Analysis of IEC 61508 based-SIL Certification Process for Application of Commercial Grade Digital Equipment in Nuclear Power Plants

Hoon-Keun Lee, Yongil Kwon, Sungbaek Park, Youngmi Kim*
Korea Institute of Nuclear Safety, 62 Gwahak-ro, Yuseong-gu, Daejeon 34142
**Corresponding author: ymkim@kins.re.kr*

1. Introduction

Due to the obsolescence of existing nuclear facilities, many nuclear power plant (NPP) operators around the world have been interested in applying digital technologies to the existing system and equipment. The digital technology can provide lots of advantages such as the enhancement of safety, operability and reliability in NPPs. However, the number of suppliers providing safety-related digital equipment has been decreased continuously due to the saturation of nuclear industry growth. To handle this problem, the United State Nuclear Regulatory Commission (U.S. NRC) approved a commercial grade item dedication based on EPRI TR-106439 which provides the guidance on how to evaluate and accept commercial grade digital equipment (CGDE) for nuclear safety application [1]. After that, as a part of modernization plans (MP) for digital I&C infrastructure (i.e., MP #3: Acceptance of Digital Equipment) [2], U.S. NRC recently issued regulatory guide (RG) 1.250 to supplement existing guidance [3]. This RG endorses Nuclear Energy Institute (NEI) 17-06 technical report which provides the guidance on how to use IEC 61508 based safety integrity level (SIL) certification in lieu of a commercial grade survey (CGS) to verify dependability critical characteristics [4].

In this paper, we introduce the SIL certification process based on IEC 61508 for evaluating the dependability critical characteristics of commercial digital equipment. In addition, we also present the attributes of dependability in EPRI TR-106439 and its comparison results of dependability verification methods between in EPRI TR-106439 and IEC 61508 for nuclear applications.

2. IEC 61508 based SIL Certification Process

To determine acceptability of the dependability critical characteristics of CGDE during the dedicating process, the CGS of supplier is considered as an appropriate method (i.e., method 2 in NP-5652 [5]). However, there has been a lack of standardized procedures and practices for CGS. Moreover, manufactures were reluctant to be surveyed due to intellectual property. As a result, licensees have been considered the CGS as a license burdensome. To manage these problems, the NRC introduced the 3rd party SIL certification process based on IEC 16508 in nuclear industry field.

2.1 Architecture of SIL Certification System

In the SIL certification process, there are basically involving three entities such as original equipment manufacturer (OEM), certification body (CB) and accreditation body (AB) as shown in Fig. 1 [6].

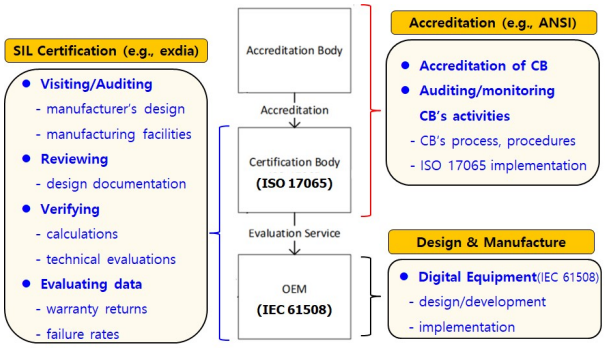

Fig. 1. Architecture of IEC 61508 based SIL certification system

The OEM proceeds the design/development/ implementation of digital equipment to be SIL-certified with target SIL (i.e., SIL 1~4) in accordance with IEC 61508. Usually, those OEMs have their own quality programs certified to ISO 9001 or similar that can apply IEC 61508 to their products [6]. Thus, once the OEM has completed the design of the digital equipment/establishment of the manufacturing processes, they will collect evidence of their compliance with the desired SIL based on IEC 61508 into a safety case. This safety case contains the evidence of meeting the reliability goals and the systematic capability requirements, typically including a Functional Safety Management plan, Safety Description, Validation Test Plan, Software Development Process, Failure Analysis and Safety Manual and so on [5]. Then the OEM delivers this safety case to a certification body (CB) for the evaluation of their efforts.

Next, the CB is reviewing the OEM's efforts by evaluating the safety case to determine whether the requirements of IEC 61508 have been met for the desired SIL. In specific, these activities include visiting/auditing the OEM's design and manufacturing facilities, reviewing design documentation and so on. The CBs that performing these activities are Exida in the USA, TUV Rheinland and TUV SUD in Germany.

On the other hand, these CBs accredited by the AB to be established as a credible entity in accordance with ISO 17065, which has the title of "Conformity

assessment – Requirements for bodies certifying products, processes and services" [7]. For this, the national AB performs auditing and monitoring the CB's activities including their review practices, processes & procedures, and their corresponding implementation follows ISO 17065. Those ABs are the ANSI in the USA and the DAkkS in Germany, etc.

2.2 Framework of IEC 61508

IEC 61508 is an international standard with the title of "Functional safety of electrical, electronic, and programmable electronic (E/E/PE) equipment" [8]. It provides a generic approach for all safety lifecycle activities for systems comprised of E/E/PE elements that are used to perform safety functions (including software). In addition, it adopts a risk-informed approach by which the safety integrity requirements can be determined according to desired target SILs. This standard consists of 7 parts (i.e., IEC 61508-1~7), which include the development process to incorporate measures to assure both systematic integrity and reliability.

In short, the IEC 61508 is based on two fundamental concepts, i.e., the safety lifecycle and safety integrity levels [8].

• Safety lifecycle

- Provision of probabilistic, performance-based system analysis and design to minimize random failures
- Adopting of an engineering process to minimize systematic faults (resulting from design and documentation errors, etc.)

• Safety integrity level

- Using to implement a graded approach (SIL 1~4) to achieving functional safety with respect to both random and systematic failures
- Types of failure probability for SIL according to the mode of operation: probability of failure per hour (PFH, high demand mode), average probability of dangerous failure on demand (PFD_{avg}, low demand mode)

The SIL correspond to orders of risk reduction magnitude and probability of failure on demand. For the specific, SIL 4 (or SIL 1) requires the highest level of risk reduction with the great rigor/the most requirements (or vice versa). Most equipment certifications are focusing on SIL 3 or SIL 2 [6]. Table I shows the low demand mode of operation (PFD_{avg}) according to the safety integrity levels [4].

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

SIL	Risk Reduction Factor	Average probability of failure on demand (Low Demand Mode of Operation)
4	100,000 to 10000	$10^{-5} \leq PFD_{avg} < 10^{-4}$
3	10,000 to 1,000	$10^{-4} \leq PFD_{avg} < 10^{-3}$
2	1,000 to 100	$10^{-3} \leq PFD_{avg} < 10^{-2}$
1	100 to 10	$10^{-2} \leq PFD_{avg} < 10^{-1}$

3. Comparison Results of Commercial Grade Survey and IEC 61508-based SIL Certification Process

To utilize the SIL certification process as an alternative method of commercial grade survey, it is helpful to understand the attributes of dependability critical characteristic and compare its verification methods between EPRI TR-106439 and IEC 61508.

3.1 Dependability Attributes in EPRI TR-106439

The term of "dependability" is defined as a broad concept incorporating various characteristics of digital equipment, including reliability, safety, availability, maintainability, and others in EPRI TR-106439 [1]. Specifically, it addresses attributes that are generally affected by the process used to produce the CGDE. Thus, it typically cannot be verified through inspection and testing alone. In addition, this term is also used to describe the relation to quality and likelihood of failures in NEI 01-01 [9]. These facts reflect that a qualitative assessment (including the design process and system design features, etc.) is required for CGDE to verify the dependability characteristics. Typical examples of the dependability attributes are as follows.

- **Reliability**: This attribute is related to the required functionality of CGDE. Acceptance criteria for reliability/availability/maintainability should be derived from the requirements of the intended applications such as numerical criteria with the specific demonstration methods (e.g., hardware reliability prediction or statistical analysis of failure rate data from field experience)
- **Built-in Quality:** Built-in quality is closely related to the quality of design & design review processes (software lifecycle, verification & validation, etc.). The acceptance criteria are based on the nuclear quality assurance program, i.e., 10 CFR 50 Appendix B. For the judgement of equivalent quality, the following lists can be considered.
  - Design & design review processes
  - Design documentation /configuration management
  - QA program and practices
  - Software requirements and its traceability
  - Failure mode and effect analysis (FMEA)
  - Qualifications & experience of personnel involved
  - Operating history for intended applications
  - Testing by the vendor or dedicator, etc.
- **Configuration control & traceability**: This attribute is entirely germane to the operating history of CGDE. To provide sufficient information for use of operating history, not only the configuration of CGDE (e.g., version of hardware/software/firmware) but also the problem reporting must be managed and traced. For example, the CGDE has to be traced back to the documents reviewed to find out related information.

For the case of problem reporting, it is necessary to establish an appropriate reporting process including coverage, timeliness, reporting to the related organization/department, and so on.

3.2 Verification methods in EPRI TR-106439

This section introduces the verification methods of each dependability attributes, e.g., reliability, built-in quality and configuration control & traceability referred in EPRI TR-106439 [1].

• **Reliability**
- Review vendor's reliability calculation and testing methods including its results.
- Review operating history data.
- Review and assess design.
- Perform reliability analysis.

• **Built-in Quality**
- Reviews of vendor processes & documentation including design/development/verification processes and QA/V&V programs and their practices
- Design reviews
  · Architecture/code reviews, walkthroughs, use of analytical techniques, etc.
  · Failure analysis at the system level including the CGDE itself
  · Comparison of device's failure modes to needs of the application

• **Configuration control & traceability**
- Review of operating history for intended applications.
- Configuration control
  · Review configuration management program and its practices of venders.
  · Examine actual practices and its records.
- Problem reporting
  · Review vendor's problem reporting procedures and its practices.
  · Assess previous performance record
- Assess maintainability of dedication.

3.3 Verification methods in SIL certification process

For the comparison with the verification methods in Section 3.2, we also present the related methods of each dependability attributes referred in IEC 61508 [8] and ISO 17065 [7].

• **Reliability**
- Numerical criteria are established by IEC 61508 in terms of PFH or PFD_{avg} according to the operation mode. For SIL certification, these failure rates must be calculated and satisfy target SIL requirements as shown in Table I (IEC 61508-2, Section 7.4.5).

• **Built-in Quality**
- The IEC 61508 provides the safety lifecycle for system (IEC 61508-2, Section 7.4.6) and software (IEC 61508-3, Section 7.4) including configuration management.
- CB's review process including the safety case (IEC 61508-2, Section 7.4.6; IEC 61508-3, Section 7.4; ISO 17065, Section 7)
- AB's review process (ISO 17065, Section 7)
- Self-diagnostics to detect dangerous failures and force the equipment to a safe state (IEC 61508-2, Section 7.4.7 & 7.4.8)
- Defect reporting (IEC 61508-2, Section 7.8.2.2)
- SIL Certification Aging (ISO 17065, Section 7.7)

• **Configuration control & traceability**
- As mentioned in the Section 6.2.6 of IEC 61508-1, "Procedures shall be developed for ensuring that all detected hazardous events are analyzed, and that recommendations are made to minimize the probability of a repeat occurrence". Thus, field failure data based on this requirement could inform the reliability determination such as PFH or PFD_{avg}.

Those comparison results indicate that the technical content of SIL certification encompass what is needed to replace CGS for the verification of dependability. The comparison matrix of dependability verification methods between in EPRI TR-106439 and IEC 61508 are summarized in Fig. 2.

Attributes		Verification Method in TR-106439	Verification Method in IEC 61508
Reliability & Maintainability	• Related to the required function • **Numerical criteria** for reliability/maintainability	• Review reliability calculation/testing method and result • Review operating history data	• Numerical criteria with PFH, PFDavg (IEC 61508-2)
Built-in Quality	• Quality of design • Quality of manufacture • Failure management • Compatibility with operators, maintainers	• Review of vendor processes and documentation • Design Review	• IEC Safety Lifecycle • CB's review process (IEC 61508-2, 3) • AB's review process (ISO 17065, Sec. 7) • Self diagnostic • Fail safe technique • SIL Certification Aging (ISO 17065)
Configuration control & traceability	• Hardware • Software • Firmware • Problem reporting	• Review of product operating history • Configuration control • Problem reporting	• Defect reporting • Operating history (field failure data for PFH, PFDavg)

Fig. 2. Comparison matrix for dependability critical characteristic between EPRI TR-106439 and IEC 61508.

4. Conclusions

IEC 61508 is an international, performance-based standard for the functional safety of E/E/PE equipment that addresses standardization issues raised by the use of programmable electronic systems [2]. The functional safety standards based on IEC 61508 are being rapidly adopted by many manufacturers in various industries such as railway application (EN 50128), automotive (ISO 26262), process industry (IEC 61511) and so on.

Recently, the U.S. NRC has issued an additional regulatory guidance to leverage the 3rd party SIL certification process based on IEC 61508 for CGDE, through the RG 1.250. It endorses the NEI 17-06 report that addressing how to use SIL certification process

instead of a commercial grade survey to verify dependability critical characteristics. According to the NEI 17-06, the technical contents of a SIL certification encompasses what is needed to substitute the CGS for the verification of dependability as shown in Fig. 2 [4].

Thus, it is expected that the introduction of IEC 61508 based SIL certification can provide a significant improvement in the verification of dependability for CGDE in nuclear power plants. Those comparison results in Section 3 will be used as a background information to develop domestic regulatory positions for the dedication of commercial digital equipment based on SIL certification in nuclear power plants.

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] RG 1.250, Dedication of Commercial-grade Digital Instrumentation and Control Items for Use in Nuclear Power Plants, U.S. Nuclear Regulatory Commission, 2022.
[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] 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 1, 2021
[5] NP-5652, Guideline for the Utilization of Commercial Grade Items in Nuclear Safety Related Applications, Electric Power Research Institute, 1988.
[6] EPRI report No. 3002011817, Safety Integrity Level (SIL) Certification Efficacy for Nuclear Power, Electric Power Research Institute, 2019.
[7] ISO/IEC 17065, Conformity Assessment-Requirements for Bodies Certifying Products, Processes, and Services, International Organization for Standardization, 2012.
[8] IEC 61508, Edition 2.0, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, International Electrotechnical Commission, 2010.
[9] NEI 01-01, Guideline on Licensing Digital Upgrades EPRI TR-102348 Revision 1, Nuclear Energy Institute & Electric Power Research Institute, 2002.