Regulatory Experience against Digital I&C CCFs of NPP

Y. M. Kim[*] and S. B. Park
Korea Institute of Nuclear Safety, 62 Gwahak-ro, Yuseong-gu, Daejeon, Korea, 305-338
[*]*Corresponding author: ymkim@kins.re.kr*

1. Introduction

The plant's I&C systems should provide high reliability in order to maintain the safety goals of the plant. However, operating plants suffer from aging problems, increased maintenance costs, and poor supplier support, including difficulties in obtaining replacement parts. In general, digital technology is expected to be used to replace equipment of power plants due to the availability and potential for performance and reliability improvements. It is also expected to use an I&C system that is more extensive and highly integrated than conventional nuclear power plants. However, the use of software-based I&C components and systems in the safety system will result in failure of the I&C due to software design flaws in the digital system. The licensee shall identify unanalyzed events for malfunctions in various systems, structures and components (SSCs). In addition, the licensee shall identify the sensitivity of unintended actions that could induce the failure of potential digital systems and plant malfunctions, including common cause failures (CCFs).

2. Background

The CCF is defined as failure of two or more structures, systems or components due to a single specific event or cause[1]. The term is usually used with reference to redundant equipment or systems or to uses of identical equipment in multiple systems. Common cause failures can occur due to design, operational, environmental, or human factor initiators[2].

2.1 Regulatory Approaches of US NRC

The U.S. NRC is presenting its regulatory position on CCF of the digital I&C systems through SRM-SECY-93-087 and SRP BTP 7-19. SRM provides specific acceptance criteria for assessing common cause failures and the SRP BTP 7-19 provides guidance for evaluation[3]. The SRM-SECY-93-087 does not provide criteria to exclude consideration for potential software flaws in defense-in-depth and diversity(D3) analysis. However, the SRP BTP 7-19 presents two criteria for eliminating further evaluation of the potential software CCFs. The first is to demonstrate that there is adequate internal diversity, and the second is to test all possible fault logic to ensure that the fault no longer exists.

2.2 Technical Approaches of IEC

IEC 60880 provides defense requirements for software design and coding faults that can lead to CCF of safety system functions[4]. Also, it requires that an analysis of the potential for CCF due to software shall be performed and documented at the system level and/or at the level of the total I&C architecture of the I&C systems important to safety of the NPP.

IEC 62340[5] gives requirements related to the avoidance of CCF of I&C systems that perform category A functions and requires the implementation of independent I&C systems to overcome CCF, while the likelihood of CCF is reduced by strictly applying the overall safety principles of IEC 61226, IEC 61513 and IEC 60880. IEC 62340 provides principles and requirements to overcome CCF by means which ensure independence as followings.

a) between I&C systems performing diverse safety functions within category A which contribute to the same safety target
b) between I&C systems performing different functions from different categories
c) between redundant channels of the same I&C system.

2.3 Common Position of MDEP

Digital I&C Working Group of MDEP(Multinational Design Evaluation Programme) provides common regulatory positions on Digital I&C CCF in new reactor designs[6].

MDEP requires that for each design basis event, an analysis should be perform to demonstrate that the plant can cope with the effects of CCF caused by software. Diversity is a way to reduce the potential effects of CCF. If CCF caused by software could adversely affect a safety function that is required to respond to a design basis event, a diverse means of effective response should be provided and its effectiveness should be justified.

2.4 Regulatory Positions of KINS

The KINS's current position on CCF is guided by Article 26 and Article 27 of Rules for Technical standards of Reactor Facilities.

An additional independent protection system ("diverse protection system") which has the functions of reactor shut down, actuation of emergency auxiliary feedwater system, and turbine trip shall be installed to prepare for ATWS.

In addition, although the software CCF in digital systems is considered beyond design basis, NPPs should be protected against the effects of anticipated operational occurrences(AOOs) and postulated accidents(PAs) with a concurrent CCF in the digital protection systems.

3. Regulatory Experience

The regulatory experience related to failures of common causes of digital instrumentation and control systems has performed during the operational licensing phase of the new nuclear power plant varies widely. Typical issues include verification of safety shutdown capability of safety control panel when CCF of safety system, D3 analysis of safety system, control System CCF Analysis, etc.

3.1 Verification of safe shutdown capability of safety control panel when CCF of safety system

For Shin-Gori NPP Unit 3 and Shin-Hanul NPP Unit 1, safe shutdown capability has been demonstrated by empirical tests that it is possible to enter the shutdown condition (operating mode 4) using the diversity facility against the CCF of the safety system. The experiment used only functions that could operate against the common cause failures specified in the plant's FSAR Table 7.8-3. In case of Sin-Hanul NPP Unit 1, safe shutdown capability was verified without POSAFE-Q platform-based facilities (PPS, ESF-CCS, QIAS-P, QIAS-N, etc.).

3.2 D3 Analysis of Safety System

D3 analysis was performed on the design basis accidents of FSAR Chapter 6 and Chapter 15, based on the available information of the I&C systems for CCF of the safety systems. For all design basis accidents, a qualitative assessment was performed to derive the accidents requiring detailed analysis (e.g., loss of coolant accident). And then, quantitative analysis was performed on derived accidents.

3.3 CCF Analysis of Control System

The control systems, including non-safety control systems described in FSAR Chapter 7.7 and Chapter 15, are evaluated for postulated control system software CCF.

Following the qualitative assessment, a quantitative assessment was performed, if necessary. And the assessment concluded that no multiple failures due to shared signal errors or software CCF result in plant conditions more severe than the acceptance criteria of the FSAR Chapter 15 AOO and PA.

3.4 Smart transmitter and CCF Analysis

Unlike the preceding units, Shin-Gori Units 3 and 4 were applied to the same smart transmitters for safety and non-safety systems. Because smart transmitters are likely to occur common cause failures due to software errors, it is necessary to assess the impact of smart transmitter CCF and plant safe shutdown upon simultaneous design basis accident.

As a result of the analysis, the smart transmitters of some systems were replaced with analog transmitters because the execution of the operation procedures for coping with the design basis accident upon failure of functions due to CCF may differ from the current procedures.

4. Conclusion

In this paper, the major issues related to digital I&C CCF were discussed when reviewing new plant operation permit such as verification of safe shutdown capability of safety control panel when CCF of safety system, D3 Analysis of safety system, CCF Analysis of control system and smart transmitter and CCF analysis. In case Shin-Hanul NPP Unit 1&2, there are some other issues related to digital I&C CCF under reviewing, but this paper did not mentioned them.

Acknowledgements

This work was supported by the Nuclear Safety Research Program through the Korea Foundation Of Nuclear Safety (KOFONS), granted financial resource from the Nuclear Safety and Security Commission (NSSC), Republic of Korea (No. 1805006).

REFERENCES

[1] IAEA Safety Glossary Ed.2.0, 2006
[2] NEI 01-01, Guideline on Licensing Digital Upgrades
[3] NUREG 0800, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition.
[4] IEC 60880, Nuclear power plants-Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions
[5] IEC 62340, Nuclear power plants-Instrumentation and control systems important to safety - Requirements for coping with common cause failure (CCF)
[6] MDEP Common Position No. DICWG-01, "COMMON POSITIONS ON THE TREATMENT OF COMMON CAUSE FAILURE CAUSED BY SOFTWARE WITHIN DIGITAL SAFETY SYSTEMS," (June 2013)