Critical Digital Assets Identification, Assessments, and Remediation in Nuclear Power Plants

Jeong-Kweon Lee *, Jin-Woong Lee
KEPCO E&C, Inc., 989-111 Daedeokdaero, Yuseong-gu, Daejeon, 34057, Republic of Korea
**Corresponding author: jklee@kepco-enc.com*

1. Introduction

Cyber security has become one of the critical issues in nuclear power plants because cyber-attacks could adversely impact the plant's ability to perform critical functions necessary to ensure public health and safety. Current cyber security regulations [1] and guidance [2] were established to address the application of traditional cyber security control methods to a digital asset against the entire list. Simply attempting to apply the security control requirements to every asset under evaluation might be a challenge. Improper or incomplete implementation of controls due to insufficient guidance can often result in costly re-evaluation to meet the requirement. This paper introduces the guidance on how to efficiently assess and implement the cyber security requirements with a risk informed methodology by applying the EPRI Technical Assessment Methodology (TAM) [3].

2. CDAs Identification

The Critical Digital Assets (CDAs) identification is performed based on the methodology guided by the NEI 10-04 [4] which provides an approach for identifying digital assets that are associated with Safety, Security, and Emergency Preparedness (SSEP) functions and are required to be protected from cyber-attacks in accordance with 10 CFR 73.54[5]. The identification is processed by the following three steps.

2.1 1st Step - Digital Assets Identification

The 1st step is a pre-CDA identification step to determine digital devices of component level such as controller module, data communication module, and I/O module. The following characteristics are considered to identify the digital devices:

- A component whose operational function is dependent on the programmed execution of an internal, electronic, and digital processor [6]
- A programmable device that uses any combination of hardware, firmware and/or software to execute internally stored programs and algorithms, including numerous arithmetic or logic operations, without operator action [4]
- Any unit of hardware that has the capability to perform digital data communications or processing and can store digital information

2.2 2nd Step - Grouping Digital Assets

At the 2nd step, the identified multiple digital assets can be grouped together on their functional bases to form a single digital asset as the following various documents:

- NUREG/CR-6847 [6]: "Digital devices that are connected together and have an integrated function should be grouped together to form a single CDA."
- NEI 10-04 [4]: "The guidance should not inhibit the licensee from designating a component with multiple digital devices or a network containing multiple digital devices as a single CDA."
- EPRI-3002012752 [3]: "A Programmable Logic Controller (PLC) is typically made up of several specific assets inserted into the PLC backplane (e.g., controller module, power supply module, data communications module, input modules, output modules, etc.). The composition of a PLC may be considered the group of 'sub-assets' because they can be taken together on a functional basis to analyze the PLC as an asset."

This grouping approach for multiple digital assets is efficient for a CDA assessment and reduces the burden of repeating from the identification, assessment and remediation of a component based CDA.

2.3 3rd Step - CDAs Identification

At the 3rd step, a digital device should be identified as a CDA if it meets one or more of the following criteria defined in the NRC DG-5061 [7].

(1) perform or are relied upon for SSEP functions,
(2) could adversely affect SSEP functions or Critical Systems (CSs) or CDAs that perform SSEP functions,
(3) provide a pathway to a CS or CDA that could be used to compromise, attack, or degrade an SSEP function,
(4) support a CS or CDA,
(5) protect any of the above from a cyber-attack, up to and including the design-basis threat, or
(6) are balance of plant equipment that affects reactivity and could result in an unplanned reactor shutdown or transient.

3. CDAs Assessments

The risk informed methodology of the TAM is adapted for performing the assessment and mitigation activities because it applies the best control methods based on the effectiveness score and implementation burden. A

Reference Cyber Security Data Sheet (CSDS) [8] for the identified CDAs in situations where multiple CDAs share the same features, options, or functions can be developed for major CDAs. Then, the baseline is set up with Reference CSDS results for Tailored CSDS. The Reference CSDS based on a simplified and generic information can be prepared by vendors, system designers or utilities for efficiency and reuse. The Tailored CSDS is created based on data collection through walk-down for plant specific features.

The CSDS (hereafter referred to as both Reference CSDS and Tailored CSDS) captures the asset characteristics for an installed configuration and data flow to identify the attack pathways and exploit sequences through Step 1. Step 2 focuses on the methods available on or via the asset under assessment, referred to as "engineered Security Control Methods (SCMs)." The engineered SCMs are allocated to mitigate each exploit sequence. If an exploit sequence is not fully mitigated, it would result in residual exploit sequences. The residual exploit sequences can be mitigated using relationship sets in Step 3. Relationship sets would be used to allow inheritance of shared SCMs so that they could be allocated to the residual exploit sequences. The shared SCMs are those that are not included as features and functions of the asset under assessment, but physical protection or administrative procedures. The CSDS documents the results of implementing Steps 1 and 2. The relationship sets are documented in a Relationship Set Data Sheet (RSDS) of Step 3.

3.1 Step 1- Attack Surface and Exploit Sequence

The CSDS Part 1(Step 1) bounds the scope to the actual attack surface characteristics and identifies the possible exploit sequences. An exploit sequence is an attack pathway and exploit mechanism that allows an attacker to achieve an exploit objective, as illustrated in Figure 1. The items of CSDS Part 1 are summarized as Table 1.

Table 1. Summary of CSDS Part 1

Part 1a[1]. Assessment Scope
· General Target Asset Description · Applicable Pictures/Diagrams · List of Manuals & Documentation · Target Asset Composition · Decomposition Level of Analysis · Technical Information Availability · Installed Configuration Detailed Description · Data Topology and Data Flow · Critical Data at Rest and in Transit
Part 1b[1]. Asset Characteristics
· Firmware Description & Version No. · Operating System & Version No. · Installed Application Software & Version No. · Installed Configuration & Maintenance Method · Physical Communication Ports and Terminals · Removable Media or Portable Devices in Use
· HMI Capabilities and Detailed Description · Data Communication Protocols · Services and Logical Communication Ports · Data Files and Software Objects · Capability for Installation of Third-Party Software? · Site Characteristics [Tailored CSDS] · Relationship Sets [Tailored CSDS] · Scanning and Vulnerabilities: Scan Performed? · Unused Features and Functions · Access Control and Authentication SCMs · Event/Alert/Audit Log SCMs · Asset Backup & Restore Capability · Cryptography · Vendor Security Advisory & Patch Program · Manufacturer Product Security Certifications · Other SCMs, Other Model No. with the Same Asset Characteristics
Part 1c[2]. Attack Pathways
· Attack Pathway Number, Attack Vector, Physical Interface, Communication Protocol, Available Logical Port Numbers, Interface ID, Interfacing Connections, Attack Pathway Description
Part 1d[2]. Identify Exploit Sequences
· Component Enable/Disablement-Immediate · Component Disablement – Delayed · Denial of Service · Malware · Operational Process Data · OEM Defined Program/Configuration Data · User Defined Program/Configuration Data · Security Operational Data

1) The CSDS is completed in the MS Word template.
2) The CSDS is identified in the MS Excel spreadsheet.

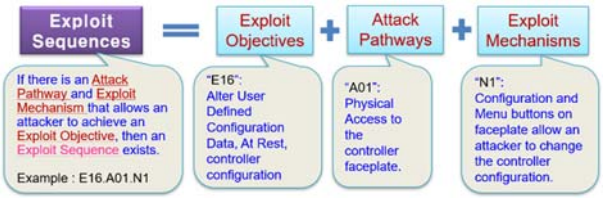

Fig. 1. Example of Exploit Sequences

3.2 Step 2 - Engineered SCM

The CSDS Part 2 (Step 2) identifies, scores, and allocates the available engineered SCMs that are implemented on the asset to the exploit sequences identified in Step 1. The engineered SCMs are native features of an asset or installed locally on an asset that is a part of its installed configuration. Once identified, a security effectiveness score is calculated for each engineered SCM based on the criteria and values from its security implementation type, implementation effectiveness and exploit difficulty. The engineered SCMs are scored for implementation effectiveness for three security functions: Protect, Detect, and Respond & Recover. The typical engineered SCMs library can be developed to reuse across multiple CDAs for efficiency and consistency. The goal is to implement only those engineered SCMs that have the highest efficacy for

mitigating the exploit sequences to achieve a combined security effectiveness target levels based on pre-computed consequence levels from NEI 13-10 [9]. If the allocated engineered SCMs do not meet the target level, then that exploit sequence would become a residual exploit sequence. Residual exploit sequences can be mitigated by shared SCMs in Step 3. The items of CSDS Part 2 are summarized as Tables 2 and 3.

Table 2. Summary of CSDS Part 2

Part 2a[1]. Engineered SCM Identification and Scoring
· SCMs, Logical Port Blocking, SCM Implementation, SCM Exploit Difficulty, Security Effectiveness Score, Implementation Burden, SCM Efficacy
Part 2b[1]. Engineered SCM Allocation
· Combined Security Effectiveness Score, Target Levels, SCM Quantity

1) The contents of CSDS are identified with MS Excel spreadsheet.

Table 3. Summary of an Engineered SCM in CSDS Part 2

Engineered SCM	
· Name: Firmware Integrity Verification	
· Description: Compare firmware hash value provided from manufacture website with download firmware file	
· Implementation	Type: Operational
	Protect: Low
	Detect: None
	Respond & Recover: None
· Exploit Difficulty	Configuration: Low
	Information: Low
	Authentication: 0
	Persistence: Medium
· Efficacy	Protect: 3
	Detect: -
	Respond & Recover: -

3.3 Step 3 - Shared SCM

The RSDS (Step 3) identifies the relationship set category, the inheritance attributes, the associated shared SCMs with Normalized Exploit Mechanisms (NEMs), the inheritance rules, and the member CSDSs. Shared SCMs are scored in the same manner as engineered SCMs. The shared Control Method Library (CML) is developed and standardized for the facility, site or fleet. After the relationship set is defined, the shared SCMs can be used to mitigate the residual exploit sequences from Step 2 within the member CSDSs. The items of RSDS are summarized as Table 4.

Table 4. Summary of RSDS

Part 3a[1]. CML
· Refer to items in Part 2a
Part 3b[1]. NEMs
· Normalized Exploit Mechanism
Part 3c[2]. RSDS
· Name, Category, and Description, References, Inheritance Attributes and Description, Associated SCMs and Exploit Mechanisms, Inheritance Rules, Member CSDSs

1) The contents of shared CML and NEMs are identified with MS Excel spreadsheet.
2) The RSDS is completed in MS Word template.

4. CDAs Remediation

Both of engineered and shared SCMs identified and scored from the assessment conducted are documented with essential information such as remediation target, security function, attack vector, implementation type and detailed implementation procedure. In addition, applicable exploit sequences to be mitigated are included in each SCM documentation. The SCMs implemented by native features of the assets or utility's physical protection system/policy including procedure are not required for further actions. However, if the SCMs are not implemented, then their implementation roadmap to eliminate exploit sequences should be established and prioritized based on the score of SCM efficacy.

5. Conclusion

As discussed above, the CDAs assessments and their remediation in Nuclear Power Plants (NPPs) are efficiently performed by the EPRI TAM which applies the best control methods based on the effectiveness score and implementation burden. The TAM guides the users through a methodical and consistent process that efficiently converges the assessment and mitigation activities to an effective result. Compared to traditional control-based methodologies that apply cyber security controls from a catalog regardless of applicability, the TAM enabled the users to tailor cyber security controls to the individual assets with more precision. Even though this paper specifies the assessments for installed CDAs only, the TAM methodology can be applied to CDAs during engineering design or lifecycle steps under the responsibilities of system designer and/or supplier.

This paper confirms that the cyber security requirement of 10CFR 73.54 can be effectively met to identify, assess and remediate through the guidance of NEI 10-04 and EPRI TAM.

REFERENCES

[1] US NRC Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Power Facilities," January, 2010
[2] NEI 08-09, Rev. 6, "Cyber Security Plan for Nuclear Power Reactors," April, 2010.
[3] EPRI-3002012752, Rev. 1, "Cyber Security Technical Assessment Methodology: Risk Informed Exploit Sequence Identification and Mitigation," November, 2018
[4] NEI 10-04, Rev. 2, "Identifying Systems and Assets Subject to the Cyber Security Rule," July, 2012
[5] US NRC 10CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks," 2009

[6] NUREG/CR-6847 “Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants,” July, 2004
[7] US NRC Draft Regulatory Guide DG-5061, Rev. 1 (Proposed Rev.1 of RG 5.71), “Cyber Security Programs for Nuclear Power Reactors,” February, 2022
[8] EPRI-3002017149, “SEL 487E Protective Relay Reference CSDS,” November, 2019
[9] NEI 13-10, Rev.6. “Cyber Security Control Assessments”, August, 2017