Design Concept of CSRAS (Cyber Security Risk Analysis and Assessment System) for Digital I&C Systems

J. G. Song, J. W. Lee, D. Y. Lee and C. K. Lee*
Korea Atomic Energy Research Institute
989-111 Daedeok-daero, Yuseong-gu, Daejeon, 305-353, Republic of KOREA
**Corresponding author:cklee1@kaeri.re.kr*

1. Introduction

The instrumentation and control (I&C) systems in nuclear power plants (NPPs) have been digitalized recently. Hence, cyber security becomes an important feature to be incorporated into the I&C systems[1,2]. The Regulatory Guide 5.71 published by U.C NRC in 2010 presents a comprehensive set of security controls for the cyber security of I&C systems in NPPs[3]. However, the application of security controls specified in the RG 5.71 in a specific I&C system still requires many analysis efforts based on the understanding of the security controls, since the guideline does not provide the details to system designers or developers regarding what, where, and how to apply the security controls[4, 5].

To apply security controls to I&C systems, cyber security requirements should be identified based on the cyber security policy and program, then the design and implementation of security controls should be performed along with the I&C system development lifecycle[6, 7, 8]. It can be assumed that cyber security requirements are identified during the system design(SD) phase and the design and implementation of security controls is performed during the component design(CD) phase. When identifying security requirements and performing the design and implementation of security controls, cyber security risk assessments should be processed with the understanding of the characteristics of target systems.

In this study, the Cyber Security Risk Analysis and Assessment System (CSRAS) has been developed as a tool for analyzing security requirements and technical security controls considering based on a general cyber security risk assessment procedure with the consideration of the characteristics of I&C systems and the development phases.

2. CSRAS

2.1 The scope of CSRAS

The CSRAS is a cyber security self-assessment tool intended for the development of digital I&C systems including digital devices, network systems, and HMIs.

2.2 Assessment process of CSRAS

The assessment process of CSRAS consists of 4 steps :

1) Identification of Critical Digital Assets(CDAs),
2) Analysis of essential requirements for CDAs,
3) Vulnerability assessments, and
4) Report.

The process follows the NPP I&C development lifecycle except for system integration, operation and maintenance. Each step has inputs and outputs, with assigned tasks for user's actions and tool's execution. Fig. 1 shows this process briefly.

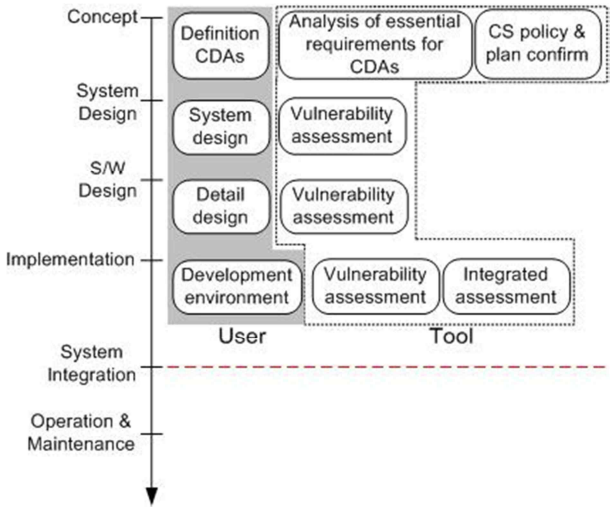

Fig. 1. CSRAS assessment process.

By analyzing user input data, the tool defines security requirements for CDAs identified in a specific- target system and the essential cyber security requirements for CDAs, while confirming cyber security policy and plan, and assesses vulnerabilities.

2.3 Functions of CSRAS

The CSRAS main functions include the followings :

1) Evaluation process for identifying CDAs
- Selecting the target system
Safety (RPS, ESF-CCS, QIAN …)
Non Safety (FWCS, SBCSM, RRS, …)
- Determine the CDAs security level

2) Analysis of essential requirements for CDAs

- Access Control

to address system-specific access control requirements and technical features.

- Audit and Accountability

to address a system-specific list of auditable events and their frequencies for auditing.

- Critical Digital Asset and Communications Protection

to address system-specific protection controls.

- Identification and Authentication

to address methods and technical controls for the identification and authentication of users, media, or digital devices.

- System Hardening

to address methods such as intrusion detection systems to prevent CDAs from unauthorized access and uses.

- Defensive in depth

to address methods for implementing a defensive strategy between different security levels.

Table I: Cyber security requirements sources

Position	Publication	Title
Main guide	U.S. NRC	CYBER SECURITY PROGRAMS FOR NUCLEAR FACILITIES
Reference	NIST	Recommended Security Controls for Federal Information Systems," National Institute of Standards and Technology
Reference	NIST	Guide for Assessing the Security Controls in Federal Information Systems and Organizations
Reference	U.S. NRC	Criteria for Use of Computers in Safety Systems of Nuclear Power Plants
Reference	IAEA	Computer Security at Nuclear Facilities
Reference	Homeland Security	Catalog of Control Systems Security: Recommendations for Standards Developers
Reference	Homeland Security	Department of Homeland Security: Cyber Security Procurement Language for Control Systems
Reference	NEI	Cyber Security Plan for Nuclear Power Reactors
Reference	U.S. NRC	Secure Network Design
Reference	NIST	Guide to Industrial Control Systems (ICS) Security
Reference	Communications Security Establishment	Harmonized Threat and Risk Assessment (TRA) Methodology
Reference	INL	NSTB Assessments Summary Report: Common Industrial Control System Cyber Security Weaknesses
Reference	United States General Accounting Office	TECHNOLOGY ASSESSMENT Cybersecurity for Critical Infrastructure Protection
Reference	Homeland Security	Cyber Security Assessments of Industrial Control Systems
Reference	Homeland Security	Recommended Practice for Patch Management of Control Systems
Reference	IEEE	IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities
Reference	Information Technology Laboratory, NIST	FIPS PUB 140-2 , SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES
Reference	Homeland Security	Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies

3) Vulnerability assessment

- Design-based threat assessments
- Analysis of data flow and the specific actions of CDAs.
- Checklist-based threat assessments
- Analysis of security features for each CDA

4) Report

- Qualitative risk assessments
- Analysis of security requirements and controls: Applicable controls, preventive measures, mitigations, and responses
- A list of recommended practices used in IT security

3. Conclusions

Digital I&C systems in NPPs should consider cyber security for protecting their availability, integrity, and confidentiality. However, it is not easy to incorporate security technologies into I&C systems.

In this paper, the CSRAS is described, which is a tool to help for system designers and component designers to analyze and identify cyber security requirements for their system based on regulatory guides and standards. By following the steps in the CSRAS, system designers and component designers can properly identify cyber security requirements and design necessary technical security controls for their system. A further study is needed to extend the scope of CSRAS to an operation and maintenance phase. Through this, the CSRAS can be a complete assessment tool for ensuring the cyber security of I&C systems in NPPs.

REFERENCES

[1] IAEA Nuclear Security Series No.17 Technical guidance, Computer security at nuclear facilities, 2011.
[2] NEI 04-04 Revision 1, Cyber Security Program for Power Reactors, Nuclear Energy Institute, November 18, 2005.
[3] USNRC Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities, 2010.
[4] Jung-Woon Lee, Jae-Gu Song, Cheol-Kwon Lee, and Dong-Young Lee, A Conceptual Framework for Securing Digital I&C Systems in Nuclear Power Plants, The 2011 International Conference on Security and Managemen, July 16-19, 2012, Las vegas, USA.
[5] Mead, Nancy R, Security Requirements Reusability and the SQUARE Methodology(CMU/SEI-2010-TN-027), Software engineering institute, Software Engineering Institute, Carnegie Mellon University, 2010, USA.
[6] Jae-Gu Song, Jung-Woon Lee, Cheol-Kwon Lee , Kee-Choon Kwon, and Dong-Young Lee, A Cyber Security Risk Assessment for the Design of I&C Systems in Nuclear Power Plants, Nuclear Engineering and Technology(NET), Korean Nuclear Society(KNS) (accepted for publication on March 13, 2012).
[7] Jung-Woon Lee, Cheol-Kwon Lee, Jae-Gu Song, and Dong-Young Lee, Cyber Security Considerations in the Development of I&C Systems for Nuclear Power Plants, The 2011 International Conference on Security and Managemen,July 18-21, 2011, Las vegas, USA.
[8] NIST SP 800-64, Rev. 2, "Security Considerations in the System Development Life Cycle," National Institute of Standards and Technology, Gaithersburg, MD, October 2008.