Mitsubishi's computerized HSI and digital I&C system for PWR plants

ITO Koji[1], HANADA Satoshi[2], and MASHIO Kenji[3]

1. Mitsubishi Heavy Industries, Ltd., Kobe 655-8585, Japan (koji_ito@mhi.co.jp)
2. Mitsubishi Heavy Industries, Ltd., Kobe 655-8585, Japan (Satoshi_Hanada@mhi.co.jp)
3. Mitsubishi Nuclear Energy Systems, Inc. Arlington, VA 22209, USA (kenji_mashio@mnes-us.com)

Abstract: The fully computerized Human-System Interface (HSI) system and digitalized Instrumentation and Control (I&C) system of Mitsubishi Heavy Industries, Ltd. (MHI) has been developed and approved in Japan. This design is currently being used in the latest Japanese Pressurized Water Reactor (PWR) plant and in Japan's Modernization Plan of I&C Systems for Operating PWR Plants. Conventional hard controls are limited to system level manual actions and a Diverse Actuation System. The digital I&C system can ensure defense-in-depth and diversity for plant safety and control, with consequent countermeasures against software common-cause failures. The design includes computer-based procedures and alarm prioritization, relying principally on a HSI system with soft controls, console based video display units and a large, heads up, overview display panel. This design is set to be applied to the US-APWR, a four loop evolutionary pressurized water reactor with a four train active safety system, which is currently under Design Certification Review by the U.S. Nuclear Regulatory Commission.
Keyword: computerized HSI; digitalized I&C; US-APWR; V&V

1 Introduction

I&C systems of nuclear power plants provide the capability to control and regulate plants' systems, either manually or automatically, during normal plant operation. However, the primary purpose of I&C systems is to provide an automatic protection of the reactor, by exercising adequate controls against unsafe or improper reactor operations during steady state and transient power operations. The systems also provide initiating signals to activate safety functions, which are assigned to mitigate the consequences of fault conditions and to ensure a secure shutdown of the plants. Thus, all these safety functions include the responses assumed in the plants' safety analyses.

The I&C systems of conventional nuclear power plants consist of analog and relay circuits, as well as other hardware devices, which are connected by several cables. However, due to the recent trend and numerous benefits of digital technology, digital I&C systems have been developed and applied, in a step-by-step approach, in Japanese PWR plants. Currently, MHI's I&C system is a fully digitalized system with several new designed features that improve the reliability and safety of nuclear power.

This digital I&C system has been implemented in Japan, in many safety and non-safety applications, including HSI systems, with excellent results. A fully digitalized I&C system is in operation in a newly constructed PWR plant[1] and digital upgrading has taken place and still is taking place in operating PWR plants in Japan[2]. Additionally, this proven technology is set to be implemented in future plants in Japan and in the US. The US-APWR [3,4] is set to use the digital I&C system. This reactor has been developed by MHI as a variation of the Japanese APWR design, in order to comply with US codes and standards. The I&C system of the US-APWR has the same design and digital platform that of Japanese PWR plants, and it also meets the US regulatory requirements and industry guidelines. Furthermore, the digital I&C system is set to be applied also in other projects, such as in EU-APWRs for the EU market.

The digital I&C system includes multiple echelons of defense so as to ensure Defense in Depth and Diversity (D3) and also to achieve countermeasures against software Common Cause Failures (CCFs). In

Received date: July 12, 2010
(Revised date: September 13, 2010)

addition, this system has a four redundant-division configuration that applies to the safety HSI system, the safety protection system and the safety plant component controls.

This paper focuses on MHI's computerized HSI system and digital I&C features and applications for new PWR plants, as well as for the digital upgrading of current PWR plants. The paper also discusses the computerized HSI system of the US-APWR design, the Verification and Validation (V&V) program data collection and analysis, and the study results on the ongoing discussion of the impacts of digital systems on human performance, such as workload, navigation, situation awareness, operator training and licensing.

2 Mitsubishi's digital I&C design features

2.1 Overview system description

This section provides an overview of MHI's digital I&C system and technology. Specific features of the I&C system are described in sections 2.2 to 2.3. The general specifications of MHI's digital I&C system are summarized as follows:

(1) Soft-operation-based HSI system in the main control room (operability improvement and reduction in operator workload)
- Fully computerized
- Safety Visual Display Units (VDUs)
- Non-safety operational VDU
- Large Display Panel (LDP)
- Minimal conventional switches

(2) Digital protection and control systems (reduction in maintenance workload through the use of software without drift, and early detection of failures by self-diagnostics)
- Fully digitalized
- Four redundant safety Protection and Safety Monitoring System (PSMS) for plant protection
- Non-safety Plant Control and Monitoring System (PCMS) for plant control and monitoring
- Non-safety analog Diverse Actuation System (DAS) for CCF of the digital system

(3) Use of data communication systems (reduction in the amount of cables)
- Fully multiplexed, including safety-related signals
- Multi-drop data bus and serial data link
- Fiber optics communication networks

This section describes the US-APWR's I&C system as a representative model of MHI's I&C system. The overall architecture of the I&C system is shown in Fig.1.

This system consists of the safety-related PSMS with the safety-related portion of the HSI system, the non-safety-related PCMS with the non-safety portion of the HSI system, and the non-safety-related DAS with the non-safety-related portion of the DAS' HSI system. The HSI system consists of safety-related VDUs for abnormal condition, including Post Accident Monitoring (PAM) indication, and of non-safety-related operational VDUs and LDPs for normal plant operation. The safety VDUs and operational VDUs are located on both the operator console in the Main Control Room (MCR) and the Remote Shutdown Console (RSC) in the remote shutdown room. Operational VDUs are also implemented for the sole purpose of providing information (i.e., no control capability) at the Technical Support Center (TSC). Information to support emergency response operations (the same information shown in operational VDUs) is provided at the Emergency Operations Facility (EOF).

The safety-related PSMS with the safety-related portion of the HSI system consists of a Reactor Protection System (RPS), an Engineered Safety Features Actuation System (ESFAS), a Safety Logic System (SLS), conventional switches (division level), and safety VDUs part of the safety-related portion of the HSI system for manual operation and monitoring of critical safety functions including PAM.

Safety functions are all actions needed to trigger the different responses assumed in the safety analyses, and those required to achieve a safe shutdown of the plant. Some safety functions are automatically initiated by the PSMS.

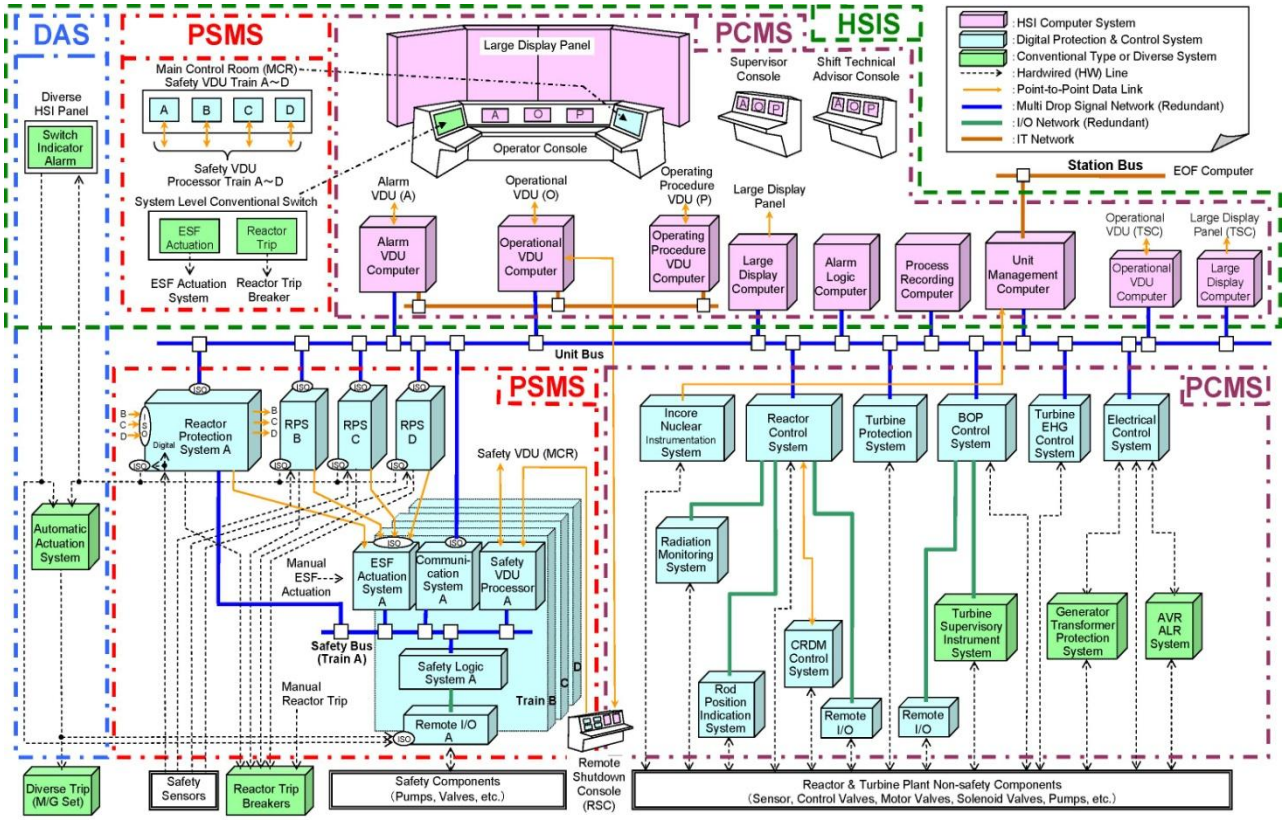

Fig. 1 Overall architecture of the I&C system (US-APWR).

These safety functions may also be manually initiated and monitored by operators using the HSI system. Additionally, the HSI system may also be used to manually initiate other safety functions that do not require time-critical actuation and safety functions that are not related to shutdown. After a manual initiation from the HSI system all safety functions are executed by the PSMS. The HSI system also provides all the plant's information to the operators, including critical parameters required for post-accident conditions. Finally, the HSI system includes both safety and non-safety sections.

2.2 Implementation in new plants

Mitsubishi's full digital I&C system has been applied, and is currently in commercial operation, in Japan. It is projected to be implemented in future Japanese APWR plants, such as Tsuruga Unit 3 and 4. This proven full digital system is also set to enter the US market by being implemented in the US-APWR. The I&C system of the US-APWR will essentially be the same than the one planned for new plants and currently being applied in the digital upgrading of operating plants in Japan. The safety I&C system design and the digital platform features for the US-APWR, summarized into topical reports, are now under licensing review by the U.S. Nuclear Regulatory Commission (NRC). Accordingly, the US-APWR design is now under a licensing process with the correspondent Design Control Document (DCD)[5], and is expected to start operating in the US in the late 2010s.

The digital system is also expected to be applied in future global markets, including EU-APWR for the case or the EU market.

2.3 Digital upgrading

Recently, the difficulty of obtaining and replacing obsolete parts of I&C systems in operating nuclear power plants has become evident. A way to address this problem is digital upgrading, which improves the system's maintainability and, therefore, contributes to the plant's long-term safety and operability. In accordance, upgrading most important I&C systems to digital systems meets the needs of I&C modernization. Furthermore, from the point of view of total cost considering long-term operational and maintenance costs- this approach seems the most cost-effective.

Mitsubishi's digital I&C system has been applied in various digital upgrading projects in Japan. Mitsubishi's large and successful experience in the digital upgrading of I&C systems, for non-safety and safety applications, shows the company's capability of providing this service in future global markets.

3 HSI system's V&V program for digital I&C design

3.1 Design features of Mitsubishi's HSI system

The soft-operation-based HSI system is designed to improve operability and to reduce operator workload by allowing it to be operated by a single person. This system consists of the operator console, the LDP, and the supervisor console through which the shift supervisor monitors the operations.

The operator console is a compact console designed to enable a centralized monitoring and control by integrating and centralizing the functions of a conventional HSI system (e.g.: indicators, recorders, indication lamps, *etc*.); it allows monitoring and control from a seated position. The operator console consists of the operational VDU, the safety VDU, the alarm VDU, and the minimal conventional switches.

The LDP shows parameters that require continuous monitoring and integrated alarms, so that the operators can have an overview of the plant's status. There are four screens on the LDP, three of which have fixed views to show system parameters and alarms, allowing operators to continuously monitor this information. The remaining screen provides a changeable view; thus, operators can choose from a range of different plant operation monitoring views available on the operation VDU.

The LDP's Specially Dedicated and Continuously Visible (SDCV) feature prevents operators from concentrating for too long on certain display screens of the operator/supervisor's console, which leads to decreasing awareness of the plant's status, what is referred as "Key-Hole effects".

The Japanese PWR Utilities (Electric Power Companies) and the Mitsubishi Group have developed an advanced-type main control board (console), reflecting on the study of human factors as well as using the above mentioned state of the art electronics technology.

3.2 Implementation of the HSI system in the US-APWR

The US-APWR's Human Factors Engineering (HFE) aims at an adequate implementation of the HSI system. Given that there is not much difference between the plants' design of Japanese PWRs and that of the US-APWRs, it has been assumed that all prior Japanese analyses and testing results are applicable to the US-APWR's HSIs, needing changes mainly to account for differences in language, operating culture and anthropometrics. To meet the HFE's goal, a V&V program has been designed, which offers guidance in the selection of a team whose purpose is to facilitate the transition from the Japanese Standard HSI design to the final US-APWR and US site specific HSI. For details on the US-APWR's I&C and HSI basic design see the Design Control Document MUAP DC018, Rev. 2[5], topical report HSI System Description and HFE Process, MUAP-07007 [6].

The overall V&V program has been divided into three phases. Phase 1 consisted on defining the US Basic HSI System based upon the Japanese Standard HSI System. Phase 1 has already been concluded and, thus, the US-APWR Basic HSI design has been completed. This Basic HSI System is not plant or site specific, but is applicable to all US nuclear power plants. As mentioned above, the modifications carried out in Phase 1 have included translating the system from Japanese to the English and converting its units to American engineering units, as well as making anthropometric changes to the consoles in order to fit American body types, and adopting US style prescriptive operating procedures. As a result, the knee space of the consoles was heightened a few inches, and the display formats and operating procedures were modified in accordance to the suggestions indicated by US nuclear plant operation/training instructors, (e.g.: using abbreviations familiar to US operators, introducing familiar functions to the computer-based operating procedure system, *etc*.).

To support Phase 1's V&V testing, a main control room dynamic simulator facility, shown in Fig. 2, was

designed and installed at the Mitsubishi Electric Power Products Inc. (MEPPI) facility in Warrendale, PA, USA. Additionally, a static HSI screen analysis tool, was developed and implemented on a PC platform, so as to support display screen and design verifications. Phase 1's V&V was further divided into two parts, Phase 1a and Phase 1b. Phase 1a consisted on identifying any changes needed due to differences in US cultural and/or operating methods.

Fig.2 US-APWR V&V facility.

In Phase 1a, a high fidelity simulation model for a conventional 4 loop PWR plant was used. Phase 1a also included the completion of the Operating Experience Review (OER) program element. This program element expanded the OER originally done for the Japanese Standard HSI System to encompass the operating experience at US nuclear plants and to consider additional generic digital HSI technology experience. The data collected included objective performance data, subjective observations by plant operations and HFE experts, and operator feedback via questionnaires, verbal debriefs, and Human Engineering Discrepancy (HED) input forms. These multiple sources of information were integrated and entered into an electronic HED tracking database. Phase 1b consisted on designing, verifying and validating any additional changes needed due to HEDs identified in Phase 1a. Thus, the HSI system simulator used in Phase 1a was modified during Phase 1b. The end of Phase 1b marked the completion of the Basic HSI System, to be applied in US new plants and in the upgrade of currently operating plants.

In accordance to the recommendations of Section 11.4.4.1 of the NUREG-0711, Rev. 2[8], a multi-disciplinary expert panel composed by the V&V team (DCD 18.1.2.3.2, MUAP DC018, Rev. 2[6]) and designer representatives was convened to review the HEDs along with the results of Phase 1a and Phase 1b, and ultimately to recommend possible solutions for those HEDs. Some of the recommendations included additional changes in the design of the US Basic HSI System. Phase 1a testing was undertaken during the second half of 2008 and it focused only on the MCR HSI. Phase 1b V&V process took place during the first half of 2009, by evaluating the changes done to the US Basic HSI System design, resulting from Phase 1a. The same testing and analysis methods, tools and group of experts of Phase 1a were used in Phase 1b. Phase 1b test scenarios focused on those parts of the main control room that were not tested in Phase 1a and on the changes needed to be done to address the HEDs identified in Phase 1a. The results from Phase 1b testing were also entered into the HED database and assessed by an expert panel, with the objective of refining the US Basic HSI System even further. This paper discusses the process, activities, results, and implications on the HSI design resulting from the V&V testing program.

Phase 2 aims to develop, verify and validate (through additional static and dynamic testing) the HSI inventory for the generic US-APWR. Phase 3 will then attempt to identify and make any final changes to that inventory and/or to the HSI, which may be required for a site-specific application, and ultimately to perform a last site-specific validation. At this point the design process assumes that only minor, if any, site-specific changes may be needed and, therefore, that Phase 3 testing effort will be limited.

3.3 V&V test methodology

The chosen methodology was based on the V&V testing to support the HSI design, as generally described in NUREG- 0711(NRC 2004)[7]. Both, Phase 1a and Phase 1b testing included:

- Experienced plant crews as test participants
- Realistic normal and emergency scenarios
- Collection of objective operator performance data as well as subjective operator feedback via questionnaires and verbal debrief sessions.

In Phase 1a, crews were tested over a four day period. Operators were provided with approximately 6.5 to 8

hours of training. Groups of two operators then participated in eight test scenarios:

- Five where all the HSI system, including the Operational VDUs and the LDP, were available
- Two where all the non-safety HSI system, including the Operational VDUs and the LDP, were not available and the operators had to accomplish operation using the Safety VDU
- One where all the digitalized HSI system, including the Operational VDUs, the LDP and the Safety VDUs, were not available and the operators had to accomplish operation using the Diverse HSI Panel (DHP)

A similar test methodology was used in Phase 1b testing. The methodology was slightly modified to address the specific goals of Phase 1b:

- Test Phase 1a HED's solutions, implemented on the MEPPI simulator.
- Test HSI features not tested in Phase 1a.
- Continue testing the full HSI.

3.4 V&V results

The verifications undertaken in Phases 1a and 1b consisted on a design verification effort, ref MUAP DC018, Rev. 2, section 18.10.2.2[6]. As the V&V program progresses, such as in task analysis through Phases 2 and 3, the verification effort will be expanded to include task support verification, as in NUREG-0711 Figure 11.1.[7] The objective of the Phase 1a and Phase 1b verifications was to meet, in part, the intention of section 18 of MUAP DC018, Rev. 2,[6];

- "The design verification confirms that the characteristics of the HSI, and the environment in which it is used, conform to HFE guidelines, as defined in the HSI Design Style Guide."
- "The design verification identifies any inventory or characterization non-conformance.
  Non-conformances that are accepted are documented with appropriate evaluation criteria and the basis for those criteria."

As a result of Phase 1a and Phase 1b V&V [5, 6], numerous HEDs were identified in VDU screens, alarms, computer-based procedures, console layouts and the DHP design. At the completion of Phase 1b, the number of HEDs was significantly reduced in comparison to the end of Phase 1a; i.e., most HEDs from Phase 1a V&V were resolved and validated, and some HEDs are to be resolved in Phase 2 or categorized as training issues. Crew performance with the modified Japanese Standard HSI System was generally good and the operators were able to adequately handle the set of scenarios presented. Operators' feedback on the overall HSI system design was positive.

The fact that operators' performance was generally adequate, despite the limited training, and that operator's feedback was positive, indicates that this Basic HSI System design is robust. However, there were a number of design issues with the modified standard Japanese HSI design that were identified to have a negative impact on operator work-load, operator ability to maintain the "big picture" and to "stay ahead" of an event (i.e., situation awareness), and to take control action in pace with the plant's dynamics. There were also limitations in "peer check" in both, the ability of reactor operators to peer check each other, and the ability of a senior reactor operator to follow and check, i.e., to supervise the activity of a reactor operator. These issues were reflected in the rating scores provided by operators on the operator feedback forms and on comments made during the debrief sessions. Nonetheless, results were generally favorable, underscoring the ease with which the US crews adjusted to the overall design.

One important generic issue is to consider operating practices and cultural differences in order to achieve a successful transition from a conventional analog HSI to a digital HSI. Results showed high level of acceptance of the new HIS design and that crews considered it to be significantly better than the conventional HSI design. Analysis result data found no indication of negative knowledge or negative training transfer. Many of the issues identified during the analysis are attributable to the fact that the Japanese design vision is not totally in line with the US operating philosophy. This differences help to explain the need of more display screens and of support functions such as task-screen and computer-based procedures. The performance of the large display panel, along with the smaller touch screen console VDU for drill-down, showed positive

results in the test environment. Operator and shift supervisor's VDUs also showed to be helpful in supporting the crews' ability to monitor progressing events in the plant. Nonetheless, maximizing situation awareness remains an important issue for digital HSI systems in general.

The statical verification of the design's compliance with US standards (NUREG-0700[9]) showed excellent results. No significant changes were needed to support the transition from the original design to the US-APWR one.

Phases 1a and 1b were successfully completed, with no unexpected circumstances.

4 Conclusions

Mitsubishi's digital I&C system for PWR plants, with a highly integrated HSI system, 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 results from Phase 1 V&V, described in this paper, suggest that the Japanese Standard HSI design can be easily adapted to US nuclear power plants and quickly understood by their operators, needing only relatively minor design changes. This conclusion is supported by the test data analysis and by the opinions of expert test observers, trainers and procedure writers, as well as by documented comments and ratings of US licensed reactor operators.

This digital I&C system may also enter the global market by being implemented into future plants and/or used for the digital upgrade of existing projects in other countries.

Mitsubishi continues improving the safety and reliability of its I&C system and is evermore committed to also enhance its design's operability and maintainability.

References

[1] SAKAMOTO, H., KITAMURA, M.: Integrated Digital I&C System for New Plants, 13th International Conference on Nuclear Engineering, ICON13-50308, 2005.

[2] MARUTA, Y., 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.2, October 2009.

[6] Mitsubishi Heavy Industries: Design Control Document for the US-APWR, MUAP DC018, Rev.2, October 2009.

[7] Mitsubishi Heavy Industries: Human-System Interface System Description and Human Factors Engineering Process, Topical Report MUAP-07007, Rev. 3, October 2009.

[8] U.S. Nuclear Regulatory Commission: Human Factors Engineering Program Review Model, NUREG-0711, Rev.2, Washington, DC, February 2004.

[9] U.S. Nuclear Regulatory Commission: Human System Interface Design Review Guidelines, NUREG-0700, Rev.2, Washington, DC, May 2002.

[10] Mitsubishi Heavy Industries: US-APWR Human System Interface Verification and Validation (Phase 1a), Technical Report MUAP-08014, Rev. 0, December 2008.

[11] Mitsubishi Heavy Industries: US-APWR HSI Design, Technical Report MUAP-09019, Rev. 0, June 2009.