Review Process for Safety Related Digital Instrumentation and Control System

Y. S. Cho[a*], H. S. Park[a], M. Y. Kim[a]
[a]*Instrumentation and Control Department, Korea Institute of Nuclear Safety(KINS), Daejeon, Korea*
[*]*Corresponding author: yscho@kins.re.kr*

1. Introduction

The safety related digital I&C systems have been fully adapted in nuclear power plants since Shin kori 3&4 nuclear power plants. Even though the digital technology provides improvements of performance and reliability, the use of digital based safety related I&C systems has been accompanied by new safety issues. The important issues to be reviewed in licensing process of those are qualification of digital I&C systems and components, defense in depth and diversity, software life cycle process, and commercial-grade digital equipment, etc. The review process for those issues are discussed in this paper.

2. Review Process for Digital I&C Systems

In this section, the review process for main topics of safety related digital I&C systems are described. The review process described below is taken from and have reference to the Safety Review Guidelines for Light Water Reactors [1].

2.1 Quality of Digital I&C Systems and Components

The safety related digital I&C systems and component shall be designed, fabricated, installed, tested, and inspected in accordance with the safety classes and standards commensurate with the importance of the safety functions to be performed [2].

One of the important factors of analog systems is that analog systems show continuous performance and the performance can be predicted over substantial ranges of input conditions. This factor allows extensive use of testing such as type testing of design outputs in qualifying the design of analog systems and components. However, digital I&C systems are fundamentally different from analog I&C systems. For example, the digital equipment has the higher functional density than analog equipment, and a multifunction microprocessor-based module can substitute many analog modules. Because of these characteristics of digital equipment, minor errors in design and implementation step of digital I&C systems can cause unexpected behavior. Therefore, the performance of digital systems over the entire range of input conditions cannot generally be inferred from testing at a sample of input conditions. Inspection, type test and acceptance test of digital I&C systems and component do not alone accomplish design qualification of high confidence level.

Consequently, digital I&C systems require additional design and qualification approaches that are typically employed for analog systems. The approach to the review of design qualification for digital I&C systems focuses to a large extent on confirming that applicant or licensee employed a high-quality development process that incorporated disciplined specification and implementation of design requirements. Inspection and test are used to verify correct implementation and to validate desired functionality of the final product but the conviction that isolation and intermittent faults will not occur is in the strict development process.

2.2 Defense in Depth and Diversity

In the case of adoption of software based digital equipment, the design concepts of defense-in-depth and diversity including manual functions shall be applied to the design of the digital I&C systems in order to assure the implementation of safety functions required at a common cause failure of software [3].

In general, the digital I&C systems have the characteristics of sharing components such as code, data transmission, data and hardware compared to analog I&C systems. Although this characteristic provides many advantages to the digital I&C systems, it also raises a key concern, common cause failure. In other words, the design of shared data or code has the potential to propagate a common-cause failure through software errors or software developed logic, which could defeat the redundancy achieved by the hardware architecture because identical copies of the software based logic and architecture are present in redundant division or channels of safety related I&C systems. Because of this concern, the review of digital I&C systems emphasizes defense in depth and diversity as protection against the propagation of common cause failures within and between digital I&C systems. As a result of reviews of advanced light-water reactor, the following four-point position on defense in depth and diversity for new reactor designs and for digital I&C system modifications to operating plants.

Point 1. The applicant shall assess the defense-in-depth and diversity of the proposed digital I&C system to demonstrate that vulnerabilities to common cause failures have adequately been addressed.

Point 2. In performing the assessment, the vendor or applicant shall analyze each postulated common cause failure for each event that is evaluated in the accident analysis section of safety analysis report using best estimate methods. The vendor or applicant shall demonstrate adequate diversity within the design for each of these events.

Point 3. If a postulated common cause failure could disable a safety function, then a diverse means with a documented basis that the diverse means is unlikely to be subject to the same common cause failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.

Point 4. A set of displays and controls located in the main control room shall be provided for manual, systems level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from safety computer system identified in point 1 and 3 above.

2.3 Software Life-cycle Process

The development of safety system software should progress according to a formally defined life cycle. No specific life-cycle model is required. However, a software life-cycle typically includes activities related to planning, requirements, design, implementation, integration, validation, installation, and operation and maintenance. The software developer should select and document the software life-cycle, and specify the products that will be produced by that life-cycle.

The review process for software in digital I&C systems includes following items, such as software life-cycle process planning, implementation, and design outputs.

The review of software life-cycle process plans confirms that the specified software development process requirements documented in the plans establish a commitment to an effective and disciplined software development process and implementation.

The review of software life-cycle process implementation confirms that the software development process conforms that requirements described in the plans and safety analysis, verification and validation, and configuration control activities are conducted adequately.

The review of software life-cycle process design output confirms that functional requirements are traceable through all intermediate design products to the final product. The review of design outputs also confirm that the software development process characteristics and the required software functional characteristics are present.

2.4 Commercial Grade Digital Equipment

Nuclear power plants are replacing or upgrading their existing analog based I&C systems with software based commercial digital equipment, because of improvement of its availability and potential performance and reliability. However, the use of commercial digital equipment for safety related I&C systems has been occurred new licensing issues, including the potential for common cause failure, electromagnetic interference, and the adequacy of the supplier's software development process and documentation.

The digital equipment, including software that is applied to safety system computers must be qualified for the intended applications. Qualification may be established either by nuclear grade quality assurance program or by commercial grade item dedication (CGID).

The review for CGID requires a determination that a suitable acceptance process provide reasonable assurance that a commercial grade item will perform its intended safety function and it is deemed equivalent to an item designed and manufactured under nuclear grade quality assurance program.

EPRI NP-5652 provides guidance on CGID and defines the basis process for CGID: a technical evaluation of "critical characteristics for acceptance," and use of any of four acceptance methods to verify the characteristics. The four methods are (1) Special Tests and Inspections, (2) Commercial Grade Survey of Supplier, (3) Source Verification, (4) Acceptable Supplier/Item Performance Record [4].

For many digital equipment, methods 1, 2, and 4 will be needed [4].

Engineering judgment applied in the acceptance process must be documented sufficiently to allow a comparable qualified individual to reach the same conclusion. The validity of the commercial grade item dedication must be maintained as along as the item remains in service. Dedicated software items should not be updated to new revision levels without prior evaluation to determine if a design change is required. Commercially dedicated items should not be operated in a configuration outside the bounds of the original dedication.

3. Conclusions

The safety related digital I&C systems have been fully implemented in nuclear power plants since Shin kori 3&4 nuclear power plants. As software based digital equipment is used for safety related I&C systems, new licensing issues arose. This paper briefly described the review process for main issues of safety related digital I&C systems, including qualification of digital I&C systems and components, defense in depth and diversity, software life cycle process, and commercial-grade digital equipment.

REFERENCES

[1] Safety Review Guidelines for Light Water Reactors, KINS/GE-N001.

[2] Nuclear Safety Laws of the Republic of Korea, Regulations on Technical Standards for Nuclear Reactor Facilities Etc., Article 12(Safety Classes and Standards).

[3] Nuclear Safety Laws of the Republic of Korea, Regulations on Technical Standards for Nuclear Reactor Facilities Etc., Article 26(Protection System).

[4] Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications, EPRI TR-106439.