Identification of the vital digital assets based on PSA results analysis

Moon Kyoung Choi [a*], Han Seong Son [b], Hyundoo Kim [c], Poong Hyun Seong [a]
[a]*Department of Nuclear and Quantum Engineering, Korea Advanced Institute of Science and Technology, 291 Daehak-ro, Yuseong-gu, Daejeon 34141, Republic of Korea*
[b]*Department of Computer and Game, Joongbu Univiersity, 201 Daehak-ro, Chubu-myun, Geumsan-gun 32713, Republic of Korea*
[c]*Cyber Security Division, Korea Institute of Nuclear Nonproliferation and Control, 1534 Yuseong-daero, Yuseong-gu, Daejeon 34054, Republic of Korea*
[*]*Corresponding author: stsk9107@kaist.ac.kr*

1. Introduction

As the main systems for managing totally about the operation, control, monitoring, measurement, and safety function in an emergency, instrumentation and control systems (I&C) in nuclear power plants have been digitalized gradually for the precise operation and its convenience [1]. However, these changes have some problems in terms of security. The digitalization of infrastructure makes systems vulnerable to cyber threats and hybrid attacks. According to ICS-CERT report, as time goes by, the number of vulnerabilities in ICS industries increases rapidly. Recently, due to the digitalization of I&C, it has begun to rise the need of cyber security in the digitalized I&C in NPPs.

However, there are too many critical digital assets (CDAs) in NPPs. More than 60% of the total critical systems are digital system. Addressing more than 100 security controls for each CDA needs too much effort for both licensee and inspector. It is necessary to focus on more significant CDAs for effective regulation [2]. Probabilistic Safety Analysis (PSA) results are analyzed in order to identify more significant CDAs which could evoke an accident of NPPs by digital malfunction or cyber-attacks. By eliciting minimal cut sets using fault tree analyses, accident-related CDAs are drawn. Also the CDAs that must be secured from outsiders are elicited in case of some accident scenario.

It is expected that effective cyber security regulation based on the graded approach can be implemented. Furthermore, defense-in-depth of digital assets for NPPs safety can be built up.

2. Elicitation of accident-related CDAs

Event tree analysis based on initiating events is conducted, and minimal cut sets using fault tree analysis are elicited. CDAs related to NPPs accidents and initiating events are derived by analyzing PSA results about internal events.

2.1 Steps for deriving accident-related CDAs

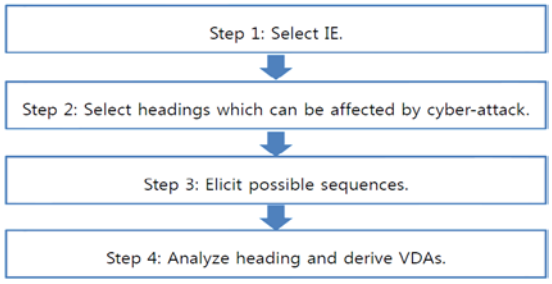

Fig. 1. Steps for deriving accident-related CDAs

Fig. 1 indicates the steps for deriving CDAs related to accidents in NPPs. First, various initiating events are selected, and then headings which can be affected by cyber-attacks or digital malfunction are selected. Third, possible sequences are elicited and finally CDAs related to accidents are derived. It is hard to handle all the accidents and situation so major cases which account for frequency of accidents and incidents.

2.2. Selection of headings which can be affected by cyber-attack or digital malfunction

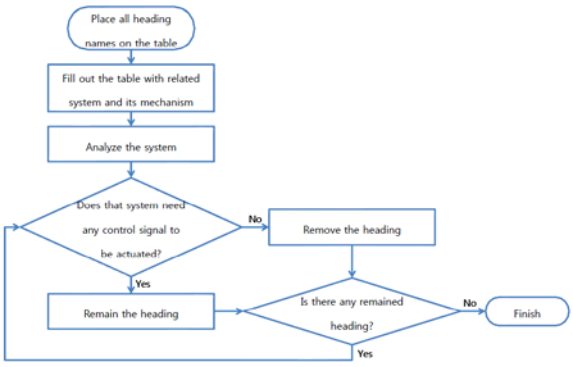

Fig. 2. Selection of headings which can be affected by cyber-attack or digital malfunction

For each initiating events, all heading names are placed on table, and then the table is filled out with related system and its mechanism. Some headings are not related to digital signals because they are caused by material, structural problem or because of its mechanism. The systems according to various events are analyzed whether the systems need any digital control signals to be actuated or not.

2.3 Elicitation of possible sequences

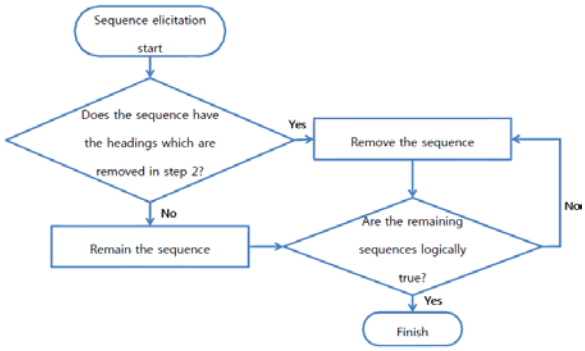

Fig. 3. Elicitation of possible sequences

For elicitation of possible sequences, the derived sequences can be logically affected by digital problems. Some sequences are unrealistic so those are removed. Through this step, logically realistic sequences are elicited.

2.4 Analysis of headings and derivation of accident-related CDAs

Analyses of derived headings and sequences are conducted. Based on PSA results about internal events, accident-related CDAs are elicited. Those must be secured from digital malfunction when accidents or incidents occurs in NPPs. Additionally, some digital components which can be affected by outsiders are also considered.

3. Conclusions

Digital technologies such as computers, control systems, and data networks currently play essential roles in modern NPPs. Further, the introduction of new digitalized technologies is also being considered. These digital technologies make the operation of NPPs more convenient and economical; however, they are inherently susceptible to problems such as digital malfunction of components or cyber-attacks [3]. Recently, needs for cyber security on digitalized nuclear Instrumentation and Control (I&C) systems are increased. However, there are too many digital assets in NPPs so it is hard to regulate them effectively. In this study, accident-related CDAs are elicited based on PSA results about internal events. It is expected that this study can contribute to effective cyber security regulation and that Graded approach for CDAs can be possible.

REFERENCES

[1] Y.D. Kang, “A study on Cyber Security Assessment Methodology of Instrumentation & Control Systems for Nuclear Power Plants”, Ph.D. thesis, 2011
[2] I.H. Shin, “ROK’s Regulatory Framework for Cyber Security of Nuclear Facilities”, KNS,2016
[3] W.G. Ahn, “Development of Cyber-Attack Scenarios for Nuclear Power Plants Using Scenario Graphs”, International Journal of Distributed Sensor Networks, Vol 2015, pp.12, 2015

Acknowledgement

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 (Grant code: 1605007-0116-WT111)