Three-channel Plant Protection System (PPS) Design for Small Modular Reactor (SMR) with no CCF potential

JongSoo Kwon*, YoungGeul Kim, HwangIn Sok, JaeHong Ha, YoonHee Lee
KEPCO Engineering & Construction Company Inc., 150-1 Deokjin-Dong, Yuseong-Gu, Daejeon, Korea, 34057
*Author:jskwon@kepco-enc.com

1. Introduction

Common cause failures (CCFs) within the plant protection system (PPS) may result in unacceptable consequences from certain combinations of CCFs and postulated initiating events. Current practice to avoid CCF is to use diverse digital components with different attributes in the design of a diverse actuation system (DAS) so as to mitigate the consequences of common cause failure within the PPS.

The instrumentation and control (I&C) system architecture in nuclear power plant (NPP) incorporates protections against CCFs through the use of diversity and defense-in-depth. Even for well-established analog-based I&C system designs, the potential for CCF of multiple systems (or redundancies within a system) constitutes a credible threat defeating the defense-in-depth provisions within the I&C system architectures. The integration of digital technologies into the I&C systems provides many advantages compared to the analog systems with respect to reliability, maintenance, operability, and cost effectiveness. However, maintaining the diversity and defense-in-depth for both the hardware and software within the digital system is challenging. In fact, the introduction of digital technologies may actually increase the potential for CCF vulnerabilities because of undetected systematic faults. [1]

During the past 20 years, there have been a significant number of safety-related and important-to-safety digital systems or components installed in operating NPPs. The safety-related digital systems were developed in accordance with the requirements in Appendix B to 10 CFR Part 50 and generally have operated safely. However, about 40% of the operating plants have reported potential and actual CCFs in many of these systems. [2] Even a high-quality development process is unable to completely eliminate latent design defects introduced during the design and integration process. [3]

In this paper, the new simplified PPS is introduced for the SMR.

2. Methods and Results

It is important to eliminate CCF vulnerabilities from further consideration in the safety systems. The I&C structure and architecture should be designed as simple as possible so that the back-up systems such as DAS are no longer necessary.

In addition, the number of channels for the PPS should be reduced, for example from 4(four) channels to 3(three) channels, for the sake of its simplicity.

The innovative plant protection system (iPPS) is a newly proposed PPS for the SMR to eliminate CCF vulnerabilities from further consideration using diversity attributes. Besides, the iPPS features 3(three) channel design for the simplicity of the I&C architecture.

2.1 Applied Diversity Methods

A diversity and defense and depth (D3) assessment is a systematic approach used to analyze a proposed Digital I&C (DI&C) system for CCFs that can occur concurrently within a redundant design, for example, within two or more independent divisions. These CCFs could cause the DI&C system to fail to perform its intended safety function or could lead to spurious operations.

Acceptable methods for an applicant to use to address or defend against vulnerabilities include, but are not limited to, the following:

The applicant can eliminate CCF vulnerabilities from further consideration through any of the methods below, either alone or in combination:

– using diversity within the DI&C system or component
– using testing
– using alternative methods
– for low-safety-significance structures, systems, and components (SSCs), using a qualitative assessment and failure analysis. [3]

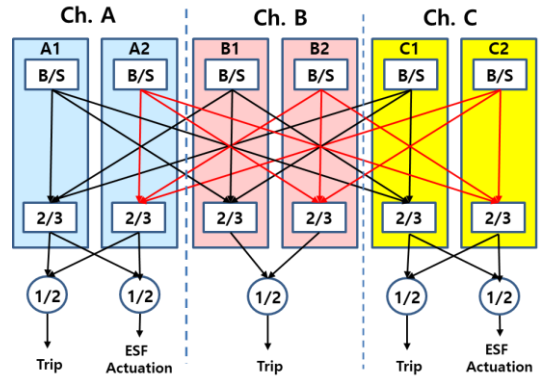
NUREG/CR-6303[4] identifies six diversity attributes (Human, Design, Software, Functional, Signal, Equipment) and 25 related diversity criteria that the reviewer can use to determine whether the system includes adequate diversity.

Applied diversity attributes in the iPPS are functional, signal, and equipment diversities.

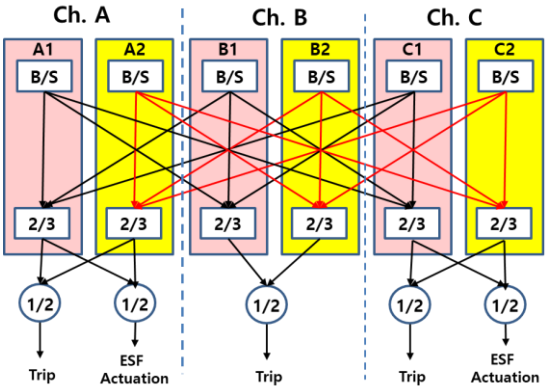
The iPPS consists of different types of FPGAs (OTP, Flash, SRAM) for the equipment diversity. Figure 1 shows the simplified block diagram of 3(three) channel system, (a) different FPGAs between channels, (b) different FPGAs in a channel.

And, the iPPS has signal and functional diversities in a channel to prevent CCFs due to a systematic failure, such as the latent faults of requirements. The functional group 1 includes A1, B1, and C1 and the functional

group 2 includes A2, B2, and C2. It is to achieve the functional independence between redundant portions in a channel. Diverse process parameters are separately monitored in groups 1 and 2 to mitigate the consequence of the design basis events. The bistable processor (B/S) provides their trip signals to the 2/3 coincidence logic of the same group only (Group 1 or Group 2) located in the three redundant channels.



(a) Different Hardware Platforms between Channels and Signal/Functional Diversity in a Channel



(b) Different Hardware Platforms and Signal/Functional Diversity in a Channel

Fig. 1. Simplified Block Diagram of 3-Channel iPPS

To minimize the impact of single failure, the independent circuits are applied by function (ex., different circuit cards for each trip parameter).

2.2 Compliance of Single Failure Criteria

In general, the PPS consists of 4(four) channels to meet the following requirement: [5]

"IEEE EEE 379-2014, Single Failure Criterion, 6.2 Procedure

i) The maintenance bypasses, shared systems, interconnected equipment, equipment in proximity and interactions with other systems shall be considered in the single failure analysis."

The failure modes and effect analysis (FMEA) is performed to show the compliance of the single failure criteria. During FMEA, it is considered that 1(one) channel is bypassed for the maintenance with another channel being inoperable state due to single failure. It makes difficult to meet the single failure criteria with limited redundancies, ex. 3(three) channels, for the PPS. (See Figure 2)

The PPS could be in the inoperable state when the limited redundancy is applied for the PPS. To meet single failure criteria, complicated design and deliberate operation are required. Also, an assessment may be performed to demonstrate that the time allowed for removal from service for maintenance bypass is sufficiently short to ensure that the overall sense and command feature reliability goals are satisfied. [6] It may be a challenging work.

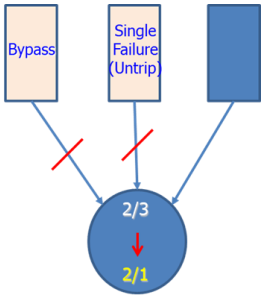


Fig. 2. 3-Channel PPS without Diversity Attributes

As shown in Figure 1, the iPPS adopts sufficient diversities to eliminate CCF vulnerability.

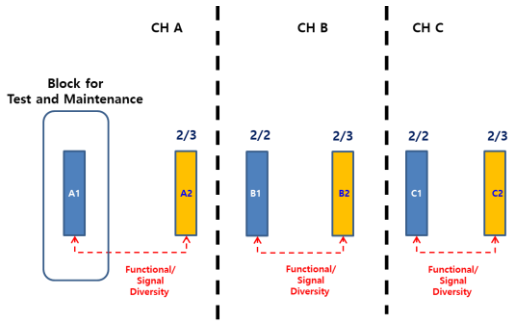


Fig. 3. Strategy to meet the Single Failure Criteria

Either FPGA logic of a channel (A1 or A2) can be out-of-service for the testing and maintenance while maintaining the system's intended functions because diverse process parameters are monitored in groups 1 and 2 to mitigate the consequence of the design basis events. It makes easier that the system meets the single failure criteria with the limited redundancy.

2.4 Power Diversity

Moreover, the diverse powers are supplied to the iPPS to eliminate the inoperable state due to single

failure unlike the conventional power supply design for the PPS. (See Figure 4)

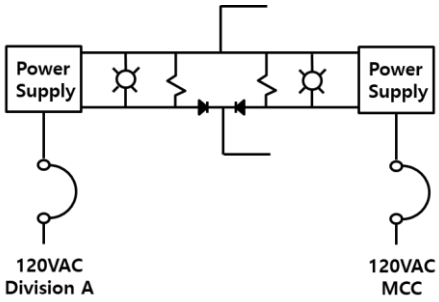


Fig. 4. Diverse Power Supplies for the iPPS

2.4 ATWS Consideration

An anticipated transient without scram (ATWS) is defined as an anticipated operational occurrence as defined in 10CFR50, Appendix A, followed by the failure of the reactor trip portion of the protection system specified in General Design Criterion 20 of Appendix A.

The failure of the trip circuit breaker is a dominant factor of the ATWS. To decrease the possibility of ATWS, the reactor trip switchgear system (RTSS) can be designed with equipment diversity between AB, AC and BC.

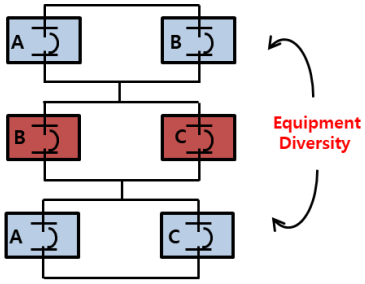


Fig. 5. Diversity in RTCB

In commercial plants in Korea, the diversity attribute for the circuit trip breakers is only different trip mechanisms (Undervoltage, Shunt). In iPPS, the additional diversities are considered, such as different arc chutes and different manufacturers to minimize CCF vulnerability of the breakers. For example, vacuum type breakers are applied for the breakers AC and AB and air type breakers for the breakers BC from different manufacturers, respectively.

2.5 Enhanced Operating Convenience

Common test module is provided for automatic test features for the testing and maintenance for the iPPS without operator's intervention. It is only interfaced to the related equipment during the maintenance.

As shown in Figure 3, 3(three) subparts (A1, B1, C1 or A2, B2, C2 or A1, B1, C2 or etc.) can be out-of-service for the maintenance while maintaining its intended function. It is very helpful to lessen the burden of the operator even in the case of multi-unit plant operation such as the SMR.

2.6 Simplified ESFAS Signal Flow

In APR1400, the ESF actuation signal is generated through the group controller (2/4 Logic) in the ESF-CCS which is a legacy practice from the analog-based PPSs. However, it could be combined in the coincidence logic of the PPS cabinet in the SMR eliminating the 2/4 logic in the group controller of the ESF-CCS for simplicity.

3. Conclusions

The iPPS is designed using diversity attributes such as equipment, signal, functional, etc. to significantly reduce the CCF vulnerabilities Besides, the number of channel for the PPS is reduced to 3(three) channels. The diversities, equipment, arc chute, manufacturer, are applied in the RTSG to enhance the reliability against the ATWS. For operating convenience, the system can be automatically tested using common test module without operator's intervention. In addition, the adequate diversity in a channel is provided to lesson operator's burden during maintenance taking the related equipment out-of-service. To simplify system, the 2/4 logic of group controller is combined into the coincidence logic of the PPS cabinet.

As a result, the proposed iPPS is concluded to be a safe and competitive protection system for the SMR.

REFERENCES

[1] IAEA-TECDOC-1848, "Criteria for Diverse Actuation Systems for NPPs". 2018.
[2] ORNL/SR-2016/130, "Technical Basis for Evaluating Software-Related Common-Cause Failure."
[3] NUREG-0800, Branch Technical Position(BTP) 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems," US NRC.
[4] NUREG/CR-6303, "Method of Performing Diversity and Defense-in-Depth Analysis of Reactor Protection Systems," December 1994.
[5] IEEE 379-2014, "IEEE Standard for Application of the Single Failure Criterion to Nuclear Power Generating Station Safety Systems."
[6] IEEE 603-1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."
[7] 10CFR 50.62, "Requirements for reduction of risk from anticipated transients without scram (ATWS) events for light-water cooled nuclear power plants.