Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.3, Jun. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.3.639

원전 계측제어시스템 사이버보안 위험도 산정 프로세스

이 우 묘,†‡ 정 만 현, 민 병 길, 서 정 택
국가보안기술연구소

Risk Rating Process of Cyber Security Threats in NPP I&C

Woomyo Lee,†‡ Manhyun Chung, Byung-Gil Min, Jungtaek Seo
National Security Research Institute

요 약

2000년대 들어 아날로그기술 기반의 원전 계측제어시스템에 디지털기술이 적용되기 시작하였고 현재 국내에서 건설 중인 신월성 원전 2호기, 신고리 원전 3·4호기, 신울진 원전 1·2호기는 국산 MMIS가 적용된 한국형 원전 APR1400 디지털 계측제어시스템을 적용하고 있어 대부분의 장비가 디지털화 되었다. 이러한 디지털 장비는 기존 아날로그 장비에 비해 사이버공격에 취약하므로 원전 계측제어시스템의 사이버보안이 중요한 이슈로 부각되고 있다. 본 논문은 원전 계측제어시스템의 사이버보안 위협별 위험도산정 프로세스를 제안하고 원전계측제어시스템개발(KINCS) 사업에서 개발된 원자로보호계통에 제안하는 프로세스를 적용하여 RPS 노드 및 인터페이스의 위협별 위험도를 산출하였다.

ABSTRACT

SInce 2000, Instrumentation and Control(I&C) systems of Nuclear Power Plant(NPP) based on analog technology began to be applied to the digital technology. NPPs under construction in the country with domestic APR1400 I&C system, most devices were digitalized. Cyber security of NPP I&C systems has emerged as an important issue because digital devices compared to the existing analog equipment are vulnerable to cyber attacks. In this paper, We proposed the risk rating process of cyber security threats in NPP I&C system and applied the proposed process to the Reactor Protection System(RPS) developed through Korea Nuclear Instrumentation & Control System(KINCS) project for evaluating the risk of cyber security threats.

Keywords: risk rating process, NPP I&C system

I. 서 론

원전 계측제어시스템은 원자력발전소의 다양한 계통, 기기 및 장비로부터 각종 데이터를 취득, 분석, 처리하여 제어함으로써 원전의 안전 운전을 담당하는 중추신경계 역할을 수행한다. 2000년대에 아날로그기술 기반의 원전 계측제어계통에 디지털기술이 적용되기 시작하였고 현재 국내에 건설 중인 신월성 원전 2호기, 신고리 원전 3·4호기, 신울진 원전 1·2호기는 국산 MMIS가 적용된 한국형 원전 APR1400 디지털 계측제어시스템을 적용하고 있어 대부분의 장비가 디지털화 되었다. 이러한 디지털 장비는 기존 아날로그 장비에 비해 사이버공격에 취약하므로 원전 계측제어시스템의 사이버보안이 중요한 이슈로 부각되고 있다[1,2].

실제로 2010년에 스턱스넷(stuxnet) 공격이 발생하여 이란의 우라늄 추출 시설의 가동이 중단되었고, 2011년에는 스턱스넷과 유사한 MS-Word 제로데이 취약점을 이용하는 듀큐(duqu) 악성코드가 발견되었다[3,4]. 이러한 지능형지속위협(APT) 공격으로 인

접수일(2013년 10월 17일), 수정일(2015년 4월 13일), 게재확정일(2015년 4월 30일)
† 주저자, wmlee@nsr.re.kr
‡ 교신저자, wmlee@nsr.re.kr(Corresponding author)

하여 외부망과 물리적으로 분리된 원전 계측제어시스템도 사이버 공격에 영향을 받을 수 있다는 가능성이 지속적으로 제기되고 있다. 이에 따라 미국 원자력규제위원회(NRC), 원자력에너지협회(NEI), 국내 원자력안전기술원(KINS) 등에서는 원전 사이버보안을 위한 지침을 발표하고 있다[5-7].

원전 계측제어시스템에 효과적인 사이버보안 대책을 수립하기 위해서는 먼저 원전시스템을 정확히 이해하여 각 노드 및 인터페이스별 발생 가능한 보안위협을 도출하고 위험도를 분석해야 한다. 현재 IT/ICS 환경에서는 다양한 위험도 산정방법론이 제안되었으나 원전 환경을 고려한 위험도 산정 평가기준은 제안되지 않았다.

본 논문은 기존에 제안된 IT/ICS 환경에서의 위험도 산정방법론을 비교하여 OWASP 방법을 기반으로 한 원전 계측제어시스템 사이버보안 위험도 산정 프로세스를 제안한다. 보안위협 발생가능성과 영향도 산출에 사용되는 기준표를 작성함에 있어 세부항목을 원전의 환경과 특성을 고려하여 결정하고 각 세부항목에 점수를 부여하는 기준을 상세히 기술함으로써 원전에 적합한 위험도 산정 방법을 도출하였다. 또한 제안한 위험도 산정 프로세스를 원전 계측제어시스템 내의 원자로보호계통에 적용하여 위험도를 측정하였다.

2장에서는 보안위협 발생가능성 평가기준, 보안위협 영향도 평가기준, 위험도 산정식을 제시하여 제안하는 위험도 산정 방법의 프로세스를 설명한다. 3장에서는 원전계측제어시스템개발(Korea Nuclear Instrumentation and Control System, KNICS) 사업에서 개발된 원자로보호계통에 제안하는 위험도 산정 프로세스를 적용하여 원자로보호계통의 노드 및 인터페이스의 위협별 위험도를 산출하고 프로세스의 유효성을 점검한다.

II. 원전 사이버보안 위험도 산정 방법

본 장에서는 보안위협 발생가능성 평가기준, 보안위협 영향도 평가기준, 위험도 산정식을 제시하여 제안하는 위험도 산정 방법의 프로세스를 설명한다.

2.1 기존 IT/ICS 환경에서의 위험도 산정방법론

IT/ICS 환경에서는 다양한 위험도 산정방법론이 제안되었으며 대표적으로 OWASP, OCTAVE, ANSI/ISA-99, DREAD 산정 방법이 있다. 이러한 방법들은 공통적으로 보안위협 발생가능성과 영향도를 평가하여 위험도를 산출하고 있으며 위협 발생 가능성과 영향도를 나타내는 인자의 수와 산정결과의 표현방식에 차이가 있다[Table 1].

Table 1. Comparison of Risk Rating Methodology

	OWASP	ANSI/ISA-99	OCTAVE	DREAD
Institution	OWASP	ISA	Carnegie Mellon, SEI	Microsoft
Risk Rating Formula	Risk=Likelihood x Impact			R=D1+R+E+A+D2
Likelihood Rating	Average grade of L factor	Threat occurrence probability x Vulnerability exploit probability	Potential of threat scenarios	Sum of R,E,D2
Likelihood Factor	8	2	1	3
Likelihood Expression	L / M / H			3 ~ 9
Impact Rating	Average grade of I factor	Present L/M/H criterion	Imfact × Ranking weight	Sum of D1, A
Impact Factor	8	9	12	2
Impact Expression	L / M / H	Maximum value	Risk Score	2 ~ 6

OWASP 산정 방법은 평가대상의 특징을 반영하여 발생가능성과 영향도를 측정하는 세부 기준들을 정하고 평가에 활용하므로 다른 산정방법론에 비해 평가대상의 특성을 반영하기에 용이하다. 또한 발생가능성과 영향도 측정에 세부기준표를 사용함으로써 다수의 인터페이스와 노드가 존재하는 복잡한 시스템에서 발생가능성과 영향도의 값을 객관적으로 비교할 수 있다는 장점을 가진다.

따라서 본 논문에서는 OWASP의 평가기준표 방식을 기반으로 발생가능성과 영향도 산출에 사용되는 기준표를 작성함에 있어 세부항목을 원전의 환경과 특성을 고려하여 결정하고 각 세부항목에 점수를 부여하는 기준을 상세히 기술함으로써 원전에 적합한 위험도 산정방법을 도출하였다. 또한 발생가능성과 영향도 측정에 사용될 세부기준표를 작성함으로써 다수의 인터페이스와 노드가 존재하는 복잡한 원전 계측제어시스템에서 위협별 발생가능성과 영향도의 값을 객관적으로 비교할 수 있다.

2.2 원전 사이버보안 위험도 산정 프로세스

원전 계측제어시스템은 크게 원자로의 안전 운행을 보장하는 안전계통과 전력생산의 효율성과 관련된 비안전계통으로 구분하며 계통의 기능 및 특성에 따라 다시 세부 계통으로 구분된다. 세부 계통은 다수의 노드 및 인터페이스로 구성되며 각 계통별로 사이버보안 위험도를 산정하여 효율성과 가독성을 높일 수 있다.

본 논문에서 제안하는 위험도 산정 프로세스는 〔그림 1〕과 같다. 1) 원전 계측제어시스템에서 발생 가능한 보안위협의 집합을 식별한다. 2) 위험도 산정을 수행할 대상 계통의 노드 및 인터페이스를 파악하여 각각의 노드 및 인터페이스별 발생 가능한 보안위협을 앞서 식별한 보안위협 집합에서 맵핑한다. 3) 대상 계통 내의 노드 및 인터페이스 별 보안위협 발생가능성(L)과 보안위협 영향도(I)를 발생 가능한 위협별로 측정한다. 2.3장에서는 보안위협 발생가능성 평가 기준과 평가방법을 제시하고 2.4장에서는 보안위협 영향도 평가기준과 평가방법을 제시한다. 4) 측정된 보안위협 발생가능성과 보안위협 영향도 값을 위험도 산정식에 적용하여 노드 및 인터페이스별 보안위협의 위험도를 상중하로 도출한다. 2.5장에서는 위험도 산정식을 설명한다.

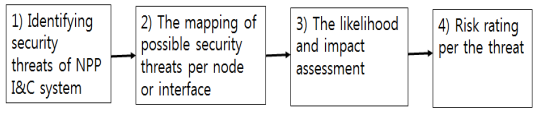

Fig. 1. Risk Rating Process

2.3 보안위협 발생가능성 평가 방법

원전 계측제어시스템은 다양한 원인에 의해 보안위협이 발생할 수 있으며, 위협의 종류와 각 노드 및 인터페이스의 특징에 따라 위협의 발생가능성 또한 달라진다. 여기서 보안위협이 발생함은 공격자의 침투, 즉 기기에 대한 공격이 성공했음을 의미한다. 즉 위협 발생가능성이 높을수록 공격이 성공할 가능성이 높아지는 것을 위미하므로 위협의 위험도가 높아진다.

본 절에서는 위협별로 원전 계측제어시스템의 노드 및 인터페이스에서의 위협 발생가능성을 평가하기 위해 〔Table 2〕와 같이 4개의 항목을 정하고 각 항목별로 세부 평가 기준을 세웠다.

평가 항목은 공격자 기술(L1), 공격기회(L2), 취약점 발견의 용이성(L3), 침입탐지 가능성(L4)으로 구분되며 각 항목별로 정량적인 평가를 수행할 수 있도록 기준을 정의하고 점수를 부여하였다. 공격자 기술(L1)은 해당 보안위협을 가하기 위해 필요로 하는 공격자의 수준을 나타낸다. 필요한 공격자의 기술수준이 낮을수록 쉽게 공격을 가할 수 있으므로 보안위협 발생가능성이 높아진다. 공격기회(L2)는 공격자가 각각의 노드 및 인터페이스에 해당 보안위협을 가하기 위해 필요한 접근 경로를 나타낸다. 공격자가 노드 및 인터페이스에 네트워크 망을 통해 접근할 수 있으면 다른 노드를 공격에 활용할 수 있으므로 직접 노드 및

Table 2. Security Threat Likelihood Criteria

Factor	Criteria	Score
Attacker technology (L1)	The attacker has a design and internal structure knowledge of NPP I&C system.	1
	The attacker has hacking expertise and the ability of penetration test.	3
	The attacker can use the tool is released.	7
	The attacker has the IT knowledge.	9
Attack opportunity (L2)	An attacker can be accessed locally.	1
	An attacker can be accessed through the internal network.	5
	An attacker can be accessed through the external network.	9
Ease of vulnerabilities (L3)	It is almost impossible.	1
	Analyze the vulnerability of similar industrial control systems.	3
	Using various means, such as social engineering methods.	7
	Using automated tools to find the vulnerability (nessus, metasploit)	9
Intrusion detection possibilities (L4)	Because real-time intrusion detection and alarm occurs, the administrator can check immediately.	1
	Logs are stored and periodically review the logs.	3
	Log is stored and does not periodically reviewed the log.	7
	Log is not stored.	9

인터페이스에 로컬로 접근할 때보다 상대적으로 공격의 가능성이 높아진다. 취약점 발견의 용이성(L3)은 공격자가 해당 보안위협과 관련된 취약점을 발견하기 위해 필요한 노력과 비용의 정도를 나타내며 취약점 발견이 용이할수록 해당 보안위협의 발생가능성이 높아진다. 침입탐지 가능성(L4)은 공격이 탐지될 가능성을 나타내며, 공격의 탐지가 지연될수록 보안위협의 발생가능성이 높아진다.

4개의 평가 항목 외에도 〔Table 3〕과 같이 공격동기(L5), 취약점 활용의 용이성(L6), 취약점이 알려진 정도(L7)를 평가항목으로 추가할 수 있다. 공격동기(L5)는 다양하며 이를 수치화 하는 것에 한계가 있으므로 본 위험도 평가에서는 제외하였다. 취약점 활용의 용이성(L6)과 취약점이 알려진 정도(L7)는 각각 발견된 취약점을 활용하여 공격하기 위해 필요한 노력의 정도와 취약점의 활용도를 나타내는 것으로 취약점 분석을 통해 발견된 취약점이 정리되어 있을 경우 위험도 평가에 활용될 수 있다.

Table 3. Security Threat Likelihood Criteria (Optional)

Factor	Criteria	Score
Attack motivation (L5)	Strategic attack by other countries. (Cyber War)	1
	Political attack by some individuals and groups. (Hacktivism)	5
	Attacked for showing off by some individuals and groups.	9
Ease of exploit (L6)	Theoretically, it is possible.	1
	It must be produced in a complicated form of program that can take advantage of the attack. (Stuxnet)	4
	Easily it can be implemented by making the program.	7
	The tools to take advantage of the publicly disclosed vulnerability exists. (metasploit)	9
Vulnerability disclosure (L7)	New and unknown vulnerabilities	1
	Uncommon vulnerability	3
	Obvious vulnerability known to the security personnel and systems	7
	Vulnerabilities that everyone knows	9

3장에서는 〔Table 2〕의 4개 항목을 이용하여 원전 계측제어시스템개발(KINCS) 사업에서 개발된 원자로보호계통에서의 보안위협 발생가능성을 평가하였다.

2.4 보안위협 영향 평가 방법

위협의 종류와 각 노드 및 인터페이스의 특징에 따라 위협이 발생하였을 때 주변 시스템에 미치는 피해 정도는 달라진다. 위협 영향도가 높을수록 공격이 미치는 피해가 커지는 것을 의미하므로 위협의 위험도가 높아진다. 원전 계측제어시스템에서 보안위협이 발생할 경우 결과적으로 트립을 유발할 수 있고 최악의 경우 노심 용융 등을 통한 방사능 유출로 인해 국가 전체에 피해를 줄 수 있다. 따라서 원전 계측제어시스템에서는 발생가능성이 적을지라도 영향도가 큰 위협들에 대해 철저한 대책마련이 필요하다는 특징을 가진다. 본 절에서는 위협별로 원전 계측제어시스템의 노드 및 인터페이스에서의 위협 영향도를 평가하기 위해 〔Table 4〕와 같이 6개의 항목을 정하고 각 항목별로 세부 평가 기준을 세웠다.

평가 항목은 가용성 피해(I1, I2), 무결성 피해(I3), 기밀성 피해(I4, I5), 재정적 영향(I6)으로 구분되며 각 항목별로 정량적인 평가를 수행할 수 있도록 기준을 정의하고 점수를 부여하였다.

가용성 피해(I1, I2)는 각각 위협이 발생한 노드 및 인터페이스의 기능 중단 기간과 기능 중단으로 인해 발생하는 주변 시스템의 피해범위를 나타낸다. 특정 노드 및 인터페이스가 중단될 경우 중단기간이 길어지고 영향을 미치는 계통의 범위가 넓어질수록 주변 시스템에 미치는 영향이 커지게 된다. 무결성 피해(I3)는 데이터 위변조로 인한 주변 시스템의 피해범위를 나타내며 영향을 미치는 계통의 범위가 넓어질수록 주변 시스템에 미치는 영향도가 높아진다. 기밀성 피해(I4, I5)는 각각 위협이 발생하였을 때 하나의 노드 및 인터페이스를 통해 유출되는 데이터의 종류와 중요성을 나타낸다. 여러 노드의 정보를 저장하고 있는 노드일 경우 하나의 노드에 위협을 가함으로써 다수의 노드의 정보를 유출할 수 있으므로 영향도가 커지게 되고, 유출되는 데이터가 단순 상태정보가 아닌 내부 시스템 정보일 경우 영향도가 커지게 된다. 마지막으로 재정적 영향(I6) 항목은 발전소의 가동률에 따른 피해규모를 나타내며 위협이 발생하여 원전에 트립이 발생할 경우 전력수급에 문제가 생기고 정전을 유발하

Table 4. Security Threat Impact Criteria

Factor	Criteria	Score
Availability (I1)	Normal operation of the node(system)/interface.	0
	Suspending the node(system)/interface.	5
	Completely stop of node(system)/interface.	9
Availability (I2)	Normal operation of the node(system)/interface.	0
	Causing problems within the same operation system.	5
	Causing problems on other operating systems.	9
Integrity (I3)	Normal operation of the node(system)/interface.	0
	Information forgery of a single node(system)/interface.	3
	Information forgery of multiple node(system)/interface.	6
	The forgery information can be transferred to the other system.	9
Confidentiality (I4)	Information was not exposed in a single node/interface.	0
	Exposure information for a single node/interface.	3
	Exposure information for multiple node / interface	6
	Exposure information over the various system	9
Confidentiality (I5)	Normal operation of the node(system)/interface.	0
	Leakage the status information.	5
	Leakage inside the system information and control information.	9
Financial impact (I6)	Normal operation.	0
	Trip generation.	5
	Reactor core melt.	9

여 재정적 피해가 발생된다. 또한 특정 공격으로 인해 노심 용융이 발생할 경우 국가적으로 막대한 재정적 피해가 발생될 것이다.

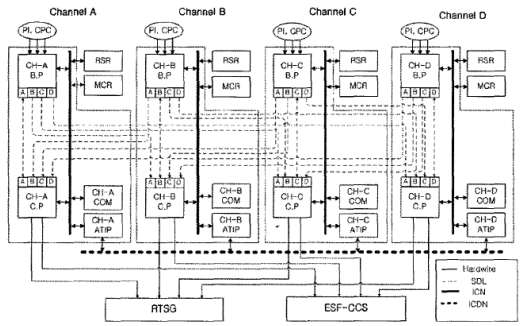

Fig. 2. RPS 4-Channel Configuration

3장에서는 〔Table 4〕의 6개 항목을 이용하여 원전계측제어시스템개발(KINCS) 사업에서 개발된 원자로보호계통에서의 보안위협 영향도를 평가하였다.

2.5 보안위협 영향 평가 방법

본 절에서는 보안위협 발생 가능성(L) 평가 결과값과 보안위협 영향(I) 평가 결과값을 이용하여 위험도를 상중하로 평가하는 방법을 설명한다. 〔Table 5〕는 보안위협의 위험도를 상중하 단계로 구분하는 산정식이다. 보안위협 발생가능성 평가를 위해 2.3절에 정리된 4가지 항목(L1~L4) 각각을 평가한 결과 값의 평균값과 보안위협 영향 평가를 위해 2.4절에서 정리한 6가지 항목(I1~I6) 각각을 평가한 결과값의 평균값을 곱하여 N2 이상일 경우 상(H), N1 이상이고 N2 미만일 경우 중(M), N1 미만일 경우 하(L)로 분류한다. 위험도 상중하 값은 상대적인 값이므로 단순히 결과값의 범위를 삼등분 하는 것 보다는 상중하의 분포가 확연히 보이는 구간을 N1과 N2의 값으로 선택하여 의미 있는 결과를 도출할 수 있다.

3장에서는 위험도 산정식을 이용하여 원전계측제어시스템개발(KINCS) 사업에서 개발된 원자로보호계통에서의 보안위협 위험도를 상중하로 평가하였다.

Table 5. Risk Rating Model

	Risk Rating Formula
H	$N_2 \le \left(\sum_{i=1}^{4}\frac{I_i}{4}\right)\times\left(\sum_{i=1}^{6}\frac{I_i}{6}\right)$
M	$N_1 \le \left(\sum_{i=1}^{4}\frac{I_i}{4}\right)\times\left(\sum_{i=1}^{6}\frac{I_i}{6}\right) < N_2$
L	$\left(\sum_{i=1}^{4}\frac{I_i}{4}\right)\times\left(\sum_{i=1}^{6}\frac{I_i}{6}\right) < N_1$

III. 사이버보안 위험도 산정 프로세스 적용사례

본 장에서는 원전계측제어시스템개발(KINCS) 사업에서 개발된 원자로보호계통에 제안하는 위험도 산정 프로세스를 적용하여 원자로보호계통의 노드 및 인터페이스의 위협별 위험도를 산출하고 프로세스의 유효성을 점검한다.

3.1 KINCS 원자로보호계통 개요

원자로보호계통(Reactor Protection System, RPS)는 원자력발전소 안전관련 운전변수가 설정된 운전범위를 초과할 경우 자동으로 트립을 발생시켜 원자로를 정지시키고 공학적안전설비-기기제어계통(ESF-CCS)의 작동을 개시하는 기능을 수행한다. RPS는 동일한 4개의 채널이 물리적·전기적으로 독립성을 유지하고 있으며 RPS를 구성하는 노드는 다음과 같다.

- 비교논리프로세서(BP) : 공정계측신호를 입력받아 디지털신호로 변환하고 트립설정치와 운전우회 조건에 의해 트립여부를 결정
- 동시논리프로세서(CP) : 자기채널 4개의 채널에서 입력된 트립변수에 대한 2/4 동시논리를 수행하여 트립을 판단하고 개시회로를 통해 원자로 정지와 ESF-CCS의 기능개시 신호를 출력
- 자동시험 및 연계프로세서(ATIP) : 해당 채널을 구성하는 모듈들의 기능이 정확하게 작동하고 있는지를 시험하고 상태정보를 수집
- 캐비닛운전원모듈(COM) : RPS의 인간기기연계(MMI) 수단으로 계통의 운전상태를 감시하고 주기시험 및 보수를 수행
- ESF-CCS 시험 및 연계프로세서(ETIP) : ESF-CCS의 ATIP

또한 각 노드를 연결하는 인터페이스는 다음과 같다.

- E1 : BP와 CP 사이에서 SDL통신으로 트립정보 전달
- E2 : BP와 ATIP 사이에서 SDN통신으로 BP 상태정보 및 시험결과 전달
- E3 : CP와 ATIP 사이에서 SDN통신으로 CP 상태정보 및 시험결과 전달
- E4 : ATIP와 COM 사이에서 SDN통신으로 ATIP 수집정보 전달
- E5 : ATIP와 BP 및 CP 사이에서 SDN통신으로 상태시험 시작정보 전달
- E6 : ATIP와 ATIP B/C/D 사이에서 SDN통신으로 ATIP 수집정보 전달
- E7 : ATIP와 ETIP 사이에서 SDL통신으로 ATIP 수집정보 및 ETIP 수집정보 전달
- E8 : CP와 ESF-CCS 사이에서 SDL통신으로 트립 개시신호 전달

3.2 RPS 위험도 산정 프로세스 적용사례

〔Table. 6〕은 제시한 위험도 산정 프로세스를 통해 RPS 계통에서의 위험도를 산정한 결과이다. 프로세스의 진행과정을 간략히 설명하면 아래와 같으며, 각각의 프로세스를 좀 더 자세히 설명한다.

1) 9개의 보안위협 식별

Table 6. Risk Rating Results of RPS

Threat		Denial of service attacks			Malware propagation			Data leakage			Data forgery			Unauthorized remote services			External network connection			Removable media, Ext H/W connection			Physical access attacks			Human error and sabotage			
		L	I	R	L	I	R	L	I	R	L	I	R	L	I	R	L	I	R	L	I	R	L	I	R	L	I	R	
Node	BP	4.5	2.5	M				4.5	2.0	M	4.5	1.8	L	6.5	5.5	M	5.5	5.5	M	3.5	6.2	M	5.0	3.2	M	6.0	3.2	M	
	BP	4.5	3.2	M				4.5	2.0	M	4.5	3.0	M	6.5	6.7	H	5.5	7.3	H	3.5	8.0	M	5.0	3.8	M	6.0	3.8	M	
	ATIP	4.5	0.8	L				4.5	1.8	L	4.5	1.5	L	6.5	4.2	M	5.5	4.2	M	3.5	5.7	M	5.0	1.5	L	6.0	1.5	M	
	ETIP										4.5	1.5	L																
	COM	6.0	0.8	L				6.0	1.8	M				6.5	4.2	M	6.5	4.2	M	5.0	5.7	M	6.5	1.5	M	7.5	1.5	M	
Interface	E1				3.5	5.7	M																						
	E2				6.0	6.7	H	6.0	1.8	M	6.0	1.0	L																
	E3				6.0	6.7	H	6.0	1.8	M	6.0	1.0	L																
	E4				6.0	6.7	H	6.0	1.8	M																			
	E5				6.0	6.7	H	6.0	1.8	M																			
	E6				6.0	6.7	H	6.0	1.8	M																			
	E7				3.5	5.7	M																						
	E8				3.5	6.3	M																						

2) 보안위협이 발생가능한 노드 및 인터페이스 맵핑 ('서비스 거부공격'은 BP, CP, ATIP, COM 노드에서 발생 가능함)
3) 각각의 보안위협마다 맵핑된 노드 및 인터페이스에서의 보안위협 발생가능성(L) 및 영향도(I)를 평가
4) 위험도 산정모델을 적용하여 RPS 계통 노드 및 인터페이스의 위협별 위험도를 상중하로 도출

3.2.1 원전 계측제어시스템 보안위협 식별

본 논문에서는 기존 IT/ICS 환경에서의 보안위협을 활용하여 원전 계측제어시스템에서 발생 가능한 보안위협의 목록을 다음과 같이 정리하였다. 원전 계측제어시스템의 특성에 따라 보안위협이 추가되거나 삭제 될 수 있다.

- (분산)서비스거부공격, (D)DoS : 서버 및 네트워크를 공격하여 정상적인 서비스를 하지 못하도록 하는 공격으로 네트워크 트래픽을 증폭시키거나 시스템의 자원(CPU, Memory 등)을 소모하도록 하여 정상적인 서비스를 지연 또는 불능상태로 만들기 위해 사용하는 위협
- 악성코드 전파 : 네트워크를 통해 악성코드가 자신을 복제하고 전파하여 네트워크를 사용하는 시스템을 감염시키는 위협
- 데이터 유출 : 시스템 및 운영 서비스 설정정보, 데이터베이스, 로그 및 감사 데이터 등의 시스템 내부 정보, 시스템이 타 시스템에서 수집하는 시스템 외부정보, 네트워크상에서 교환되는 정보 등을 취득하여 유출하는 위협
- 데이터 위변조 : 시스템 내부 정보, 시스템 외부 정보, 네트워크상에서 교환되는 정보 등을 취득하여 계측제어 시스템을 제어하는 명령 또는 계통의 상태정보를 포함한 메시지를 위변조하는 위협
- 비인가 원격 서비스 : 제품 공급자 및 외부 서비스 공급자가 유비보수나 관리를 위해 설치한 비인가 원격서비스 또는 원전 운영에 불필요한 서비스를 제거하지 않아 원격으로 시스템 접속이 발생하는 위협
- 외부망(인터넷)과의 연결 ; 조직 내부망에 인터넷망과의 접점이 존재 할 경우 외부에서 인터넷망을 이용하여 공격하는 위협
- 이동매체 · 외부 H/W 연결 : 데이터 백업 및 이동을 위하여 사용하는 이동식 매체 및 노트북 등의 외부 H/W를 통하여 악성코드가 원전 계측제어시스템으로 감염되는 위협
- 물리적 접근 공격 : 시스템에 대한 물리적 접근을 통한 위협
- 사람의 실수와 사보타지 : 운전원, 시스템 관리자의 실수 및 사보타지에 의한 위협

3.2.2 RPS 노드 및 인터페이스별 발생 가능한 보안위협 맵핑

앞에서 정의한 9개의 보안위협은 원전 계측제어시스템의 모든 노드 및 인터페이스에서 발생되는 것이 아니므로 노드 및 인터페이스 별 발생 가능한 위협을 맵핑하였다.

각각의 노드 및 인터페이스에서 발생 가능한 위협들은 노드 및 인터페이스의 통신방법, 저장 및 전송하는 데이터의 종류, 연계되는 계통 등 노드 및 인터페이스의 특성에 따라 위협의 위험도가 달라질 수 있다. 다음은 RPS의 노드 및 인터페이스 별 발생 가능한 위협을 맵핑한 것이다.

- BP 데이터 위변조
  BP는 채널정보를 분석하고 트립 필요할 때 CP로 트립신호를 전송한다. 공격자는 트립신호를 삭제하여 트립이 필요한 상황에서 트립신호가 아닌 정상신호를 송신 할 수 있다(E1). BP에 문제가 발생하였을 때 BP가 ATIP로 전송하는 상태정보를 삭제하거나 단순 상태정보로 변조하여 전송함으로써 운영자의 위험 감지를 방해할 수 있다(E2).
- CP 데이터 위변조
  CP에 문제가 발생하였을 때 CP가 ATIP로 전송하는 상태정보를 삭제하거나 단순 상태정보로 변조하여 전송함으로써 운영자의 위험 감지를 방해할 수 있다(E3). CP는 트립신호를 수신하고 트립을 판단하여 ESF-CCS 개시신호를 전송한다. 공격자는 CP에서 ESF-CCS 개시신호를 위변조하여 ESF-CCS 가동에 문제를 발생 시킬 수 있다(E8).
- ATIP 데이터 위변조
  ATIP는 CP, BP의 상태정보를 COM에 전송한다. 공격자가 전송정보를 삭제하거나 단순 상태정보로 변조하여 COM에 전송할 경우 운영자는 위험을 감지할 수 없게 된다(E4). ATIP에서

BP, CP의 상태체크 및 운전우회관련 신호를 변조하여 상태체크 및 운전우회를 공격자 의도대로 실행하게 할 수 있다(E5). ATIP가 타채널의 ATIP에 상태정보를 전송한다. ATIP에서 타 채널의 ATIP에 상태정보를 변조하여 공격자가 의도하는 상태정보를 전송한다(E6).

- ETIP 데이터 위변조
  동일 채널의 ESF-CCS에 있는 ETIP에 ATIP에서 수집한 상태정보를 변조하여 공격자가 의도하는 상태정보를 전송한다(E7). COM 데이터 위변조
  공격자가 COM에서 전송정보를 삭제하거나 단순 상태정보로 변조할 경우 운영자는 위험을 감지할 수 없게 된다.
- BP, CP, COM, ATIP 서비스거부공격
  노드 및 시스템이 인터페이스를 통해 연결된 시스템에 서비스거부공격을 시행하여 정상적인 운전을 방해 할 수 있다.
- BP, CP, COM, ATIP 데이터 유출
  시스템 및 운영 서비스의 설정정보 및 시스템 정보를 수집하여 외부로 유출 할 수 있다.
- BP, CP, COM, ATIP 비인가 원격 서비스
  시스템의 공급자 및 관리자가 유지보수 및 관리의 편이성을 위해 원격서비스 이용하거나 원전 운영에 불필요한 서비스를 제거하지 않아 원격으로 시스템 접속이 가능 할 수 있다.
- BP, CP, COM, ATIP 외부망(인터넷)과의 연결
  외부망(인터넷)과의 접점이 존재하여 외부에서 공격이 발생 할 수 있다.
- BP, CP, COM, ATIP 이동매체·외부 H/W 연결
  데이터 백업 및 유지보수를 위한 이동식 매체 및 외부 H/W의 연결을 통하여 악성코드가 감염 될 수 있다.
- BP, CP, COM, ATIP 물리적 접근
  물리적 접근이 용이하면 공격자에게 데이터 위변조, 악성코드 삽입 등 다양한 공격의 기회를 제공할 수 있다. 또한 물리적인 파괴를 통해 정상적인 동작을 방해할 수 있다.
- BP, CP, COM, ATIP 사람의 실수와 사보타지
  시스템 관리자 및 유지보수 책임자의 실수 및 사보타지에 의해 문제가 발생 할 수 있다.
- E2(BP, ITP) 데이터 위변조
  공격자는 BP에서 전송하는 상태정보를 SDN망을 사용하는 COM을 통해 정보를 획득하여 다시 ATIP에 재전송하여 운영자에게 잘못된 정보를 제공 할 수 있다.
- E3(CP, ITP) 데이터 위변조
  공격자는 CP에서 전송하는 상태정보를 SDN망을 사용하는 COM을 통해 획득하여 다시 ATIP에 재전송하여 운영자에게 잘못된 정보를 제공할 수 있다.
- E2, E3, E4, E5, E6 데이터 유출
  공격자에 의해 시스템 및 노드 간 데이터 통신을 할 때 암호화되지 않은 통신 데이터를 사용하여 데이터가 유출될 수 있다.
- 모든 인터페이스 악성코드 전파
  악성코드가 감염된 시스템 및 노드에서 인터페이스가 연결된 시스템으로 전파 될 수 있다.

3.2.3 RPS 보안위협 발생가능성(L)과 영향도(I) 평가

보안위협 맵핑 결과에서 알 수 있듯이 하나의 보안위협이 모든 노드 및 인터페이스에 적용되지는 않으므로 각 보안위협마다 해당 노드 및 인터페이스에서의 보안위협 발생가능성과 영향도를 평가해야 한다. 예를 들어 '서비스 거부공격'은 BP, CP, ATIP, COM 노드에 발생 가능하며 EITP 노드와 인터페이스에는 맵핑되지 않는다. 따라서 BP, CP, ATIP, COM 노드에서 서비스거부공격의 발생가능성과 영향도를 발생가능성 평가 기준표와 영향 평가 기준표를 이용하여 평가하고 각각의 평균값을 계산한다. 나머지 8개의 위협에 대해서도 각각 맵핑되는 노드 및 인터페이스에서

Table 7. Likelihood and Impact of DoS attack in RPS

Node	Likelihood						Impact							
	L1	L2	L3	L4	Sum	Avg	I1	I2	I3	I4	I5	I6	Sum	Avg
BP	1	5	3	9	18	4.5	5	5	0	0	0	5	15	2.5
BP	1	5	3	9	18	4.5	5	9	0	0	0	5	19	3.2
ATIP	1	5	3	9	18	4.5	5	0	0	0	0	0	5	0.8
COM	3	5	7	9	24	6.0	5	0	0	0	0	0	5	0.8

Table 8. Risk of DoS attack in RPS

노드	$\left(\sum_{i=1}^{4}\frac{I_i}{4}\right)\times\left(\sum_{i=1}^{6}\frac{I_i}{6}\right)$	Risk
BP	11.25	M
CP	14.4	M
ATIP	3.6	L
COM	4.8	L

의 보안위협 발생가능성과 영향도를 〔Table 7〕과 같이 평가한다.

3.2.4 위협별 위험도 상중하 도출

위험도 산정 프로세스의 마지막 단계로 보안위협 발생가능성과 영향도 평가결과를 앞에서 제시한 위험도 산정식에 적용하여 각각의 노드 및 인터페이스에서 보안위협들의 위험도를 상중하로 표현한다. 〔Table 8〕은 RPS 계통에서 서비스거부공격의 보안위협 발생가능성과 영향도 평가 값을 위험도 산정식에 적용한 것으로 N1과 N2의 값을 각각 9와 36으로 정하여 상중하를 산출하였다.

3.3 위험도 산정 프로세스의 활용

안전계통의 경우 강력한 수준의 안정성을 요구하고 있으므로 위험도가 하(L)일지라도 위협을 제거할 수 있는 보안대책을 적용해야 한다. 따라서 위험도 평가를 통해 상중하의 단계를 구분하는 것이 위험도가 낮은 위협에 대한 대책을 소홀히 해도 된다는 뜻으로 받아들여서는 안 될 것이다. 안전계통에서의 위험도 평과 결과표는 9개의 보안위협이 원전 각 계통에서 어떠한 노드 및 인터페이스에 위험도를 얼마만큼 가지고 있는지를 한눈에 살펴볼 수 있다는 점에서 의미를 가진다. 반면 비안전계통의 경우 안전계통에 비해 상대적으로 낮은 안전성이 요구되며 상용 시스템들이 사용되고 있는 특징을 가진다. 따라서 위험도 평가를 통해 위험도를 상중하 단계로 구분하고 상의 위험도를 가지는 위협에 대해 우선적으로 보안대책을 적용하는 방식으로 위험도 평가 방법을 활용할 수 있을 것으로 예상된다.

IV. 결 론

본 논문은 중추신경계 역할을 수행하는 원전 계측제어시스템의 위협별 위험도산정 프로세스를 제안하고 원전계측제어시스템개발(KINCS) 사업에서 개발된 원자로보호계통에 제안하는 프로세스를 적용하여 RPS 노드 및 인터페이스의 위협별 위험도를 산출하였다.

위험도 산정을 위해 보안위협 발생 가능성 평가 항목 4가지와 보안위협 영향도 평가 항목 6가지를 설계하였으며, 각 항목의 정량적인 평가가 가능하도록 항목별 세부 기준을 정의하고 0~9점의 점수를 부여하였다. 또한 위험도 산정식을 설계하여 보안위협 발생가능성 및 영향도 평가 결과를 이용하여 위협의 위험도를 상중하로 구분하였다.

제시한 위험도 산정 프로세스는 원전 사이버보안 대책수립의 준비단계로 원전에 사이버보안 위협이 각각의 기기 및 인터페이스에 얼마만큼의 위험도를 가지는지 분석하고 보안대책 우선순위를 결정하는데 활용될 수 있다.

References

〔1〕 Lee Cheol Kwon, "Nuclear Power Plant Instrumentation and Control Systems Cyber Security Technology Trends," Jonornal of The Korea Institute of information Security & Cryptology, 22(5), 28-34, Aug. 2012

〔2〕 Jaekwan Park, JeYun Park, Youngki Kim, "Cyber Security Consideration on Digital Instrumentation and Control System Development Process in Nuclear Power Plants," Journal of Korean Institute of Information Scientists and Engineers, 39(1D), 354-356, Jun. 2012

〔3〕 Nicolas Falliere, Liam O Murchu, Eric Chien, "W32.Stuxnet Dossier," Symantec Security Response, Rev. 1.4, Feb. 2011

〔4〕 B. Bencsath, G. Pek, L. Buttyan, and M. Felegyhazi. "Duqu: Analysis, detection, and lessons learned," In ACM European Workshop on System Security(EuroSec), volume 2012, Apr. 2012

〔5〕 Nuclear Regulatory Commission, "Cyber Security Programs for Nuclear Facilities," NRC Regulatory Guide 5.71,

Jan. 2010
〔6〕 Nuclear Energy Institute, "Cyber Security Plan for Power Reactors," NEI 08-09, Jan. 2010
〔7〕 Korea Institute of Nuclear Safety, "Cyber security of instrumentation and control systemsCyber security of instrumentation and control systems," KINS/RG-NO 8.22, 681-688, 2011

〈저자소개〉

사 진

이 우 묘 (Woomyo Lee) 정회원
2010년 2월: 경북대학교 전자전기컴퓨터학부 졸업
2012년 2월: 포항공과대학교 전자공학과 석사
2011년 12월~현재: 국가보안기술연구소 연구원
〈관심분야〉 정보보호, 제어시스템 보안

사 진

정 만 현 (Manhyun Chung) 정회원
2006년 2월: 동국대학교 컴퓨터학과 학사
2009년 2월: 고려대학교 정보경영공학대학원 석사
2012년 8월: 고려대학교 정보보호대학원 박사수료
2012년 9월~현재: 국가보안기술연구소 연구원
〈관심분야〉 정보보호, 원자력보안, 제어시스템 보안, 침입탐지시스템

사 진

민 병 길 (Byung-gil Min) 정회원
2002년 2월: 충북대학교 컴퓨터공학과 졸업
2004년 2월: 포항공과대학교 컴퓨터공학과 석사
2004년 3월~현재 국가보안기술연구소 선임연구원
〈관심분야〉 원자력보안, 제어시스템 보안, 취약성 분석평가, 정보보안관리체계

사 진

서 정 택(Jungtaek Seo) 종신회원
1999년 2월: 충주대학교 컴퓨터공학과 졸업
2001년 2월: 아주댛가교 컴퓨터공학과 석사
2006년 2월: 고려대학교 정보보호대학원 정보보호공학 공학박사
2000년 11월~현재: 국가보안기술연구소 책임연구원
〈관심분야〉 스마트그리드 보안, 제어시스템 보안, 원자력 사이버보안, 취약성 분석평가, DDoS 공격 탐지 및 대응