Introduction of Performance Measure Cases for Nuclear Cyber Security Inspection

Kookheui Kwon [a*], Seungmin Kim [a]
[a]*Korea Institute of Nuclear nonproliferation And Control, Daejeon, the Republic of Korea*
[*]*Corresponding author: vivacita@kinac.re.kr*

1. Introduction

The regulatory standard of cyber security for domestic nuclear facilities (KINAC/RS-015) includes requirements for establishing cyber security program that the licensee should carry out such as roles and responsibilities of security organization, identification of Critical Digital Assets (CDAs), Defense-in-Depth protective strategies, implementation of security controls, continuous monitoring and assessment, and an incident response plan. And licensees are implementing cyber security measures gradually to establish the program.

In addition, various regulatory activities are being carried out to evaluate the cyber security program and security measures of nuclear facilities. However, there is still a need for study on quantitative performance measures and/or indicators for security evaluation. Quantitative performance evaluation is easy to judge the security status and allows regulators and licensees to present efficient evaluation results. Through the 2019 auditing, the NRC pointed out that no performance measure was identified for the current nuclear cyber security program, and accordingly, it studied cyber security performance indicators to improve security performance and inspection efficiency. I would like to introduce the performance testing and performance metrics that the NRC is currently planning to apply as part of the performance measure in cyber security inspection.

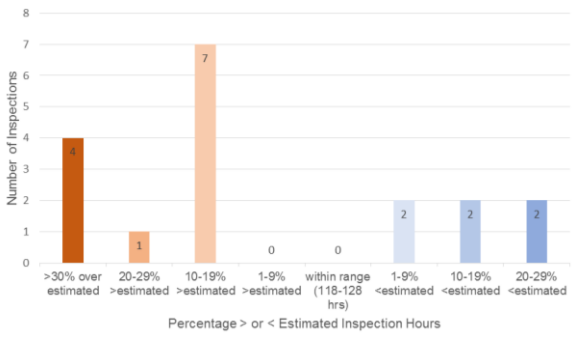

Fig. 1. Difference between Estimated and Actual Cyber Security Inspection Time, NRC, 2018

2. Performance Testing

The NRC performs inspections based on regulatory requirements during cyber security inspections, but the NRC plans to waive the related inspection if the licensee presents the appropriate performance testing results for the security requirements.

If the licensee elects to demonstrate performance and function test, inspector should verify that the performance and function testing reflects the onsite cyber system physical configuration and performance. If the answer to the following are “yes”, then the inspector may determine that the demonstration of the performance and function test is adequate.

- In accordance with the cyber security plan (CSP), licensees are required to collect data, to document results, and to evaluate the effectiveness of existing cyber security programs and cyber security controls. Did the licensee submit information that describes and documents results of its performance testing assessment program as part of the Request for Information (RFI) submission?

- Was the cyber-attack performance and functional test authentic and realistic? Specifically, the virtual network test configuration had to reasonably match the site’s specific computer network configuration(s) and the cyber-attack testing performed, and realistically challenged the virtual network.

- If the licensee identified issues during the performance testing, did they appropriately categorize and correct the deficiencies? If the testing deficiency revealed a noncompliance with the CSP, did the licensee implement appropriate compensatory measures, prioritize the deficiency, and implement corrective actions? Licensees are required to monitor the cyber security program through random testing of cyber security intrusion monitoring tools, periodic functional testing, and vulnerability scans/assessments.

3. Performance Metrics

The NRC plans to utilize performance metrics presented by licensee as one of performance measures during cyber security inspections.

If the following data is provided completely to the inspection team during the RFI submission, the inspection team shall be reduced by contractor.

3.1 Access Control

- Number of violations of access control policy identified during the quarter

- Number of days to disable and remove user credentials of employees due to a change of duty or of employment
- Number of non-compliance incidents of cyber security controls by third-party personnel
- Number of unauthorized PMMD connected to CDAs

Table I: Performance Metrics

Control Classification	Good Peformance	Corrective Action	Performance Deficiency
Access control	0	1-2	3 or more
Third-party	0-1	2	3 or more
PMMD connected	0-1	2	3 or more
Security flaws	0-1	2-3	4 or more
Config. change	0-1	2-3	4 or more
Mal. code	0-1	2-3	4 or more
Periodic scan	0	0~1%	> 1%
Security func.	0-1	2-3	4 or more
Training	100-95%	94-90%	< 90%
Open port	0-1	2-3	4 or more

3.2 Flaw Remediation

Number of security flaws not corrected (identify the security alerts and vulnerability assessment process, communicate vulnerability information, correct security flaws in CDAs, and perform vulnerability scans or assessments of the CDA to validate that the flaw has been eliminated before the CDA is put into production).

3.3 Configuration Management

Number of configuration changes that are not documented or approved in accordance with the CSP or procedures, and the number of incorrect baseline configurations noted by the licensee

3.4 Malicious code identification

- Number of incidents where malicious code was not detected at the security boundary device entry and exit points and on the network
- Number of periodic scans not performed in accordance with procedures and periodicity requirements

3.5 Security functionality

- Number of security functions not tested manually or through automated means (the correct operation of security functions of CDAs are verified and documented periodically)
- The mean time to respond and to report, as a result of testing intrusion detection systems, drills, and actual events

3.6 Software and information integrity

Number of software integrity verification failures (reassessing and documenting the integrity, operation, and functions of software and information by performing regular integrity, and operation and functional scans, in accordance with the CSP.)

3.7 Security Awareness and Assessment Team

- Personnel training and specialized training commensurate with their assigned duties are completed
- The minimum required staff was assigned, and any vacancies were filled with fully qualified and trained personnel, at the time of inspection
- Personnel staffing, qualifications, and training

3.8 System Hardening

Number of unnecessary open ports and protocols for communication for firewalls discovered and removed

3. Conclusions

In this paper, cases of performance measures are introduced to evaluate the current status of implementation of cyber security programs and security measures in nuclear facilities. Quantitative performance evaluation is easy to grasp the security status and allows regulators and licensees to present efficient evaluation results. the NRC pointed out that no performance measure was identified for the current nuclear cybersecurity program, and accordingly, it studied cybersecurity performance indicators to improve security performance and inspection efficiency. In recent cybersecurity inspections, performance testing and performance metrics, which are planned to be applied as part of a performance measure, are introduced. In Korea, cybersecurity inspections in accordance with regulatory standards are currently qualitatively performed, so it is necessary to identify quantitative performance measures suitable for domestic sites by referring to these cases.

REFERENCES

[1] Regulatory Guide 5.71. "Cyber Security Program for Nuclear Facilities", U.S. NRC, 2010
[2] Draft Inspection Procedure 71130.10. "Cyber Security Inspection Procedure", U.S. NRC, 2021
[3] Nuclear Energy Series(draft). "Engineering and Design Aspects of Computer Security for I&C systems at Nuclear Power Plants", IAEA, 2017
[4] IAEA Safety Standards No. SSG-39. "Design of Instrumentation and Control Systems for Nuclear Power Plants", IAEA, 2016
[5] NEI 13-10(rev.6). "Cyber Security Control Assessments", NEI, 2017
[6] NIST Planning Report 02-3. "The Economic Impacts of Inadequate Infrastructure for Software Testing", NIST, 2002
[7] NIST 800-53(rev.2). "Guide to Industrial Control System Security", NIST, 2015
[8] KINAC/RS-015, "Cyber Security Regulatory Standard for Nuclear Facilities", KINAC, 2014