Development Methodology of a Cyber Security Risk Analysis and Assessment Tool for Digital I&C Systems in Nuclear Power Plant

K. H. Cha, C. K. Lee, J. G. Song, Y. J. Lee, J. Y. Kim, J. W. Lee, and D. Y. Lee
Korea Atomic Energy Research Institute
1045, Daedeok-Daero, Yusong, Daejon, 305-600, Republic of KOREA
{khcha, cklee1, jgsong, yjlee426, jykim, leejw, dylee2}@kaeri.re.kr

1. Introduction

With the use of digital computers and communication networks the hot issues on cyber security were raised about 10 years ago. The scope of cyber security application has now been extended from the safety Instrumentation and Control (I&C) system to safety important systems, plant security system, and emergency preparedness system [1]. Therefore, cyber security should be assessed and managed systematically throughout the development life cycle of I&C systems in order for their digital assets to be protected from cyber attacks. Fig. 1 shows the concept of a cyber security risk management of digital I&C systems in nuclear power plants (NPPs). A lot of cyber security risk assessment methods, techniques, and supported tools have been developed for Information Technology (IT) systems, but they have not been utilized widely for cyber security risk assessments of the digital I&C systems in NPPs. The main reason is a difference in goals between IT systems and nuclear I&C systems. Confidentiality is important in IT systems, but availability and integrity are important in nuclear I&C systems. Last year, it was started to develop a software tool to be specialized for the development process of nuclear I&C systems. This paper presents a development methodology of the Cyber Security Risk analysis and Assessment Tool (CSRAT) for the digital I&C systems in NPP.

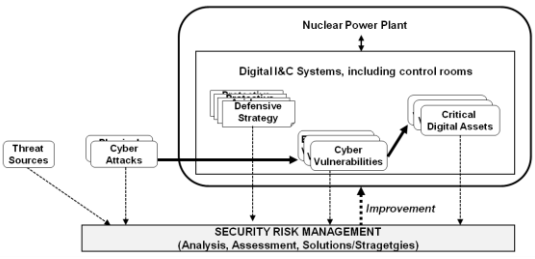

Fig.1. Concept of a cyber security risk management of digital I&C systems in NPP.

2. Development Methodology

The CSRAT is a software system to assist developers or cyber security assessors of nuclear digital I&C systems. The CSRAT provides a lifecycle-based framework for identifying, analyzing, and assessing various cyber threats and vulnerabilities of the digital I&C systems in NPPs. Requirements of the CSRAT are based on the nuclear cyber security codes and standards including regulatory guides. Fig. 2 shows the development methodology of CSRAT for cyber security risk analysis and assessments of the digital I&C systems in NPPs.

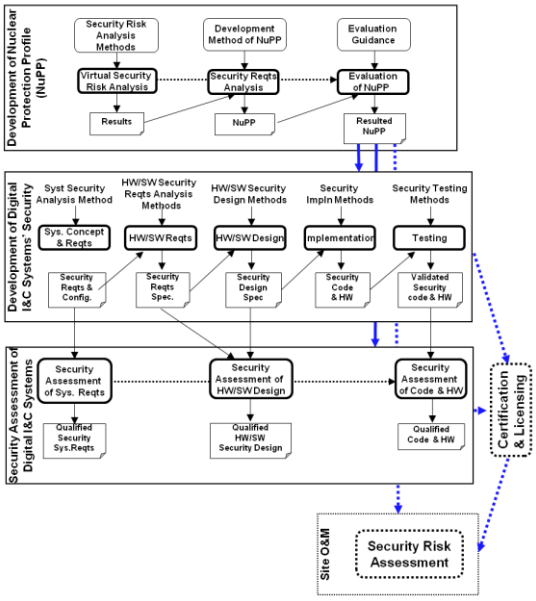

Fig.2. Development methodology of CSRAT.

2.1 Nuclear Protection Profile (NuPP)

Cyber security requirements, called Nuclear Protection Profile (NuPP) [3], can be derived from the cyber security codes and standards for nuclear I&C systems, industrial control systems, and IT systems. Fig. 3 shows the cyber security codes and standards for the development of NuPP.

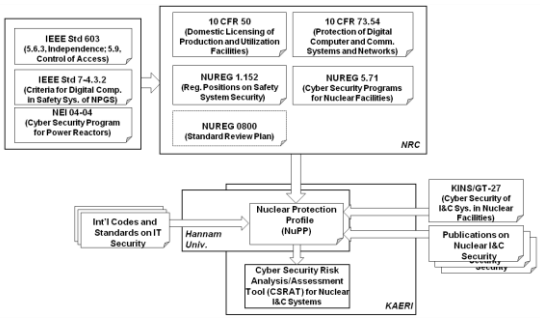

Fig.3. Nuclear codes and standards for NuPP.

The NuPP being developed with the analysis and evaluation processes defined in Fig. 2 is used for a design requirement of CSRAT.

2.2 Definition of cyber security life cycle process and its tasks

A CSRAT process was defined by considering a reference model for a development of digital I&C systems [5]. The CSRAT activities, in compliance with the cyber security requirements mentioned in section 2.1, will be performed during the system design phase, the hardware (HW) / software (SW) design phase, and the validation phase. Fig. 4 shows the cyber security life cycle process and CSRAT activities.

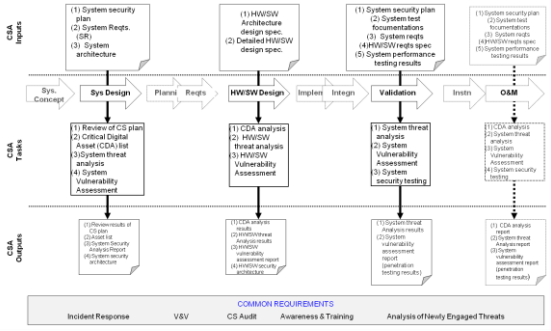

Fig.4. Definition of cyber security life cycle process and its tasks for CSRAT.

At the system design phase, the CSRAT provides the software-implemented functions for identifying Critical Digital Assets (CDAs) [8], analyzing data flows in cyber security aspects, analyzing threats, and assessing their vulnerabilities. All of the safety-graded digital equipment and I&C systems, operating procedures, and human operators are regarded as CDAs in the CSRAT. If any cyber vulnerability in the system design is found from this activity, the CSRAT presents strategies or solutions for avoiding, reducing, transferring, or accepting the identified cyber vulnerability. At the HW/SW design phase, the CSRAT provides the software-implemented functions for analyzing cyber threats, and assessing the vulnerabilities of CDAs. When any cyber vulnerability is found from the cyber security risk analysis and assessment of the CDAs and development environments, the CSRAT presents the strategies or solutions for avoiding, reducing, transferring, or accepting the identified cyber vulnerability. At the validation phase, the CSRAT provides the functions for assuring cyber security of the HW/SW-integrated system, including security testing such as penetration tests. This approach at the validation phase may be applied seamlessly for the cyber security risk assessment of digital I&C systems at the operation and maintenance phase.

2.3 Others

All of digital assets, including the development environments, deliverable documents, software codes, etc., shall be controlled and managed as configuration items under a configuration management program. Especially, software security must be maintained for both the CSRAT itself and its development environment, because the CSRAT contains information important to cyber attacks.

3. Conclusions

Cyber Security Risk analysis and Assessment Tool (CSRAT) as a standalone software system, has been developed for supporting the cyber security risk analysis and assessment of the digital I&C systems in NPPs since last year. A cyber security life cycle process and cyber security assessment activities with using the CSRAT have been defined, and a development methodology of the Nuclear Protection Profile (NuPP) for the CSRAT is described. The CSRAT will a tool for supporting effectively the development of more secure digital I&C systems in NPPs.

Acknowledgement

The work has been performed with the support of the Ministry of Knowledge and Economy since 2010.

REFERENCES

[1] C. K. Lee, et al., “Cyber Secure Penetration Test for Digital Safety I&C Systems,” Transactions of the Korean Nuclear Society Autumn Meeting, p.1171-1172, Oct. 21-22, 2010, Jeju, Korea.
[2] NEI 04-04, “Cyber Security Program for Power Reactors (Draft 3),” 2004.
[3] “Cyber Security Risk Analysis and Assessment System (Seminal Material),” S.E. Research Lab., Hannam Univ, 2011.
[4] USNRC Regulatory Guide 1.152, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants,” 2009.
[5] USNRC Regulatory Guide 0800, “Standard Review Plan”
[6] IEEE Std. 7-4.3.2, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,” 2010.
[7] Y. D. Kang, et al., “Introduction of Cyber Security Assessment Methodology for the I&C Systems in Nuclear Facilities,” Proceedings of NPIC&HMIT 2010, p.992-1000, Nov. 7-11, 2010, Las Vegas, Nevada.
[8] USNRC Regulatory Guide 5.71, “Cyber Security Programs for Nuclear Facilities,” 2010.
[9] I. N. Fovino, et al., “Cyber security assessment of a power plant,” Electric Power Systems Research 81, p.518–526, 2011.