THE DEVELOPMENT OF KNGR CONTROL ROOM MAN–MACHINE INTERFACE DESIGN

SUNG-JAE CHO
Center for Advanced Reactor Design

YEONG-CHEOL SHIN
Nuclear I&C Group,
Nuclear Power Research Laboratory,
Korea Electric Power Institute,
Korea Electric Power Corporation

Taejon, Republic of Korea

Abstract

KNGR MMI design has been developed for the last 7 years as a part of Korea Next Generation Reactor (KNGR) design development. The KNGR control room has the common features of advanced control room such as large display panel, redundant compact workstations, soft control, and computerized procedure system. A conventional type safety console is provided as a backup when operation at the workstations is impossible. The strong points of an advanced control room are based on the powerful information processing and flexible graphic presentation capability of computer technology. On the other hand, workstation based design has a weak point that the amount of information to be presented in one VDU is limited. This can cause navigational overload and inconsistent interfaces and provide chances for performance errors/failures, if not designed carefully. From this background, the regulators require licensees to follow strict top-down human factor engineering design process. Analysis of operating experiences and iterative evaluations are used to address the potential problems of the KNGR advanced control room MMI design. But, further study is necessary in design area like CPS design, where experiences or design guidance is insufficient. Further study topics for KNGR advanced control room MMI design development are discussed briefly in this paper.

1. DESIGN PROCESS OF THE KNGR ADVANCED CONTROL ROOM

A structured Man– machine Interface (MMI) design process is being coordinated throughout the KNGR design program, which is to develop a standard Advanced Light Water Reactor (ALWR) design for commercial operation after the year 2010 in Korea. The program is organized in three phases according to each developmental state. Major activities of the Phase I, which was completed in 1994, were to develop the plant design requirements and concepts. The concept of MMI design had been developed with other plant design concepts through the Phase I program. In Phase II, completed in February 1999, basic design activities have resulted in a MMI basic design and documentation supporting submittal of a Standard Safety Analysis Report (SSAR) for licensing. The current Phase III stage is planned to be a three year program creating detailed design information and performing additional design evaluations. This phase is scheduled to be followed by a construction project for the first KNGR units.

1.1. Creation of the control room design concept

The goal of the conceptual design phase was to establish a point of departure for evaluating and refining the MMI design through a formal human factors-based design process. To that end, basic features, called MMI resources, and their characteristics were identified. In addition, the control facilities including an initial Main Control Room (MCR) layout were created. The preliminary conceptual designs evolved from the current Korea Standard Nuclear Plant (KSNP) designs, with insight from the ABB-CE advanced control room(Nuplex 80+™) design and Design Certification process. Driving forces including the

EPRI ALWR Utility Requirements Document (URD) requirements, an OECD Halden Reactor Project study, and a KEPRI advanced control room survey transitioned the design towards a full-function compact workstation MCR.

In mid 1997, a MMI Joint Design Development team was convened at the initiation of Phase II. An experienced team of control complex designers and I&C engineers was assembled, complemented by experienced PWR operators. The mission of the team was to systematically assess the preliminary conceptual design features to determine those to be carried forward in the basic design.

The entire team and technical managers of KNGR design organizations formally reviewed the results and recommendations for each feature in periodic design review meetings. The resulting designs were integrated into a complete conceptual design, and were optimized where specific fundamental concerns were identified. The detailed evaluation results were documented in evaluation reports for each feature [1][4]. The ability of the design to address integrated design considerations, such as common mode failure of software based systems and continued operation with MMI equipment failures, was also assessed.

1.2. Development of a basic MMI design and documentation

The KNGR MMI design effort were made until early 1999 with design details and formal documentation being developed for each MMI feature and control facility. Human Factor Engineering (HFE) program plan [2] and other implementation plans for the HFE program element were established and executed to direct the HFE activities so that human centered goal can be met. Dynamic rapid prototypes of all MMI resources were developed for initial evaluation. Alarms, displays and controls were implemented for a selected set of plant systems and incorporated into a dynamic mockup. This part-scope control room workstation was driven by plant simulator models to allow operator-in-the-loop verification and validation testing. In parallel a set of human factors analyses supporting the design were performed.

A primary activity of Phase II was continued for the development and documentation of the MMI design. Early documentation of the design served three important functions; (1) to provide a concise design for mockup development, (2) to allow internal and external design review and (3) to support SSAR development and submittal.

Initially, an operation philosophy document was developed to establish a vision of how the KNGR would be operated. The operation philosophy provided staffing assumptions and operator functions in all modes of operation to allow a common perspective for MMI resource and system designers to proceed. A Human Factors Engineering Standards, Guidelines, and Bases (HFESGB) document was produced specifically for the KNGR MMI design. This program guidance document, based on an extensive set of accepted human factors sources [3], facilitates consistent application of the HFE principles by all design team members and organizations.

The focus of Phase II centered on the basic design development of the MMI resources and control facilities. MMI resource functional requirements and control facility system requirements systematically documented from a wide variety of sources. The conceptual MMI designs developed through the Phase I were refined to meet these requirements, as well as functional and task requirements obtained from the results of human factors analyses and the guidance of the KNGR HFESGB. The resulting designs were documented in design reports for MMI resources and system descriptions for control facilities.

The complete set of MMI design documentation has been captured in a document handling system that supports formal tracking of the review and comment process. Review of the design documents was performed by both MMI design team members and independent review organizations. The standard issues of the above KNGR documents have completed through the Phase II program.

1.3. Mockup developments and evaluations

A fundamental approach in the KNGR MMI basic design process is early development and use of prototypes and a dynamic mockup. Rapid prototypes were developed in parallel to MMI resource designs to facilitate interactive review and refinement. The rapid prototypes were used to evaluate design alternatives or confirm acceptability of design decisions, particularly for new and unique MMI resources.

A "deep slice" of the basic design process was conducted to create displays, controls and alarms for a small set of selected plant systems and computerized operating procedures for a specific event scenario. The designs were based on the KSNP systems and the results of a limited scope task analysis. The "deep slice" designs were used to create a dynamic mockup of one complete compact workstation. The mockup includes an alarm Video Display Unit (VDU) and three multi-function VDUs, three soft control devices with associated confirmation switches, and system level actuation switches. A complete Large Display Panel (LDP) is implemented in one-quarter scale using rear projection technology. The entire mockup is driven by KSNP full-scope simulator models.

Two principal evaluative activities conducted in Phase II were suitability verification and preliminary validation. Suitability verification is an iterative process to be continued throughout the MMI design. It addresses the issue of whether the form and arrangement of individual MMI resources support operator task accomplishment. This is accomplished by (1) using a top-down approach to assess usability of the mockup MMI resources for task performance and assess adherence to high-level human factors design principles, and (2) using a bottom-up approach to determine conformance of the mockup implementations to established HFE criteria in the HFESGB. The initial suitability verification effort was performed by human factors specialists and MMI designers, supplemented by licensed plant operators. The result was a number of formally documented findings that are providing feedback to designers early in the design process to avoid costly design changes.

Preliminary validation activities were also conducted on the mockup to allow an initial assessment of the integrated ensemble of MMI resources. For the assessment, two crews of licensed operators from a KSNP unit joined the design team for a while to conduct post-trip operations on the mockup for a hypothetical steam generator tube rupture event. The evaluations were performed for the cases of using the computerized operating procedure and paper procedure respectively. The specific topics including workload, task performance, crew errors, and situational awareness were also assessed.

1.4. The detailed design

Phase III of the KNGR MMI design will focus primarily on the application of the basic MMI design to a wider range of plant systems and on continued evaluation of the design. The detailed designs will be generated by cognizant engineers based on input from task analysis and plant systems requirements, and will be transmitted to I&C system designers for implementation and used for mockup expansion.

The continued evaluation of the MMI resources and control facilities will be performed as following:

- Continued suitability verification of individual MMI resources to maintain conformance to human factors guidance and task requirements as additional design details are developed and design changes are implemented on the mockup,
- Design validation as the mockup facility becomes more robust, to evaluate and demonstrate the integrated operational capability of the KNGR MMI and MCR during normal, abnormal and accident conditions,
- Demonstrations (and evaluation, if necessary) of KNGR MCR operations (1) with actual performance parameters, such as time responses, and (2) with postulated degraded MMI operating conditions including testing of proposed mitigation strategies, where required,

2. CONTROL ROOM AND MMI DESIGNS

Some of the most evident changes are in the KNGR Man–machine Interface Systems (MMIS), where state-of-the-art technologies are replacing conventional control room and the Instrumentation and Control (I&C) systems. The KNGR MMIS distinguishes itself from current designs by employing all digital I&C systems and data communications, and primarily video-based Man–machine Interfaces (MMI) which incorporate modern human factors principles. The MMI maintains well-proven KSNP features, such as critical function monitoring, while adding advanced design features. Advanced design features being incorporated include: (1) a compact workstation-type control room layout, (2) a large display panel, (3) computerized operating procedures, (4) soft controls, and (5) a reduced number of fixed location displays and alarms

The primary control and monitoring facilities for operators are full-function compact workstations, which provide unprecedented operational flexibility and integration. Each of three redundant workstations features paired sets of monitoring VDUs and soft control flat panels, allowing access to, and effect of, both safety and non-safety controls. Complementing these soft interface devices, computerized operating procedures reduce operator response time variability and operator error probabilities. This full complement of soft devices accommodates varied task requirements and operator preferences, and permits incremental MMI refinements with minimal impact throughout the plant design process and operating life. A Large Display Panel is located in the front of the control room. It provides fixed-location indication of high priority alarms, parameters and component status otherwise unavailable in the compact workstation environment. It also provides continuous display of critical safety function status as per regulatory requirements. A minimum set of fixed-position component controls and operator modules are located on a safety console, designed to complement the workstations during post-trip conditions. The control facilities support control room operator staff reductions, compared to conventional designs, while offering unprecedented expansion and reconfiguration potential. The control room is designed to explicitly meet the requirements of the Korean-URD. The control facilities feature the main control room, including its compact workstations, large display panel and safety console. Each of these will be briefly described in the succeeding sections. Other control facilities include a remote shutdown room and local control stations.

2.1. Main control room

The KNGR Main Control Room (MCR) layout is shown in Figure 1. The key features supporting the operating crew's ability to maintain efficient and safe plant operation include:

- Two identical, full-function workstations supporting direct plant control and monitoring by a Reactor Operator (RO) and a Turbine Operator (TO), respectively,
- A third identical workstation supporting normal monitoring and crew coordination functions of a Control Room Supervisor(CRS) and serving as a backup to the RO/TO workstations,
- A Large Display Panel (LDP) providing overall plant operational and safety assessment,
- A Safety Console providing control capability for all Class 1E, safety-related components for the plant safe shutdown even in the event of complete workstation failure.

Advantages of this control room layout include enhanced communication between operators, good visibility of the extended scope LDP, ease of accommodating design and job allocation changes, and convenient access and egress routes.

2.2. Large display panel

The Large Display Panel is a wall-mounted overview display including Safety Parameter Display System (SPDS) and Bypassed and Inoperable Status Indication. The fixed display section of the LDP provides continuous, parallel display of key alarm, component, system, and parameter information. This complements the workstations' MMI with a spatially dedicated graphical depiction of the plant. A variable display section allows operators to selectively display pertinent information to support crew coordination. The LDP reference design used on the dynamic mockup is shown in Figure 2.

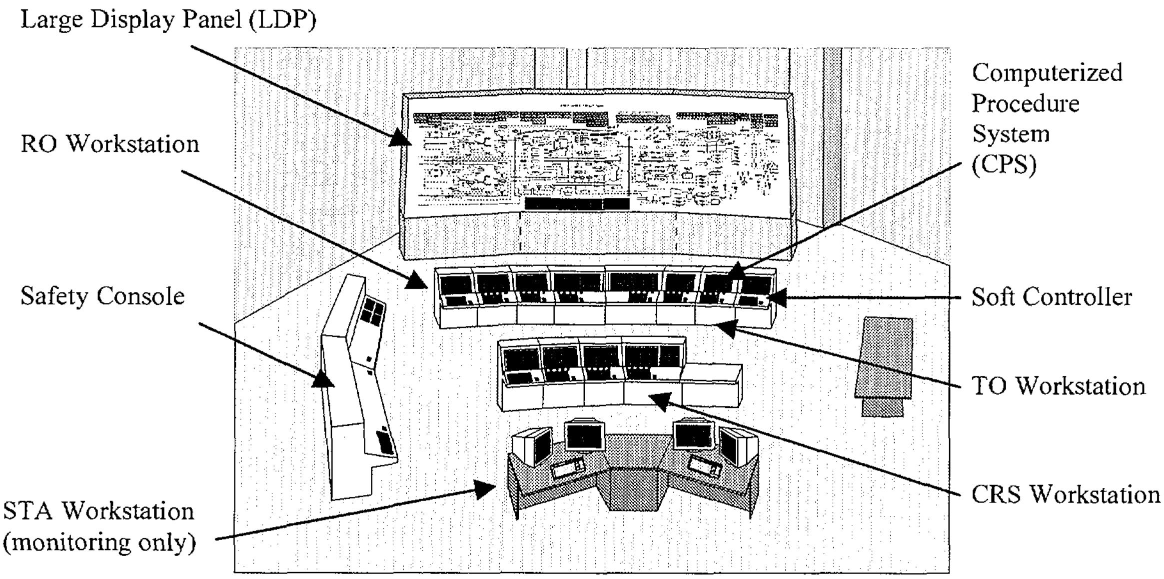

FIG. 1. Main control room layout.

2.3. Compact workstations

Each MCR workstation provides devices for access to all information and controls necessary for one person to monitor and control all processes associated with the plant operation and safety. This includes both safety and non-safety systems. The workstation design for Rector Operator (RO) and Turbine Operator (TO) is illustrated in Figure 3. Each workstation contains the following:

- One alarm VDU with trackball user interface,
- Three VDUs supporting process monitoring or electronic procedures with trackball user interface,
- Three flat panel displays used as soft controllers for process and component control; each working in conjunction with one VDU and using a touch sensitive user interface,
- Dedicated push-buttons for Manual Reactor Trip and ESF system actuation
- Laydown area for logs, drawings, backup paper procedures, etc.

The major advantages of the compact workstation approach are its (1) operational and design flexibility, (2) compactness and simplicity, (3) ability to cost effectively accommodate changes, and (4) provision of an enhanced integrated environment for CPS and operator aids.

2.4. Safety console

The control room includes a safety console providing Class 1E controls for all safety-related components, independent of the workstations. The safety console is intended to be used for surveillance testing during normal operations and to be staffed by an additional RO during post-trip operation. It provides all of the required safe shutdown capabilities, including mitigation of accidents, and helps address the common mode failure issue in the compact workstation design.

YGN 3&4 LARGE DISPLAY PANEL

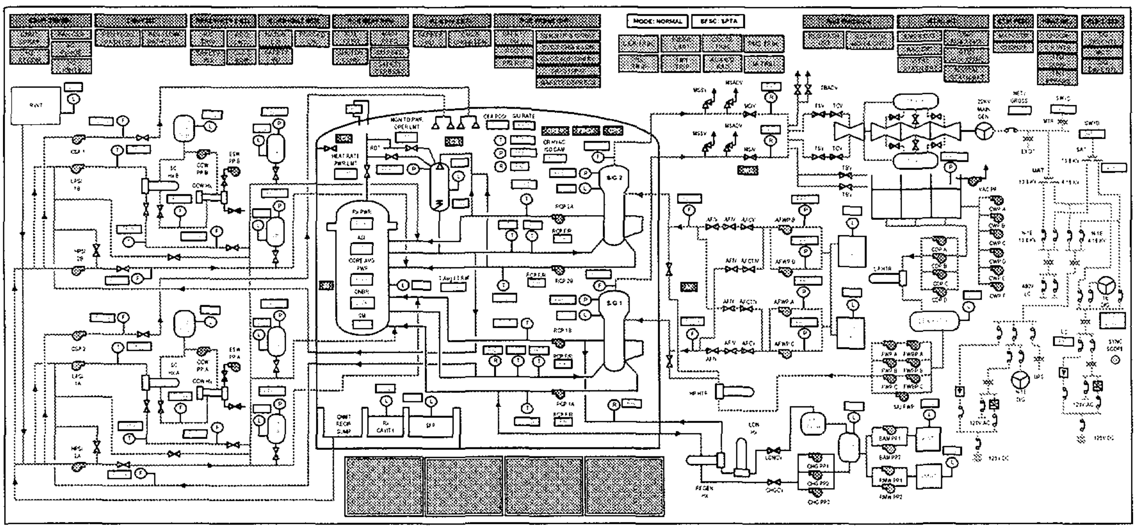

FIG. 2. Large display panel.

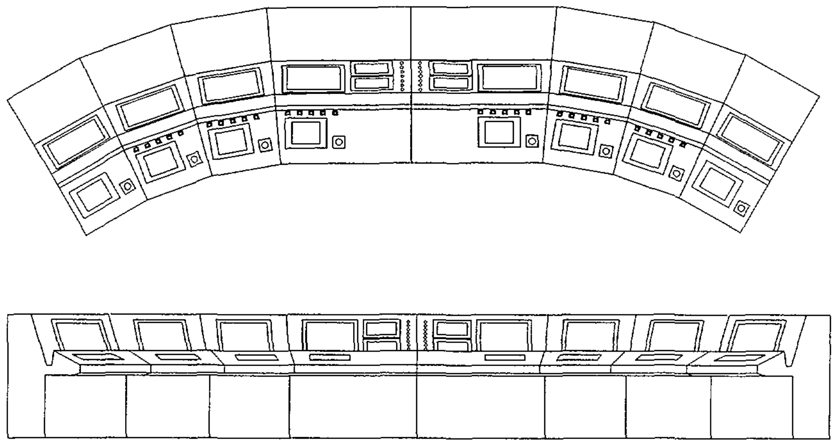

FIG. 3. Workstation design.

The MMI resources provide a standardized set of monitoring and control MMI designs that are designed to and evaluated by human factors principles. The MMI resources are used to implement the detailed MMI designs for all plant operator interfaces. Each of the primary MMI resources is described briefly below.

2.5. Workstation VDU displays

The MCR workstations allow simultaneous access to plant information through selectable displays on four VDUs per workstation. A wide variety of display formats include system mimics, major plant functions or conditions, technical data sheets, trends and graphical information, and application program access. All are designed to support specific operator functions. Multiple methods are provided for convenient access to the display set including navigational access through menus, direct access through format chaining from other displays (or alarms and procedures) and a dedicated mechanism such as function buttons or voice entry. A major function of the VDU displays is to provide a soft control link allowing the operator to quickly select a component or process control on the soft controllers directly from display pages.

2.6. Soft control

The KNGR program has adopted a "Soft Control" approach as the primary means to effect control actions. The "Soft Controls" utilize flat panel displays to emulate the physical switches and manual/auto stations that populate conventional plant control panels. Use of software-based control allows a standard interface device to assume the role of numerous physical devices. This has the advantage of allowing operator access to all plant controls from a single workstation, design flexibility and the ability to easily accommodate changes, and simplification of hardware procurement and maintenance. A set of divisional confirmation switches maintains divisional independence allowing safety and non-safety control to be effected from the same device.

2.7. Alarm system

The alarm system is designed to improve the annunciation process, by incorporating methodologies that:

- Reduce the total number of alarms that an operator must cope with
- Distinguish between true process deviations and sensor failures
- Minimize the occurrence of "nuisance" alarms
- Prioritize the relative importance of alarms so the operator can focus on the most critical alarm conditions first while deferring less critical alarm conditions
- Determine the impact of alarms on plant operations and distinguish these from lower level system alarms.

Highest priority alarms, such as those for critical safety functions, are presented in fixed locations on the LDP. All alarms are presented in list form on a dedicated workstation VDU as well as through relevant locations in the VDU display hierarchy.

2.8. Computerized procedure system (CPS)

The CPS is implemented as a passive design incapable of originating direct control action. The center section of a VDU screen shows a procedure overview in the form of a scrollable flowchart of all procedure steps. CPS allows assignment of procedural steps to specific operators (e.g., the RO and TO). An instruction window provides a general statement of the action(s) the operator should perform. An "action details" window provides the list of manual actions taken to perform the procedure step. To support decision-making the CPS provides real-time plant information or format chains to appropriate VDU displays. Direct access to the soft control MMI is afforded through format chaining as well. A "forcing function" approach keeps the operator in the evaluation loop, preventing the human from blindly following the computer for procedure execution.

Major advantages of the KNGR CPS include a significantly improved approach to continuously applicable procedural steps, direct access to information and controls for procedure execution, improved procedure integration in the compact workstation environment, and reduced error probabilities and response variability.

3. ISSUES OF KNGR CONTROL ROOM MMI DEVELOPMENT

3.1. Challenges in designing an advanced control room

Even though the computer technologies provide the high functionality for design flexibility to make the man machine interface more suitable for human being, they have several problems in application to nuclear power plant operation. The computer systems are usually highly centralized performing several functions in one processor. This is very undesirable in view of system reliability because it is prone to simultaneous failure of multiple functions. Conventional control rooms are better in this sense because they are highly distributed. Another problem with the computer system is that its software verification is very difficult because of the complexity of the software itself.

The information processing provides opportunities for relieving operators from complex data handling that are not suitable for operators in complicated operational situations. The computer graphic technologies allow presentation of operational information in a form that facilitates operators' intuitive use of information without big cost. However this inherent computer capability for flexibility and automation brings the complexity of MMI and provides chances for performance errors/failures by operation staff in nuclear power plants if not designed carefully. In an advanced control room, many resources are typically used to support the operator task. Therefore, the lack of integration of multiple MMI resources can create performance problems. The limited amounts of information that can be presented in one VDU at a time make the advanced control room design difficult. This is because of navigational overload problems and inconsistent interface representing the same part of the plant. From this background, the regulators require licensees to follow strict top-down HFE design process.

3.2. Human factor engineering process

Systematic application of HFE is the key element for the successful development of safe and efficient control room and man machine interface[3]. For the successful completion of the complex KNGR MMI design process, a multidisciplinary team of human factor specialists, computer specialists, system engineers, and plant operators work together as a team from the stage of conceptual design through the validation process. Starting from the KNGR MMI design concept, the design has been going and will go through several iterations of analysis, design and evaluation. The system hazard analyses such as operator experience review, analysis of plant safety functions, analysis of critical operator actions from PRA, are performed to identify high risk tasks and critical operator errors against plant safety. The results are addressed or used in the MMI design. For the systematic application of HFE principles, related principles are searched and adapted to KNGR MMI concept to become HFE standards and guidelines for MMI design. The usability of the MMI design will continuously improve as iterative evaluations and improvements are implemented until final validation of the MMI design. The acceptability of the design will be demonstrated not only by the final validation but also by the repeated evaluation and studies throughout the design process. In this process, high fidelity full scope simulators will be used to facilitate and accelerate the improvement. A group of plant operators has been and will be extensively involved to provide operating experiences to identify any unforeseen issues in the design. An independent multi-disciplinary team will review the design to reflect diverse input for the design and thereby to correct the design and remove any bias in the design.

3.3. Control room design against computer system failures

Defense in depth strategy is reflected in KNGR control room design. There is a safety console where operator can perform Emergency Operational Procedure (EOP) or safe shut down operation when the workstations are unavailable for operation. There are three redundant workstations in main control room. When one of the RO or TO workstation fails, CRS workstation is used by the RO or TO. When one of the Cathode Ray Tube (CRT) or Flat Panel Display (FPD) is not working, there are still three pairs of information display and soft control display whose operation can continue. In case of CPS failure, operators can use the paper procedure whose format is consistent with the computerized procedures. Thus, the KNGR control room is designed to be very robust to any computer failures.

3.4. Design against common mode failure(CMF) of software

Design and analyses were performed to resolve the CMF issue as per the NRC positions stated in SECY-93-087. It should be noted that the KNGR MMIS differs from other advanced MMIS designs in that the non-1E soft control MMIs provide control input signals both to the safety and the non-safety equipment. Since the soft control MMIs provide a common interface for both safty and non-safety system control inputs, it is necessary to evaluate the potential impact of a common mode failure of the software used in the soft control MMIs to ensure it does not compromise the basic CMF protection provided by the diverse safety and non-safety systems.

CMF of Safety System Software: An overall strategy has been developed for the KNGR MMIS and is to make sure that the occurrence of a CMF of safety system software can be safely mitigated. In other works, the KNGR MMIS with diverse non-safety controls and indications at the RO and TO workstations, and non-safety systems such as Alternate Protection System(APS) provide sufficient means to bring the plant to a safe shutdown condition, and that the capability is adequate for any of the Chapter 15 event initiators. One notable feature of the KNGR MMIS would be that control actions could be taken through the soft controls. No credit would be taken, however, for the safety analyses, except for the hard wired switches incorporated on the workstation panel to comply with the NRC SECY-93-087 Position 4, which requires, independently from safety system, system level controls for safety functions.

CMF of Workstation Soft Control: For the KNGR MMIS, careful consideration is made to evaluate how a failure of this non-1E qualified soft control is related to the software CMF issue. A criterion for the acceptance of the soft control is if the plant can be brought to a safe shutdown condition when a CMF of the soft control MMI occurs. For the KNGR design, the failure will have no impact on the automatic protection system actuation or manual safety control through Class 1E MMI. This will be achieved through the safety console capabilities which will be credited to address this failure. Since the soft control MMI provides input signals to the safety system, it must be demonstrated that the CMF failure in soft control MMI can not impact the operation of the safety systems.

Four Quadrant I&C Architecture: The KNGR I&C architecture maintains a four quadrant architecture for both monitoring and control. This architecture provides distinction between 1) safety and non-safety I&C systems and 2) monitoring and control systems as shown in Figures 4 and 5. The distinction between safety and non-safety systems is particularly important because it is the defining line for design diversity which provides a means to address the concern of common mode failure of digital I&C systems. The distinction between control and monitoring is also important to separate the processing intensive monitoring functions from the less processing intensive, yet more time critical, control functions. Safety control MMI is provided by Class IE, flat panel display operator modules and switches on the Safety Console for credited control capability of safety equipment. Non-safety control MMI is provided by soft control MMIs on the workstations, which use diverse technology from the operators modules. As shown in Figure 4, the soft control also allows a control of safety equipment. Figure 5 illustrates similar diversity between qualified non-safety monitoring systems and MMI. Qualified monitoring is provided by the Type 1 Qualified Indication and Alarm System (QIAS). Non-Safety monitoring is provided by the diverse Information Processing System (IPS). The qualified MMI is provided by seismically qualified FPDs and LDP. Non-safety MMI is provided by the workstation CRTs, which are diverse from the flat panel displays.

3.5. Communication independence of soft control MMI

With regard to the independence of safety system, IEEE 603-1991 states in section 5.6 that "redundant portions of a safety system provided for a safety function shall be independent... and that no credible failure on the safety side of an isolation device shall prevent any portion of the safety system from meeting its minimum performance requirement."

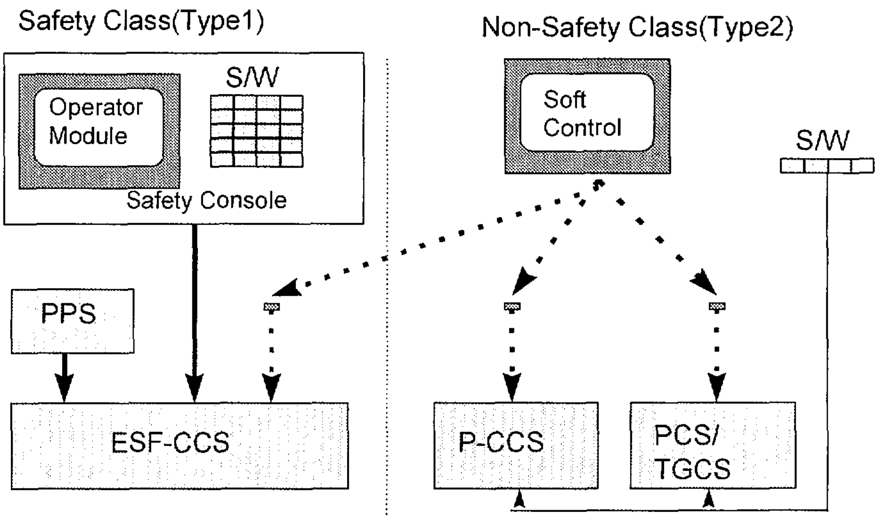

FIG. 4. The concept of control MMI diversity.

US NRC SRP provides guidance for the evaluation of conformance to IEEE 603 for computer based systems like the following: "If a digital computer system used in a safety system is connected to a digital computer used in a non-safety system, the review should confirm that a logical or software malfunction of the non-safety system cannot affect the functions of the safety system." With regard to the communication independence of computers that are part of the safety system, IEEE 7-4.3.2-1993 states that "No data communication between safety channels and between safety and non-safety systems shall inhibit the performance of the safety function."

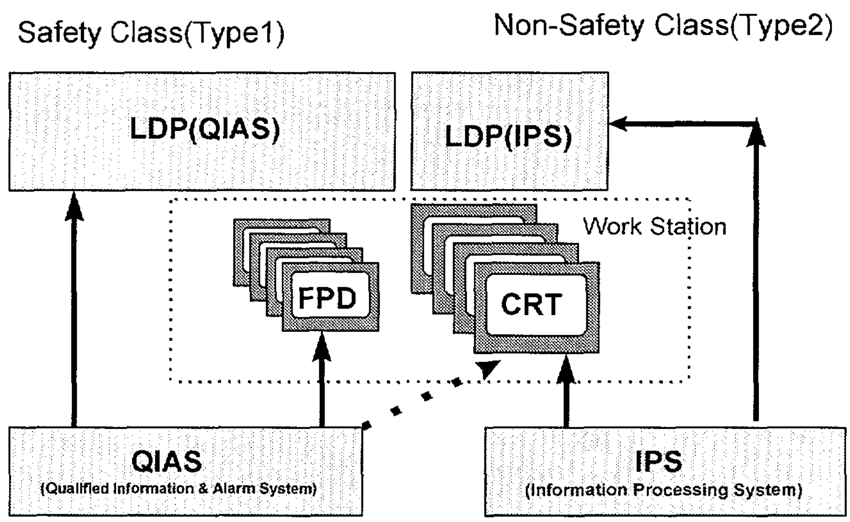

FIG. 5. The concept of monitoring MMI diversity.

In KNGR, the signal from a soft control MMI is connected to only one division of the Component Control System (CCS) at a time by using two design features. One is the divisional confirmation switches which allow control signals from a soft control MMI to take effect to the confirmed division only. The design approach is to select the control component via non-safety soft control MMI, then initiate the control action using a Class 1E actuation circuit confirm switch at each control station. The confirm switch is completely isolated from soft control MMI to ensure independence. The other feature is the use of a simple de-multiplexer which connects the communication lines between the soft control MMI to one division of CCS using an addressing signal from the soft control MMI. This is the second line of defense against soft control malfunction impacting more than one division. A simple non-1E de-multiplexing scheme that does not use any processor or memory is adopted to ensure the high reliability of the de-multiplexing function.

Non-safety Computer Function Overridden By Safety Function: In order to meet the basic independence requirement, the safety computer (ESF-CCS) must be able to override the non-safety computer (soft control MMI) when the safety system is performing its safety function. One of the design method to ensure this capability is a priority interlock. The priority interlock blocks any effect on ESF component control (system level) from the soft control MMI during safety function performance. ESFAS signals from the PPS override soft control signals at all times. The actuation signal from Class 1E ESF-CCS MMI (switches and operator modules) can also override the component actuation from soft control MMI. Control signals from the soft control MMI have the lowest priority. The operator can override the priority 2 interlock of ESFAS by using the soft control MMI or ESF-CCS MMI if the plant is in a safe state.

Communication Isolation Between Soft Control MMI and ESF-CCS: Buffering circuits in ESF-CCS division gateway are used to allow the handshaking with address checking between the soft control MMI and one division of ESF-CCS. This will assure the integrity of safety function by detecting and blocking the connection of soft control MMI to unintended division of ESF-CCS.

Operator Detection of Soft Control Malfunction: Prior to initiating the control action, it is expected that the operator would press the confirm switch for actuation after he checks the display of component selection which is not based on the selection signal generated from soft control, but based on the selection information fed back from the ESF-CCS. This enables the operator to detect any discrepancy between what he demanded at soft control MMI and what was actually received at the ESF-CCS.

3.6. Integration of SPDS and emergency operating procedure (EOP)

KNGR does not provide a stand-alone Safety Parameter Display System (SPDS), but the SPDS functions are integrated into the overall control room design. The violation of critical safety functions are annunciated through LDP tiles and CRT display to indicate the entry conditions to the proper optimal or functional EOP. The critical plant variables sufficient to provide information about critical safety functions are also provided on the LDP as an integral part of the fixed mimic displays. Plant function displays to assist the operator for the execution of EOPs in verifying and planning mitigation for violated critical functions are available in workstation CRT displays for RO, TO, CRS and all other operation staff, and personnel in TSC and EOF. Critical function and success path alarms are a meaningful framework to aid the operator in quickly identifying the significance of important alarm information. In KNGR, the Safety Function Status Checks (SFSCs) are a post-trip monitoring supplement to the emergency procedures. In the course of an event, violation of one or more SFSCs alerts the control room staff to emerging problems with the on-going mitigation strategy. Success path monitoring (SPM) algorithms provide alarms and displays of system/component availability and performance for each of the success paths.

4. FURTHER STUDY

4.1. Addressing the advanced control room (ACR) issues

As a compact workstation type control room is adopted for KNGR, It is necessary to address the potential problems of advanced control room for MMI resources design. It is believed that new type of cognitive errors are highly likely in VDU based advanced control rooms. To address this, we have taken the approach of identifying potential problems/issues, designing MMI against the potential problems, and evaluating the design to verifying the existence of the potential problems in the design product. KEPRI will perform this analysis with collaboration with the foreign consultants who have experiences in advanced control room design.

4.2. CPS design issues

Despite many potential advantages, there are also challenges in designing an effective computer-based procedure system such as decrease of operator competence for operation by exercising knowledge and the decrease of operator vigilance during operation using a computerized procedure. Results of the studies on computer-based procedures show many types of usability concerns. For example, since computer-based display devices may not be able to display all of these documents adequately, and partial scope may inhibit personnel performance. Integration with other MMI resources in the KNGR MCR, coordination among operators in use of CPS, appropriate level of automation in CPS design are some of the important issues to resolve in the design of the KNGR CPS.

4.3. Configuration management of S/W and computerized procedures

While the functionality of advanced control increase as new operator aids are incorporated in the man machine interface system, the burden of developing, maintaining the vast amounts of S/W became high. To be economical, it became crucial to develop qualification process and tools to be used for verification, validation, and configuration management of S/W. The development of methodology and tools for validating computerized procedure are necessary to reduce the efforts required for initial development and maintenance of the procedure.

4.4. Plant detection/diagnosis aids

As computer technology can provide complex information processing aids, further research is necessary to explore the possibility of aiding operator in detecting slowly developing problems and diagnosing the faults from the plant process and alarm information. The endeavour to enhance plant control automation based on the modern computer technology will be also necessary to improve plant availabilty and safety.

5. CONCLUSION

The basic design of KNGR MMI has been completed and the detailed design is undergoing. In this paper, we discussed on the development process of the KNGR MMI, its major features, and some licensing issues for KNGR MMI. Some of the research topics to be undertaken in the future were discussed briefly as well. Presently, the licensing precedents in U.S. ALWRs provide KNGR MMI designers with general directions for addressing the issues related to full digital MMIS and human factor engineering design process of advanced control room. Systematic development of requirements and design documentation as well as early human factors evaluation of the design using a simulator-driven dynamic mockup have been achieved. This leaves the KNGR program well prepared to pursue licensing of the standard design, as well as to implement the detailed design in KNGR construction.

REFERENCES

[1] Conceptual Design Summary Report for KNGR MMI, Rev. 0, KEPRI, December 1997.

[2] Human Factors Engineering Program Plan for KNGR MMI, Rev.0, KEPRI, January 1998.

[3] NUREG-0700, Human-System Interface Design Guideline Rev. 1, U.S. Nuclear Regulatory Commission, Washington, D.C., February 1995 (Draft Report).

[4] Joint Design Development Reports for KNGR MMI, KEPRI, October, 1997.