Transactions of the Korean Nuclear Society Spring Meeting
Jeju, Korea, May 17-18, 2018

A Study on Effective Implementation of Security Controls to Critical Digital Assets in NPPs

Ki-Jong Cha [a*], Jae-Hee Roh [b], Ki-Hwang Kim [b], Seok-Ki Lee [b,], Choul-Woong Son [b,]
[a,b]NSE technology Inc., 218 Gajeong-ro, Yuseong-gu, Daejeon 34129, Rep. of Korea
[*]Corresponding author: kjcha@nsetec.com

1. Introduction

Due to increasing national anxiety about nuclear safety caused by cyber threats from a group of nuclear hackers in December 2014, Korean nuclear regulatory agency requires nuclear licensees to establish Cyber Security Plan in accordance with the Radiological Emergency Preparedness Law and related regulatory guidelines [1,2] and to implement the plan in seven phases by 2018 [3]. In this Cyber Security Plan, nuclear licensees should identify Critical Digital Asset (CDA) that performs safety, security, or emergency preparedness (SSEP) functions and which, if compromised would adversely impact these functions. As a result, a large number of CDAs were identified at the NPPs. The CDAs include assets which have direct impact on safety and security functions and which, if compromised do not have impact on safety and security. Furthermore, over 100 technical, operational and management security controls should be implemented to each CDA [2].

Such requirements stated in R.G 5.71 and KINAC RS-015 seem that all CDAs which perform SSEP functions are at same level of risk, but the only differences between CDAs are network placement and use of wireless. Therefore, it's not true that the CDAs are at the same level of risk. Compromising the ability for the plant to know wind speed and direction will not and cannot have the same impact to the plant as compromising the ability to provide emergency power. Additionally, when I&C of operating NPPs was introduced, security was not in consideration and it consisted of various heterogeneous systems. thus, there are difficulties in applying identical security system and limitations in implementing technical security controls required by regulation. To accomplish security controls implementation efficiently, NRC classifies CDAs according to direct and indirect impact of SSEP functions and implements the minimum security controls to the CDAs which have indirect impact [4]. Despite there are such efficient methods suggested by NRC, Korean cyber security regulatory agency does not reflect such method into requirements.

This paper identifies CDAs of representative classified type of NPPs I&C and assessments their security. Based on the work, this paper researches NRC cases, suggests consistent process from CDAs identification to security controls implementation and confirms its effectiveness

2. Process for Implementing Security Controls

The security controls implementation process of CDAs suggested in this paper is indicated in Fig. 1. The process falls into CDAs identification and assessment. In CDAs assessment, impact of CDAs is assessed referring to NRC cases and different security controls are implemented depending on the level of the impact.

2.1 Plant System Classification

Plant system classification is a preliminary task for facilitating CS identification. To comprehensively classify all devices, communication systems, networks, support systems and etc., in the NPPs, nuclear licensees should classify the plant system according to SSEP functions shown in Table I referring to the Final Safety Analysis Report (FSAR), Physical Protection Regulation and Radiological Emergency Plan.

Table I: Plant System Classification

System Function	References
Safety Related System	- FSAR
Important-to-Safety System	
Security System	- Physical Protection Regulation
Emergency Preparedness System	- Radiological Emergency Plan
Support System	- FSAR - Physical Protection Regulation

2.2 CS Identification and Analysis

In CS identification and analysis, nuclear licensees should perform initial consequence analysis and dependency analysis of the systems based on the result of plant system classification. To identify CS, it is required to make judgement of total 34 questions (SR: 3, NSR/ITS: 6, SEC: 18. EP: 4, Supp: 3) stated in KINAC RS-019. Table II indicates an example of CS identification.

Table II: Example of CS Identification.

System classification	Initial consequence analysis					Dependency analysis		CS result
System name	SR.	NSR/ ITS	SEC.	EP.	Supp.	Supported	Supports	
	Q 1-3	Q 1-6	Q 1-18	Q 1-4	Q 1-3			
Control Room HVAC					○			CS
Plant Monitoring					○			CS
DC Distribution								Not CS

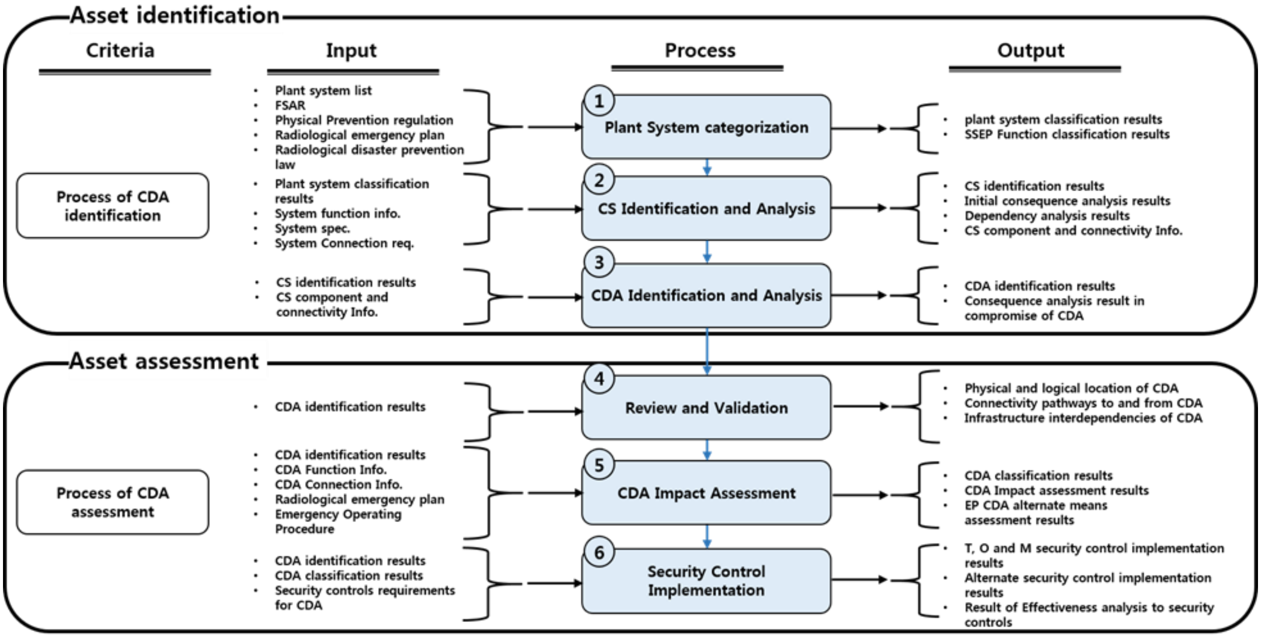
Asset identification
Criteria
Input
Process
Output
Process of CDA identification
Plant system list
FSAR
Physical Prevention regulation
Radiological emergency plan
Radiological disaster prevention law
1
Plant System categorization
plant system classification results
SSEP Function classification results
Plant system classification results
System function info.
System spec.
System Connection req.
2
CS Identification and Analysis
CS identification results
Initial consequence analysis results
Dependency analysis results
CS component and connectivity Info.
CS identification results
CS component and connectivity Info.
3
CDA Identification and Analysis
CDA identification results
Consequence analysis result in compromise of CDA
Asset assessment
Process of CDA assessment
CDA identification results
4
Review and Validation
Physical and logical location of CDA
Connectivity pathways to and from CDA
Infrastructure interdependencies of CDA
CDA identification results
CDA Function Info.
CDA Connection Info.
Radiological emergency plan
Emergency Operating Procedure
5
CDA Impact Assessment
CDA classification results
CDA Impact assessment results
EP CDA alternate means assessment results
CDA identification results
CDA classification results
Security controls requirements for CDA
6
Security Control Implementation
T, O and M security control implementation results
Alternate security control implementation results
Result of Effectiveness analysis to security controls

Fig. 1. Process for implementing effective security controls

2.3 CDA Identification and Analysis

In CDA identification and analysis, nuclear licensees should list all assets of the system identified as CS and analyze communication connectivity and impact of cyber compromise of each asset. To identify CDA, it is required to make judgment of total 5 questions stated in KINAC RS-019. If it comes under more than one questions, it is identified as CDA. Table III indicates an example of CDA identification

Table III: Example of CDA Identification

Asset Classification					Criteria of CDA identification				
System name	Plant System Code	PBS No.	SR/ NSR	Component name	CDA -1	CDA -2	CDA -3	CDA -4	CDA -5
Plant Monitoring	CK	721	NSR	Switch1			○		
				I/O Unit	○				
				Server1	○				
				Server2	○				
				LAN			○		
				Time Server				○	

2.4 Review and Validation

As shown below, nuclear licensees should review and valid direct and indirect connectivity between CDAs and access path to the CDAs. This can be efficiently utilized to implement security controls to each CDA and to describe the vulnerability of the CDAs

1) Identify and document the physical and logical location of CDA.
2) Identify and document direct and indirect connectivity pathways to and from the CDA.
3) Identify and document infrastructure
4) interdependencies of the CDA.

2.5 CDA Impact Assessment

The impact assessment is a method of implementing the minimum security controls by classifying the CDAs into Direct CDAs, Indirect CDAs, EP CDAs, BOP CDAs. However, redundancy should not be used as a factor for determining if a CDA is an Indirect, BOP, EP or Direct CDA. Fig. 2 indicates the simplified process of CDA impact assessment.

2.5.1 Minimum Security Controls

According to the impact assessment, the Direct CDAs should implement all security controls required by the regulations. The Indirect CDAs, EP CDAs, and BOP CDAs require the following minimum security controls to prevent cyber-attacks up to and including the design basis threat (DBT). The minimum security controls are classified into seven categories as indicated in Table IV. Each security control is related to the attack vector described in NEI 10-09[5] and periodical check. The minimum security controls should be implemented to Indirect CDAs and d, e, f, g of minimum security controls should be implemented to EP CDAs. In addition, the following additional security controls are implemented where technically feasible to BOP CDAs whose failure or cyber compromise could cause a reactor scram/trip.

1) 1.1.1 “Account Management”
2) 1.1.5 “Least Privilege”
3) 1.1.6 “Unsuccessful Login Attempts”

4) 1.4.1 “Identification and Authentication Policies and Procedures”
5) 1.4.2 “Password Requirements”
6) 1.5.5 “Installing Operating Systems, Applications and Third-Party Software Updates”

‘Where technically feasible’ means that in case of currently installed BOP device is capable of implementing the additional security controls, the additional security controls should be implemented. otherwise, it is not required to implement the additional security controls and to document an alternate need. Thus, above additional security controls can be implemented through documenting technically infeasible cases.

Table IV. Minimum security controls criteria

No.	Baseline minimum security controls	Related attack vector
a	The CDA is located within a Protected or Vital Area	Direct Physical Access
b	The CDA and any interconnected assets do not have wireless internetworking communications technologies.	Wireless Network Capability
c	The CDA and any interconnected assets are either air-gapped or isolated by a deterministic isolation device.	Direct Network Connectivity
d	Use of portable media and mobile devices is controlled in order to ensure the CDA will not be compromised as a result of the use of portable media and mobile devices.	Portable Media and Equipment
e	Changes to the CDA are evaluated and documented	Supply Chain
f	The CDA, or the interconnected equipment that would be affected by the compromise of the CDA, is periodically checked to ensure the equipment is capable of performing its intended function.	Supply Chain
g	Ongoing Monitoring and Assessment is performed to ensure the security posture of the CDA is maintained by verifying that baseline security criteria remain in place.	Supply Chain

2.5.2 Security Controls Assessment to Direct CDA

The Direct CDAs should implement all security controls required by the regulations. The followings are reasonable techniques which can be used to implement the security controls.

1) “Common Controls”: a particular security control whose implementation provides a security benefit to multiple CDAs.
2) “Inherited Controls”: a situation in which a CDA receives protection from technical security controls (or portions of security controls) that are developed and implemented elsewhere such as on another CDA.
3) “Type assessments”: a situation in which multiple CDAs share substantially similar technical features, functions and capabilities.

In NEI 13-10[6], the Direct CDAs is classified into six types of class according to hardware and software attributes through the type assessment. Security controls corresponding to each class can be implemented by following four methods. Table V indicates simplified example of the classification method according to the CDA attribute.

1) "Common": the control may be implemented organizationally and applied to all CDAs.
2) "Apply to CDA": licensee must address this control for the CDA or class.
3) "Alternate": the cyber security control may be met through alternate means.
4) "Not Applicable": the cyber security control is not applicable to the CDA.

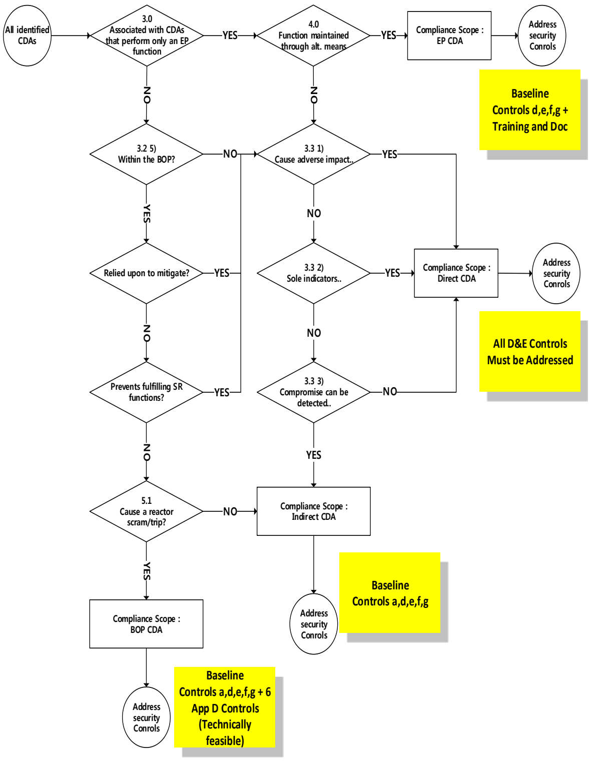
All identified CDAs
3.0 Associated with CDAs that perform only an EP function
YES
4.0 Function maintained through alt. means
YES
Compliance Scope : EP CDA
Address security Conrols
Baseline Controls d,e,f,g + Training and Doc
NO
NO
3.2 5) Within the BOP?
NO
3.3 1) Cause adverse impact..
YES
YES
NO
Relied upon to mitigate?
YES
3.3 2) Sole indicators..
YES
Compliance Scope : Direct CDA
Address security Conrols
All D&E Controls Must be Addressed
NO
NO
Prevents fulfilling SR functions?
YES
3.3 3) Compromise can be detected..
NO
NO
YES
5.1 Cause a reactor scram/trip?
NO
Compliance Scope : Indirect CDA
YES
Baseline Controls a,d,e,f,g
Address security Conrols
Compliance Scope : BOP CDA
Address security Conrols
Baseline Controls a,d,e,f,g + 6 App D Controls (Technically feasible)

Fig. 2. Process of simplified CDA impact assessment

Table V. Direct CDA classification

Class	Attribute	Example
Class A.1	- Changes to operational parameters or operational settings can only be implemented using maintenance and test equipment	- Love Controls Series SC1290 & SC1490 Thermocouple Limit/Alarm Switch Module - KNS Perfecta Model: VPI-3EAN unit - Rosemount 3153N digital transmitters
Class A.2	- Only operational parameters (no configuration settings) can be changed using the local, integral HMI - Configuration setting changes can only be made using a maintenance tool and only by taking the CDA out of service	- Micon model# AI-518 Universal PID Controller - HANYOUNG model# BK-6 Digital Temperature Indicator
Class A.3	- Operational parameters can be changed using the local, integral	- CubicleBus model# 3WL11 low-voltage bus air breaker

	HMI	- TORAY UVT-300 Automatic Water Chemical Analyzer
Class B.1	- Can extract information or data via serial communication	- SEL Model# 2414 Transformer Monitor with DNP3.0 - VAMP 245 Feeder and Motor Protective Relay with DNP3.0
Class B.2	- Designed to allow CDA information extraction through the asynchronous serial communications channel - asynchronous communication protocols also support pre-configured control function execution, output (analog, pulse, and/or contact) manipulations	- Omron Model# GCF-612 PLC with DNP 3.0 protocol - KH300AG-Kehao-Universal Colored Recorder with Modbus RTU - KOYO 'Click' PLC Family with Ethernet and RS485 Modbus RT
Class B.3	- Configuration changes may also be made locally via a console port and/or USB thumb drive/memory card as well as remotely via the asynchronous serial communication channel, - CDA supports firmware update/replacement with removal of the CDA from the service and use of special tools and software - The CDA has a local, special-purpose communications interface (a.k.a. a console port),	- SEL Model 351S Multi-Function Relay with Serial DNP 3.0 Communications - Modicon Quantum PLC with Modbus-plus (MB+) Communications - BOSH LTC0385 Series DinionXF Security Camera

2.6 Security Controls Implementation

When implementing security controls to CDAs, it is necessary to check whether they have adverse impact on SSEP functions as indicated in Fig. 3. If security controls adversely impact SSEP functions or performance (system response time and complexity increment, etc.,), alternative countermeasures should be considered instead of those security controls to protect CDAs from cyber-attacks.

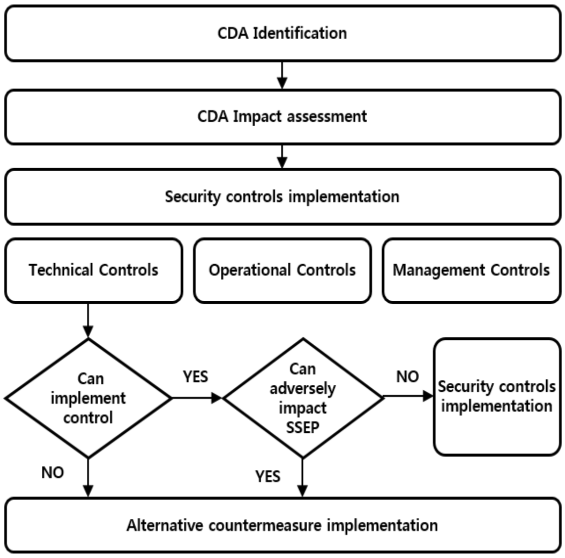
CDA Identification
CDA Impact assessment
Security controls implementation
Technical Controls
Operational Controls
Management Controls
Can implement control
YES
Can adversely impact SSEP
NO
Security controls implementation
NO
YES
Alternative countermeasure implementation

Fig. 3. Process of alternative countermeasure implementation.

3. Conclusion

This paper proposes an efficient and consistent process from CDA identification to security controls implementation according to the Cyber Security Plan. Additionally, it researches the CDA impact assessment and the simplified method of implementing security controls of each class in the security controls implementation phase. [3] suggests that implementing the minimum security controls to Indirect CDAs can reduce total 47.1% of security controls compared to existing security controls implementation.

If security controls implementation method proposed in this paper is additionally approved, it will not only reduce costs imposed to nuclear licensees but also lead to implementing consistent cyber security activities through reasonable reduction for security controls. In addition, security controls required by regulations are not useful for all CDAs. For an example, as one of CDAs, a badge card reader is connected to a network to query the security computer in order to determine if an owner of badge card presented to the reader has access authorization. However, many security controls required by regulations provide useless and useless and unnecessary security functions. As a result, continuous research on cyber security of Korean NPPs is crucial and eventually it is highly required to introduce an effective security control policy for domestic industry reality.

Acknowledgements

This work was supported by the Korea Institute of Energy Technology Evaluation and Planning(KETEP) and the Ministry of Trade, Industry & Energy(MOTIE) of the Republic of Korea (No. 20171510102110)

References

[1] U.S. NRC, "Cyber Security Programs for Nuclear Facilities", Regulatory Guide 5.71, Jan. 2010.
[2] KINAC, KINAC/RS-015, Technical Standard on Cyber Security for Computer and Information System of Nuclear Facilities, Oct. 2014.
[3] Siwon Kim, "A Study on the Effectiveness of Grouping of the Critical Digital Assets at the Nuclear Facilities," The Korean Institute of Communications and Information Sciences, Oct. 27-28, 2016.
[4] KINAC, KINAC/RS-019, Technical Standard on Identification of Critical Digital Assets for Nuclear Facilities, Dec. 2015.
[5] Nuclear Energy Institute, NEI 10-09, Rev. 0, "Addressing Cyber Security Controls for Nuclear Power Reactors," Sep. 2011.
[6] Nuclear Energy Institute, NEI 13-10, Rev. 5, "Cyber Security Control Assessments," Nov. 2016.