Perspective on Secure Development Activities and Features of Safety I&C Systems

Youngdoo Kang [a*], Yeong Jin Yu, Hyungtae Kim, Yong il Kwon,
Yeunsoo Park, Jaeyul Choo, Jun young Son, Choong heui Jeong [a]
[a]*Korea Institute of Nuclear Safety, 62 Gwahak-ro, Yuseong-gu, Daejeon*
[*]*Corresponding author: Y.Kang@kins.re.kr*

1. Introduction

The Enforcement Decree of the Act on Physical Protection and Radiological Emergency (ED-APPRE) was revised December 2013 to include security requirements on computer systems at nuclear facilities to protect those systems against malicious cyber-attacks. It means Cyber-Security-related measures, controls and activities of safety I&C systems against cyber-attacks shall meet the requirements of ED-APPRE. Still regulation upon inadvertent access or non-malicious modifications to the safety I&C systems is covered under the Nuclear Safety Act.

The objective of this paper is to propose KINS' regulatory perspective on secure development and features against non-malicious access or modification of safety I&C systems.

2. Understanding of Secure Development Activities and Features

This section is for the understanding of secure development activities and secure features with comparing the cyber security aspect. And this section also covers KINS' regulatory perspective and position following to the changes of regulatory environment.

2.1 Changes of Regulatory Environment

KINS' regulatory guide 8.22 was developed July 2011 to describe the regulatory position on the cyber security of safety I&C systems with the goal of ensuring the Safety of nuclear facilities. Basically, this guide covers cyber security activities against malicious cyber-attacks and also non-malicious access to the systems. Cyber-attacks are malicious act that target critical digital assets with the intent of altering or destroying, and cyber security refers to measures and controls against cyber-attacks. In comparison, secure development activities and features aim to prevent inadvertent and non-malicious access, and to prevent unwanted action from personnel or connected systems for ensuring reliable operation of safety I&C systems.

The Enforcement Decree of the Act on Physical Protection and Radiological Emergency (ED-APPRE) require licensees to develop programmatic cyber security provisions for high assurance against cyber-attacks. And the scope of KINS' regulation is decided to cover non-malicious and inadvertent access, i.e., regulation on secure development activities and features, for ensuring reliable operation of safety I&C systems.

2.2 Secure development activities and features

Secure development activities of safety I&C systems are life cycle activities to ensure unwanted, unneeded and undocumented code is not incorporated into the systems. Vulnerability assessment for secure development environment shall be performed to identify potential challenges during development life cycle phases to exclude possibilities of inclusion of unwanted, unneeded and undocumented code. Strict verification and validation (V&V) and configuration management (CM) for safety I&C systems, e.g., software requirement traceability matrix (RTM), configuration control of implemented source codes, may be useful to prevent introduction of unwanted and undocumented requirements and code into the systems.

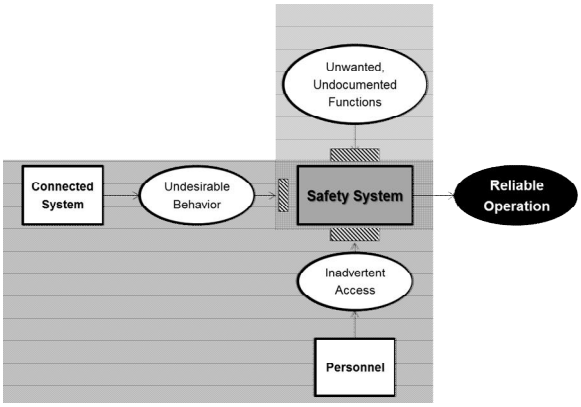

Fig. 1. Secure development activities and features

Secure features of safety I&C systems are not designed against cyber-attacks. Those may selected through vulnerability assessment at the early phase of development. Independence or isolation of safety I&C systems, software integrity checks, correlation check function of setpoint between redundant channels, or 'cabinet door open alarm' function are acceptable methods for secure features of safety I&C systems. Once those secure features are identified as a system design requirements or software requirement e.g., software based Cyclic Redundancy Check for application program, those secure features shall be developed, verified and qualified throughout the development life cycle. In that secure features are for

the reliable operation of safety I&C systems against inadvertent access or non-malicious modification, those may helpful to prevent and detect cyber-attacks during operation.

2.3 Cyber security measures for safety I&C systems

Cyber security measures, such as intrusion detection or protection systems, are generally implemented at nuclear facilities to protect against cyber-attacks that may compromise safety. Safety measures and cyber security measures for a nuclear power plant should be designed and implemented so that they do not compromise one another [3]. Table I is the 5-position of MDEP DICWG about impact of Cyber Security Features (CSF) on digital I&C safety systems. Those common positions are based upon Safety-Security Interface principle. It means cyber security features shall be implemented not to compromise safety, and KINS' position on CSFs is on the same side.

Table I: Common Position of MDEP DICWG (CP-08)

1	CSF should not adversely impact the performance, effectiveness, reliability or operation of safety systems
2	CSF directly in the safety system should be avoided when practical
3	Where CSF need to be implemented, they should not adversely impact the operator's ability to maintain the safety of the plant
4	Where CSF need to be implemented, adequate measures should be taken to ensure that CSF do not adversely affect the ability of a system
5	CSF included in safety systems should be developed and qualified to the same level of qualification as the systems CSF reside in

2.4 Regulatory Perspective

KINS regulatory guide 8.13 provides staff's position about secure development and operational environment for the safety I&C systems. KINS will revise this guide to include more detailed regulatory position including safety-security interface principle such as the guide on impact analysis of CSFs. And for the reason that ED-APPRE address cyber security requirements of nuclear facilities, KINS regulatory guide 8.22, Cyber security of I&C systems, which is will be repealed in conformity with Nuclear Safety Act.

KINS will review secure development activities from the early phase of development life cycle, and will evaluate the secure features through the review of new reactor licensing and periodic inspection of operating plants.

3. Conclusions

Secure development activities and features aim to prevent inadvertent and non-malicious access, and to prevent unwanted action from personnel or connected systems for ensuring reliable operation of safety I&C systems. Secure development activities of safety I&C systems are life cycle activities to ensure unwanted, unneeded and undocumented code is not incorporated into the systems. Secure features shall be developed, verified and qualified throughout the development life cycle.

KINS will revise regulatory guide 8.13 to include more detailed regulatory position on secure development activities and features. KINS regulatory guide 8.22, which addresses cyber security, will be repealed.

REFERENCES

[1] KINS Regulatory Guide 8.13, Utilization for Digital Computers of Safety Systems, 2014
[2] NRC Regulatory Guide 1.152, Rev.3, Criteria for use of computers in safety systems of nuclear power plants, July 2011
[3] MDEP Common Position, No. DICWG-08, Common Position on the Impact of Cyber Security Features on Digital I&C Safety Systems, Dec 2012

ACKNOWLEDGEMENT

This work was supported by the Nuclear Safety Research Program through the Korea Radiation Safety Foundation(KORSAFe), granted financial resource from the Nuclear Safety and Security Commission(NSSC), Republic of Korea (No. 1305003)