Typical Characteristics of Vulnerability for the Safety Controller used in NPP

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

1. Introduction

As a part of cyber security evaluation for the digital assets in NPP, we analyzed the typical characteristics of vulnerability for the safety controller in NPP. In this paper, the elements of vulnerability, the general design features and environments, and the characteristics of vulnerability for the safety controller in NPP are described.

2. The Elements of Vulnerability for the Safety Controller

The elements of vulnerability for the controller are classified into 4 categories - software, data network, configuration management and hardware. We extract the detail elements of vulnerability for the safety controller analyzing the technology of industrial controller. Table 1 shows the elements of vulnerability for software.

Table I: Elements of Vulnerability - Software

Type	Vulnerability
Improper Input Validation	Buffer overflow
	Bounds Checking
	Command Injection
	SQL Injection
	Cross-Site Scripting(XSS)
	Directory Traversal
	Denial-of-Service(DoS) attack
Insecure Code	Use of Insecure Functions
	Use of Insecure Cryptographic Algorithm
	NULL pointer Dereference
Permissions, Privileges and Access Controls	Improper Access Control
	Insufficiently Protected Credentials
	Execution with Unnecessary Privileges
Improper Authentication	Authentication Bypass
	Authentication Absence
	Authentication of Client-Side Management
Insufficient data integrity	Absence of Data Integrity Check
Communication	Use of Plain text
	Use of public protocols
	Use of insecure protocols

3. Design Features and Application Environments of the Safety Controller

In this section, the design features and application environments of safety controller which are used for the basis of the evaluation of vulnerability are described.

3.1 Design Features of the Safety Controller

Design features of safety controller are analyzed with 4 categories - software, data network, configuration management and hardware. The major characteristics of safety controller related with software are as follows;

- Software for the safety controller is verified and validated through the entire development life cycle, therefore potential risk elements are expected to be eliminated during the V&V process.
- The OS of the safety controller has the non-interrupt, deterministic task scheduling structure. The safety controller has the diagnostic capability related with the execution of software program.
- The communication protocol is implemented using deterministic method such as token-passing.
- Engineering development tool is based on PC and interface to main processor using the standard serial communication means.

3.2 Application Environment of the Safety Controller

The safety system, as the application environments of safety controller, has the strict requirements of the physical environments, and the access or interface to the safety system are restricted or limited. The major characteristics of safety system are as follows;

- Each system is configured with 4 channel redundancy. As the digitalizing of system, the redundancy for internal channel is considered for avoiding the multiple loss of function.
- The physical separation, electrical isolation and the communication independence between the inter-channel and the non-safety system should be maintained.
- All the components of safety system are enclosed in the key-lock protected cabinet.
- The response time of safety system shall meet the requirements imposed by safety analysis.

4. Vulnerability Assessment of the Safety Controller

The vulnerability of safety controller is evaluated for the extracted all elements of vulnerability based on the analyzed design features and application environments for the safety controller. Table 2 shows the example of evaluation for a part of software. As shown in the table 2, some of the vulnerability are expected to eliminated, but detailed check is required. The important consequences of the evaluation results are as follows;

Table Ⅱ: Example of Vulnerability Assessment

Type	Vulnerability	Design Features of the Safety Controller	Assessment
Improper Input Validation	Buffer overflow	- Any external input function is not possible while online - Validating function for Input value is exist - Buffer over flow is verified in the code development process	None
	Bounds Checking		None
	Command Injection	- Disable of external command	None
	SQL Injection	- Not using SQL	None
	XSS	- Not using web application	None
	Directory Traversal	- Not using web application	None
	DoS attack	- Not using TCP/IP - Fixed type for transmission data, scan time, task number, and etc.	None

- *Software Security*

Software including all the functions is verified for its integrity in the design and V&V process and unused code is eliminated in the code development process. Therefore, most of the vulnerability related with software integrity such as the buffer overflow, insecure function and NULL pointer dereference are expected to be eliminated.

- *Protocol and Communication Security*

As the safety controller only interfaces with its closed network and does not have any function of remote or web application, the vulnerability related to those element are not expected. Encryption function to protect data should be checked and confirmed.

- *Detection of Security Incidents*

Although the safety controller does not have the dedicated function for the security-related detection, it is possible to monitor the cyber security incident using status diagnosis function.

- *Access control Security*

Proper access control is performed by having the function of session lock after within predetermined time of inactivity and more than a predefined number of unsuccessful logon attempts.

- *Account Management*

In developing process of the safety controller, two types of account, that is developer account and administrator account, are used.

- *Authentication (Password) Management*

It is necessary to confirm the cryptographic algorithm for password and the authentication process.

5. Conclusions

We analyzed and established the typical characteristics of vulnerability for the safety controller in NPP through extracting the detail elements of vulnerability, analyzing design features and application environments of the safety controller. Most of vulnerabilities for the safety controller are expected to be eliminated by the characteristics of safety controller such as restriction of external access, closed network architecture, strict development and V&V process, but some of vulnerabilities such as cryptographic algorithm for password, authentication process, and the monitoring of intrusion are to be carefully checked and confirmed during the cyber evaluation of the safety controller. The analysis method of vulnerability and evaluated results for the safety controller would be used in implementing of cyber evaluation of the safety controller.

ACKNOWLEDGMENTS

This work was supported by the Nuclear Safety Research Program through the Korea Foundation Of Nuclear Safety(KoFONS) using the financial resource granted by the Nuclear Safety and Security Commission(NSSC) of the Republic of Korea. (No. 1605007)

REFERENCES

[1] NIST, 800-82(rev2) “Guide to Industrial Control Systems (ICS) Security”, 2015.
[2] DHS, “Common Cyber security Vulnerabilities in Industrial Control Systems”, 2011.
[3] DOE/INL, “Vulnerability Analysis of Energy Delivery Control Systems”, 2011
[4] D. W. Kim, B. G. Min, H. D. Park, S. W. Park, “PLC – Based Control System Vulnerability Analysis Method”, *Infor. Secur*., vol. 25, no. 5, pp.26-36, 2004.
[5] K. J. Cha, J. H. Ahn, Y. M. Kim, Y. G. Kwon, “A Study of PLC System Vulnerability Checklists in Nuclear Power Plants”, KNS, Gyeongju, Oct 25-26, 2016.
[6] KINAC, KINAC/RS-015 “Regulatory Standard on Computer Security of Nuclear Facilities”, 2014.