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

KNS 2024
Korean Nuclear Society Autumn Meeting

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

Introduction

❖ 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.

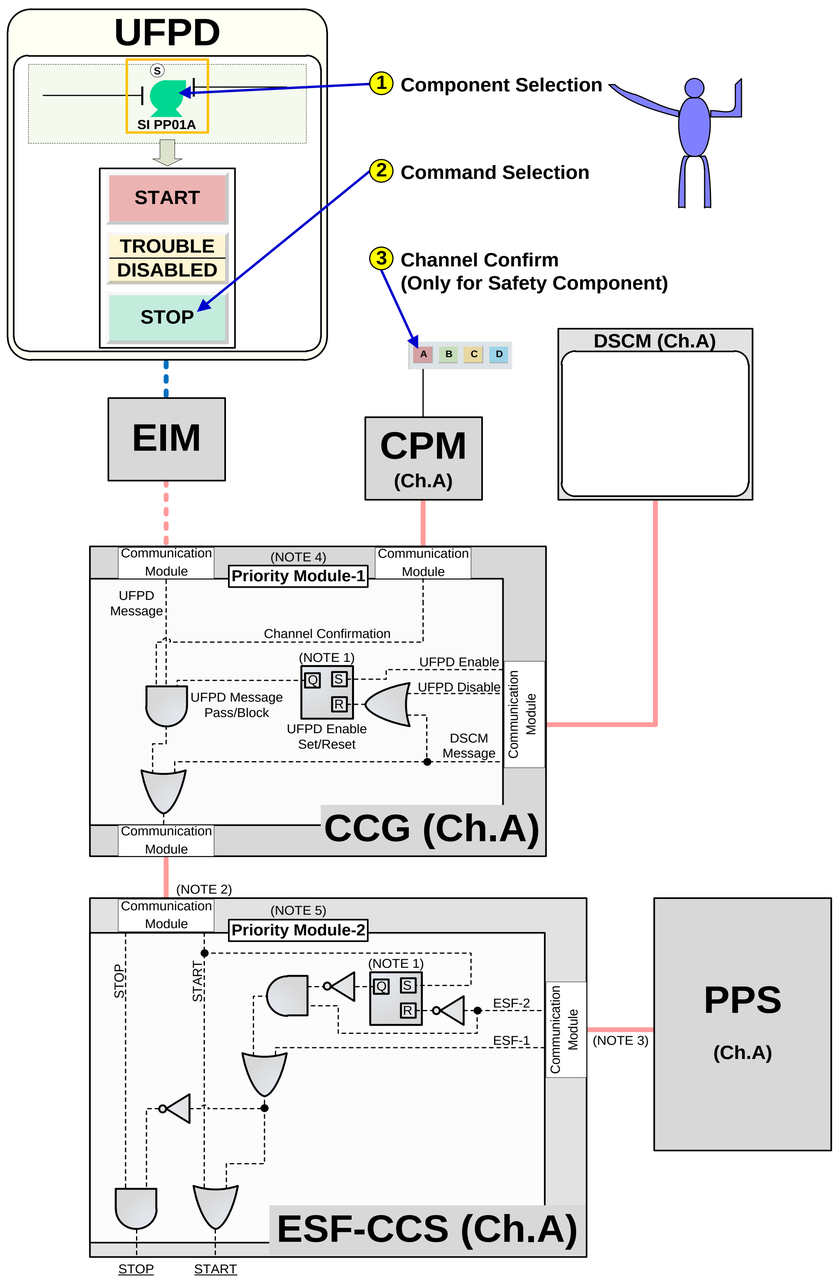
Design Principles

❖ The design adheres to ISG-04 and is based on two principles to ensure practical application in the nuclear industry:

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.

ii. **Minimizing Design Changes:** Minimize design changes by adhering as closely as possible to the current I&C system architecture of the APR1400.

Design Overview



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

Safety PLC Platform
Non-safety DCS Platform
Non-safety Ethernet
Safety Data Network
Safety Serial Data Link
Internal Logic Connection

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 UFPD is a soft control-based device designed to operate both safety and non-safety components, replacing the 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.
ii. A control template pops up on the UFPD screen for command selection.
iii. When the channel lamp flashes on the channel confirm switch (CS), the operator confirms 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 EIM. The EIM serves as the ESCM 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.

❖ Additionally, this design includes the DSCM, which replaces the ESCM located in the safety console of the existing APR1400. Unlike the APR1400, this soft control module is designed as a dedicated unit for each channel. To ensure complete channelization, each DSCM is connected to the CCG via individual serial data links.

Licensing Design Basis

❖ **Physical & Electrical Independence:** Compliance with physical and electrical separation as per IEEE 384.

❖ **Functional Independence:** Prioritized commands prevent failures in non-safety systems from affecting safety functions.
Priority Module-1: 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.
Priority Module-2: When an ESF actuation signal occurs, all conflicting command signals are blocked in the component control logic.

❖ **Communication Independence:** Achieved through dual-ported memory and communication error prevention mechanisms.

Comparison with APR1400 and Evaluation

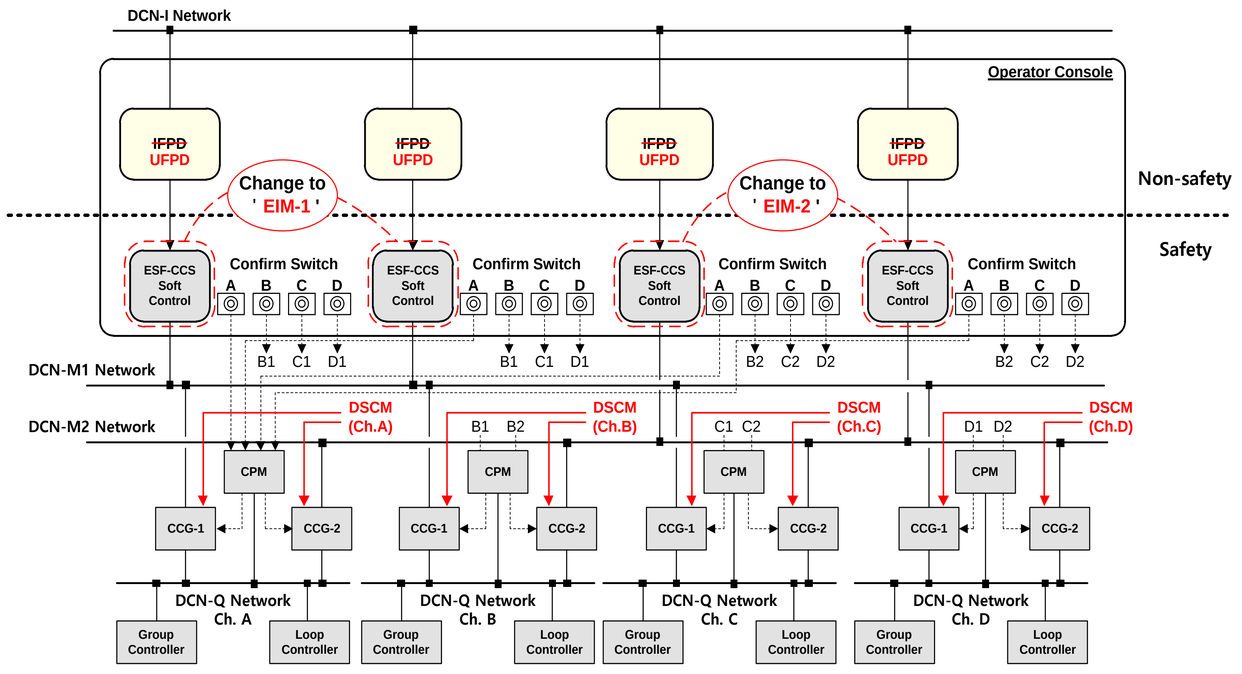


Fig 2. Design Changes in Soft Control Network

❖ **ESCM to EIM Replacement:** The EIM replaces the ESCM in the operator console, removing the VDU, reducing the console size, and enabling a more integrated design.

❖ **Channel-dedicated DSCM:** The DSCM replaces the ESCM in the safety console, with each channel connected via dedicated communication links, enhancing safety.

❖ **UFPD Functionality:** The UFPD replaces the IFPD with no significant hardware changes. While the UFPD transmits control commands, the probability of unintended signals is extremely low with just predefined message formats and CRC error detection. With fiber-optic Ethernet, which typically has a target BER of around 10^{-10}, the probability of an undetected error with a 4-bit difference and CRC-16 is 1.53×10^{-45}.

Conclusions

❖ By reducing the number of safety VDUs from 22 to 4, the design optimizes the MCR layout, improves cost-efficiency, and enhances operational convenience.

❖ The introduction of DSCM to each channel provides a reliable and independent backup of the UFPD, ensuring enhanced safety.

❖ 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

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, 2003.
[2] 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.
[3] DI&C-ISG-04, “Highly-Integrated Control Rooms -Communications Issues (HICRc),” Rev. 1, U.S. Nuclear Regulatory Commission, March 2009.
[4] IEEE Std. 603, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,” Institute of Electrical and Electronics Engineers, 1998.
[5] IEEE Std. 384, “IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits,” Institute of Electrical and Electronics Engineers, 2008.
[6] IEEE Std. 1012, “IEEE Standard for Software Verification and Validation,” Institute of Electrical and Electronics Engineers, 2004.
[7] 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.