Common Cause Failure Potential for Safety System Digital Platform - MELTAC

Non Proprietary Version

December 2007

Prepared: Tomonori Yamane — 11/01/'07
Tomonori Yamane, Manager
DCS Development Section
Date

Prepared: Shigeru Sugitani — 11/01/'07
Shigeru Sugitani, Manager
Control & Protection Systems Section
Date

Reviewed: Hidetoshi Matsushita — 11/01/'07
Hidetoshi Matsushita, Manager
Control & Protection Systems Section
Date

Approved: Tokihiro Fukuhara — 11/01/'07
Tokihiro Fukuhara, Section Manager
Control & Protection Systems Section
Date

Approved: Toru Ito — 11/01/'07
Toru Ito, Project Manager
Nuclear Power Department
Date

Approved: Shuichi Kobashi — 11/01/'07
Shuichi Kobashi, Department Manager
Nuclear Power Department
Date

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

List of Acronyms

CCF	Common Cause Failure
CFR	Code of Federal Regulations
COTS	Commercial Off The Shelf
CPU	Central Processing Unit
DAS	Diverse Actuation System
FBD	Functional Block Diagram
FMU	Frame Memory Unit
F-ROM	Flash Electrically Erasable Programmable Read Only Memory
GBD	Graphic Block Diagram
GUI	Graphic User Interface
IEEE	Institute of Electrical and Electronics Engineers
I/O	Input/Output
MELENS	Mitsubishi Electric Total Advanced Controller Engineering Station
MELCO	Mitsubishi Electric Corporation
MELTAC	Mitsubishi Electric Total Advanced Controller
MHI	Mitsubishi Heavy Industries, Ltd.
NPD	Nuclear Power Department in Mitsubishi Electric Corporation
NRC	Nuclear Regulatory Commission
QA	Quality Assurance
QAP	Quality Assurance Program
RAM	Random Access Memory
RG	Regulatory Guide
ROM	Read Only Memory
SPC	Standard Parts Committee
SPL	Standard Parts List
VDU	Visual Display Unit
V&V	Verification and Validation
UCP	MELTAC US Conformance Program
UV-ROM	Ultra-Violet Erasable Programmable Read Only Memory

1.0 INTRODUCTION

1.1 Purpose

All safety and control systems provided by Mitsubishi Heavy Industries are built on the MELTAC digital platform, from Mitsubishi Electric Corporation (MELCO). MHI has submitted a Topical Report to obtain NRC approval of the MELTAC platform for nuclear safety applications. A second Topical Report has been submitted to obtain NRC approval of specific safety system designs which utilize the MELTAC platform. A third Topical Report has been submitted to obtain NRC approval for MHI's approach to Defense-in-Depth and Diversity. These docketed Topical Reports describe the basic features of these systems that result in a low common cause failure (CCF) probability. However, regardless of this low probability, all of these Topical Reports still assume that a CCF exists that could completely disable all functions performed by the MELTAC systems. Therefore, MHI provides a Diverse Actuation System (DAS) to cope with plant accidents with a concurrent CCF that disables all of the MELTAC systems.

Although MHI has committed to provide a DAS to accommodate an assumed CCF in the MELTAC systems, MHI believes this may be an overly conservative and complicated solution for a CCF that has very low probability. MHI has taken this conservative licensing approach due to the lack of regulatory guidance that would allow an applicant to demonstrate that the probability of a CCF is sufficiently low to preclude the need for diverse backups. This report is intended to assist NRC Research in developing that regulatory guidance.

This report describes the attributes of the MELTAC design and design process that contribute to a low probability of CCF. MHI believes these attributes can form the basis of regulatory guidance that would allow an applicant to demonstrate that the potential for CCF in the digital platform is insignificant and therefore allows CCF of the platform to be eliminated from consideration. Eliminating consideration of platform CCF could lead to a defense-in-depth strategy that credits application functional diversity in the overall I&C system design. Application functional diversity is not a subject of this report.

1.2 MELTAC Platform Overview

The MELTAC Platform is the basis of the Mitsubishi Heavy Industries (MHI) safety and non-safety digital I&C systems. MELTAC is the digital platform for nuclear application with the following key design features:

- Modular structure hardware allowing various configurations for nuclear applications needs
- Simple single task, no-interruption Basic Software architecture [
  ]
- Easy application programming by combining simple Graphical Block Diagram (GBD), which represents functional modules

[

]

- Hardware qualification by Environmental, Seismic and Electromagnetic tests

1.3 Structure of the Report

Section 2 provides the development and operational history of the MELTAC platform. Section 3 presents MELTAC Hardware/Software design related to safety. Section 4 presents MELTAC life cycle (Development, V&V and corrective action processes). Section 5 provides a conclusion.

2.0 MELTAC DEVELOPMENT AND OPERATING HISTORY

Figure 1.3-1 summaries the history of the MELTAC development, the records of operation, and the application plans.

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.

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.
e) There has never been an error in the platform hardware or software design that would have prevented proper execution of the application function.

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.

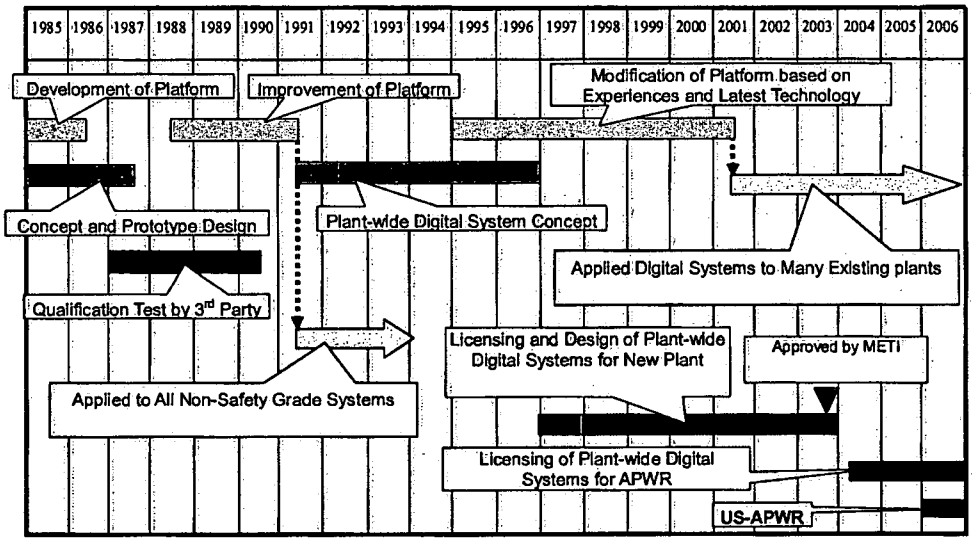


Figure 1.3-1 MELTAC Development and Operating History

3.0 MELTAC HARDWARE/SOFTWARE DESIGN

This section describes the basic hardware and software components of the MELTAC platform.

3.1 MELTAC System Configuration

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

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

Plant safety systems have multiple divisions. A typical configuration of the MELTAC Platform for a single division of a plant safety system with an interface to a Controller in another division is described in Figure 3.1-1.

The Controller runs Application Software on top of the Basic Software and performs Input/Output (I/O) and network communication.
[

]

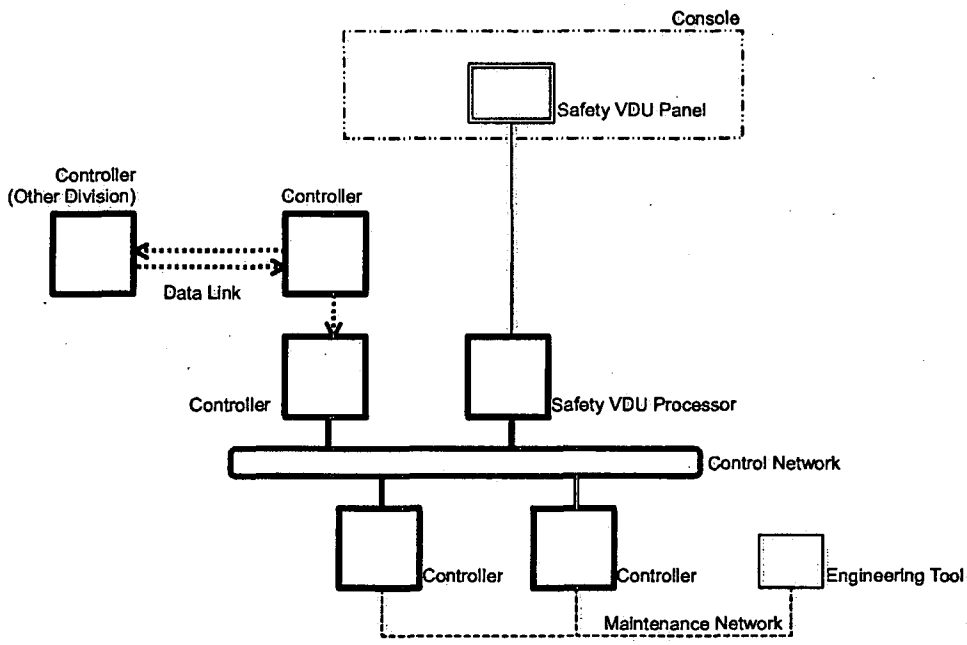


Figure 3.1-1 Typical Configuration of MELTAC Platform

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. However, it is noted that the Redundant Standby Controller Configuration is not used in the MHI 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.

As an example, the Redundant Parallel Controller Configuration is shown in Figure 3.1-2.

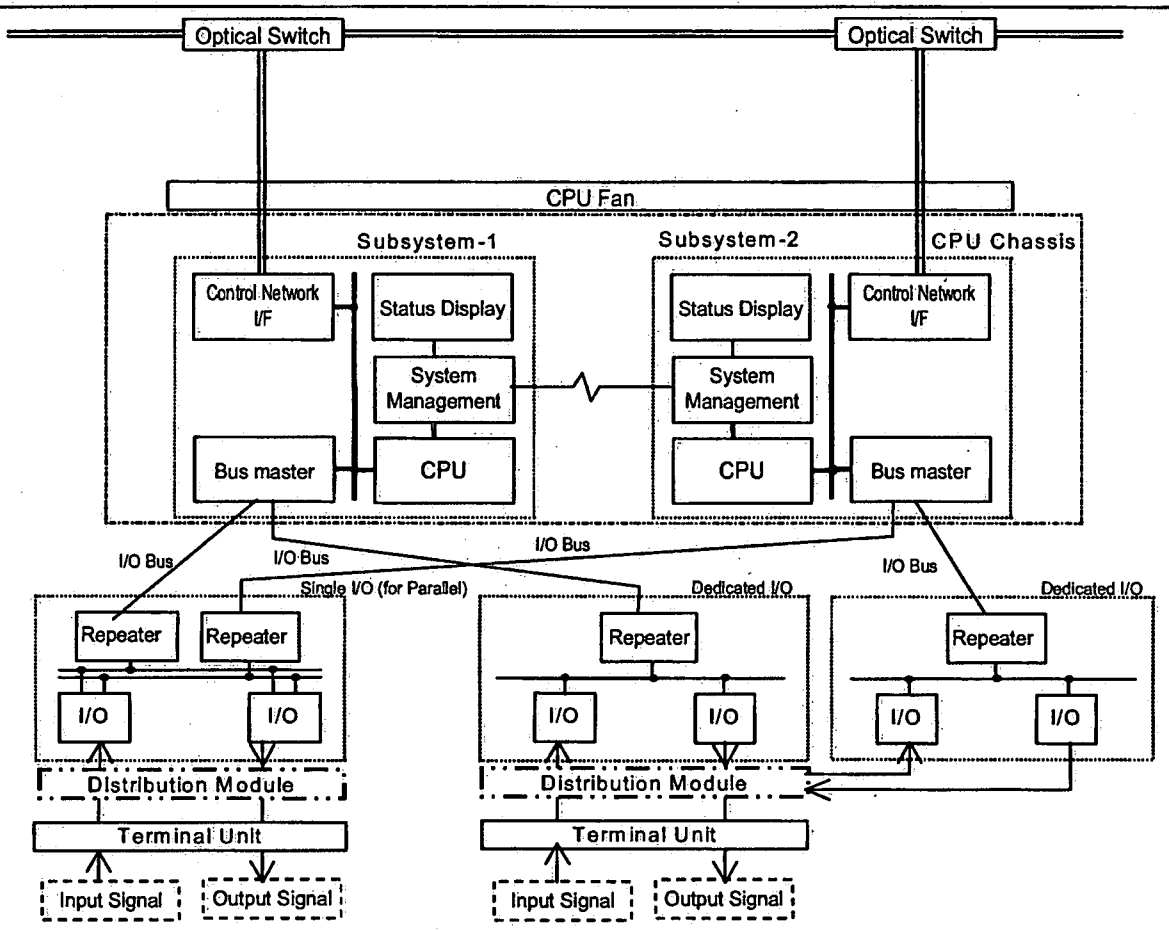


Figure 3.1-2 Redundant Parallel Controller Configuration

Each module is qualified by Environmental, Seismic and Electromagnetic tests and conforms to the corresponding U.S. standards.

3.2 MELTAC Communication Subsystem Design

The Control Network is used to communicate data between multiple Controllers, and between Controllers and the Safety VDU Processor(s), all in the same division. A separate 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.

Data Links are used to transmit process signals between the Controllers in different safety divisions. A separate unidirectional Data Link is used for sending data from each division (e.g. A to B, C, D; B to A, C, D; etc.) Separate Data Links are used so there is no single failure in the communication interface that can adversely affect the data originating from more than one division.

Both Control Network and Data Link have electrical and communication isolation necessary for nuclear applications. Electrical isolation ensures faults cannot propagate between safety divisions. Communication isolation, using 2 port memory and only predetermined data sets,

ensures that the deterministic functional operation of both the sending and receiving MELTAC controllers cannot be disrupted by the data communications interface.

3.3 Hardware Components

[

]

3.4 MELTAC Software Design

3.4.1 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.
[

]
These basic design principles used in the Basic Software ensure thorough V&V, including completely transparent white box testing.

The processes within the Basic Software and the order of their execution are shown in Figure 3.4-1.

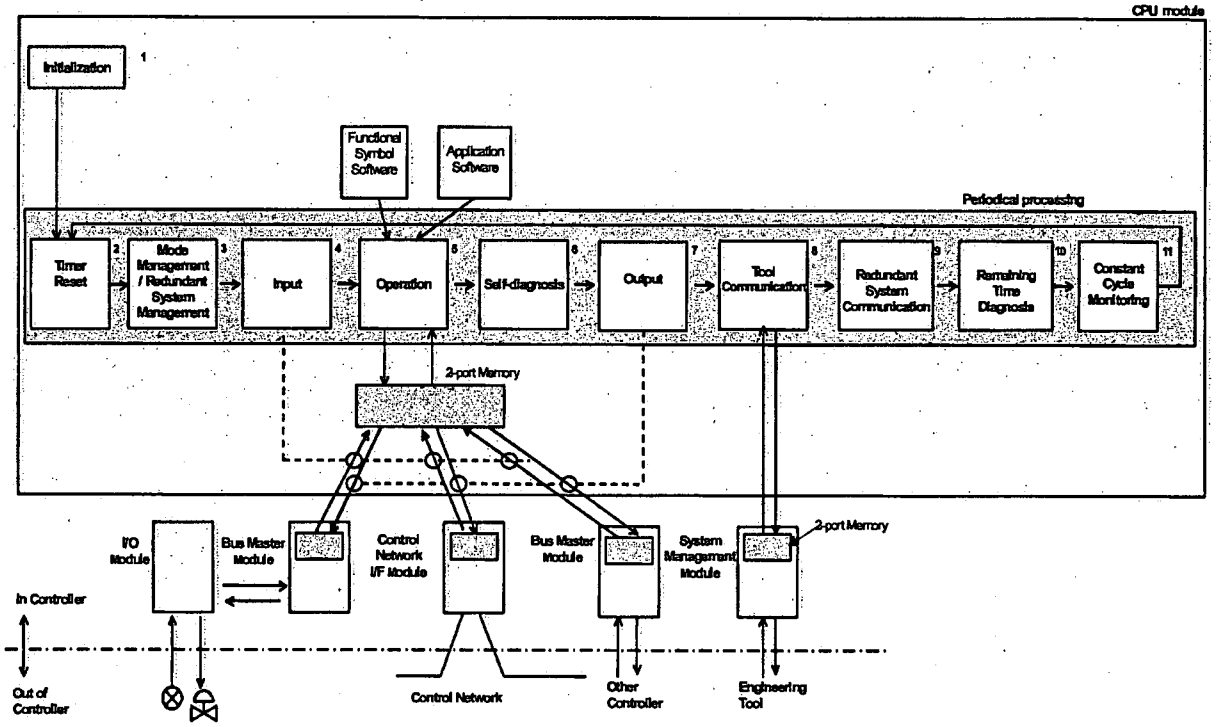


Figure 3.4-1 Basic Software Processes and Execution Order

The processes of the MELTAC Basic Software are described below.
[

]
The Basic Software and Hardware are designed to ensure the Engineering Tool cannot disrupt deterministic execution of the Basic Software as follows:
[

]

3.4.2 Application Software

The Application Software of the MELTAC Platform is designed using the Engineering Tool (called "MELENS"). Application Software for functional algorithms is designed by combining simple graphical logic symbols such as "And", "Or", and "Not" using the Graphical User

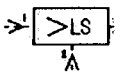
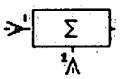
Interface (GUI) of the Engineering Tool. A GUI is used to reduce the potential for design errors in building or modifying the application software. It also makes it easier for the Independent Verifier to ensure the Application Software Graphical Block Diagrams (GBD), which are created by the I&C system 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. The application designer can manually verify the Execution Data, however this is not necessary since errors can be detected during application level testing.

Application Software Execution Data is stored in the F-ROM of the CPU module.

The examples of graphical logic symbols are listed below.

Example of Graphical Logic Symbols

Symbol	Name	Function
	OR3	Defines the output signal (Y) with respect to the input signals (X_1, X_2, X_3) as follows: $Y= X_1$ or X_2 or X_3
	2 out of 3	Outputs if 2 or more inputs out of 3 inputs are ON.
	LOW SIGNAL SELECTOR / UPPER LIMIT CONTROLLER	Defines the output signal (Y) with respect to the input signals (X_1, X_2) as follows: $X_1=X_2$ or $X_1<X_2$ $Y=X_1$, $X_1>X_2$ $Y=X_2$
	ADDER-SUBTRACTOR	Defines the output signal (Y) with respect to the input signals (X_1, X_2) as follows: $Y= G_1 \cdot X_1+G_2 \cdot X_2$
	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.)
	ANALOG INPUT	
	DIGITAL INPUT	
	DIGITAL OUTPUT	

[

]

3.5 MELTAC Self Testing

The MELTAC Platform has built-in self-testing features. They are for detecting hardware or software defects. The details of these features, including hardware based watchdog timers, are described in Sections 4.1.5 and 4.2.3 of the MELTAC Platform Topical Report. Among them, several features contribute to reducing CCF probability.
[

]

4.0 LIFE CYCLE

4.1 Development Quality Program

The original quality assurance program (referred to as Original QAP) used for the MELTAC Platform development was based on the Japanese Regulatory Requirements. Since MELCO now plans to apply the platform to safety systems in US nuclear facilities, a new quality assurance program has been adopted as NPD Procedure for Safety System Platform Quality Assurance Program (referred to as NQAP). NQAP addresses all requirements of 10CFR Part 50 Appendix B and IEEE7-4.3.2-2003, including the applicable Regulatory Guides and IEEE software standards. NQAP covers the following requirements:

- Quality Assurance
- Management
- Development and V&V (RG1.168 and IEEE1012-1998)
- Configuration Management (RG1.169 and IEEE828-1990)
- Cyber Security Management (RG1.152)
- Software Safety Plan

All new MELTAC development or revisions to current platform components will be in accordance with NQAP.
[

]

4.2 Verification and Validation

NQAP defines six activity phases - Platform Design, Software Design, Program Design, Coding, Unit Test, and Integration Test. The activities for Program Design, Coding, and Unit Test are executed separately for each software unit. All verification activities defined above are conducted by appropriate checklists and fully controlled by MELCO.

- Since MELCO developed the MELTAC Basic Software Design from scratch, we can guarantee that only necessary and documented features are included.

[

]

4.3 Failure and Error Reporting and Corrective Action

[

]

4.4 Obsolescence Management

[

]

5.0 CONCLUSION

There are many attributes of the MELTAC Platform discussed in this report that contribute to a conclusion that the MELTAC Platform basic hardware and software have no hidden defects that could lead to Common Cause Failure.

MELTAC Platform was developed by MELCO for various nuclear applications. The design, qualification and Life Cycle management processes conform to all U.S. Regulatory requirements. The reliability of the Basic Software is ensured by the combination of a very simple deterministic software architecture and extensive V&V.
[

]
MELCO is directly engaged in the operations and maintenance life cycle of the equipment. Field records in Japan demonstrate the reliability of the MELTAC platform. During the course of the phased field experience from non-safety applications to safety applications there have been no errors in the Basic Software that would adversely impact the critical functional operation of the system.

Reference
Topical Report "Safety System Digital Platform - MELTAC " JEXU-1012-1002P (MUAP-07005-P)