Summary of MELTAC Platform Reliability

Non-Proprietary

May 2016

Prepared:	Akira Kubo Akira Kubo, Engineer Control & Protection Systems Section, Nuclear Power Department	May 30, 2016 Date	Kazuhiro Eguchi Kazuhiro Eguchi, Manager Radiation Monitoring Instrumentation Section, Nuclear Power Department	May 30, 2016 Date
Reviewed:	Manabu Taniguchi Manabu Taniguchi, Manager Control & Protection Systems Section, Nuclear Power Department	May. 30. 2016 Date	Shingo Nakamura Shingo Nakamura, Manager Radiation Monitoring Instrumentation Section, Nuclear Power Department	May. 30, 2016 Date
Approved:	Shigeru Sugitani Shigeru Sugitani, Senior Manager Control & Protection Systems Section, Nuclear Power Department	May. 30, 2016 Date	Yasuo Uranaka Yasuo Uranaka, Senior Manager Radiation Monitoring Instrumentation Section, Nuclear Power Department	May. 30, 2016 Date

Signature History

	Rev.0, January 2015			
Prepared	Tomohide Ishikawa			
Reviewed	Manabu Taniguchi			
Approved	Hidetoshi Matsushita			

Revision History

Revision	Date	Page (section)	Description
0	January 2015	All	Initial issue
1	May 2016	0-6,8, 10,13 (List of Tables,6.0, 7.3,8.3) 10,11,13 (7.3,8.3) 13 (8.3)	- Deleted Table 3 “List of MELTAC Platform Modules” to avoid repetition of the description regarding the modules type. - Modified the table number as below. From Table 4 to Table 3 From Table 5 to Table 4 - Modified information described in Table 3 and Table 4 to be consistent with JEXU-1041-1008. - Updated the summary information regarding the FMEA results.

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

Table of Contents

List of Tables

1.0 INTRODUCTION

This summary describes the reliability analysis and the Failure Mode and Effects Analysis (FMEA) associated with the Mitsubishi Electric Corporation (MELCO) Energy Systems Center (ESC) Mitsubishi Electric Total Advanced Controller (MELTAC) Platform. The reliability analysis and FMEA encompass the MELTAC Platform hardware and the basic software, which includes the firmware and Field Programmable Gate Arrays (FPGAs) on all MELTAC Platform modules.

The “Safety System Digital Platform - MELTAC - Topical Report” (JEXU-1041-1008) section 7.2 “Controller Reliability Analysis” provides an example safety system reliability analysis to satisfy the reliability requirements in Digital I&C-ISG-06 “Digital Instrumentation & Control Licensing Process”. The system-level reliability analysis requires several variables related to the MELTAC Platform and the specific application.

This document supports the “Safety System Digital Platform - MELTAC - Topical Report” (JEXU-1041-1008) and satisfies the commitments made under Table 1 sections 2.8 and 2.15 of “Mapping of MELTAC Platform Licensing Documents to the Digital I&C-ISG-06 Guidance” (JEXU-1041-1012).

2.0 REFERENCES

Document Name	Document Number	Revision
Safety System Digital Platform –MELTAC– Topical Report	JEXU-1041-1008	Current
Mapping of MELTAC Platform Licensing Documents to the Digital I&C-ISG-06 Guidance”	JEXU-1041-1012	Current
Digital I&C-ISG-06 “Digital Instrumentation & Control Licensing Process”	ML110140103	1
Military Handbook: Reliability Prediction of Electronic Equipment	MIL-HDBK-217F	F
General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems	IEEE Std. 352-1987	1987
Summary of MELTAC Platform QA	JEXU-1041-1025	Current
Quality Manual Based on U.S. Nuclear Regulations	ARQ-14P001	Current
MELTAC Software Program Manual	JEXU-1041-1016	Current
Criteria for Safety Systems for Nuclear Power Generating Stations	IEEE Std. 603-1991	1991
Guidance on Software Reviews for Digital Computer-Based I&C Systems	NUREG 0800 BTP 7-14	2007
Criteria for use of Computer in Safety Systems for Nuclear Power Plants	RG 1.152	3
Criteria for Digital Computers in Safety Systems for Nuclear Power Generating Stations	IEEE Std. 7-4.3.2-2003	2003

Document Name	Document Number	Revision
Verification, Validation, Reviews, and Audits for Digital Computer Software used in Safety Systems of Nuclear Power Plants	RG 1.168	2
IEEE Standard for Software Verification and Validation	IEEE Std. 1012-2004	2004
IEEE Standard for Software Reviews and Audits	IEEE Std. 1028-2008	2008
Configuration Management Plans for Digital Computer Software used in Safety Systems of Nuclear Power Plants	RG 1.169	1
IEEE Standard for Software Configuration Management Plans	IEEE Std. 828-2005	2005
Software Test Documentation for Digital Computer Software used in Safety Systems of Nuclear Power Plants	RG 1.170	1
IEEE Standard for Software and System Test Documentation	IEEE Std. 829-2008	
Software Unit Testing for Digital Computer Software used in Safety Systems of Nuclear Power Plants	RG 1.171	1
IEEE Standard for Software Unit Testing	IEEE Std. 1008-1987 (R 2002)	1987
Software Requirements Specification for Digital Computer Software and Complex Electronics used in Safety Systems of Nuclear Power Plants	RG 1.172	1
IEEE Recommended Practice for Software Requirements Specifications	IEEE Std. 830-1998	1998
Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants	RG 1.173	1
IEEE Standard for Developing a Software Project Life Cycle Process	IEEE Std. 1074-2006	2006

3.0 TERMS AND ABBREVIATIONS

Abbreviations	Terms
CPU	Central Processing Unit
EEPROM	Electrically Erasable Programmable Read Only Memory
ESC	Energy Systems Center
O/E, E/O	Optical / Electrical Converter
FIT	Failures In Time
FMEA	Failure Mode and Effect Analysis
FMU	Frame Memory Unit
FPGA	Field Programmable Gate Array
I/O	Input / Output
LED	Light Emitting Diode
MELCO	Mitsubishi Electric Corporation
MELTAC	Mitsubishi Electric Total Advanced Controller
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair
VDU	Visual Display Unit
WDT	Watch Dog Timer

4.0 ANALYSIS OVERVIEW

4.1 Reliability Analysis

The MELTAC Platform reliability analysis addresses hardware as well as software reliability.

4.1.1 Hardware Reliability

The “Safety System Digital Platform - MELTAC - Topical Report” (JEXU-1041-1008) section 7.2 “Controller Reliability Analysis” provides an example safety system reliability analysis which requires several variables related to the MELTAC Platform and the specific application.

The MELTAC Platform variables described in this document are as follows:

λi: MELTAC Platform module failure rate [Failures In Time (FIT); Failures per billion hours]
Pi: Probability of the MELTAC Platform self-diagnostic features detecting a failure affecting a safety function.
MTBF: 1/ (λi) [hours]

The methodology used to determine each of these variables and the resultant values for all MELTAC Platform modules are given in or referenced by this document.

The following variables are not described in this document because they are unique to the application and are not dependent on the MELTAC Platform:

Ti: Manual test interval [hours]
MTTR: Mean Time To Repair [hours]

4.1.2 Software Reliability

The “Safety System Digital Platform - MELTAC - Topical Report” (JEXU-1041-1008) section 6.0 “Quality Assurance and Life Cycle” provides an overview of the MELCO ESC 10 CFR 50 Appendix B Quality Assurance Program and the MELCO ESC Software Program for Nuclear Safety Software. A detailed description of the MELCO ESC Software Program for nuclear safety software is provided within “MELTAC Software Program Manual” (JEXU-1041-1016).

The methodology used for software reliability analysis is given in or referenced by this document.

4.2 FMEA

The “Safety System Digital Platform - MELTAC - Topical Report” (JEXU-1041-1008) section 7.3 “Failure Mode and Effect Analysis (FMEA)” describes the process for conducting the FMEA, which is a method of determining the failure modes for each MELTAC Platform module and the resulting effects.

The methodology used to perform the FMEA for each MELTAC Platform module and the FMEA acceptance criteria and results are given in or referenced by this document.

5.0 METHODOLOGY

5.1 Hardware Reliability Analysis

a) λi: MELTAC Platform module failure rate [Failures In Time (FIT); Failures per billion hours]

The MELTAC Platform module failure rate (λi) is calculated for each module type, based on MIL-HDBK-217F. λi is calculated as the sum of the failure rates of each component which makes up each module.

In MIL-HDBK-217F, the failure rate is defined for each type of component with consideration given to operating conditions and reliability factors. Therefore it represents a generic reliability assessment technique.

[

]

b) Pi: Probability of the MELTAC Platform self-diagnostic features detecting a failure affecting a safety function.

To obtain Pi, the failure rate of each MELTAC Platform module is calculated separately for failures that can affect the safety function and other failures based on the FMEA results. Pi is calculated as below, where "*a"* denotes the rate of failures that can affect the safety function and "*b"* denotes the rate of undetectable failures that can affect the safety function.

$$Pi = 1 - (b/a)$$

5.2 Software Reliability Analysis

The software reliability analysis of the MELTAC Platform basic software includes an assessment of the following items against the referenced requirements.

Table 1 Software Reliability Requirements

Item	MELCO ESC Document	Requirements
MELCO ESC Quality Assurance Program	"Quality Manual Based on U.S. Nuclear Regulations" ARQ-14P001	IEEE Std. 603-1991 clause 5.3
MELCO ESC Software Program for Nuclear Safety Software	"MELTAC Software Program Manual" JEXU-1041-1016	IEEE Std. 603-1991 clause 5.3 NUREG 0800 BTP 7-14 (March 2007) RG 1.152 (Rev. 3) Endorsed IEEE Std. 7-4.3.2- 2003 RG 1.168 (Rev. 2) Endorsed IEEE Std. 1012-2004 IEEE Std. 1028-2008 RG 1.169 (Rev. 1) Endorsed IEEE Std. 828-2005 RG 1.170 (Rev. 1) Endorsed IEEE Std. 829-2008 RG 1.171 (Rev. 1) Endorsed IEEE Std. 1008-1987 (R 2002) RG 1.172 (Rev. 1) Endorsed IEEE Std. 830-1998 RG 1.173 (Rev. 1) Endorsed IEEE Std. 1074-2006
MELCO ESC Safety Software Testing, Error Recording and Trending	"MELTAC Software Program Manual" JEXU-1041-1016 "Safety System Digital Platform - MELTAC - Topical Report" (JEXU-1041-1008) section 6.18 "Reliability Database"	IEEE Std. 7-4.3.2-2003 clause 5.15

5.3 FMEA

FMEA is performed using the methodology and acceptance criteria given in the “Safety System Digital Platform - MELTAC - Topical Report” (JEXU-1041-1008) section 7.3 “Failure Mode and Effect Analysis (FMEA)”. The FMEA is performed using the following steps:

- Divide the MELTAC Platform module circuits into function blocks
- Determine failure modes for each of the identified function blocks
- Determine the states of MELTAC Platform module outputs based on the identified function block failure modes
- Determine the effects on the overall MELTAC Platform based on the MELTAC Platform module output failure states

The above analysis methodology is based on the approach described in IEEE Std. 352-1987 sections 4.1 and 4.4.

The FMEA is based on the configuration of the CPU and I/O components and the arrangement of the network given in Figure 4.0-1 “MELTAC Platform Typical Plant Safety System Configuration” in the “Safety System Digital Platform - MELTAC - Topical Report” (JEXU-1041-1008). Therefore a failure in the I/O components is detected by the CPU and a failure of any single controller or network is detected by another controller. It is assumed that unrelated failures will not occur simultaneously.

[

]

Table 2 Acceptance Criteria

6.0 MELTAC PLATFORM MODULES

The MELTAC Platform modules subject to the reliability analysis and FMEA are shown in Appendix A of “Safety System Digital Platform - MELTAC - Topical Report” (JEXU-1041-1008)”.

7.0 ANALYSIS

7.1 Hardware

The detailed MELTAC Platform module hardware reliability analyses are located in the following design analysis document:
[

]

7.2 Software

No quantitative reliability goals have been established for the MELTAC Platform. The following software reliability analysis is a qualitative analysis.

The MELCO ESC quality assurance program complies with 10 CFR 50 Appendix B and ASME NQA-1-1994 as described in “Summary of MELTAC Platform QA” (JEXU-1041-1025) and the “Quality Manual Based on U.S. Nuclear Regulations” (ARQ-14P001).

The implementation of the MELCO ESC quality assurance program, and compliance with 10 CFR 50 Appendix B and ASME NQA-1-1994, meets the requirements given in IEEE Std. 603-1991 clause 5.3 which mandates the usage of a prescribed quality assurance program.

The MELCO ESC Software Program for Nuclear Safety Software is subordinate to the MELCO ESC quality assurance program and is described in detail in “MELTAC Software Program Manual” (JEXU-1041-1016). The MELCO ESC Software Program for Nuclear Safety Software commits to compliance with the requirements given in Table 1.

MELCO ESC Safety Software Testing is described in “MELTAC Software Program Manual” (JEXU-1041-1016) sections 3.10 “Software Verification and Validation Plan” and 3.12 “Software Test Plan”.

MELCO ESC maintains a reliability database for the MELTAC Platform. When MELCO ESC is notified by a customer that an error or failure has occurred, MELCO ESC will execute an investigation of the customer’s request. Troubleshooting procedures are prepared to solve the problem and to identify preventive actions.

MELCO ESC processes identify non-conformances per the MELCO ESC QAP. The format and form of troubleshooting report to customers will be discussed between MELCO ESC and each customer, in consideration of the MELCO ESC QAP and US regulations (10 CFR 21).

MELCO ESC records all phenomena, causes, solutions, and other information regarding issues. Based on this information, MELCO ESC analyzes the MELTAC Platform reliability to improve the quality of the MELTAC Platform. MELCO ESC maintains the database of failure information reported from nuclear power plants through all sources, including complaint reports and process reports.

The reliability database serves 2 key purposes:

(1) Problem Applicability
The applicability of the failure to other plants is identified. The information is used to report common defects to internal MELCO ESC departments and MELCO ESC customers.

(2) Problem handling process improvement
The MELCO ESC QA department tracks and expedites the progress of failure handling. Trends are created to monitor the performance of the problem resolution process.

[

]

7.3 FMEA

The detailed MELTAC Platform module FMEAs are located in the following design analysis documents:

Table 3 List of FMEA Documents

8.0 CONCLUSION

8.1 Hardware Reliability

The failure rate (λi) and MTBF of each MELTAC Platform module is provided in the “Safety System Digital Platform - MELTAC - Topical Report” (JEXU-1041-1008) section 7.1 “Mean Time Between Failures (MTBF) Analysis” and the detailed design analysis document referenced in section 7.1.

The probability (Pi) of the MELTAC Platform self-diagnostics features detecting a failure which affects a safety function of a MELTAC Platform module is provided in the detailed design analysis document referenced in section 7.1.

The design analysis document referenced in section 7.1 may be revised at a later time due to ongoing MELTAC Platform upgrade activities.

8.2 Software Reliability

The qualitative software reliability goals established in section 7.2 above have been achieved based on the following:

- The implementation of the MELCO ESC quality assurance program, and compliance with 10 CFR 50 Appendix B and ASME NQA-1-1994, meets the requirements given in IEEE Std. 603-1991 clause 5.3 which mandates the usage of a prescribed quality assurance program.

- The implementation of MELCO ESC Software Program for Nuclear Safety Software as a subordinate to the MELCO ESC quality assurance program complies with the requirements given in Table 1.

- The reliability of the MELTAC Platform basic software has been demonstrated to be sufficient to meet the requirements of IEEE Std. 7-4.3.2-2003 clause 5.15 through successful software testing and positive operating experience record.

8.3 FMEA

Table 4 4 and the detailed design analysis documents referenced in section 7.3 summarize the FMEA results for each MELTAC Platform module.

Table 4 Summary of the FMEA Results for Each MELTAC Platform Module

The design analysis documents referenced in section 7.3 may be revised at a later time due to ongoing MELTAC Platform upgrade activities.