Suggestion of a Framework to Analyze Failure Modes and Effect of Cyber Attacks in NPP

Chanyoung Lee [a], Poong Hyun Seong [a*],
[a]*Department of Nuclear and Quantum Engineering, KAIST, Daejeon Korea*
[*]*Corresponding author: phseong@kaist.ac.kr*

1. Introduction

In recent year, digital I&C systems have been developed and installed in operating nuclear power plants (NPPs). However, due to installation of digital I&C systems, cyber security concerns have been emerged. Although many standards and guidance documents have been published for cyber security management, these standards and guidance are not well suited for NPP I&C systems. There are unique specifications and characteristics in NPP I&C systems comparing to IT systems in terms of the architecture and functions [1].

One of the major problems for the nuclear industry is that cyber security measures are not designed into I&C systems from the design stage. This is due to industry's tendency to consider cyber threats to be relatively inconsequential compared to other safety and physical problems. And also the rather late adoption of digital systems has resulted in a lower level of cyber security advancements than in other industries [2]. It is essential that the control system designers take cyber security into account during the initial conceptual phase. In addition, to assist in design of the plant with high reliability and safety, it is necessary to analyze risk caused by cyber attacks.

2. Characteristics of cyber security in NPP I&C

NPP I&C systems are operated in different conditions from ICSs (Industrial Control Systems) in terms of network architectures. While ICSs are connected in general off-site corporate business systems or the Internet, NPP I&C systems have been isolated from the outside. Although NPP I&C systems generally use closed data and isolated communication networks, non-Internet cyber threats are still possible [1]. Only one track path from the outside can be expected through the EWS (Engineering Work Station) being connected to the PLCs during the maintenance and tests of them [3]. During maintenance and test activities, external devices can be connected to the CDAs (Critical Digital Assets) and may provide a path for cyber attacks [3]. Thus, performing appropriate risk analysis including cyber security for the NPPs digital I&C systems has become more important.

3. Introduction to FMEA

3.1 Performing qualitative analysis is considered for cyber security.

In the NPP I&C systems, the quantification or rating of risks caused by cyber attacks may be inappropriate and hard to validate [3]. In additions, the probability or the frequency of failures can not be obtained in cyber security problems because cyber attacks are intended and can not be predicted. With this regards, to provide the designers with an identification of the various failure modes of the parts of system and to aid in the systematic assessment of system safety, performing qualitative analysis of cyber attacks should be considered for cyber security.

3.2 Overview of FMEA method.

FMEA (Failure Mode and Effect Analysis) method is generally used as the basic step of a qualitative analysis. The FMEA is intended for the systems reliability analysis during design stages and it is devoted to the specification of failure modes, their sources, causes, criticality and influence on system's operability [4]. The results of FMEA method can be used for making priority of actions to reduce the chance of failure and for evaluation of design validation.

The basic approach to carry out an FMEA is described in Figure 1 [5].

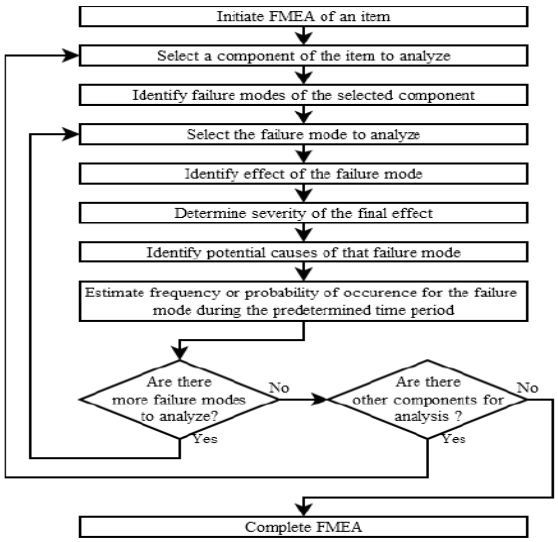

Fig.1. FMEA – analysis flow chart [5]

4. Consideration to apply FMEA to analyze failure mode and effect of cyber attacks in the nuclear industry

To apply the FMEA method for cyber security in nuclear industry, there are some further points to be considered since the cause and effect of cyber attacks on NPPs are significantly varied.

Firstly, in FMEA method, it analyzes the failure mode of each component independently and it assumed that failure of each component does not affect the other component. However, with respect to cyber security, cyber attacks affect a PLC (Programmable Logic Controller) directly causing it to malfunction, or installs malware into a PLC to expand infections to other CDAs (Critical Digital assets) in the system [3]. The FMEA method which only addresses the failures of each component independently, should be amended to analyze failures of PLCs which are dependent on each other.

Secondly, redundant channels are usually considered to be compensating provisions because failure in single channel is thought to have no effects on other channels. However, for cyber security, the original and the redundant channels should be simplified into one channel [3]. Because the redundant channels are not reliable compensating provisions in cyber security, security controls such as monitoring system, firewalls, etc. should be considered. It is necessary to investigate whether the requisite security controls are in right position. Also, adverse effect of security control should be inspected.

Thirdly, there are more diverse failure modes due to cyber attacks than failure modes of physical component. FMEA is difficult to cover diverse failure modes due to cyber attacks. In this regard, types of failure modes due to cyber attacks and system's vulnerabilities should be investigated.

Then, in order to apply FMEA method for cyber security analysis, aforementioned limitations should be considered.

5. Conclusions

One of the major problems for the nuclear industry is that cyber security measures are not designed into I&C systems from design stage. To assist design of the plant with high reliability and safety, it is necessary to analyze risk caused by cyber attacks. However, the quantification or rating of risks caused by cyber attacks may be inappropriate and hard to validate. In additions, the frequency of failures can not be obtained in cyber security problems. With this regard, qualitative analysis can be considered for cyber security. FMEA method is often the general first step of a qualitative reliability analysis. The results of FMEA method can be used for making priority of actions to reduce the chance of failure and for evaluation of design validation. However, to apply the FMEA method for cyber security, there are some limitations and further points to be considered. Therefor it is important to compensate the FMEA method for analyzing failure modes and effect of cyber attacks in NPP.

REFERENCES

[1] JG. Song, JW. Lee, CK. Lee, KC. Kwon, DY. Lee, A cyber security risk assessment for the design of I&C systems in nuclear power plants, Nuclear engineering and technology, Vol.44 No.8, pp. 919-928, December 2012.

[2] C. Baylon, R. Brunt, D. Livingstone (2015), Cyber Security at Civil Nuclear Facilities Understanding the Risks, Chatham House Report, London, U.K. (The Royal Institute of International Affairs), September.

[3] JG. Song, JW. Lee, GY. Park, KC. Kwon, DY. Lee, and CK. LEE, "An analysis of technical security control requirements for digital I&C systems in nuclear power plants", Nuclear Engineering and Technology, vol. 45, no.5, pp. 637-652, 2013.

[4] Kharchenko, V., Kovalenko, A., Andrashov, A., Siora, A. Gap-and-IMECA-based Assessment of I&C Systems Cyber Security, Complex Systems and Dependability, Advances in Intelligent and Soft Computing, pp. 149-164, 2012.

[5] IEC 60812: Analysis Techniques for System Reliability – Procedure for Failure Mode and Effects Analysis (FMEA). International Electrotechnical Commission, 2006.