# A Study on Considerations to Apply Technical Security Controls for Nuclear Facilities

Chaechang Lee*
Korea Institute of Nuclear Nonproliferation and Control, 1534, Yuseong-daero, Yuseong-gu, Daejeon, Republic of Korea
*chiching@kinac.re.kr

## 1. Introduction

Nuclear facilities in South Korea and the United States should implement cyber security programs in accordance with their respective regulatory standards. ‘Technical Security Controls’, which contains about 70 security requirements, is part of the cyber security programs required by regulatory standards, originated from NIST in the United States [1, 2]. It is difficult to expect these security controls to be implemented properly on the site simply by listing the 70 requirements set forth by regulatory standards and to apply them uniformly at once. Therefore, this paper presents considerations for efficiently applying the requirements of RG 5.71 to nuclear facilities.

## 2. Considerations to Apply Technical Security Controls

### *2.1 Cyber Security Control Assessments*

The Nuclear Energy Institute (NEI) of the U.S. has established NEI 13-10, Cyber Security Assessments, to streamline requirements for security controls and U.S. nuclear licensees are implementing them with the endorsement of U.S. NRC [3]. The NEI document classifies Critical Digital Assets (CDAs) based on their software and hardware characteristics. It also presents whether or not the attack vectors, corresponding to each security control, exist by the characteristics of the classified types. Based on this, it gives what security controls should be implemented and what security controls are not applicable.

Thus, nuclear licensees could reduce the burden of documenting for the justifications that cannot be applied to technical security controls, once they classify their own CDAs in accordance with the document.

### *2.2 Alternative Controls*

NEI 13-10 referred to other technical security controls in RG 5.71 when presenting alternative security controls for each type of CDAs. That is, one security control can be implemented as an alternative to another. With the analysis of the security controls which refer to alternative security controls, it helps licensees to identify the security controls that they should apply with priority. As a result of the analysis, ‘Access Enforcement’ and ‘Separation of Functions’ were cited the most as alternative controls, 10 times.

### *2.3 Periodic Monitoring and Review*

Some technical security controls in RG 5.71 demand periodic monitoring and review. These security requirements should be noticed separately to ensure that the involved employees at the site, such as engineers, do not miss the period they should implement the security activities. The table below outlines the items of technical controls that require periodic review and monitoring.

Table 1. The Technical Security Controls that Should Be Periodically Reviewed and Monitored

| Section | Technical Security Controls |
|---|---|
| Access Control | Account Management |
| | Information Flow Enforcement |
| | Wireless Access Restrictions |
| | Access Control for Portable and Mobile Devices |
| Audit and Accountability | Response to Audit Processing Failures |
| Identification and Authentication | Password Requirements |
| | Non-authenticated Human Machine Interface Security |
| | Authenticator Management |
| System Security Hardening | Removal of Unnecessary Services and Programs |
| | Hardware Configuration |

### *2.4 Role based Access Control*

Lots of security controls in RG 5.71 are involved in Role-based Access Control (RBAC). RBAC is a method of access control where access is allocated to roles rather than granting access to individual users. The table below shows an example of implementation of RBAC-applied technical security controls, which can be used to meet the various requirements listed in RG 5.71 at a time.

Table 2. The Example of RBAC Applied by the Security Controls in RG 5.71

| Account | Role | Security Function | Non-Security Function |
|---|---|---|---|
| Administrator | Engineers | Scan, Account management | Install and delete, Change set points |
| | Cyber Security Personnel | Change security configurations | None |
| User | Operators | Scan | Control, Monitoring |
| | 3rd party personnel | None | Logic management (accompanied by engineers) |

## 3. Conclusions

In this paper, a couple of considerations were presented for applying technical controls in RG 5.71. Cyber security personnel at a nuclear facility should be able to clearly identify what goals of the security controls are intended to achieve. It is up to licensees to find optimal methods to ensure that technical security controls are implemented properly considering the environment of each nuclear facility.

## REFERENCES

[1] NIST SP 800-53, Rev. 3, “Recommended Security Controls for Federal Information Systems,” National Institute of Standards and Technology, Gaithersburg, MD, August 2009.

[2] U.S. NRC, Regulatory Guide 5.71, “Cyber Security Programs for Nuclear Facilities”, 2010.

[3] NEI, 13-10, “Cyber Security Controls Assessments”, 2013.