Transactions of the Korean Nuclear Society Autumn Meeting
Gyeongju, Korea, October 24-25, 2013

An Advanced Detecting Scheme against a Signal Distortion with a Smart Transmitter

JunYoung Son, Young-Mi Kim

Korea Institute of Nuclear Safety, P.O.Box 114, Yuseong-gu, Daejeon, Korea, 305-600
Corresponding author: JYSonPaperInfo@gmail.com

1. Introduction

As IT technology has been much developed, measuring nuclear I&C (Instrument & Control) systems also is going to be evolving. At this point, the smart transmitter has been developed and tried to be applied. Recently, constructed nuclear power plants in Korea have adopted the smart meters. In case of Shin-Kori unit 3, about 59 safety grade smart transmitters and about 180 non-safety grade smart transmitters are used for measuring various signals [1]. Fig. 1 shows the communication between the smart transmitter and the receiver. In the field of measuring nuclear I&C (Instrument & Control) systems, the cyber security problems can happen more. Thus, providing defense methods against possible cyber attacks are essential. In particular, the defense schemes for providing data information integrity will be essential. In addition, it is necessary to detect the analog signal distortion between the host smart transmitters and the client cabinet. In this paper, applicable one of directions and methods against the above two problems are proposed. With proposed schemes in this paper, the analog signal distortion could be detected. Also the data integrity for information security could be provided.

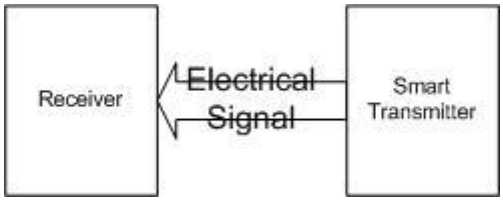

Fig. 1 Communication of Nuclear I&C System with Smart Transmitter

2. Research Background

2.1 Smart Transmitter

The smart transmitter has been adopted in the nuclear power plants system. The system has the microprocessor in order to process digital information and various useful functions. Since the microprocessor is utilized, the effective, useful, various softwares can be developed and additional. In this system infrastructure, the defense methods against cyber attacks have to be considered. The reason is that many kinds of cyber attacks have been tried and studied for the nuclear I & C system in the nuclear power plants system in the world-wide. And in the future, the cyber security problems can be more important.

2.2 Digital System Communication Security

The recent IT technology has been much developed. As the digital system has been developed, the field of information security has grown significantly in recent years. For secure from malicious cyber attacks, the information security requirements are necessary. Those elements include confidentiality, integrity, availability, authentication, non-repudiation [2]. It is essential to ensure the information data from the measuring nuclear I&C system. In this paper, applicable methods are proposed for cyber security in terms of integrity.

2.3 Analog Communication Signal Distortion

An electrical signal can be distorted in many causes of attacks and disturbances. The signal integrity is a important point of the quality of an electrical signal. In particular, the analog signal communication from the smart transmitter has to be provided with confidential integrity. In the present nuclear power I&C system, the analog signal integrity is considered. However, in the recent and future, advanced attacks and new causes of signal distortion can be tried. As the new system is applied in the nuclear I&C system, the more efficient schemes against signal distortion could be studied.

3. A Proposed Scheme

As explained in 2. Research Background, through the smart transmitter many useful softwares could be designed. Especially the software which has the secure function of verifying information integrity could be utilized. Fig 2. shows the example which has the commitment scheme for a integrity between smart transmitter and the receiver. In general, the digest and SHA algorithms are adopted for proving integrity in digital communication system. Those algorithms are able to be additional in the recent smart transmitter system. Defense schemes for integrity should get ready before converting the information into analog signal.

Using these proposed schemes, the integrity for digital information between the smart transmitter and the receiver could be provided.

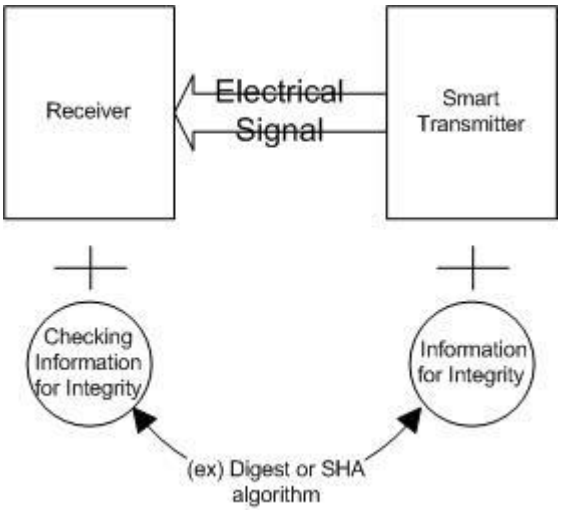

Fig. 2 Example of providing integrity in Nuclear I&C System with Smart Transmitter

Since the analog signal can be distorted, the modification of the signal must have the assurance with authorization.

4. Conclusions

The assurance of the integrity in digital information as well as analog signals is necessary. The above proposed schemes can be utilized for detecting the modification of the digital information or analog signal distortion without any of authentication. These effects have merits of the defenses for analog signals and cyber security in terms of information integrity. There are many kinds of measuring nuclear I&C system. Thus, the applicable algorithms may be different according to the lightness or the level of the security in each measuring system. In the future, finding and applying the efficient algorithms in each measuring systems in the nuclear power plant should be studied. As the I&C system will be gradually digitalized, the requirements for basic security concepts should be considered and applied.

REFERENCES

[1]Young-Mi Kim and Young-Il Kwon, “Development of Test Platform for Digitl I&C System Evaluation”, October, 2012.
[2]NIST, Engineering Principles for Information Technology Security, 2004
[3]IAEA Safety Standard Series No. NS-G-1.3, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, 2002.
[4]KINS regulatory guide 8.22, Cyber security for nuclear I&C
[4]US NRC regulatory guide 5.71, Cyber security program for nuclear facilities
[5]NUREG/CR-7006, Review Guidelines for Field-Programmable Gate Arrays in Nuclear Power Plant Safety Systems, 2009.
[6]KINS/RR-890, A Study on Evaluation Technique of Wireless Communication System for Digital I&C System, 2011.