

Safety System Digital Platform -MELTAC-

Non Proprietary Version

December 2008

**©2008 Mitsubishi Heavy Industries, Ltd.
All Rights Reserved**

Revision History

Revision	Date	Page (Section)	Description
0	March 2007	All	Original issued
1	July 2007		Refer to Revision History of JEXU-1012-1002-P(R1)
2	August 2008		Refer to Revision History of JEXU-1012-1002-P(R2)
3	December 2008		Refer to Revision History of JEXU-1012-1002-P(R3)

© 2008

MITSUBISHI HEAVY INDUSTRIES, LTD.

All Rights Reserved

This document has been prepared by Mitsubishi Heavy Industries, Ltd. ("MHI") in connection with its request to the U.S. Nuclear Regulatory Commission ("NRC") for a pre-application review of the US-APWR nuclear power plant design. No right to disclose, use or copy any of the information in this document, other than by the NRC and its contractors in support of MHI's pre-application review of the US-APWR, is authorized without the express written permission of MHI.

This document contains technology information and intellectual property relating to the US-APWR and it is delivered to the NRC on the express condition that it not be disclosed, copied or reproduced in whole or in part, or used for the benefit of anyone other than MHI without the express written permission of MHI, except as set forth in the previous paragraph.

This document is protected by the laws of Japan, U.S. copyright law, international treaties and conventions, and the applicable laws of any country where it is being used.

Mitsubishi Heavy Industries, Ltd.
16-5, Konan 2-chome, Minato-ku
Tokyo 108-8215 Japan

Abstract

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

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

Safety System Digital Platform - MELTAC -

Non-proprietary Version

December 2008

**© 2008 MITSUBISHI ELECTRIC CORPORATION
All Rights Reserved**

Prepared: Shigeru Sugitani 12/11/08 Tomonori Yamane 12/11/08
Shigeru Sugitani, Manager Date Tomonori Yamane, Manager
Control & Protection Systems Section DCS Development Section

Reviewed: Hidetoshi Matsushita 12/11/08 Makoto Itoh 12/11/08
Hidetoshi Matsushita, Manager Date Makoto Ito, Manager
Control & Protection Systems Section DCS Development Section

Approved: Tokihiro Fukuhara 12/11/08 Hiroaki Ohno 12/11/08
Tokihiro Fukuhara, Section Manager Date Hiroaki Ohno, Section Manager
Control & Protection Systems Section DCS Development Section

Approved: Toru Ito 12/11/08
Toru Ito, Project Manager Date
Nuclear Power Department

Approved: Keisuke Ichieda 12/11/08
Keisuke Ichieda, Department Manager Date
Development Department

Approved: Shuichi Kobashi 12/11/08
Shuichi Kobashi, Department Manager Date
Nuclear Power Department

Approved: Tatsuaki Kawabata 12/11/08
Tatsuaki Kawabata, Department Manager Date
Nuclear Power Plant Quality Assurance Department

Signature History

	Rev.0	Rev.1	Rev.2	
Prepared	Shigeru Sugitani	Shigeru Sugitani	Shigeru Sugitani	
	Tomonori Yamane	Tomonori Yamane	Tomonori Yamane	
Reviewed	Tokihiro Fukuhara	Hidetoshi Matsushita	Hidetoshi Matsushita	
	Makoto Ito	Makoto Ito	Makoto Ito	
Approved	Katsumi Akagi	Tokihiro Fukuhara	Tokihiro Fukuhara	
	Hiroaki Ohno	Hiroaki Ohno	Hiroaki Ohno	
	Kunio Yugami	Toru Ito	Toru Ito	
	Keisuke Ichieda	Keisuke Ichieda	Keisuke Ichieda	
	Masahiko Yamawaki	Shuichi Kobashi	Shuichi Kobashi	
	Yasuo Shiraishi	Yasuo Shiraishi	Tatsuaki Kawabata	

Revision History

Revision	Date	Page (section)	Description
0	March 2007	All	Original issued
1	July 2007	<div>47 (Sec.4.1.3.1)</div> <div>[</div> <div>51 (Sec.4.1.4)</div> <div>51,52 (Sec.4.1.4.1)</div> <div>53 (Sec.4.1.4.2)</div> <div>[</div> <div>85,86 (Sec.4.3.4)</div> <div>[</div> <div>125 (Sec.6.1.5)</div>	<p>The following items are revised based on NRC comments or correction of simple spelling errors.</p> <p>Figure 4.1-10 is modified.</p> <ul style="list-style-type: none"> • Tool Communication is added. <p>Description of Engineering Tool is modified.</p> <p>Description of download is modified. "Controller failure diagnosis display" is added. "Adjustment of field changeable constants and setpoints" is added.</p> <p>Description of network for Engineering Tool is modified.</p> <p>Description of Maintenance Network configuration and isolation are added.</p> <p>Spelling errors are corrected (They -> The)</p>

Revision	Date	Page (section)	Description
3	December 2008	i	Spelling error is corrected (that -> than).
		6,9,13 (Sec.3.0)	Descriptions in Paragraphs 6, 16, and 44 are revised in accordance with the response to RAI.
		15,16,17,19 (Sec.3.0)	Paragraphs of the sections and procedures that include descriptions related to each standard are indicated. (Number 54, 55 – 57, 59, 61, 64 – 74)
		18 – 20 (Sec.3.0)	Two standards (IEEE802.3 and IEEE802.17) are deleted and the paragraph numbers thereafter are reassigned.(Paragraphs 76 – 87)
		84 (Sec.4.3.3.1)	Omission in writing in Figure 4.3-5 is corrected in accordance with the response to RAI.
		97 (Sec.5.0)	Descriptions of environmental, seismic, and EMC test reports are added in accordance with the response to RAI.
		164 (Appendix A.5)	Description of the accuracy of analog input is added in accordance with the response to RAI on Safety I&C System. (**)
		168 (Appendix A.8)	Error in writing is modified (1.6A _{0-P} -> 16A _{0-P}).

© 2008

MITSUBISHI ELECTRIC CORPORATION

All Rights Reserved

This document has been prepared by Mitsubishi Electric Corporation ("MELCO") in connection with Mitsubishi Heavy Industries, LTD. ("MHI")'s request to the U.S. Nuclear Regulatory Commission ("NRC") for a pre-application review of the US-APWR nuclear power plant design. No right to disclose, use or copy any of the information in this document, other than by the NRC and its contractors in support of MHI's pre-application review of the US-APWR, is authorized without the express written permission of MELCO.

This document contains technology information and intellectual property relating to the MELCO's Safety System Digital Platform(MELTAC) and it is delivered to the NRC on the express condition that it not be disclosed, copied or reproduced in whole or in part, or used for the benefit of anyone other than MELCO without the express written permission of MELCO, except as set forth in the previous paragraph.

This document is protected by the laws of Japan, U.S. copyright law, international treaties and conventions, and the applicable laws of any country where it is being used.

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

Abstract

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

The MELTAC Platform was developed specifically for nuclear applications. The modular structure, deterministic response time and testability can be applied to solve plant-wide needs for safety and non-safety applications. Moreover the MELTAC Platform has been developed using a rigorous safety related design process that ensures suitable hardware and software quality and reliability for critical applications such as the Reactor Protection System or Engineered Safety Features Actuation System.

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

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

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

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

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

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

The complete MHI digital I&C design is described in four Topical Reports:

- Safety I&C System Description and Design Process
- Safety System Digital Platform - MELTAC - (this report)
- HSI System Description and HFE (Human Factor Engineering) Process
- Defense in Depth and Diversity

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

Table of Contents

List of Tables	vi
List of Figures	vii
List of Acronyms	viii
1.0 PURPOSE.....	1
2.0 SCOPE.....	1
3.0 APPLICABLE CODE, STANDARDS AND REGULATORY GUIDANCE	2
4.0 MELTAC PLATFORM DESCRIPTION.....	21
4.1 Controller	22
4.1.1 Hardware Configuration	22
4.1.2 Hardware Descriptions.....	37
4.1.3 Software	48
4.1.4 Engineering Tool	52
4.1.5 Self-Diagnosis.....	55
4.2 Safety VDU Panel and Processor.....	62
4.2.1 Hardware	62
4.2.2 Software	67
4.2.3 Self-Diagnosis.....	74
4.3 Communication System.....	75
4.3.1 General Description	75
4.3.2 Control Network	75
4.3.3 Data Link.....	84
4.3.4 Maintenance Network	86
4.4 Response Time.....	89
4.4.1 Processing Time of MELTAC Fundamental Cycle.....	89
4.4.2 Processing Time of MELTAC Application	90
4.4.3 Examples of Response Time Calculations.....	94
4.5 Control of Access.....	96
4.5.1 Control of Access for Hardware	96
4.5.2 Control of Access for Software.....	96
5.0 ENVIRONMENTAL, SEISMIC AND ELECTROMAGNETIC QUALIFICATION	97
5.1 Environmental Test	97
5.1.1 Environmental Specification and Outline of Test	97
5.1.2 Contents of Environmental Test	97
5.2 Seismic Test.....	102
5.2.1 Overview	102
5.2.2 Seismic Resistance Test	102
5.3 Electromagnetic Compatibility and Radio Frequency Interference.....	107
5.3.1 Test Configuration	108
5.3.2 Description of Tests.....	110
5.4 Electrostatic Discharge Test	116
6.0 LIFE CYCLE.....	118
6.1 Life Cycle Process.....	118
6.1.1 Overview of the MELTAC Quality Assurance Program	118
6.1.2 Quality Assurance	120
6.1.3 Management	123

6.1.4 Development.....	124
6.1.5 Configuration Management.....	129
6.1.6 Cyber Security Management.....	131
6.1.7 US Conformance Program for Previously Developed Components	135
6.1.8 Software Installation.....	139
6.1.9 Maintenance	141
6.1.10 Training	142
6.1.11 Operations.....	143
6.1.12 Software Safety Plan.....	145
6.2 Life Cycle Management.....	146
6.2.1 Quality Records Management.....	146
6.2.2 Failure and Error Reporting and Corrective Action	146
6.2.3 Obsolescence Management	148
7.0 EQUIPMENT RELIABILITY.....	150
7.1 History of Operation.....	150
7.2 Mean Time between Failures (MTBF) Analysis	151
7.3 Controller Reliability Analysis.....	152
7.3.1 Reliability Model.....	153
7.3.2 FTA for Spurious Actuation of the Safety Function.....	154
7.3.3 FTA of Failure to Actuate the Safety Function.....	155
7.3.4 Detailed Controller Reliability Analysis.....	156
7.4 Failure Mode and Effects Analysis (FMEA)	159
7.5 Periodic Replacement Equipment (Parts) to Keep Reliability.....	160
APPENDIX A HARDWARE SPECIFICATIONS.....	162
Appendix A.1 CPU Module PCPJ-11 Specification.....	162
Appendix A.2 System Management Module Specification.....	162
Appendix A.3 Bus Master Module Specification	163
Appendix A.4 Control Network I/F Module Specification.....	163
Appendix A.5 I/O Module Specification.....	164
Appendix A.6 Isolation Module Specifications	167
Appendix A.7 E/O Converter Modules Specifications.....	167
Appendix A.8 Power Interface Modules Specifications.....	168
Appendix A.9 Power Supply Modules Specifications.....	168
Appendix A.10 Safety VDU Panel Specification	169
Appendix A.11 FMU Module Specification	169
Appendix A.12 Touch Panel Interface Module Specification.....	169
APPENDIX B FUNCTIONAL SYMBOL SOFTWARE SPECIFICATIONS	170

List of Tables

Table 4.1-1 Scale and Capacity	34
Table 4.1-2 Environmental Specifications	35
Table 4.1-3 Module in the CPU Chassis	37
Table 4.1-4 CPU Chassis	38
Table 4.1-5 Cabinet of MELTAC Platform Specifications	45
Table 4.2-1 Explanation of the Screen	70
Table 4.2-2 Data Details	72
Table 4.3-1 Configuration of Control Network	76
Table 4.3-2 The Specification of Control Network	79
Table 4.3-3 Self-Diagnosis Functions of Control Network	83
Table 4.4-1 Description of Processing in Each Component (maximum/minimum values)	92
Table 5.3-1 MELTAC Modules for the EMC Test	109
Table 6.1-1 Conformance of the MELCO Quality Program to 10CFR50 Appendix B	121
Table 6.1-2 Contents of Activity in Each Phase	126
Table 6.1-3 Contents of Hardware Development Activity in Each Phase	128
Table 6.1-4 Security Measures of the Software Development/Storage Environment	133
Table 6.1-5 Security Measures in the Software Development Process	134
Table 6.1-6 Classification of Previously Developed Software Units	137
Table 6.1-7 Information Provided in Maintenance Manual	141
Table 6.1-8 Hardware Measurement	143
Table 6.1-9 Software Upgrades Relation	144
Table 6.1-10 Possible Hazards	145
Table 7.5-1 List of Periodic Replacement Parts	161

List of Figures

Figure 4.0-1 Typical configuration of MELTAC Platform.....	21
Figure 4.1-1 Single Controller Configuration.....	23
Figure 4.1-2 Redundant Parallel Controller Configuration	25
Figure 4.1-3 Redundant Standby Controller Configuration	27
Figure 4.1-4 Picture of Modules in a CPU Chassis for a Redundant Standby Controller Configuration	28
Figure 4.1-5 Mode Management of Single Controller and Redundant Parallel.....	30
Figure 4.1-6 Mode Management of Redundant Standby Controller	32
Figure 4.1-7 Location of Isolation Module	42
Figure 4.1-8 Cabinet External Dimensions and Rack Up as a Sample.....	46
Figure 4.1-9 Configuration of Power Supply for Controller Cabinet	47
Figure 4.1-10 Basic Software Processes and Execution Order	48
Figure 4.1-11 Coverage of Self-diagnosis function of the controller	57
Figure 4.2-1 Configuration of Safety VDU Processor	64
Figure 4.2-2 Configuration of Power Supply for Safety VDU	66
Figure 4.2-3 Software Structure of Safety VDU Processor	67
Figure 4.2-4 Screen Transition of the Safety VDU Processor.....	69
Figure 4.2-5 A Sample of Operation Switch Pictogram on the Safety VDU Panel.....	71
Figure 4.2-6 Explanation of the Safety VDU Processor Operation	73
Figure 4.3-1 Configuration of Control Network.....	77
Figure 4.3-2 Explanation of Bypass Operation by the Optical Switch.....	78
Figure 4.3-3 Protocol Stack of Control Network.....	79
Figure 4.3-4 Separation in Communication of Control Network.....	82
Figure 4.3-5 Data Link Configuration	84
Figure 4.3-6 Separation in Communication of Data Link	85
Figure 4.3-7 Maintenance Network Configuration.....	86
Figure 4.3-8 Separation in Communication of Maintenance Network.....	87
Figure 4.4-1 The Time Chart of Fundamental Process in Cyclic	89
Figure 4.4-2 Internal Process Divisions of the MELTAC Platform to Perform Response Time Calculations	91
Figure 6.1-1 Outline of In-house QA Procedures System and Relationship of Various Plans.....	120
Figure 6.1-2 Outline of Software Development Plan.....	125
Figure 6.1-3 Outline of Problem Tracking/Resolution Process	127
Figure 6.1-4 Security Measures of the Software Development/Storage Environment...	132
Figure 6.1-5 Software Installation	140
Figure 7.1-1 MELTAC Development and Operating History	150
Figure 7.3-1 Reliability Model.....	153
Figure 7.3-2 Fault Tree for Output Failure Spurious Actuation	154
Figure 7.3-3 Fault Tree for Failure to Actuate	155
Figure 7.3-4 Reliability Model of Subsystem.....	156
Figure 7.3-5 Fault Tree of Subsystem.....	156
Figure 7.3-6 Reliability Model of Dedicated I/O	157
Figure 7.3-7 Fault Tree of Dedicated I/O	157
Figure 7.3-8 Input/Output Line	158
Figure 7.3-9 Fault Tree of Input/Output Line.....	158
Figure 7.5-1 Failure Rate Curve.....	160

This page is intentionally left blank.

List of Acronyms

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

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

1.0 PURPOSE

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

The MELTAC Platform is applied to the Protection and Safety Monitoring System, which includes the Reactor Protection System, Engineered Safety Feature Actuation System, Safety Logic System, Safety Grade HSI System, and any other safety system. In addition, the MELTAC Platform is applied to non-safety systems such as the Plant Control and Monitoring System. The MELTAC equipment applied for non-safety applications is the same design as the equipment for safety applications. However, there are differences in Quality Assurance methods for software design and other software life cycle processes.

The goal of this report is to seek approval from the U.S. Nuclear Regulatory Commission for the use of the MELTAC Platform for nuclear safety systems in new reactors and in operating plants.

2.0 SCOPE

The scope of this report includes the hardware and software associated with the MELTAC Platform. The MELTAC Platform described herein encompasses design, qualification, and reliability.

The MELTAC Platform will be used for the safety systems of new plants (US-APWR) and operating plants.

3.0 APPLICABLE CODE, STANDARDS AND REGULATORY GUIDANCE

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

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

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

Code of Federal Regulations

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

GDC 1: Quality Standards and Records

The current Quality Assurance program meets the requirements of 10CFR50 Appendix B. An assessment of the QA program in place during the original development of this Equipment is provided in this TR.

GDC 2: Design Bases For Protection Against Natural Phenomena

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

GDC 4: Environmental And Dynamic Effects Design Bases

This Equipment is located in a mild environment that is not adversely effected by plant accidents.

GDC 5: Sharing of Structures, Systems, and Components

In general, there is no sharing of this Equipment among nuclear power units. Any sharing is discussed in specific Plant Licensing Documentation.

GDC 12: Suppression Of Reactor Power Oscillations

Specific reactor trip functions implemented within this Equipment are described in Plant Licensing Documentation.

GDC 13: Instrumentation And Control

Specific instrumentation and control functions implemented within this Equipment are described in Plant Licensing Documentation.

GDC 17: Electric Power Systems

The electric power sources for this Equipment and the plant components controlled by this Equipment are discussed in Plant Licensing Documentation. This document describes the interface requirements for these power sources.

GDC 19: Control Room

This Equipment provides safety related Human System Interfaces (HSI) for the control room. The MHI non-safety digital I&C systems and the MELCO non-safety digital I&C platform provide non-safety HSI for the control room. The Human Factors design aspects of the HSI and the control room design are described in other digital system licensing documentation.

GDC 20: Protection System Functions

Specific protection system functions implemented within this Equipment are described in Plant Licensing Documentation.

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. Most manual tests may be conducted with the plant on line, and with the Equipment bypassed or out of service. Equipment that cannot be tested with the plant on line can be tested with the plant shutdown. 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 other digital system 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 the Safety I&C System Description and Design Process Topical Report and Plant 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 effect multiple divisions. The qualification limits of this equipment are described in this Topical Report. The Safety I&C System Description and Design Process Topical Report describes the analysis methods used to demonstrate conformance to those limits for actual plant conditions. Plant 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 are described in the Safety I&C System Description and Design Process Topical Report. Administrative controls are described in Plant 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 ESFAS functions are described in the Safety I&C System Description and Design Process Topical Report.

GDC 24: Separation of Protection and Control Systems

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 in the control system prevents 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 ensures prioritization of safety functions.

GDC 25: Protection System Requirements For Reactivity Control Malfunctions

Specific functions implemented within this Equipment to protect against Reactivity Control Malfunctions are described in Plant Licensing Documentation. Specific features designed into the MHI non-safety control systems to limit the extent of Reactivity Control Malfunctions is described in Plant Licensing Documentation.

GDC 29: Protection Against Anticipated Operation Occurrences

The Equipment achieves an extremely high probability of accomplishing its safety functions through components with conservative design margins, redundancy to accommodate random failures, a quality program that minimizes the potential for design or manufacturing errors.

2. 10CFR50.34 (f)(2) Post-TMI Requirements**(iii) Control room**

The Human Factors design aspects of the HSI and the control room are described in the HSI Topical Report and other digital system plant licensing documentation.

(iv) Safety Parameter Display

The non-safety HSI systems provide safety parameter displays in the control room. Some data presented on safety parameter displays originates in this Equipment.

(v) Bypassed and inoperable status indication

This indication is provided by this Equipment and by the non-safety HSI system. All bypassed or inoperable signals for safety systems originate in this Equipment.

- (xi) Relief and safety valve position Indication
- (xii) Auxiliary feedwater system initiation and flow indication
- (xiii) Pressurizer heater control
- (xiv) Containment isolation systems
- (xvii) Accident monitoring instrumentation
- (xviii) Inadequate core cooling monitoring
- (xix) Instruments for monitoring plant conditions following core damage
- (xx) Pressurizer level indication and controls for pressurizer relief and block valves

Specific functions implemented within this Equipment to meet the Post-TMI requirements, items xi thru xx above, are described in Plant Licensing Documentation.

3. 10 CFR 50.36 Technical specifications

1) Safety limits, limiting safety system settings, and limiting control settings.

This Equipment is used in digital safety systems to maintain safety limits. The MELCO non-safety digital I&C platform is used in non-safety control systems to maintain control limits.

2) Limiting conditions for operation.

This Equipment can be configured at the application level with N or N+1 redundancy, as discussed above for conformance to GDC 21. The Limiting Conditions for Operation (LCO) related to bypassed or out of service conditions for a single division are dependent upon the extent of redundancy. The Safety I&C System Description and Design Process Topical Report describes the LCO for this Equipment.

3) Surveillance requirements

This Equipment includes extensive self-diagnostic testing, as discussed above for conformance to GDC 21. Provisions are included for periodic surveillances to confirm the operability of the self-diagnostic test features. Provisions can also be included at that application level to manually test features of the system that are not tested automatically. The test interval for all manual tests is based, in part, on Equipment reliability which is described in this report. Specific manual surveillance features are described in the Safety I&C System Description and Design Process Topical Report.

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

This Equipment is located in a mild environment. A mild environment is an environment that would at no time be significantly more severe than the

environment that would occur during normal plant operation, including anticipated operational occurrences. Therefore this criteria is not applicable. This criteria is applicable to some instrumentation that interfaces to this Equipment. The qualification of this instrumentation is described in Plant Licensing Documentation.

5. 10 CFR 50.55a

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

This Equipment was originally developed under a Japanese nuclear quality program that is equivalent to 10CFR50 Appendix B. Other licensing documents describe this equivalence. An approved 10CFR 50 Appendix B quality program is now in effect for all Equipment.

(h) Invokes IEEE Std. 603-1991

See conformance to IEEE 603-1991

6. 10 CFR 50.62 ATWS Rule

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

7. 10 CFR 52.47

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

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

(a)(1)(vii) Interface Requirements

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

(a)(2) Level of Detail

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

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

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

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

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

Staff Requirements Memoranda

9. SRM to SECY 93-087

II.Q Defense Against Common-Mode Failures in Digital I&C Systems

Conformance is described in the Defense-in-Depth and Diversity Topical Report.

II.T Control Room Annunciator (Alarm) Reliability

This Equipment and the MHI non-safety I&C systems can be configured at the application level to generate alarms. Alarm annunciators are provided by the MHI non-safety HSI system. Conformance to requirements for redundancy, and conformance to separation and independence criteria between safety divisions and between safety and non-safety divisions is described in the Safety I&C System Description and Design Process Topical Report.

NRC Regulatory Guides

10. RG 1.22 Periodic Testing of Protection System Actuation Functions

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

11. RG 1.29 Revision 03 Seismic Design Classification

The Equipment is designated Seismic Category I.

12. RG 1.47 Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems

See conformance to 10CFR50.34 (f)(2)(v). The Equipment can be configured at the application level so that alarms are provided for all bypassed or inoperable safety functions. The ability to manually actuate bypassed or inoperable alarms can also be configured for conditions that are not automatically detected. The

detail is described in the Safety I&C System Description and Design Process Topical Report.

13. RG 1.53 Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems

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 can not prevent proper protective action at the system level. Single failures considered in the divisions are described in the Failure Modes and Effects Analyses (FMEA) for each system. The FMEA method for the components of this Equipment is provided in this Topical Report. The FMEA method for specific plant applications is described in the Safety I&C System Description and Design Process Topical Report. The actual plant specific FMEA is described in Plant Licensing Documentation .

14. RG 1.62 Manual Initiation of Protective Actions

The Equipment can be configured at the application level so that all RPS and ESFAS safety functions can be manually initiated at the system level by conventional switches located in the main control room. Additional system level manual initiation switches may also be located at the Remote Shutdown panel, depending on the specific plant design; these are described in Plant Licensing Documentation . The Equipment can be configured at the application level so that manual initiation requires a minimum of Equipment, the Equipment common to manual and automatic initiation paths is kept to a minimum and no credible single failure in the manual, automatic or common portions will prevent initiation of a protective action by manual or automatic means. Manual initiation is described in the Safety I&C System Description and Design Process Topical Report.

15. RG 1.75 Physical Independence of Electric Systems

endorses IEEE 384-1992

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. Conventional isolators prevent propagation of transverse and common mode faults from the maximum credible energy source. Fiber optic cable communication interfaces, and specifications and qualification of conventional isolators are discussed in this Topical Report.

-
16. RG 1.89 Qualification for Class 1E Equipment for Nuclear Power Plants
endorses IEEE323-1974
The environmental qualification of this Equipment is by an appropriate combination of type testing and analysis. This Equipment is located in a mild environment that is not adversely effected by plant accidents. Therefore qualification for radiation is by analysis of component specifications. Qualification for temperature and humidity is by type test, and by analysis of room ambient conditions and heat rise calculations for the installed configuration. Seismic qualification and EMI qualification are by type testing. This Equipment has no known aging mechanisms, except as noted in Section 7.5; random failures will be detected through self-diagnostics and periodic surveillance testing. Type testing for conformance to RG 1.89 is described through the aggregate of all qualification reports – Environmental, Seismic and EMC, see section 5.
17. RG 1.97 Instrumentation for Light Water Cooled Nuclear Power Plants to Assess Plant Conditions During and Following an Accident
endorses IEEE Std. 497-2002
This Equipment is used to process and display signals from accident monitoring instrumentation of all variable Types. It meets all the applicable requirements. Signals from some accident monitoring instrumentation are also transmitted from this Equipment to the non-safety HSI system for displays and alarms. Independence is maintained between all divisions. Specific accident monitoring instrumentation is described in Plant Licensing Documentation .
18. RG 1.100 Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants

This Equipment is designated Seismic Category I. It is designed and qualified to withstand the cumulative effects of a minimum of five (5) Operational Basis Earthquakes (OBEs) and one (1) 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 Plant Licensing Documentation .
19. RG 1.105 Setpoints for Safety-Related Instrumentation
endorses ISA-S67.04-1994 and ANS-10.4-1987
The uncertainties associated with the Equipment are described in this Topical Report. This includes uncertainties for signal conditioning modules, signal splitters, instrument loop power suppliers and analog to digital converters. The uncertainties associated with specific process instrumentation and the resulting safety related setpoints are described in Plant Licensing Documentation. The methodology used to combine all uncertainties to establish safety related setpoints is described in the Safety I&C System Description and Design Process. Topical Report. The plant specific uncertainty/setpoint analysis is described in Plant Licensing Documentation.
-

-
20. RG 1.118 Periodic Testing of Electric Power and Protection Systems
endorses IEEE 338-1987
See conformance to GDC 21, 10CFR50.36 and RG 1.22. The Equipment can be configured so that all safety functions are tested either automatically or manually, and so that manual tests do not require any system reconfiguration, such as jumpers or fuse removal. The periodic test features are described in the Safety I&C System Description and Design Process Topical Report.
21. RG 1.151 Instrument Sensing Lines
endorses ISA-S67.02
Compliance is described in Plant Licensing Documentation .
22. RG 1.152 Criteria for Programmable Digital Computers in Safety Systems of Nuclear Power Plants
endorses IEEE 7-4.3.2-2003
The methods used for specifying, designing, verifying, validating and maintaining software for this Equipment conforms to these requirements. The life cycle process for the digital platform software is described in this Topical Report. The life cycle process for the system application software is described in the Safety I&C System Description and Design Process Topical Report. The methods used for controlling cyber threats throughout the life cycle are described in these documents.
23. RG 1.153 1996 Criteria for Safety Systems
endorses IEEE Std 603-1991
Compliance with the General Design Criterion identified in this Regulatory Guide is discussed above. Compliance with IEEE 603-1991 is discussed below.
24. RG 1.168 Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
endorses IEEE Std 1012-1998 and IEEE Std 1028-1997
This Equipment uses processes for verification, validation, reviews and audits that conform to this Regulatory Guide. The design processes for the digital platform are described in this Topical Report. The design processes for plant systems are described in the Safety I&C System Description and Design Process Topical Report.
25. RG 1.169 Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
endorses IEEE Std 828-1990 and IEEE Std 1042-1987
This Equipment is designed and maintained using a Configuration Management process that conforms to this Regulatory Guide. The Configuration Management process for the digital platform is described in this Topical Report. The Configuration Management process for plant systems is described in the Safety I&C System Description and Design Process Topical Report.
-

26. RG 1.170 Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
endorses IEEE Std 829-1983
The test documentation for this Equipment conforms to this Regulatory Guide. The test documentation for the digital platform is described in this Topical Report. The test documentation for plant systems is described in the Safety I&C System Description and Design Process Topical Report.
27. RG 1.171 Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
endorses IEEE Std 1008-1987
Unit testing for this Equipment conforms to this Regulatory Guide. This unit testing for the digital platform is described in this Topical Report. Unit testing for plant systems is described in the Safety I&C System Description and Design Process Topical Report.
28. RG 1.172 Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
endorses IEEE Std 830-1993
The Software Requirements Specifications for this Equipment conforms to this Regulatory Guide. The Software Requirements Specifications for the digital platform are described in this Topical Report. The Software Requirements Specifications for plant systems are described in the Safety I&C System Description and Design Process Topical Report.
29. RG 1.173 Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
endorses IEEE Std 1074-1995
The Software Life Cycle Process for this Equipment conforms to this Regulatory Guide. The Software Life Cycle Processes for the digital platform is described in this Topical Report. The Software Life Cycle Processes for plant systems is described in the Safety I&C System Description and Design Process Topical Report.
30. RG 1.180 Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems
endorses MIL-STD-461E, IEC 61000 Parts 3, 4, and 6, IEEE Std C62.41-1991, IEEE Std C62.45-1992, IEEE Std 1050-1996, EPRI TR-102323
This Equipment conforms to the EMI/RFI requirements of this standard. Qualification testing for the digital platform is described in this Topical Report. Requirements and features of plant systems that ensure conformance to the platform qualification envelope are described in the Safety I&C System Description and Design Process Topical Report.

NRC Branch Technical Positions

31. BTP HICB-1 Guidance on Isolation of Low-Pressure Systems from the High-Pressure Reactor Coolant System
32. BTP HICB-2 Guidance on Requirements of Motor-Operated Valves in the Emergency Core Cooling System Accumulator
33. BTP HICB-3 Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps out of Service
34. BTP HICB-4 Guidance on Design Criteria for Auxiliary Feedwater Systems
35. BTP HICB-5 Guidance on Spurious Withdrawals of Single Control Rods in Pressurized Water Reactors
36. BTP HICB-6 Guidance on Design of Instrumentation and Controls Provided to Accomplish Changeover from Injection to Recirculation Mode
Compliance with BTP HICB 1 thru 6, above, is described in Plant Licensing Documentation.
37. BTP HICB-8 Guidance for Application of Regulatory Guide 1.22
The Equipment includes extensive self-diagnostics which run continuously. The Equipment can be configured at the application level with additional manual test 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-diagnostics are described in this Topical Report. Manual test features are described in the Safety I&C System Description and Design Process Topical Report.
38. BTP HICB-9 Guidance on Requirements for Reactor Protection System Anticipatory Trips
In general there are no non-safety anticipatory trips used in the protection system. Any exception to this will be described in Plant Licensing Documentation. If any non-safety trips are used in the protection system the Equipment can be configured at the application level to meet the following requirements:

- All non-safety equipment can be isolated from the safety system to prevent electrical fault propagation and adverse communication interaction.
- Safety functions can have priority over all non-safety functions.

39. BTP HICB-10 Guidance on Application of Regulatory Guide 1.97

The Equipment conforms to this BTP for processing all instrumentation signals. However, RG 1.97 Revision 4 has superseded Revisions 2 and 3, for which this BTP was written. Therefore, where there are conflicts, the Equipment meets the requirements of RG 1.97 Revision 4.

40. BTP HICB-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.

41. BTP HICB-12 Guidance on Establishing and Maintaining Instrument Setpoints
See conformance to RG 1.105.

42. BTP HICB-13 Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors

The methods used for periodically verifying the accuracy and response time of RTDs conforms to this standard. The method is described in Plant Licensing Documentation.

43. BTP HICB-14 Guidance on SW Reviews for Digital Computer-Based I&C Systems

endorses IEEE Std 730

See conformance to RG 1.168 thru 1.173.

44. RG1.206 Combined License Applications for Nuclear Power Plants (LWR Edition)

For the MELTAC Platform described in this Topical Report, there is no Design Acceptance Criteria (DAC). The level of detail provided in this report conforms to this Regulatory Guide and is expected to be sufficient for the NRC staff to make a final safety determination regarding the suitability of the MELTAC Platform for safety related applications. This document is intended to supplement the information provided in COL applications. This document may be referenced directly or indirectly (via reference to a certified design, which references this document).

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

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

46. BTP HICB-18 Guidance on Use of Programmable Logic Controllers in Digital Computer-Based I&C Systems
This Equipment is not a commercial-grade computer system; it was designed originally for nuclear safety applications in Japan. Since it has been deployed in numerous non-safety nuclear applications in Japan and will be deployed in nuclear safety applications in Japan in the near future. All of this operating experience in Japan is directly applicable to expected nuclear safety applications in the US.
47. BTP HICB-19 Guidance on Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based I&C Systems
The MHI safety related digital I&C systems utilize the MELCO safety related digital I&C platform (ie. this Equipment). The MHI non-safety digital I&C systems utilize the MELCO non-safety digital I&C platform. The two MELCO platforms are essentially the same, however some QA aspects of design and manufacturing are not equivalent between safety and non-safety platforms. The Defense-in-Depth and Diversity Topical Report describes the functional diversity within the safety and non-safety I&C systems. The report also describes the methodology for coping with a common cause failure of all of these systems and provides an example of this methodology for one Design Basis Accident (DBA). Coping for all Design Basis Accidents (DBAs) is described in Plant Licensing Documentation.
48. BTP HICB-21 Guidance on Digital Computer Real-Time Performance
The real-time performance for this Equipment conforms to this BTP. The method for determining response time performance for plant systems (including the digital platform) is described in the Safety I&C System Description and Design Process Topical Report. The response time performance for digital platform components is described in 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 Plant Licensing Documentation.

NUREG-Series Publications (NRC Reports)

49. 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 MHI non-safety HSI system which can provide this display for the control room and for emergency support facilities.

- Indication and Control for Safety Components (eg. 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 MHI non-safety HSI system.

These features are described in the Safety I&C System Description and Design Process Topical Report .

50. NUREG-0800 Chapter 7 of the USNRC Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, Rev 4
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 Plant Licensing Documentation.
51. 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. The assessment of diversity within this Equipment and between this Equipment and other I&C systems is described in the Diversity and Defense-in-Depth Topical Report. The Diversity and Defense-in-Depth Topical Report also describes the method of coping with common mode failure vulnerabilities.
52. 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.

IEEE Standards

53. IEEE 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, including key requirements for:
- Software quality and life cycle processes
 - Independent Verification and Validation
 - Communications independence
- Conformance is described in Sections 4 through 6.
54. IEEE 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.

-
- | | |
|-----|--|
| 55. | <p>IEEE 338 1987 Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems</p> <p>The self-diagnostics that are credited for Periodic Surveillance Testing are described throughout this document. As described in RG 1.22 item 10, RG1.22 and IEEE338 test features that are configured at the system level or within the application software are not described in this Topical Report but in "Safety I&C System Description and Design Process Topical report".</p> |
| 56. | <p>IEEE 344 1987 Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations</p> <p>This Equipment conforms to this standard as augmented by RG 1.100. Conformance is described in the Seismic Qualification Report.</p> |
| 57. | <p>IEEE 379 2000 Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems</p> <p>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. The system configuration for nuclear safety applications is provided in MUAP-07004.</p> |
| 58. | <p>IEEE 383 1974 Type Test of Class 1E Electric Cables, Field Splices, and Connections for Nuclear Power Generating Stations</p> <p>The cable and electrical connections used within this Equipment and between this Equipment conform to this standard, including requirements for flame retarding qualification requirements. Cables for interfaces to/from this equipment to other I&C systems and components are discussed in Plant Licensing Documentation.</p> |
| 59. | <p>IEEE 384 1992 Criteria for Independence of Class 1E Equipment and Circuits</p> <p>This Equipment conforms to this standard as augmented by RG 1.75. All safety functions are implemented within multiple divisions with physical separation and electrical independence between redundant safety divisions and between safety and non-safety divisions. Electrical independence is accomplished primarily through the use of fiber optic technology. Independence of electrical circuits is accomplished with isolators and physical separation or barriers, such as conduits. MELTAC components credited for physical, electrical, and functional isolations and independences are described in Section 4 (4.3.2.3, 4.3.3.2, 4.3.4.2) of this Topical Report. These components are used for interfaces between safety divisions and between safety and non-safety divisions, as described at the system level in MUAP-07004.</p> |
| 60. | <p>IEEE 420 1982 Design and Qualification of Class 1E Control Board, Panels and Racks.</p> <p>Standard enclosures for this Equipment conform to this standard. These enclosures are described in this Topical Report. Other enclosures, including any deviations from this standard, are described in Plant Licensing Documentation.</p> |
-

61. IEEE 472 IEEE Guide for Surge Withstand Capability (SWC) Tests
Input/Output modules used within this Equipment conform to this standard. Conformance to surge withstand requirements is described in the EMC Qualification Report.
62. IEEE 494 1974 Method for identification of Documents Related to 1E Equipment.
The documentation for this Equipment conforms to this standard by having the term "Nuclear Safety Related" applied on the face of each document and drawing that is provided to the licensee. Generic documents and drawings used only for internal use by MELCO do not contain this designation.
63. IEEE 497 2002 Accident Monitoring Instrumentation for Nuclear Power Generating Stations
See conformance for RG 1.97.
64. IEEE 603 1991 Safety Systems for Nuclear Power Generating Stations
1998 version is currently not endorsed by NRC
This Equipment conforms to this standard, as augmented by RG 1.153, including key requirements for:
- Single failures
 - Completion of Protective Action
 - Quality
 - Qualification
 - Independence
 - Testability
 - Monitoring and Information
 - Bypasses
- Conformance is described in Sections 4 through 7. MUAP-07004 Appendix A provides a detailed conformance assessment at the system level.
65. IEEE 730 1989 Software Quality Assurance Plans
The Software Quality Assurance Plans are described in Section 6. Common elements that do not depend on individual projects are described in []. Project-dependent individual elements are described in the Project Plan and the Software V&V Plan.
66. IEEE 828 1990 IEEE Standard for Software Configuration Management Plans
The software Configuration Management Plan is described in Section 6.1.5. It is controlled by internal documents [] and [].

-
- | | |
|-----|---|
| 67. | <p>IEEE 829 1983 Software Test Documentation</p> <p>The software test documentation is described in Section 6.1.4. It is controlled by internal documents [] and [].</p> |
| 68. | <p>IEEE 830 1993 IEEE Recommended Practice for Software Requirements Specifications</p> <p>The software requirements are documented in the "Safety System Digital Platform MELTAC-Nplus System Specification", which is described in Section 6.1.4.</p> |
| 69. | <p>IEEE 1008 1987 IEEE Standard for Software Unit Testing</p> <p>Software unit testing is described in Section 6.1.4. It is controlled by [] and [].</p> |
| 70. | <p>IEEE 1012 1998 IEEE Standard for Software Verification and Validation Plans (2004 not yet endorsed by NRC)</p> <p>Software V&V is described in Section 6.1.4. It is controlled by [].</p> |
| 71. | <p>IEEE 1016 1987 IEEE Recommended Practice for Software Design Descriptions</p> <p>The Software Design Description is documented in the "Safety System Digital Platform MELTAC-Nplus Software Specification", which is described in Section 6.1.4.</p> |
| 72. | <p>IEEE 1028 1997 IEEE Standard for Software Reviews and Audits</p> <p>Software reviews and audits are described in Section 6.1. Reviews and audits are controlled by [], [], and [].</p> |
| 73. | <p>IEEE 1042 1987 IEEE Guide To Software Configuration Management</p> <p>Configuration Management is described in Section 6.1.5. It is controlled by [] and [].</p> |
| 74. | <p>IEEE 1074 1995 IEEE Std for Developing Software Life Cycle Processes
1997 version not yet endorsed by NRC</p> <p>The software life cycle process is described in Section 6. It is controlled by [], [], [], and [].</p> |
| 75. | <p>IEEE 497 2002 Accident Monitoring Instrumentation for Nuclear Power Generating Stations</p> <p>See conformance for RG 1.97.</p> |
| 76. | <p>IEEE 896 1991 Standard For Futurebus+® - Logical and Physical Layers</p> <p>The communication between Modules in the same Subsystem of the MELTAC Platform conforms to this standard.</p> |
-

Other Industry Standards

- | | | |
|-----|--|--|
| 77. | <p>ANS-10.4 1987 Guidelines for the Verification and Validation of Scientific and Engineering Computer Programs for the Nuclear Industry</p> <p>The computer programs used to develop setpoints for this Equipment are described in the Safety I&C System Description and Design Process Topical Report.</p> | |
| 78. | <p>ANSI C62.41 IEEE Recommended Practice on Surge Voltages in Low-Voltage AC Power Circuits</p> <p>This Equipment conforms to the sections of this standard endorsed by RG 1.180.</p> | |
| 79. | <p>ANSI C62.45 IEEE Guide on Surge Testing for Equipment Connected to Low-Voltage AC Power Circuits</p> <p>This Equipment conforms to the sections of this standard endorsed by RG 1.180.</p> | |
| 80. | <p>IEC 61000 Electromagnetic compatibility (Basic EMC publication)</p> <p style="margin-left: 40px;">This Equipment conforms to the following sections of this standard:</p> <ul style="list-style-type: none"> • IEC 61000-4-2: Testing and measurement techniques - Electrostatic discharge immunity tests. Basic EMC publication • IEC 61000-4-4: Testing and measurement techniques - Electrical fast transient/burst immunity test. Basic EMC publication • IEC 61000-4-5: Testing and measurement techniques - Surge immunity test • IEC 61000-4-12: Testing and measurement techniques - Oscillatory waves immunity test. | |
| 81. | <p>ISA-S67.04 1994 Setpoints For Nuclear Safety Related Instrumentation Used in Nuclear Power Plants</p> <p>See conformance to RG 1.105. The methodology used to develop setpoints for this Equipment is described in the Safety I&C System Description and Design Process Topical Report.</p> | |
| 82. | <p>MIL-STD-461E Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment</p> <p>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.</p> | |
| 83. | <p>ISO9001: 2000 International Organisation for Standardisation Quality Management Systems</p> | |

MELCO original Quality Assurance program conforms to this standard.

Japanese Domestic Standards

- | | | |
|-----|---|--|
| 84. | JIS-C0704-1995 Insulation Test for Control Gear (in Japanese)
This standard is the defined as the Japanese Industrial Standard. The withstand voltage of this Equipment conforms to this standard. | |
| 85. | JEC-210-1981 Control Circuit Terminal Test Voltage (in Japanese)
This standard is issued by Japanese Electrotechnical Committee. The Lightning impulse resistance of this Equipment conforms to this standard. | |
| 86. | JEIDA-63-2000 Guideline for the Environmental Condition for the Industrial Information Processing and Control Equipment (in Japanese)
This standard is issued by Japan Electronics and Information Technology Industries Association. This Equipment conforms to the class B of this standard regarding dust and dirt tolerance. | |
| 87. | JEAG-4101 Guidelines for Quality Assurance in Nuclear Power Plant (in Japanese)
This standard is the guidelines for the quality assurance in the nuclear power plant in Japan and issued by Japan Electric Association. This Equipment conforms to this standard. | |

4.0 MELTAC PLATFORM DESCRIPTION

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

- Controller
- Safety VDU (Visual Display Unit) Panel
- Safety VDU Processor
- Control Network
- Data Link
- Engineering Tool
- Maintenance Network

A typical configuration of the MELTAC Platform for a safety system is described in Figure 4.0-1. Plant safety systems have multiple divisions, as described in the Safety System Topical Report. The configuration shown in Figure 4.0-1 is typical for a single division of a plant safety system, with an interface to a Controller in another division.

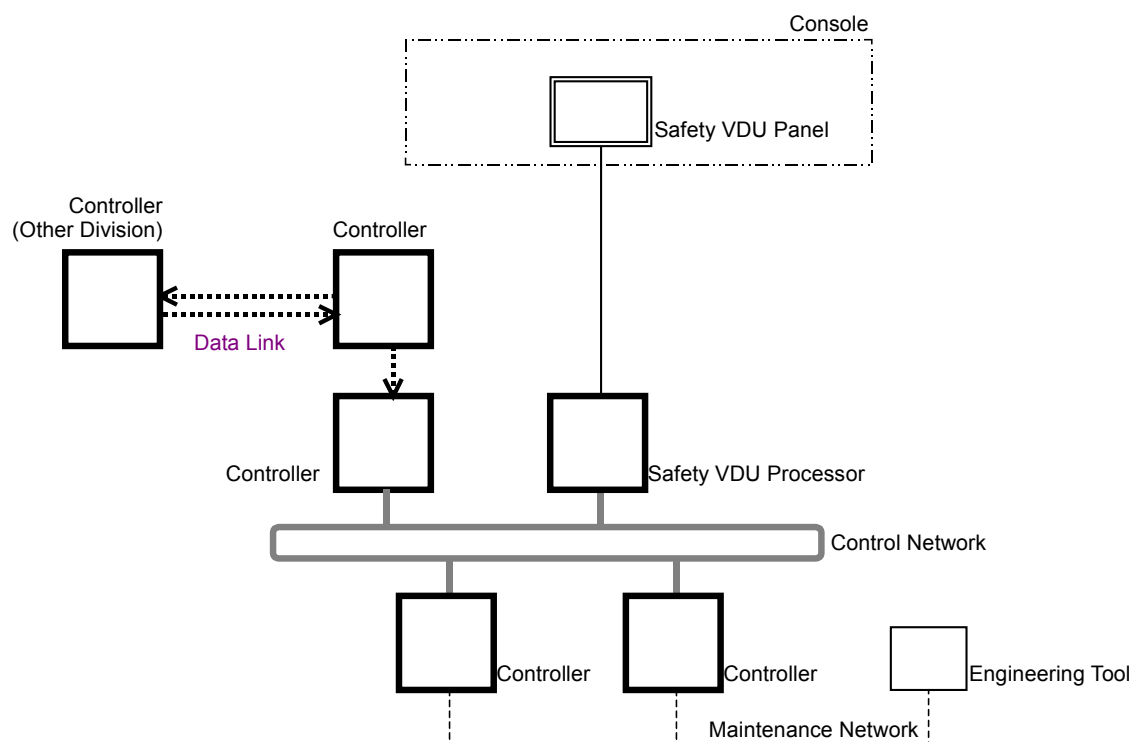


Figure 4.0-1 Typical Configuration of MELTAC Platform

4.1 Controller

4.1.1 Hardware Configuration

The Controller for the MELTAC Platform consists of the following parts.

- a) One CPU Chassis including one or two Subsystems, one Switch Panel and one Fan Unit. Each Subsystem consists of a Power Supply module, CPU Modules, Control Network I/F Module, System Management Module and two Bus Master Module. Each Subsystem communicates with the Control Network via its own Optical Switch.
- b) Multiple Input/Output (I/O) Chassis, each with multiple I/O Modules

4.1.1.1 Concept of Configuration

The MELTAC Platform is capable of taking three different kinds of configuration as shown below:

- a) Single Controller Configuration
The Controller includes one 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 two Subsystems. Each Subsystem operates in Control Mode.
- c) Redundant Standby Controller Configuration
The Controller includes two Subsystems. One 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, so that 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 three configurations may be applied to safety systems.

For redundant configuration, 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.

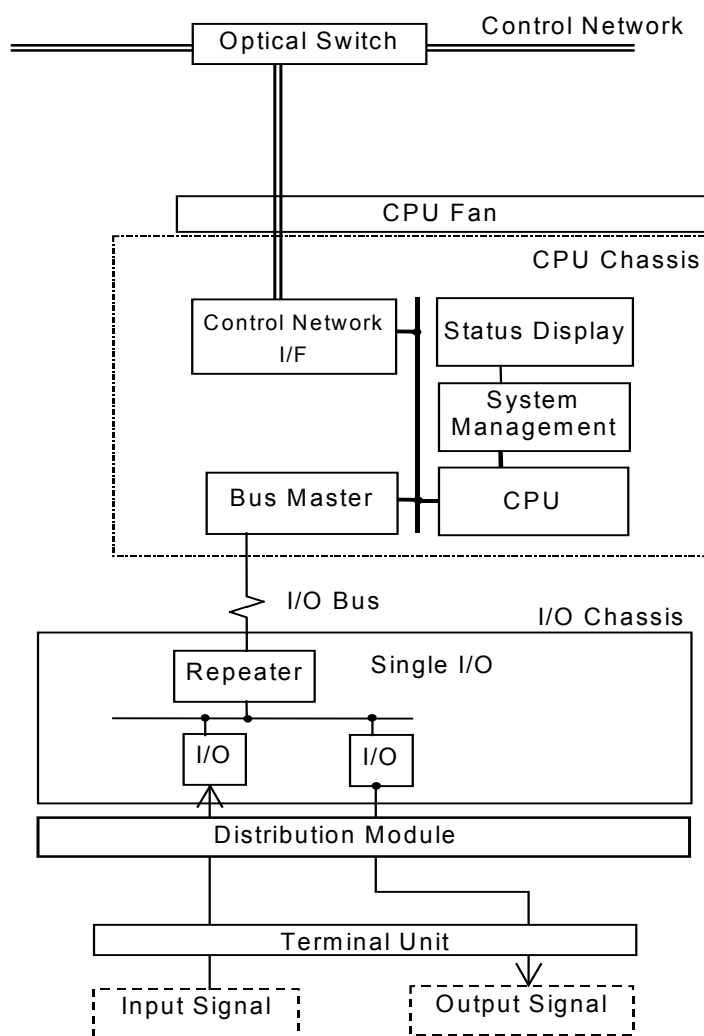


Figure 4.1-1 Single Controller Configuration

The Single Controller consists of the following:

a) CPU Chassis

The CPU Chassis includes one 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. The Subsystem is capable of taking a number of Control Network I/F Modules and Bus Master Modules depending on the scale of the application.

b) Input/Output (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 4.1-2.

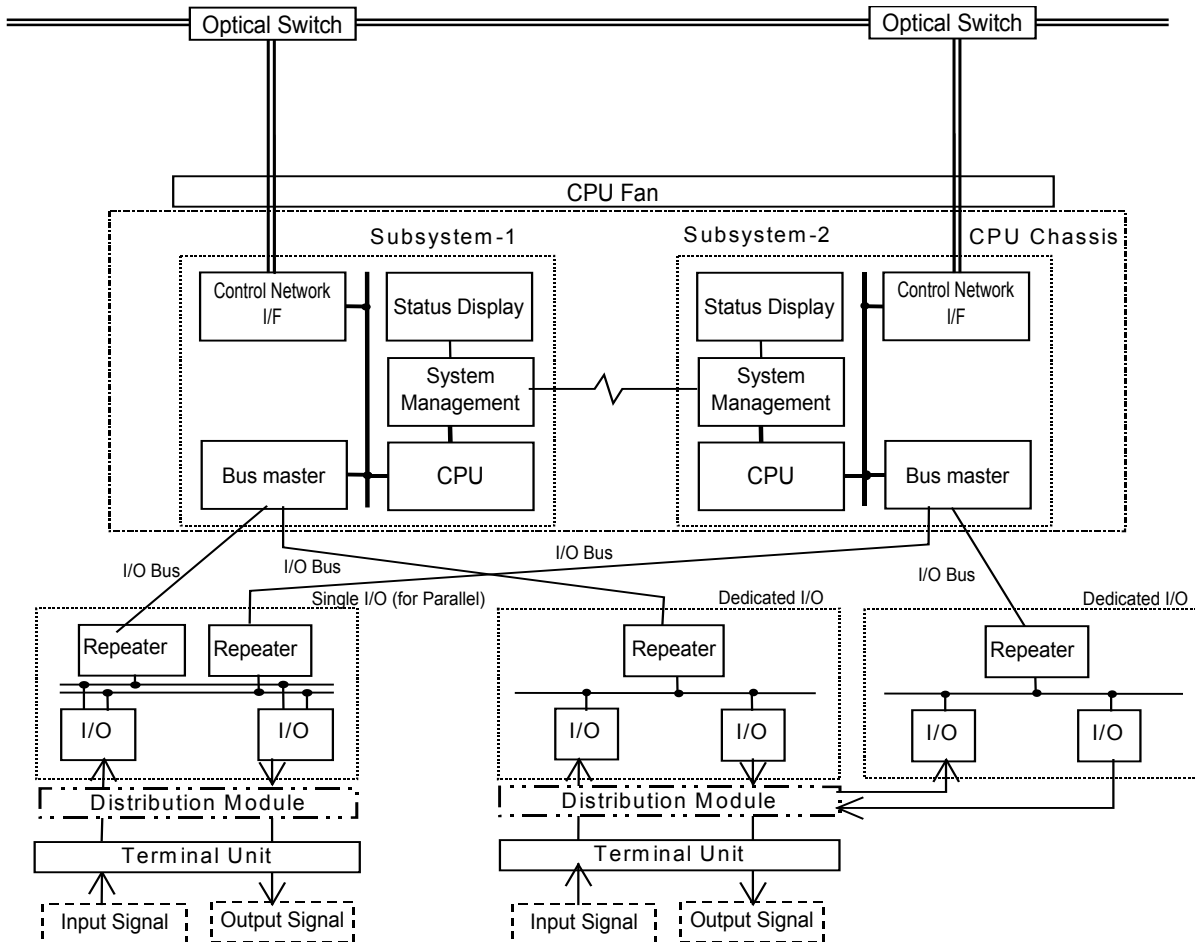


Figure 4.1-2 Redundant Parallel Controller Configuration

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 taking 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 other Subsystem is already in the Control Mode. Since both systems operate in the 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) Input/Output (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 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 two 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 one 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. Same input signals are distributed to each Dedicated I/O input module via the Distribution Module and output signals from each Subsystem are combined in the Distribution Module by using 1-out-of-2 (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 4.1-3.

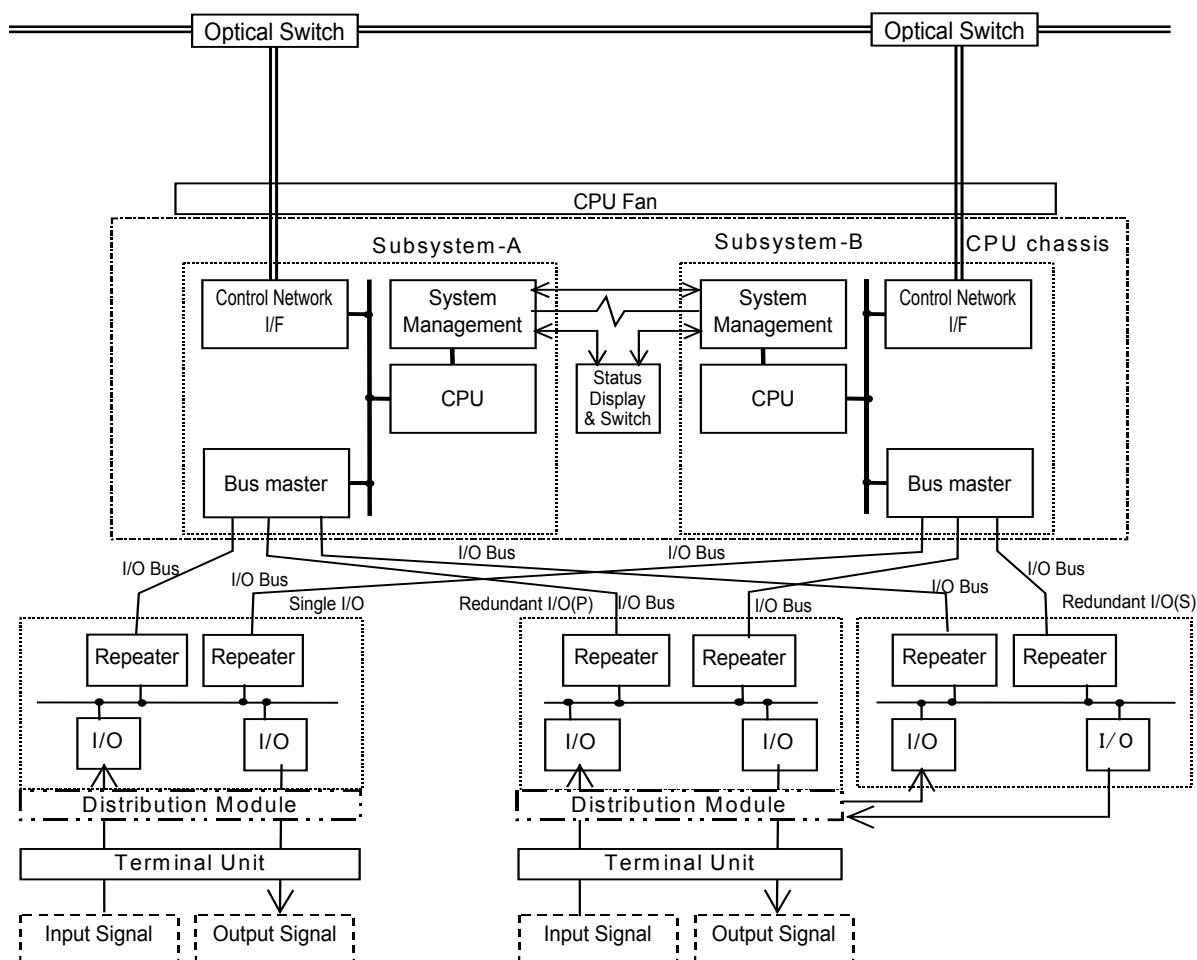


Figure 4.1-3 Redundant Standby Controller Configuration

A photograph of the MELTAC Redundant Standby Controller Configuration is shown in Figure 4.1-4.

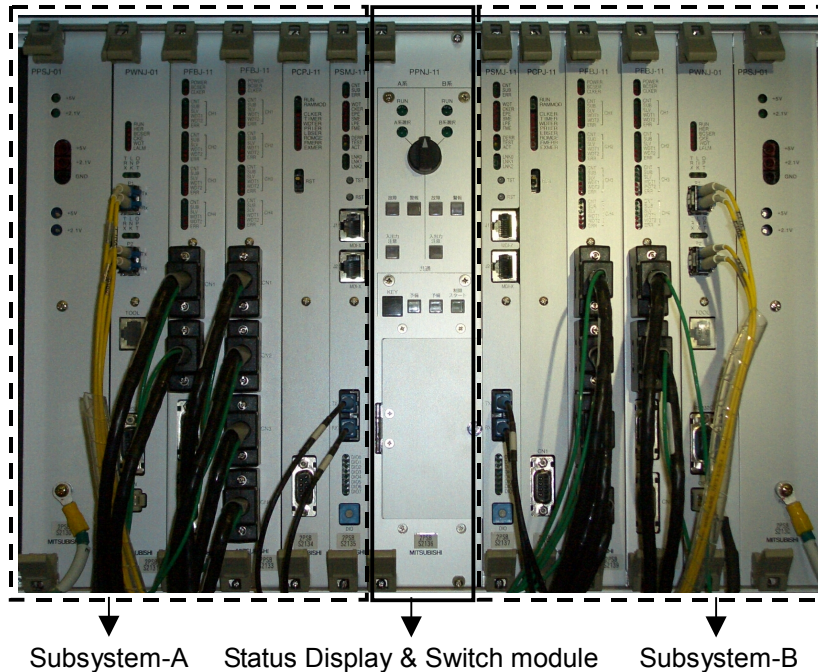


Figure 4.1-4 Picture of Modules in a CPU Chassis for a Redundant Standby Controller Configuration

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 taking 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 the Control Mode while the other one is in the Standby Mode. Each Subsystem operates independently.

When the Subsystem in the Control Mode stops operating due to a self detected fault, the Subsystem in the 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) Input/Output (I/O) Chassis

The Redundant Standby Controller includes either Redundant I/O and/or Single I/O.

The Single I/O consists of two 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 the Control Mode. When the Subsystems switch modes, communication with the I/O Modules also switches. Process input signals and output signals are connected to 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). Two 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 the Control Mode and the other is in the Standby Mode. Only the I/O Module in the Control Mode generates output signals.

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

4.1.1.2 Mode Management

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 two modes: Control Mode and Failure Mode.

Mode management of the Subsystem in a Single controller is the same as mode management of each Subsystem in a Redundant Parallel Controller.

Mode management of these controllers is shown in Figure 4.1-5.

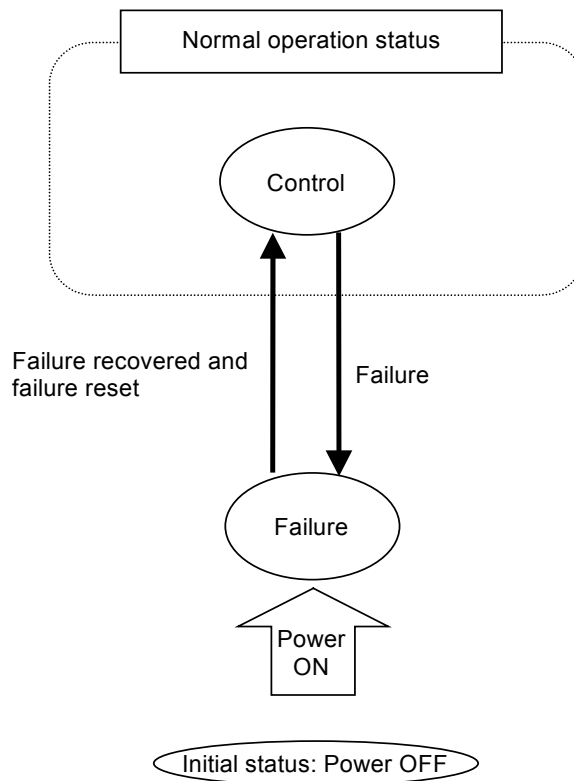


Figure 4.1-5 Mode Management of Single Controller and Redundant Parallel

The Subsystem has the following two 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-diagnostics), it automatically changes from the Control Mode to the Failure Mode. A failure signal, that can be used for external alarming, is generated for this transition.

Failure Mode: The Subsystem initializes to the Failure Mode after initial power activation. The Subsystem also shifts to this mode automatically after it detects its own failure.

A Subsystem shifts from the Failure Mode to the Control Mode only by pushing the reset button on the Status Display & Switch module.

In the Parallel Redundant Controller, Subsystem-A and Subsystem-B operate independently with the Mode Management described above.

4.1.1.2.2 Mode Management of Redundant Standby Controller

In a Redundant Standby Controller, there are three 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 4.1-6.

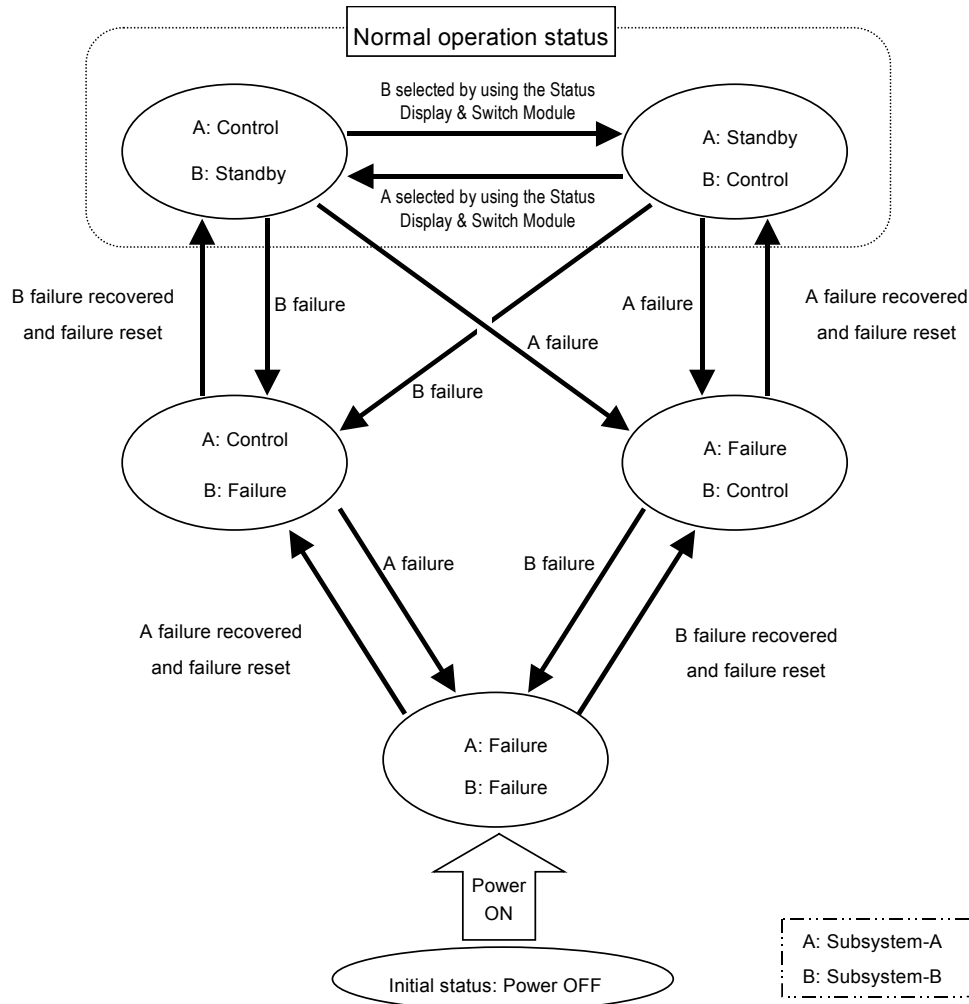


Figure 4.1-6 Mode Management of Redundant Standby Controller

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-diagnostics), it automatically changes from the Control Mode to the Failure Mode

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

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

4.1.1.3 Scale and Capacity

The scale and capacity of the MELTAC Platform Controller is described in Table 4.1-1.

Table 4.1-1 Scale and Capacity

Item	Scale/Capacity
Input/Output	I/O per controller 864 analog points, 3456 digital points, maximum
Software	Cycle time: 20 msec to 1 sec

4.1.1.4 Environmental Specifications

The MELTAC Controller is designed to operate within the environmental conditions described in Table 4.1-2.

Table 4.1-2 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) This temperature range is expected during heat/air conditioning failure conditions. 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: 5MΩ or more (500 VDC megger) (input - ground, input - DC output) Analog I/O line: 5MΩ or more (500 VDC megger) (I/O - ground, input - output) Digital I/O line: 5MΩ 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)
EMC (Electro Magnetic Compatibility)	EMI (Electro Magnetic Interference)	Complies with MIL-STD-461E for emissions: 1. Conducted emissions Conducted emissions from the power line (field discharge) CE102: High-frequency, 10kHz to 2MHz 2. Radiated emission RE101: Magnetic field, 30Hz to 100kHz RE102: Electric field, 2MHz to 10GHz

Item	Specifications	
	EMS (Electro Magnetic Susceptibility)	<p>Complies with MIL-STD-461E for susceptibility:</p> <ol style="list-style-type: none"> 1. Conducted susceptibility <ul style="list-style-type: none"> CS101: Low-frequency, 30Hz to 150kHz CS114: High-frequency, 10kHz to 30MHz CS115: bulk cable injection, impulse excitation CS116: damped sinusoidal transients, 10kHz to 100MHz 2. Radiated susceptibility <ul style="list-style-type: none"> RS103: Electric field, 30MHz to 10GHz 3. Surge to the power line <ul style="list-style-type: none"> • IEEE std 472 • Should be provided with the magnetic susceptibility for the following items included in IEC61000-4: <ul style="list-style-type: none"> - IEC61000-4-12: Ring wave - IEC61000-4-5: Surge (Switching, lightning) - IEC61000-4-4: Electrically Fast <p>Transients/bursts</p> <ol style="list-style-type: none"> 4. Static noise resistance <ul style="list-style-type: none"> IEC61000-4-2-1999 Level 2 5. Lightning impulse resistance <ul style="list-style-type: none"> AC power source line: Applied voltage 4 kV, waveform 1.2/50 μsec Digital I/O signal line: 4 kV, waveform 1.2/50 μsec Applicable standard: JEC-210-1981 (Japanese Standard) Circuit category: 6
Seismic resistance	MELTAC Cabinet (at floor mounting)	<p>Horizontal: 2.5G (X- and Y-directions)</p> <p>Vertical: 1G</p>
	MELTAC modules (at chassis mounting)	<p>Horizontal: 10G (X- and Y-directions)</p> <p>Vertical: 2G</p>
Radiation resistance	Environment in which radiation is negligible.	
Dust	<p>1.87×10^{-8} lb/ft³ (0.3 mg/m³)</p> <p>Reference standard: JEIDA-63-2000 Class B (Japanese Standard).</p>	
Corrosive gas	Environment where no corrosive gas is detected.	

4.1.2 Hardware Descriptions

4.1.2.1 CPU Chassis

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

Table 4.1-3 Module in the CPU Chassis

	Name	Model	Function
Basic Function Module	CPU Module	PCPJ-11	<ul style="list-style-type: none"> Executes Basic Software Executes Application Software, including control computation processing
	System Management Module	PSMJ-11	<ul style="list-style-type: none"> Communication between the redundant Subsystems Communication with the Engineering tool. Auxiliary DI and DO functions
Communication Module	Control Network I/F Module	PWNJ-01	Communication with the Control Network.
	Bus Master Module	PFBJ-11	<ul style="list-style-type: none"> Communication with I/O Data link communication with other Controllers <p>This module has four communication channels.</p>
Power Supply Module	CPU Power Supply Module	PPSJ-01 PPSJ-11	Supplies power to the modules within the CPU chassis.
Display & Switch Module	Status Display & Switch Module	PPNJ-11	<ul style="list-style-type: none"> Mode display LED Subsystem Mode switch Operation switch (described below) <p>This module is only used in the Redundant Standby Controller Configuration.</p>
	Status Display Module	PPNJ-12	<ul style="list-style-type: none"> Mode display LED Operation switch (described below) <p>This module is used for the Single Controller Configuration or the Redundant Parallel Controller Configuration.</p>

MELTAC has 3 types of CPU Chassis as shown in Table 4.1-4.

Table 4.1-4 CPU Chassis

Type	Use
Mirror-split CPU Chassis	- For Redundant Standby Controller Configuration
Slide-split CPU Chassis	- For Redundant Standby Controller Configuration - For Redundant Parallel 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 the 3 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 Slide-Split CPU Chassis is used. If each Subsystem in Redundant Standby Controller Configuration or a Redundant Parallel Controller Configuration has more than 5 modules, two Non-split CPU Chassis are used. If Subsystem in Single Controller Configuration has more than 5 modules a Non-split CPU Chassis is used.

4.1.2.1.1 CPU Module (PCPJ-11)

The CPU Module utilizes a 32-bit microprocessor, with enhanced speed due to the high-speed SRAM and cache. This processor module is IEEE standard Futurebus+ compliant, and performs internal operations and data transmission with modules such as the Bus Master Module and Control Network Interface Module via Futurebus+.

This module utilizes UV-ROM (Ultra-Violet Erasable Programmable Read Only Memory) for storing the Basic Software and F-ROM (Flash Electrically Erasable Programmable Read Only Memory) for storing the Application Software, such as logic symbol interconnections, setpoints and constants.

Specifications of the CPU Module are in Appendix A.1.

4.1.2.1.2 System Management Module (PSMJ-11)

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 Engineering Tool.
- Transmits and receives the changeover signal for Redundant Subsystem configurations via a dedicated backplane bus, as shown in Figure 4.1-3. In addition, this module is provided with a 2-port memory data link used for that the Standby Mode Subsystem receives operation data from the Control Mode Subsystem.

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

4.1.2.1.3 Bus Master Module (PFBJ-11)

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

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

Description of the Data Link is shown in Section 4.3.3.

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

4.1.2.1.4 Control Network I/F Module (PWNJ-01)

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

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

The description of the Control Network, including the Control Network I/F Module is shown in Section 4.3.2.

4.1.2.1.5 Status Display & Switch Module (PPNJ-11)

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

4.1.2.1.6 Status Display Module (PPNJ-12)

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

4.1.2.2 Input/Output (I/O) Modules

The I/O Modules in the MELTAC Platform include the process input/output function 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 are one analog input or output per analog I/O Module and four digital inputs or outputs per digital I/O Module.

Specifications of I/O Modules are in Appendix A.5.

4.1.2.3 Isolation Module

Isolation Modules provided electrical isolation between safety systems and non-safety systems. Analog Isolation Modules receive safety related current or RTD input signals and transmit non-safety analog output signals to other systems, without any software processing. Binary Isolation Modules receive non-safety contact inputs from other systems and transmit safety related signals to the MELTAC Power Interface Module (described below). 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. Each analog module processes one signal. Each binary module processes 2 signals.

The location of Isolation Modules is shown in Figure 4.1-7.

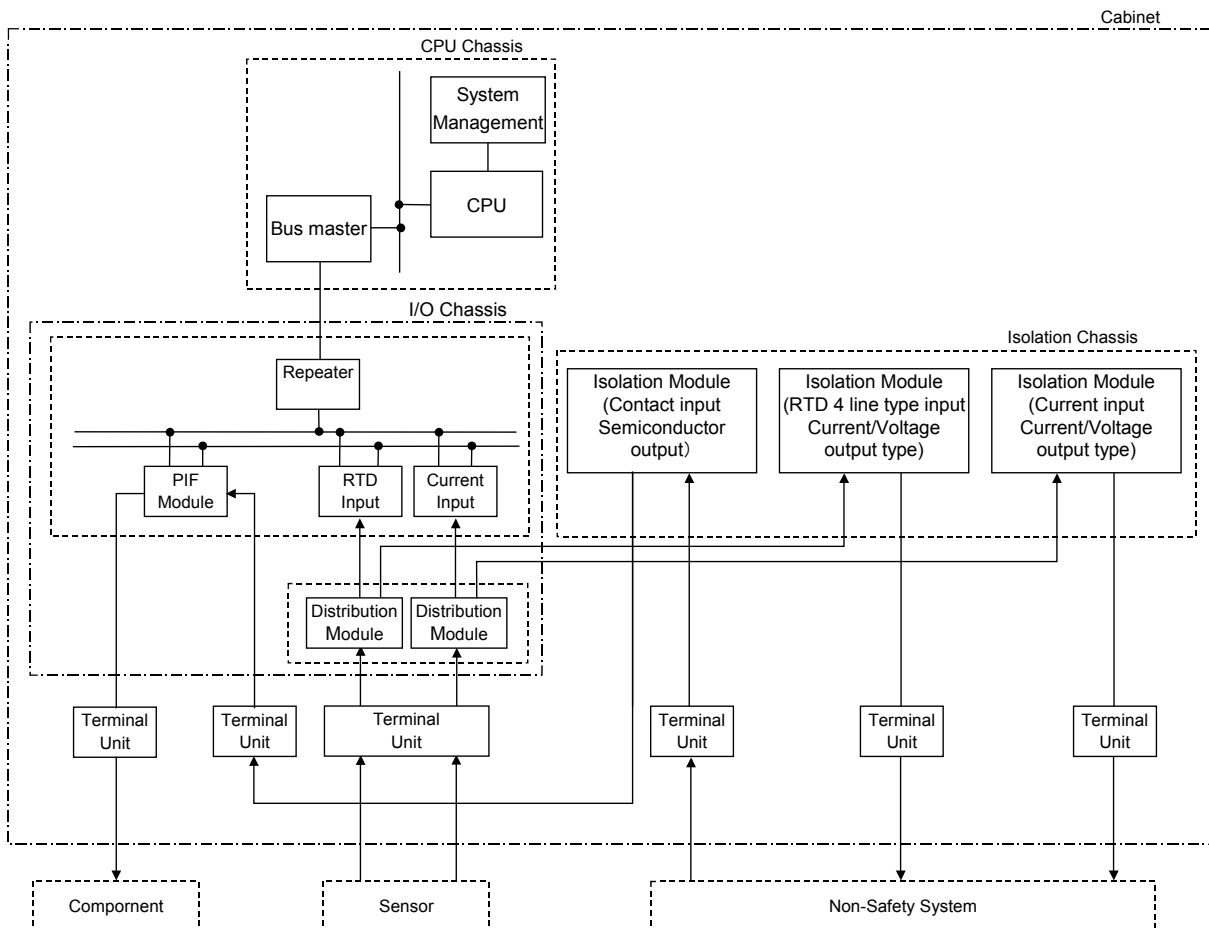


Figure 4.1-7 Location of Isolation Module

Specifications of Isolation Modules are in Appendix A.6.

4.1.2.4 Power Interface Module

The Power Interface (PIF) Modules have the same I/O Bus interfaces as in 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 Power Interface Modules include Interposing Logic (IPL) sub-boards that control the components in direct response to external contact inputs, independent of the Subsystem output commands. There are several types of IPL sub-boards, for different types of plant components (eg. switchgears, solenoid valves, etc.). Each PIF is configured with the appropriate IPL sub-board for the component being controlled. The IPL is realized by discrete logic Integrated Circuits.

Specifications of the Power Interface Module are in Appendix 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 one communication link per module.

Specifications of the E/O Converter Modules are in Appendix 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.

4.1.2.7.2 Door Fan Unit

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

4.1.2.7.3 Power Supply Fan Units

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

4.1.2.8 Power Supply Module

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

There are two types of Power Supply Modules. The CPU Power Supply (PS-1, PPSJ-01 and PPSJ-11) provides multiple outputs of +2.1VDC and +5VDC for the CPU Chassis. The I/O Power Supply (PS-2) provides +24VDC for I/O modules, Isolation Modules, Power Interface Modules, E/O Converter Modules and fan units. PPSJ-01 and PPSJ-11 are mounted in the CPU Chassis. PS-1 and PS-2 are mounted outside of the chassis.

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

The CPU Power Supply Module is also equipped with AC power input monitoring. When loss of AC power is detected, an alarm signal is sent to the Subsystem to actuate switching to the standby Subsystem.

Specifications of the Power Supply Modules are in Appendix 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

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.
- Field cables entered the back side of the cabinet (through top and/or bottom entry) and are connected to the Terminal Unit.

b) Controller Cabinet specifications

The MELTAC Platform Cabinet is described in Table 4.1-5. A typical configuration of a MELTAC Platform Cabinet is shown in Figure 4.1-8.

Table 4.1-5 Cabinet of MELTAC Platform Specifications

Item	Specifications
External dimension	2.62(W) x 2.95(D) X 7.55(H) ft (800 (W) x 900(D) x 2300(H) mm) per a cabinet
Weight	Approximately 1600 lb (750kg) per cabinet including inside modules and units.
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 rear part of the cabinet. 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 naturally-cooled.

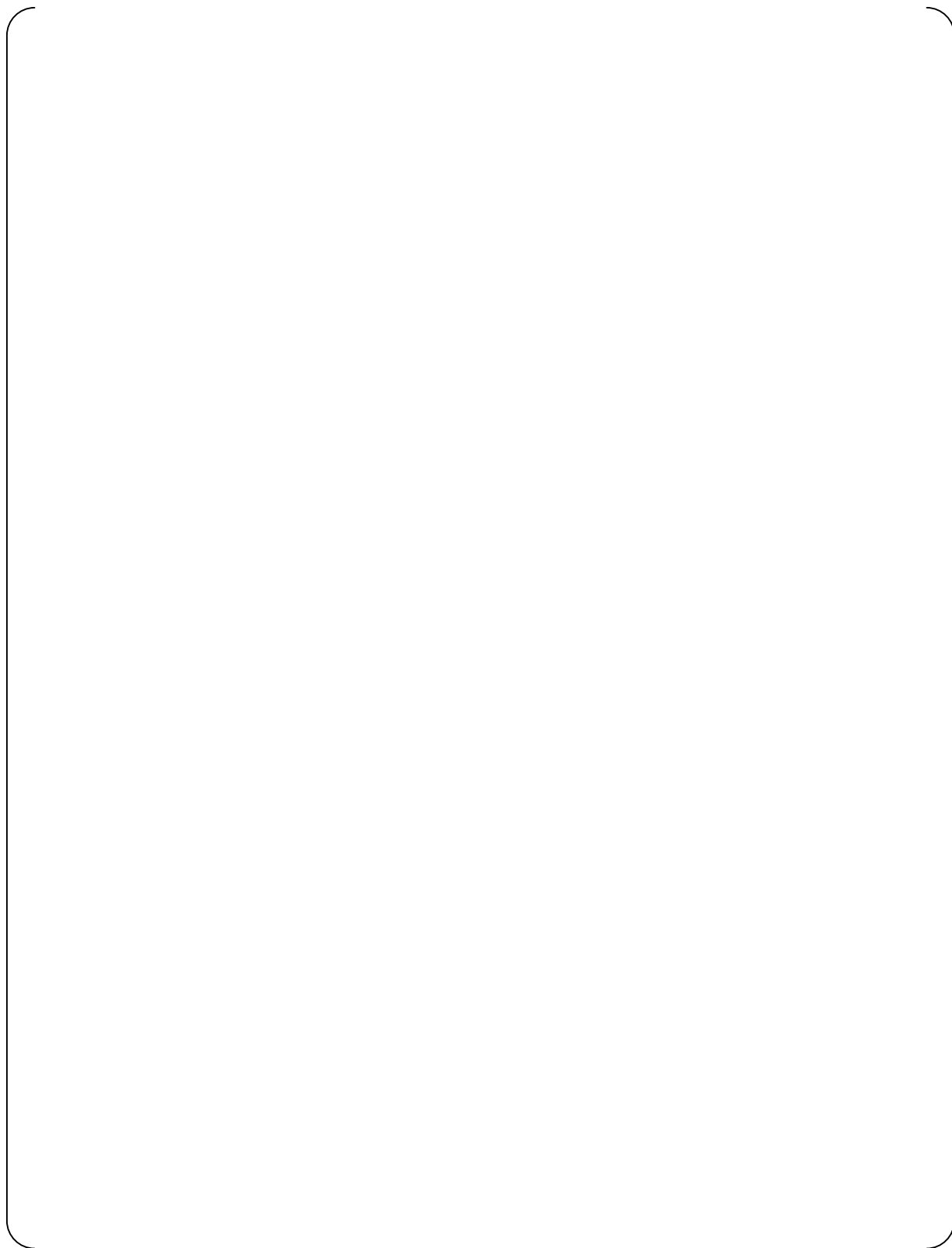


Figure 4.1-8 Cabinet External Dimensions and Rack Up as a Sample

4.1.2.10 Power Supply Configuration

Redundant AC power from two separate sources is 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 4.1-9. The two AC power sources are from within the same safety division, but should be as independent as practical. The source of AC power is described in system application documentation.

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 4.1-9 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) Interrupts are not employed for any processing other than error processing.

The processes within the Basic Software and the order of their execution are shown in Figure 4.1-10.

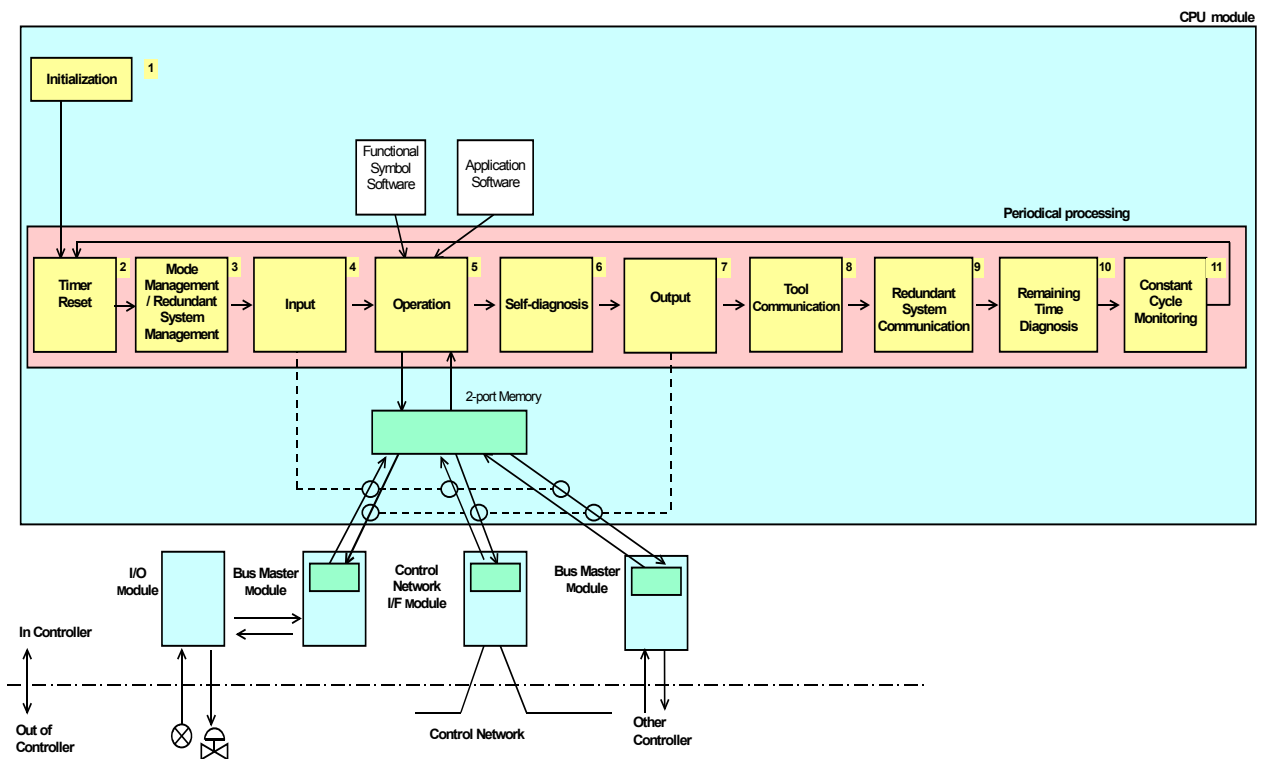


Figure 4.1-10 Basic Software Processes and Execution Order

The processing time from No.2 to No.8 is based on the application logic and the input/output signal quantity of each system. During the system design phase, the approximate processing time from No.2 to No.8 is calculated. If the processing time exceeds about 80% of the processing cycle required for the system, the application is divided into two 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.

[

1

4.1.3.2 Application Software

The Application Software of the MELTAC Platform is designed using the Engineering Tool. Application Software for functional algorithms is designed by combining simple graphical logic symbols such as “And”, “Or”, and “Not” using the Graphical User Interface (GUI) of the 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 the Application Software Graphical Block Diagrams (GBD), which are created by the I&C system designer are consistent with the Functional Block Diagrams (FBD), which are created by the process system designer.

Using the 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 Functional Symbols are listed in Appendix B.

4.1.4 Engineering Tool

The MELTAC Platform Engineering Tool (called "MELENS") provides various functions aimed at steadier and more efficient software management during all system life cycle phases (including design, fabrication, test, adjustment and maintenance).

MELENS is installed on a non-safety Personal Computer running the Microsoft Windows Operating System.

Access to MELENS is controlled by means of the PC password (BIOS, OS) and the MELENS password.

The Application Software Execution Data generated by MELENS is downloaded to the controller via the Maintenance Network and is stored in the F-ROM of the CPU Module. The functions of MELENS are described as follows.

4.1.4.1 Function Description

The functions of MELENS are as follows.

a) Creation of Application Software

The Application Software Graphical Block Diagram (GBD) is created from the Functional Block Diagrams (FBD) which is created with a commercial MITSUBISHI-made CAD software package called "RAPID". (Access to RAPID is controlled by a password.)

MELENS can automatically translate the RAPID FBD to the MELTAC GBD. MELENS can then automatically generate the Application Software Execution Data directly from the GBD by compiling.

This automated process eliminates human translation errors.

GBDs can also be created manually using the MELENS GUI editor.

Whether the GBD is generated automatically from RAPID or manually using the MELENS GUI, the assignment of GBDs to controllers and the assignment of Input/Output signals are configured manually using MELENS.

b) Download

New Application Software can be downloaded to the Controllers from the Engineering Tool PC via the Maintenance Network. This process is controlled by a hardware enable switch (write permission switch) on each Controller. Normally the switch is not enabled, because the PC and the Engineering Tool are not safety related.

c) Verifying F-ROM and UV-ROM data

The MELTAC Engineering Tool provides a manually initiated function which automatically compares the F-ROM data and UV-ROM data in the Controller, bit by bit, with the Basic Software data and Application Software data stored in MELENS. This function is used during periodic surveillance tests to confirm that the data in F-ROM and UV-ROM is the same as the data in MELENS, and therefore has not changed.

d) Controller failure diagnosis display

The MELTAC Engineering Tool displays the self-diagnostic result of the Controllers. It shows which module(s) is failed.

e) Adjustment of field changeable constants and setpoints

Constants and setpoints are adjusted by using the MELTAC Engineering Tool. This process is controlled by a hardware enable switch (Write Permission Switch) on each Controller.

4.1.4.2 Network for Engineering Tool

In order to communicate between the Engineering Tool and the Controller, the Maintenance Network is used. The Engineering Tool, which runs on a Personal Computer, is temporarily connected via the Maintenance Network to the System Management Modules of each Controller in the division. This interface allows all functions described above. The Maintenance Network is connected to all 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 PC for each division. The specification of the Maintenance Network is described below.

(Specification)

Function: Transmission of maintenance date for Engineering tools

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

Transmission media: UTP Category5 cable

[

]

4.1.5 Self-Diagnosis

The MELTAC Platform Controller is equipped with three 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.

a) Hardware based detection process

With this feature, self-diagnosis is implemented by special diagnostic circuitry on the CPU Module. The feature involves a watchdog timer, 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 healthy check, ROM error check, RAM error 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 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 Engineering Tool connected via the Maintenance Network.

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

1) Failure

The fatal abnormality by which the Subsystem cannot continue its functions is categorized as the Failure.

When the Subsystem detects this type of error, it transits to the Failure mode.

In the Failure mode, the processing of input/output and operation are stopped, although the processing of sending the own status data of the Failure mode is continued.

In case of Redundant Standby Controller configuration, when the Subsystem in the Control mode changes to the Failure Mode and the Subsystem in the Standby mode changes from the Standby Mode to the Control Mode and continues the control function.

When there is no Subsystem which communicates with the Output Module, the Output Module transits to the Failure mode which is "as-is mode" or "off mode". This mode is set preliminarily.

2) Alarm

The minor abnormality with which the Subsystem can continue its functions is categorized as the Alarm. This includes the error of the Controller Cabinet.

When the Subsystem detects this type of error, it does not change its mode and only warns of the alarm.

3) I/O Alarm

The abnormality of I/O is categorized as the I/O Alarm.

When the Subsystem detects this type of error, it does not change its mode and only warns of the alarm.

In 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 input values are kept as they are in the normal state and Application Software is informed of the abnormal state of the input signals.

4.1.5.1 Coverage of Self-diagnosis

Coverage of Self-diagnosis of the controller is shown in Figure 4.1-11.

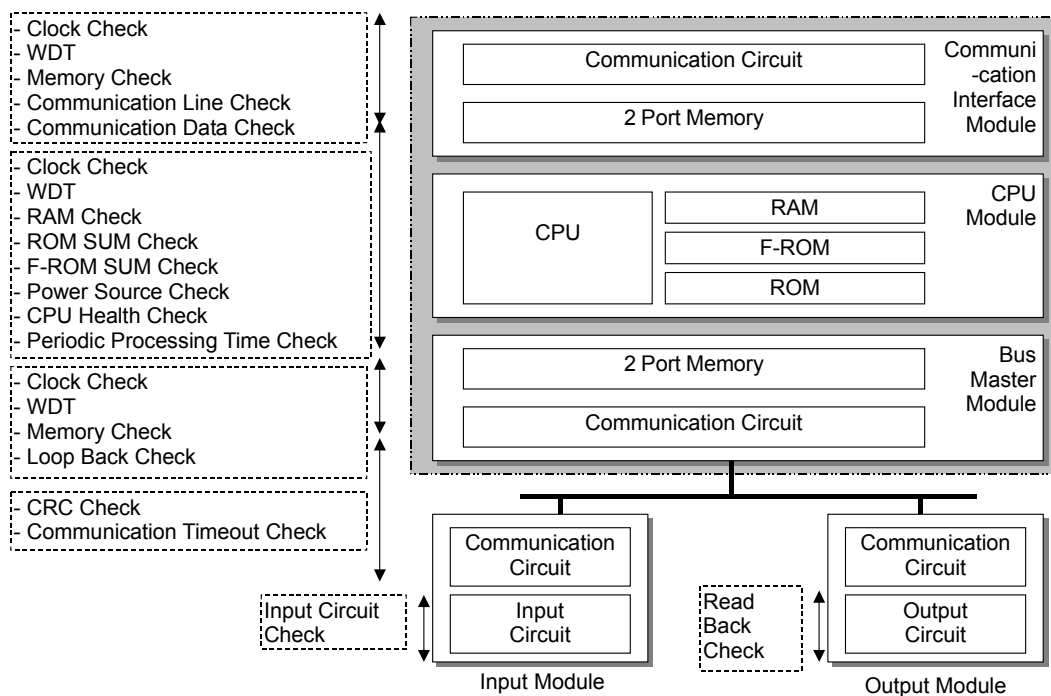


Figure 4.1-11 Coverage of Self-diagnosis function of the controller

4.1.5.2 Self-diagnosis of the controller

The self-diagnosis of the processor modules is described below.

4.1.5.2.1 CPU Module

[

]

4.1.5.2.2 Bus Master Module

[

]

4.1.5.3 Self Diagnosis of Power Supply Modules in the CPU Chassis

[

]

4.1.5.4 Self-diagnosis of the Control Network I/F Module

See Section 4.3.

4.1.5.5 Self-diagnosis of I/O Modules

The self-diagnosis 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

[

]

4.2 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. Each division has its own Safety-VDU. Since the total I&C system has 4-divisions, a single failure of only one Safety-VDU doesn't cause loss of all HSI functions.

4.2.1 Hardware

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 red/green/blue (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 a RS-232C data link.

The complete HSI functional design, including screen navigation, is described in the HFE Process and HSI System Design Topical Report. 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. The CPU Module and Control Network I/F Module hardware and Basic Software are the same as in the MELTAC Controller.

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 red/green/blue (RGB) interface. The RGB interface is generated by the Frame Memory Unit (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 Touch Panel I/F Module. This is an RS-232C data link, which is converted from electrical to optical only to increase the transmission distance. The optical interface is not credited for any isolation function since the Safety VDU Processor and Safety VDU Panel are located in the same safety division and always in the same fire zone. 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.

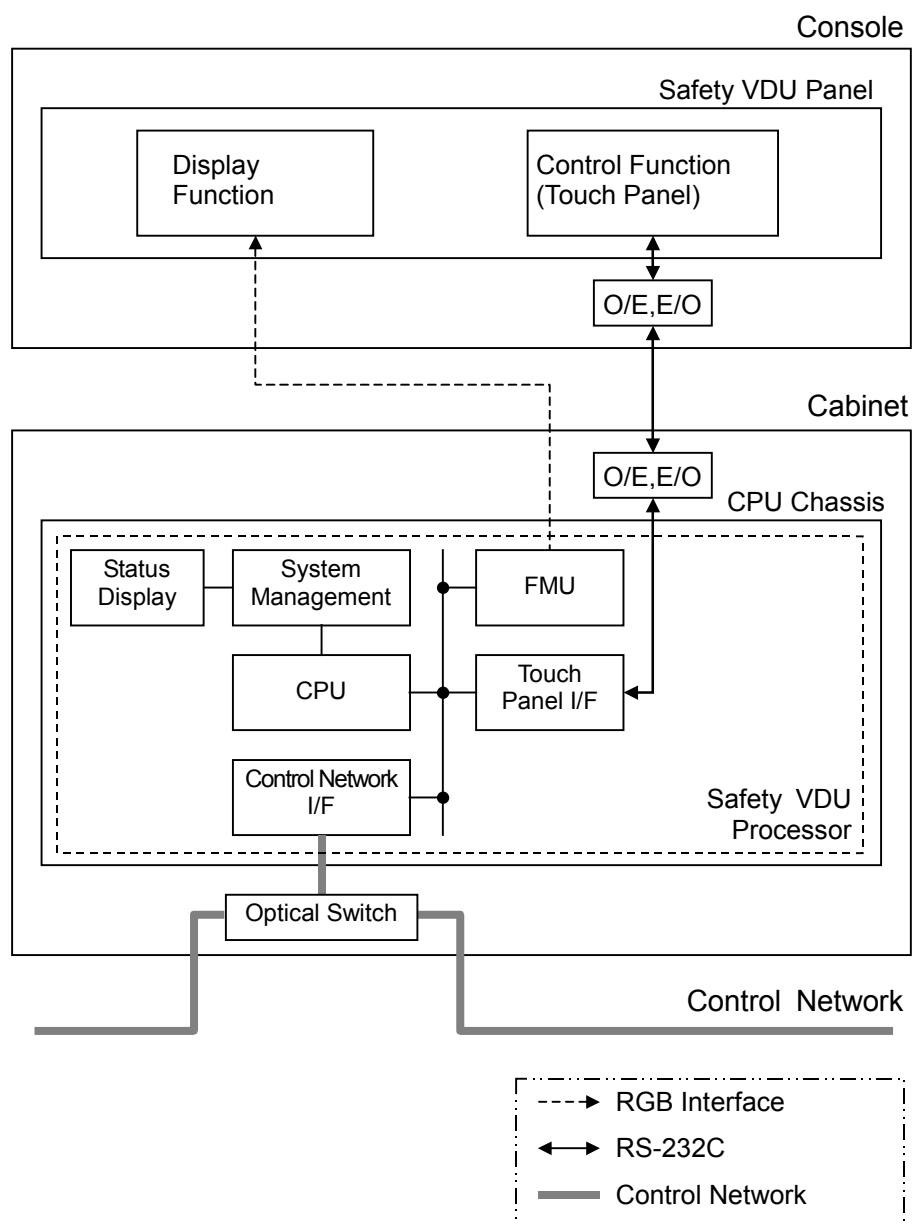


Figure 4.2-1 Configuration of Safety VDU Processor

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
- Touch Panel I/F Module
- Frame Memory Unit (FMU) Module.
- Status Display Module

The FMU and Touch Panel Interface (I/F) Modules are 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 communicates with the CPU Module inside the chassis by means of the Futurebus+ backplane.

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

b) Touch Panel I/F Module

The Touch Panel I/F Module provides the touch panel interface signal from the Safety VDU Panel to the Safety VDU Processor. The Touch Panel I/F Module communicates with the CPU Module inside the chassis by means of the Futurebus+ backplane.

Specifications of Touch Panel I/F Module are in Appendix A.12.

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. 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

4.2.2 Software

4.2.2.1 Basic Software

The Safety VDU Processor software configuration is shown in Figure 4.2-3.

The software structure ensures reliable deterministic operation.

The software structure configuration is based on the same design as that of the Controller Basic Software. With fixed cycle control and no-interrupts, the Basic Software provides high reliability, and deterministic processing. The Basic Software structure is simple, so it is verified with white box testing.

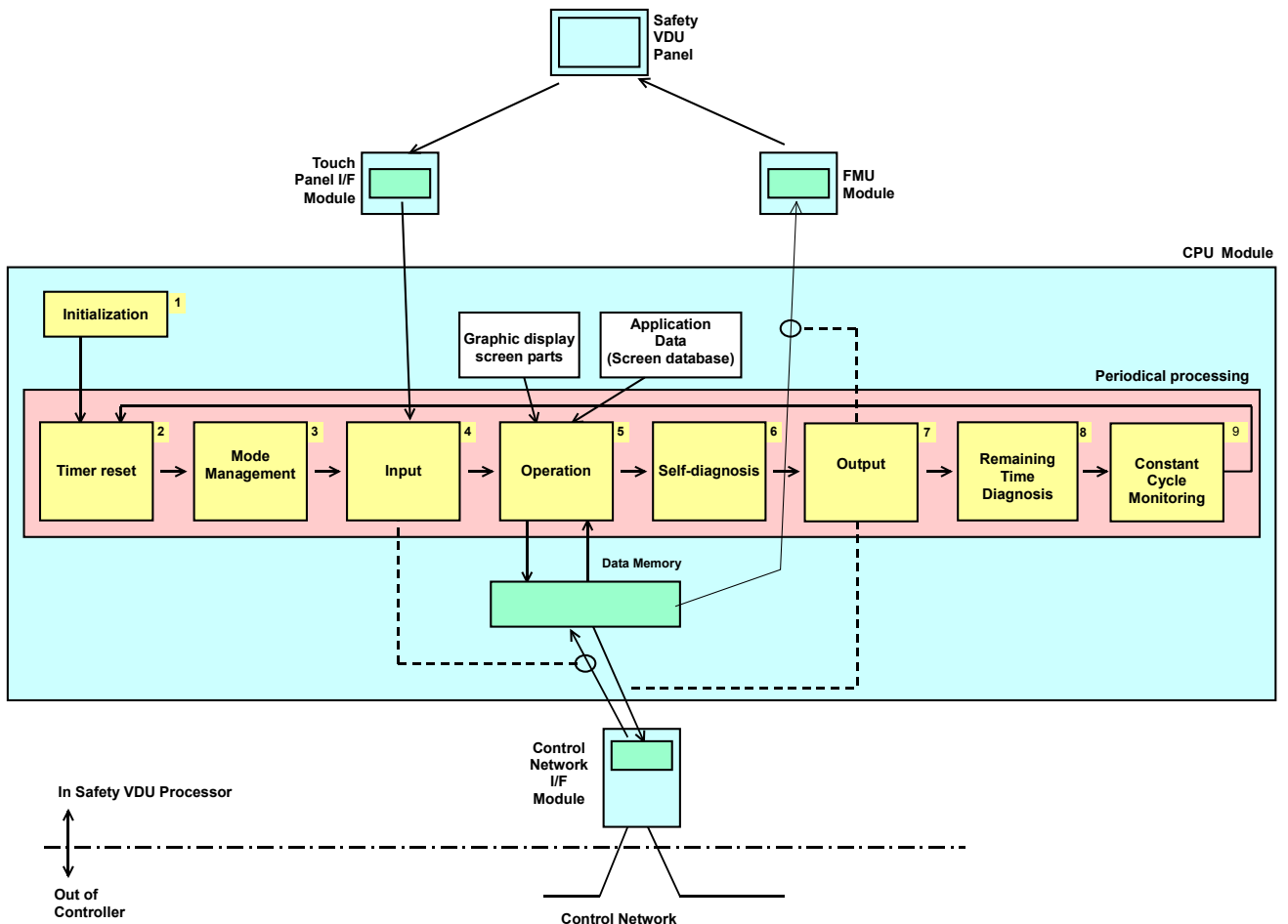


Figure 4.2-3 Software Structure of Safety VDU Processor

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

[

]

[

]

4.2.2.1.1 Screen Selection of 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 Plant Licensing Documentation.

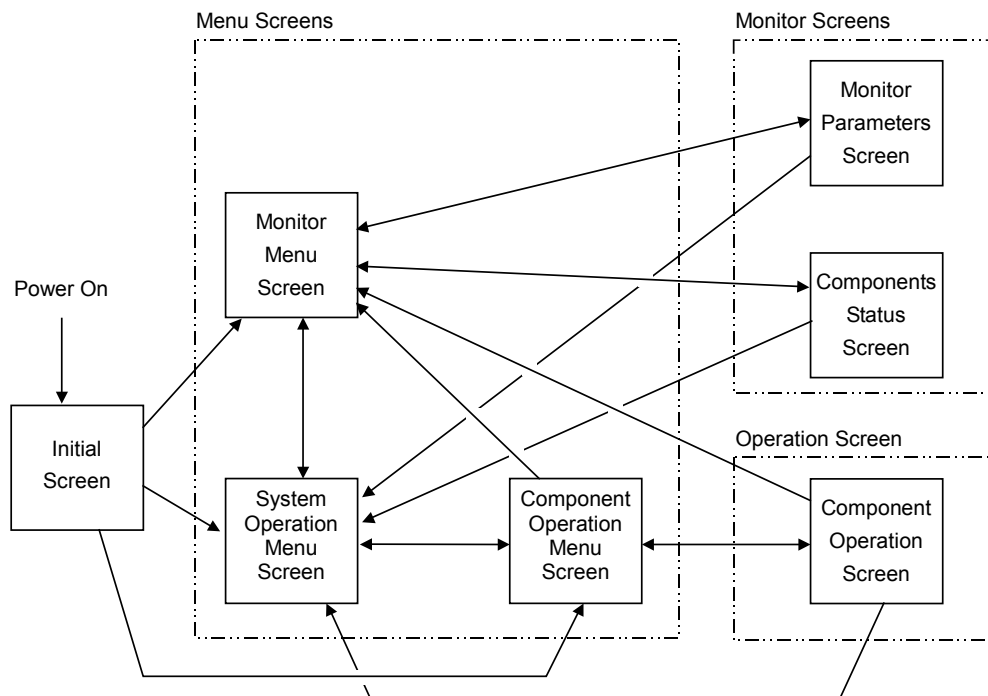


Figure 4.2-4 Screen Transition of the Safety VDU Processor

Table 4.2-1 Explanation of the Screen

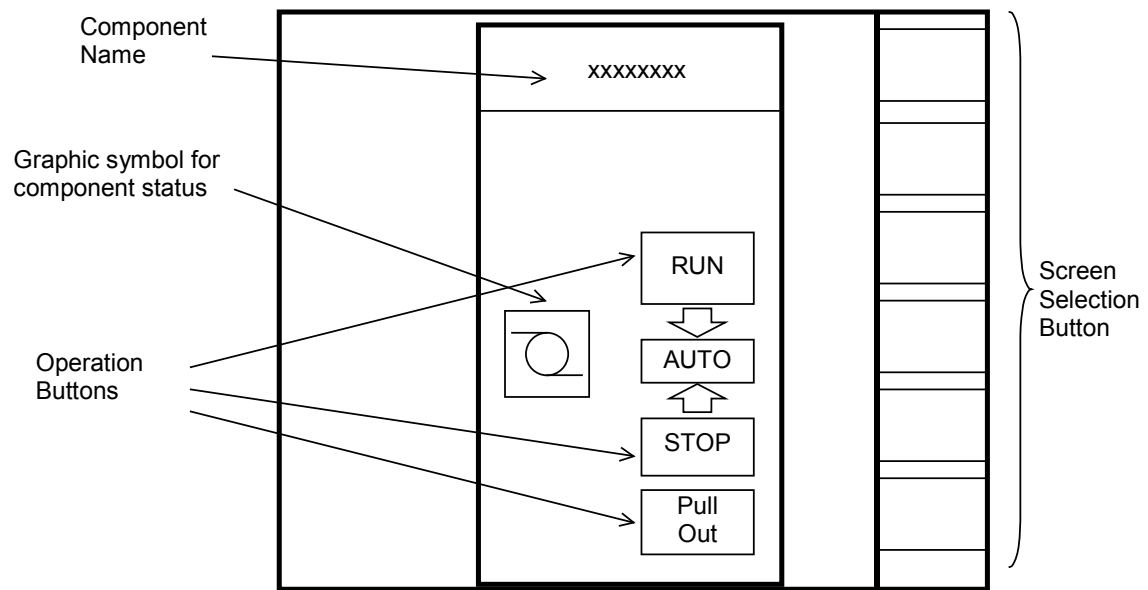


Figure 4.2-5 A Sample of Operation Switch Pictogram on the Safety VDU Panel

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
[

]

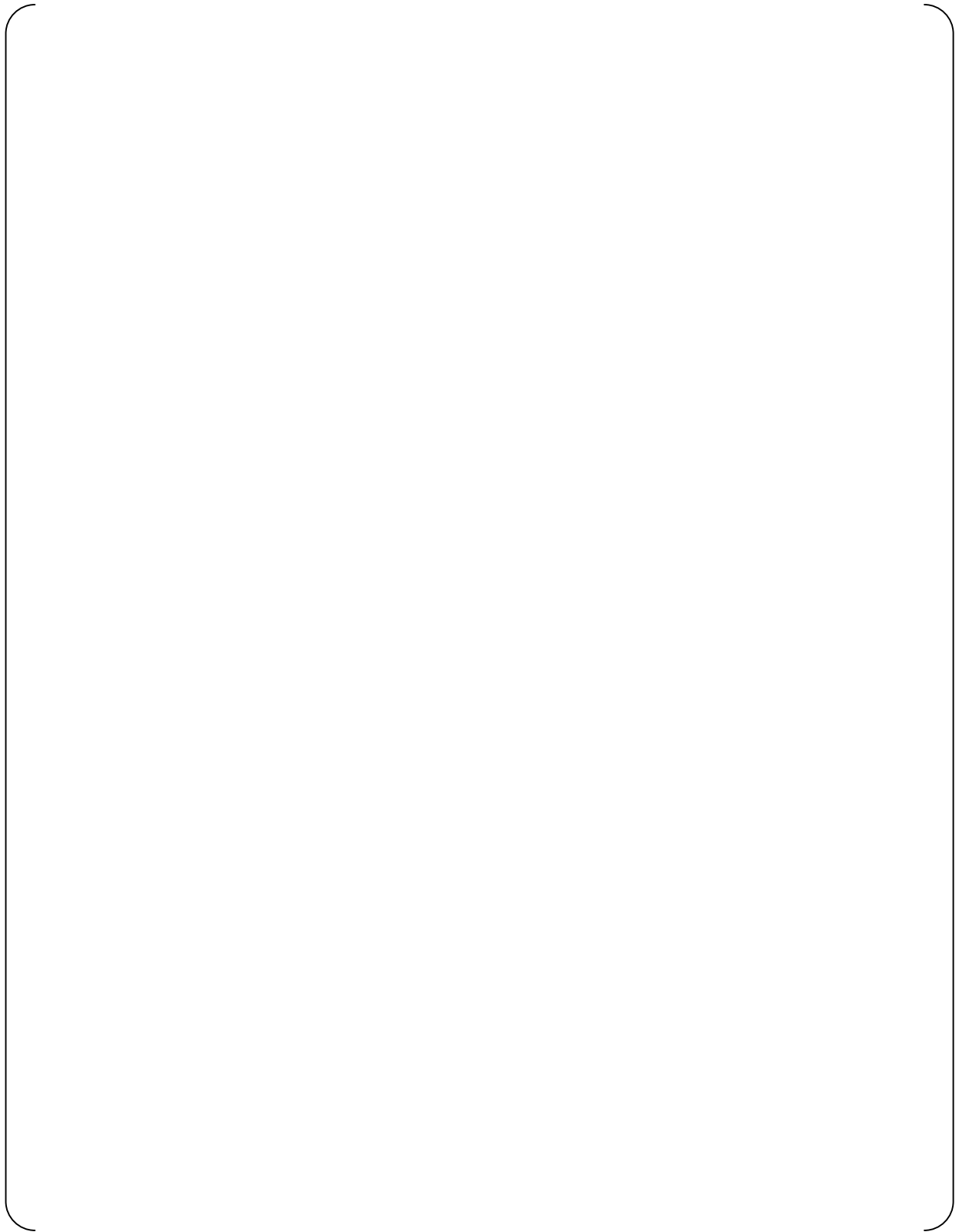


Figure 4.2-6 Explanation of the Safety VDU Processor Operation

4.2.2.2 Application Software and Engineering Tool

[

]

4.2.3 Self-Diagnosis

[

]

4.3 Communication System

4.3.1 General Description

The key design basis of the Control Network, Data Link and Maintenance Network are provided below.

a) Control Network and Data Link:

- Asynchronous communications is used. Controller performs no communication handshaking that could disrupt deterministic logic processing.
- Predefined data size and structure ensure deterministic communication.
- Communications independence – Electrical or communication processing faults in one electrical division cannot adversely affect performance of the safety function in other divisions.

b) Maintenance Network:

- Hardwired interlocks in the Controller or Safety VDU Processor ensure changes to software cannot be made through the data communication interface while the Controller or Safety VDU Processor are operating.

4.3.2 Control Network

This section describes the Control Network.

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

The Control Network is used for the following applications:

- a) The Control Network is used most frequently to communicate data between multiple Controllers, and between Controllers and the Safety VDU Processor(s), all in the same division.
- b) The Control Network can also be used to communicate data between different divisions including non-safety system. This may be between multiple Controllers in different divisions. Or it may be between Operational VDU Processors and multiple Controllers in different divisions.

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 six Controllers is shown in Figure 4.3-1.

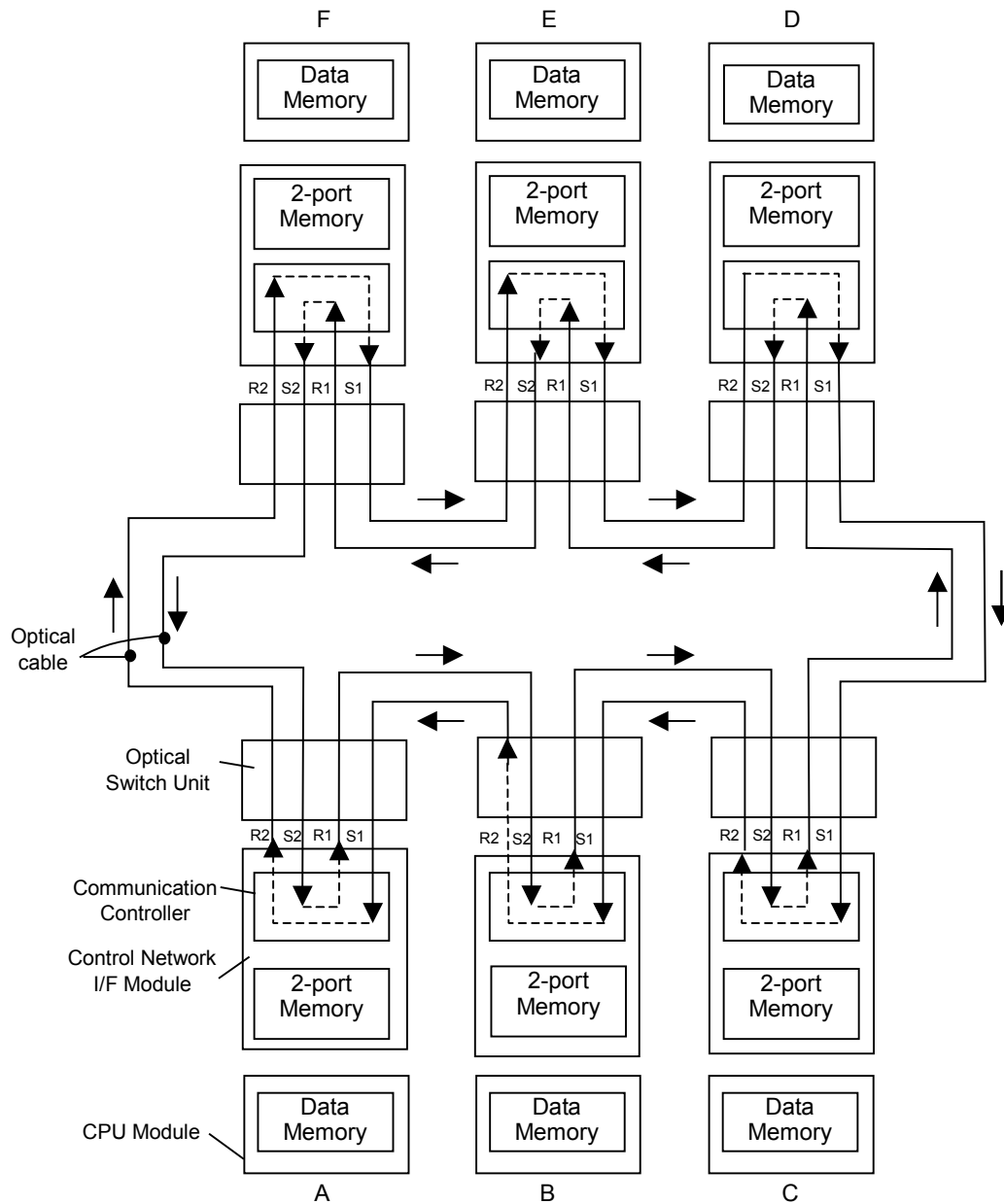


Figure 4.3-1 Configuration of Control Network

The Control Network I/F Modules are interconnected in a ring configuration. Each module communicates through an Optical Switch using two independent optical cables, one for transmission and the other for reception. 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 in the case where subsystem (B) is halted. In this case the Optical Switch bypasses subsystem (B) and directly connects subsystem (A) and (C).

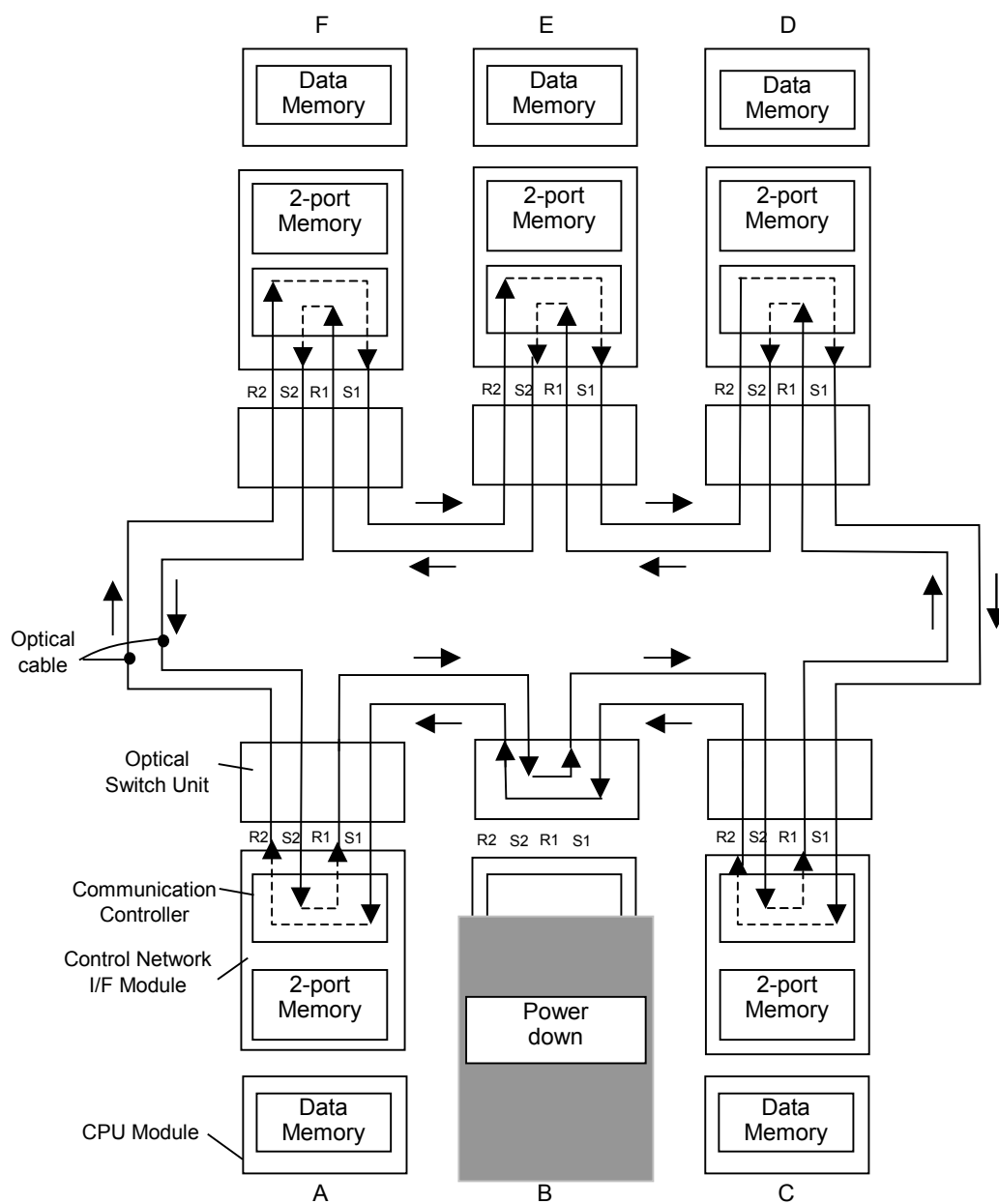


Figure 4.3-2 Explanation of Bypass Operation by the Optical Switch

4.3.2.2 Specifications

The protocol stack of Control Network is described in Figure 4.3-3.
The optical G-bit Ethernet is used for the physical layer.
RPR based on IEEE Standard 802.17 is applied to the Data Link Layer protocol.
(RPR: Resilient Packet Ring)

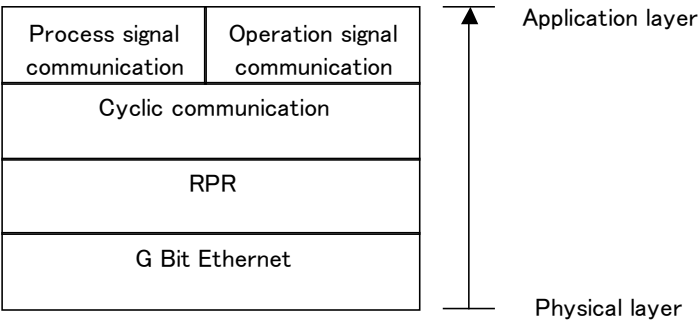


Figure 4.3-3 Protocol Stack of Control Network

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

Table 4.3-2 The Specification of Control Network

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

[

]

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

4.3.2.3 Isolation

The MELTAC Platform maintains electrical isolation and communication isolation for the interface between Controllers in separate safety divisions and for the interface between safety Controllers and any non-safety division. 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 4.3-4

b) Communication Isolation

[

]

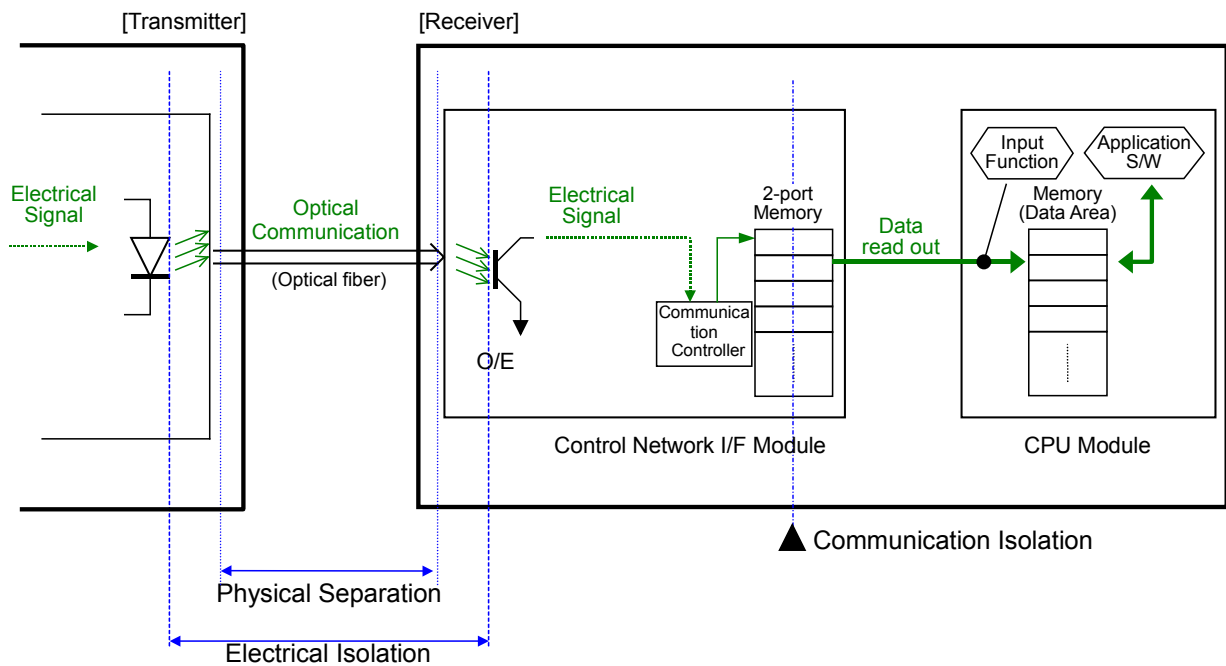


Figure 4.3-4 Separation in Communication of Control Network

4.3.2.4 Self-Diagnosis

The Self-diagnosis function of the Control Network is described below.

Table 4.3-3 Self-Diagnosis Functions of Control Network

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 divisions. The Data Link uses a broadcast protocol at 1Mbps, with no communication handshaking.

Figure 4.3-5 shows communication among Controllers in four divisions.

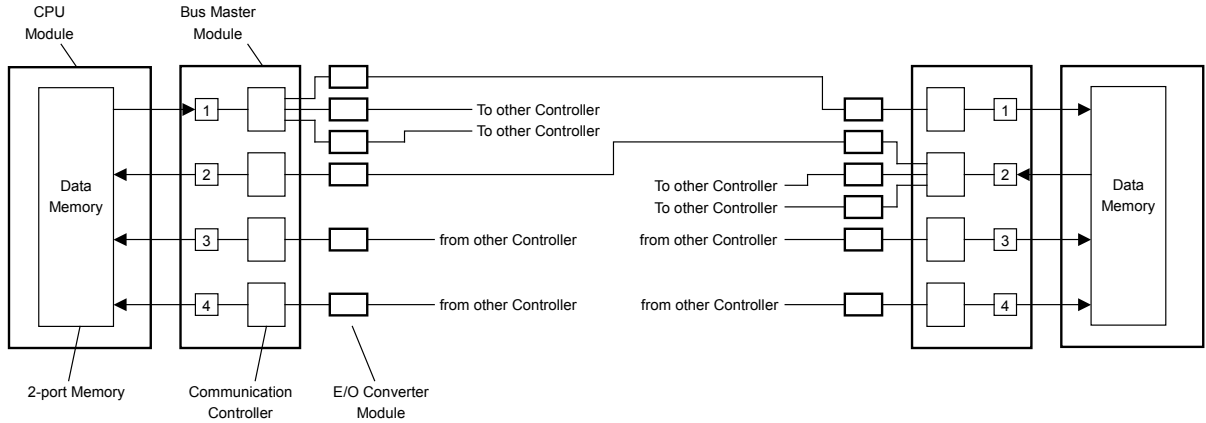


Figure 4.3-5 Data Link Configuration

The Data Link is interfaced through Bus Master Modules. The Bus Master Module provides four communication ports. Each port is set either as a transmission port or a reception port. The Bus Master Module produces an electrical output, which is converted by the Electrical/Optical Converter Module to an optical signal. The transmission port of the Electrical/Optical Converter Module is connected by the optical cable to the reception port of the Electrical/Optical Converter Module in another division.

[

]

4.3.3.2 Isolation

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

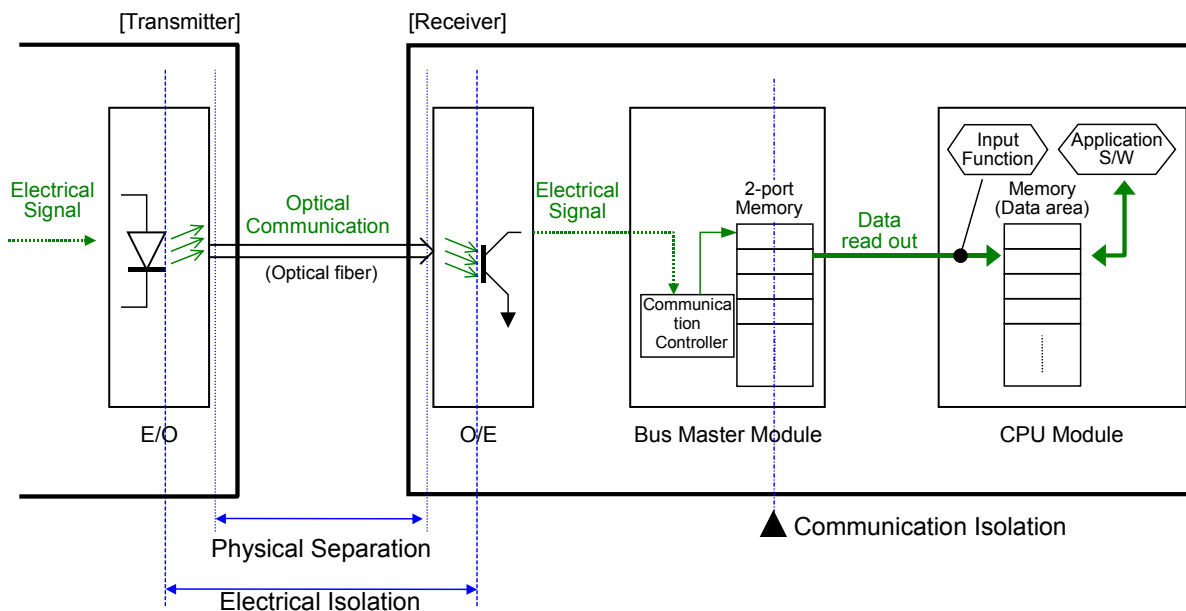


Figure 4.3-6 Separation in Communication of Data Link

4.3.3.3 Self-Diagnosis

[

]

4.3.4 Maintenance Network

4.3.4.1 Configuration

The Maintenance Network is used to communicate between the Controllers and the Engineering Tool to download new application software to the Controllers, or to read/write inside memory of controller. There may be up to three Engineering Tools connected to the Maintenance Network at any one time.

The description of the Controller's processing of data for the Engineering Tool is described in Section 4.1.4.2.

Figure 4.3-7 shows the Maintenance Network configuration.

The Maintenance Network is connected to the controllers.

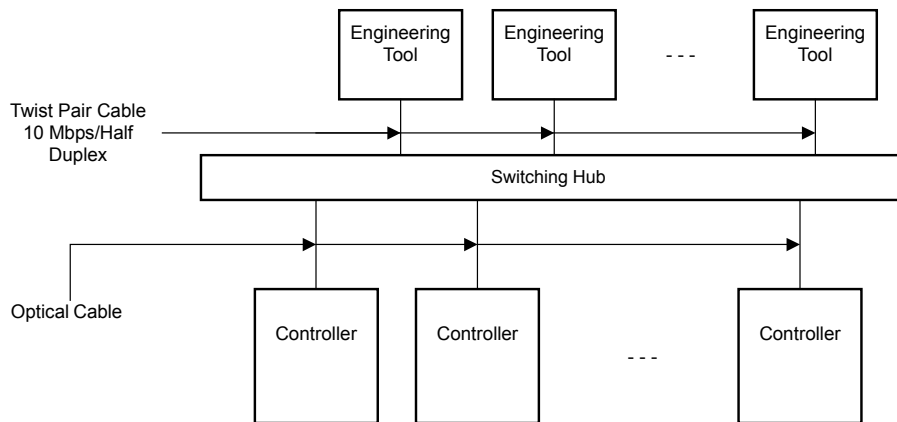


Figure 4.3-7 Maintenance Network Configuration

4.3.4.2 Isolation

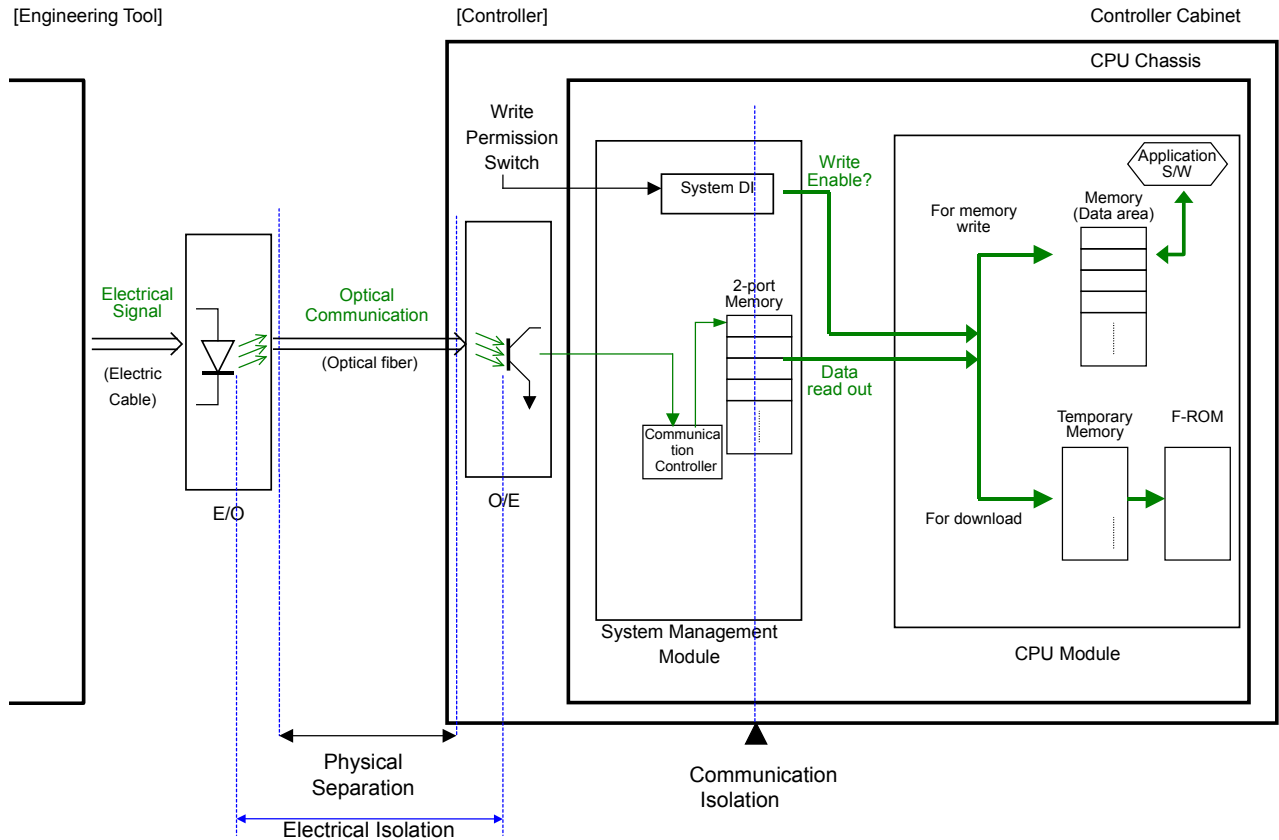


Figure 4.3-8 Separation in Communication of Maintenance Network

The Engineering Tool and Switching Hub are connected to the Controller based on the following design features:

- The non-safety Engineering Tool and Switching Hub are electrically isolated from the safety components through qualified fiber optic isolators with E/O converters.
- 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.
- When the Controllers are in service (ie. not declared inoperable by Technical Specifications) they provide only unidirectional outbound communication to the Engineering Tool (ie. there is no ability for the Engineering Tool to write information to the Controller's memory).

[

]

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 a specific application by exemplifying a typical hardware configuration. As described in the following sections, the worst case response time is deterministic. Therefore the response time conforms to BTP HICB-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

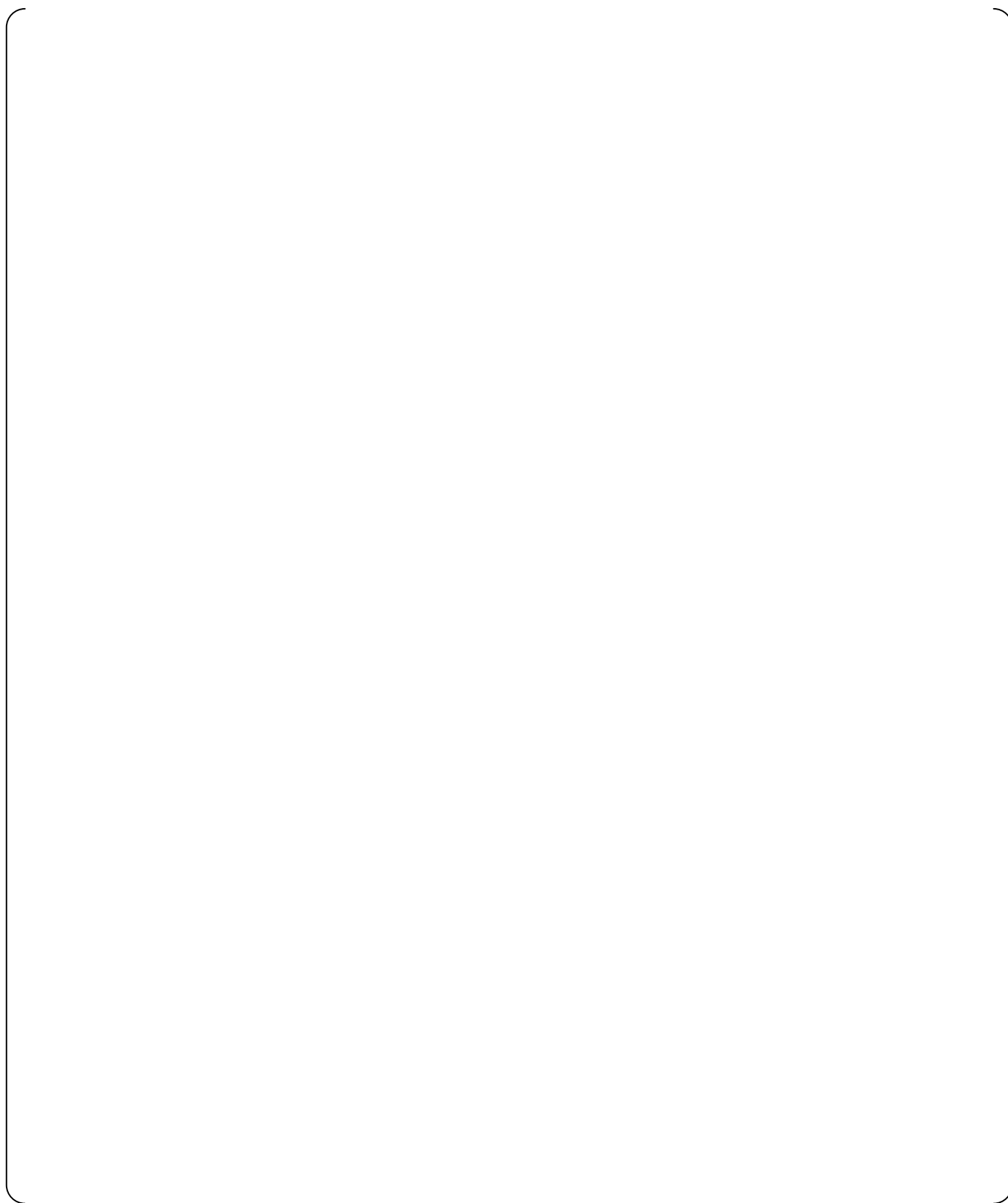
The MELTAC Platform is composed of the CPU Module, Bus Master Module, various types of I/O Modules, Communication I/F Module and Safety VDU Panel. An external input is processed by each of these components before the control result is output to external terminal(s).

Figure 4.4-2 is an example of a typical MELTAC hardware configuration, including communication between two controllers. Table 4.4-1 shows the method to calculate the minimum and maximum response time for each process.



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

[

]

5.0 ENVIRONMENTAL, SEISMIC AND ELECTROMAGNETIC QUALIFICATION

This section describes environmental, seismic and electromagnetic qualifications of MELTAC Platform.

Environmental and seismic qualifications have been verified by the tests described in Section 5.1 and 5.2, respectively. Section 5.3 describes Electromagnetic compatibility (EMC) tests. Section 5.4 describes electrostatic discharge (ESD) tests. Environmental, seismic, EMC and ESD tests have been completed. The EMC acceptance criteria are described in this topical report. The results of Environmental test, Seismic test and EMC test are presented in the following test reports.

“Environmental Test Summary Report for the MELTAC Platform (JEXU-3300-2160)”

“Seismic Test Summary Report for the MELTAC Platform (JEXU-3300-2161)”

“EMC Qualification Test Summary Report for the MELTAC Platform (JEXU-1016-0022)”.

5.1 Environmental Test

5.1.1 Environmental Specification and Outline of Test

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

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

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

5.1.2 Contents of Environmental Test

5.1.2.1 System Level Environmental Test

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

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

- Power Interface Module
- Distribution Modules
- Power Supply Modules

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

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

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

[

Thus, the system environmental tests showed that the MELTAC Platform would continue to operate under all expected environmental conditions.

5.1.2.2 Module Environmental Test

[

]

Thus, the modules tests demonstrated that the individual modules of the MELTAC Platform would continue to perform as designed under all expected environmental conditions.

5.2 Seismic Test

5.2.1 Overview

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

The Cabinet Seismic Resistance Test was performed with a MELTAC Cabinet fully loaded with MELTAC components. For the Cabinet Seismic Resistance Test, a test specimen was prepared that is typical of a safety protection system application. The test specimen was vibration-excited on a large shaker table. During the test the physical integrity and vibration characteristics of the cabinet were confirmed. All system functions were also confirmed before, during and after the excitation. For the input acceleration used for the Cabinet Seismic Resistance Test, a floor response spectrum was selected that is high enough to cover the range of power plants in Japan.

There are no components with aging mechanisms that would affect the equipment's susceptibility to failure during these seismic tests. Therefore there was no special age related preconditioning for these tests.

The test facility for the Cabinet Seismic Resistance Test is a famous facility for conducting seismic test of large equipment for nuclear power plants. Tests were conducted on a 3-Direction large shaker table.

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

Chassis loaded with MELTAC modules were vibration-excited with this input acceleration. During and after this testing, the physical and functional integrity of the module is confirmed.

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

5.2.2 Seismic Resistance Test

5.2.2.1 Cabinet Seismic Resistance Test

For the Cabinet Seismic Resistance Test, a specimen that simulates a fully loaded safety protection system cabinet was prepared. The loading configuration represents the worst case expected stress on internal mounting hardware.

The major MELTAC components located inside the cabinet are as follows:

- CPU Module
- System Management Module

- Bus Master Module
- Status Display Module
- Repeater Modules
- Analog Input Modules
- Analog Output Modules
- Digital Input Modules
- Digital Output Modules
- Power Interface Module
- Distribution Modules
- E/O Converter Modules
- Power Supply Modules

[

]

[

1

5.2.2.2 Module Seismic Resistance Test

For the Module Seismic Resistance Test, physical and functional integrity was confirmed for a single chassis loaded with the following modules:

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

[

]

5.3 Electromagnetic Compatibility and Radio Frequency Interference

The EMI/RFI emission and susceptibility tests are performed for the MELTAC Platform based on the methods and acceptance criteria of RG1.180. The EMC qualification to RG1.180 is confirmed for the MELTAC Platform. The tests are performed with a MELTAC cabinet fully equipped with a typical configuration of MELTAC components required for a safety protection system.

[

]

The specific test method used for the EMI/RFI emission and susceptibility tests described below, was that specified by MIL-STD-461E.

- Conducted emissions, high frequency, 10kHz to 2MHz (CE102)
- Radiated emissions, magnetic field, 30Hz to 100kHz (RE101)
- Radiate emissions, electric field, 2MHz to 1GHz, 1GHz to 10GHz (RE102)
- Conducted susceptibility, low frequency, 30Hz to 150kHz (CS101)
- Conducted susceptibility, high frequency, 10kHz to 30MHz (CS114)
- Conducted susceptibility, bulk cable injection, impulse excitation (CS115)
- Conducted susceptibility, damped sinusoidal transients, 10kHz to 100MHz (CS116)
- Radiated susceptibility, electric field, 30MHz to 1GHz, 1GHz to 10GHz (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 method used for theses tests is that specified by IEC61000-4.

- Surge Withstand Capability, Ring Wave
- Surge Withstand Capability, Combination Wave
- Surge Withstand Capability, Electrically Fast Transients/bursts

Surge Withstand Capability; Oscillatory Wave Test has been successfully performed based on IEEE Std 472 for MELTAC modules. 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 were applied.

For all susceptibility and surge withstand tests the following acceptance criteria is applied:

- There is no equipment damage
- Processors continue to function
- Data communications is 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 occurrence of any system function abnormality, data communication abnormality, and equipment failure is confirmed by referring to the results of the self-diagnosis function of the MELTAC Platform.

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

5.3.1 Test Configuration

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

The Safety VDU Panel is supplied power from the CPU cabinet and connected with the power cable and the signal cable.

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

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

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

Table 5.3-1 MELTAC Modules for the EMC Test

Module	Model
CPU Module	PCPJ-11
System Management Module	PSMJ-11
Bus Master Module	PFBJ-11
Control Network I/F Module	PWNJ-01
Touch Panel I/F Module	PRSJ-01
FMU Module	PFDJ-01
Status Display Module	PPNJ-12
Repeater Module	MRPJ-01
Repeater Module	MRPJ-02
Repeater Module	MRPJ-21
Analog Input Module (Current input)	MLPJ-01
Analog Input Module (Current input for automatic testing)	MLPJ-02
Analog Input Module (RTD input)	MRTJ-34
Analog Input Module (RTD input for automatic testing)	MRTJ-61
Analog Output Module (Current output)	MAOJ-01
Analog Output Module (Voltage output)	MVOJ-01
Digital Input Module (Contact input)	MDIJ-04
Digital Input Module (Contact input for automatic testing)	MDIJ-06
Digital Input Module (Contact input for Redundant Parallel Controller)	MDIJ-62
Digital Output Module (Relay contact output)	MDOJ-03
Digital Output Module (Relay contact output for Redundant Parallel Controller)	MDOJ-61
Digital Output Module (Semiconductor output)	MDOJ-22
Isolation Module (Current input, Current/Voltage output)	KILJ-01
Isolation Module (RTD 4line type input, Current/Voltage output)	KIRJ-01
Isolation Module (Contact input, Semiconductor output)	KIDJ-01
Power Interface Module	DPOJ-21
E/O Converter Module (RS485)	MEOJ-02
E/O Converter Module (RS232C)	MEOJ-11
CPU Power Supply Module	PS-1
I/O Power Supply Module	PS-2
CPU Power Supply Module (Small capacity type)	PPSJ-01
CPU Power Supply Module (Large capacity type)	PPSJ-11
CPU Fan	814JND
Door Fan	815JND
Power Supply Fan	503AH0HE
Safety VDU Panel	KA20A1019
Optical Switch	RJMA-02

5.3.2 Description of Tests

5.3.2.1 Conducted Emissions, High Frequency (CE102) Test

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

a) Method

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

b) Test Subject

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

[

]

5.3.2.2 Radiated Emissions, Magnetic Field (RE101) Test

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

a) Method

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

b) Test Subject

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

[

]

5.3.2.3 Radiated Emission, Electric Field (RE102) Test

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

a) Method

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

b) Test Subject

The test subjects are the EUT enclosure, the all interface cables and the Safety VDU Panel.

[

]

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

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

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

a) Method

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

b) Test Subject

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

[

]

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

The CS114 test is applicable to all interconnecting leads including the power leads of the EUT. This section describes the CS114 test that is applied to the power and control lines described in section 4.1.2 of RG1.180.

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

a) Method

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

b) Test Subject

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

[

]

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

The CS114 test is applicable to all interconnecting leads including the power leads of the EUT. This section describes the CS114 test that is applied to the signal line described in section 4.2 of RG1.180.

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

a) Method

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

b) Test Subject

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

[

]

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

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

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

a) Method

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

b) Test Subject

One each of the signal cables (input and output cables of the Analog I/O Modules, the Digital I/O Modules, Power interface Module, the Isolation Modules and the RGB cables) to the EUT

[

]

5.3.2.8 Conducted Susceptibility, Damped Sinusoidal Transients (CS116) Test

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

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

a) Method

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

b) Test Subject

One each of the signal cables (input and output cables of the Analog I/O Modules, the Digital I/O Modules, Power Interface Module, the Isolation Modules and the RGB cables) to the EUT

[

]

5.3.2.9 Radiated Susceptibility, Electric Field (RS103) Test

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

a) Method

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

b) Test Subject

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

[

]

5.3.2.10 Surge Withstand, Ring Wave Test

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

a) Method

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

b) Test Subject

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

[

]

5.3.2.11 Surge Withstand, Combination Wave Test

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

a) Method

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

b) Test Subject

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

[

]

5.3.2.12 Surge Withstand, Electrically Fast Transients/bursts Test

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

a) Method

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

b) Test Subject

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

[

]

5.4 Electrostatic Discharge Test

For the MELTAC Platform, the ESD test has been successfully performed based on IEC61000-4-2 with test level-2, in accordance with Annex A (maximum charge voltage is 4 kV). This maximum charge voltage is based on the MELTAC Cabinet being installed in Japan on the floor using antistatic materials or concrete.

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

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

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 is 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 acceptance criteria is only to ensure no equipment damage.

The ESD test is performed according to the method set forth in IEC61000-4-2, as follows:

a) Method

Confirm that the EUT can withstand ESD, which may occur from personnel coming into contact at human-machine interface points of equipment during normal operation and when the equipment is out of service during maintenance.

b) Test Subject

The following equipment points are likely to be accessed by personnel during normal equipment 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 points of the equipment are expected to be accessed only during maintenance.

[

]

6.0 LIFE CYCLE

6.1 Life Cycle Process

6.1.1 Overview of the MELTAC Quality Assurance Program

This section describes key elements of the lifecycle process for the Basic components (software and hardware) of the MELTAC Platform.

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

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

These procedures address all requirements of 10CFR Part 50 Appendix B and IEEE7-4.3.2-2003, including the applicable Regulatory Guides and IEEE software standards. The requirements of these quality assurance procedures are described in the Sections below. All new MELTAC development or revisions to current platform components will be in accordance with [].

Platform components (hardware or software) developed prior to these new procedures (referred to as Existing Platform) will be reused for US nuclear applications. The Original QAP and records of the Existing Platform have been assessed against these new procedures, to ensure suitable quality of the Existing Platform. The result shows the development process for the Existing Platform conforms to [] except the independent V&V requirement and other minor deficiencies.

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

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

- Quality Assurance (6.1.2)
- Management (6.1.3)

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

- Development (6.1.4)

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

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

- Cyber Security Management (6.1.6)

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

6.1.2 Quality Assurance

The requirements for MELTAC Platform quality assurance are set forth in various in-house procedures, in accordance with the 10CFR50 Appendix B and IEEE7-4.3.2-2003 and IEEE1012-2004. These in-house QA procedures are shown in Figure 6.1-1.

These procedures apply to new and revised components of the MELTAC platform. Table 6.1-1 shows the conformance of the MELCO quality program to 10CFR50 Appendix B.



Figure 6.1-1 Outline of In-house QA Procedures System and Relationship of Various Plans

[

]

Table 6.1-1 Conformance of the MELCO Quality Program to 10CFR50 Appendix B

10CFR50 Appendix B Item/Title	Conformance of MELCO Quality Program	Conformity
I. Organization	QA activities are carried out by an QA organization that is independent from Design and Inspection sections.	Affirmed
II. Quality Assurance	The QC Flow Chart, ensures suitable consistent quality assurance activities throughout the MELTAC product life. Appropriate training programs are in place for maintaining the necessary technical quality standards.	Affirmed
III. Design Control	The standards and procedures for design activities and verification activities are documented. Procedures for reviewing or changing designs are also documented.	Affirmed
IV. Procurement Document Control	All purchased materials are checked in accordance with the documented procurement procedures for their compliance with the required specifications.	Affirmed
V. Instructions, Procedures, and Drawings	All activities concerning quality are based on the documented procedures.	Affirmed
VI. Document Control	There are written procedures about control , reviews, and changes of the design	Affirmed
VII. Control of Purchased Material, Equipment, and Services Control of Special Process	The quality of all purchased materials is controlled in accordance with the procedures for purchased materials (parts, products) including requirements for acceptance test and the supplier audits.	Affirmed
VIII. Identification and Control of Materials, Parts, and Components	All products have their own traceability that can be individually identified.	Affirmed
IX. Control of Special Processes	Procedures are in place for the control of special processes and the skill of the staff in charge. Skill or expertise of any staff who was involved in past development was approved.	Affirmed
X. Inspection	Inspections are conducted according to the established plans by the Inspection section. The inspection procedures and their results are documented.	Affirmed

10CFR50 Appendix B Item/Title	Conformance of MELCO Quality Program	Conformity
XI. Test Control	Test procedures and reports are generated by the Design or V&V section. These documents are reviewed by the organization responsible for system design(eg. MHI)	Affirmed
XII. Control of Measuring and Test Equipment	The calibration of measuring instruments and measuring tools is controlled according to established rules. For development of Existing Platform, It has been performed adequate calibration.	Affirmed
XIII. Handling, Storage and Shipping	Storage, shipment and handling of parts and products are controlled according to established rules.	Affirmed
XIV. Inspection, Test, and Operating Status	The completion of all required reviews, tests and Inspections, is clearly identified.	Affirmed
XV. Nonconforming Materials, Parts, or Components	All nonconforming materials are correctly sorted and controlled according to established rules to avoid erroneous usage.	Affirmed
XVI. Corrective Action	Corrective actions and remedial measures regarding nonconforming materials are realized in accordance with the documented rules.	Affirmed
XVII. Quality Assurance Records	Quality Records are controlled in accordance with the documented rules. Records include operation logs, result of reviews and audits, tests, etc. All records are stored, and can be retrieved.	Affirmed
XVIII. Audits	Quality assurance audits are realized in accordance with the documented rules including planning, audit procedures, selection of person to execute, and handling of the results. Periodic QA audits of the Design and V&V organizations are performed by the independent QA organization.	Affirmed

[

]

6.1.3 Management

This section describes requirements for management of MELTAC platform development. These requirements are based on 10CFR50, Appendix B and IEEE 7-4.3.2-2003 and IEEE1012-2004.

6.1.3.1 Organization

[

]

6.1.3.2 Project Plan

[

]
6.1.3.3 Personnel Ability
[

]

Existing Platform Assessment

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

6.1.4 Development

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

[

]



Figure 6.1-2 Outline of Software Development Plan

[

]

Table 6.1-2 Contents of Activity in Each Phase

[

]



Figure 6.1-3 Outline of Problem Tracking/Resolution Process

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

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

--	--

[

]

Existing Platform Assessment

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

6.1.5 Configuration Management

The configuration management process is in accordance with NPD Standard [], which conforms to RG1.169 and IEEE828-1990. The key elements of the configuration management program are described below.

6.1.5.1 Organization/Responsibility

[

]

6.1.5.2 Base-Line

[

]

6.1.5.3 Other Configuration Management Items

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

[

]

6.1.5.4 Reporting

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

6.1.5.5 Change Management

[

]

6.1.5.6 Storage and Retrieval

[

]

6.1.5.7 Reviews

[

]

Existing Platform Assessment

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

[

]

6.1.6 Cyber Security Management

The Cyber Security Management Program is in accordance with NPD Standard [], which conforms to RG1.152. The overall Cyber Security Management Program ensures the followings:

- a) There is no unintended code included in the software during the process of software development.
- b) Unintended changes to the software installed in the system are prevented and detected.

For item a), the Section 6.1.6.1 and 6.1.6.2 in this Topical Report describe the security measures in the development process of the MELTAC Platform Basic Software and Engineering Tool. These requirements and procedures are documented. The security measures in the development process of the Application Software are described in the Safety I&C System Description and Design Process Topical Report. The Safety I&C System Description and Design Process Topical Report also describes change management and security measures for the Application Software during the final integration and testing of plant systems prior to shipment.

For item b), the Safety I&C System Description and Design Process Topical Report describes security measures in the system design which prevent unintended changes while the system is in the plant. This applies to pre-operational testing and operation. Section 6.1.6.3 in this Topical Report describes features of the MELTAC Platform, which prevent unintended changes during system operation and allow changes to be detected, should they occur.

The Section 6.1.6.4 describes the Existing platform assessment.

6.1.6.1 Software Development/Storage Security Measures

[

]

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

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

[

]

6.1.6.2 Security Measures In Each Phase of Development Process

This security measures shown in Table 6.1-5 ensure that no unintended code can be introduced during the development process.

Table 6.1-5 Security Measures in the Software Development Process

6.1.6.3 Cyber Security Measures During System Operation

[

]

6.1.6.4 Existing Platform Cyber Security Assessments

[

]

6.1.7 US Conformance Program for Previously Developed Components

[

]
6.1.7.1 Platform Design
[

]
6.1.7.2 Software Design
[

]

6.1.7.3 Program Design, Coding, Unit Test

[

]

Table 6.1-6 Classification of Previously Developed Software Units

--

[

]

6.1.7.4 Integration Test

This section describes the result of new Integration Tests performed for the UCP and the assessment of past Integration Test. The combination of the both results fulfills the Platform Specification, which conforms to the regulatory requirements.

[

] Final assessment result - The V&V Team confirmed that all items for the Existing MELTAC Platform Integration Test satisfied the requirements of 10CFR50 Appendix B.

[

]

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

6.1.8 Software Installation

[

]



Figure 6.1-5 Software Installation

6.1.9 Maintenance

[

]

Table 6.1-7 Information Provided in Maintenance Manual

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

Existing Platform Assessment

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

6.1.10 Training

MELCO supports training that assists customers in understanding the working and proper use of the MELTAC Platform. This training is comprised of lecture classes and hands-on training using actual MELTAC Controllers. Below are the major trainings courses:

[

]

Additional application specific training is described in the Safety I&C System Description and Design Process Topical Report.

6.1.11 Operations

6.1.11.1 Hardware

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

Table 6.1-8 Hardware Measurement

6.1.11.2 Software

This section describes the upgrade process for the MELTAC Basic Software. Upgrades or changes to Application Software are described in the Safety I&C System Description and Design Process Topical Report.

Table 6.1-9 Software Upgrades Relation

6.1.12 Software Safety Plan

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

[

]

Table 6.1-10 Possible Hazards

--

[

]

The Software Safety Plan to address potential software hazards related to the application software are discussed in the Safety I&C System Description and Design Process Topical Report.

6.2 Life Cycle Management

6.2.1 Quality Records Management

Quality records are collected and controlled in accordance with NPD []. This Quality Assurance Program ensures records of completed items and activities affecting quality are appropriately stored. The records and their retention times are defined.

6.2.2 Failure and Error Reporting and Corrective Action

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

6.2.2.1 Policy of MELTAC Troubleshooting

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

MELCO has recorded all phenomena, causes, solutions, and all information about troubles at all plants. So MELCO collects all field equipment Failure and Error Information in-depth. Based on these information, MELCO has analyzed the platform reliability to improve quality of the MELTAC platform.

6.2.2.2 Troubleshooting Summary

The rule, method and form of troubleshooting report to customer will be discussed between MELCO and each customer, in consideration of US regulations(10CFR21) and customer's situation.

This subsection describes the general problem handling process of MELCO. Changes to this process are likely to occur through the normal course of MELCO's process improvements.

[

]

6.2.3 Obsolescence Management

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

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

6.2.3.1 Obtaining Information on Part Availability

[

]

6.2.3.2 Selecting Replacement Parts

[

]

6.2.3.3 Verification after Replacement

[

]

7.0 EQUIPMENT RELIABILITY

7.1 History of Operation

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

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

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

Shown in Figure 7.1-1 is the history of the MELTAC development, the records of operation, and the application plans. The current MELTAC operation status is described below.

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

The latest MELTAC Platform has now been applied for a Japanese nuclear plant under construction. The platform is used throughout the plant, including the digital protection system. The complete digital system was shipped to the plant site recently after completing a 22 month factory acceptance test. Commercial operation of this plant is expected to begin in 2009.

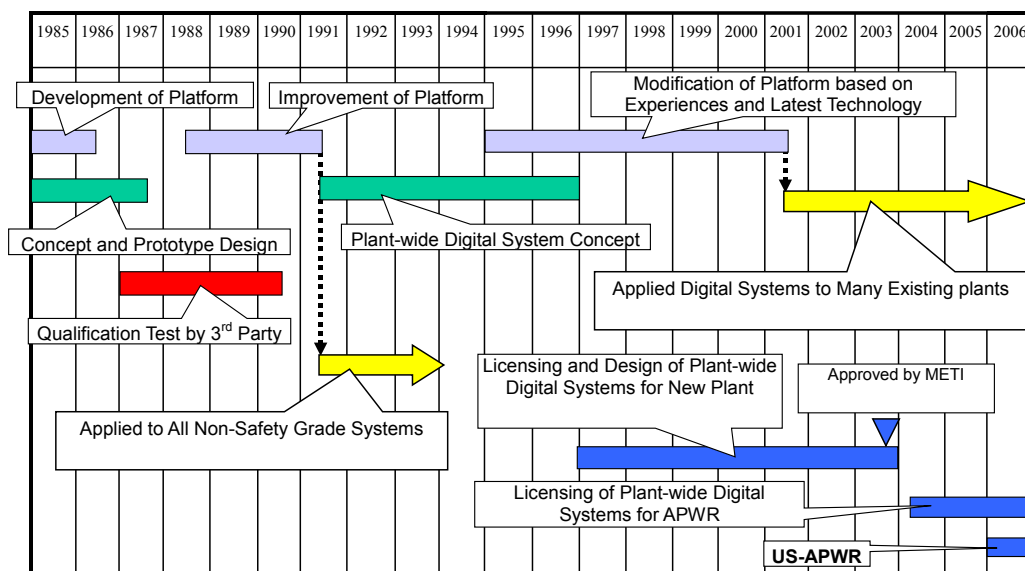


Figure 7.1-1 MELTAC Development and Operating History

7.2 Mean Time between Failures (MTBF) Analysis

MTBF is calculated for each MELTAC module. These values are then used to assess the reliability of complete MELTAC controllers for each system, as explained in Section 7.3. The calculation of MTBF values is based on MIL-HDBK-217F NOTICE2. MTBF values are calculated by adding up the failure rates of the components which make up each module and finding the reciprocal of the module's failure rate thus obtained. For the MIL-HDBK, failure rate is defined by the type of the component, taking operating conditions and reliability factor into consideration, so it represents a generic reliability assessment technique. Environmental conditions used for the calculation are described below.

[

]

The actual MTBF value determined from recent operating history is more than the calculated MTBF value.

Therefore, the calculation method and the resulting calculated values are appropriate for assessing system reliability.

7.3 Controller Reliability Analysis

The failure rate of any MELTAC system, as a whole, depends on the complete system configuration. Variations for each application include:

- the number and configuration of redundant divisions
- the number and configuration of controllers within each division
- the redundancy configuration within each controller
- the configuration of I/O and Communications Interface modules and the criticality of those interfaces to the safety function (ie. the safety function logic design)

The overall reliability for safety system applications is described in the Safety I&C System Description and Design Process Topical Report. The MTBF numbers and reliability models used in that Topical Report are based on the methods described in this report.

This section describes the method used to determine the reliability of the generic Redundant Parallel Controller. The method for the Single Controller architecture can be extracted from this method.

Controller Reliability Analysis is performed as follows.

- A reliability model for the system's safety function is built
- Using the reliability model, Fault Tree Analysis (FTA) is used to determine the frequency of:
 - Spurious actuation of the safety function
 - Failure to actuate the safety function

The reliability model for a simple system is shown in section 7.3.1. To exemplify the reliability analysis process, Figure 7.3-2 shows the fault tree for spurious actuation of the safety function. The FTA for spurious actuation is explained below.

7.3.1 Reliability Model

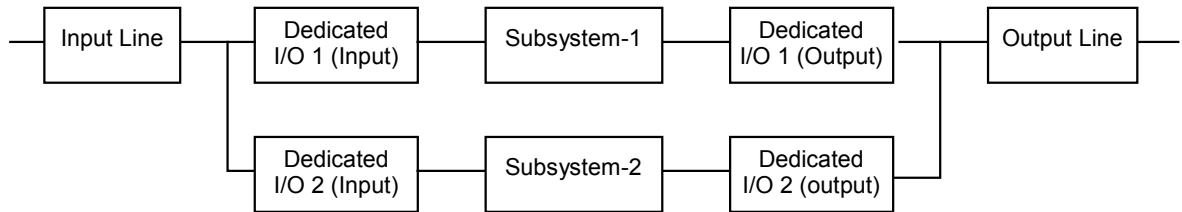


Figure 7.3-1 Reliability Model

The above figure shows Reliability Model of Redundant Parallel Controller, which includes one input module and one output module for each Subsystem.

In the Reliability model, the Status Display is not included in the Subsystem, because the Status Display only displays the current state of the Subsystem; its failure doesn't affect the safety function of the Subsystem. The Control Network I/F Module and Optical Switch Module are not included 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.

7.3.2 FTA for Spurious Actuation of the Safety Function

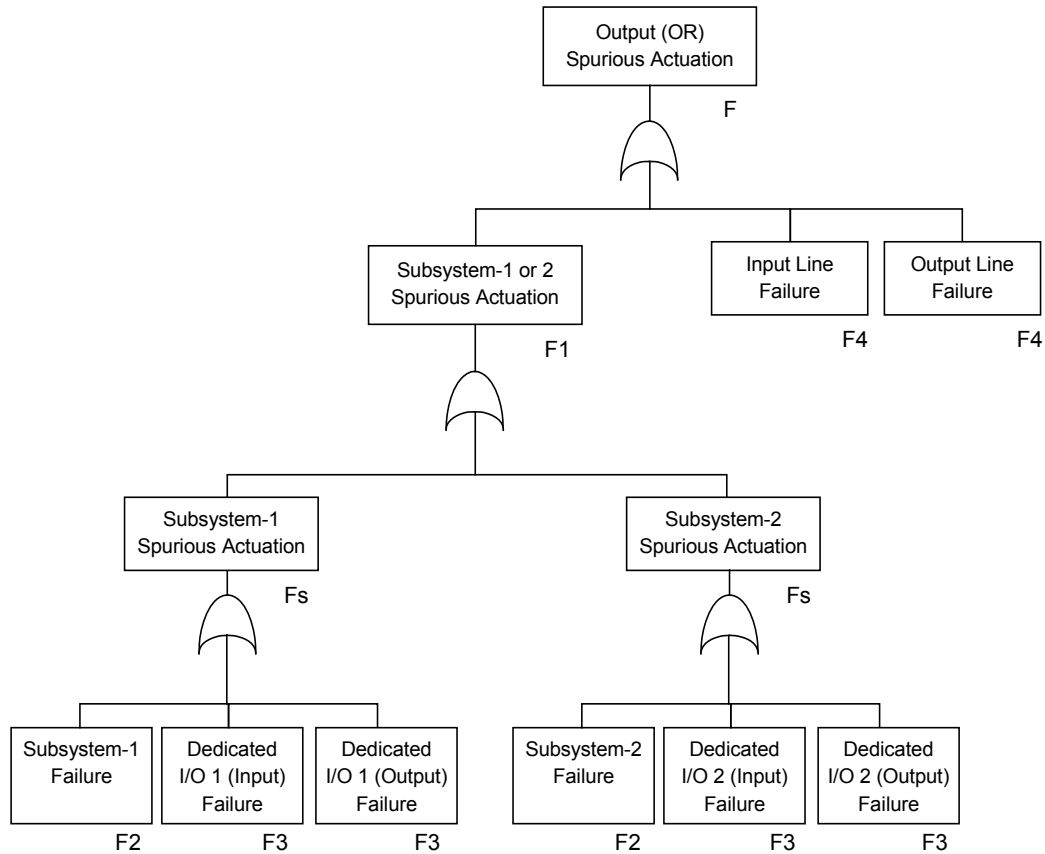


Figure 7.3-2 Fault Tree for Output Failure Spurious Actuation

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

$$F = F1 + F4 + F4$$

$$F1 = Fs + Fs$$

$$Fs = F2 + F3 + F3$$

Failure rate F_i cause spurious action of each module or Subsystem is defined below.

$$F_i = \lambda_i \times (1 - P_i)$$

λ_i = Failure rate

P_i = probability of detecting the failure which effects the safety function by self-diagnosis

F2, F3 and F4 are calculated as described below in section 7.3.4.1, 7.3.4.2 and 7.3.4.3. The failure rate of Input Line and Output Line are the same, because they consist of same module and unit.

This FTA model assumes for this very simple system that the input has a direct effect on the system output. Systems with more complex logic may validate inputs (eg. voting) within the application logic so that spurious actuation requires multiple input failures.

7.3.3 FTA of Failure to Actuate the Safety Function

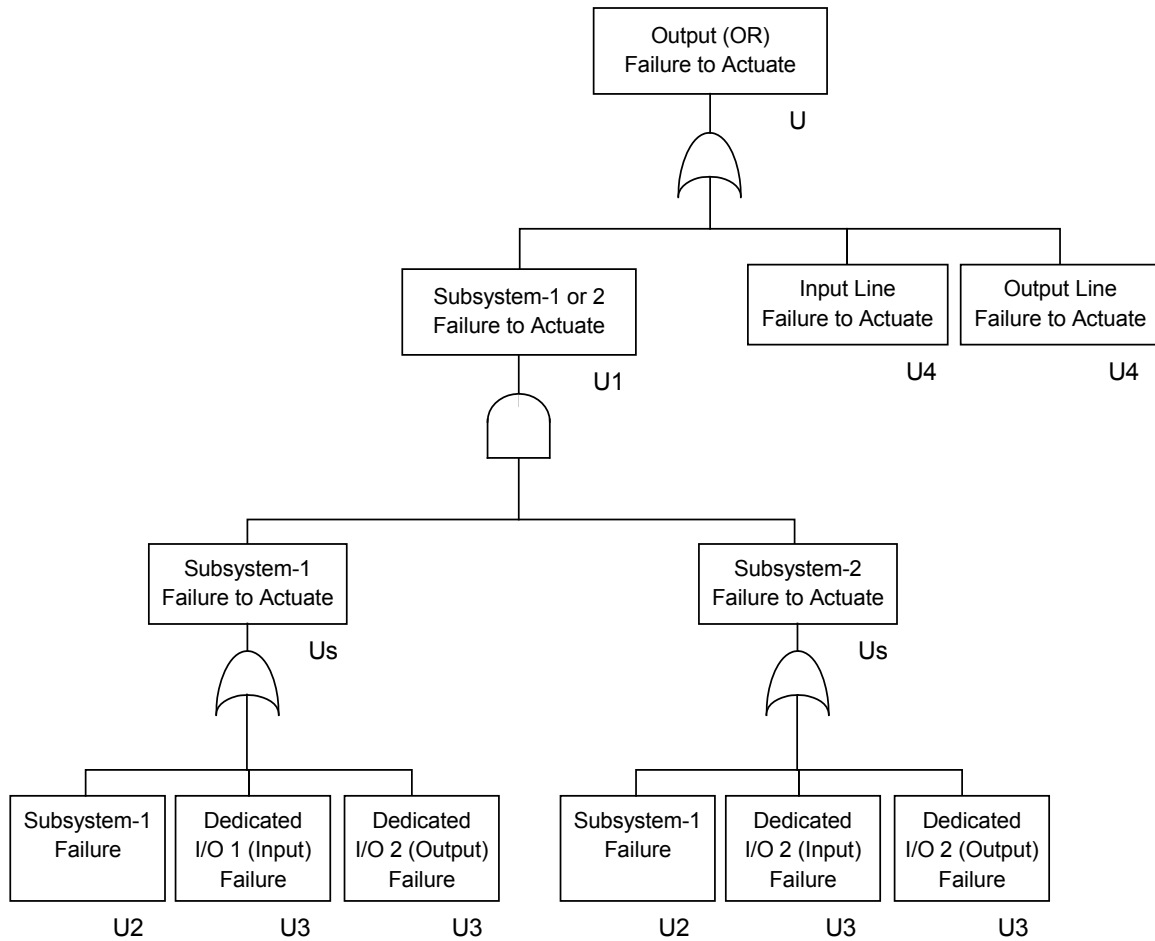


Figure 7.3-3 Fault Tree for Failure to Actuate

For the cause of failure to actuate, Unavailability is described below.

$$U = U1 + U4 + U4$$

$$U1 = Us \times Us$$

$$Us = U2 + U3 + U3$$

Where U_i is the unavailability each module or Subsystem is defined below.

$$U_i = 1 - \text{MTBF} / (\text{MTBF} + (1 - P_i) \times (T_i / 2) + \text{MTTR})$$

T_i = Manual Test interval

$$\text{MTBF} = 1 / \lambda_i$$

T_i and MTTR are unique values for each application.

7.3.4 Detailed Controller Reliability Analysis

7.3.4.1 Subsystem

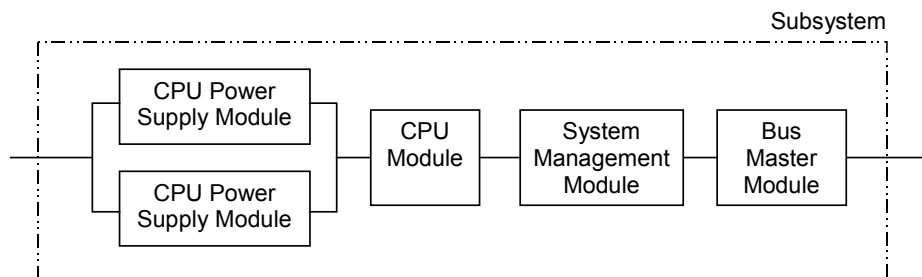


Figure 7.3-4 Reliability Model of Subsystem

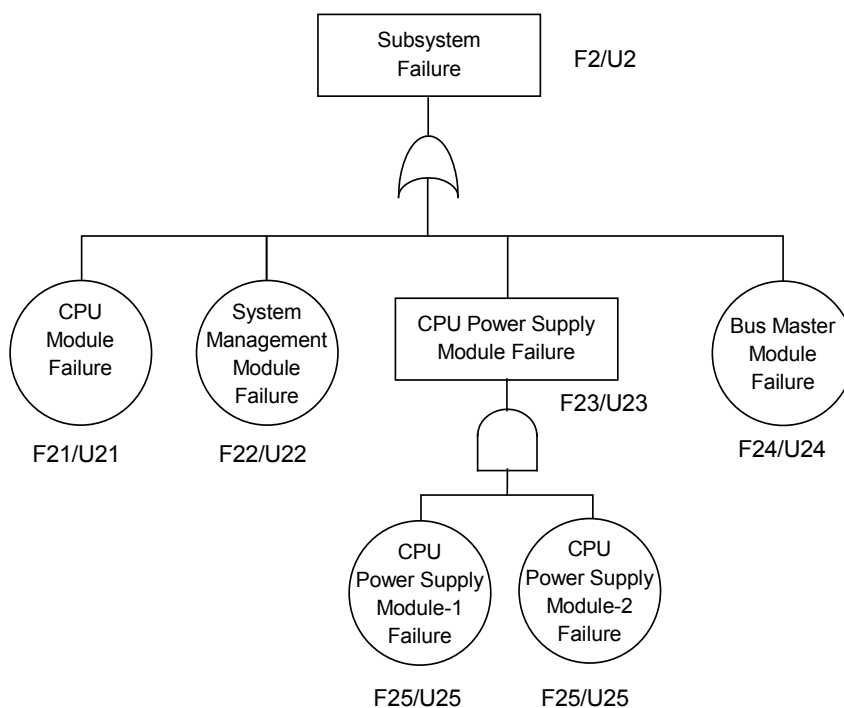


Figure 7.3-5 Fault Tree of Subsystem

Failure rate of Subsystem (F2) is as follows.

$$F2 = F21 + F22 + F23 + F24$$

$$F23 = F25 \times F25 \times \text{MTTR} \times 2$$

Unavailability of Subsystem (U2) is as follows.

$$U2 = U21 + U22 + U23 + U24$$

$$U23 = U25 \times U25$$

7.3.4.2 Dedicated I/O (Input/Output)

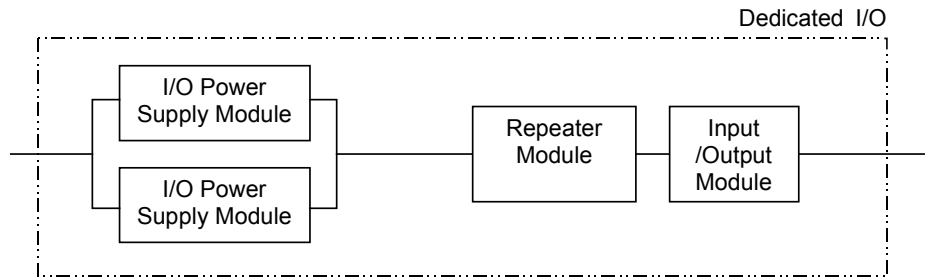


Figure 7.3-6 Reliability Model of Dedicated I/O

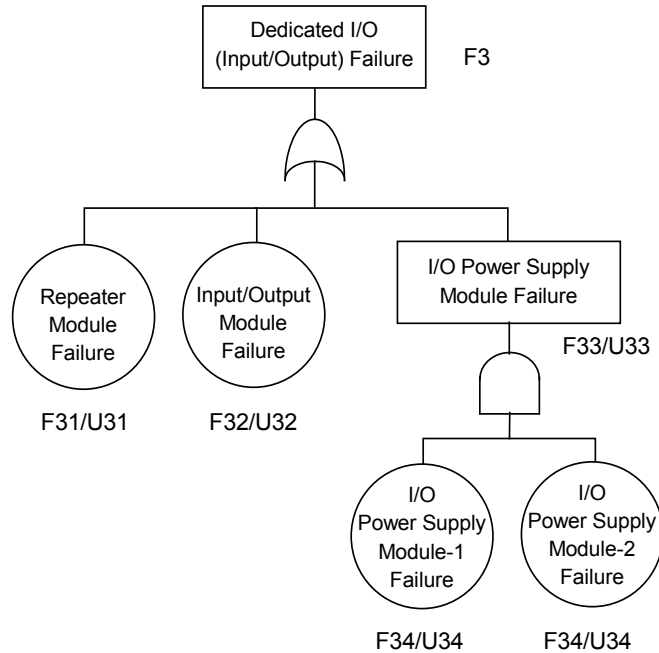


Figure 7.3-7 Fault Tree of Dedicated I/O

Failure rate of Subsystem ($F3$) is as follows.

$$F3 = F31 + F32 + F33$$

$$F33 = F34 \times F34 \times \text{MTTR} \times 2$$

Unavailability of Subsystem ($U3$) is as follows.

$$U3 = U31 + U32 + U33$$

$$U33 = U34 \times U34$$

7.3.4.3 Input/Output Line

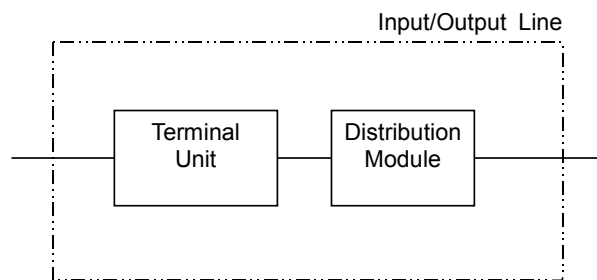


Figure 7.3-8 Input/Output Line

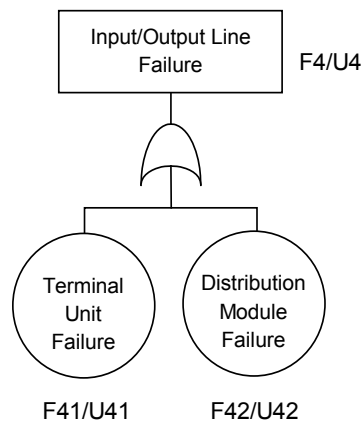


Figure 7.3-9 Fault Tree of Input/Output Line

Failure rate of Subsystem (F4) is as follows.

$$F4 = F41 + F42$$

Unavailability of Subsystem (U4) is as follows.

$$U4 = U41 + U42$$

7.4 Failure Mode and Effects Analysis (FMEA)

This section describes the method for conducting the FMEA, which is the method of determining the failure mode for each type of MELTAC Module and the resulting effects at the Controller level. The effects of failures at the system application level are described in the Safety I&C System Description and Design Process Topical Report.

The method of conducting the FMEA is as follows:.

- Module circuits are divided into function blocks.
- Determine the failure modes of the function block.
- Determine the state(s) of the module output(s) caused by the failure mode(s) of the function block.
- Determine the effects at the Controller level based on the module output failure states.

For a module to be 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 by the self-diagnosis function through a combination of modules.

The parts that do not affect the control function are identified through the FMEA, such as RS-232C communication port which is used only for CPU Module debugging,

For a module to be 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 contact of the relay output module 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.

7.5 Periodic Replacement Equipment (Parts) to Keep Reliability

Some components within the MELTAC Platform have service life limits due to age related failure mechanisms. As shown in Figure 7.5-1, the failure rate of these components rises as the component reaches its service life limit. Therefore, it is necessary to periodically replace those components to maintain platform reliability.

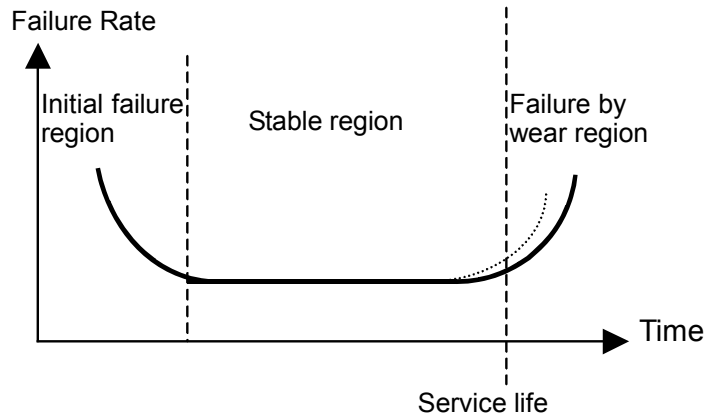


Figure 7.5-1 Failure Rate Curve

The components of the digital platform that have a known limited service life are as follows:

- a) Capacitor within Power Supplies
- b) Fan Fuse
- c) Liquid Crystal Display within Safety VDU Panel

For item a) above, the entire power supply module should be replaced. For item b) above, the fuse inside the fan unit should be replaced without replacing the entire fan unit. For item c) above, the entire Safety VDU Panel should be replaced. Parts may be replaced at any time with the equipment energized or de-energized. Any on-line replacement restrictions are governed only by specific plant applications.

The periodic replacement parts are as shown in Table 7.5-1.

Table 7.5-1 List of Periodic Replacement Parts

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

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

APPENDIX A HARDWARE SPECIFICATIONS**Appendix A.1 CPU Module PCPJ-11 Specification**

Item	Specification
CPU	intel Pentium 133MHz
Memory	High-speed SRAM: 2Mbytes Low-speed SRAM: 4Mbytes EPROM: 1Mbyte Flash memory: 8Mbytes Local RAM: 512kbytes
Current consumption	+5V: 2.7A
External dimensions	290×265×25(mm)
Hot-pluggability	Power supply must be disabled when plugging module off.

Appendix A.2 System Management Module Specification

Item	Specification
Communication Between Redundant Subsystems	Optical module transmission speed: 100Mbps Maximum transmission distance: 100m
System DI	Number of inputs: 32 Rated voltage: 24V (30V, maximum) external supply Contact current: 3mA Dielectric voltage: AC500V
System DO	Number of outputs: 11 Rated voltage: 24V (30V, maximum) Rated current: 50mA (100mA, maximum) Dielectric voltage: AC500V
CPU	intel 80960 (33.3MHz)
Onboard memory	2-port memory:1Mbyte Dedicated transmission memory:1Mbyte Dedicated receiving memory:1Mbyte Local memory:1Mbyte EPROM:512kbyte Flash memory:4Mbyte
Ethernet I/F	Module Chassis, rear side: 10Mbps 1ch module front side: 100Mbps/10Mbps (Speed: Automatically switched), 2ch
Current consumption	+5V: 9A
External dimension	290X265X20(mm)
Hot-pluggability	Power supply must be disabled when plugging module off.

Appendix A.3 Bus Master Module Specification

Item	Specification
Protocol	1:N master poling (Case of Communication with I/O) One way communication (Case of data link communication)
Configuration	Number of channels: 4 channels/module (Whether to use communication with I/O or serial data link communication can be defined for each channel.)
Interface	RS-485 transformer insulation.
Baud rate	1Mbps
Error detection method	CRC check
Transmission capacity	1kbyte/channel maximum (Case of Communication with I/O) 3kbyte/channel maximum (Case of data link communication)
Onboard memory	Dedicated transmission memory: 1Mbyte (256kbyte/channel)
Current consumption	+5V: 2.5A
External dimension	290X265X30(mm)
Hot-pluggability	Power supply must be disabled when plugging module off.

Appendix A.4 Control Network I/F Module Specification

Item	Specification
Protocol	Communication method: Cyclic Multiplexing method: RPR (Resilient Packet Ring) IEEE std 802.17
Configuration	Loop (redundant)
Medium	Optical fiber
Speed	Transmission rate: 1Gbps
Capacity	Transmission capacity: - 256kbytes, maximum for normal speed communication - 128kbytes, maximum for high speed communication Number of connected stations: - 126 stations, maximum for normal speed communication - 32 stations, maximum for high speed communication Distance between stations: - 2km, maximum
CPU	intel 80200 (400MHz)
Current consumption	+5V: 5.3A
External dimension	290X265X30(mm)
Error detection	CRC detection
Hot-pluggability	Power supply must be disabled when plugging module off.

Appendix A.5 I/O Module Specification**Analog Input Module Specifications**

Module Model	Function	Main Specifications	Remarks
MLPJ-01	Current input	AI: 1 input/module 4 to 20mA (Transmitter power supply is provided.) Input impedance: 10M Ω or greater Accuracy**: $\pm 0.25\%$ FS Temperature coefficient: ± 50 ppm/ $^{\circ}$ C	
MLPJ-02	Current input	AI: 1 input/module 4 to 20mA (Transmitter power supply is provided.) Input impedance: 10M Ω or greater Accuracy**: $\pm 0.25\%$ FS Temperature coefficient: ± 50 ppm/ $^{\circ}$ C * Auto testing function is provided.	For automatic testing *
MRTJ-34	RTD 4 line type	AI: 1 input/module 4-line Pt200 Ω , 32 to 392 $^{\circ}$ F (0 to 200 $^{\circ}$ C) Input impedance: 10M Ω or greater Accuracy**: $\pm 0.25\%$ FS Temperature coefficient: ± 50 ppm/ $^{\circ}$ C	
MRTJ-61	RTD 4 line type	AI: 1 input/module 4-line Pt200 Ω , 32 to 752 $^{\circ}$ F (0 to 400 $^{\circ}$ C) Input impedance: 10M Ω or greater Accuracy**: $\pm 0.25\%$ FS * Auto testing function is provided. Temperature coefficient: ± 50 ppm/ $^{\circ}$ C	For automatic testing *
MRTJ-62	RTD 4 line type	AI: 1 input/module 4-line Pt200 Ω , 500 to 662 $^{\circ}$ F (260 to 350 $^{\circ}$ C) Input impedance: 10M Ω or greater Accuracy**: $\pm 0.25\%$ FS * Auto testing function is provided. Temperature coefficient: ± 50 ppm/ $^{\circ}$ C	For automatic testing *

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

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

Analog Output Modules Specifications

Module Model	Function	Main Specifications	Remarks
MAOJ-01	Current output	AO: 1 output/module Maximum load: 600Ω Accuracy: $\pm 0.25\%$ FS	
MVOJ-01	Voltage output	AO: 1 output/module Minimum load: 500Ω Accuracy: $\pm 0.25\%$ FS	

Digital Input Modules Specifications

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

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

Digital Output Modules Specifications

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

Appendix A.6 Isolation Module Specifications

Module Model	Function	Main Specifications	Remarks
KILJ-01	Current input Current/Voltage output	AI: 1 input/module 4 to 20mA Input impedance: 10MΩ or greater Accuracy: $\pm 0.5\%$ FS Temperature coefficient: ± 100 ppm/°C AO: 1 output/module 4 to 20mA / 0 to 10VDC (selectable)	
KIRJ-01	RTD 4 line type input Current/Voltage output	AI: 1 input/module 4-line Pt100Ω, 32 to 302°F (0 to 150°C) 4-line Pt100Ω, 32 to 392°F (0 to 200°C) 4-line Pt200Ω, 32 to 752°F (0 to 400°C) Input impedance: 10MΩ or greater Accuracy: $\pm 0.5\%$ FS Temperature coefficient: ± 100 ppm/°C AO: 1 output/module 4 to 20mA / 0 to 10VDC (selectable)	
KIDJ-01	Contact input Semiconductor output (open collector)	DI: 2 inputs/module Contact impressed voltage: DC48V DO: 2 outputs/module (power DO) Maximum impressed voltage: AC110V/DC125V Output current: 10mA	

Appendix A.7 E/O Converter Modules Specifications

Module Model	Function	Main Specifications	Remarks
MEOJ-01/02	Electrical/optical conversion	Electrical to Optical: 1 channel Optical to Electrical: 1 channel Electrical interface: RS-485 Optical signal: Single mode optical fiber	

Appendix A.8 Power Interface Modules Specifications

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

Appendix A.9 Power Supply Modules Specifications

Module Model	Function	Main Specifications	Remarks
PS-1	CPU Power Supply	Input voltage: AC85V to AC132V Frequency: 47Hz to 63 Hz Output voltage: DC5V (50A), DC2.1V (11A)	
PS-2	I/O Power Supply	Input voltage: AC85V to AC132V Frequency: 47Hz to 63 Hz Output voltage: DC24V (12A)	
PPSJ-01	CPU Power Supply (Small capacity type)	Input voltage: AC85V to AC132V Frequency: 47Hz to 63 Hz Output voltage: DC5V (30A), DC2.1V (11A)	Mounted at Mirror-split and Slide-split CPU Chassis
PPSJ-11	CPU Power Supply (Large capacity type)	Input voltage: AC85V to AC132V Frequency: 47Hz to 63 Hz Output voltage :DC5V (50A), DC2.1V (11A)	Mounted at non-split CPU Chassis

Appendix A.10 Safety VDU Panel Specification

Item	Specification
Type	Thin Film Transistor Liquid Crystal Display (TFTLCD) module
Operator Interface	Touch interface (Acoustic type)
Communication Interface	<ul style="list-style-type: none"> - Safety VDU Processor to Panel Display signal : RGB, Horizontal Sync (HSYNC), Vertical Sync (VSYNC) - Safety VDU Panel to Processor RS232C electrical or optical fiber with E/O,O/E converters







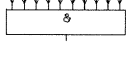
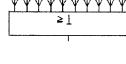
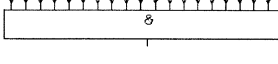
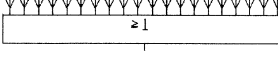
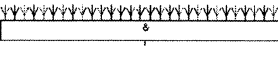

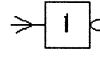
Appendix A.11 FMU Module Specification

Item	Specification
Picture Size	VGA (640*480 dots) to SXGA(1280*1024 dots)
Interface	Coaxial 5-line type (RGBHV)
Memory	Frame Memory (Memory for graphic images): 4Mbytes Font Memory (Memory for symbols, characters bit map data): 4Mbytes

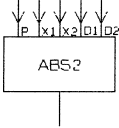
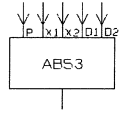
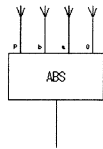


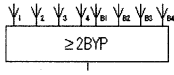
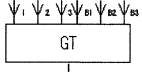
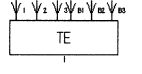
Appendix A.12 Touch Panel Interface Module Specification

Item	Specification
Configuration	1:1 serial interface
Communication Medium	RS-232C.
Medium	Electrical Interface or Optical fiber with E/O Converter if the distance exceeds 15 meters
Speed	Baud rate: 76.8 kbps
Capacity	Number of channels: 2 channels/module (Only one channel is used) Transmission capacity: 2kbytes/channel for acceptance 2kbytes/channel for sending
Error Detection	Parity check

APPENDIX B FUNCTIONAL SYMBOL SOFTWARE SPECIFICATIONS**List of Function Symbols Discrete Control Processes**

No	Symbol	Name	Function
1		AND	Defines the output signal (Y) with respect to the input signals (X_1, X_2) as follows: $Y = X_1 \text{ and } X_2$
2		OR	Defines the output signal (Y) with respect to the input signals (X_1, X_2) as follows: $Y = X_1 \text{ or } X_2$
3		AND3	Defines the output signal (Y) with respect to the input signals (X_1, X_2, X_3) as follows: $Y = X_1 \text{ and } X_2 \text{ and } X_3$
4		OR3	Defines the output signal (Y) with respect to the input signals (X_1, X_2, X_3) as follows: $Y = X_1 \text{ or } X_2 \text{ or } X_3$
5		AND4	Defines the output signal (Y) with respect to the input signals (X_1, X_2, X_3, X_4) as follows: $Y = X_1 \text{ and } X_2 \text{ and } X_3 \text{ and } X_4$
6		OR4	Defines the output signal (Y) with respect to the input signals (X_1, X_2, X_3, X_4) as follows: $Y = X_1 \text{ or } X_2 \text{ or } X_3 \text{ or } X_4$
7		AND5	Defines the output signal (Y) with respect to the input signals (X_1, X_2, X_3, X_4, X_5) as follows: $Y = X_1 \text{ and } X_2 \text{ and } X_3 \text{ and } X_4 \text{ and } X_5$
8		OR5	Defines the output signal (Y) with respect to the input signals (X_1, X_2, X_3, X_4, X_5) as follows: $Y = X_1 \text{ or } X_2 \text{ or } X_3 \text{ or } X_4 \text{ or } X_5$
9		AND10	Defines the output signal (Y) with respect to the input signals (X_1, X_2, \dots, X_{10}) as follows: $Y = X_1 \text{ and } X_2 \text{ and } \dots \text{ and } X_{10}$
10		OR10	Defines the output signal (Y) with respect to the input signals (X_1, X_2, \dots, X_{10}) as follows: $Y = X_1 \text{ or } X_2 \text{ or } \dots \text{ or } X_{10}$
11		AND20	Defines the output signal (Y) with respect to the input signals (X_1, X_2, \dots, X_{20}) as follows: $Y = X_1 \text{ and } X_2 \text{ and } \dots \text{ and } X_{20}$
12		OR20	Defines the output signal (Y) with respect to the input signals (X_1, X_2, \dots, X_{20}) as follows: $Y = X_1 \text{ or } X_2 \text{ or } \dots \text{ or } X_{20}$
13		AND30	Defines the output signal (Y) with respect to the input signals (X_1, X_2, \dots, X_{30}) as follows: $Y = X_1 \text{ and } X_2 \text{ and } \dots \text{ and } X_{30}$
14		OR30	Defines the output signal (Y) with respect to the input signals (X_1, X_2, \dots, X_{30}) as follows: $Y = X_1 \text{ or } X_2 \text{ or } \dots \text{ or } X_{30}$
15		NOT	Defines the output signal (Y) with respect to the input signals (X) as follows: $Y = \bar{X}$

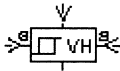

No	Symbol	Name	Function
16		ON DELAY TIMER	Turns the output signal ON after the delay time when the input signal changes from OFF to ON.
17		OFF DELAY TIMER	Turns the output signal OFF after the delay time when the input signal changes from ON to OFF.
18		ONE SHOT TIMER	Turns the output signal ON only for a set time span when the input signal changes from OFF to ON.
19		FLIP-FLOP	Latches output ON with Set signal input, and clears output with Reset signal input.
20		2 out of 3	Outputs if 2 or more inputs out of 3 inputs are ON.
21		2 out of 4	Outputs if 2 or more inputs out of 4 inputs are ON.
22		3 out of 4	Outputs if 3 or more inputs out of 4 inputs are ON.
23		1-INPUT FLIP-FLOP	Inverse-outputs the output signal every time the input signal changes OFF (0) -> ON (1).
24		1-INPUT FLIP-FLOP WITH RESET	Performs same 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 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 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 computation.

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 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 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 computation.
31		ON FIXED OUTPUT	Outputs the ON signal.
32		OFF FIXED OUTPUT	Outputs the OFF signal.
33		2/4-LOGIC WITH BYPASS FUNCTION	Outputs if 2 or more inputs 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	Provided with the bypass function for the partial trip. Outputs status to the multi-bypass input tag.
35		TRIP ENABLE LOGIC	Provided with the bypass function for the partial trip.















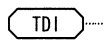
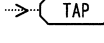
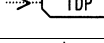


List of Function Symbols Analog Control Processes

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		SUBTRACTOR	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		MULTIPLIER	Defines the output signal (Y) with respect to the input signals (X_1 , X_2) as follows: $Y = X_1 \times X_2$
5		DIVIDER	Defines the output signal (Y) with respect to the input signals (X_1 , X_2) as follows: $Y = X_1 \div X_2$
6		ABSOLUTE VALUE	Defines the output signal (Y) with respect to the input signals (X) as follows: $Y = X $
7		SQUARE ROOT	Defines the output signal (Y) with respect to the input signals (X) as follows: $Y = G \cdot \sqrt{X}$
8		DEAD ZONE	Defines the output signal (Y) with respect to the input signals (X) as follows: $d_1 < X, d_2 > X \quad Y = X$ $d_2 \leq X \leq d_1 \quad Y = (d_1 + d_2)/2$
9		HIGH SIGNAL SELECTOR / LOWER LIMIT CONTROLLER	Defines the output signal (Y) with respect to the input signals (X_1 , X_2) as follows: $X_1 < X_2 \quad Y = X_2, \quad X_1 = X_2 \text{ or } X_1 > X_2 \quad Y = X_1$
10		LOW SIGNAL SELECTOR / UPPER LIMIT CONTROLLER	Defines the output signal (Y) with respect to the input signals (X_1 , X_2) as follows: $X_1 = X_2 \text{ or } X_1 < X_2 \quad Y = X_1, \quad X_1 > X_2 \quad Y = X_2$
11		UPPER LIMIT MONITOR	Outputs an output signal when the input signal reaches a set value. At the time the system is reset, the input signal is below the gap with respect to the set value.
12		LOWER LIMIT MONITOR	Outputs an output signal when the input signal reaches a set value. At the time the system is reset, the input signal is below the gap with respect to the set value.
13		PROPORTIONAL	Outputs an output signal with a proportional constant in response to the input signal.





No.	Symbol	Name	Function
14		DIFFERENTIATION	Outputs a differentiated output signal in response to the input signal.
15		LAG	Outputs the lag operation results as the output signal in response to the input signal.
16		LEAD/LAG	Outputs the lead/lag operation results as the output signal in response to the input signal.
17		SIGNAL SWITCH	Switches the digital input signal (SW) in response to the input signals (X_1 , X_2) and outputs the output signal (Y). $SW=1 \ Y=X_1$, $SW=0 \ Y=X_2$
18		DEAD TIME	Outputs an output signal in response to the input signal after delaying output for a specified period of time.
19		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.
20		SIGNAL GENERATOR	Outputs a set value
21		LOGISTICS CONVERSION	Outputs the results of logistics output computation to the input signal.
22		4-CH 2ND-HI SIGNAL SELECTOR	Selects the 2nd High to the 4-ch analog value.
23		4-CH MEAN VALUE SIGNAL SELECTOR	Outputs the mean to the 4-ch analog value (for 3 groups).
24		4-CH MEAN VALUE SIGNAL SELECTOR	Outputs the mean to the 4-ch analog value (for 4 groups).
25		20-POLYGONAL LINE FUNCTION	Outputs the polygonal function of up to 20 points to the input signal.
26		3-CH INTERMEDIATE VALUE SIGNAL SELECTOR	Outputs the intermediate value to the 3-ch analog input signal.
27		UPPER/LOWER LIMIT LIMITER	Outputs the output signal within the set range of the output upper/lower limit to the input signal.

No.	Symbol	Name	Function
28		VARIABLE UPPER LIMIT MONITOR	Outputs the output 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.)
29		ANALOG SIGNAL BCD CONVERSION	Converts the analog signal to the BCD code.

The Function Symbols for Input and Output Process

No	Symbol	Name
1		ANALOG INPUT
2		ANALOG OUTPUT
3		DIGITAL INPUT
4		DIGITAL OUTPUT
5		POWER I/F INPUT
6		POWER I/F OUTPUT
7		COMMUNICATION INPUT (ANALOG)
8		COMMUNICATION OUTPUT (ANALOG)
9		COMMUNICATION INPUT (DIGITAL)
10		COMMUNICATION OUTPUT (DIGITAL)
11		STATUS COMMUNICATION INPUT (DIGITAL)
12		STATUS COMMUNICATION OUTPUT (DIGITAL)
13		OPERATION SIGNAL COMMUNICATION INPUT (ANALOG)
14		OPERATION SIGNAL COMMUNICATION INPUT (DIGITAL)
15		TEST INPUT
16		ANALOG TEST OUTPUT
17		DIGITAL TEST OUTPUT
18		APPLICATION DIAGNOSIS ERROR OUTPUT
19		ANSWER BACK ERROR DIAGNOSIS OUTPUT

The Function Symbols for Status Getting and Setting

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