with respect to the input signals (X_1, X_2, X_3) as follows: $Y= G_1 \cdot X_1+G_2 \cdot X_2+G_3 \cdot X_3$ (G_1, G_2, G_3 :GAIN)
5		MULTIPLIER	Defines the output signal (Y) with respect to the input signals (X_1, X_2) as follows: $Y= X_1 \times X_2$
6		DIVIDER	Defines the output signal (Y) with respect to the input signals (X_1, X_2) as follows: $Y= X_1 \div X_2$
7		ABSOLUTE VALUE	Defines the output signal (Y) with respect to the input signals (X) as follows: $Y= \|X\|$
8		SQUARE ROOT	Defines the output signal (Y) with respect to the input signals (X) as follows: $Y= G \cdot \sqrt{X}$
9		DEAD ZONE	Defines the output signal (Y) with respect to the input signals (X) as follows: $d_1<X, d_2>X$ $Y= X$ $d_2 \leqq X \leqq d_1$ $Y=(d_1+d_2)/2$
10		HIGH SIGNAL SELECTOR / LOWER LIMIT CONTROLLER	Defines the output signal (Y) with respect to the input signals (X_1, X_2) as follows: $X_1<X_2$ $Y=X_2$, $X_1=X_2$ or $X_1>X_2$ $Y=X_1$
11		LOW SIGNAL SELECTOR / UPPER LIMIT CONTROLLER	Defines the output signal (Y) with respect to the input signals (X_1, X_2) as follows: $X_1=X_2$ or $X_1<X_2$ $Y=X_1$, $X_1>X_2$ $Y=X_2$
12		UPPER LIMIT MONITOR	Outputs a signal when the input signal is equal or greater than a set value. At the time the system is reset, the input signal is below the gap with respect to the set value.

Table B.2 List of Function Symbols for Analog Control Processes

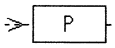
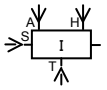
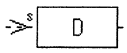
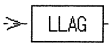
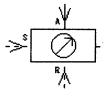
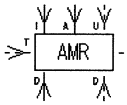
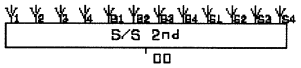
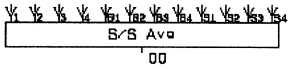
No.	Symbol	Name	Function
13		LOWER LIMIT MONITOR	Outputs a signal when the input signal is equal or less than a set value. At the time the system is reset, the input signal is below the gap with respect to the set value.
14		PROPORTIONAL	Outputs a signal with a proportional constant in response to the input signal.
15		INTEGRAL	Outputs an integrated output signal in response to the input signal.
16		DIFFERENTIATION	Outputs a differentiated output signal in response to the input signal.
17		LAG	Outputs the lag operation result as the output signal in response to the input signal.
18		LEAD/LAG	Outputs the lead/lag operation result as the output signal in response to the input signal.
19		SIGNAL SWITCH	Switches the digital input signal (SW) in response to the input signals (X_1, X_2) and outputs the output signal (Y). SW=1 Y= X_1, SW=0 Y= X_2
20		DEAD TIME	Outputs a signal in response to the input signal after delaying the output for a specified period of time.
21		ANALOG MEMORY	Gets parameters externally and, considering the digital input signal a trigger, outputs an output signal in proportion to the change rate set externally.
22		SIGNAL GENERATOR	Outputs a defined set value
23		LOGISTICS CONVERSION	Outputs the results of logistics output computation to the input signal.
24		SATURATION TEMPERATURE OPERATION	Outputs the operation result Y as indicated below with respect to the input signal X. $Y=a\cdot(X+b)^c$ (a:Coefficient, b: Bias, c: Power)
25		4-CH 2ND-HI SIGNAL SELECTOR	Selects and outputs second highest value with respect to the input values (1-4).
26		4-CH MEAN VALUE SIGNAL SELECTOR 3	Calculates and outputs the average value of normal channels for a 3-loop plant with respect to the input values (1 to 4).

Table B.2 List of Function Symbols for Analog Control Processes

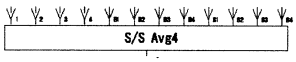
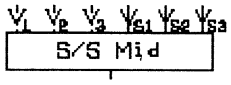
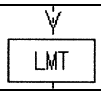
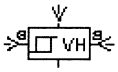
No.	Symbol	NAME	Function
27		4-CH MEAN VALUE SIGNAL SELECTOR 4	Calculates and outputs the average value of normal channels for a 4-loop plant with respect to the input values (1 to 4).
28		20-POLYGONAL LINE FUNCTION	Outputs the polygonal function of up to 20 points to the input signal.
29		3-CH INTERMEDIATE VALUE SIGNAL SELECTOR	Outputs the intermediate value with respect to the input values (1 to 3). The channels are compared and if the deviation is larger than the deviation upper limit setting value (A), the larger deviation status output flag is set ON after T seconds.
30		UPPER/LOWER LIMIT LIMITER	Outputs a signal within the set range of the output upper/lower limit to the input signal.
31		VARIABLE UPPER LIMIT MONITOR	Outputs a signal when the input signal reaches the set value. The input signal should be below the gap value in relation to the set value. (The gap value can be changed by using the input signal.)
32		ANALOG SIGNAL BCD CONVERSION	Converts the analog signal to BCD code.

Table B.3 List of Function Symbols for Input and Output Process

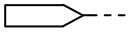
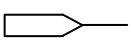
No	Symbol	Name
1		ANALOG INPUT
2		ANALOG OUTPUT
3		DIGITAL INPUT
4		DIGITAL OUTPUT
5		POWER INTERFACE DIGITAL INPUT
6		POWER INTERFACE DIGITAL OUTPUT
7		COMMUNICATION ANALOG INPUT
8		COMMUNICATION ANALOG OUTPUT
9		COMMUNICATION DIGITAL INPUT
10		COMMUNICATION DIGITAL OUTPUT
11		STATUS COMMUNICATION DIGITAL INPUT
12		STATUS COMMUNICATION DIGITAL OUTPUT
13		OPERATION ANALOG INPUT
14		OPERATION DIGITAL INPUT
15		TEST DIGITAL INPUT
16		TEST ANALOG OUTPUT
17		TEST DIGITAL OUTPUT
18		APPLICATION DIAGNOSIS ERROR OUTPUT
19		ANSWER BACK ERROR DIAGNOSIS OUTPUT
20		CROSS REFERENCE ANALOG INPUT
21		CROSS REFERENCE DIGITAL INPUT

Table B.3 List of Function Symbols for Input and Output Process

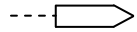
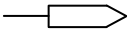
No	Symbol	NAME
22		CROSS REFERENCE ANALOG OUTPUT
23		CROSS REFERENCE DIGITAL OUTPUT

Table B.4 List of Function Symbols for Obtaining and Setting Status Values

No	Symbol	Name
1		ANALOG STATUS RESET
2		DIGITAL STATUS RESET
3		ANALOG ATTACHMENT BIT TAKEOUT
4		DIGITAL ATTACHMENT BIT TAKEOUT

APPENDIX C DEFINITION

Alarm

A minor abnormality with which the subsystem can continue its functions. When the subsystem detects this type of error, it does not change its mode and only warns of the error.

Application Software

Software which provides or supports user specific functions. This software resides on a CPU Module with the basic software.

Basic Software

System software that operates the controller (or hardware) and peripheral modules. This software consists of initialization code, device drivers, communication layers, function blocks, diagnostics, etc. for the MELTAC platform including firmware and FPGA.

Bus Master Module

A module that has 4 communication interface channels to use for communication with I/O modules or Data Link communications. This module resides in the CPU Chassis.

Control Mode

A state in which the subsystem performs input, operation, output processing, and self-diagnosis for the purpose of controlling plant systems.

Control Network

A MELTAC dedicated ring topology network which continuously communicates plant process data and control signal data within a deterministic periodic cycle.

Control Network I/F Module

A module that connects the controller to the Control Network. This module resides in the CPU Chassis .

CPU Chassis

A chassis which can accommodate various modules such as the Power Supply Module, CPU Module, Control Network I/F Module, System Management Module and Bus Master Module.

CPU Fan

A fan installed on top of the CPU Chassis to cool the modules within the CPU Chassis.

CPU Module

A module that utilizes a microprocessor and performs internal operations and data transmission with other modules (i.e.: Bus Master Module, Control Network I/F Module and System Management Module).
This module utilizes F-ROM for storing both the basic software and the application software. This module resides in the CPU Chassis

Data Link

A communication type used to transmit process signals between controllers of different safety divisions. This communication is unidirectional.

Dedicated Re-programming Chassis

The CPU Module F-ROM can be updated only when the CPU Module is placed in this chassis after removing it from the on-line controller chassis.

Distribution Module

A module that interfaces with field signals. This module distributes the field signal to input modules on the rear side of the I/O Chassis. Similarly, the output signal is sent out through this module. This module resides in the I/O Chassis.

Door Fan Unit

A Fan Unit installed at the top rear of the cabinet to cool internal cabinet components.

EEPROM

Electrically Erasable Programmable Read Only Memory.
This memory can be erased and reprogrammed repeatedly through the application of higher than normal electrical voltage.

Electrical/Optical (E/O) Converter Module

A module for Data Link communication, which converts electrical signals to optical signals or optical signals to electrical signals.

Electrical/Optical Converter Chassis

A chassis which can accommodate up to 14 E/O converter modules.

Failure

A fatal abnormality with which the subsystem cannot continue its functions.
When the subsystem detects this type of error, it transitions to Failure Mode.
In Failure Mode, the processing of I/O and operation is stopped.

Failure Mode

The subsystem initializes in this mode after initial power activation. The subsystem also shifts to this mode automatically after it detects its own failure or there is a loss of power greater than 20 ms. A subsystem can shift from this mode to the Control Mode only by pushing the reset button on the Status Display Module.

FPGA

Field Programmable Gate Array.
FPGA has many internal logical blocks consisting of logic gates and arithmetic circuits. Internal logical blocks are located on a matrix. Required circuit configurations are implemented by connecting these internal logical blocks.

Frame Memory Unit (FMU) Module

A module that provides the analog RGB signal for the graphic images to the safety VDU panel. This module also provides the touch panel interface signal from the safety VDU panel to the safety VDU processor by means of an RS-232C data link. This module resides in the CPU Chassis.

F-ROM

Flash Read Only Memory. Also called flash memory.
One of the nonvolatile semiconductor memory type in which data does not disappear even after a device is turned off.

I/O Alarm

This alarm indicates I/O abnormality. When the subsystem detects this type of abnormality, it does not change its mode and only warns of the alarm.

I/O Bus

A communication line between the Bus Master Module and the I/O Chassis. This bus is used for transmission of data, such as process inputs from the I/O module to the CPU Module and outputs commands from the CPU Module to the I/O module.

Input/Output Chassis

A chassis which can accommodate up to 16 I/O modules.

Input/Output(I/O) Modules

Modules that interface with process signals. These modules provide process input/output functions and signal conditioner functions, including signal conversion and noise reduction.

Isolation Module

A module which provides electrical isolation between safety systems and non-safety systems.

Maintenance Network

The network used to communicate between the controllers / safety VDU processors and the MELTAC engineering tools.

MELTAC Controller

Mitsubishi Electric Total Advanced Controller.
MELCO’s safety system digital platform for nuclear power plants.

MELTAC engineering tool

A tool that generates applications which operate on the MELTAC platform. The tool downloads generated applications to the MELTAC controllers, and displays failure and status information of the MELTAC platform (see Section 4.1.4.1 for details). This tool consists of (Windows-based) non-safety PC and software called "MELENS”.

NI Chassis

A chassis which can accommodate NI modules.

NI modules

Modules that interface to neutron detector or other modules. These modules provide signal conditioner functions.

Optical Switch

A switch which bypasses the Control Network communication line in the Control Network I/F Module during controller maintenance.

POL

Problem Oriented Language.
This is the control language used in the MELTAC controllers.

Power Interface Module (PIF Module)

A module that receives output commands as a result of subsystem operation, and controls the power that drives the switchgears, solenoid valves, etc. for plant components. This module resides in the CPU Chassis.

Power Supply Fan Unit

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

Power Supply Module

A module that converts the AC power into DC power voltages suitable for the individual modules and units. This module resides in the CPU Chassis and I/O Chassis.

Redundant Parallel Controller

In the "Redundant Parallel" configuration, the controller includes 2 subsystems. Each subsystem operates in Control Mode.
Even if one of the subsystems fail, this configuration allows a system to maintain its safety function without a subsystem changeover.

Redundant Standby Controller

In the "Redundant Standby" configuration, the controller includes 2 subsystems. One subsystem operates in Control Mode while the other subsystem operates in Standby Mode.
This configuration allows a system to maintain high reliability even when an error is detected in the subsystem in Control Mode by the self-diagnosis function, with a backup of the subsystem in Standby Mode (i.e.: status switching when the control subsystem fails).

Repeater Module

A module that is used to shape and amplify data communication signals between I/O modules and the Bus Master Module. This module resides in the I/O Chassis.

ROM writing tool

A tool used to write binary code to nonvolatile devices (ROM).

Safety VDU Panel

An HSI device which provides a color graphic display with an integral touch screen.

Safety VDU Processor

A processor which transfers operation signals received from the safety VDU panel to the safety systems and displays information from the safety systems on the safety VDU panel.

Self-Diagnosis

The integrity of digital I&C components is continuously checked by their self-diagnostic features. These self-diagnostic features result in early detection of failures.

Single Controller

In the "Single" configuration, the controller includes only one subsystem.
This subsystem operates in Control Mode.

Standby Mode

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

Status Display & Switch Module

A module that displays the mode and alarms of subsystems and provides the manual mode change over switch.
This module is used in a CPU Chassis configured for a Redundant Standby Controller.

Status Display Module

A module that displays the mode and alarms of single subsystem.
This module is used in a CPU Chassis configured for a Redundant Parallel Controller or a Single Controller.

System Management Module

A module that monitors the status of the CPU Module and executes auxiliary controller functions that are not directly related to the CPU Module such as Ethernet I/F for communicating with the MELTAC engineering tool. This module resides in the CPU Chassis.

V&V

Verification and Validation.
The process of determining whether:

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

APPENDIX D REGULATORY REQUIREMENTS AND GUIDANCE APPLICABILITY MATRIX

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

10 CFR 50, 10 CFR 52, AND 10 CFR 73

Criteria (1)	Title	Applicability	Design Information(2)
50.55a(a)(1)	Quality Standards for Systems Important to Safety	X	JEXU-1041-1008 6.0
50.55a(h)(2)	Protection Systems (IEEE Std. 603-1991 or IEEE Std. 279-1971)	X	See applicability to IEEE Std. 603.
50.55a(h)(3)	Safety Systems (IEEE Std. 603-1991)	X	See applicability to IEEE Std. 603.
50.34(f)(2)(v) [I.D.3]	Bypass and Inoperable Status Indication	N/A	Described in Application Licensing Document.
50.34(f)(2)(xi) [II.D.3]	Direct Indication of Relief and Safety Valve Position	N/A	
50.34(f)(2)(xii) [II.E.1.2]	Auxiliary Feedwater System Automatic Initiation and Flow Indication	N/A	
50.34(f)(2)(xvii) [II.F.1]	Accident Monitoring Instrumentation	N/A	
50.34(f)(2)(xviii) [II.F.2]	Instrumentation for the Detection of Inadequate Core Cooling	N/A	
50.34(f)(2)(xiv) [II.E.4.2]	Containment Isolation Systems	N/A	
50.34(f)(2)(xix) [II.F.3]	Instruments for Monitoring Plant Conditions Following Core Damage	N/A	
50.34(f)(2)(xx) [II.G.1]	Power for Pressurizer Level Indication and Controls for Pressurizer Relief and Block Valves	N/A	
50.34(f)(2)(xxii) [II.K.2.9]	Failure Mode and Effect Analysis of Integrated Control System	N/A	
50.34(f)(2)(xxiii) [II.K.2.10]	Anticipatory Trip on Loss of Main Feedwater or Turbine Trip	N/A	
50.34(f)(2)(xxiv) [II.K.3.23]	Central Reactor Vessel Water Level Recording	N/A	
50.62	Requirements for Reduction of Risk from Anticipated Transients without Scram	N/A	
52.47(b)(1)	ITAAC for Standard Design Certification	N/A	
52.80(a)	ITAAC for Combined Licensee Applications	N/A	
73.54	Protection of digital computer and communication systems and networks	N/A	

(1) The applicable criteria in NUREG-0800 Standard Review Plan (SRP) Sec. 7.1 Rev. 5, ISG-06, and each clause of IEEE Std. 603-1991 and IEEE Std. 7-4.3.2-2003 are listed in this table to ensure all technical and quality requirements for the safety-related I&C platform are included.

(2) Design information to describe that the safety-related I&C platform design conforms to the NRC regulations and guidance, and meets the technical and quality requirements of the safety-related I&C platform.

GDC 10 CFR 50 APPENDIX A

Criteria [1]	Title	Applicability	Design Information[2]
GDC 1	Quality Standards and Records	X	JEXU-1041-1008 6.0
GDC 2	Design Bases for Protection Against Natural Phenomena	X	JEXU-1041-1008 5.0
GDC 4	Environmental and Dynamic Effects Design Bases	X	JEXU-1041-1008 5.0
GDC 10	Reactor Design	N/A	Described in Application Licensing Document.
GDC 13	Instrumentation and Control	N/A	
GDC 15	Reactor Coolant System Design	N/A	
GDC 16	Containment Design	N/A	
GDC 19	Control Room	N/A	
GDC 20	Protection System Functions	N/A	
GDC 21	Protection Systems Reliability and Testability	X	JEXU-1041-1008 4.1.5, 4.1.7, 4.2.3, 4.2.4, 7.0
GDC 22	Protection System Independence	X	JEXU-1041-1008 4.1.2.3, 4.1.2.5, 4.3, 5.5, Appendix A.3, A.4, A.6, A.7
GDC 23	Protection System Failure Modes	X	JEXU-1041-1008 4.1.5, 4.2.3
GDC 24	Separation of Protection and Control Systems	X	JEXU-1041-1008 Appendix B (Signal Selection [S/S] Function)
GDC 25	Protection System Requirements for Reactivity Control Malfunctions	N/A	Described in Application Licensing Document.
GDC 28	Reactivity Limits	N/A	
GDC 29	Protection Against AOOs	N/A	
GDC 33	Reactor Coolant Makeup	N/A	
GDC 34	Residual Heat Removal	N/A	
GDC 35	Emergency Core Cooling	N/A	
GDC 38	Containment Heat Removal	N/A	
GDC 41	Containment Atmosphere Cleanup	N/A	
GDC 44	Cooling Water	N/A	

STAFF REQUIREMENTS MEMORANDA

Criteria [1]	Title	Applicability	Design Information[2]
SRM to SECY 93087 II.Q	Defense Against Common-Mode Failures in Digital I&C Systems	N/A	Described in Application Licensing Document.
SRM to SECY 93087 II.T	Control Room Annunciator (Alarm) Reliability	N/A	

REGULATORY GUIDE

Criteria [1]	Title	Applicability	Design Information[2]
RG 1.22	Periodic Testing of Protection System Actuation Functions	X	See applicability to GDC 21.
RG 1.47	Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety System	N/A	Described in Application Licensing Document.
RG 1.53	Application of the Single-Failure Criterion to Safety Systems	X	See applicability to GDC 21 and 24.
RG 1.62	Manual Initiation of Protection Actions	N/A	Described in Application Licensing Document.
RG 1.75	Independence of Electrical Safety Systems	X	See applicability to GDC 22.
RG 1.97	Instrumentation for Light Water Cooled NPPs to Assess Plant Conditions During and Following an Accident and Criteria for Accident Monitoring Instrumentation for NPPs	N/A	Described in Application Licensing Document.
RG 1.105	Setpoints for Safety-related Instrumentation	X	JEXU-1041-1008 Appendix A.5, A.6, A.9
RG 1.118	Periodic Testing of Electric Power and Protection Systems	X	See applicability to GDC 21.
RG 1.151	Instrument Sensing Lines	N/A	Described in Application Licensing Document.
RG 1.152	Criteria for Use of Computers in Safety Systems of Nuclear Power Plants	X	See applicability to IEEE Std. 7-4.3.2.
RG 1.168	Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	X	JEXU-1041-1008 4.1.3, 4.2.2, 6.0
RG 1.169	Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants		
RG 1.170	Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants		
RG 1.171	Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants		
RG 1.172	Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants		
RG 1.173	Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants		
RG 1.174	An Approach for Using PRA in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis	N/A	Described in Application Licensing Document.
RG 1.177	An Approach for Plant-Specific Risk-Informed Decision Making: technical specifications	N/A	
RG 1.180	Guidelines for Evaluating Electromagnetic and Radiofrequency Interference in Safety-Related I&C Systems	X	JEXU-1041-1008 5.3, 5.4
RG 1.189	Fire Protection for Operating Nuclear Power Plants	N/A	Described in Application Licensing Document.
RG 1.200	An Approach for Determining the Technical Adequacy of PRA Results for Risk-Informed Activities	N/A	
RG 1.204	Guidelines for Lightning Protection of Nuclear Power Plants	X	JEXU-1041-1008 5.3
RG 1.209	Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants	X	See applicability to GDC 21.
RG 1.32	Criteria for Power Systems for Nuclear Power Plants	N/A	Described in Application Licensing Document.
RG 1.89	Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants	X	JEXU-1041-1008 5.1

BRANCH TECHINCAL POSITION

Criteria [1]	Title	Applicability	Design Information[2]
BTP 7-1	Guidance on Isolation of Low-Pressure Systems from the High-Pressure RCS	N/A	Described in Application Licensing Document.
BTP 7-2	Guidance on Requirements on Motor-Operated Valves in the Emergency Core Cooling System (ECCS) Accumulator Lines	N/A	
BTP 7-3	Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps Out of Service	N/A	
BTP 7-4	Guidance on Design Criteria for Auxiliary Feedwater Systems	N/A	
BTP 7-5	Guidance on Spurious Withdrawals of Single Control Rods in Pressurized Water Reactors	N/A	
BTP 7-6	Guidance on Design of I&Cs Provided to Accomplish Changeover from Injection to Recirculation Mode	N/A	
BTP 7-7	Not used	N/A	N/A
BTP 7-8	Guidance on Application of RG 1.22	X	See applicability to RG 1.22 and GDC 21.
BTP 7-9	Guidance on Requirements for RPS Anticipatory Trips	N/A	Described in Application Licensing Document.
BTP 7-10	Guidance on Application of RG 1.97	N/A	
BTP 7-11	Guidance on Application and Qualification of Isolation Devices	X	See applicability to RG 1.75 and GDC 22.
BTP 7-12	Guidance on Establishing and Maintaining Instrument Setpoints	N/A	Described in Application Licensing Document.
BTP 7-13	Guidance on Cross-Calibration of Protection System Resistance	N/A	
BTP 7-14	Guidance on Software Reviews for Digital Computer-Based I&C Systems	X	See applicability to RG 1.168 thru 1.173.
BTP 7-15	Not used	N/A	N/A
BTP 7-16	Not used	N/A	
BTP 7-17	Guidance on Self-Test and Surveillance Test Provisions	X	See applicability to RG 1.22, 1.118 and GDC 21.
BTP 7-18	Guidance on Use of Programmable Logic Controllers in Digital Computer-Based I&C Systems	N/A	Described in Application Licensing Document.
BTP 7-19	Guidance on Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based I&C Systems	N/A	
BTP 7-20	Not used	N/A	N/A
BTP 7-21	Guidance on Digital Computer Real-Time Performance	X	JEXU-1041-1008 4.1.3, 4.2.2, 4.4

IEEE STD. 603-1991

Criteria [1]	Title	Applicability	Design Information[2]
1.	Scope	N/A	Described in Application Licensing Document.
2.	Definitions	N/A	
3.	References	N/A	
4	Safety System Designation	No Request	N/A
4.1	Design Basis Events	N/A	Described in Application Licensing Document.
4.2	Safety Functions and Corresponding Protective Actions	N/A	
4.3	Permissive Conditions for Each Operating Bypass Capability	N/A	
4.4	Variables Required to be Monitored for Protective Action	N/A	
4.5	The Minimum Criteria for Each Action Controlled by Manual Means	N/A	
4.5.1	Allowed Time and Plant Condition	N/A	
4.5.2	Justification of Permitting Initiation or Control Subsequent to Initiation	N/A	
4.5.3	Control Room Habitability	N/A	
4.5.4	Display of Variable	N/A	
4.6	Spatially Dependent Variables	N/A	
4.7	Range of Conditions for Safety System Performance	N/A	
4.8	Functional Degradation of Safety Functions	N/A	
4.9	Reliability	X	JEXU-1041-1008 4.1.5, 4.2.3, 7.0
4.10	The Critical Points in Time or the Plant Conditions	X	JEXU-1041-1008 4.1.3, 4.2.2, 4.4
4.11	Equipment Protective Provisions	X	JEXU-1041-1008 4.1.5, 4.2.3
4.12	Other Special Design Basis	No Request	N/A
5	Safety System Criteria	No Request	N/A
5.1	Single Failure Criterion	N/A	Described in Application Licensing Document.
5.2	Completion of Protective Action	N/A	
5.3	Quality	X	JEXU-1041-1008 6.0
5.4	Equipment Qualification	X	JEXU-1041-1008 5.0
5.5	System Integrity	N/A	Described in Application Licensing Document.
5.6	Independence	X	JEXU-1041-1008 4.1.2.3, 4.1.2.5, 4.3, 5.5, Appendix A.3, A.4, A.6, A.7
5.6.1	Between Redundant Portions of a Safety System		
5.6.2	Between Safety Systems and Effects of a Design Basis		
5.6.3	Between Safety Systems and Other Systems		
5.6.3.1	Interconnected Equipment		
5.6.3.2	Equipment in Proximity		
5.6.3.3	The Effects of a Single Random Failure		
5.6.4	Detailed Independence Criteria		

Criteria [1]	Title	Applicability	Design Information[2]
5.7	Capability for Test and Calibration	X	JEXU-1041-1008 4.1.5, 4.2.3, 7.0
5.8	Information Displays	No Request	N/A
5.8.1	Displays for Manually Controlled Actions	N/A	Described in Application Licensing Document.
5.8.2	System Status Indication	N/A	
5.8.3	Indication of Bypasses	N/A	
5.8.4	Location of Displays	N/A	
5.9	Control of Access	X	JEXU-1041-1008 4.5
5.10	Repair	X	JEXU-1041-1008 4.1.4, 4.1.5, 4.2.3
5.11	Identification	N/A	Described in Application Licensing Document.
5.12	Auxiliary Features	N/A	
5.13	Multi-Unit Stations	N/A	
5.14	Human Factors	N/A	
5.15	Reliability	X	JEXU-1041-1008 7.0
5.16	Common Cause Failure (IEEE 603-1998)	X	JEXU-1041-1008 4.1.3, 4.2.2, 5.0, 6.0
6	Sense and Command Features - Functional and Design Requirements.	N/A	Described in Application Licensing Document.
6.1	Automatic Control	N/A	
6.2	Manual Control	N/A	
6.3	Interaction between the Sense and Command features and other Systems	X	JEXU-1041-1008 Appendix B (S/S Function)
6.4	Derivation of System Inputs	N/A	Described in Application Licensing Document.
6.5	Capability for Testing and Calibration	N/A	
6.6	Operating Bypasses	N/A	
6.7	Maintenance Bypass	N/A	
6.8	Setpoint	No Request	N/A
6.8.1	Setpoint Uncertainties	N/A	Described in Application Licensing Document.
6.8.2	Multiple Setpoints	N/A	
7	Executive Features - Functional and Design Requirements	N/A	
7.1	Automatic Control	N/A	
7.2	Manual Control	N/A	
7.3	Completion of Protective Action	N/A	
7.4	Operating Bypass	N/A	
7.5	Maintenance Bypass	N/A	
8	Power Source Requirements	N/A	

IEEE STD. 7-4.3.2-2003

Criteria [1]	Title	Applicability	Design Information[2]
1.	Scope	N/A	Described in Application Licensing Document.
2.	References	N/A	
3.	Definitions and Abbreviations	N/A	
4	Safety System Designation	No Request	N/A
5	Safety System Criteria	No Request	
5.1	Single Failure Criterion	No Request	
5.2	Completion of Protective Action	No Request	
5.3	Quality	X	JEXU-1041-1008 4.1.3, 4.2.2, 6.0
5.3.1	Software Development		
5.3.1.1	Software Quality Metrics		
5.3.2	Software Tools		
5.3.3	Verification and Validation		
5.3.4	Independent V&V (IV&V) Requirements		
5.3.5	Software Configuration Management		
5.3.6	Software Project Risk Management		
5.4.	Equipment Qualification	X	JEXU-1041-1008 4.1.5, 4.3, 5.0, 6.0
5.4.1	Computer System Testing		
5.4.2.	Qualification of Existing Commercial Computers	N/A	Described in Application Licensing Document.
5.5.	System Integrity	X	JEXU-1041-1008 4.1.3, 4.2.2, 6.0
5.5.1	Design for computer integrity		
5.5.2	Design for test and calibration	X	JEXU-1041-1008 4.1.5, 4.2.3, 7.0
5.5.3	Fault detection and self-diagnostics		
5.6	Independence	X	JEXU-1041-1008 4.1.2.3, 4.1.2.5, 4.3, 5.5, Appendix A.3, A.4, A.6, A.7
5.7	Capability for Test and Cal bration	No Request	N/A
5.8	Information Displays	No Request	
5.9	Control of Access	No Request	
5.10	Repair	No Request	
5.11	Identification	X	JEXU-1041-1008 6.1.8
5.12	Auxiliary Features	No Request	N/A
5.13	Multi-Unit Stations	No Request	
5.14	Human Factors	No Request	
5.15	Reliability	X	JEXU-1041-1008 7.0
6	Sense and Command Features - Functional and Design	No Request	N/A
7	Executive Features - Functional and Design Requirements	No Request	
8	Power Source Requirements	No Request	