Transactions of the Korean Nuclear Society Spring Meeting
Jeju, Korea, May 18-19, 2023

Analysis of General Requirements for Introducing IEC International Standards into the Domestic Nuclear Digital I&C Systems

Youngmi. Kim*, Hoon-Keun Lee and Sungbaek Park
Korea Institute of Nuclear Safety, 62 Gwahak-ro, Yuseong-gu, Daejeon, Korea, 305-338
*Corresponding author: ymkim@kins.re.kr

1. Introduction

In most countries, the regulatory basis is based on the regulatory laws and requirements of the U.S.NRC or IAEA standards. The domestic digital I&C system's reliability related regulatory system consists of related guidelines and IEEE technical standards endorsed by each regulatory guideline based on IEEE Std 603-1991 referenced in 10 CFR 50.55(a)h of U.S. NRC. Currently, NRC is making efforts to harmonize the IEC technical standards based on the IAEA safety standards with the NRC technical standards. Also, NRC is considering endorsement of IEC technical standards that are being used as international standards for reorganizing digital I&C infrastructure.

In this paper, general requirements of IEC and IEEE-based technical standards of domestic digital I&C systems are compared and analyzed to derive matters to be considered when introducing IEC technical standards to domestic digital I&C systems.

2. Background

2.1 Safety Standard Systems for Nuclear I&C

IEEE is an organization created by experts in the fields of electricity, electronics, and computers, and performs activities such as sharing related technologies and writing standards. NPEC is one of the Technical Committees (TCs) of the IEEE Power & Energy Society. NPEC scope covers all nuclear power related technical and standards writing activities within the IEEE, and so far developed more than 50 nuclear-related standards, including IEEE Std 603.

IEC international standards reflect the global consensus of thousands of technical experts delegated by their countries to participate in the IEC. The IEC TC45 Technical Committee is establishing international standards relating to electrical and electronic equipment and systems for instrumentation specific to nuclear applications. The IEC TC45 operates two technical subcommittees (SCs), SC45A, "instrumentation, control and electrical power system of nuclear facilities" and SC45B, "radiation protection instrumentation".

2.2 Endorsement of Regulatory Body for use of Standards

US NRC has a system that reviews and endorses industrial standards including IEEE standards to be applied to nuclear facilities through regulatory guidelines. Software-related standards (e.g., IEEE Std 1012, etc.) developed by IEEE Software Engineering Standards Committee not covered by IEEE NPEC have been endorsed for use with exceptions for application to the nuclear I&C systems.

On the other hands, IEC is composed of standardized institutions representing each country and voting rights of IEC standards shall be held by one institution or one organization in one country. IEC standards are developed to meet the criteria of IAEA safety requirements (i.e., No. SSR-2/1) and safety guidelines (i.e., No. SSG-39), but it does not mean approval for use by each national regulatorory body[1][2]. The IAEA just sets out the direction and purpose of the development of IEC standards. For the specific, if the IEC standards are to be used in the design of nuclear facilities, their applicability must be reviewed and approved for use by the country's regulatory body.

2.3 General Requirements of IEEE and IEC

IEEE Std 603 establishes minimum functional and design criteria for the power, instrumentation and control portions of nuclear power plant safe systems. In addition, IEEE Std 7-4.3.2 extends the criteria of IEEE Std 603 and establishes minimum functional and design requirements for digital computers intended to be used as equipment for nuclear plant safety systems. The IEEE Std 603 and IEEE Std 7-4.3.2 describe technology-oriented criteria for specific issues such as single failure criteria, independence, quality, and common cause failures, etc. IEEE Std 603 has the disadvantage of having to be revised when the I&C structure or application technology is changed such as FPGA, EDD, and so on.

IEC 61513 addresses technology-neutral standards, as one of top-level standards, covering step-by-step general requirements for the safety life cycle of nuclear power plant I&C systems. Thus, it does not need to revise the related IEC standards due to the changes in digital I&C structures or digital technologies [3].

3. Considerations for Digital I&C Systems in Introducing IEC Technical Standards

3.1 Application of IAEA Safety Requirements and Safety Guides

The IAEA establishes a development program for IAEA safety standards, which makes it systematically possible to develop safety standards after drafting, reviewing member states, and meeting experts. The hierarchy of safety standards consists of the following.

- fundamental safety principles: safety concepts, goals, and basic principles
- safety requirements: the basic requirements for the implementation of safety assurance
- safety guides: recommendations, conditions or procedures that meet safety requirements
- safety reports, etc.: glossary of terms, TECOCs, safety and INSAG reports, etc.

When comparing the IAEA safety standard system with the domestic nuclear safety law, the fundamental safety principles, safety requirements, and safety guides are corresponding to the level of the Atomic Energy Act, the Regulation on Technical Standards (for Nuclear Reactor Facilities, etc.), and regulatory guides of KINS, respectively. Noting that IAEA safety requirements and safety guides are used as basic inputs for the development of IEC standards. Thus, when introducing IEC technical standards, the application of IAEA safety requirements and safety guides should be considered from the perspective of general requirements of digital I&C systems within the domestic nuclear safety legislation system.

3.2 Application of IEC Technical Standards

IEC standards are based on IAEA No. SSR-2/1 and IAEA No. SSG-39, and these can be generally divided into four levels. The first level presents the general requirements at the top level, and the second level is the standard at the specific system level. Then, the third level is the standard for a particular device level, and the fourth level is the technical reports on a specific subject.

IEC 61513 is a first level standard that sets out the general requirements of I&C Systems Critical to Nuclear Safety. When introducing IEC standards, the application of them at the system-level and device-level, including IEC 61513, should be considered in terms of general requirements for digital I&C systems.

In the case of IEC international standards, there is no regulatory body that endorses the use of standards, such as NRC, so when the IAEA presents safety requirements and safety guidelines, the IEC usually presents detailed guidelines for implementation in I&C designs based on those safety guidelines.

To use IEC standards in the design of domestic nuclear digital I&C systems, domestic regulatory body needs to review their application and approve their use.

3.3 Classification of Safety Grade

The purpose of safety grade classification is to identify safety-critical structures, systems and devices based on the safety importance of their functions and to apply appropriate design and quality assurance requirements according to relevant laws, licensing commitments and operator procedures.

When introducing IEC technical standards for the construction and operation of domestic nuclear power plants, the following matters shall be considered in terms of safety grade classification[4].

- Principles and methods for classification of safety grades
- Target systems according to safety grade classification
- Applied design requirements, etc. according to safety grade classification

3.4 Considerations in terms of the Digital I&C General Requirements

3.4.1 Quality

For IEEE standards, the quality of the digital I&C system is based on the criteria in IEEE Std. 603 and 7-4.3.2. Specially, for software quality, it is utilized the related standards in the field of software engineering. For IEC standards, the quality of digital I&C systems is based on the criteria of IAEA No. SSG-39 and IEC 61513.

Since the IEEE standards-based software engineering standards are not developed solely in consideration of the digital I&C system of nuclear power plants, their contents are vast and difficult to understand and apply. On the other hand, for IEC standards, the quality of the software applies IEC 60880 to digital I&C systems that perform Category A functions, and IEC 62138 to digital I&C systems that perform Category B and C functions.

The applicability of these IEC standards is considered more useful than IEEE standards because they provide specific criteria only for nuclear facilities. To use IEC's quality related I&C standards, domestic regulatory body should review the suitability of nuclear power application in domestic.

3.4.2 Commercial Grade Item Dedication

IEC international standards dealing with qualification of existing commercial digital devices have not yet been developed. However, IAEA No. SSG-39 briefly deals with the contents of software tools. IEC 60880 and IEC 62138 address software tools with Category A features and Category B & C features, respectively. On the other hand, IEC 62671 deals with the criteria for the selection and use of industrial digital devices of limited functionality for important to safety I&C systems of nuclear power plants. However, the approach method in IEC 62671 is completely different from those of IEEE Std 7-4.3.2 and EPRI TR-106439. Thus, in order to use IEC standards, domestic regulatory body needs to specifically consider the issue of dedication of commertial grade items.

3.4.3 Defense-in-Depth and Diversity

For the case of IEEE standards, in the IEEE 7-4.3.2-2016, which has not been endorsed yet by KINS, Section 5.16 presents common cause failure criteria, and its Appendix B addresses defense-in-depth and diversity (D3) analysis. However, KINS/GE-N001 App. 7-16 addresses D3 for digital I&C systems. For the case of IEC standards, IEC 61513, Appendix C, describes a qualitative defense against common cause failures, and IEC 62340 sets out requirements for common cause failure response in I&C systems that are critical to safety.

The IEEE standard requires D3 analysis, including qualitative assessments, as well as quantitative assessments reflecting the purpose of NRC BTP 7-19 with respect to common cause failure defense in the digital I&C system. On the other hand, IEC standards focus on independence between I&C systems that perform various safety functions within Category A with the same safety objective, i.e. independence between I&C systems that perform Category B functions as backups for Category A functions. In addition, the focus is on defense measures such as independence between multiple channels of the same I&C system. Noting that IEC and IEEE are developing consensus standards (i.e., JPT IEC/IEEE 63160) that address the analysis and diversity of common cause failures in digital I&C systems. Thus, in order to use IEC standards, domestic regulatory body needs to specifically consider issues of D3 analysis against common cause failures in digital I&C systems.

3.4.4 Design and Performance Issues

Unlike analog designs, digital based I&C systems should further consider equipment qualification, real-time performance, online and periodic test features, communication independence, human engineering, and cyber security considerations, including EMC, in the design. Followings are some of considerations from the perspective of equipment qualification, real time performance, and cyber security.

Based on IEEE 323, the IEEE standard has issued approximately 20 standards covering the qualification of a number of specific devices. However, in the case of IEC, no standards have been issued to address the qualification of specific equipment. For the specific, the related IEC standards include IEC 60780 for electrical equipment qualification and IEC 60980 for seismic qualification. Thus, it is necessary to establish a regulatory position on them.

IEEE standards and domestic regulatory documents provide specific details on real-time deterministic performance, but IEC standards refer to real-time performance, focusing on problems caused by communication. To use IEC standards, real-time timing analysis of digital I&C systems should be considered to ensure deterministic performance.

Finally, the IEEE standard provides security criteria from the perspective of secure development and operating environment (SDOE), while the IEC standard covers the establishment and management of security programs, implementation of security standards according to life cycles, and security management systems. It looks like that the IEC standards cover a wider range of fields than the IEEE standards. To use IEC standards, it is required for the domestic regulatory to assess the step-by-step criteria for SDOE from the cyber security perspective of digital I&C systems.

4. Conclusions

In this study, the gap between of the I&C system regulatory requirements of IEEE-based domestic nuclear power plants and the IEC technical standards in terms of the general requirements was analyzed, and considerations were drawn when introducing IEC technical standards related digital I&C in Korea.

When introducing IEC standards, it is necessary to consider applying of them, including IEC 61513, at the system-level and device-level from the perspective of general requirements of digital I&C systems. For this, general requirements for digital I&C systems should be considered from the perspective of quality, commercial grade item dedication, defense-in-depth & diversity, and design & performance related issues such as equipment qualification, real-time performance, online and periodic test characteristics, communication independence, human engineering, and cyber security.

The results of this study will be used to set the regulatory position when the IEC technical standards are introduced in the design of domestic digital I&C systems in the future.

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. 2106005). Also, I would like to thank B. R. Kim, a retired employee of KINS, for his help in writing the thesis.

REFERENCES

[1] IAEA Specific Safety Requirements No. SSR-2/1, “Safety of Nuclear Power Plants: Design,” January 2012
[2] IAEA Specific Safety Guide No. SSG-39, “Design of Instrumentation and Control Systems for Nuclear Power Plants,” International Atomic Energy Agency, 2014.03.21
[3] IEC 61513, “Nuclear power plants - Instrumentation and control important to safety - General requirements for systems,” International Electrotechnical Commission, 2011
[4] Y. M. Kim, “Analysis of Safety Classes Classification Criteria for I&C Systems on NPP, ” Transactions of the KNS Spring Meeting, 2022