Priority design of safety related component control for autonomous operation in NPP

Yun Goo Kim*, Dae Seung Park

Korea Hydro and Nuclear Power Co., ltd, Central Research Institute, Daejeon, Korea
**Corresponding author: ygkim.stpn@khnp.co.kr*

1. Introduction

Artificial intelligence(AI) technology has been reviewed for the nuclear power plant application. One of challenging application is AI based Autonomous Operation System(AOS) which provide automatic control of nuclear power plant startup and shutdown operation[1,2,3,4]. During the startup and shutdown operation, safety related component should be controlled. Therefore, AOS may have control function of safety related component. AOS may designed as non-safety grade as other control system in NPP. Therefore, AOS should be designed to keep independence between safety-related and non-safety related system.

2. Independence requirement and priority design

10 CFR Part 50, Appendix A, GDC 24 states, that the protection system shall be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.

In APR1400 I&C design, there is component interface module(CIM) which handle the control signal from protection system and non-safety grade diverse protection system(DPS). The CIM is a qualified safety module that uses hardware logic devices to cope with a common-cause failure (CCF) of the digital protection and safety systems. The CIM receives component control signals from the ESF-CCS, DPS, diverse manual ESF actuation (DMA) switches, and front panel control (FPC) switch.

The CIM combines these control signals through conventional hardware priority logic and then sends the resulting signal to the controlled component such as an MOV, pump motor, or solenoid-operated valve. The CIM provides the priority logic function between ESF CCS actuation signals and DMA switch signals and also provides the interface function from the ESF CCS to the plant component.

When AOS send control signal to safety related component, that control signal should not interference the safety functions. The priority for AOS and other signal can be implemented in the CIM. Fig. 1 shows the configuration of CIM which include the priority function for autonomous operation system. The configuration in dashed line represent the typical CIM design. The control signal for autonomous operation is connected to CIM for priority selection.

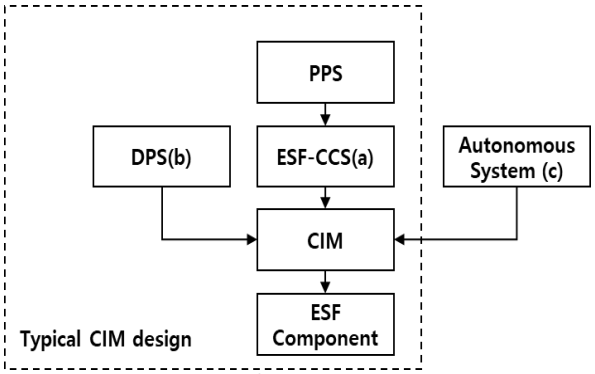

Figure 1. Priority design for autonomous operation system

The priority of autonomous control signal has lowest priority to ensure that the safety function. Following shows the details about priority in CIM including autonomous control signal. The priority of (a) control signal from ESF-CCS and (b) control signal from DPS are based on state priority. For each ESF component the state priority has been defined according to the design of safety function. The priority of (c) control signal from autonomous operation system is always lower than other control signal to ensure that the safety function.

- **priority rule** : $(\,(\boldsymbol{a}) = (\boldsymbol{b})\,) > (\boldsymbol{c})$

3. Reachable operation state by autonomous control system and safety

The aviation industry also applied safety function for mission critical system. The Simplex architecture, which uses verified safety controller and verified switching logic, has been proposed by Stanley Bak, et al[5]. In the Simplex architecture, complex controller and safety controller are used and the decision module which has verified switch logic decide which controller will be used according to the plant status. This architecture enables the safe use of high-performance, untrusted and complex control algorithms without requiring them to be formally verified [5]. In this paper for the autonomous operation, priority design has been applied instead of verified switching logic to ensure safety function. Priority design is more simple than selection logic, because one priority logic can be applied to all control signal while selection logic may depend on various state of operation status.

When the safety protection system provides safety function without failure, the status of plant may be controlled in safe status. APR1400 control system has

been analyzed for common cause failure of control system [6,7]. It means that every possible failure and spurious control from non-safety related control system can be mitigated by safety related protection system. The qualitative analysis shows that the appropriate actuation of the safety systems, and the inherent sufficient safety margin, keep the plant in acceptance criteria of safety goal. This analysis includes the effects of failure of autonomous system related to non-safety component control. Figure 2 shows that the reachable operation state by control system is maintained in safety limit by protection system. The approach for common cause failure analysis in control system can be used directly to the analysis of autonomous operation system.

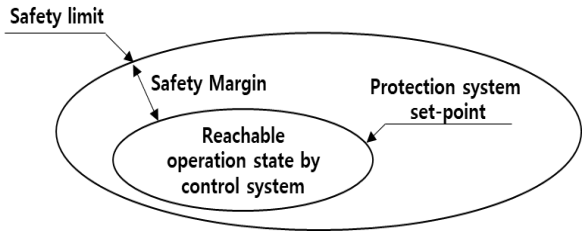

Figure 2. Reachable operation state and safety limit

4. Discussion

The priority design for autonomous operation has been suggested. The existing CIM can be used as priority module for autonomous operation system. CIM already includes the priority design for protection system and diverse system and it has enough quality for safety function. The priority logic in CIM has been suggested to ensure the safety functions against the failure control from autonomous operation system.

For the non-safety component control of autonomous operation system, CCF analysis for control system can be used. For the APR1400 design, the effects of worst case CCF in control system is mitigated by protection system. Therefore, the worst control failure of autonomous operation system is not affect the plant safety.

REFERENCES

[1] Y.G. Kim, et al, "Consideration on data mapping of convolutional neural networks to diagnose abnormal status in nuclear power plant operation," KNS spring meeting, 2018
[2] Y.G. Kim, et al, "Operator support system with diagnosis of abnormal status by convolutional neural networks", NPIC, 2019
[3] Y.G. Kim, et al, "Development of Convolutional Neural Networks to Diagnosis Abnormal Status in Nuclear Power Plant Operation", KNS spring meeting, 2019
[4] Alejandro Barredo Arrieta, et al, "Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI" Information Fusion 58, p82–115, 2020
[5] Satanley Bak, et al, "Real-time reachability for verified simplex design", IEEE Real-Time Systems Symposium, p138, 2014
[6] Korea Hydro & Nuclear Power Co., Ltd., APR1400 Design Control Document Tier 2, Chapter 7 Instrumentation and Controls, APR1400-K-FS-14002-NP, 2014
[7] Y.G. Kim, et al, "Evaluation method for common cause failure hazards on non-safety related system" KNS spring meeting, 2020

ACKNOWLEDGEMENT

This work was supported by the Energy Efficiency & Resources of the Korea Institute of Energy Technology Evaluation and Planning (KETEP) grant funded by the Ministry of Trade, Industry and Energy. (No. 20211510100020)