Cyber Security Risk Assessment for the KNICS Safety Systems

C. K. Lee, G. Y. Park, Y. J. Lee, J. G. Choi, D. H. Kim, D. Y. Lee, K. C. Kwon
Korea Atomic Energy Research Institute, I&C & HF Research Div.,
1045 Daedeok-daero, Yuseong-gu, Daejeon, 305-353, Korea
**Corresponding author: cklee1@kaeri.re.kr*

1. Introduction

In the Korea Nuclear I&C Systems Development (KNICS) project the platforms for plant protection systems are developed, which function as a reactor shutdown, actuation of engineered safety features and a control of the related equipment. Those are fully digitalized through the use of safety-grade programmable logic controllers (PLCs) and communication networks. In 2006 the Regulatory Guide 1.152 (Rev. 02) was published by the U.S. NRC [1] and it describes the application of a cyber security to the safety systems in the Nuclear Power Plant (NPP). Therefore it is required that the new requirements are incorporated into the developed platforms to apply to NPP, and a cyber security risk assessment is performed. The results of the assessment were input for establishing the cyber security policies and planning the work breakdown to incorporate them.

2. Cyber Security in Nuclear Industries

With the advent of digital computers and networks the issues on cyber security are raised and the solution market is becoming bigger in the IT industry. Nowadays these digital technologies have also been popular in manufacturing plants, especially including NPPs, and it has reported that some plants were attacked by some intruders. So it has been said that the security control for unauthorized access to the plant systems through internet or other paths should be strengthened. Prior to the R.G. 1.152 (Rev. 02) the cyber security for nuclear facilities has been studied for more than a decade based on the technologies being used in IT industry [2]. And 9/11 accelerated these studies. National laboratories and utilities, including regulatory bodies, tried to find out the best way to cope with not only the attacks by intruders from outside but the sabotage from inside [3,4]. In spite of these efforts it is hard for reference to find out the results of studies and the evidences for applications to real plants. The authors agree that the result may be a secret in itself. In my opinion, however, the more we hide them the bigger the cyber risks will be. Therefore it is time to coordinate the individual efforts and experience to resolve the actual problem that no system can be free from the intruders as far as the system has a data communication network..

3. Cyber Security Risk Assessment

To apply the cyber security requirements to the design of man-machine interface system (MMIS) in the NPP, it is recommended by the regulatory documents that a policy and a detailed plan should be prepared and a risk assessment followed. Those documents define detailed activities for the assessment which includes a threat analysis, a vulnerability analysis, a risk analysis and defensive techniques, etc [5].

In KNICS project we prepared two documents, a cyber security policies and plans for the platforms of KNICS safety systems. Prior to the documentation we performed a risk assessment with an IT security company in accordance with the regulatory guides.

3.1 Asset Analysis

The assets are identified to the KNICS safety systems cabinets. The importance of assets from the viewpoint of confidentiality, integrity and availability, which are top-tier properties for the cyber security, is evaluated. The importance has three levels shown as table 1, and the evaluation criteria for each property established in advance, which shows the degree of risk to the plant and the public when the problems occur in each property.

Table 1: A Part of Asset Analysis

Asset	Device	Module ID	Configuration	Importance		
				C	I	A
IDiPS-RPS	PLC	Bistable Processor (BP)	2 per channel	M	H	H
	PC	Cabinet Operator Module (COM)	1 per channel	M	H	M
	CIR-CUITS	Initiation Circuits (IC)	8 per channel	M	H	H
	CIR-CUITS	Watch Dog Timer (WDT)	External device	M	H	H

3.2 Threat Analysis

Threat is a risk element which attacks the vulnerabilities existing in the real systems. In the analysis of KNICS safety system it is identified that an authorized, an unauthorized, the environments, the system and their combination can be a threat. As well, an authorized and an unauthorized can be internal or external threat. Then we analyzed the effects from each threat to the KNICS systems.

3.3 Vulnerability Analysis

The scope of this analysis is defined as circled numbers in the fig. 1, which are determined on the basis of asset analysis. Table 2 is a part of this analysis. By

the checklist we developed 27 items are identified and by the scenario 7 items identified.

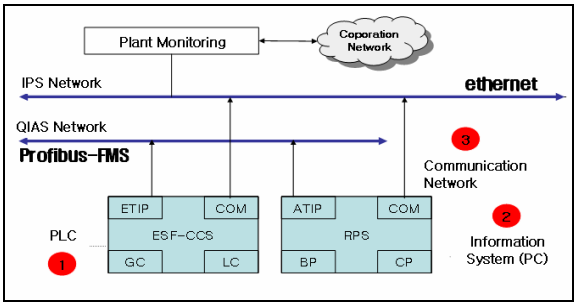

Fig. 1. The Scope of Vulnerability Analysis

Table 2: A Part of Vulnerability Analysis

Target	Vulnerability	Risk
PLC	Vulnerable to DoS Attack	L
PLC	No Authentication in Connection to RS232C Port in PLC	H
Inform. Sys.	DoS Attack to COM(QNX) Sys.	H
Comm. Network	Plaintext Data Transfer between COM to MCR	M
Comm. Network	No Data Integrity Check between COM to MCR	M

3.4 Risk Analysis

The risks are analyzed through the following steps. First the list of risks is derived from the threats and vulnerabilities identified. Then the three-level (high/medium/low) basis is developed based on the possibility of occurring risks and the degree of affection to the system when occurring risks. Next we calculate the degree of risk (R) by a simple equation, multiplication of the possibility of occurring risks (P) and the degree of affection (A). Table 3 shows a part of the analysis.

Table 3: A Part of Risk Analysis

List of risks	P	A	R	Asset
When accessing to PLC through pSET, an unauthorized or authorized people can upload malicious codes (control programs) and execute them.	H	H	H	A001-A003, A014~A016, A018, A019
With tapping or alteration of data being transferred between COM and IPS in MCR, the monitoring system in MCR can be mis-operated and it can make the operators in MCR confused.	M	M	H	A013,A029

3.5 Simulation Test

We confirmed, through the hacker simulation, that the risks identified in the previous steps can be occurred in the real systems. Especially the cabinet operator module (COM) system is more carefully analyzed since it has interfaces with non-safety grade control room devices.

3.6 Defensive Techniques and Strategy

Based on the results of risk analysis, we can choose the optimized defensive techniques and strategies generally used in IT industry for each risk.

Table 4: A Part of Defensive Techniques and Strategies

Risk	Policies /Guides	Defensive Techniques and Strategies
With tapping or alteration of data being transferred between COM and IPS in MCR, the monitoring system in MCR can be mis-operated and it can make the operators in MCR confused.	Important data being transferred to the external, should be in cryptograph .	Recommend that important data should be in cryptograph. However decrease of data transfer speed on networks can be anticipated, but it will be not severe because of the good quality of H/W and the use of UNIX for OS.

4. Cyber Security Policies and Plan

To apply the cyber security requirements to the design of KNICS safety systems, it is required to prepare the policies and the plan applicable to the overall design lifecycle. The results of risk assessment can provide us with the basic information for the design. The policies define design requirements for cyber security, and the plan specifies the detail activities and products for each design lifecycle.

5. Conclusions

Through the risk assessment we can obtain the supporting data for applying the new cyber security requirements to the KNICS safety systems. One thing to remember is that the isolation of safety systems from externals is not a unique solution to external cyber intrusions. In conclusion it is identified from this study that the application of cyber security technology is not difficult and in addition there is good infra around us [6].

REFERENCES

[1] U.S. NRC, Regulatory Guide 1.152, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants, Rev. 02, 2006.
[2] IAEA, Guidance on the Security of Computer Systems at Nuclear Facilities,
[3] U.S. CERT Control System Security Center, Case Study Series: Vol. 1.2, An Undirected Attack Against Critical Infrastructure: A Case Study for Improving Your Control System Security, Sep. 2005.
[4] NIST Special Publication 800-18, Guide for Developing Security Plans for Federal Information Systems, Rev. 01, Feb., 2006.
[5] KINS (Korea Institute of Nuclear Safety), Regulatory Guide KINS/GT-N27, Cyber Security of Instrumentation and Control Systems in Nuclear Facilities, Dec., 2007
[6] C. M. King, C. E. Dalton, T. E. Osmanoglu, Security Architecture: Design, Deployment and Operations, RSA Press, 2001.