Regulatory Experience of the Embedded Digital Devices for Safety I&C Systems on Nuclear Power Plants

Y. M. Kim*, H. K. Lee, and H. S. Park
Korea Institute of Nuclear Safety, 62 Gwahak-ro, Yuseong-gu, Daejeon, Korea, 305-338
Corresponding author: ymkim@kins.re.kr

1. Introduction

Conventional I&C(Instrumentation & Control) systems are tend to becoming unavailable and being replaced by smart equipment. These smart equipment is usually called embedded digital devices (EDDs) or industrial digital devices of limited functionality[1-2]. Usually, some of these devices are found embedded in plant equipment such as sensing instrumentation, motors, pumps, actuators and breakers. They typically have a micro-processor, RAM, communication interface, a power source, etc. The U.S. Nuclear Regulatory Commission (US NRC) is concerning that these EDDs might exist in procured equipment used in safety systems without the devices having been explicitly identified in procurement documentation[1]. Also, they have not been developed specifically for use in nuclear power applications[3].

This paper addresses the regulatory experiences of KINS of the EDDs for safety I&C systems and the future works for them.

2. Background

US NRC is issuing regulatory issue summary (RIS) to clarify the NRC's technical position on existing regulatory requirements for safety-related equipment with EDDs. In this RIS, an embedded digital device is a component consisting of one or more electronic parts that requires the use of software, software-developed firmware, or software-developed programmable logic, and that is integrated into equipment to implement one or more system safety functions [1].

MDEP (Multi-national Design Evaluation Programme) and IEC 62671 use the term "industrial digital device of limited functionality" instead of EDD. The definition of the term is as follows [2-3] :

- The device is a pre-existing digital device that contains pre-developed software or programmed logic (e.g. an hardware description language programed device) and is a candidate for use in an application important to safety.
- The primary function performed is well-defined and applicable to only one type of application within an I&C system, such as measuring a temperature or pressure, positioning a valve, controlling speed of a mechanical device, or performing an alarm function.

Figure 1. Examples of Potential EDDs in NPP

3. Regulatory Experience

3.1 Regulatory Experiences of NRC

US NRC have published several information notices for events which were caused by the failure of EDDs. This section shows the survey results of the events and how they followed up.

On March 23, 2015, During Emergency Diesel Generator (EDG) loading test at the Brunswick Steam Electric Plant unit 1, EDG 3 and 4 could not have been able to tie to their respective emergency buses simultaneously for a period of 12 minutes[4]. This event was resulting from the Allen Bradley 700-RTC time delay relays installed in breaker control logic of EDGs. It was so susceptible to electrical noise from near by relays de-energizing that the output breakers could not maintain proper closing state. To solve this problem, the licensee installed the transient voltage suppressor across all four EDG relays. The design of RTC time relays was changed to use a complex programmable logic device (CPLD) instead of a solid-state integrated circuit by the manufacturer at some point. However, there was no notification for design change and modification of the part number. The licensee purchased and dedicated the relays only with a material evaluation method that relied on dimensional and configuration check. As result, the CGID process for the modified relays was failed to detect the design change.

On November 4, 1993, at Beaver Valley Unit 2 Power Station, during the test of EDG load sequencer for train A, the sequencer failed to automatically load safety-related equipment onto the emergency bus. Two

days later, the same situation was also happened for train B. Then, NRC inspection team was sent to check the circumstances of the site[5]. This problem was caused by the timer/relays in the EDG load sequencer. These timer/delays were used to load the safety-related equipment according to the designed discrete steps. It was found that the timer/relays were seriously affected by the electrical noise such as electromagnetic interference (EMI) that generated by the auxiliary relay coil. As a result, the timer/relays could not operate its safety function. To correct this problem, the licensee installed the diodes across the auxiliary relay coils. These timer/relay were replaced electro-mechanical type with microprocessor-based type in 1990. At that time, it was purchased as commercial grade items and dedicated for safety function. However, the modification design data did not identify the potential for EMI generated by another circumstances.

3.2 Regulatory Experiences of KINS

The SKN 3&4 are the first nuclear power plants in Korea which adopted safety grade smart transmitters. The safety grade smart transmitters are EDDs which have digital devices and firmware. KINS reviewed smart transmitters using IEEE Std. 7-4.3.2[6] and IEEE Std. 1012[7]. IEEE Std. 7-4.3.2 provides guidance on performing an engineering evaluation of software common cause failures, including use of manual action and non-safety-related systems, or components, or both, to provide means to accomplish the function that would otherwise be defeated by the common-cause failure. Also, SRP Appendix 7.0-A and SRP BTP 7-19 provide the additional guidance on assessment of the diversity and the defense-in-depth for the digital I&C systems.

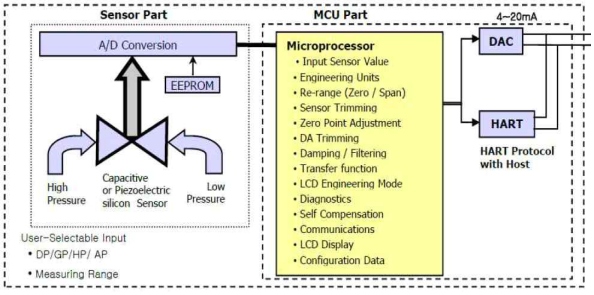

Figure.2. Basic Block Diagram of Smart transmitters

The software which was firmware of the safety grade smart transmitters must met the V&V requirements of the IEEE Std. 1012[7]. KINS reviewed the software whether it met the IEEE Std. 1012 or not. It was developed as integrity level 4 or equivalent according US NRG Reg. Guide 1.168. The equipment was qualified by IEEE Std. 323-2003.

SKN 3&4 also used digital relays for Emergency Diesel Generator (EDG). These digital relays are EDDs which contain digital devices and firmware. KINS reviewed that as commercial grade items (CGIs) which must be dedicated as the EPRI/TR-106439[8]. Also, KINS reviewed the quality assurance program, problem reporting, maintenance & troubleshooting process and operating experiences for the digital relays.

Followings are major review points for the EDDs.

- Quality and reliability (quality assurance program and V&V process)
- CCFs (Common Cause Failures) via software errors
- Electromagnetic compatibility (EMC)
- CGI dedication (procurement planning, review, test, and control, etc)

5. Conclusions and Future Works

In this paper, we showed regulatory experiences of EDDs which used for safety grade equipments. EDDs might exist in safety grade procured equipment without explicit identification. Undetected defects of EDDs might be the potential safety concerns. EDDs should meet certain specific requirements in order to be selected and used in safety I&C system.

We have plan to develop technical positions for identification and qualifying them. The technical position will address, but may not be limited to, quality and reliability, CCFs via software errors, EMC, and CGID for EDDs.

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. 1305003-0315-SB130).

REFERENCES

[1] NRC Regulatory issue summary (RIS), embedded digital devices in safety-related systems, 2016.5
[2] IEC 62671, Nuclear power plants − Instrumentation and contol important to safety − Selection and use of industrial digital devices of limited functionality, 2013.02
[3] MDEP, Generic Common Position DICWG NO7: Common Position on Selection and Use of Industrial Digital Devices of Limited Functionality, 2014.07
[4] NRC Information Notice (IN) 2016-01, Recent issues related to the commercial grade dedication of allen bradley 700-RTC relays, 2016.02
[5] NRC Information Notice (IN) 1999-20, Common-cause failures due to inadequate design control and dedication, 1994.03
[6] IEEE Std. 7-4.3.2-1993, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations
[7] IEEE Std. 1012-2004, IEEE Standard for Software Verification and Validation, 2004
[8] EPRI TR-106439, “Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications,” Electric Power Research Institute, Palo Alto, CA, October 1996