SAFETY EVALUATION BY THE OFFICE OF NEW REACTORS

LICENSING TOPICAL REPORT MUAP-07007-P (REVISION 5)

"HUMAN SYSTEM INTERFACE SYSTEM DESCRIPTION AND HUMAN FACTORS ENGINEERING PROCESS"

MITSUBISHI HEAVY INDUSTRIES, LTD.

TABLE OF CONTENTS

1.0 INTRODUCTION 1

2.0 REGULATORY EVALUATION 2

3.0 TECHNICAL EVALUATION 3

3.1 Design Overview 3

3.2 Evaluation of Topical Report Application to Operating Nuclear Plants 3

3.3 Evaluation of Topical Report, Part 4, MHI HSI Design Description 4

3.3.1 General Infrastructure of the US-Basic HSI System 8

3.3.2 HFE Design Principles for the US-Basic System 9

3.3.2.1 VDU Configuration and Design 10
3.3.2.2 Large Display Panel 18
3.3.2.3 Alarm System 20
3.3.2.4 Soft Control System 26
3.3.2.5 Computer based procedures 29

3.4 Evaluation of Topical Report, Section 5, HFE Design Process 32

4.0 FINDINGS AND CONCLUSIONS 33

5.0 PLANT SPECIFIC HFE DESIGN
(e.g. US-APWR DC APPLICATION) ACTION ITEMS 34

6.0 REFERENCES 35

7.0 LIST OF ACRONYMS 36

SAFETY EVALUATION BY THE OFFICE OF NEW REACTORS

LICENSING TOPICAL REPORT MUAP-07007-P (REVISION 5)

"HUMAN SYSTEM INTERFACE SYSTEM DESCRIPTION AND HUMAN FACTORS ENGINEERING PROCESS"

MITSUBISHI HEAVY INDUSTRIES, LTD.

1.0 INTRODUCTION

By letter dated April 10, 2007, (Agency-wide Documents Access and Management System (ADAMS) Accession Number ML071080363), Mitsubishi Heavy Industries, Ltd. (MHI) submitted a request for the U.S. Nuclear Regulatory Commission (NRC) staff to review Topical Report MUAP-07007, "HSI System Description and HFE Process", Revision 0. Specifically, MHI requested the NRC staff to review and approve a functional design for the basic MHI Human System Interface (HSI) System and the Human Factors Engineering (HFE) process by which this basic design would be adjusted to reflect MHI's United States - Advanced Pressurized Water Reactor (US-APWR) and the operating nuclear power plants that install the associated MHI Instrumentation and Control (I&C) platform and I&C system design. In response to the NRC staff's comments raised at a non-public (proprietary) meeting held on June 12, 2007, MHI submitted Revision 1 (ADAMS number ML072040096) of this topical report on July 3, 2007.

By letter dated October 11, 2007 (ADAMS number ML072760340), the NRC staff identified their intent to review MHI's approach to the Control Room HFE design as described in the topical report. The topical report consists of two parts. The first part, Section 4, describes the US-Basic HSI system design and describes the applicant's plan to use the US-Basic HSI system as the starting point for US control room designs. Within this section, the applicant segregated the generic HSIs enabled by a distributed I&C system and then described their generic design. While specific to the MHI I&C and protective systems, the HSIs themselves have not yet been made plant-specific. The HSIs described in the topical report (referred to as the US-Basic HSI design) represent a generic, basic design platform whose structure can accept the specific design input required by a plant-specific application. These HSIs constitute basic building blocks used to support any plant-specific configuration. The second part, Section 5, describes the design process used to translate the US-Basic HSI system to the US-APWR HSI system or other plant-specific configuration. The applicant seeks approval of the MHI US-Basic HSI system and HFE design process for both new and operating nuclear plants. Both the US-APWR design certification (DC) and future licensing submittals for operating plant control room modifications using the MHI distributed I&C system would reference this topical report as the starting point for the plant specific HFE design.

By letter dated September 5, 2008 (ADAMS number ML082560781), MHI submitted Revision 2 (ADAMS number ML082560803) for this topical report to incorporate results of Phase 1 of the "Overall HFE Implementation Procedure" and to incorporate, where appropriate, responses to Requests for Additional Information (RAIs) by the NRC staff. The "Overall HFE Implementation Procedure" describes the translation of the Japanese HFE design to a US plant-specific HFE design. This phased implementation procedure is summarized in Appendix C of Topical Report MUAP-07007 and more completely described in MUAP-09019, "HSI Design", Part 1. Phase 1 is specific to the translation of language and cultural differences from the Japanese HFE design to the US-Basic HSI system.

By letter dated October 30, 2009 (ADAMS number ML093090164), MHI submitted Revision 3 (ADAMS number ML093090181) for this topical report as a result of the responses to RAIs by the NRC staff.

By letter dated July 15, 2011 (ADAMS number ML11217A010), MHI submitted Revision 4 (ADAMS number ML11217A015) for this topical report to address RAIs by the NRC staff.

By letter dated November 25, 2011, MHI submitted Revision 5 for this topical report to address RAIs by the NRC staff (ADAMS number ML113350172).

2.0 REGULATORY EVALUATION

The acceptance criteria used by the NRC staff as the basis for the review of MHI's HSI system are provided in NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," hereafter referred to as the Standard Review Plan (SRP). This document provides a method for complying with applicable sections of Title 10 of the *Code of Federal Regulations* (10 CFR), Part 50, "Domestic Licensing of Production and Utilization Facilities," and 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants".

SRP Chapter 18, "Human Factors Engineering," Revision 2 (March 2007), was the primary section of the SRP the staff used for reviewing MHI's HSI system. MHI first submitted the topical report for review in April 2007, referencing Revision 1 of Chapter 18 of the SRP. 10 CFR 52.47(a)(9) identifies that applicants must reference the SRP revision in effect six months prior to docketing the application and the US-APWR DC application was docketed on March 10, 2008. Since the topical report was submitted a month after the new revision of Chapter 18 was issued, the NRC staff finds it acceptable that MHI referenced Revision 1 of Chapter 18, but the NRC staff performed its review using Revision 2. The following are the regulatory requirements identified in Chapter 18 of the SRP as being applicable to HSI systems and HFE processes:

1. 10 CFR 50.34(f)(1)(i), Plant/site specific probabilistic risk assessment
2. 10 CFR 50.34(f)(2), Control Room design that reflects state-of-the-art human factor principles
3. 10 CFR 50.34(f)(3)(i), Administrative procedures
4. 10 CFR 50.34(f)(3)(vii), Management plan for design and construction activities
5. 10 CFR 50.54 (i) to (m), License responsibilities and minimum staffing level
6. 10 CFR 50.120, Training and qualification of nuclear power plant personnel
7. 10 CFR 52.47, Technical information required in Design Certifications
8. 10 CFR 52.79, Technical information required in Combined Operating License final safety analysis report

The following NUREG-Series publications and interim staff guidance (ISG) provide supplemental information, recommendations, and guidance. In addition, they serve as acceptable bases for implementing the above-noted requirements in the HFE approach in nuclear power plant design.

- SRP, Chapter 18, Section II.A, "Review of the HFE Aspects of a New Plant," Revision 2 dated March 2007

- NUREG-0700, “Human-System Interface Design Review Guidelines,” Revision 2 dated May 2002.

- NUREG-0711, “Human Factors Engineering Program Review Model,” Revision 2 dated February 2004.

- Digital I&C-ISG-05, “Highly Integrated Control Rooms - Human Factors Issues,” Revision 1 dated November 3, 2008.

3.0 TECHNICAL EVALUATION

3.1 Design Overview

In Topical Report MUAP-07007, the complete set of safety and non-safety HSI components is referred to as the HSI System. The safety-related HSI components are part of the Protection and Safety Monitoring System (PSMS). The PSMS includes the following I&C systems: Reactor Protection System (RPS), the Engineered Safety Feature Actuation System (ESFAS), the Safety Logic System and the Safety-Grade HSI System. The non-safety HSI components are part of the following I&C systems: Plant Control and Monitoring System (PCMS) or the Diverse Actuation System (DAS). The PCMS includes reactor and turbine control systems. The hardware and software supporting both PSMS and PCMS is referred to as the Mitsubishi Electric Total Advanced Controller (MELTAC) platform and is described in detail in Technical Report MUAP-07005, “Safety System Digital Platform, -MELTAC-”. Maximum utilization of a common digital platform throughout a nuclear plant reduces maintenance, training and changes due to obsolescence, thereby minimizing the potential for human error. The DAS is provided to accommodate beyond design basis common cause software failures that could adversely affect the PSMS and PCMS concurrent with operational occurrences and design basis accidents. The DAS provides diverse automation for time critical functions and diverse HSI to allow the operator to monitor critical safety functions and manually actuate safety process systems.

The system infrastructure (e.g., sensors, signal processing, computer processing, software) for PSMS, PCMS, and DAS is described in separate I&C related topical and technical reports (MUAP-07004 “Safety I&C System Description and Design Process”, MUAP-07005 and MUAP-07006 “Defense-In-Depth and Diversity”). These systems are described in this Safety Evaluation (SE) only to the extent necessary to understand their HSI.

3.2 Evaluation of the Topical Report Application to Operating Nuclear Plants

The HFE design interfaces with the I&C systems described in MUAP-07005-P and MUAP-07004-P. The NRC staff has not approved these reports for application to operating reactors. The NRC staff asked MHI to clarify the dependencies between the HFE design described in MUAP-07007, Section 4, and the I&C design described in the reports listed above. In the RAI response letter UAP-HF-10144, dated May 25, 2010, MHI explained that the US-Basic HSI System is tightly coupled to the MELTAC digital platform and to the system designs of the PSMS, PCMS and DAS. Therefore, MHI has no intention of implementing the US-Basic HSI System on an alternate I&C system design. With this constraint, the NRC staff determined that the conclusions of this report are equally applicable to the MHI I&C design if installed in an operating plant.

Therefore, the NRC staff approves the application of the HFE design to operating plants but only for those operating plants that install the associated MHI I&C platform and I&C system designs if and when they are approved for use by the NRC.

3.3 Evaluation of Topical Report, Part 4, MHI HSI Design Description

The MHI HSI System, hereafter called the US-Basic HSI system, is based on the Japanese Basic HSI System developed by MHI and Mitsubishi Electric Corporation for nuclear power plants in Japan. To create the US-Basic HSI System, MHI applied combinations of design review, redesign, and design verification to the Japanese HSI system through a phased implementation plan. Phase 1a of the implementation plan addressed language, engineering units, and cultural differences. It also made improvements identified from completing the Operating Experience Review program element from NUREG-0711 which included US nuclear plants and additional, generic, digital HSI technology experience. Phase 1b of the plan resolved deficiencies from Phase 1a, validated design changes, and updated Section 4 of the topical report (Revision 2) to reflect these changes.

The topical report describes the applicant's plan to use the US-Basic HSI system as the starting point for the US-APWR design. The following information was provided to support this plan.

1. The Japanese HSI design process is similar to the process described in NUREG-0711.

   The process used to develop the Japanese design is illustrated in Figure 4.0-1 from Topical Report MUAP-07007 (Figure 1).

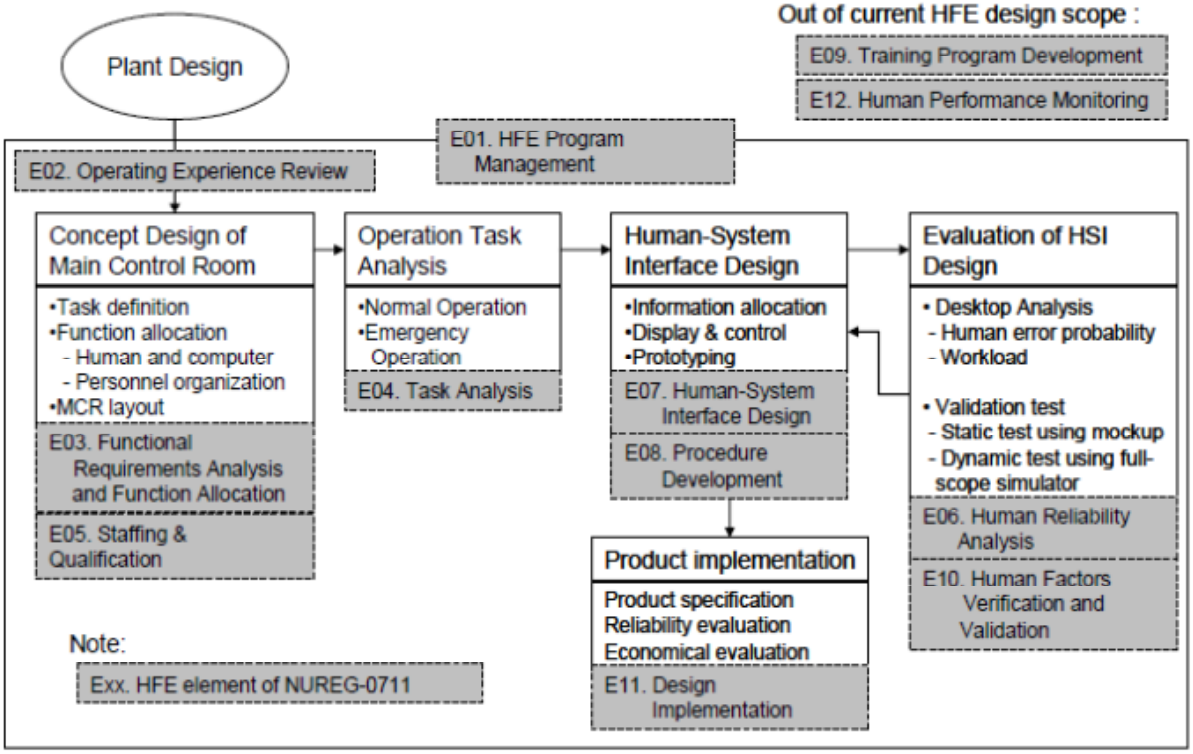

Figure 1: HFE Design Process for Japanese Standard HSI System

This process contains the major elements of NUREG-0711.

Initially, the NRC staff requested process descriptions and results summary reports describing the Japanese HSI design development so this information could be evaluated against the HFE guidance contained in NUREG-0711. This information was not readily available. Through a series of public meetings and teleconferences, the applicant explained that their intent was not to license the specific Japanese HSI design but to use the generic, foundational elements of that design as a generic starting point for what would eventually be a 10 CFR, Part 52 certified design that would use the NUREG-0711 process to develop the plant specific HFE design requirements.

2. Robust testing activities were applied to ensure the US-Basic HSI system met US standards.

Topical report MUAP-07007, Appendix A, describes the history of the Japanese Pressurized Water Reactor (PWR) main control room (MCR) and documents a significant engagement of Japanese operators in validating HSIs including the large display panel (LDP), Video Display Unit (VDU) applications, alarm processing, display design, and plant status diagnosis.

Topical Report MUAP-07007, Appendix B describes the testing methods that were used for the MCR during both development and implementation phases. For the development phase, a two-step process was used. First, a static verification confirmed that all monitoring and operating functions were available, that all operation controls are possible, and that the control boards conformed to ergonomic standards. This was followed by a “Dynamic Validation” where actual plant situations were simulated iteratively using the plant simulator.

Topical Report MUAP-07007, Appendix C describes the phased implementation plan that translates the Japanese HSI design to the US-Basic HSI system (Phase 1) and then to the US-APWR HSI system (Phase 2). US utility operators are engaged in each phase. Each phase utilizes a full scale HSI simulator with high fidelity plant simulation models. Phase 1 falls within the scope of the topical report.

The objective of Phase 1 was to define the US-Basic HSI system using the Japanese Standard HSI system as a basis. The Japanese HSI System, as applied in the US, is comprised of two components; the Basic HSI System and the HSI Inventory. The US-Basic HSI system is based on the Japanese Standard HSI design modified for application in the US. Initial modifications include translation to the English language and American engineering units; anthropometric changes to the consoles for American body types; and adoption of the US-style step-by-step operating procedures. Additional changes needed for the US-Basic HSI are to be identified through a HFE testing process using licensed US nuclear power plant operators.

To support Phase 1 testing, a main control room dynamic simulator facility was used to support dynamic testing of the US-Basic HSI system. Additionally, a static portable HSI system analysis tool, on a personal computer platform, was developed to support display screen design verification. Phase 1 is divided into

two parts. Phase 1a testing, which is the subject of technical report MUAP-08014, "US-APWR Human System Interface Verification and Validation, Phase 1a", Part 1, assessed the Japanese Standard HSI system to identify changes needed for the US-Basic HSI Design. Eight licensed operating crews participated in the testing activities. Each crew went through seven scenarios that included normal and emergency maneuvers under normal and degraded HSI conditions. Data collected included objective performance data, subjective observations by plant operations and HFE experts, and operator feedback solicited via Likert Rating scale questionnaires, verbal debriefs, and Human Engineering Discrepancy (HED) input forms. These multiple sources of information were used in combination to identify HEDs that were then entered into an electronic HED tracking database.

Phase 1b continued the testing process by evaluating the design changes to the Japanese Standard HSI system resulting from Phase 1a. Phase 1b used the same tools and experts as described in Phase 1a above. The results from the Phase 1b testing were also entered into the HED database and assessed by an Expert Panel with the end objective of defining the US-Basic HSI system. Technical Report MUAP-09019, "US-APWR HSI Design," Part 3 describes the method and results of Phase 1b testing.

The documents submitted by the applicant refer to this testing as "Validation and Verification testing." While this testing provides a functional validation and verification (V&V) of HSI design elements, the NRC staff has not used this terminology in order to avoid confusion with how "V&V" is used in NUREG-0711. From the NUREG perspective, V&V evaluations comprehensively determine that the design conforms to HFE design principles and that it enables plant personnel to successfully perform their tasks to achieve plant safety and other operational goals. Thus V&V is applied to the final design not interim stages of design development.

3. Operating Experience Review (OER) was completed.

The applicant submitted Technical Report MUAP-08014-P, "US-APWR Human System Interface Verification and Validation, Phase 1a," which, in Part 2, contains a description of the OER. In Part 2, Section 2, the applicant states the OER process was conducted for the development of the Japanese Standard HSI System. Part 2, Section 7, provides a generic description of this process and explains that information sources included:

- NUREG/CR-6400, "HFE Insights For Advanced Reactors Based Upon Operating Experience"
- Institute of Nuclear Power Operations (INPO) database
- Nuclear Information Archives (NUCIA) database - Japan Nuclear Technologies Institute (JANTI) databases are called NUCIA. NUCIA includes data from thousands of events, including failures, operational errors etc. from Japanese nuclear power stations.

The significant events from these sources, which influenced the design of the Japanese HSI System, are included in Technical Report MUAP-08014, Tables 6, 7 and 8.

The original operating experience evaluation has been updated and expanded. Recognized nuclear industry HFE issues and issues related to HFE technology were included in the review. Since the nuclear industry lacks significant experience with the modern HSI technology used in the US-APWR, the OER also encompassed the utilization of similar HSI technologies from other industries (nuclear processing and chemical facilities, transportation industries, and electrical transmission infrastructure). Findings of this expanded operating experience review that were generically applicable to all nuclear applications were included in the standard US-Basic HSI system which is the system being presented for approval in Topical Report MUAP-07007.

The NRC staff evaluated this OER report against the review criteria in NUREG-0711, Section 3, "Operating Experience Review" as part of the US-APWR Design Certification Document, Chapter 18 review. The staff concluded that the OER conformed to the NUREG review criteria. The safety evaluation for the US-APWR Design Certification provides additional detail describing how each review criteria was met. In summary, these review criteria suggest that operating experience should be collected from predecessor plant experience, documentation of recognized industry issues, related HFE technologies, and plant personnel. As outlined in the previous two paragraphs all these sources were used and the material that was applicable to the US-Basic HSI design was appropriately applied to that design.

By updating the operating experience review and including the results in the US-Basic HSI system, the NRC staff concluded that the applicant has effectively used operating experience information to update the HSI design described in the topical report.

Based on these three elements (Japanese design process, testing activities, and operating experience), the NRC staff determined that these elements provide a satisfactory basis for using the US-Basic HSI design as the starting point for plant specific designs, provided the generic HSI elements incorporated in the US-Basic HSI Design (as described by the topical report) are consistent with accepted HFE design principles. The remainder of this report explains how the principles were incorporated satisfactorily into the US-Basic HSI design. To facilitate the NRC staff's evaluation, the HSI design configuration presented in the topical report was characterized as general infrastructure, HFE design principles, or plant specific HFE design.

Aside from the design detail being used as an example, the NRC staff determined that the topical report does not contain plant-specific HFE design. MHI indicated that this material is developed as part of the plant-specific analysis phase of the HFE design program and submitted to the NRC as part of a license application process for new plants or license amendment process for operating plants. For example, Part 4, Section 4.9, "Large Display Panel" contains a list of parameters included on the panel and photos illustrating information layout and mimics. Normally this detail is derived from and/or supported by the function and task analyses elements described in NUREG-0711. The topical report acknowledges this in Section 4.9.2.1, where the parameters and their layout are referred to as "typical." Specific plant configuration is determined using the process described in Section 5 of the topical report.

Appendix D of the topical report provides a useful table describing the scope of the US-Basic HSI system in comparison with the plant-specific HSI system. The NRC staff found this approach acceptable because the US-APWR specific design is being developed following the regulatory guidance in NUREG-0711. This insures there will be complete and documented basis for the inventory of controls, alarms and displays that are incorporated within the HSIs described in the Topical Report. The Topical Report contains no information that would preempt the design work needed to identify the US-APWR inventory

The NRC staff's assessment of general infrastructure and HFE design principles is provided below.

3.3.1 General Infrastructure of the US-Basic HSI System (Topical report Section 4.1 and Section 4.2)

The US-Basic HSI system includes the following elements:

- The HSI system uses soft (touch screen or mouse based) operation. An operator, using a VDU, performs soft operations by requesting a system on the diagram screen and then touching or clicking an operational area of a soft switch displayed on the screen. This mode of control reduces operator workload compared with conventional HSI by providing relevant process control information in integrated VDUs displays and utilizing a compact console that minimizes required operator movement.

- Integration of monitoring and operation - The VDU interface introduces the capability of consolidating large amounts of data into meaningful information displays. The MHI design integrates safety and non-safety monitoring and control providing the following benefits:

  - Continuous awareness of critical safety functions while immediate focus may be plant maneuvering and power production.

  - A single operator can execute procedures that historically involve multiple operators to coordinate multiple safety divisions and non-safety systems. This simplifies task coordination for maintaining critical safety functions.

  - Operators can execute computer based procedures with integrated information and manual controls (e.g., via hyperlinks).

  - Minimizes operator transitions between safety and non-safety VDUs, thereby reducing operator workload during critical plant situations.

- Automatic verification of component status - The status of components such as valves and breakers and the status associated with plant trip signals, emergency core cooling system (ECCS) signals and isolation signals are automatically checked by comparing their status with the expected status defined in the computer archives.

- Inter-linked screen requests - Individual display screens are designed for monitoring specific plant systems or functions. All the related information required for related tasks (such as alarm diagnosis, control actions, procedure execution, monitoring auxiliary

functions, etc.) can be requested on the screen. Screens for related tasks are inter-linked in terms of the functional and/or operational relationship.

- LDP for situation awareness and information sharing - The primary purpose of the LDP is to provide spatially dedicated continuously visible (SDCV) information to operation personnel to enhance situation awareness. The LDP helps operators maintain continuous awareness of overall plant status and critical status changes, while they are engaged in operational details on a VDU display for a specific plant system or function. The secondary purpose of the LDP is to help the operations staff's coordination and communication by providing a common visualization of the plant information. The following functions are provided by the LDP so that all of the operators can understand overall plant conditions:

  - Display of key parameters and key component status for normal operation and emergency conditions.

  - Grouped alarm displays and dynamic alarm prioritization to aid operator response decisions.

  - Display the computer-checked results of component status verifications which support the operator's confirmation task.

  - Integration of all information in a graphic display that allows easy understanding of the plant situation and quick recognition of status changes.

- Alarm prioritization system - A dynamic prioritized alarm system is provided to avoid information overload and facilitate plant state identification. The alarm function in the PCMS compiles many simultaneous alarms and displays them on the alarm VDUs and on the LDP, with color coordination identifying three priority levels. Moreover, the priority of an individual alarm is changed automatically depending on the importance of additional alarms, so that when more critical/important alarms are activated, the overall plant status is easily recognized.

The NRC staff determined that these infrastructure elements are commonly used applications of digital control system technology. While the applications described above are specific to the nuclear power plant control room, the use of digital control technology in other industries (i.e., transportation, chemical, petrochemical, manufacturing) have demonstrated that similar applications reduce operator task burden and reduce the potential for human error. The NRC staff concludes that these infrastructure elements provide reasonable assurance that plant personnel will be able to effectively monitor plant status, identify opportunities to improve the performance of equipment and systems, and to anticipate, understand, and respond to potential issues and problems in meeting both the production and safety goals. These infrastructure elements and the HFE design principles they are subject to (as described in section 3.3.2 below) conform to the regulatory requirement in 10 CFR 50.34(f)(2)(iii) that the Control Room design reflects state-of-the-art human factor principles.

3.3.2 HFE Design Principles for the US-Basic HSI System (Topical report Sections 4.3 through 4.11)

HFE design principles are implemented within the infrastructure elements described above and address information display characteristics, user-interface interaction and management, controls, functionality requirements, and workstation layouts. These design principles are derived from research and operating experience and are collected in documents such as NUREG 0700, "Human-System Interface design Review Guidelines". The majority of the US-Basic HSI system design information presented in Part 4 of the topical report falls into this area. The design principles are either specifically stated or illustrated and frequently cross referenced to the applicable NUREG-0700 guidance. For example, VDU's are used as the HSI for accomplishing the first four general infrastructure elements (soft operation, integration of monitoring and operation, automatic verification of component status, and Inter-linked screen requests). The design principles applied to the VDUs are described in Topical Report MUAP-07007 Sections 4.3 through 4.6 at a level of detail comparable to NUREG-0700, and include console layout, VDU display organization, display design, and display navigation. While the details of the HSI design are subject to improvements based on the results of the HFE program described in Section 5 of the topical report, the NRC staff concludes that the HFE design for the infrastructure elements conforms to the HFE design standards found in NUREG-0700. The NRC staff reached this conclusion based on two separate evaluations. First, the design as described in the topical report was compared directly with guidance in NUREG-0700 and second, an audit was performed to verify that the MHI HFE design procedures, including the Style Guide described in NUREG-0711, contained comparable information to that in NUREG-0700. Both evaluations used a sampling approach to verify that the regulatory guidance in NUREG-0700 was implemented effectively. More detailed information on these evaluations is provided in the following sections of this SE.

3.3.2.1 VDU Configuration and Design

The VDU is the primary HSI for the first four general infrastructure elements listed in Section 3.3.1 of this SE. In the US-Basic HSI design, VDUs providing four functions are installed at the operator console, the supervisor console and the Shift Technical Advisor's console. The following table describes these functions:

VDU application	**Main purpose**
operational VDU	To execute all of the plant control and monitoring functions, including control of the safety systems.
safety VDU	To execute the safety-related control and monitoring functions as a backup for the Operational VDU. It can control operation signals from the Operational VDU.
alarm VDU	To acknowledge and display individual alarms using prioritization color codes. Alarm VDU also provides the alarm confirmation/non-confirmation information to the operator.
operating procedure VDU	To provide computer-based operation procedure displays near the operational VDU and the alarm VDU in order to facilitate and simplify the performance of operation procedure.

Each VDU has an associated navigation system designed to provide the operator with easy access to each display. And similarly, each display is designed to be easily understood and used. The NRC staff compared the VDU HFE design against applicable guidance from NUREG-0700, Sections 1 and 2, to verify the HFE design is effective in accomplishing these

goals. The more general criteria from these sections are stated in Topical Report MUAP-07007, Section 5.7.3.2, which illustrate how the style guide conforms to NUREG-0700. These general criteria are restated below to provide an understanding of the criteria that the NRC staff is using in the evaluation that follows.

- Display design consistency:

  Consistent interface design conventions are evident for all display features, and displays are consistent in word choice, format, and basic style with requirements for data and control entry. There is an explicit mapping between the characteristics and functions of the system to be represented and the features of the display representation.

- Understandability of Information:

  Information is displayed consistently according to standards and conventions familiar to users. The characteristics and features of the display used to represent the process are readily perceived interpreted by the operator. The methods by which lower-level data are analyzed to produce higher-level information and graphical elements are understandable to users.

- Grouping of Information:

  Related information is organized into groups. Information that must be compared or mentally integrated is presented in the close spatial proximity and use similar physical dimensions to convey meaning. If information must be mentally integrated, similar color codes is used for the information items.

- Readability of Information:

  Important display elements and codes are identifiable and readable from the maximum viewing distance and under minimal ambient lighting conditions. Coding shall not interfere with the readability of displayed information.

- Distinctive Coding:

  Distinctive means of coding/highlighting is used when a user's attention must be directed to changes in the state of the system, critical or off-normal data, and hazardous conditions. When a graphic display contains some outstanding or discrepant feature that merits attention by a user, supplementary text is displayed to emphasize that feature.

- Uncluttered Displays:

  Displays are as uncluttered as possible.

- Indication of Display:

  A display feature is provided to indicate to the user that the system is operating properly. Information system failures (due to sensors, instruments, and

components) result in distinct display changes, which directly indicate that depicted plant conditions are invalid.

- Display Update Rate Requirements:

  The maximum update rate is determined by the time required for the user to identify and process the changed feature of the display.

- Character:

  Rule for using character in title, message and label is provided, and guideline includes appropriate character size, height-to-width ratio.

- Labels:

  Each individual aspect of a display (e.g., data group, field, or message) contains a distinct, unique, and descriptive label.

- Color:

  Where color is used for coding, it is employed conservatively and consistently. Table 5.7-1 shows the example of color coding rule.

- Tables and Lists:

  Information is organized in some recognizable logical order to facilitate scanning and assimilation. A table is constructed so that row and column labels represent the information a user has prior to consulting the table. Labels include the unit of measure for the data in the table; units of measurement are part of row or column labels.

- Graphs:

  Graphs convey enough information to allow the user to interpret the data without referring to additional sources. When multiple curves are included in a single graph, each curve is identified directly by an adjacent label, rather than by a separate legend.

- Mimics:

  Mimics and diagrams contain the minimum amount of detail required to yield a meaningful pictorial representation. All flow path line origin points are labeled or begin at labeled components. All flow path line destination or terminal points are labeled or end at labeled components. Flow directions are clearly indicated by distinctive arrowheads. Where symbols are used to represent equipment components and process flow or signal paths, numerical data is presented reflecting inputs and outputs associated with equipment.

- Icons and Symbols:

The primary use of icons in graphic displays is to represent actual objects or actions. Icons are designed to look like the objects, processes, or operations they represent, by use of literal, functional, or operational representations. Icons are simple, closed figures when possible. Special symbols to signal critical conditions are used exclusively for that purpose.

General HFE design for VDUs

In general, the MHI display network is designed to use touch screen commands. Displays have been designed with sufficient space that the operator can reliably touch the active component desired. The spacing required for touch screen operation results in good separation in lists enhancing their readability. When a system mimic is too large for one display, sections of the mimic are moved to additional pages that are accessed via a function toolbar at the bottom of the display. In general, lists that are too long for one display page use a scroll bar to access the bottom of the list.

The information hierarchy is limited to two or three levels depending on which VDU is used. This supports easy recognition of where one is in the hierarchy and ensuring efficient access to needed information. General display pages provide an overview of the information structure. Information is coded by the system or, in the case of the alarm VDU by priority, to allow for quick recognition and retrieval. Display pages are titled and numbered making it clear where the user is within the data network. Information priority is established by position on the page and color coding. Screen design is consistent in the use of labeling, color, and function key placement facilitating quick recognition and use of information. Additional detail describing how each VDU accomplishes HFE guidance is provided below:

Evaluation of operational VDU display and navigation

The top level system display uses a containment mimic to separate containment systems from others, and uses lines to illustrate functional dependencies between systems. With only three levels of information, this display network has a flat information hierarchy simplifying the task of recognizing where in the network the current display is situated and thereby minimizing confusion in navigation or information location. The transition from higher level information such as critical safety function or the emergency display request area is accomplished with minimum navigation steps thus keeping lower level supporting information readily available. Consistent formatting within each information level and unique content at each level make each information level easy to differentiate from displays in other parts of the display network. Additionally, each display page is labeled with the system and/or component title(s) to further communicate the position of a display in the larger information space.

The emergency display request area of the top navigation display provides immediate access to safety status information that would typically be needed during implementation of emergency procedures. Examples could include plant trip status, ECCS valve status, and Containment isolation status. This feature expedites information retrieval (discussed next) but in the context of orientation features it completes the overview of information available to the operator and continues to support a flat information hierarchy for key safety information that would otherwise have to be collected from numerous system level display screens.

In Topical Report MUAP-07007, Section 4.4.2a, the applicant explains that the top navigation display described above is the screen typically used to access information but an alternative method is available. By selecting the “Screen List Menu” the operator can display system

groupings in alpha-numeric order. The emergency information categories are included in the list and color (dark verses light blue) is used to maximize the visibility of display groups. A function toolbar at the bottom of either display allows the operator to easily change between the two top level displays. At the second level, system mimics are provided that contain system information and access to control features. Lateral movement between systems without returning to the top level navigation displays is supported by a vertical function bar at the right hand edge of the VDU display that allows the mimics for associated systems to be called up. Mimic displays consistently use a black background with various light colors representing the system mimic indications. Active components on the mimic are configured to look like convex shaped buttons providing the operator with a simple, visible cue for accessing the third level of the display network which provides the soft controls for the associated component. When the buttons are touched (or clicked on) the soft control becomes available. The default popup position is consistent (right-lower side) and if the related information is hidden by the popup window, the default popup position is automatically set in the other corner of the screen. The operator can manually move the popup window in the unusual case that other information relevant to the operation may be hidden. This design minimizes display clutter and provides the operator with a consistent transition between display hierarchies. Function toolbars are also available on all second and third level displays allowing the operator to move forward and backward between displays and a “MENU” button for returning to the top navigation display. This functionality provides for simple, efficient movement both vertically and horizontally in the display network. Functional controls are kept with required information in the following manner. On/Off switches and controllers which are used in a manner similar to an on/off switch are displayed on the system mimic display (second level display on the operational VDU) where the status of the component is shown. Controllers and mode selectors providing control functions are only available in fixed positions on the controller screen (third level display on the operational VDU) that displays trend graphs and related parameters required to monitor the changing trends.

The NRC staff concluded that the general design of the operational VDU satisfactorily implements regulatory guidance for display selection and navigation. The design provides reasonable assurance that the operator will be able to efficiently and reliably manage information within the display network structure.

Evaluation of safety VDU display and navigation

The safety VDUs provide monitoring and component level control for safety functions. The safety VDUs are designed to satisfy class 1E requirements. They are divided into two groups: two multidivisional safety VDUs and four selectable train-based safety VDUs. The orientation and retrieval features of the safety VDU network are similar to the operational VDU network but there is significantly less information being managed.

The multidivisional safety VDUs are dedicated to monitoring Post Accident Monitoring variables and parameters supporting credited manual operator actions. All parameters displayed are spatially dedicated and continuously visible and include alarm color coding. These VDUs and their design features minimize navigation needed to monitor critical safety parameters and improve situation awareness of total plant status particularly during a loss of the non-safety related PCMS system. These VDUs fulfill the requirement for a dedicated display of the key safety parameters. These parameters are also available on the large display panel.

The selectable train-based safety VDUs are normally in a system monitoring mode with plant control functions being implemented through the non-safety related operational VDU. Function buttons in the right hand navigation tool bar allow isolation of the operational VDU outputs and

component control from the safety VDU if required. There are two modes of operation. In the train-based mode, safety function control and monitoring are arranged by plant systems and are provided separately for each train. In the task-based mode, monitoring and control are still provided separately for each train, however, the monitoring and control functions are grouped so that a single screen supports a predefined set of tasks needed to execute emergency operating procedures. This mode reduces the navigational task burden that would be necessary during Emergency Operating Procedure execution.

The selectable train-based safety VDUs retain the three-level information hierarchy. The top level display is organized by system number with a name following the number. This does not provide an easy method for identifying the system of interest unless the system numbers or screen locations have been memorized. Alphanumeric presentation of the systems and components within those systems is not used. There does not appear to be any organizing principle. The second level displays the components associated with the system selected on the top level display. One page can display 20 components. The organizing principle used is not apparent and requires the operator to memorize position locations. MHI addressed this concern by reorganizing the screens so systems and components are presented in alphabetical order. This change is reflected in MUAP-07007, Revision 5. The NRC staff concludes that this change provides for efficient navigation through the information hierarchy. The third level of the information hierarchy contains the component soft controls either grouped by systems or by tasks. It is structured the same as the operational VDU third level but only contains safety-related soft controls.

Similar to the operational VDU, the safety VDUs use contrast between light and dark colors to maximize the visibility of display groups at both the first and second information levels. The third level (safety controls) uses a black background with light colors for controls and associated information.

Based on observations of the VDUs during simulator demonstrations, the NRC staff concluded that there was no distortion of the foreground information and that the contrast between foreground and background supported effective use of the VDU displays.

The NRC staff concluded that the general design of the safety VDUs satisfactorily conforms to regulatory guidance for display selection and navigation. The design provides reasonable assurance that the operator will be able to efficiently and reliably manage information within the display network structure.

Evaluation of alarm VDU display and navigation

The alarm VDUs present one level of information and contain lateral connectivity to the operating procedure VDUs and the operational VDUs. It uses functional grouping (primary systems in containment, primary system outside containment, secondary systems, and electrical systems as well) as grouping by alarm type as the initial organization principle then within each of these categories uses a chronological sequence to display the alarms. Again, organization of information by system is carried across all VDUs as a fundamental organizing principle and provides a logical and easily understood method for data retrieval. Alarm groups (first out alarm, alarm, caution, status, and alarm cleared) are segregated on individual pages providing simple prioritization of information to the operator. The conventional alarm color scheme is used (red, yellow, green, white) providing clear differentiation between the alarm groups as well as providing simple clear orientation coding for the display page that the operator is using. Black letters on yellow, green, white and light gray backgrounds and white letters on

red background provide sufficient contrast to easily read the information. Function buttons are provided on a horizontal toolbar at the bottom of the display providing alarm controls (acknowledgement and silence), page selection for alarm lists that exceed the 15 available message lines, and an alarm group select which allows the operator to toggle between the types of alarm the operator is investigating. These function buttons maintain a flat information hierarchy and allow the operator to move laterally through the display network using one touch (or mouse click) to reach the display screen of interest. The alarm VDU interfaces with either the operating procedure VDU or the operational VDU depending on which is selected in the function tool bar. The operator touches (or clicks) the alarm name field to call up either the alarm response procedure or the system mimic (from which he can initiate component control functions). The hypertext links all used text descriptions (verses symbols or cursor coding). The text descriptions are one to two words for the function toolbar and the alarm name. The out-of-specification condition is included in the alarm description (e.g., high, low) and did not add visual clutter to the display. Some abbreviations were used but followed conventional nuclear industry abbreviations and did not introduce confusion.

The NRC staff concluded that the general design of the alarm VDU satisfactorily conforms to regulatory guidance for display selection and navigation. The design provides reasonable assurance that the operator will be able to efficiently and reliably manage alarm information within the display network structure. Electronic interfaces with alarm procedures and component control function provide reasonable assurance that the operator will be able to effectively use the alarm VDU to manage plant operation.

Evaluation of operating procedure VDU display and navigation

The operating procedure VDU displays procedures that are structured in accordance and compliant with the textual images from the hardcopy procedure. This provides a task sequence the operator is familiar with. It also retains the writer's guide formatting designed to enhance usability of the procedure. Procedures are presented in a standardized format with title and a specific procedure index in a left column display allowing the operator to move to the desired section of a procedure. The function bar is available at the bottom of the page to allow interface with the operational VDU where control functions are initiated. Or, as an alternative, by selecting hyper-links on the operating procedures VDU, the related operational VDU display is automatically displayed. The related soft switch or controller is not requested directly on the operating procedures VDU to avoid operator's omission of relevant information confirmation. The procedure menu (including alarm response) and bookmarking controls are also provided allowing for simple lateral movement into controls and/or information needed to implement the procedure. The alarm VDU supports similar lateral movement by using a function key to bring up alarm response procedures on the operating procedures VDU. In case of emergency, such as plant trip, the operators can request the emergency procedure for reactor trip or ECCS by touching the first-out alarm on the alarm VDU. Distinctive accident procedures (e.g., loss-of-coolant accident (LOCA), Steam Generator Tube Rupture (SGTR)) are requested from the Computer Based Procedure (CBP) menu screen after the operator identifies the plant status.

The use of CBPs with VDU interface is a generally accepted approach. The evaluation of the CBP as a basic HSI is provided later in this SE. The VDU interface described in the topical report incorporates general HFE design principles similar to the other VDU displays. Since the role of the operating procedure VDU is to facilitate access and use of procedures rather than present plant information supporting the operators' decision making and control actions as the other VDUs do, the NRC staff concluded that the basic HFE description associated with the operational VDU was sufficient. The HFE design that is included in the writing and presentation

of emergency operating procedures is more prescriptive and is evaluated as part of licensing activities.

Audit of HFE design related documents

Many NUREG-0700 VDU related criteria are of a detailed technical nature. They are not evident by observation of the VDU display and are typically captured in the applicant's HSI style guide or in equipment specification documents. The NRC staff conducted an audit of these MHI documents on May 26, 2010, and July 12, 2010, to verify that a sample of applicable NUREG guidance is captured in controlled documents. In general, these criteria maximize the operator's ability to quickly and accurately use the VDU displays.

During the audit, the MHI staff used the following procedures to demonstrate where, and to illustrate how, the NUREG-0700 criteria selected by the NRC staff were addressed:

- General display page characteristics as outlined in NUREG-0700, Section 1.5 were addressed in the I Design Style Guide (JEJC-1763-1001) and the Functional Specification of Operational VDU system (NO-EK16009).

- System response time, as outlined in NUREG-0700, Section 2.4.3, is addressed in the Basic Requirements of I&C System (NO-EK10001).

- Orientation features for display and navigation as outline in NUREG-0700, Section 2.5.1.1 were addressed in the Functional Specification of Operational VDU system (NO-EK16009), Functional Specification of Safety VDU (NO-EK16008), and the I Design Style Guide (JEJC-1763-1001).

- Retrieval features for the display selection and navigation as outlined in NUREG-0700, Section 2.5.1.2, were addressed in the Functional Specification of Operational VDU system (NO-EK16009), the Functional Specification of Safety VDU (NO-EK16008), and the Basic Requirements of I&C System (NO-EK10001).

- CBP System information Display attributes as outlined in NUREG-0700, Section 8.1 and Section 8.2, were addressed in the CBP System Specification (JEJS-U04004).

The NRC staff found one to one correspondence between the NUREG criterion evaluated and the design procedures. Additionally, specific design guidance had been substituted for the generic guidelines in the NUREG as would be expected in a completed design.

The NRC staff concludes that the general design of the operational VDU, satisfactorily implements regulatory guidance for display selection and navigation. The design provides reasonable assurance that the operator will be able to efficiently and reliably manage information within the display network structure.

The NRC staff concludes that the general design of the safety VDU, satisfactorily implements regulatory guidance for display selection and navigation. The design provides reasonable assurance that the operator will be able to efficiently and reliably manage information within the display network structure.

The NRC staff concludes that the general design of the alarm VDU, satisfactorily implements regulatory guidance for display selection and navigation. The design provides reasonable assurance that the operator will be able to efficiently and reliably manage alarm information within the display network structure. Electronic interfaces with alarm procedures and component control function provide reasonable assurance that the operator will be able to effectively use the alarm VDU to manage plant operation.

The NRC staff concludes that the general design of the operating procedure VDU, satisfactorily implements regulatory guidance for display selection and navigation. There are satisfactory interfaces with the other VDUs to facilitate use of the operating procedure VDU. Basic HFE principles used in the operating procedure VDU (i.e., function tool bar, titles and labels) are consistent with those used in the other VDUs.

3.3.2.2 Large Display Panel

The purpose of the large display panel (LDP) is to ensure all relevant plant information is continuously visible to the plant operator and to make the same information simultaneously available to all control room operating staff to support the operator activities. The LDP contains fixed and variable display areas on four, 100 inch diagonal screens. Three of these screens are dedicated to the fixed display area which provides:

- The main plant parameters required for monitoring the plant status during normal operation, enabling quick error detection.
- The main plant parameters required for monitoring the plant status during power fluctuation and parameters that may cause a plant trip.
- Information required for verification of trip status information related to the reactor, turbine and generator immediately following a plant trip.
- The engineered safety features components status and process values indicating system performance.
- Type A and B parameters of RegulatoryGuide1.97, “Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants.”
- Alarm groupings.
- Safety system bypass or inoperable state indication.

This information is organized using a plant mimic showing primary systems, containment systems and turbine-generator/electrical systems. Alarm groupings are provided across the top of the fixed area display and provide:

- Alarms relevant to Post Accident Monitoring parameters.
- Alarms demanding urgent responses.
- Alarms used for identification of major events.

- Alarms important for overall supervision of plant status (Pressurizer Press Low, etc.).

- Alarms from automatically checking RPS and ESFAS actuations.

- Alarms from automatically checking the operability of engineering safety features (ESF) plant components.

- Alarms from automatically checking the critical safety function status tree logic.

- Alarms resulting from partial trip of RPS and ESFAS Channels.

The fourth screen is the variable display area where detailed plant information and trend displays on the operational VDU display can be displayed. The content of the variable display area can be selected from the operator console and from the supervisor console, thereby helping the operating staff's common awareness and communication. The variable display area can also automatically display pre-selected screens based on trigger signals such as a first out alarm or any operational VDU display the operator chooses.

The NRC staff used applicable guidance from NUREG-0700, Sections 1, 5 and 6, to verify that the HFE design would effectively support these functions. The NRC staff found that the LDP conforms to the guidance in NUREG-0700. The NRC staff noted that the LDP design provides a significant contribution to maintaining awareness of overall plant status, maintaining awareness of crew member actions, and facilitating team communications. These three areas are recognized as challenges when shifting from conventional control rooms to control rooms with computer-based work stations. The MHI design provides for a seamless display of the information (even though three screens are being used and the plant mimic used coordinates and organizes the information so that operators can efficiency and reliably locate needed information. The LDP presents a significant amount of information but always within a construct (such as safety function, ESF status) that associates the information with higher level safety objectives. The "OK Monitor" that provides a status of automatic checks on actuation results for RPS and ESFAS and the "Critical Safety Function Monitor" which provides a status of automatic checks of the critical safety function status tree logic are examples of how the information is managed to minimize the time operators spend completing verification checks while at the same time providing summarized critical safety information. The LDP maintains the same label, symbol, and color conventions used in the VDU display design thus minimizing operator confusion in moving between HSIs. Placement of the operator and supervisor consoles, as described in the topical report, Section 4.3.1, provides for acceptable visibility of the LDP displays and conforms to guidance in NUREG-0700. The NRC staff had several opportunities to observe the LDP during meetings with the applicant, as the applicant described the LDP components and as operators used it during scenario demonstrations. The NRC staff's observations reinforced the conclusions outlined above.

Audit of HFE design related documents

Many NUREG-0700 LDP related criteria are of a detailed technical nature. They are not evident by observation of the system displays and are typically captured in the HSI style guide or in equipment specification documents. The NRC staff conducted an audit of these documents on May 26, 2010, and July 12, 2010, to verify a sample of applicable NUREG guidance is captured in controlled documents.

During the audit, the MHI staff used the following procedures to demonstrate where and to illustrate how the NUREG-0700 criteria selected by the NRC staff were addressed:

- LDP Functional Specification (Draft procedure NO-EK16013)

- Basic Design Requirement of HSI System (NO-EK16002)

The NRC staff found a direct correspondence between the NUREG criterion evaluated and the design procedures. Additionally, specific design guidance had been substituted for the generic guidelines in the NUREG as expected in a completed design.

The NRC staff concludes that the general design of the LDP, as specified in the "LDP Functional Specification" and the Basic Design Requirement of HSI System," conforms to the regulatory guidance for display design, safety parameter displays, and group-view displays. The design provides reasonable assurance that the operating crew will be able to maintain awareness of overall plant status, maintain awareness of crew member actions, and facilitate team communications.

3.3.2.3 Alarm System

In the Topical Report MUAP-07007, Section 4.7, the applicant states that the alarm system provides all information necessary for detecting abnormal plant conditions and ensures that the operator can easily recognize the fault conditions even when the number of fault conditions or the severity of the faults are increasing. The alarm system supports this objective by:

- Providing adequate information presentation that allows the operator to acknowledge and recognize alarm information and take appropriate corrective actions.

- Establishing an alarm prioritization system that allows the operator to identify the relevant and important alarm information and not to deal with "alarm avalanche."

- Implementing a navigation system display that provides easy access from the alarm display to the relevant system display and the alarm response procedures.

Alarm information is displayed on the alarm VDU, LDP and the operational VDU.

The alarm VDU has a navigation system designed to provide the operator with easy and simple access to each display. And similarly, each display is designed to be easy to understand and use. An overview of HFE design of the alarm VDU is provided in Section 3.3.2.1 of this SE. In Section 3.3.2.1, the NRC staff provides an evaluation of the alarm system HFE design as compared to applicable guidance in NUREG -0700, Section 4. The NRC staff found that the alarm system conforms to the guidance in NUREG-0700.

- NUREG-0700, Section 4.1.1, contains criteria associated with the alarm definition. The alarm definition is the specification of the types of process parameters to be monitored and displayed by the alarm system and the setpoints to be used to represent those parameters.

Evaluation: The alarm system interfaces with the LDP, operational VDUs, and alarm VDUs. The displays on these interfaces demonstrate that alarms will be provided for critical safety functions and the key parameters needed to monitor all plant conditions. Specific alarms and setpoints are defined and then verified and validated later in plant specific applications that implement the HFE design process described in NUREG-0711. The alarm system design includes logic to avoid nuisance alarms. A darkboard configuration (no alarms lit) is the normal state for the alarm system. Accordingly the NRC staff concludes that the design for alarm definition conforms to the applicable NUREG-0700 guidance.

- NUREG-0700, Section 4.1.2, contains criteria associate with alarm processing. Alarm processing has two components.

  Alarm signal processing refers to the process by which signals from sensors are automatically evaluated to determine whether any of the monitored parameters have exceeded their setpoints and to determine whether any of these deviations represent true alarm conditions. Alarm condition processing refers to the rules or algorithms used to determine the operational importance and relevance of alarm conditions; this process determines whether the alarm messages that are associated with these conditions should be presented to the operator.

  Evaluation: In the topical report, Section 4.7.2 the applicant describes the Alarm prioritization. Many alarms are statically prioritized by importance based on plant impact including release of radioactive materials and the demand for operator action. The prioritization levels are displayed on an alarm message area on the alarm VDU. The priority of other alarms is dynamically determined by the alarm processing logic which focuses on the relationship between each issued alarm as measured by physical relationships such as the plant process and equipment status. Based on that dynamic determination, each alarm is prioritized at the given moment to its importance. The rules used for this prioritization are described and examples are provided of how they are applied.

  The prioritization rules that the applicant has applied to the alarm processing have significantly reduced the number of alarms that the operators must respond to during off-normal events as compared to a conventional alarm system. This is accomplished by the following methods.

  - Information needing operator action or confirmation is segregated from the status information which requires no operator acknowledgement.

  - Mode dependence processing allows alarms only in the modes where the condition is applicable.

  - System configuration processing allows associated component alarms only when the alarm is pertinent to the existing system configuration.

  - Logical consequences processing is used to characterize lower importance as status information when higher priority alarms are activated.

It should be noted that the effectiveness of these alarm processing strategies must be verified as part of the staff's review of the integrated system validation in the design control document (DCD), that is completed as part of the HFE process described in NUREG-0711.

The NRC staff concludes that the current alarm system configuration provides reasonable assurance that alarm processing for the US-Basic HSI design is consistent with a "State of the Art Control Room" HFE design. It provides prioritized alarms designed to minimize the potential for information overload for Control Room operators during off-normal plant conditions. The proposed design for alarm processing conforms to the applicable NUREG-0700 guidance.

- NUREG-0700, Section 4.1.3, contains criteria associated with alarm prioritization and message availability.

  Evaluation: Alarms are separated into three priorities based on static and dynamic prioritization rules described above. Priority 1 alarms require operator actions and are color coded red on the alarm VDU and LDP. Priority 2 alarms require operator acknowledgement and are color coded yellow on the alarm VDU and LDP. Other alarms including those that have been suppressed, filtered, or made low priority by the prioritization rules are displayed as green Priority 3 alarms and are displayed on the alarm VDU. Accordingly, the NRC staff concludes this design for alarm prioritization and the message availability conforms to the applicable NUREG-0700 guidance.

- NUREG-0700, Sections 4.2.1 through 4.2.3, contain criteria associated with general alarm display guidelines. The information display aspects of alarms include both auditory and visual components.

  Evaluation: The alarm display features of the alarm system support the operator's rapid understanding of the alarm condition by its use of the following features:

  - Priority is communicated using color coding. Red is used to identify any alarm condition requiring operator action. These alarms are listed in the order they occur on a dedicated alarm VDU display screen. Less important alarms and cleared alarms are moved to lower priority alarm screens and are color-coded as yellow and green. The cleared alarm screen is color-coded as white.

  - Alarm states (new, acknowledged, cleared and reset) are communicated by visual and audible coding. The operator becomes aware of a new alarm by the blinking display and audible tone, and recognizes the new alarm information in the alarm VDU display. When the alarm is acknowledged the alarm display area on the alarm VDU stops blinking. When alarm conditions return to normal, the alarm is displayed as cleared. Cleared alarms are identified by low speed blinking and white color indications. Cleared alarms are manually reset by operator acknowledgement. Reset alarms return to normal indication (i.e., no-indication on the Alarm display and normal color (gray color) on the LDP).

- First out alarms are provided for reactor trip, turbine trip, generator trip, and ECCS actuation. The first out alarms are displayed at the top of the alarm VDU and the LDP.

- The operator can call up the related alarm procedure display on the operating procedure VDU and the related operational display on the operational VDU, respectively, directly by touching or clicking the alarm message display area on the alarm VDU in order to diagnose and take actions.

Spatially dedicated, continuously visible alarms are provided on the LDP. In addition to the first out alarms mentioned above, alarm groupings are provided across the top of the fixed area display and provide:

- Alarms relevant to Post Accident Monitoring parameters.

- Alarms demanding urgent responses.

- Alarms used for identification of major events.

- Alarms important for overall supervision of plant status (Pressurizer Press Low, etc.).

- Alarms from automatically checking RPS and ESFAS actuations.

- Alarms from automatically checking the operability of ESF plant components.

- Alarms from automatically checking the critical safety function status tree logic.

- Alarms resulting from partial trip of RPS and ESFAS Channels.

Accordingly, the NRC staff concludes this design for general alarm display conforms to the applicable NUREG-0700 Guidance.

- NUREG-0700, Section 4.2.4,"Display of Shared Alarms," and Section 4.2.5, "Alarm Controls," address HFE design characteristics at the specific alarm level. This design detail is developed later in plant specific applications that implement the HFE design process described in NUREG-0711. NUREG-0700, Section 4.2.6, contains criteria associated with coding of alarm system information. Visual coding refers to how color, shape, brightness, texture/pattern, and flash rates are used. Auditory coding refers to how frequency, volume, tonal character, and audio pattern are used.

  Evaluation: In general alarm-coding methods, because of their detailed technical nature, are specified in the alarm design specifications. The NRC staff conducted an audit of these documents on May 26, 2010, and July 12, 2010. During this audit, the NRC staff verified a sample of NUREG-0700 criteria which was addressed in the design documents. The results of this audit are discussed below.

Based on the alarm system coding described in Topical Report MUAP-07007 and demonstration of the alarm system on the MHI simulator, the NRC staff determined that the color and audible coding used is well below the maximum coding limits suggested in the NUREG and is consistent with the alarm coding in use at operating plants. Accordingly, the NRC staff concludes alarm system coding conforms to the applicable NUREG-0700 guidance.

- NUREG-0700, Section 4.2.7, contains criteria associated with the organization of alarms. The intent of the criteria is to ensure that the alarm displays have a logical arrangement that facilitates the operator's ability to recognize the alarms.

  Evaluation: The LDP and alarm VDU share the same strategy for grouping alarm information. Alarm information is listed in one of the following four categories: Primary systems outside the containment, Reactor/Nuclear Steam Supply systems in the containment, Secondary systems and electrical systems. Within this structure, the alarm VDU information is then organized by priority in a time sequenced list. Unacknowledged alarms are recognizable within their priority group by a blinking alarm message field. The LDP and the operational VDU both contain alarm information within system mimic diagrams where the alarm information is captured via color coding as part of the indication or component symbol. For example, a pump that has stopped and should be running would be indicated in red. The "first out" alarm grouping is available at the top of both the LDP and the alarm VDU. The LDP provides additional groupings such as the critical safety function check and the "OK Monitor." These latter groupings are combined with diagnostics that limit the information on the LDP to the results of the diagnostic and thus provide the operator with deviations from the expected configuration for the existing plant condition or confirmation that the configuration is appropriate. From both the observation of control room displays and descriptions of these displays in the topical report and in the equipment specification documents, the NRC staff determined that the alarm information was presented consistently with logic that facilitated the operator's understanding of the condition. Accordingly, the NRC staff concludes that the alarm organization conforms to the applicable NUREG-0700 guidance.

- NUREG-0700, Section 4.3, contains criteria associated with the user-system interaction and controls. The user-system interaction addresses control functions needed by the operators and the controls addresses how the functions are accomplished by the HSIs provided.

  Evaluation: The US-Basic HSI design uses the typical functions used in the alarm systems in the current operating plants, which are: silence, acknowledge, and reset. These functions are accomplished at the alarm VDU via dedicated function keys. The operator acknowledges a new alarm by touching (or clicking) the blinking new alarm display area, which then stops the blinking and silences the audible alarm.

  The acknowledge button will only affect the alarms that are visible to the operator. If there are multiple alarm pages, each page must be acknowledged separately.

An associated alarm group button in the bottom function bar blinks until all priority 1 (alarm) and priority 2 (caution) alarms are acknowledged thus alerting the operator to alarms on pages that are not displayed. When alarm conditions return to normal, the alarm is displayed as cleared on a dedicated display panel accessed via a function button. Cleared alarms are identified by low speed blinking and white color indications. Cleared alarms are manually reset by operator acknowledgement. In addition to acknowledging and resetting, there is an alarm sound stopping function. This function stops the sound associated with existing new alarms. The blinking will remain so the unacknowledged alarms are identifiable. The alarm sound is stopped using an alarm sound stop button on the alarm VDU. The NRC staff concludes that there is a clear, unambiguous display of each alarm state. Coding is used effectively to communicate the display state and the function buttons provide an easy control of the alarm conditions. Accordingly, the NRC staff concludes that the alarm use-system interface and controls conform to the applicable NUREG-0700 guidance.

- NUREG-0700, Section 4.4, contains criteria associated with the Reliability, Test, Maintenance, and Failure Indication Features. This section was not specifically assessed since the alarm system is now just a component of the MELTAC Plant Control and Monitoring System which provides for these functions.

- NUREG-0700, Section 4.5, contains criteria associated with the interface between the alarm system and Alarm Response Procedures. The content of the alarm response procedures themselves are evaluated as part of the procedure operating program. Consistency between the alarm system terminology and the alarm procedures is verified later in plant specific applications that implement the HFE design process described in NUREG-0711.

  Evaluation: The US-Basic HSI design provides for direct access to the associated alarm response procedure by touching (or clicking) the alarm message area. Depending on their position, function buttons at the bottom of the alarm VDU display the alarm response procedure on either the operational VDU or the operating procedure VDU. Accordingly, the NRC staff concludes that the HSI with alarm response procedures is simple and efficient and conforms to the applicable NUREG-0700 guidance.

- NUREG-0700, Section 4.5, contains criteria associated with the integration of controls and displays. These criteria ensure the alarm system is in close proximity to the operator who will be responding and to the operating systems the operator will be using.

  Evaluation: The US-Basic HSI design places five VDU screens (alarm VDU, operating procedure VDU, and three operational VDUs) directly in front of each operator. As described above, the alarm response procedures can be called up on any of the VDU screens except the alarm VDU itself. Controls are available on any of the operational VDUs. The LDP is directly ahead of the operators.

  All screens are readily visible to the operator (within the 60 degree minimum arc) facilitating his ability to integrate available information with necessary actions.

Accordingly, the NRC staff concludes that the alarm system information is satisfactorily integrated with system controls and both indications and controls are readily available to the operator.

Audit of HFE design related documents

Some of the NUREG-0700 alarm system related criteria are of a detailed technical nature. They are not observable using the alarm system displays and are typically captured in the applicant's HSI style guide or in equipment specification documents. The NRC staff conducted an audit of these documents on May 26, 2010, and July 12, 2010, to verify that a sample of the applicable NUREG guidance is captured in controlled documents.

During the audit, the MHI staff used the following procedures to demonstrate where and to illustrate how the NUREG-0700 criteria selected by the NRC staff were addressed:

- Alarm system high level functions as outlined in NUREG-0700, Section 4.1.1 were addressed in the alarm system basic specification (NO-EK16015) and the I&C system Basic Requirements (NO-EK10001).

- Alarm processing as outlined in NUREG-0700, Section 4.1.2, were addressed in the alarm system basic specification (NO-EK16015)

The NRC staff found direct correspondence between the NUREG criterion evaluated and the design procedures. Additionally, specific design guidance had been substituted for the generic guidelines in the NUREG as one would expect in a completed design.

The NRC staff concludes that the general design of the alarm system satisfactorily conforms to the regulatory guidance for display design and alarm system functionality. The design provides reasonable assurance that the operating crew will be able to respond efficiently to alarm conditions.

3.3.2.4 Soft Control System

In Topical Report MUAP-07007, Section 4.5.2, the applicant provides a description of the soft control system embedded in the operational VDU. The basic function of the soft control system is to provide the operators with control interfaces that are mediated by software rather than by direct physical connections.

In this section, the NRC staff provides an evaluation of the soft control system HFE design as compared to applicable guidance in NUREG -0700, Section 7.

- NUREG-0700, Section 7.1, provides general guidance for soft controls. Only one criterion is applicable. It states that if a soft control can be accessed from more than one location in the HSI, protective measures should ensure its coordinated use among multiple users.

  Evaluation: Besides the division of responsibilities established by watch station assignments, coordination problems are minimized by limiting access to a soft control to the operator who has selected that control. The other control room operational VDUs identify this operator and display any actions he is directing.

- NUREG-0700, Section 7.2, contains criteria associated with information displays. This includes quick recognition and access to specific controls, coordination of process displays with soft controls, and design and use of input devices. Section 7.3, contains criteria associated with the use-system interface. Interactions with soft controls include selecting a plant variable or component to be controlled, providing the control input, and monitoring the system's response.

  Evaluation: System soft controls are accessed via the second level information displays on the operational or safety VDUs. The operational VDU uses system mimics and access to soft controls is embedded in these mimics. All soft operation areas on a screen appear as convex buttons, allowing the operators to distinguish operable components from non-operable components. Soft operation areas appear concave when depressed, thereby providing local feedback indicating touch or click input acceptance. The mimic labeling clearly identifies which component is being selected for operation and the same labeling is used on the soft control pop-up. On/Off switches, when selected, pop up on the second level system mimic display. There is only one switch popup on the screen at any one time in order to avoid erroneous operation. The default popped up position is consistent (right-lower side) and if the related information is hidden by the popup window, the default popup position is automatically set in the other corner of the screen. The popup window can be moved by the operator if relevant information is still hidden. In general, controllers and mode selectors are only available in fixed positions on a Controller screen (level three) that displays trend graphs and related parameters required to monitor the effectiveness of the control action. Thus process information is maintained in close proximity to the soft control making it efficient and simple for the operator to verify that the control actions have had the desired effects on plant systems and processes.

  The safety VDU uses a component listing to access soft switches and controls. Again, labeling is consistent between the component listing and the controller. The configuration of soft switches and controls are configured and operated the same as those on the operational VDU.

  Labeling is consistent across all controls with the noun name and alpha-numeric identifier at the top of the control. The switch noun name field serves as a switch software cover (an HSI interlock function) which requires double action for executing the operation in order to avoid erroneous manipulation. Whenever the soft switch pops up, it is inoperable until the cover is unlocked by touching or clicking on the switch name area. Controls also contain an icon providing status information (i.e., open, closed, tagged) as well as a physical representation of the component being operated. These elements work together to minimize the potential of selecting and using the wrong control.

  Figures 2 and 3 of a typical soft switch and a soft controller are provided below to help illustrate the HFE design that has been incorporated in each.

  Abbreviations used are: Manual Value (MV), Process Value (PV), Setpoint Value (SV), Deviation Value (DV), and Lift Value (LV)

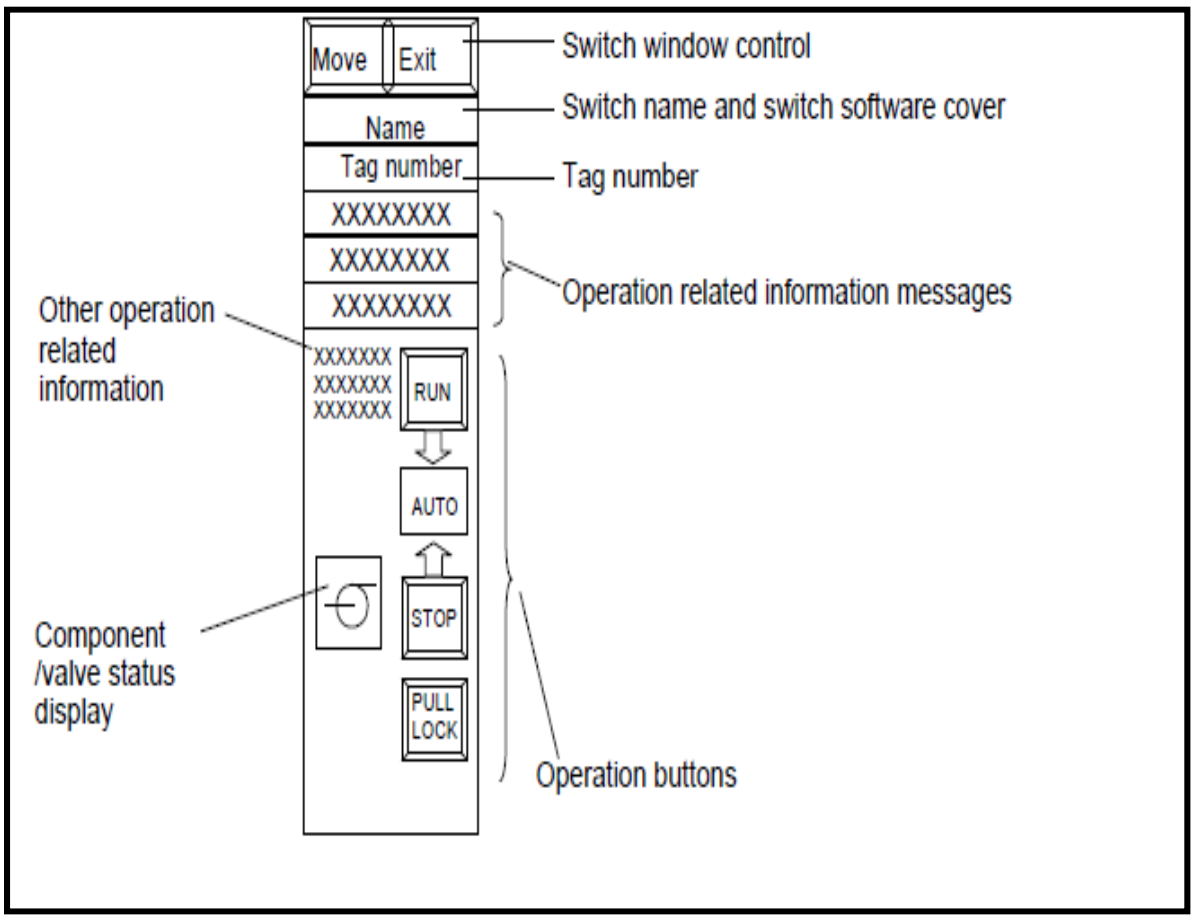

Figure 2: SOFT SWITCH

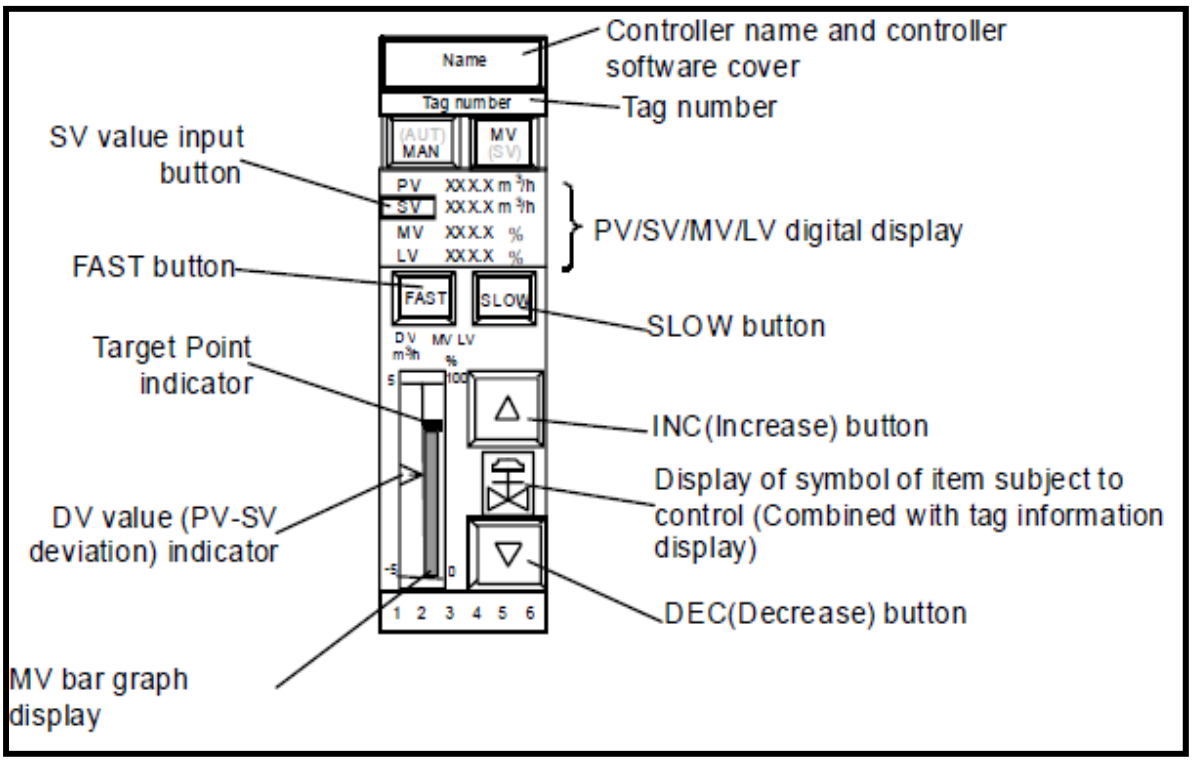

Figure 3: SOFT CONTROLLER

Soft control input is made by way of discrete-adjustment interfaces usually in the form of a button (i.e., start/stop, open close for a soft switch an increase/decrease buttons for controller settings). Discrete verses continuous-adjustment interfaces are preferred because the settings can be established by fairly gross movements. For controllers, setpoints can also be input using a numeric keypad function. Immediate feedback on the control activity is provided via the component status icons and in the case of controllers the bar graph display of target, process and deviation values. Since controllers provide continuous control functions they can be difficult to use due to digital system processing delay. To avoid the stress, confusion, and overshoot often caused by typical manual demand feedback indication delay, the soft control system accepts the demand signal, displays the target point in the manual value bar and sends the target values to the controller. A discrepancy between the demanded value and the value in the controller is easily seen by the operator.

The NRC staff concludes that the general design of the soft control system conforms to the regulatory guidance for display design and user-system interactions. The design provides reasonable assurance that the operating crew will be able to implement control actions in a timely manner.

3.3.2.5 Computer based procedures

The NRC staff's use of two types of guidance in the evaluation of CBP systems: procedure guidance and HSI guidance. Procedure guidance addresses the human factors aspects of procedure design and is intended to ensure that procedures are technically correct, usable, and applying consistent formatting conventions. This guidance is used as part of the SRP, Chapter 13 reviews and subsequent operating program inspections. The second type, HSI guidance, covers the design characteristics of the interface used to display the procedures. This guidance is used in the following evaluation and emphasizes HSI characteristics specific to implementing procedures in computerized form, such as features that help users manage concurrent procedures or monitor continuously applicable steps in an ongoing operation.

Evaluation using DI&C-ISG-05 (ML072540140) CBP system review criteria:

Criterion 1: A CBP system that displays operating procedures should be designed as an integral part of the MCR.

Evaluation: In the Topical Report MUAP-07007, Section 4.8, the applicant states the CBP system is designed as an integral part of the Basic HSI System for the MCR.

Criterion 2: The procedure user (e.g., operators) should always be in control of the procedure system. That is, the system should accomplish a procedure step, including automated steps, only at the direction of the user. The CBP system should be designed to provide the user with sufficient information to know they are in control.

Evaluation: In the Topical Report MUAP-07007, Section 4.8, the applicant states the CBP system ensures the procedure user (e.g., operators) is always in control of the procedure system, since bookmarks can be entered only by the user and only the user can initiate page or procedure selection.

Other aspects of Criteria 2 are not applicable to the Basic HSI System, because there is no control or information automation in the CBP system.

Criterion 3: The CBP system always present the most recently approved and issued version of a procedure.

Evaluation: In the Topical Report MUAP-07007, Section 4.8, the applicant states that configuration controls within the design and the procedure modification process ensure the CBP system always presents the most recently approved and issued version of a procedure.

Criterion 4: Measures should be taken to ensure that the CBP system will display the selected procedure. Measures should be taken to inform the operator, if the selected procedure is not or cannot be displayed.

Evaluation: In the Topical Report MUAP-07007, Section 4.8, the applicant states that V&V activities ensure that the CBP system always displays the selected procedure. Failure to display a procedure is easily recognized (procedure not indexed, procedure won't display on the VDU, software won't process status updates) and prompts the operator to utilize backup HSI. Procedure titles are available to verify that the operator has selected the procedure he desired.

Criterion 5: The design of a CBP system should allow the operator to easily transition from one procedure to another procedure, at any time.

Evaluation: In the Topical Report MUAP-07007, Section 4.8, the applicant states the CBP system allows the operator to easily transition from one procedure to another procedure, at any time through the use of multiple procedure VDUs and multiple procedure windows within each VDU.

Criteria 6-7: Address the use of plant data incorporate in the CBP system. These criteria are not applicable because there is no control or information automation in the CBP system.

Criteria 8-13: Address the use of automated procedures. These criteria are not applicable because there is no control or information automation in the CBP system.

Criteria 14-19: Address the use of soft controls integrated within the CBP system. These criteria are not applicable because there is no control or information automation in the CBP system.

Criterion 20: When implementing a CBP system into a MCR via a modernization project, the HSI conventions should include plant-specific standards that are in place at the site where the CBP system will be implemented. Failure to understand local conventions can result in conflicting sets of mental models and lead to an operational error.

Plant specific design is addressed via the HFE process outlined in Section 5 of the Topical Report.

Criteria 21-24: Address HFE attributes of the procedures contained on the CBP system. These criteria are addressed as part licensing activities.

Criterion 25: Back-up procedures should be maintained to ensure the ability to perform all emergency operating procedures and any procedure needed for accident mitigation, safe shutdown, emergency response, severe accident management, or the performance of other critical manual actions identified in the plant Probabilistic Risk Assessment. The backup procedures can be either paper based or a safety-related, CBP system.

Evaluation: In the Topical Report MUAP-07007, Section 4.8, the applicant states that back-up paper procedures are maintained for continued operation under degraded HSI conditions (i.e., loss of non-safety VDUs), and accident mitigation and/or safe shutdown under degraded HSI conditions (i.e., loss of non-safety VDUs or common cause failure affecting all VDUs), and emergency response.

Criterion 26: Backup procedures should be available to those who need them in a manner and location that is timely for their use.

Evaluation: In the Topical Report MUAP-07007, Section 4.8, the applicant states that backup paper procedures are easily accessible in the MCR. Paper procedures are used under all conditions at the remote shutdown room, technical support center and emergency operating facility; these procedures are easily accessible in these locations.

Criterion 27: Backup procedure systems should be subject to the same procedural controls as the primary CBP system.

Evaluation: In the Topical Report MUAP-07007, Section 4.8, the applicant states the CBPs and back-up paper procedures are generated from the same original computer files. All are under the same configuration controls.

Criterion 28: A means should be provided to ensure that operators can quickly, easily and effectively transition to backup procedures when necessary.

Evaluation: In the Topical Report MUAP-07007, Section 4.8, the applicant states the ability for operators to quickly, easily and effectively transition to backup procedures is confirmed through formal V&V activities, which include tests of the fully integrated HSI using dynamic high fidelity full scope simulation.

Criterion 29: Procedures presented on different media should be compatible, such that the operator can use them equally effectively.

Evaluation: In the Topical Report MUAP-07007, Section 4.8, the applicant states that, with the exception of bookmarks and navigational controls (e.g., hyperlinks), CBPs looks identical to back-up paper procedures, such that the operator can use them equally effectively.

Criterion 30: The content of the back-up procedure should be the same as the content of the primary procedure.

Evaluation: In the Topical Report MUAP-07007, Section 4.8, the applicant states that CBPs and back-up paper procedures are generated from the same source file, to ensure the contents are the same.

The NRC staff concludes that the general design of the CBP interface satisfactorily conforms to the regulatory guidance for display design and the system-user interface. The design provides reasonable assurance that the operating crew will be able to efficiently use the CBPs while maintaining back-up procedures if the CBPs are not available.

3.4 Evaluation of Topical Report, Section 5, HFE Design Process

MUAP-07007, Section 5, describes a general HFE design process. The process includes all elements described in NUREG-0711. However, the process has been described at the programmatic versus the implementation plan level, using the terminology in NUREG-0711.

In recognition of the general nature of the HFE design process description, the applicant makes the following statement in MUAP -07007, Section 5.0:

> The plant licensing documentation for each project provides an individual HFE program plan which can accommodate each project integrating some citation of the general portion of a HFE program plan in the topical report and specific information considering each project condition. Chapter 18 of the US-APWR DCD exemplifies a plant specific program plan, which fulfills the requirement for "plant licensing documentation".

For applicant activities that require a staff review and a Safety Evaluation Report (e.g., a Design Certification application), a programmatic level HFE submittal does not provide the NRC staff sufficient detail to develop the safety case needed for a Safety Evaluation Report. The NRC staff finds that to be the case for this Topical Report. The general HFE design process described in MUAP-07007, Section 5, while an acceptable starting point because of its similarity to NUREG-0711, does not contain sufficient detail on how the NUREG criteria are being implemented. This greater level of detail (e.g., corresponding to an implementation plan or a completed activity) is needed for the staff to develop the safety case. Therefore the NRC staff has not included the general HFE design process described in MUAP-07007, Section 5 in this safety evaluation.

The HSI configuration described in MUAP-07007, Section 4 is not a complete design until the inventory of controls, displays, and alarms is incorporated within it. The inventory is developed in accordance with the direction provided in the plant specific HFE program plan referenced in the quotation above. The plant specific HFE program plan contains the detailed implementation guidance the NRC staff uses to develop the safety case. Therefore, the NRC staff has established the following action item as an additional constraint for applicants using Topical Report MUAP-07007 and this safety evaluation.

- Action Item: An applicant's plant specific HFE design process shall be described at a level of detail commensurate with an implementation plan level submittal as described in NUREG-0711. The plant specific HFE design process should clearly identify whether the topical report is being credited. If credited, the following portions of the NUREG-0711 HFE program do not need to be repeated as they are specifically addressed within this safety evaluation of MUAP-07007:

    - Operating Experience Review for generic human performance issues and US-Basic HSI system

    - Functional allocation associated with the US-Basic HSI system

- Functional requirement specification for the US-Basic HSI system
- HSI concept design
- HSI detailed design (style guide) and integration associated with the US-Basic HSI system
- HSI tests, evaluations, trade off studies, and performance based tests used to develop the US-Basic HSI system
- Design documentation associated with the US-Basic HSI system
- Design verification associated with the US-Basic HSI system

4.0 FINDINGS AND CONCLUSIONS

The applicant has separated the Control Room HFE design into two parts. The first reflects the basic HSIs adopted from predecessor plants and enabled by digital I&C technology. The HSIs described in the topical report and referred to as the US-Basic HSI design, represent a generic, basic design platform whose structure can accept the specific design input required by a plant-specific application (the second part of the Control Room design). The NRC staff finds this to be an acceptable approach because:

- The HFE attributes included in the US-Basic HSI System conform to regulatory guidance in NUREG-0700.

- The applicant's controlled design documents contain guidance consistent with the regulatory guidance in NUREG-0700. This demonstrates that HFE attributes not specifically addressed in the topical report or viewable as part of the design have been addressed.

The applicant has provided a programmatic level description explaining how the US-Basic HSI design will be further developed into a plant specific application. In summary, the topical report requires plant specific implementation plans describing execution of the NUREG-0711 program elements. These plant specific plans are exemplified by the HFE program implementation plans for the US-APWR, which are currently under NRC review. The NRC staff finds the approach acceptable because it conforms to the process described in NUREG-0711.

The NRC staff had the opportunity to observe the MHI simulator which utilizes most of the US-Basic HSI system. These observations included MHI personnel operating the simulator during design basis event scenarios, qualified US operators doing the same, as well as a detailed explanation of the VDU and LDP displays and the navigation associated with them from the MHI staff. While more qualitative, the NRC staff noted that the US operators were able to quickly understand and apply the interface requirements. The NRC staff's observations reinforced the conclusions outlined in this SE.

Therefore, the NRC staff concludes that the US Basic HSI design is an acceptable starting point for the US-APWR design or other plant specific HFE design with the limitations stated in Section 5 below.

5.0 PLANT SPECIFIC HFE DESIGN (e.g. US-APWR DC APPLICATION) ACTION ITEMS

As a result of the NRC staff's review, the actions in Table 5-1 shall be performed when requesting NRC approval for using the HSI design described in topical report MUAP-07007:

Table 5-1 Action Items

Number	SE Referenced Section	Description
5-1	3.2	The US-Basic HSI design is tightly coupled with MHI Instrumentation and Control (I&C) systems. For the US-APWR these systems are described in MUAP-07005-P, "Safety System Digital Platform-MELTAC,", and MUAP-07004-P, "Safety I&C System Description and Design Process," which are currently under NRC review for the US-APWR design. Application of the US-Basic HSI design described in Topical Report MUAP-07007 to other plants (including the US-APWR) requires NRC approval of the MHI I&C design for those plants.
5-2	3.4	An applicant's plant specific HFE design process shall be described at a level of detail commensurate with an implementation plan level submittal as described in NUREG-0711. The plant specific HFE design process should clearly identify that the topical report is being credited. When credited, the following portions of the NUREG-0711 HFE program do not need to be repeated as they are specifically addressed within this safety evaluation: • Operating Experience Review for generic human performance issues and US-Basic HSI system • Functional allocation associated with the US-Basic HSI system • Functional requirement specification for the US-Basic HSI system • HSI concept design • HSI detailed design (style guide) and integration associated with the US-Basic HSI system • HSI tests, evaluations, trade off studies, and performance based tests used to develop the US-Basic HSI system • Design documentation associated with the US-Basic HSI system • Design verification associated with the US-Basic HSI system

6.0 REFERENCES

6.1-1 Topical Report MUAP-07007-P, "HSI System Description and HFE Process," Revision 5, Mitsubishi Heavy Industries, Ltd., dated November 2011 (ML11335A068).

6.1-2 Technical Report MUAP-07005-P, "Safety System Digital Platform-MELTAC," Revision 8, Mitsubishi Heavy Industries, Ltd., dated July 2011 (ML11223A276).

6.1-3 Technical Report MUAP-07004-P, "Safety I&C System Description and Design Process," Revision 7, Mitsubishi Heavy Industries, Ltd., dated May 2011 (ML11160A139).

6.1-4 MUAP-DC018, "Design Certification Document".

6.1-5 Technical Report MUAP-09019-P, "US-APWR HSI Design," Revision 1, Mitsubishi Heavy Industries, Ltd., dated December 2011 (ML12041A153).

6.1-6 Technical Report MUAP-08014-P, "US-APWR Human System Interface Verification and Validation, Phase 1a," Revision 1, Mitsubishi Heavy Industries, Ltd, dated May 2011 (ML11160A204).

6.1-7 NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, Chapter 18 – Human Factors Engineering," Revision 2, U.S. Nuclear Regulatory Commission, Washington, DC, dated March 2007 (ML070670253).

6.1-8 NUREG-0711, "Human Factors Engineering Program Review Model," Revision 2, U.S. Nuclear Regulatory Commission, Washington, D.C, dated February 2004 (ML040770540).

6.1-9 NUREG-0700, "Human-System Interface Design Review Guidelines", U.S. Nuclear Regulatory Commission, Washington, D.C., dated May 2002.

6.1-10 Interim Staff Guidance DI&C-ISG-05, "Highly-Integrated Control Rooms - Human Factors Issues (HICRC)," Revision 1, U.S. Nuclear Regulatory Commission, Washington, DC, dated November 3, 2008.

6.1-11 10 CFR, Part 50, "Domestic Licensing of Production and Utilization Facilities."

6.1-12 10 CFR, Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants."

6.1-13 UAP-HF-08104, Y. Ogata to J.A. Ciocco, "MHI's Responses to Request for Additional Information on Topical Report, MUAP-07007-P(R0)," dated July 17, 2009 (ML082030592).

6.1-14 UAP-HF-09288, Y. Ogata to J.A. Ciocco, "MHI's Responses to 2nd round MHI US-APWR Topical Report, MUAP-07007," dated June 30, 2009 (ML091830350).

6.1-15 UAP-HF-10094, Y. Ogata to J.A. Ciocco, "MHI's responses to 3rd round MHI US-APWR Topical Report, MUAP-07007," dated April 2, 2010 (ML100960248)

6.1-16 UAP-HF-10144, Y. Ogata to J.A Ciocco, "MHI's Responses to 4th round MHI US-APWR Topical Report, MUAP-07007," dated May 25th, 2009 (ML101480045).

7.0 LIST OF ACRONYMS

ADAMS	Agency-wide Document Access and Management Systems
APWR	Advanced Pressurized-Water Reactor
CBP	Computer Based Procedure
COLP	Operator Licensing and Human Performance Branch
CFR	*Code of Federal Regulations*
DAS	Diverse Actuation System
DCD	Design Certification Document
DV	deviation value
ECCS	Emergency Core Cooling Systems
EOP	emergency operating procedure
ESF	engineering safety features
ESFAS	engineered safety feature actuation system
HED	human error discrepancy
HICRC	Highly-Integrated Control Rooms-Communications Issue
HFE	human factors engineering
HSI	human systems interface
HSIS	Human Systems Interface System
I&C	instrumentation and control
IEEE	Institute of Electrical and Electronics Engineers
ISG	interim staff guidance
LDP	large display panel
LOCA	Loss of Coolant Accident
LV	Lift Value
MCR	main control room
MELTAC	Mitsubishi Electric Total Advanced Controller
MHI	Mitsubishi Heavy Industries
MV	manual value
NRC	U.S. Nuclear Regulatory Commission
OER	Operating Experience Review
PCMS	Plant Control and Monitoring System
PSMS	Protection and Safety Monitoring System
PV	process value
QA	quality assurance
RAI	request for additional information
RPS	reactor protection system
RTS	Reactor Trip System
SAR	Safety Analysis Report
SDCV	Spatially dedicated, continuously visible
SE	Safety Evaluation
SECY	Secretary of the Commission, Office of the (NRC)
SER	safety evaluation report
SGTR	Steam Generator Tube Rupture
SPDS	Safety Parameter Display System
SRP	Standard Review Plan
SV	setpoint value
US-APWR	United States - Advanced Pressurized Water Reactor
VDU	video display unit