Cyber Security Analysis by Attack Trees for a Reactor Protection System

Gee-Yong Park, Cheol Kwon Lee, Jong Gyun Choi, Dong Hoon Kim, Young Jun Lee, and Kee-Choon Kwon
Korea Atomic Energy Research Institute, I&C & HF Research Div.,
1045 Daedeok-daero, Yuseong-gu, Daejeon, 305-353, Korea
**Corresponding author: gypark@kaeri.re.kr*

1. Introduction

As nuclear facilities are introducing digital systems, the cyber security becomes an emerging topic to be analyzed and resolved. The domestic and other nation's regulatory bodies notice this topic and are preparing an appropriate guidance. The nuclear industry where new construction or upgrade of I&C systems is planned is analyzing and establishing a cyber security.

A risk-based analysis for the cyber security has been performed in the KNICS (Korea Nuclear I&C Systems) project where the cyber security analysis has been applied to a reactor protection system (RPS) [1]. In this paper, the cyber security analysis based on the attack trees [2] is proposed for the KNICS RPS.

2. System Description

The first thing to do in the cyber security analysis is the problem definition or the system description. The KNICS RPS consists of four redundant channels where each channel is further composed of two bistable processors (BPs), two coincidence processors (CPs), an automatic test and interface processor (ATIP), and a cabinet operator module (COM). A simplified schematic for a single channel of KNICS RPS is shown in Fig.1.

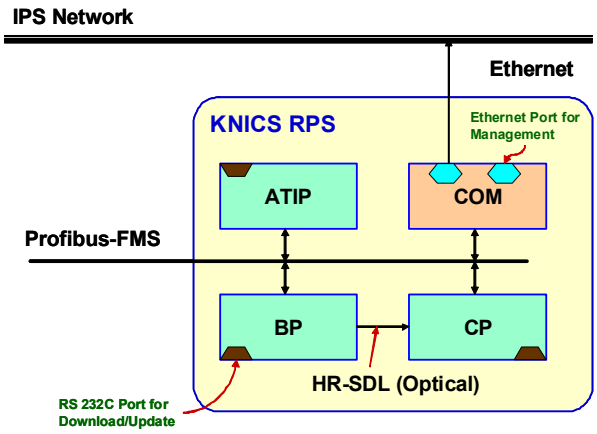

Fig. 1. Overall Schematic of KNICS RPS

The BP, CP, and ATIP have a same PLC platform and the COM is a safety-grade industrial PC. As can be seen in Fig.1, the KNICS RPS has its own network that is separated and isolated from external network such as the internet. The field devices for providing the necessary input signals for a trip function are connected to BPs via a hardwired connection. The communication between PLCs is based on the profibus-FMS. The trip signal from a BP is transferred to a CP via the HR- SDL.

Each PLC has a RS-232C port for communication with an engineering work station or a managerial computer for downloading a program into a PLC or modifying setpoints of trip variables. The COM has an Ethernet port for the connection with the information processing network (IPS) through which the operational information of the KNICS RPS is transferred. And it has also the other Ethernet port for management.

3. Cyber Security Analysis

This paper presents the cyber security analysis for the KNICS RPS in the following sequence: the asset assessment, the preliminary vulnerability identification, the attack tree construction, and the risk analysis.

For the cyber security for a digital safety system in nuclear power plants (NPPs), regulatory bodies require that the confidentiality, integrity, and availability (CIA) must be secured from cyber threats [3][4]. Regarding this fact, the cyber security analysis is performed with respect to the CIA perspective, and, in this paper, the cyber security analysis on the availability is proposed.

3.1 Asset Assessment

The asset for the cyber security is categorized into two classes: one is the direct asset and the other the indirect asset. The direct asset is the property which is directly affected when a compromise for the system occurs. The indirect asset is the property which is affected by the result of a loss of a direct asset.

The direct asset for the KNICS RPS is the set of the PLCs, the COM PC, and various networks. The indirect asset is the set of a trip malfunction, the misleading operational information, the plant safety, and so forth.

The direct assets that are assessed with respect to the CIA perspective are presented in table 1.

Table 1: Asset Assessment

System	Asset	Asset Description	Configuration	Importance		
				C	I	A
RPS	PLC	Bistable Processor (BP)	2 per channel	M	H	H
	PLC	Coincidence Processor (CP)	2 per channel	M	H	H
	PLC	ATIP	1 per channel	M	H	H
	PC	Cabinet Operator Module (COM)	1 per channel	M	H	M
	Network	HR-SDL		M	H	H
	Network	Profibus-FMS		M	H	M
	Network	Ethernet		M	H	M

3.2 Preliminary Vulnerability Identification

When the overall schematic and detailed mechanisms of the KNICS RPS are surveyed, a few vulnerabilities are identified in the COM and PLCs.

During the vulnerability identification, threats are also evaluated. Threat is a risk element which exploits a vulnerability existing in the systems. For the KNICS RPS, an authorized/unauthorized person, a system, and environments can be a threat. An authorized and an unauthorized person can be a insider or outsider.

3.3 Attack Tree Construction

Based on the vulnerabilities and threats, the attack trees are constructed. One sample of attack trees is shown in Fig.2. The attack trees in Fig.2 are for the availability of the KNICS RPS. This is a simplified version for the sake of better representation within the limited space.

The form of attack trees (at least, in the opinion of authors) is same as that of the fault trees and only difference is the subject to be focused. Fault trees are expanded downward by focusing the propagation or flow of a fault. But, the attack trees branch down by focusing on the success of an attack.

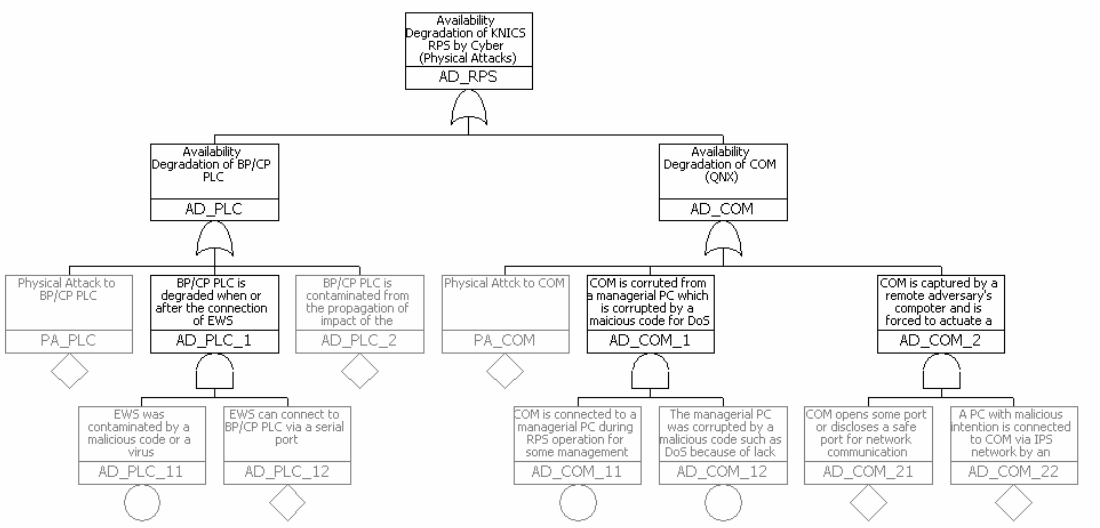

Fig. 2. Attack Trees for Availability of KNICS RPS

3.4 Risk Analysis

When attack trees for each of the CIA perspectives are constructed, the risk analysis is performed by considering the likelihood of an attack tree branch and the consequence from the success of an attack. The likelihood and consequence are evaluated qualitatively such as high, medium, and low, or quantitatively when the data for an evaluation is accumulated sufficiently.

Some intrusion/detection experiments can obviously supplement the decision of the attack possibility. In the KNICS project, various cyber attack experiments have been performed [1].

By analyzing attack branches, and by the aid of experimental results, the physical attacks such as PA_PLC and PA_COM are seemed to occur seldom. The attack event AD_PLC_2 to penetrate a PLC through a COM PC is nearly impossible, resulting from the intrusion experiment. The other events in Fig.2 are supposed to be possible and the degree of likelihood with their resulting effects is evaluated qualitatively.

For the attack event AD_PLC_1, the compromise of a PLC from a DoS (Denial-of-Serivce) attack can lead to a trip malfunction. The consequence of the attack event AD_COM_1 may affect the operating information to be displayed in the main control room. The event AD_COM_2 is plausible but its degree of occurrence is very low.

Numerous countermeasures for the cyber security have been proposed during the KNICS project [1] and a few treatments among them can be again extracted from the simplified attack trees. One is that a computer system which will be connected to a PLC should be checked so that any malicious/virus program must be prohibited from entering or be eliminated, if any and a validation mechanism between a computer and a PLC is required for disabling the connection of an unauthorized computer into a PLC.

REFERENCES

[1] C. K. Lee, et al., A Cyber Security Risk Assessment for the KNICS Safety Systems, Korean Nuclear Society Spring Meeting, Gyeongju, Korea, May 29-30, 2008.
[2] B. Schneier, Attack Trees - Modeling security threats, Dr. Dobb's Journal, pp.21-28, December, 1999.
[3] U.S. NRC, Regulatory Guide 1.152, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants, Rev. 02, 2006.
[4] KINS, Regulatory Guide KINS/GT-N27, Cyber Security of Instrumentation and Control Systems in Nuclear Facilities, Dec., 2007.