Regulatory Experiences of Digital Upgrade in Domestic Nuclear Power Plants

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

1. Introduction

The nuclear licensee has upgraded existing instrumentation & control (I&C) system and/or equipment because of the growing problems of obsolescence, difficulty in procuring analog replacement parts and increased maintenance costs. Moreover, due to the limitation on the market growth of nuclear industry, the number of suppliers providing the safety-related equipment (accordance to 10 CFR 50, Appendix B) is steadily decreasing.

Typically, these upgrades are based on the changes from analog to digital technology. The digital technology can provide lots of advantages such as performance and reliability improvements. However, the digital I&C systems have a possibility to present potential vulnerabilities such as failures due to increased complexity of digital systems and the introduction of coding errors, common cause failure(CCF) and so on [1].

To handle this problem, NRC has approved a guideline on digital I&C upgrade process (referred as NEI 01-01[2]). In this guideline, it is emphasized on the necessity of failure analysis and dependability assessment.

In this paper, we present several digital upgrade cases in domestic nuclear power plants to enhance the regulatory background of digital I&C upgrades.

2. Cases of Digital Upgrade of Domestic Nuclear Power Plant

2.1 Digital Upgrade of Plant Protection System in Kori Unit 1 Nuclear Power Plant

2.1.1 Overview

Digital upgrade of plant protection system in Kori unit 1 nuclear power plant was the first case of replacing analog facilities to digital based facilities. The purpose of this digital upgrade is to enhance the reliability and safety of nuclear power plant by replacing the analog-based plant protection system and control system to digital facilities. The improvement of digital facilities was to replace existing analog modules of Foxboro, H-Line, to microprocessor-based equipment, SPEC 200 Micro and SPEC 200 input/output modules. The changed digital-based facilities should meet regulatory requirements (10 CFR 50.55a(h), IEEE Std. 603[3], etc.) and should not affect other systems that were not changed. Although digital equipment was changed, some analog type input/output modules were retained without replacement to guarantee diversity in case of vulnerable to CCFs.

2.1.2 Evaluation results

The plant protection system of Kori unit 1 shall be designed to maintain the plant variables with the allowable limits set by the design basis accident with accuracy and reliability as a safety system.

The updated digital protection system was assessed conformity of applied technical standards such as IEEE Std. 603 and IEEE Std. 7-4.3.2, suitability of software quality assurance (process planning, execution, document and etc.) and suitability of defensive design against CCFs and so on. Following are some of the evaluation results of the issues.

- Conformity of applied technical standards

Criteria in IEEE Std. 603 were checked whether it satisfies design requirements such as single failure criteria, quality, operation of fail-safe in case of failure, test & calibration capability and access control. Also, for digital design, conformity was verified in accordance with IEEE Std. 7-4.3.2 endorsed by RG 1.152.

- Defensive design against CCFs

According to TMI (Three Mile Island) action plan, there are post-accident monitoring instrumentations in case of Condition Ⅱ (moderate frequency events), Ⅲ (infrequent events) and Ⅳ (limiting faults) accident events that need to manual action by the operator. Six variable signals passing through the non-safety (NSSS Control System) require to transmit directly to the main control room (MCR).

As a result of analyzing the defense in depth and diversity of CCFs for Condition Ⅱ, Ⅲ and Ⅳ accident events in chapter 15 of FSAR (Final Safety Analysis Report), the events identified as vulnerable to CCFs were retained to same analog type instrumentation instead of replaced with digital facilities.

Among the events that require various protection functions, the events that do not satisfy the requirements of at least two protection layers are “uncontrolled boron dilution” and “excessive heat removal due to failure of the main feedwater system”.

2.2 Digital Upgrade of Diverse Protection System in Hanul Unit 5,6 Nuclear Power Plants

2.2.1 Overview

The DPS (Diverse Protection System) prepares for possibility of ATWS (Anticipated Transient Without Scram) that does not occur reactor trip despite of the condition that the reactor should be shutdown. The DPS generates reactor trip signal and auxiliary feedwater supply actuation signal in accordance with 10 CFR 50.62.

The components of inside control cabinet were replaced for PLC (Programmable Logic Controller)-based equipment to FPGA (Field Programmable Gate Array)-based equipment, and other systems were not changed.

2.2.2 Assessment results

The new FPGA-based DPS has been identified as the conformity of requirements related to the DPS and suitability of the structure and logic of DPS, HW/SW design and environmental qualification and so on Followings are some of the evaluation results.

- Design requirement and composition DPS

Although DPS is non-safety system, it should be designed by applying concept of defense in depth and diversity. It applies FPGA-based DPS system to secure diversity with the existing PLC-based nuclear reactor protection system. Therefore, there were no changes to the design of defense in depth and diversity. The DPS uses same input/output signals and operation logic as before.

- HW/SW design

The FPGA-based HW consisted of two channels with hot-standby controller structure. It was designed to shut off the DPS signal and generate and alarm when a fault is occurred to prevent abnormal operation (reactor shutdown, auxiliary feedwater actuation). A manual bypass switch was installed to prevent similar case of reactor shutdown during period test of ASTS (Automatic Seismic Trip System) in Hanbit unit 2.

The software (ITS, Important to Safety) for DPS operation and maintenance test software (ITA, Important to Availability) were confirmed that life cycle activities were properly performed such as development, verification and validation (V&V) and test according to IEEE Std. 1012[5].

2.3 Digital Upgrade of Rod Control System

2.3.1 Overview

The DRCS (Digital Rod Control System) is equipment that insert, withdraw and hold by supplying power to the CEDM (Control Element Drive Mechanism). Since it consisted of single structure, a failure might result in an unplanned reactor shutdown. There have been more than 17 times reactor shutdown since 1995.

To improve reliability and maintainability of system, digital upgrade of the system proceeded to replace analog equipment with digital-based redundant equipment in all nuclear power plants. In order to reduce the unexpected reactor shutdown due to equipment failure, redundant double hold rod control systems were applied. It was designed to automatically supply holding current to movable gripper coil and stationary gripper coil to prevent to drop the rod due to the power failure.

2.3.2 Assessment results

The DRCS is non-safety system, it is required to apply suitable requirements such as software V&V, environmental qualification, EMC (Electromagnetic Compatibility) test, power and power cable capacity, physical and electrical independence.

- SW V&V

The ITA software is installed for moving and holding of rod, generating alarm in logic cabinet and power cabinet. It confirmed that life cycle activities were properly performed according to IEEE Std. 1012.

The rod control system is a non-safety (quality class A) that does not require safety function and is not need to environmental qualification. However, in order to confirm reliability, the environment test was performed to check function and performance according to IEEE Std. 323[6].

- Rod falling time measuring

The falling time of rod is the time specified in 3.1.5.3 of the Technical Specification, it should be periodically calibrated in accordance with KEPIC (Korea Electric Power Industry Code) QAP (Quality Assurance Program)-1 requirement 12. However, it was confirmed that the calibration procedure was not prepared, therefore it was requested to prepare a periodic calibration procedure.

2.4 Digital Upgrade of Flow Meter Type Change in Hanbit Unit 3,4 Nuclear Power Plants

2.4.1 Overview

The flow meter of charging pump outlet header installed in Hanbit unit 3,4 should satisfy the KEPIC MOB 4812 measurement range that is requirements related to required measuring range of instrumentation during the in-service test. During the 16th periodic inspection of Hanbit unit 3, a inspection finding report was issued. It was a design change that meets the KEPIC MOB 4812 by changing analog flow meter to digital flow meter for ensuring the reliability of in-service test.

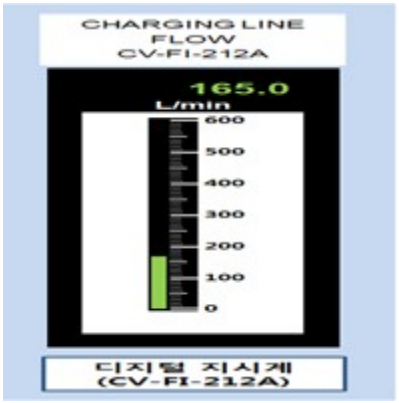

Figure 1. Digital flow meter

2.4.2 Assessment results

The new digital flow meter has been evaluated the conformity of the applied technical standards, suitability of the software V&V, environmental qualification, and so on. Followings are some of the results of the evaluations.

- SW V&V

The software used in digital recorders, it was verified that documents were developed by applying appropriate procedures and techniques at each phase of development. The software confirmed that 3'rd party independent verification was performed and that the regulatory requirements for each stage of development were satisfied.

- Environmental qualification

The digital recorders are installed in the MCR and operate in a mild environment. To verify the design life, EQ tests were conducted with a verification life of six years in the normal operation environment of the device with the shortest life span. As a result, it was confirmed that the replacement cycle was six years based on the 40 ℃ usage.

- Measuring range and precision of digital flow meter

The analog and digital flow meter during in-service test should meet KEPIC MOB 4812 that is maximum range of analog flow meter should not be greater than 3 times the reference value, reference value of digital flow meter should not exceed 70% of the calibration value.

The maximum range of existing analog flow meter is 3.3 times the reference value (maximum range: 600 lpm, test reference value: 165~180 lpm), it did not satisfy KEPIC MOB 4812. But, the replaced digital flow meter satisfies KEPIC MOB 4812 that the reference value should not exceed 70% of the calibration value (0~600 lpm). It also was confirmed that the accuracy of the digital indicator was 0.25%, which was improved from that of the existing analog indicator (1%).

3. Conclusion

As the nuclear power plant facilities are obsolete and discontinued, it is becoming increasingly difficult to secure replacement. The digital system different from analog system should consider CCFs, environmental qualification, EMC, real-time performance, periodic test, physical and electric independence and so on. In order to secure reliability and safety of digital system, technical standard and problems to be newly considered were checked through the regulatory experiences of domestic nuclear power plants. These digital upgrades will continue to increase and it should be assessed by appropriate standards and criteria.

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] SECY-16-0070, "Integrated Strategy to Modernize the Nuclear Regulatory Commission's Digital Instrumentation and Control Regulatory Infrastructure, U.S. Nuclear Regulatory Commission", 2016.
[2] NEI 01-01, "A Revision of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule", 2002
[3] IEEE Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations"
[4] 10 CFR 50.62, "Requirements for Reduction of Risk from Anticipated Transients Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants:, 1996
[5] IEEE Std. 1012-2004, "IEEE Standard for Software Verification and Validation"
[6] IEEE Std. 323-2003, "Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations"