A Study of a Guide Development for Regulatory Acceptance Criteria of Technical Security Controls

Jae-Gu Song *, Jung-Woon Lee , Jinsoo Shin, Cheol-Kwon Lee
Korea Atomic Energy Research Institute, Yuseong-gu, Daejeon 305-353, Republic of Korea
**Corresponding author: jgsong@kaeri.re.kr*

1. Introduction

In order to respond to the issue of cyber security for nuclear facilities, in 2010, the US NRC announced RG 5.71 to establish a cyber security regulatory plan for digitalized system in the nuclear facilities[1]. Korea has implemented cyber security regulations for domestic nuclear facilities by KINAC's regulatory requirement RS-015 since 2014[2]. KINAC has conducted special inspections until 2019 based on RS-015, and plans to perform regular inspections during every overhaul period. Through a special inspection, a lesson learned that is a difficulty in implementing a consistent cyber security assessment due to the different nuclear power plants type, the variety of digital assets, the operating environment, and the continuous changing security threats.

This paper introduces a study of guide development to support the regulation acceptance of technical security controls and inspection through the development of baseline assessment data, checklists, and acceptance criteria based on regulatory requirements for domestic power plants.

2. Guide development of regulatory acceptance criteria for technical security controls

This chapter describes the strategy and development process for developing the baseline assessment data, checklist, and acceptance criteria for technical security controls of RS-015, which is a cyber security regulatory standard for nuclear facilities in Korea.

2.1. Analysis of technical security assessment documents for nuclear power plants

To develop acceptance criteria based on the analysis of technical security control items of KINAC/RS-015, it is required to analyze major documents that suggest cyber security evaluation methods. In this study, IEC 63096, EPRI TAM, NEI13-10, and NRC regulatory documents were analyzed as the security assessment guide for nuclear facilities [3, 4, 5, 6]. Through the survey of each document, the correlation with the RS-015 technical security control items was classified.

2.2. Baseline assessment data development

Baseline assessments data is that need to be checked according to RS-015 requirements, and guides of the information that should include in the security assessment data. It defines the base information to confirm the compliance check for each require items. An example of baseline assessment data are as follows.

- RS-015 Requirements: (A) 1.1.1 Account Management, a. Mandatory digital asset account management (approval, use, change, disuse, and deletion procedures) and documentation.
- Baseline assessment data: Identification of critical digital assets requiring account management for each CDA. Check the analyzed data according to the following;

1) In the case of network switches, all accounts included for account management. Physical settings type can except.
2) User can directly access and use.
3) CDA running Operating system information what capable of account management functions(windows, Linux, Unix, etc.).
4) CDA can access and change information through remote access.
5) If the CDA used only by the operator, do not need to consider access controls for operators(located in MCR).

Baseline assessment data needs to present in the form of the following table 1 with basic information of CDA.

Table I: Example of Baseline assessment data

CDA	Installation location	OS Info.	User Info.	Requiring account management	Selected answer
A	MCR	Proprietary OS	Operator	N	5)
B	Computer room	RTOS	System Engineer	Y	2), 3)
C	Electrical equipment room	Proprietary OS	System Engineer	Y	1)

2.3. Checklist development

The checklist defines what the regulator checks when reviewing the operator's cyber security assessment report.

The checklist developed to check the status of security measures by analyzing network connectivity, security levels, and digital properties, physical security environments, access environment of user and media, etc.

An example of a checklist is below.

- RS-015 Requirements: Same as item (A).
- Checklist:

1) Prepared documents (Top-level policy, guidelines, procedure document) on account management (including approval, use, change, disuse, and deletion procedures)

2) Are there any missing CDAs that require account management?

2-1) Include all of network switches information except physically configured network switches

2-2) Include CDAs requiring user access information (installation, operation, maintenance/test, etc.)

2-3) Include CDAs running Operating System information (Windows, Linux, Unix series operating system, etc.)

2-4) Include CDAs change information by accessing remotely from another CDAs or digital devices.

2-5) CDAs location information.

2.4. Testing and revision

To review the adequacy of the developed baseline assessment data and checklist, it is necessary to conduct a security assessment to I&C test system. For this test, use the TEST-BED developed by KAERI[7]. By using the TEST-BED in this step, the level of guide that baseline assessment data and checklist review the possibility of application to the I&C system assessments.

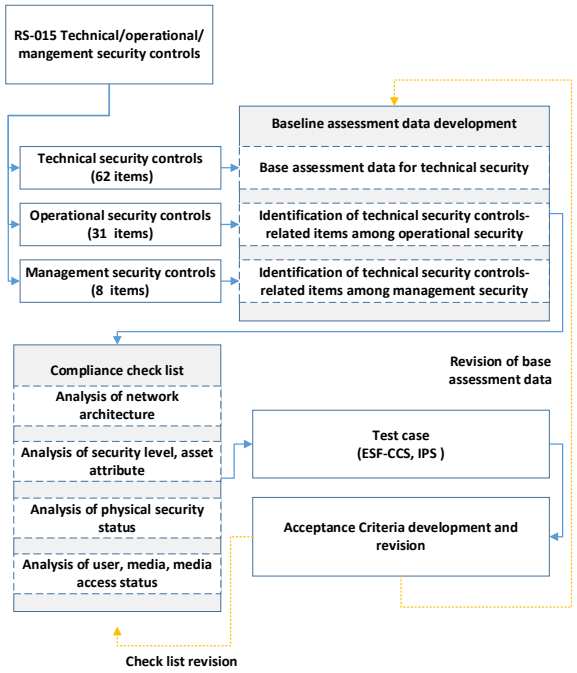

Fig. 1. The guide development process for acceptance criteria of regulatory standards.

2.5. Development of regulatory acceptance criteria

Acceptance criteria developed as a guide to support the evaluator's judgment.

An example of developing acceptance criteria is as follows.

- RS-015 Requirements: 1.1.1. Account management, B. Establishment of review procedure and periodic review of illegal use or change of CDA account accordingly (at least once a quarter)
- Acceptance criteria: It confirmed that the following audit status explained for each CDA.

1) User login/logout record data

2) Records of administrator access and use of administrator commands (including physical access)

3) Illegal execution data of specific administrator functions (including physical access)

3. Conclusions

This study explains how to develop a guide for regulating cyber security assessment based on RS-015. Baseline assessment data, checklist, and acceptance criteria guide will be developed through this study, and specific data will be described through the N-STAR report of the Korea Foundation of Nuclear Safety.

Acknowledgments

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. (No. 2003022)

REFERENCES

[1] Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities, U.S. Nuclear Regulatory Commission, 2010.
[2] KINAC/RS-015, Technical standard for the security of computer and information systems in nuclear facilities, Rev. 1, KINAC, 2014.
[3] IEC SC 45A, Nuclear power plants – Instrumentation, control and electrical power systems – Security controls, Draft version IEC, 2019.
[4] EPRI Cyber Security Technical Assessment Methodology (TAM), Risk Informed Exploit Sequence Identification and Mitigation, Revision 1, ERPI, 2018.
[5] NEI 13-10 rev.5, Cyber Security Control Assessments, Nuclear Energy Institute, 2017.
[6] NUREG-0800, STANDARD REVIEW PLAN, Revision 8, U.S. Nuclear Regulatory Commission, 2020.
[7] J. G. Song, J. W. Lee, G. Y. Park, K. C. Kwon, D.Y. Lee, C. K. LeeAn Analysis of Technical Security Control Requirements for Digital I&C Systems in Nuclear Power Plants, Nuclear Engineering and Technology, Volume 45, Issue 5, October 2013.