# Development and assurance of high integrity of digital I&C systems for Mitsubishi PWR plants


## MASHIO Kenji[1], and SHIRASAWA Hiroshi[2]

*1. Nuclear Electrical, Instrumentation & Control Engineering Department, Mitsubishi Heavy Industries, LTD. 1-1 Wadasaki-Cho 1-Chome Hyogo-Ku Kobe, 652-8585, Japan (kenji_mashio@mhi.co.jp)*

*2. Nuclear Electrical, Instrumentation & Control Engineering Department, Mitsubishi Heavy Industries, LTD. 1-1 Wadasaki-Cho 1-Chome Hyogo-Ku Kobe, 652-8585, Japan (hiroshi_shirasawa@mhi.co.jp)*



**Abstract:** This document provides the development process and the high integrity assurance process of the digital I&C systems for the Mitsubishi PWR plants. To enhance the reliability of the digital I&C systems and the dependability of the software used in these systems, several design and quality assurance aspects are considered throughout the development, design, verification, tests and implementation phases of the Mitsubishi digital I&C system. This document also provides the overview of the Mitsubishi I&C systems for new PWR plants to understand the design and quality assurance process of the Mitsubishi I&C systems.



**Keyword:** Mitsubishi digital I&C; software dependability; software integrity; verification and validation


## 1 Introduction

This document provides the development process and the high integrity assurance process of the digital I&C systems for the Mitsubishi PWR plants.

To enhance the reliability of the digital I&C systems and the dependability of the software used in these systems, following design and quality assurance aspects are considered throughout the development, design, verification, tests and implementation phases of the Mitsubishi I&C system

- Software architecture
- Self-testing
- Functional diversity
- Software secureness
- Software life cycle process control
- Software verification and validation
- Safety operation enhancement

The Mitsubishi I&C system consists of digital I&C systems, computerized HSI systems and minimum hardwired systems to cope with potential software common cause failure as shown in Fig.1.

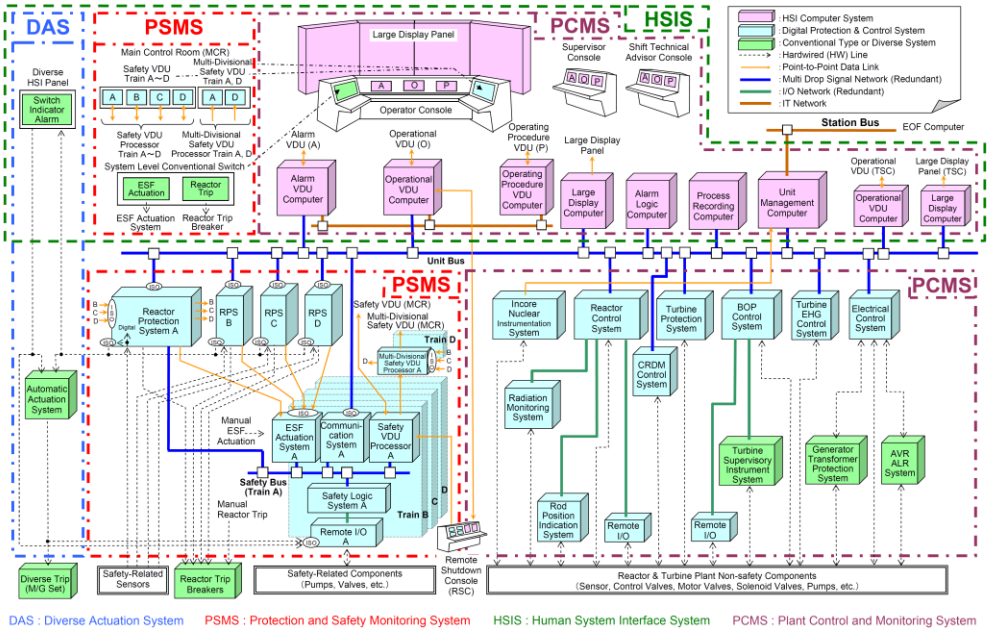



Fig.1 Overall architecture of Mitsubishi I&C systems.


**Received date: February 5, 2015**
(Revised date: February 12, 2015)

The overall Mitsubishi I&C system consists of the following I&C systems;

- Protection & Safety Monitoring System (PSMS)
  - Four trains redundant
  - Fully digital system
  - Safety I&C (Class 1E)
- Plant Control & Monitoring System (PCMS)
  - Duplex redundant
  - Fully digital system
  - Non-safety I&C
- Diverse Actuation System (DAS)
  - Two subsystems redundant
  - Analog circuit base hardwired system
  - Diverse & independent of digital I&C systems
  - Non-safety I&C
- Human System Interface System (HSI)
  The HSI systems in a main control room consist of the following components, and the typical architecture and arrangement is shown in Fig.2.
  - Large display panel (LDP)
  - Safety VDU (Class 1E)
  - Non-Safety operational VDU
  - Conventional switches (Class 1E)
- Data Communication System (DCS)
  - Multi-drop networks
  - Point to point data links
  - Fully redundant with self-testing features

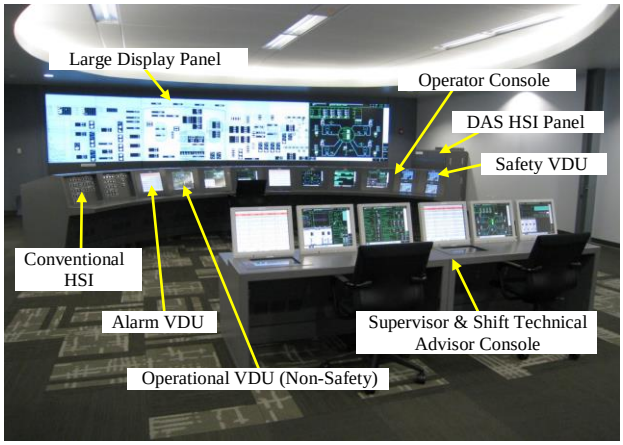



Fig.2 Overall HSI system architecture.

# 2 Histories of Mitsubishi I&C system

### 2.1 Digital I&C systems

The development of the digital I&C system for the Mitsubishi PWR plants began in 1985 with the initial goal of non-safety applications and the long term goal of safety applications. The developed digital I&C system has been firstly applied for the major non-safety I&C systems, such as, reactor control systems and turbine/generator control systems, in 1991, and has been applied to over 450 systems, include safety systems, in 30 PWR plants. The total operating experience of the Mitsubishi digital I&C system is over 30 million hours and there are no plant shutdowns/transients caused by software or hardware failures of the digital I&C system.

### 2.2 Computerized HSI Systems

The development of the computerized HSI system began in 1987, and the verification and validation (V&V) tests with Japanese and U.S. PWR utilities shift operators with the full-scale simulator have been performed and finished. The performances of the operators have been checked by the V&V tests, and the review results and all comments by the V&V tests have been reflected to the HSI design. The standard design specification and overall architecture of the computerized HSI systems have been established and the computerized HSI systems have been applied for the latest PWR plants in Japan and the operating plants modernization projects.

# 3 Software architecture

The software of the Mitsubishi digital I&C system consists of the basic and application software as shown in Fig.3, and is designed based on the following design principles to assure simplicity, enable high efficiency and dependability of software ;

- All functions execute cyclically with single task processing
- Inputs are updated cyclically, but asynchronously, from periodic function processing
- Function processor reads data cyclically from two port memory
- Self-testing run with no effect on the pre-defined fixed deterministic time cycle
- No interrupts, except by self-testing
- Time cycle cannot be disrupted by other systems

# 4 Self-testing

The integrity of digital components is continuously and automatically checked by the self-testing features of the Mitsubishi digital I&C system. The self-testing features cover all digital components, including all memories in the controller and inter-controller data

communication, from input to output as shown in Fig.4. All functions of the memories that control the self-testing and setpoints are also confirmed by the continuous automatic self-testing features.

Additionally, following manual surveillance tests controlled by technical specifications, including the operability of the self-testing functions, confirm the operability of the digital I&C systems;

- Channel Calibration
  Calibration from sensor through controllers and data communication to VDUs
- Trip Actuating Device Operational Test
  Testing from VDUs through data communication and controllers to plant components, including Reactor Trip Breakers (RTB)
- Memory Integrity Check
  Divers test (from the self-testing functions of memories) of all basic and application software

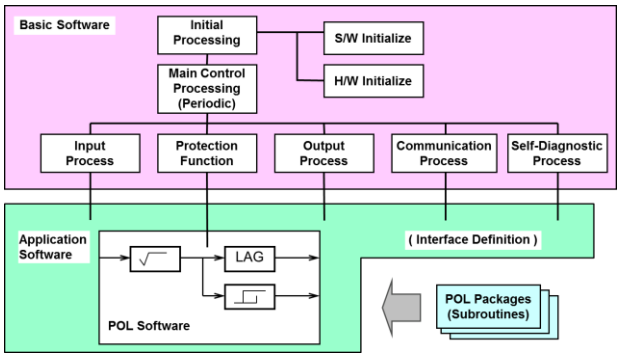



Fig.3 Software architecture.

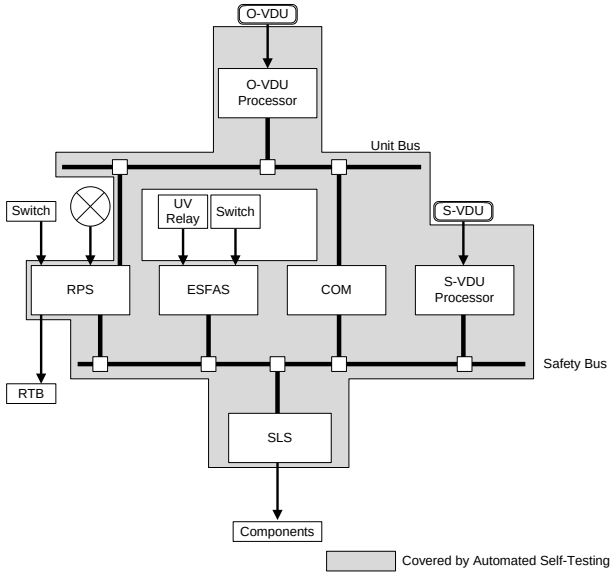



Fig.4 Coverage of self-testing features.

# 5 Functional diversity

Each train of the reactor protection system consists of the two separate digital I&C subsystem groups to achieve defense-in-depth through functional diversity. Two or more initiating signals are identified for each postulated event in the plant accident analysis and shown in Table 1. Two diverse parameters are used to detect an event and initiate protective actions. Two diverse protection functions are processed in the two separate digital subsystem groups in each reactor trip system. Effects by common cause failures (CCFs) of the application software can be mitigated by the functional diversity design.

**Table 4 Typical Functional Diversity Allocation**

| Protection | Group-1 | Group-2 |
|---|---|---|
| Over Power | • Over Power Delta-T High<br>• PR Neutron Flux Rate High | • PR Neutron Flux High |
| Core Heat Removal | • RCP Speed Low<br>• Over Temp. Delta-T High | • RC Flow Low<br>• Pressurizer Press. Low |
| Loss of Heat Sink | • SG Water Level Low<br>• Pressurizer Water Level High | • Pressurizer Press. High |
| Nuclear Startup | • SR Neutron Flux High<br>• IR Neutron Flux High | • PR Neutron Flux High (Low Setpoint) |
| Primary Over Pressure | • Pressurizer Water Level High | • Pressurizer Press. High |
| Loss of Coolant | • C/V Press. High | • Pressurizer Press. Low-Low |
| Steam Line Break | • C/V Press. High-High | • Main Steam Line Press. Low |

# 6 Software secureness

The secureness of the software of the safety (Class 1E) digital I&C systems are assured to comply with the secure development and operational environment (SDOE) requirements of U.S. Regulatory Guide (RG) 1.152. During the development phase, the software secureness is ensured by the independent V&V and configuration control. During implementation and operation phase, the software secureness is ensured by system design features (e.g., locked doors, alarms,

module removal restrictions) and the memory integrity checks.

To comply with the SDOE requirements of RG 1.152, the digital I&C systems can be assured that unintended functions have not been introduced at any point in software development, and the digital I&C systems contain the design features that prevent and detect unintended alterations.

All safety functions of safety digital I&C systems are installed in the non-volatile memory that cannot be altered in any manner while operating of the digital I&C system. The safety software changes require following actions to avoid unauthorized alternations:

- Equipment room access (locked and alarmed)
- Cabinet access (locked and alarmed)
- Module removal (alarmed and controlled by the technical specifications)
- Module reprogramming in external chassis

The redundant safety digital I&C systems divisions are finically separated in four I&C equipment rooms under administrative controls by the operator with door locks and door open alarms features, etc. Also, an unintended software changes are detectable by the periodic testing (by the memory integrity check).

# 7 Software life cycle process control

## 7.1 Overview of software life cycle process

To provide adequate confidence in the quality and dependability (*) of the digital I&C system software, software life cycle process controls are performed for the safety (Class 1E) digital I&C systems.

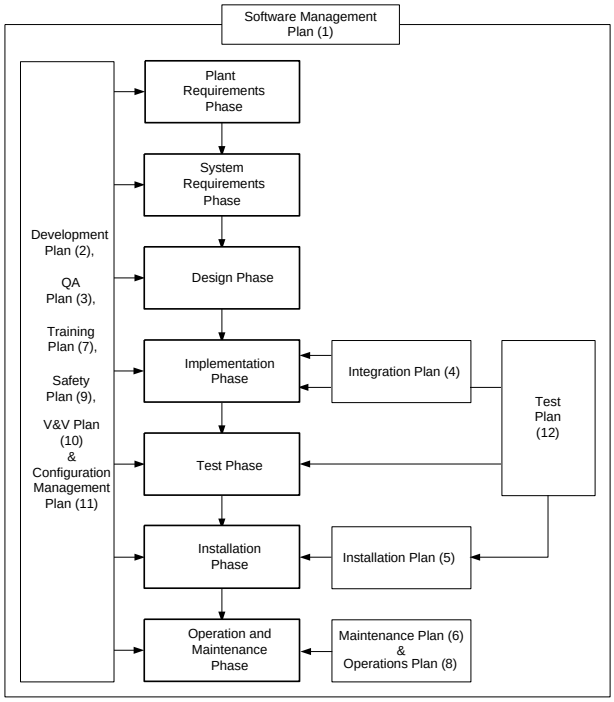
*) Reliability, availability, maintainability, integrity, safety and security are attributes of dependability.

The software life cycle of the safety digital I&C systems are implemented, operated and maintained based on the following plans;

1. Software Management Plan
2. Software Development Plan
3. Software Quality Assurance Plan
4. Software Integration Plan
5. Software Installation Plan
6. Software Maintenance Plan
7. Software Training Plan
8. Software Operation Plan
9. Software Safety Plan
10. Software Verification & Validation (V&V) Plan
11. Software Configuration Management Plan
12. Software Test Plan

Above plans govern the software life cycle process of the safety digital I&C systems throughout the all phases, development phase, requirements phase, design phase, implementation phase, test phase, installation phase, operation phase and maintenance phase, of the nuclear power plant (NPP).

Relations between each plan and each phases of the software life cycle process of the Mitsubishi digital I&C system are shown in Fig.5.




Note: Each plan corresponds to the subsections in Sec.7.2.

Fig.5 Relations between plans and phases.

## 7.2 Individual software life cycle process

7.2.1 Software management plan

a. Basic strategy and process for managing the software life cycle.
b. Method for monitoring progress against a NPP project plan.
c. Method for identifying any deviations from the NPP plan or this plan.
d. Procedure for managing the software.

7.2.2 Software development plan

a. Technical aspects for the design & development activities of the software.
b. Phase activities in the software life cycle for a NPP project.
c. Inputs to and outputs from each activity.

7.2.3 Software qualification assurance

a. Organizational responsibilities, security, quality assurance requirements, procedure, and methodology for the software.
b. Metrics used to measure the specific quality
c. Reviews and audits in accordance with IEEE Std. 1028-1997.
d. Problem reporting and corrective action.

7.2.4 Software integration plan

a. Procedures for software integration.
   1) Integrate application software units together to form an execution module.
   2) Integrate the result of 1) with the target digital I&C system hardware modules.
   3) Test the resulting integrated product.

7.2.5 Software installation plan

a. Procedures for software installation.
   1) Plan installation
   2) Distribute software
   3) Install software
   4) Accept software in operational environment

7.2.6 Software maintenance plan

a. Processes for correcting faults and errors of the software during plant operation.
b. Activities for the maintenance of the software.
   1) Failure reporting
   2) Fault correction
   3) Re-release software
   4) Configuration management system

7.2.7 Software training plan

a. Metrics for the effectiveness of the training.
b. Procedures for software training.
   1) Training activities
   2) Software training manual and material
   3) Specification and requirements of effective and sufficient training resources

7.2.8 Software operation

a. Definition and requirements of the software during the Operation and Maintenance phase.

7.2.9 Software safety plan

a. Methodologies for software safety for all life cycle process of the software.
b. Definition and requirements of technical requirements and organizational responsibilities for specific software safety activities.
c. Software safety management accordance with IEEE Std. 1228-1994
d. Software Safety Analysis (SSA)
   1) Plant requirement phase SSA
   2) System requirement phase SSA
   3) Design and implementation SSA
   4) Test phase SSA

7.2.10 Software V&V plan

a. V&V activities during the software design, integration and testing phases.
b. Procedures and methodologies for each V&V activity in accordance with IEEE Std. 1012-1998
   1) System requirement phase V&V
   2) Design phase V&V
   3) Implementation phase V&V
   4) Test phase V&V
   5) Installation V&V
   6) Maintenance and operation V&V
   7) Requirements for reporting of V&V process, anomaly and resolution

Above V&V activities are performed during phases including, development, design, implementation, test, operation and maintenance phases, of the software life cycle process of the safety digital I&C systems.

7.2.10.1 Basic software V&V activities

During the safety software development phase, the V&V activities combination with the static test (analysis) and the dynamic tests are also performed to the basic software and POL (Problem Oriented Language) of the safety digital I&C systems.

a. Static Tests
   The static tests (analysis) are performed by the source code review and the code audit.
b. Dynamic test

The dynamic tests are performed by the functional test (black box test) and the structural test (white box test) as shown in Fig. 6.

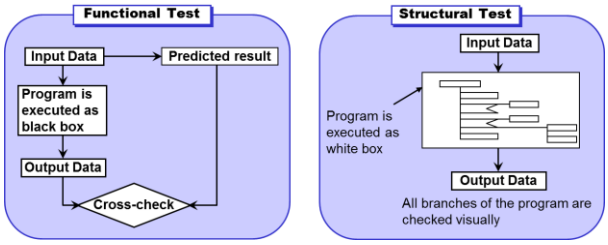



Fig.6 Basic software V&V.

7.2.10.2 Application V&V activities

During the safety software design, integration, test, implementation, operation and maintenance phases, the V&V activities as shown in Fig.7 are performed based on the Japanese standard which refer to IEEE Std. 7-4.3.2, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations".

Complete independent V&V activities are performed as shown in Fig.7, and the verifier independent from the designer has same grade of capability of designing of the designer. Also, the V&V activities include integration of complete system including hardware, basic software, and application software.

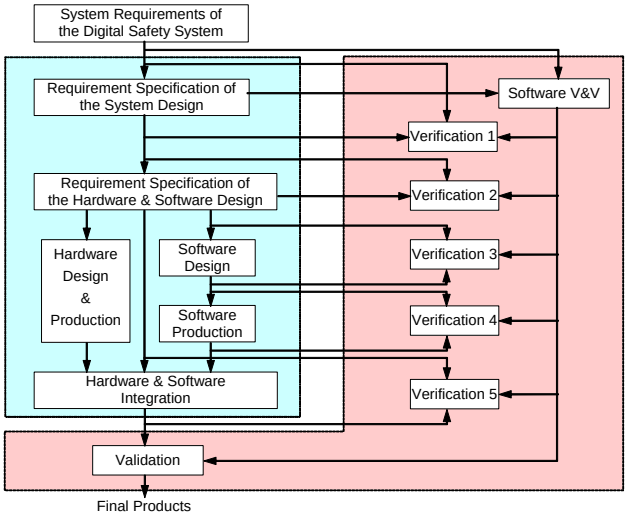



Fig.7 Application software V&V.

To perform the V&V activities easier, the software architecture of the Mitsubishi digital I&C systems consider the following design aspects;

- execute fixed sequence tasks only with no interruption
- perform necessary protective functions only
- structured and modular architecture for easier verification
- use visible symbolic language (POL) to clarify design requirements

7.2.11 Software configuration management plan

a. Methods required for maintaining the project specific application software configuration items in a controlled configuration
b. The six classes of the software configuration management (SCM) of information required by IEEE Std. 828-1990
   1) Introduction
   2) SCM management
   3) SCM activities
   4) SCM schedules
   5) SCM resources
   6) SCM maintenance
c. Procedure in each phase

7.2.12 Software test plan

a. Methodologies for the following V&V test activities
   1) Component V&V test
   2) Integration V&V test
   3) System V&V test
   4) Acceptance V&V test
b. Test documents in accordance with IEEE Std. 829-1983.

# 8 Safety operation enhancement

## 8.1 Degraded HSI condition

The normal plant operation and the accident mitigate operation are performed by the non-safety grade HSI, such as, LDP, the operational VDU and the alarm VDU, and the safety grade (Class 1E) HSI, such as, the safety VDU is installed to provide bask-up to comply with the safety requirements.

The following dedicated HSI systems and the related support features are implemented in the Mitsubishi digital I&C systems and the fully computerized main control room.

a. Dedicated operating procedure (paper based)
b. Dedicated display navigation system for easy access operation/monitoring objects

c. Safety VDUs provide back-up Class 1E information and control for all safety functions
d. Safety VDUs provide spatially dedicated, continuously visible (SDCV) monitoring aid for Class 1E information

### 8.2 Validation of degraded HSI design

The degraded HSI design has been validated by the Japanese and US operators by using a dynamic simulator for a degraded HSI condition.

The validation tests are performed to consider the actual degraded HSI design as shown in Fig. 8 and 9.

a. Simulator scenarios and evaluation process have been developed.
b. Correct operator's operation logs along with scenario process (using observations, video review and operation logger in the digital system)
c. Correct operator's feedback briefing of scenario reviews, interview and questionnaires

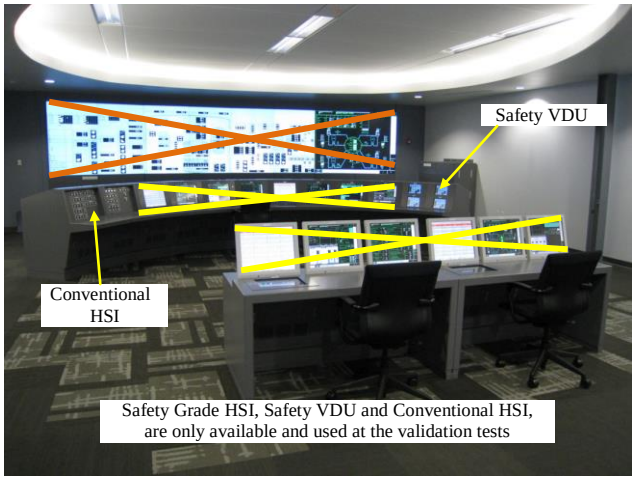



Fig.8 Degraded HSI Condition (Overview).

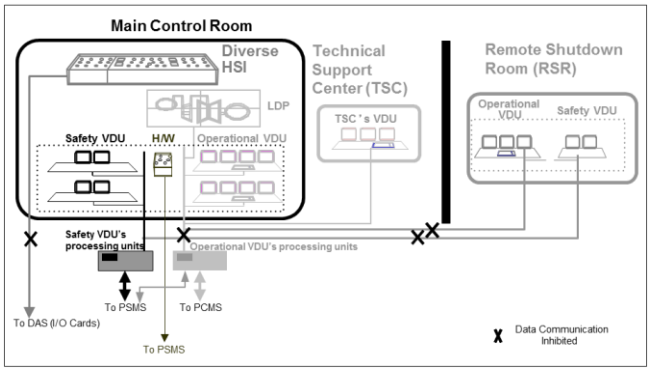



Fig.9 Degraded HSI Condition (System Configuration).

## 9 Conclusions

The Mitsubishi digital I&C system for PWR plants, with the highly integrated life cycle assurance process, has been applied to many safety and non-safety system applications, including a full digital I&C system in a new plant and digital upgrading in other operating plants in Japan. Based on the positive experiences of this proven technology, the digital I&C system is also about to be applied into US plants (*e.g.*, in the US-APWR).

The Mitsubishi digital I&C system may also enter the global market, future plants and used for the digital upgrade of existing projects, in other countries.

Mitsubishi continues improving the safety and reliability of the digital I&C systems and the dependability of the software to consider the important aspects to described on this document, and the Mitsubishi digital I&C is evermore committed to also enhance the operability and maintainability.

## References

[1] SAKAMOTO H., and KITAMURA M.: Integrated Digital I&C System for New Plants, 13th International Conference on Nuclear Engineering, ICON13-50308, 2005
[2] MARUTA Y., and UTSUMI M.: 2005, Modernization Plan of Instrumentation and Control System for Operating PWR Plants in Japan, IAEA Technical Meeting on Impact of Modern Technology on Instrumentation and Control in Nuclear Power Plants, 2005
[3] OBA M., *et al.*: Utilization of Digital I&C system for the US-APWR, 15th International Conference on Nuclear Engineering, ICONE15-10527, 2007.
[4] SHIRASAWA H., *et al.*: Digital I&C System in the US-APWR, 16th International Conference on Nuclear Engineering, ICONE16-48220, 2008.
[5] Mitsubishi Heavy Industries: Design Control Document for the US-APWR, MUAP-DC007, Rev.4, September 2013.
[6] Mitsubishi Heavy Industries: Design Control Document for the US-APWR, MUAP DC018, Rev.4, September 2013.
[7] Mitsubishi Heavy Industries: Safety I&C System Description and Design Process, Technical Report MUAP-07004-NP, Rev. 8, November 2013.