Independence Design Solution for MMI Design in Compliance with ISG-04

Jin Ku Kim, Joon Kon Kim, Seung Ha Jung, Jeong Hyeong Lee, Yeong Su Kim, You-Sung Ro
KEPCO Engineering & Construction, Inc., 269, Hyeoksin-ro, Gimcheon-si, Gyeongsangbuk-do, South Korea
jinkoo@kepco-enc.com, joonkkim@kepco-enc.com, para80@kepco-enc.com, tntljh@kepco-enc.com,
kysngo@kepco-enc.com, ysnoh@kepco-enc.com

1. Introduction

Multidivisional-Man Machine Interface (MD-MMI) represents a significant evolution in nuclear I&C/MMI systems. MD-MMI integrates the indicators and controls from multiple divisions into a single integrated Video Display Unit (VDU) based MMI design. This significantly improves the Human Factors Engineering (HFE) aspects of the interface. The challenge for I&C/MMI designers is to accomplish this HFE integration, while maintaining the historical fault tolerance inherent in separate divisions.

The NRC developed Digital I&C - Interim Staff Guidance 04 (ISG-04). This guidance provides detailed design criteria for bi-directional data communication to allow functions such as the MD-MMI for control and display, while ensuring divisional independence is maintained so that conformance with the single failure criteria is not compromised.

Compliance to ISG-04 for non-safety to safety communication has become even more important since the issuance of the cyber security rule, 10 CFR 73.54, and RG 5.71. Non-safety communication to safety systems will receive extraordinary NRC review to ensure it does not open a potential breach in cyber security. It is noted that the original draft of RG 5.71 precluded non-safety to safety communication. After much infighting between the I&C Branch and the Security Branch of the NRC, the issued version of RG 5.71 allows this bi-directional communication if the non-safety system is in the same cyber security defensive layer as the safety systems. Cyber security is a complex subject that is not addressed in this paper.

2. Design Configuration of MD-MMI in Compliance with ISG-04

2.1 Controllers

Most safety and non-safety controllers are redundant (hot standby configuration) to ensure high reliability. This redundancy is not credited for single failure compliance or to limit spurious actuations. Redundancy does not apply to Reactor Protection System (RPS) and Engineered Safety Features Actuation System (ESFAS) controllers, since there is already sufficient redundancy between the safety divisions for these functions.

Multiple controllers within each division allow compliance with the spurious actuation requirements of ISG-04 Section 3.1-5. Control functions and plant components are distributed to different controllers so that any plant transient resulting from the failure or spurious actuation of all functions/components within a single controller is bounded by the plant's safety analysis. This applies to both safety and non-safety controllers.

The priority logic is applicable to MD-MMI at the component. The safety and non-safety component level controllers implement identical standard component control logic for typical plant components such as solenoids, motor-operated valves, motor starters and switchgear. However since the safety controllers receive non-safety MD-MMI control signals, the safety controllers also include logic to ensure that safety functions have priority over non-safety functions; this logic is for compliance to ISG-04 Section 2. The priority logic is implemented within the application software of the safety controllers. Therefore it must be non-volatile as required by ISG-04 Section 2 Position 7.

The priority logic in the controller ensures that control commands originating from within the safety system block control commands for the opposite state of the component, such as those that may originate from non-safety systems.

In addition, another priority logic is also needed for diverse functions credited for compliance to BTP 7-19; for simplicity these will be referred to as Defense-in-Depth & Diversity (DiD&D) functions. The key difference in these different priority logics is that MD-MMI priority logic can be subject to the same Common Cause Failure (CCF) that causes failure of the safety system itself, therefore it can be implemented within the safety application software. On the other hand, the priority logic used for DiD&D functions must be independent of the postulated CCF.

To accomplish this independence, Component Interface Module (CIM) is used to interface to plant equipment. The CIM is implemented by transistor devices or completely diverse firmware; this can be diverse programmable gate array technology. While it is possible to implement this using programmable gate array technology, the priority logic is so simple that a conventional integrated circuit implementation

simplifies compliance to ISG-04 Section 2 Positions 6 and 8, which require 100% testing.

2.2 Safety Video Display Unit (S-VDU)

While MD-MMI provides a significant Human Factors Engineering (HFE) improvement for plant operators, the Main Control Room (MCR) and Remote Shutdown Room (RSR) must also contain Class 1E MMI for system level actuations, as required by IEEE603 and RG 1.62, and Class 1E MMI for all component level actions credited as primary success paths in the Emergency Operation Procedures (EOPs). Primary success paths means there is no automation for the action. Primary success paths exclude contingency actions for functions that are automated.

The requirements for safety related MMI are fulfilled in the I&C Architecture by conventional pushbuttons and Safety VDUs on the Safety Console which is a backup MMI panel. MD-MMI is the primary MMI for all plant conditions including accident conditions. The Safety Console is used only when operators detect MD-MMI failure. While MD-MMI is typically used with computer based procedures, paper procedures are used with the Safety Console. This is because computer based procedure systems are typically non-safety, therefore a backup is needed.

2.3 Communication Independence

Each safety controller or safety VDU that interfaces to a multi-division communication network includes one or more communication modules. This module provides electrical independence between divisions through its fiber optic interface. It also provides communications independence through shared two-port memory and an independent communication controller.

The shared two port memory allows the processor's main Central Processing Unit (CPU) and communication controller to write and read the same memory device asynchronously from each other. Therefore, normally neither the CPU nor the communication controller needs to wait for the other to complete their read memory or write memory operations. Two port memory read and write cycles are typically less than 10 micro seconds, therefore there is minimal potential for the CPU and communication controller to attempt to access the same memory location simultaneously. However, should this occur, the communication module includes arbitration logic. Higher priority is given to the main CPU so the communications interface cannot interfere with the deterministic cyclical operation of the safety function performed by the main CPU.

Alternately, higher priority can be given to the communication controller. If this is done, then the main CPU should poll the two port memory for a fixed time. This polling must be included in the calculation of main CPU cycle time. If the two port memory does not become accessible after a fixed time-out, the main CPU should alarm a failure of the communication interface and take pre-defined safe state actions. This technique also maintains the deterministic operation of the main CPU, for compliance to ISG-04 Section 1 Position 4.

For compliance to ISG-04 Section 1 Position 7 and 12, the communication controller includes message error detection features such as message header checks, format checks, size checks, Cyclical Redundancy Checks (CRC), watchdog timer and alive counter. The main CPU writes all communication data to pre-defined fixed memory locations within the CPU module. This avoids any potential for errors related to dynamic memory allocation, as required by ISG-04 Section 1 Position 9.

2.4 Memory Protection

Both safety controllers and safety VDUs rely on operating system program memory to maintain the communication independence functions described in Section 2.3. For compliance to ISG-04 Section 2 Position 7, all of this memory must be non-volatile and protected against undesired alteration. For reliability, modern digital systems use non-volatile memory, such as FLASH or EPROM, for both application programs and operating systems. This complies with the non-volatile memory requirements of ISG-04.

2.5 MD-MMI Design

Equipment qualification - As required by ISG-04 Section 3.1.5, MD-MMI stations must be qualified to demonstrate that they do not generate spurious control commands during adverse environmental conditions. All qualification tests are intended to demonstrate that no spurious control commands will be generated. Therefore, during these tests, the MD-MMI shall be executing software that represents the actual functions of the MD-MMI. Seismic qualification must also demonstrate Category 2 physical integrity.

Although it is not necessary to demonstrate correct functionality of MD-MMI VDUs for these qualification tests, correct functionality is highly desirable, since MD-MMI is the preferred MMI for all plant conditions, including plant shutdown after a Safe Shutdown Earthquake.

Two distinct operator actions - ISG-04 Section 3.1.5 recommends two distinct operator actions to initiate control commands from a MD-MMI workstation.

The MD-MMI communications interface design, which generates two distinct communication signals from two distinct operator actions. The first operator action selects the component to be controlled (eg. Valve 123). The second action selects the control command (eg. Open/Close). Both actions result in communication messages that contain routinely employed features to detect data transmission/reception errors, such as CRC. More importantly, both messages contain common data, such as the component identification tag. The safety system checks the messages to ensure common data matching, before control commands are accepted.

Software quality - The functionality prevents spurious control commands by two distinct operator actions, is implemented primarily in the non-safety software of the MD-MMI. Therefore, the MD-MMI commits to an augmented software quality program for these functions. This augmented quality is primarily through rigorous design specifications and independent verification and validation of the software.

Failure Detection - Based on two distinct messages, MD-MMI failures that result in mismatched communication messages will be detected by the safety system. Therefore, these errors can be alarmed. However, these types of failures are very unlikely. The most likely MD-MMI failures will result in complete communication or CPU freeze. Operators will eventually detect this failure when attempting to navigate between MD-MMI display pages or take control actions, since the MD-MMI VDU will not respond correctly.

3. Conclusions

This paper presents background information on the evolution of divisional independence requirements, which have historically prevented MD-MMI. It discusses recent changes in NRC regulatory guidance which facilitate MD-MMI. This paper presents key features of I&C/MMI designs needed to meet this regulatory guidance. It also discusses designs currently under NRC regulatory review. It is important to understand that the licensing activities pertinent to MD-MMI are ongoing. The NRC is currently reviewing MD-MMI designs for the APR1400, AP1000 (Westinghouse), US-EPR (AREVA) and US-APWR (Mitsubishi).

REFERENCES

[1] DI&C-ISG-04, Interim Staff Guidance on Highly-Integrated Control Rooms – Communications Issues (HICRc), March 2009

[2] IEEE Std 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,” Institute of Electrical and Electronics Engineers, Piscataway, NJ.

[3] 10 C.F.R.73.54, “Protection of digital computer and communication systems and networks”, U.S. Nuclear Regulatory Commission, Washington, DC.

[4] Regulatory Guide 5.71 – “Cyber Security Programs for Nuclear Facilities”, U.S. Nuclear Regulatory Commission, Washington, DC.

[5] NUREG-0800, “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants (LWR Edition),” Branch Technical Position 7-19, “Guidance for Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems,” U.S. Nuclear Regulatory Commission, Washington, DC.

[6] Regulatory Guide 1.62 – “Manual Initiation of Protective Actions”, U.S. Nuclear Regulatory Commission, Washington, DC.

[7] IEEE Std 7-4.3.2-2003, “Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,” Institute of Electrical and Electronics Engineers, Washington, DC.