Practical Integrated Design of Safety and Non-safety Soft Control for Small Modular Reactor (SMR)

Yeongsu Kim [ab*]
[a] *KEPCO E&C, 269, Hyeoksin-ro, Gimcheon-si, Gyeongsangbuk-do, Republic of Korea*
[b]*Kumoh National Institute of Technology, 61 Daehak-ro, Gumi, Gyeongbuk, 39177, Korea*
[*]Corresponding author: kysngo@kepco-enc.com

Keywords: SMR(small modular reactors), MMIS Design, Communication Independence, Licensing Design

1. Introduction

Recently, small modular reactors (SMRs) have become a key focus in the field of nuclear power plants (NPPs). The compact design of the SMRs offers advantages for various applications, such as marine vessels and spacecraft. In this context, optimizing the size of the control room is crucial to enhance design flexibility. The workstation-based operator console adopted in the APR1400 has significantly reduced the size of the main control room (MCR) panel compared to the OPR1000 by employing visual display unit (VDU)-based soft control. However, to satisfy strict independence requirements, the soft control in the APR1400 is designed with separate displays for safety class and non-safety class soft controls. This design causes several challenges, such as increased equipment costs, expansion of the operator console size, and additional maintenance workload

This study proposes a practical integrated design of safety and non-safety control modules aimed at optimizing the size of the MCR to maximize design flexibility in Korean NPPs, specifically for application in SMRs.

2. Methods and Results

The integrated soft control design inherently needs to meet the strict requirements for communication independence. The initial guidance for communication independence in the nuclear industry was provided in Annex G of IEEE-7-4.3.2-1993 [1], which was later revised to Annex E in the 2003 edition [2]. However, Annex E was deemed insufficient in providing the necessary criteria and, as a result, was not endorsed in RG 1.152 [3]. Consequently, Digital I&C Interim Staff Guidance 04 (ISG-04) [4] was developed to provide detailed design criteria for communication independence. Therefore, ISG-04 serves as a crucial reference, and design features that ensure compliance with ISG-04 are described to meet these independence requirements in this paper.

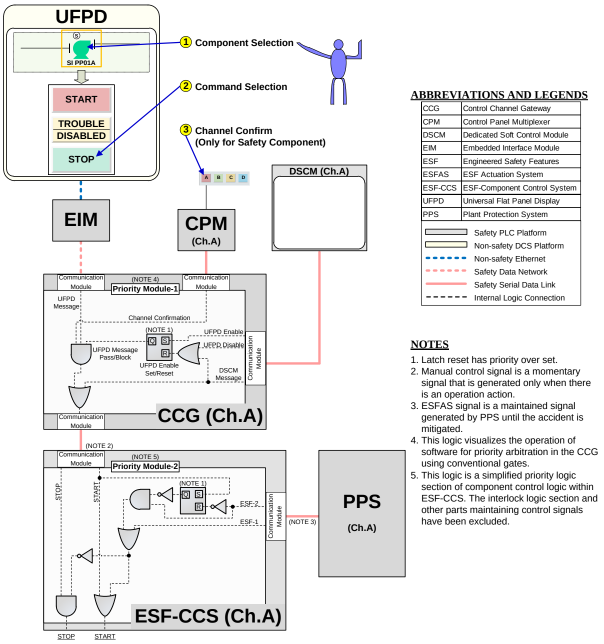
In addition to complying with the design criteria of ISG-04, the design discussed in this paper is firmly based on two principles to ensure its practical application in the nuclear industry as follows:

i. **No adverse effect**: No single or multiple failures within non-safety digital devices shall cause a repositioning (e.g., open/close) of safety components. Repositioning of safety components by soft control can only be enabled when interlocked with additional operator actions and signals from safety digital device.

ii. **Minimizing Design Changes**: Minimize design changes by adhering as closely as possible to the current I&C system architecture of the APR1400. This principle ensures that the design utilizes the existing, validated I&C system architecture, thereby simplifying the implementation process and enhancing acceptance within the industry.

2.1 Design Overview

Figure 1 shows the block diagram of the integrated design for safety and non-safety soft control.



ABBREVIATIONS AND LEGENDS

CCG	Control Channel Gateway
CPM	Control Panel Multiplexer
DSCM	Dedicated Soft Control Module
EIM	Embedded Interface Module
ESF	Engineered Safety Features
ESFAS	ESF Actuation System
ESF-CCS	ESF-Component Control System
UFPD	Universal Flat Panel Display
PPS	Plant Protection System

NOTES
1. Latch reset has priority over set.
2. Manual control signal is a momentary signal that is generated only when there is an operation action.
3. ESFAS signal is a maintained signal generated by PPS until the accident is mitigated.
4. This logic visualizes the operation of software for priority arbitration in the CCG using conventional gates.
5. This logic is a simplified priority logic section of component control logic within ESF-CCS. The interlock logic section and other parts maintaining control signals have been excluded.

Fig. 1. Integrated Soft Control Design Block Diagram

The universal flat panel display (UFPD) is a soft control-based device designed to operate both safety and non-safety components, replacing the information flat panel display (IFPD) of the existing APR1400. The operational procedure through the UFPD is as follows:

i. The operator selects the component to be controlled on the UFPD screen of the operator console.
ii. When the control template pops up on the UFPD screen, the operator selects the desired control command.
iii. When the corresponding channel lamp of the selected component is flashing on the channel confirm switch (CS) located in front of the UFPD, the operator confirms it and pushes the switch.

When an operator selects a component and a command through screen navigation, the non-safety UFPD transmits the corresponding signal via the Ethernet to the embedded interface module (EIM), a safety component installed within the operator console. The EIM serves as the engineered safety features-component control system (ESF-CCS) soft control module (ESCM) located in the operator consoles of the existing APR1400, with the VDU removed and mounted inside the console, thus maintaining the same signal flow configuration as in the original APR1400.

The message received by the EIM is divided into two types: a message containing component selection information and a message containing control command selection information. Each of these messages undergoes validation within the EIM. Once validated, a signal for the message is sent to the control channel gateway (CCG) to flash the corresponding channel confirm switch on the operator console. The operator confirms the channel and pushes the flashing switch if the channel is correct. When the CCG receives the confirmation signal of pushed switch, it forwards the signal to the ESF-CCS, completing the operator's manual control signal transmission.

Additionally, this design includes the dedicated soft control module (DSCM), which replaces the ESCM located in the safety console of the existing APR1400. Unlike the APR1400, however, this soft control module is designed as a dedicated unit for each channel. Since the DSCM does not require a channel confirmation switch, it has been excluded from the design. Consequently, a total of four DSCMs (one per channel) are provided in the MCR. To ensure complete channelization, each DSCM is connected to the CCG via individual serial data links. The DSCM also includes an enable/disable function for the UFPD.

The manual control signals generated from the non-safety UFPD are given a lower priority than the signals generated by the safety DSCM. This priority arbitration is performed by the CCG, which is designed to ignore signals from the EIM when the operator controls a component through the DSCM or activates the UFPD disable function on the DSCM. The disable function remains active until the CCG receives an UFPD enable signal from the DSCM. Additionally, engineered safety feature (ESF) actuation signals from the plant protection system (PPS) always take precedence over manual control signals within the component control logic of the ESF-CCS. The design distinguishes between ESF-1 and ESF-2, where ESF-2 is used for components requiring the operator override function through the UFPD or DSCM, and ESF-1 is applied to components where the override function is not needed, consistent with the design of the APR1400.

To prevent unnecessary consumption of system resources on safety system due to spurious signals from UFPD, a workstation disable switch (WDS) is provided that allows the operator to block signals from the UFPD when an anomaly is detected. Figure 2 briefly show the configuration of the WDS.

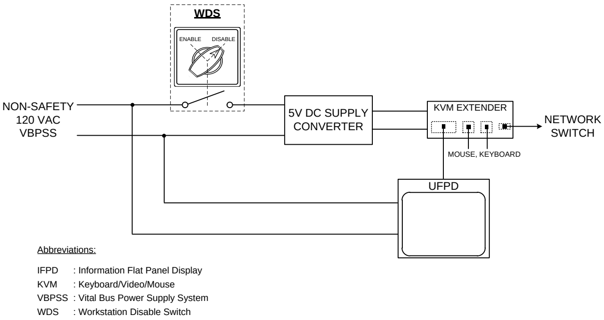

WDS
ENABLE
DISABLE
NON-SAFETY
120 VAC
VBPSS
5V DC SUPPLY
CONVERTER
KVM EXTENDER
NETWORK
SWITCH
MOUSE, KEYBOARD
UFPD
Abbreviations:
IFPD : Information Flat Panel Display
KVM : Keyboard/Video/Mouse
VBPSS : Vital Bus Power Supply System
WDS : Workstation Disable Switch

Fig. 2. Configuration of WDS

Table I show the proposed classification of each component for the integrated soft control design.

Table I: Classification of Components

Component	H/W (Refer to [5, 6])	S/W (Refer to [7])
UFPD	Non-class 1E	Software Integrity Level (SIL)-3
EIM	Class 1E	SIL-3
DSCM	Class 1E	SIL-4
CCG	Class 1E	SIL-4
CPM	Class 1E	SIL-4

2.2 Licensing Design Basis

2.2.1 Physical & Electrical Independence

The connection between the Non-class 1E UFPD and the Class 1E EIM shall comply with the physical and electrical separation requirements of IEEE 384 [6]. Accordingly, this connection is implemented via fiber-optic communication to ensure electrical isolation, with the physical separation distance incorporated into the console design. In this proposed design, the EIM is compactly housed within the console, allowing for an increased separation margin compared to the current distance between the IFPD and ESCM in the APR1400.

2.2.2 Functional Independence

Functional independence ensures that safety systems can perform their required functions without adverse effects from external resources, particularly those outside the safety channel. This is achieved by using priority modules.

In the proposed design, two priority modules are applied to the safety components, as shown in Figure 1.

Priority Module-1 is implemented within the CCG. Messages from the UFPD are transmitted to the ESF-CCS only when a channel confirmation signal is present, ensuring that only verified signals affect the safety system. Even if multiple errors occur in the non-safety components, this mechanism guarantees that they cannot impact the safety components unless a signal from the safety system is initiated through additional operator actions, and each signal affects only a single component. Additionally, the priority module ensures that the operation of the DSCM, a fully channelized safety soft control module, is not interrupted.

Priority Module-2 is embedded in the ESF-CCS component control logic. When an ESF actuation signal occurs, all conflicting command signals are blocked in the component control logic. This guarantees that manual control signals do not interfere with ESF actuation signals. As a result, signals from the UFPD cannot compromise the safety function.

These design features meet the requirements stated in ISG-04, Section 3.1, Position 3, "non-safety stations controlling safety-related equipment."

2.2.3 Communication Independence

The interface between the non-safety UFPD and the safety EIM, as well as the interface between the safety EIM and the CCGs in other safety channels, are both classified as interdivisional communications as defined by ISG-04.

Dual-ported Memory

Each interdivisional communication is executed using dual-ported memory on the receiving system. Additionally, the control processor and communication processor are separated, allowing asynchronous access to the dual-ported memory. By utilizing dual-ported memory, both the control processor and communication processor can perform asynchronous read/write operations on the same memory device. The dual-ported memory serves the role of a buffering circuit, as stated in Annex E of IEEE 7-4.3.2, and has a design feature that meets the requirements of Section 1, Position 4 of ISG-04.

The cycle time for access and processing of read/write operations in the dual-ported memory shall be minimized to reduce the likelihood of the control processor and the communication processor simultaneously accessing the same memory space.

Preventing Adverse Effects from Communication Errors

To comply with Section 1, Position 7 of ISG-04, each interdivisional communication uses predefined data sets and deterministic transmission. Data messages follow predefined formats, including headers, data order, length, and error detection bits, and are transmitted periodically. Although UFPD messages are event-based, deterministic transmission is maintained by sending null datasets when no commands are issued.

Additionally, to comply with Section 1, Position 12 of ISG-04, erroneous messages are blocked through communication error detection on the receiving side. The communication processor checks headers, formats, and sizes, and uses cyclical redundancy checks (CRC), a watchdog timer, and an alive counter to block nonconforming messages and reject single or multiple bit errors. The alive counter detects outdated or repeated data, while the watchdog timer identifies timeouts caused by message rejections or network failures.

When communication errors occur, an alarm triggers, prompting the operator to take predefined actions according to established procedures (e.g., switching the WDS). UFPD failures, such as communication or processor freezes, are likely the most common issues. Since operators may not constantly monitor the UFPD screen, the system uses the alive counter (i.e., heartbeat) to trigger an alarm if no updates are detected, immediately notifying the operator of potential failures.

2.3 Comparison with APR1400 and Evaluation

Figure 3 highlights the changes in red when compared to the existing APR1400 soft control network configuration.

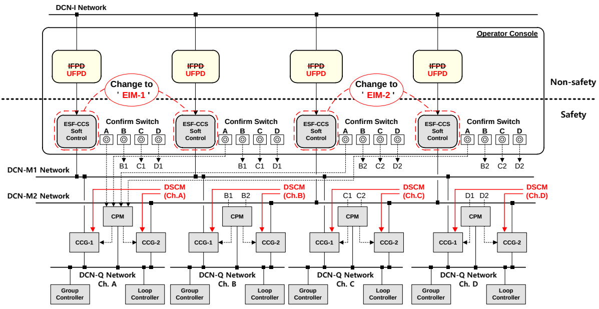


Fig. 3. Design Changes in Soft Control Network

The main changes include replacing the ESCM in the operator console with the EIM, eliminating the VDU, reducing the overall size, and allowing integration into the console as a compact interface module. In addition, the ESCM in the safety console has been replaced by channel-dedicated DSCMs, with separate dedicated data communication links for each channel. Although the IFPD has been replaced by the UFPD, there are no changes to the hardware design.

One difference from the APR1400 in terms of message transmission is that the UFPD also transmits control command, which raises concerns about the possibility of unintended commands being transmitted. However, the probability of an incorrect manual control signal being transmitted to the safety system is extremely low, with just the predefined message format and CRC error detection features. For example, the probability of an 'ON' command being sent as 'OFF' is reduced by ensuring a 4-bit difference between commands, assuming a 1-byte data format for the control command. The bit error rate (BER) indicates the likelihood of errors during signal transmission, and the error probability is calculated as BER raised to the power of the number of differing bits. In the industry, both CRC-16 and CRC-32 are commonly used, but since the detailed specifications are not determined, CRC-16 is conservatively assumed here. With fiber-optic Ethernet, which typically has a target BER of around 10^{-10} as specified in IEEE 802.3 [8], the probability of an undetected error with a 4-bit difference and CRC-16 is:

$$P = (10^{-10})^4 \times \frac{1}{2^{16}} \approx 1.53 \times 10^{-45}$$

This means the probability of an incorrect command affecting the safety system is an almost impossible occurrence. Other key differences between the proposed design and the existing APR1400 are summarized as shown in the following table.

Table II: APR1400 and Proposed Design Comparison

Item	APR1400	Proposed Design
Soft Control Composition	IFPD for non-safety control	UFPD for integrated safety and non-safety control
	ESCM for multi-channel safety control	DSCM for channel-dedicated safety control
Soft Control in Operator Console	IFPD & ESCM with CS	UFPD with CS
Soft Control in Safety Console	ESCM with CS	DSCM (No CS)
Priority Module Function in CCG	Control signal can be blocked by CS	Control signal can be blocked by CS; Prioritizes DSCM signal over UFPD signal
Numbers of Safety VDUs	22 VDUs for operator and safety console	4 VDUs for safety console
Soft Control Classification	IFPD: Non-class 1E & SIL-2	UFPD: Non-class 1E & SIL-3
	ESCM: Class 1E & SIL-3	DSCM: Class 1E & SIL-4

As presented in the table, the integration of safety and non-safety controls has reduced the number of safety VDUs required in the MCR from 22 to 4. This reduction results in a smaller control room size and lowers hardware costs, thereby improving economic efficiency. Additionally, operators will have reduced eye movement by using the integrated soft control display during normal operations.

Despite the reduction in the number of safety VDUs, the availability of soft control on the operator consoles remains unaffected. In the APR1400, the ESCM and IFPD must operate together, and if the IFPD fails, continued operation on the corresponding console becomes difficult. Although the ESCM can function independently, without the IFPD serving as the indication means, it is practically impossible to operate the console. The UFPD, while utilizing the same hardware as the IFPD, requires a higher software integrity level and is therefore less or equally likely to fail compared to the IFPD.

Regarding the safety console, while the APR1400 employed a multi-channel ESCM with a SIL-3, the proposed design introduces channel-dedicated DSCMs with a SIL-4, ensuring enhanced reliability and independence. The DSCM, compared to the ESCM in the APR1400, serves as a much more reliable and independent backup control means.

3. Conclusions

This study proposes a practical approach to integrating safety and non-safety control modules in the MCR of Korean NPPs, particularly aimed at SMRs. The design not only considers the licensing design basis but also adheres to essential principles that ensure practical implementation. By reducing the number of safety VDUs from 22 to 4, the design optimizes the MCR layout, improves cost-efficiency, and enhances operational convenience. Additionally, the introduction of DSCM to each channel provides a reliable and independent backup of the UFPD, ensuring enhanced safety.

Further research is necessary for the application of SIL-4 software in soft control for the DSCMs. Comprehensive testing of the UFPD system is also crucial to validate its performance under a variety of operational conditions. These tests should include scenarios simulating potential communication failures or system malfunctions to ensure system robustness.

In summary, this proposed design offers an effective solution that not only optimizes space and enhances safety but also fulfills the demands for flexibility and ease of implementation in Korean SMRs. However, further research and testing are essential to fully unlock the design's potential and address any operational challenges.

REFERENCES

[1] IEEE Std. 7-4.3.2, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,” Institute of Electrical and Electronics Engineers, 1993.

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

[3] Regulatory Guide 1.152, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants,” Rev. 3, U.S. Nuclear Regulatory Commission, July 2011.
[4] DI&C-ISG-04, “Highly-Integrated Control Rooms - Communications Issues (HICRc),” Rev. 1, U.S. Nuclear Regulatory Commission, March 2009.
[5] IEEE Std. 603, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,” Institute of Electrical and Electronics Engineers, 1998.
[6] IEEE Std. 384, “IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits,” Institute of Electrical and Electronics Engineers, 2008.
[7] IEEE Std. 1012, “IEEE Standard for Software Verification and Validation,” Institute of Electrical and Electronics Engineers, 2004.
[8] IEEE Std. 802.3, “IEEE Standard for Information Technology - Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks - Specific Requirements, Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications,” Institute of Electrical and Electronics Engineers, 2008.