A Study on Application of SIL-based Certification System for Dedication of Commercial Digital Equipment in Nuclear Power Plants

Hoon-Keun Lee [a], Jaeyul Choo [b], Kyungseok Lee [a], Sungbaek Park [a], Youngmi Kim[a*]
[a]*Korea Institute of Nuclear Safety, 62 Gwahak-ro, Yuseong-gu, Daejeon 34142*
[b]*Andong National University, 1375 Gyengdong-ro, Andong-si, Gyeongsangbuk-do, 36729*
[*]*Corresponding author: ymkim@kins.re.kr*

1. Introduction

Until now, many nuclear power plants have been applied digital technologies to the existing system and equipment due to the difficulty in procuring replacement parts and increasing maintenance costs. However, because of limitation on the market growth of nuclear industry, the number of suppliers providing the safety-related digital equipment (accordance to Appendix B to 10 CFR 50) is steadily decreasing. For this, the United State Nuclear Regulatory Commission (U.S. NRC) has approved an alternative method through a commercial grade item dedication based on EPRI TR-106439 [1].

As mentioned in EPRI TR-106439, to utilize a commercial digital equipment as a basic component (i.e., a safety-related equipment), the critical characteristic of "dependability" should be verified for the commercial equipment via the commercial grade survey of supplier (method 2 mentioned in the EPRI NP-5652 [2]). However, licensees considered the commercial grade survey to be a license burdensome, and manufactures were reluctant to be surveyed. As one of the solutions, U.S. nuclear industry stated an introduction of 3rd party safety integrity level (SIL)-based certification system instead of the commercial grade survey of supplier [3].

In this paper, we introduce the 3rd party SIL-based certification system for evaluating the dependability critical characteristic of commercial digital equipment and a brief overview of IEC 61508 standard.

2. Dedication of Commercial Digital Equipment

2.1 Relevant Regulatory and Technical Standards

According to KINS regulatory guides, i.e., KINS/RG-N8.13 [4] and KINS/RG-N17.12 [5], the dedication of commercial digital equipment needs to meet the requirement/guideline as below.

- KEPIC ENB 6370, clause 5.4.2 "Qualification of existing commercial computers" [6] (equivalent with IEEE std. 7-4.3.2-2003 [7])
- EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Application" (1996)

Dedication is an acceptance process undertaken to provide reasonable assurance that a commercial grade item accepted for use as a basic component will perform its intended safety function [1]. For this, the NRC has endorsed EPRI TR-106439 as an acceptable method for dedicating commercial grade digital equipment for use in nuclear power plant.

2.2 Dedication Process for Commercial Digital Equipment

As shown in Figure 1, the dedication process for commercial digital equipment can be simply divided into two steps: 1) technical evaluation process and 2) acceptance process.

First, the technical evaluation needs to identify the safety function of commercial digital equipment, and the critical characteristics also. The types of critical characteristics can be included such as physical, performance and dependability characteristics. Specially, "Dependability" is a unique type of critical characteristic that existing only in the digital equipment. Moreover, the dependability attributes (such as reliability, built-in quality and configuration control, etc.) cannot be verified through inspection and testing alone, and these are generally affected by the process used to produce the digital equipment.

Second, through the acceptance process, the acceptance criteria for each critical characteristic are verified with the combination of 4 methods proposed in EPRI NP-5652, i.e., (1) special tests and inspections (2) commercial grade survey of supplier (3) source verification (4) acceptable supplier/item performance record. However, no one method will suffice by itself. For many digital equipment, methods of (1), (2) and, (4) will be needed all.

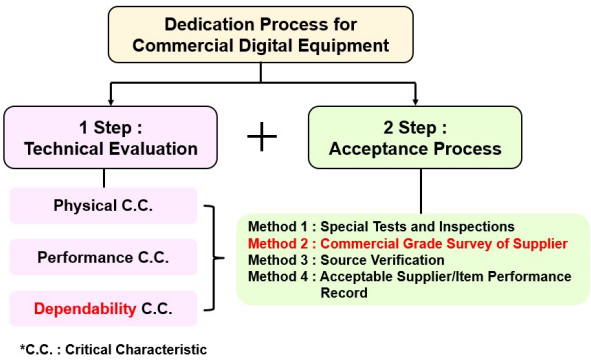

Fig. 1. Dedication process for commercial digital equipment.

3. Introduction of SIL-based Certification System

Among four acceptance methods above, the commercial grade survey of supplier (method 2) is germane to the verification of "dependability" critical characteristic. However, licensees have been considered the commercial grade surveys as a license burdensome and manufactures has been reluctant to be surveyed. Moreover, there has been a lack of standardized procedures and practices for survey. To handle these problems, the NRC is now considering an introduction of 3rd party SIL-based certification system through the modernization plan of digital I&C regulatory infrastructure based on SECY-16-0070 [3].

3.1 Framework of the SIL-based Certification System

The SIL certification process involves manufacture producing a digital equipment in accordance with IEC 61508, the 3rd party certification body (CB) reviewing the efforts of manufacture, and an accreditation body (AB) verifying the 3rd party CB's review practices, as shown in Figure 2 [8].

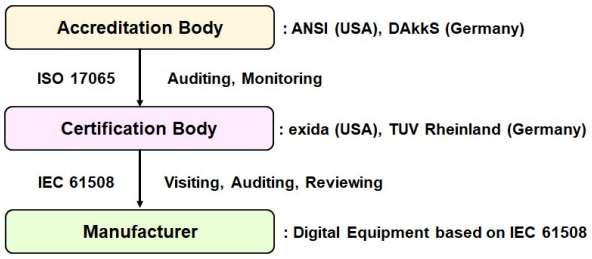

Fig. 2. Organization of SIL-based certification system

The CB proceeds to evaluate the documentation, manufacturer, and product to determine whether the requirements of IEC 61508 have been met for the desired SIL. The roles of the CB include visiting & auditing the manufacturer's design and manufacturing facilities, reviewing design documentation and so on. The CBs that primarily perform this type of work are the exida in the USA, TUV Rheinland in Germany, etc.

To maintain the role of certifier, the CB is accredited by the national AB in accordance with ISO 17065. The AB performs auditing and monitoring the CB's activities in order to confirm that their processes and procedures, and their corresponding implementation follows ISO 17065 [8]. The ABs include the DAkkS in Germany, and the ANSI in the USA, and so on.

3.2 Overview of IEC 61508

IEC 61508 is an international standard for the "functional safety" of electrical, electronic, and programmable electronic equipment. This standard consists of 8 parts including "Part 0: Functional safety and IEC 61508" [9]. IEC 61508 is based on two fundamental concepts: the safety lifecycle and safety integrity levels [8].

- Safety lifecycle, which uses (1) probabilistic, performance-based system analysis and design to minimize random failures and (2) an engineering process to minimize systematic faults (resulting from design and documentation errors)
- SILs, which are used to implement a graded approach to achieving functional safety with respect to both random and systematic failures

The SILs 1~4 correspond to orders of magnitude of risk reduction. For the specific, SIL 4 has the highest level of risk reduction with the great rigor and the most requirements. On the contrary, SIL 1 has the lowest level of risk reduction with the least rigor and the fewest requirements. Most equipment certifications are done to SIL 3 or SIL 2. The SIL table for low demand mode of operation (PFD_{avg}) is shown in Table I.

Table I: Average probability of a dangerous failure on demand of the safety function (PFD_{avg}) according to SIL

SIL	PFD_{avg}
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

3.3 Consideration on Application of SIL-based Certification System

As mentioned above, the NRC is now considering the introduction of SIL-based certification system. In domestic, it is also necessary to review the application of SIL-based certification system to improve the reliability of commercial digital equipment and enhance the regulatory efficiency. For this, related regulatory studies are needed from various perspectives as below.

- Possibility to establish an ecosystem for 3rd party SIL certification process; if the domestic nuclear industry wants to introduce a SIL-based certification system
- Development of regulatory guidelines and/or related procedures; if the domestic nuclear industry intends to use the commercial digital equipment which is SIL-certified in abroad
- If not, another plans need to be considered such as introduction of a new certification system or utilization of the existing method (i.e., commercial grade survey of supplier).

4. Conclusions

For the safety-related digital equipment, the NRC has approved an alternative method through a commercial grade item dedication based on EPRI TR-106439.

However, in verifying the "dependability" critical characteristic, licensees considered the commercial grade survey to be a license burdensome, and manufactures were reluctant to be surveyed. To solve these problems, the NRC is now considering the introduction of SIL-based certification system via the modernization plan of digital I&C regulatory infrastructure based on SECY-16-0070.

In domestic, it is necessary to review the application of SIL-based certification system to improve the reliability of commercial digital equipment and enhance the regulatory efficiency. To do that, related regulatory studies are needed with a variety of perspectives.

ACKNOWLEDGEMEMT

This work was supported by the Nuclear Safety Research Program through the Korea Foundation Of Nuclear Safety (KoFONS) using the financial resource granted by the Nuclear Safety and Security Commission (NSSC) of the Republic of Korea. (No. 2106005).

REFERENCES

[1] TR-106439, Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications, EPRI, 1996.
[2] NP-5652, Guideline for the Utilization of Commercial Grade Items in Nuclear Safety Related Applications, EPRI, 1988.
[3] SECY-16-0070, Integrated Strategy to Modernize the Nuclear Regulatory Commission's Digital Instrumentation and Control Regulatory Infrastructure, U.S. Nuclear Regulatory Commission, 2016.
[4] KINS/RG-N8.13, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants, 2018.
[5] KINS/RG-N17.12, Quality Verification for Alternating of CGIs in Nuclear Safety-Related Application, 2015.
[6] KEPIC ENB 6370, Digital Computers in Safety Systems of Nuclear Power Generating Stations, 2010.
[7] IEEE Std. 7-4.3.2, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, 2003.
[8] NEI 17-06, Guidance on Using IEC 61508 SIL Certification to Support the Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Related Applications, Nuclear Energy Institute, Revision B, 2019.
[9] IEC 61508, Edition 2.0, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, International Electrotechnical Commission, 2010.