Regulatory Experience on Safety Smart Transmitter's CCF of SKN 3&4

Y.M. KIM* and C. H. JEONG
Korea Institute of Nuclear Safety, 62 Gwahak-ro, Yuseong-gu, Daejeon, Korea, 305-338
**Corresponding author: ymkim@kins.re.kr*

1. Introduction

Nuclear I&C equipments have increased the use on digital technology in safety system. The use of digital equipment may improve their reliability and reduce maintenance costs. But, it is important to review their reliability and safety and to ensure that their potential software CCF could not lead to an adverse safety consequence. Smart transmitters are digital I&C equipment which can replace analog transmitters. Non safety grade smart transmitters have been used for I&C systems of NPP(Nuclear Power Plant). But, recently, smart transmitters have been used for safety grade I&C systems as well as non-safety grade I&C system for SKN 3&4. Smart transmitters execute measuring sensor values, generating output signals and adjusting range using software. Also, smart transmitters are basically capable of remote calibration through digital communication. The operating capability is more reliable and effective with remote calibration of smart transmitters, but there is potential vulnerability that causes the result no one wanted such as cyber attacks or software CCF. This paper addresses our regulatory experiences how to evaluate safety smart transmitter's CCF of SKN 3&4.

2. Background

2.1 Smart transmitters and SKN 3&4 design status

148 EA smart transmitters for safety grade I&C systems and 333 EA smart transmitters for non-safety grade I&C systems have been used for SKN 3&4. Best benefit of the smart transmitters is network capability. Fig. 1 shows the basic block diagram of the typical smart transmitter and Table. 1 shows the main differences between analog transmitters and smart transmitters.

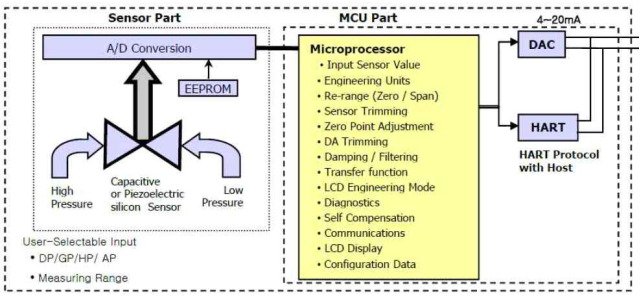

Fig. 1. Basic Block Diagram of Smart Transmitters

Smart transmitter has memory and microprocessor which can execute remote calibration with digital communication. The digital communication follows HART(Highway Addressable Remote Transducer) communication protocol.

Table. 1. Differences between Analog transmitter and Smart transmitter

Item	Analog Type	Smart Type
Measurement	H/W (100%)	S/W & H/W
Generation of output signal	H/W(100%)	S/W & H/W
Damping	H/W(100%)	S/W
Transfer	Only Linear Output	Linear or SQRT Output Select
Range adjustment	H/W adjustment	S/W adjustment
Units	appearance identification	Unit configuration using S/W

2.2 Software CCF Related Standards and Regulatory Criteria

The digital equipment which is used for nuclear I&C systems must follow the IEEE Std. 603 and IEEE Std. 7-4.3.2. IEEE Std 603-1998 refers that plant parameters shall be maintained within acceptable limites established for each design basis event in the presence of a single common cause failure[1]. And, IEEE Std 7-4.3.2-1993 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[2]. If functional diversity dose not exist, a defense-in-depth analysis should be performed to determine if diversity exists within the echelons of defense. SECY 93-087, SRM, II.Q provides regulatory positions for common-mode failures in Digital I&C Systems[3]. It says that applicant shall assess the defense-in-depth and diversity of the proposed instrumentation and control

system to demonstrate that vulnerabilities to common mode failures have adequately been addressed. KINS Regulatory Guide 8.13 refers that adequacy of the software diversity in system should be reviewed at equipment level[4]. Also, SRP Appendix 7.0-A and SRP BTP 7-19 provide additional guidance on assessment of diversity and defense-in-depth for digital I&C systems[5,6].

3. Regulatory Experiences

3.1 Concerns about Digital Characteristics

Safety grade smart transmitters have been first used in SKN 3&4. These have been reviewed as followings like other safety digital I&C systems.

- Software V&V
- Digital communication
- Cyber security
- CCFs(Common Cause Failures) via software errors
- Equipment Qualification
- Etc

The transmitters for SKN 3&4 have not been used for providing input variables for RTS or ESFAS. Only input variables from analog transmitters are used for Plant Protection System(PPS). Also, the network capability of these are not used yet. Fig. 2 shows the simple structure for signal flow of SKN3&4 input variables.

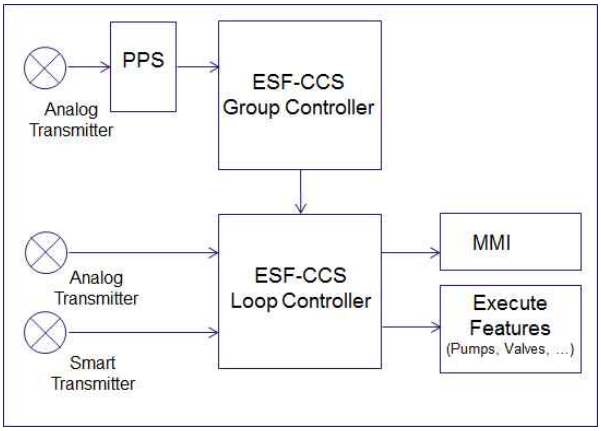

Fig. 2. Signal Flow of SKN3&4 Input Variables

In this paper, only software CCF related regulatory experiences were described.

3.2 Safety Evaluation Experience

SKN 3&4 have used same smart transmitters for safety and non-safety grade I&C systems unlike previous NPPs. Smart transmitters have microprocessor and software, so the error of software can be a potential source of CCF. It was required the answers for the several questions about smart transmitter's CCF. It was required to assess potential vulnerability that could result from software CCFs of safety grade and non-safety grade smart transmitters and to assess that these CCFs could not lead to an adverse safety consequence.

Licensee analyzed effects of smart transmitter's CCF with DBA. They assumed that protection system such as RTS and ESFAS and CPCS, PORV, ASDV, etc which did not use smart transmitters operate normally per each DBA at SKN 3&4 FSAR chater 6 and 15. They reviewed the smart transmitter's CCFs to assess what impact may have on mitigation actions and plant operation after that.

Even smart transmitter's CCFs with DBA occur, reactor protection and control system can be usable, and there are no effect on ESFAS actuations. So the plant can trip after DBA.

Depending analysis results, some smart transmitters were decided to change analog transmitters because some smart transmitter's CCF with DBA could affect operating procedures for coping with accident.

4. Conclusions

Nuclear I&C equipments have increased the use on digital technology in safety system. According that, interest in a postulated software CCF is increasing. The software may be firmware or operating system of digital equipment. During SKN 3&4 operating license process, safety grade smart transmitter's adequacy was reviewed such as software V&V processes and equipment qualification. Also, it was analyzed that effect of the software CCFs of smart transmitters under DBA condition.

Main concern was whether the postulated smart transmitter's software CCF may lead to an adverse safety consequence. We have future research plan to execute proof tests about our concerns and develop regulatory guide for smart transmitters.

REFERENCES

[1] IEEE Std. 603-2009, IEEE Standard Criteria for Safety Systems for Nuclear Power Generation Stations,
[2] IEEE Std. 7-4.3.2, IEEE Standard Criteria for Ditital Computers in Safety Systems of Nuclear Power Generating Stations, 1993
[3] U.S.NRC SECY 93-087, Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor(ALWR) Designs, 1993
[4] KINS Regulatory Guide 8.13, Use of Digital Computers for Safety System
[5]U.S.NRC SRP 0800 Appendix 7.0-A, Review Process for Digital Instrumentation and Control Systems
[6]U.S.NRC SRP 0800 BTP 7-19, Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems.