Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.3, Jun. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.3.561

원전 디지털 계측제어시스템 사이버보안 기술 체계 수립 방법 연구*

정 만 현,† 안 우 근, 민 병 길, 서 정 택‡
ETRI 부설연구소

A Study on Method to Establish Cyber Security Technical System in NPP Digital I&C*

Manhyun Chung,† Woo-Geun Ahn, Byung-gil Min, Jungtaek Seo‡
The Attached Institute of ETRI

요 약

원자력 발전소(이하 원전)의 계측제어시스템은 원자력 발전소를 안전하게 운전하기 위한 설비로 아날로그 기술에서 디지털기술로 변하고 있다. 그리고 2010년 이란의 부셰르 원자력 발전소의 원심분리기의 가동을 중단시킨 스턱스넷 공격으로 인해 원전의 사이버공격의 가능성이 많이 증가하고 있다. 하지만 국내외 원전 디지털 계측제어시스템의 사이버보안 강화를 위해 발간된 규제지침들은 보안요구사항들과 정책 및 절차 수립 방법들에 대하여 기술하고 있으며, 실제 적용 가능한 사이버보안 기술을 개발하기 위한 지침으로는 사용하기에 적합하지 않다. 이러한 이유로 원전 디지털 계측제어시스템의 보안을 강화 할 수 있는 원전에 특화된 사이버보안 기술 개발이 필요하다. 이에 본 논문은 원전에 특화된 사이버보안 기술 개발을 위한 기술 개발 체계를 제안하고, 이를 KINCS 사업에서 개발된 공학적안전설비-기기계통에 적용하였다.

ABSTRACT

Nuclear Power Plant Instrumentation and Control System(NPP I&C) which is used to operate safely is changing from analog technology to digital technology. Ever since NPP Centrifuge of Iran Bushehr was shut down by Stuxnet attack in 2010, the possibility of cyber attacks against the NPP has been increasing. However, the domestic and international regulatory guidelines that was published to strengthen the cyber security of the NPP I&C describes security requirements and method s to establish policies and procedures. These guidelines are not appropriate for the development of real applicable cyber security technology. Therefore, specialized cyber security technologies for the NPP I&C need to be developed to enhance the security of nuclear power plants. This paper proposes a cyber security technology development system which is exclusively for the development of nuclear technology. Furthermore, this method has been applied to the ESF-CCS developed by The KINCS R&D project.

Keywords: CyberSecurity, Digital Instrumentation & Control System, Logical, Logical Architecture, Threat

I. 서 론

원전의 계측제어시스템은 원전을 안전하게 운전하기 위해 계측, 제어 및 보호, 감시 기능을 수행하는 설

접수일(2013년 11월 19일), 수정일(2014년 4월 3일), 게재확정일(2014년 4월 16일)
* 본 연구는 2013년도 산업통상자원부의 재원으로 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 연구과제입니다. (No. 20121510100030)

† 주저자, manhyun@ensec.re.kr
‡ 교신저자, seojt@ensec.re.kr(Corresponding author)

비로서, 아날로그 기술에서 컴퓨터와 데이터통신망을 기반으로 하는 디지털 기술로 변하고 있다. 그리고 원전 디지털 계측제어시스템에서 기존에 사용하던 산업용 제어기기 대신 IT자원을 사용하는 비율이 증가하고 있다. 하지만 원전 디지털 계측제어시스템의 경우 아직은 많은 부분 산업용 시스템인 PLC, DCS 시스템들이 사용되고 있으며, 일반적인 IT 시스템처럼 범용적으로 사용되지 않고 계측제어시스템의 정보 또한 쉽게 접근할 수 없다는 이유로 계측제어시스템은 사이버공격에 안전하다는 생각이 지배적이었다[1,2]. 하지만 2010년에 이란의 부셰르 원자력 발전소의 원심분리기의 가동을 중단시킨 스턱스넷의 출현[3]으로 인해 원전도 사이버공격의 안전지대가 아니라는 것이 증명되면서, 원전 관계자들 역시 사이버공격을 간과할 수 없는 문제라고 인식하게 되었다. 원전 디지털 계측제어시스템이 사이버공격을 통해 시스템의 오작동이나 데이터의 변조가 이루어지거나 통제가 불가능해질 경우 원자로 노심용융 및 방사선 노출 등의 피해를 유발할 수 있으며, 발전소 가동 중단을 통해 국가 전력수급에 문제를 발생시킬 수 있다. 이처럼 국가와 국민에게 피해가 야기되는 일이 없도록 원전 디지털 계측제어시스템의 사이버보안은 강화되어야 한다.

원전 디지털 계측제어시스템은 기능 및 시스템 구성, 규제 등급에 따라 안전계통과 비안전계통으로 구분된다. 안전계통은 원전의 사고를 방지하거나 완화시키는 기능을 수행하는 계통으로서, 원전 특성으로 인한 고유한 기능을 갖추고 있고, 비안전계통은 일반 산업분야와 마찬가지로 플랜트 운전에 요구되는 계측, 제어, 감시 및 정보처리 기능을 수행한다[4]. 리고 안전과 비안전계통은 내부에 여러 시스템으로 구성되어 운영되고 있다. 이러한 원전 디지털 계측제어시스템의 구성은 기존 IT 시스템 구성과의 차이점이 존재한다. 이러한 차이점을 보완하여 원전 디지털계측제어시스템 사이버보안 기술 개발을 위해서는 원자력 분야와 사이버보안 분야의 전문가들이 서로 협력하여 기술개발을 추진하여야 한다. 하지만 사이버보안 전문가와 원자력 분야의 전문가들은 서로의 분야에 대한 이해도가 낮은 편이다.

원전 디지털 계측제어시스템의 특성을 고려한 사이버보안 강화를 위해서는 원전 분야의 전문가와 IT 보안 전문가들의 협력과 사이버보안 기술개발을 위한 체계 수립이 시급한 요건이다.

본 논문에서는 원전 디지털 계측제어시스템 사이버보안 기술 개발 체계를 수립하기 위한 방법을 제안하고자 한다. 2장에서는 원자력 분야에서 사이버보안 강화를 위한 국내외 규제지침 동향에 대하여 설명하고, 3장에서는 본 논문에서 제안하는 체계 수립 방법을 기술한다. 4장은 제안 방법을 적용한 결과를 제시하고 5장에서 결론을 기술한다.

II. 규제지침 동향

미국의 원자력규제위원회(NRC)는 원자력 시설의 디지털 컴퓨터와 통신 시스템, 네트워크를 사이버공격으로 부터 보호하기 위한 규제지침으로 Regulatory Guide(RG) 5.71 발간하였다. RG 5.71[6]은 미연방법 10 CFR 73.54에서 명시한 사이버보안에 대한 법령을 보다 구체화한 규제지침으로 사이버 공격으로부터 보호해야 하는 디지털 자산을 식별하여 “주요 디지털 자산”(Critical Digital Asset)이라 명명하고 있다.

규제 지침은 식별된 방어 아키텍처와 포괄적 보안 통제수단을 적용하여 CDA의 사이버보안 위험 가능성을 처리하도록 하고 있으며, 사이버보안 적용범위를 SSEP (Safety, Security, & Emergency Preparedness) 기능을 수행하는 하는 CDA로 규정하고 있다. 그리고 RG 5.71은 1) 디지털 컴퓨터와 통신 시스템, 네트워크를 분석, 2) CDA 식별, 3)방어 아키텍처를 적용, 4) CDA의 잠재적 사이버 위험을 처리의 일련의 과정을 수행하는 사이버보안 프로그램을 재정하고 Fig. 1과 같이 사이버보안 수명주기 활동을 이행하여 사이버보안 프로그램을 유지하도록 명시하고 있다.

RG 5.71은 부록 A에 사이버보안 계획 템플릿을 제공하고 부록 B, C에는 NIST SP 800-53[17] 및 800-82[18]의 권고에 따라 CDA에 대한 잠재적 사이버보안 위험을 처리하기 위한 보안 통제수단의 목록을 제공한다. 특히 NIST 표준은 18개 유형으로 분류되는 100개 이상의 보안 통제수단을 권장하고 있다. 이러한 보안 통제수단의 유형은 기술, 운영, 관리 등 3개 등급으로 세분된다.

IAEA는 원자력시설에 대한 사이버요건을 기술한 Nuclear Security Series No.17 Computer Security at Nuclear Facilities[9]는 원자력 시설 파괴 및 다른 악의적 행위로부터 계측제어시스템, 네트워크, 정보시스템 등 원자력 시설에 대한 보안 및 안전을 보장하기 위해 권고사항 및 이행에 관한 기술지침 제공하고 있으며, ISO27000[19]시리즈 및 다

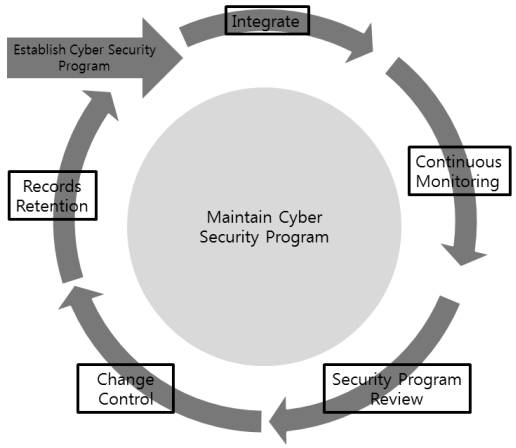

Fig. 1. RG 5.71 CyberSecurity Lifecycle

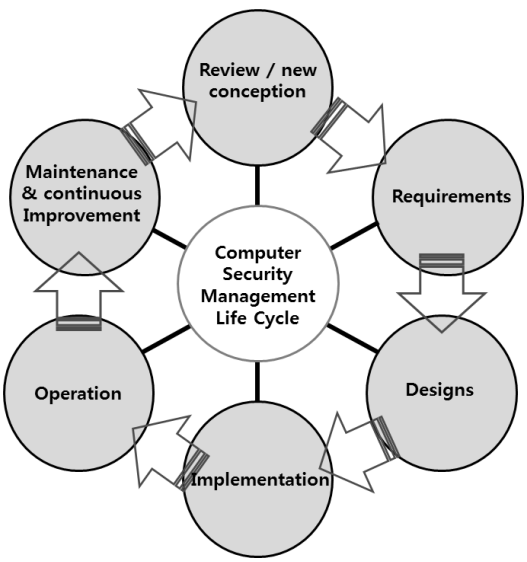

Fig. 2. IAEA security management life cycle

른 표준 문서들의 내용들과 원자력시설에 특화된 사이버보안 요건을 고려하였다.

NSS No.17의 Part Ⅰ는 정책, 설계 및 사이버보안 관리 관련한 정책을 결정하는데 도움을 주며, 사이버보안에 대한 규제적 관리적 가이드를 제공하고 Part Ⅱ는 종합적인 사이버보안계획을 이행을 하는데 기술적이고 행정적인 가이드를 제공한다. NSS No.17은 보안 정책이 해당 시설과 환경의 조건 변화에 적응해야하며 일회성 측정을 통해 지속적으로 실행할 수 있는 것이 아니라 지속적인 평가와 개선을 요구되기 때문에 Fig. 2의 관리 프로세스의 수명주기를 예시를 통해 보안관리를 유지 하도록 명시하고 있다.

국내에서는 원전 인허가 기관인 한국원자력안전기술원(KINS)에서 사이버보안 요건을 명시한 규제지침을 발행했다. KINS 규제지침 8.22[5]의 적용범위는 안전기능을 수행하는 계측제어계통과 이를 시험 및 평가하는 디지털 보조기기로 하고 있으며, 그 외 계측제어계통은 이행을 요구하지는 않으나 안전기능에 영향이 없음을 보장하는 사이버 위협에 대한 분석을 수행하도록 명시하고 있다. 사이버보안 활동을 수행하기 위하여 먼저 사이버보안 정책을 개발하고 사이버보안 계획을 수립한 다음 이에 따라 철저하게 이행하라고 명시하고 있다. 사이버 위협의 유형과 가능성은 지속적으로 변화하는 특성을 보이기 때문에 적용 대상에 영향을 미칠 수 있는 사이버 위협의 분석 및 적용 대상의 취약성 분석을 포함한 사이버보안성 평가는 모든 생명주기 동안 주기적으로 수행되어야 함을 명시하고 있다.

위의 국내외 규제지침들은 원전에 영향을 미치는 사이버공격을 탐지, 완화, 예방에 필요한 요구사항들과 정책 및 절차 수립 방법들에 대하여 기술하고 있다. 하지만 규제지침의 특성상 원전에 범용적으로 적용할 수 있는 큰 틀을 제공하고 있을 뿐 실제 적용 가능한 사이버보안 기술을 개발하기 위한 지침으로 사용하기에 적합하지 않다.

III. 원전 사이버보안 기술 개발 체계

본장에서는 논리적 아키텍처 개발, 사이버보안 위협 식별, 사이버보안 요구사항 식별로 이어지는 Fig. 3와 같이 3단계 절차를 이용하여 원전 디지털 계측제어시스템의 구조와 시스템을 이해하고 특화된 원전 사이버보안 위협과 사이버보안 요구사항을 식별한 후 이들 결과를 이용하여 사이버보안 기술을 도출하는 방법을 설명한다.

3.1 논리적 아키텍처 개발

원전 디지털 계측제어시스템을 구성하는 안전·비안전계통은 각 계통별로 다양한 세부 시스템들로 구성된다. 계통의 논리적 아키텍처 개발을 위해 먼저 각 계통의 세부 시스템과 시스템 간에 구성되어 있는 인터페이스를 식별하고 계통, 노드, 인터페이스 간 정보흐름 및 연계를 분석하여 사용사례를 분석하고 이를 통해 논리적 아키텍처를 구성한다.

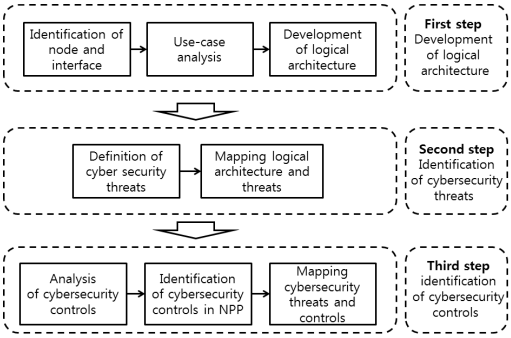

Fig. 3. procedures of NPP Cybersecurity technology development Architecture

Table 1. Node information form

Node name	Explanation
Node Definition	Definition of the node functions and characteristics

Table 2. form of nodes and Interfaces

Related nodes		type of communication media	Exchanged Data
GC	LC	SDL	actuation signal

Table 1.과 같이 원전 계측제어시스에서 사용되는 PLC, DCS, 산업용 PC 및 일반 PC를 구성노드로 식별하고 구성노드를 설명한다. 그리고 Table 2.의 형식으로 구성노드 간 연결을 인터페이스로 정의하고 인터페이스를 구성하는 통신매체, 구성노드 간 정보 흐름 및 연계 정보를 시스템 단위별로 기술한다. 단 전기적 신호를 전달하는 하드와이어는 인터페이스에서 제외한다.

이렇게 수집된 시스템 별 정보를 이용하여 사용사례를 다음 Table 3.의 형식으로 구성한다. 그리고 각 시스템의 구성노드와 인터페이스 사용사례를 이용하여 각 시스템의 논리적 아키텍처를 작성한다.

Table 3. use-cases form

○ Use case Identifier and Name
- The identifier is a unique number which we can classify from the whole use case list and it is composed by domain-indentifier-classification-sequence number(specific sequence alphabet)

○ Use case Objective
- The results of a successful performance of the Use case procedure.

○ Use case Explanation
- An Explanation of the Use case Objective

○ Use case Starting Trigger
- This explains what conditions are needed to start the use case

○ The Security Characteristics of the Use case
- Elaborate the Security Characteristics of the Use case
- The security characteristics should show the cyber threats which can occur when the use case is conducted in the point of view of confidentiality, integrity and availability.

○ use case scenario
- This explains the specific sequential protocol for the use case to achieve its goal

3.2 사이버보안 위협 식별

원전 디지털 계측제어시스템의 경우 IT에 사용되는 일반 PC, 서버를 일부 운영하지만 PLC, DCS, 산업용 PC와 산업용 네트워크 등의 산업용 장비들이 대부분 이용된다. 이러한 이유로 기존의 사이버보안 위협을 바로 적용하기에는 적합하지 않다. 원전 디지털 계측제어시스템에 적용 가능한 사이버보안 위협을 식별하기 위해서 IT, ICS 등에서 식별된 사이버보안 위협 연구 결과 및 보안 지침, 가이드에 설명된 사이버보안 위협을 비교 분석하고, 대상시스템의 기능 및 특징들을 분석한 후 원전에 적용 가능한 사이버보안 위협을 도출해야한다. 원전의 경우 가용성과 안전성이 우선시되며, 안전계통의 경우 결정론적인 통신구조로 구성하여 통신상의 어떠한 불확실성도 갖지 않도록 하고 있다.

원전 디지털 계측제어시스템에 발생 가능한 사이버보안 위협 검증을 위해 기존의 사이버보안 위협을 분석하고 이를 3.1에서 분석한 시스템 논리적 아키텍처와 비교하여 가능한 위협을 식별한다. 그리고 사이버보안 위협이 계측제어시스템의 각 시스템에 미치는 영향을 산정하기 위하여 위협이 각 시스템의 구성노드 및 인터페이스에 발생할 수 있는 가능성과 보안위협 영향도를 평가할 수 있는 위험도 산정식을 선별하여 도출된 사이버보안 위협이 3.1에서 작성된 각 시스템의 논리적 아키텍처에 미치는 위험도를 산정한다.

3.3 사이버보안 요구사항 분석

사이버보안 요구사항은 시스템에 발생 가능한 사이버보안 위협을 차단하고 그에 따른 영향을 최소화할 수 있는 방법을 제공하는 것으로 사이버보안 기술 개발 체계 구성에 필수요소이다. 원전 디지털 계측제어시스템에 적합한 사이버보안 요구사항의 항목을 식별하기 위해서 먼저 IT 시스템에서 사용하고 있는 NIST SP 800-53[17], ISO 27001[19]와 ICS에 적용하기 위한 NIST SP 800-82[18] 등의 사이버보안 요구사항을 제공하는 지침서와 원자력 분야에 사용되는 RG 5.71[6], NEI 08-09[8]를 분석하고 사이버보안 요구사항의 항목을 상세히 하기 위해서 국내외에 사용되는 관리지침의 내용을 추가하여 원전 디지털 계측제어시스템에 특화된 사이버보안 요구사항을 식별하고 식별된 원전 사이버보안 요구사항을 3.1, 3.2의 논리적 아키텍처와 사이버보안 위협의 매핑결과와 매핑하여 사이버보안 요구사항을 만족 시킬 수 있는 사이버보안 기술을 식별한다.

IV. 사이버보안 기술 개발 체계 적용사례

본장에서는 3장에서 설명한 원전 디지털 계측제어시스템 사이버보안 기술 개발 체계를 KNICS 사업에서 개발한 안전계통의 공학적 안전설비 기기제어 계통(ESF-CCS)에 적용 하였다[10,11,12,13].

공학적 안전설비 기기제어 계통은 발전소 보호 계통(PPS)과 방사선 감시 계통(RMS)으로부터 구동신호를 받아 공학적 안전설비 계통 기기를 작동시키고 공학적 안전설비 관련 기기를 포함한 모든 안전 관련 기기의 제어기능을 수행하는 계통이다. Fig. 4.는 공학적 안전설비 기기제어 계통의 세부 구성도 이다.

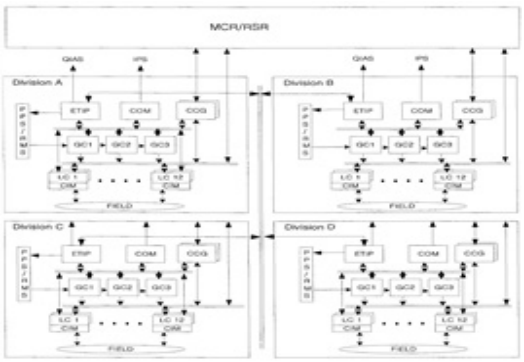

Fig. 4. Configuration of ESF-CCS

4.1 ESF-CCS의 논리적 아키텍처

다음은 공학적 안전설비 기기제어계통의 논리적 아키텍처 결과이다. 구성노드는 6개로 구성되어 있으며, 노드 간 또는 노드와 시스템 사이의 인터페이스는 7개로 Table 4,5와 같이 구성된다. 그리고 사용사례의 경우 총 7개가 작성되었으며 하나의 사례를 Table 6,7과 같이 작성하였다.

Table 4. Configuration Nodes of ESF-CCS

Node	Explanation
GC	After receiving the ESF-CCS start signal, The PLC which transmits engineered safety-facilities start signal to LC
LC	after receiving the operation signal, The plc depends on the result by applying the voting logic of the 2/3 and controls the devices in the field
ETIP	The PLC which collects status information of modules and test if they are operating properly.
COM	The system which collects information from the ETIP and delivers it to the operator
CCG	After confirming the input signal, The PLC which process the transmission and reception
PPS	Plant Protection System

Table 5. Interfaces of ESF-CCS

Related nodes		type of communication media	Exchanged Data
GC	LC	SDL	actuation signal
GC	ETIP	SDN	GC status information and test results
LC	ETIP	SDN	LC status information and test results
ETIP	COM	SDN	ETIP information
ETIP	GC, LC	SDN	test signal to GC, LC
CCG	GC	SDL	actuation signal
PPS	GC	SDL	trip signal

Table 6. use-case of ESF-CCS

No	Use-case name	Explanation	Related nodes and interface
ESF-CCS-01	ESF-CCS start signal transmission	the PPS transmits start signal to GC	PPS GC

Table 7. Sample use-case of ESF-CCS

ESF-CCS start signal transmission
○ Use case Objective
- Receive the ESF-CCS start signal

○ Use case Explanation
- Receive the ESF-CCS start signal in GC

○ Use case Starting Trigger
- Start signal transmission from the PPS

○ The Security Characteristics of the Use case
- Integrity: integrity service is needed to prevent the start signal from being tampered with.
- The GC receiving module must always be running and the communication equipement and network infrastructure must operate normally.
○ use case scenario
- 1. the PPS transmits start signal to GC
- 2. Receive the ESF-CCS start signal in GC

4.2 원전 디지털 계측제어시스템 사이버보안 위협

원전 디지털 계측제어시스템에 발생 가능한 사이버보안 위협을 도출하기 위해 본 논문에서는 ENISA에서 발행한 Threat Landscape[14]에 제시된 위협과 ICS-Cert[15]에서 발행한 ICS 취약점 정보를 분석하고, 3.1에서 작성된 논리적 아키텍처와 비교 분석하여 Table 8.와 같이 원전 디지털 계측제어시스템의 사이버보안 위협과 해당 위협이 노드 및 인터페이스에 발생 가능한 22개의 보안위협 시나리오를 식별했다. 단 본 논문에서는 보안상 보안위협 시나리오는 기술하지 않는다.

Table 8. List of Security Threat in NPP

Classification	Security Threat	Security Threat Scenario
T_1	DoS	…
T_2	Malicious code propagation	…
T_3	data forgery attacks in network	…
T_4	data forgery attacks in system	…
T_5	Unauthorized use of remote service access	…
T_6	Attacks on network components	…
T_7	Introduction of malicious code on removable media and external hardware	…

Table 9. Likelihood of Security Threat in ESF-CCS

Systems \ Threats	T1	T2	T3	T4	T5	T6	T7
ESF-CCS	O			O	O		O

식별된 사이버보안 위협을 사용하여 Table 9.와 같이 공학적 안전설비 기기제어계통의 구성노드 및 인터페이스에 해당 위협이 발생 할 때 발생가능성과 위협이 원전 디지털 계측제어시스템에 미치는 영향을 평가하기 위해서 사이버보안 전문가와 원자력 전문가의 의견을 설문과 인터뷰를 수행하였다. 그리고 의견을 바탕으로 사이버보안 위협 발생 가능성과 영향을 평가하여 발생 가능성(L)과 영향도(I)를 0~9점의 점수를 부여하고 이를 수식(1)을 통해 평가 평균값을 계산하여 상, 중, 하 평가를 수행하였다. 높은 점수일수록 중요도가 높다. Table 10.은 공학적 안전 설비 기기제어계통 노드에 대한 위험도 산출결과이다.

$$N=\left(\sum_{i=1}^{E}\frac{L_i}{E}\right)\times\left(\sum_{i=1}^{E}\frac{I_i}{E}\right) \quad (1)$$

E: 설문응답자수(사이버보안 전문가, 원자력 전문가)
L: 발생가능성
I: 영향도

Table 10. The result table of risk calculation of nodes of ESF-CCS

ESF-CCS	T1	T2	T3	T4	T5	T6	T7
GC	M			L	M		M
LC	M			M	H		M
ETIP	L			L	M		M
CCG				L			
COM	L				M		M

4.3 원전 디지털 계측제어시스템 사이버보안 요구사항 식별

원전 디지털 계측제어시스템에 발생 가능한 사이버보안 위협에 대응할 수 있는 사이버보안 요구사항을 식별하기 위해서 IT·ICS·원자력 분야의 사이버보안 요구사항이 제시된 표준 및 지침[16,17,18,19,20,21,22,23,24]을 분석하고 원전 디지털 계측제어시스템에 적합한 사이버보안 요구사항을 도출하였다. 그리고 각 사이버보안 요구사항들의 기능 및 특성을 고려하여 보안영역으로 그룹화 하였다. 끝으로 식별된 사이버보안 요구사항과 사이버보안 위협의 매핑 테이블을 구성하고, 이를 이용하여 보안요구사항의 세부 항목을 작성하였다.

식별된 사이버보안 요구사항은 총 139개로, 기능 및 특성을 고려하여 NIST 800-53에서 제안하는 18개의 보안영역으로 구분하였다. 그리고 다음 Table 11. 는 식별된 사이버보안 요구사항 샘플로 식별된 영역 중 접근제어영역의 접근관리항목이다. Table 11. 의 구성은 사이버보안 요구사항 항목명과 세부 요구사항내용과 참고문서를 기술하였다.

Table 11. Cyber security control Sample of NPP

AC-2	
Name	Access Enforcement
Control	• enforcing assigned authorizations for controlling access to system in accordance with established policies and procedures, • defining and documenting privileged functions and security-relevant information for the system, • restricting access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to authorized personnel (e.g., security administrators), • defining and documenting privileged functions for system, • requiring dual authorization for critical privileged functions and the creation of any privileged access for users • Ensures and documents that access enforcement mechanisms do not adversely impact the operational performance of system • employs alternate compensating security controls when access enforcement cannot be used.
Ref,	NPP security control	reference documentation for detailed security control
	• RG 5.71 B.1.3 • NEI 08-09 D.1.3	• ISMS 10.4.1

식별된 18개 보안 영역의 사이버보안 요구사항을 4.2에서 식별된 보안 위협과 매핑 하여 Table 12.과 같이 사이버보안 위협을 보완, 방어, 탐지 할 수 있는 항목을 식별하였다. Table 12. 은 18개 사이버보안 영역 중 하나의 샘플(Access Control: AC)을 제시하였다.

Table 12. Sample table of identified security controls for each security threat in NPP

Cyber Security Requirements			Cyber security Threat						
Classification	No.	Controls	T_1	T_2	T_3	T_4	T_5	T_6	T_7
AC	AC-1	Account Managements			O	O	O		
	AC-2	Access Enforcement	O		O	O	O		O
	AC-3	Information Flow Enforcement	O	O	O			O	O
	AC-4	Separations of Duties	O		O	O	O		O
	AC-5	Least Privilege	O	O	O	O	O	O	O
	...	...	...	...	...	...	...	...	...

식별된 Table 12.과 같은 형식으로 식별된 18개 영역의 사이버보안 요구사항 정보를 Table 13.와 같이 공학적 안전설비 기기제어계통의 논리적 아키텍처와 비교 분석을 통해 필요한 사이버보안 요구사항을 식별하고 이를 구현하는 사이버보안 기술을 도출한다.

Table 13. table of suitable security controls in GC of ESF-CCS

	Cyber Security Requirements			Cyber security Threat			
Node	Classification	No.	Controls	T_1	T_4	T_5	T_7
GC	AC	AC-1	Account Managements		O	O	
		AC-2	Access Enforcement	O	O	O	O
		AC-3	Information Flow Enforcement	O			O
		AC-4	Separations of Duties	O	O	O	O
		AC-5	Least Privilege	O	O	O	O
		...	...	...	...	...	...

4.4 적용 결과 분석

본 논문에서 제안한 방법을 적용한 결과 논리적 아키텍처 개발단계에서는 적용 대상의 구성 노드, 인터페이스 및 사용사례 분석을 통해 대상시스템을 정확히 파악 할 수 있었다. 그리고 사이버보안 위협 식별 단계에서는 ICS의 사이버보안 위협을 분석하여 원전 디지털 계측제어시스템에 발생 가능한 사이버보안 위협을 정의하기에는 정보가 부족하였다. 마지막으로 원자력 분야의 사이버보안 요구사항의 경우 다양한 환경으로 구성된 원전 디지털 계측제어시스템에 적용을 위해서 요구사항의 기술적 측면에서 상세화가 필요하다. 그리고 기존 IT 및 ICS 분야의 사이버보안 요구사항은 원전 디지털 계측제어시스템에서 사용하지 않는 인터넷, 웹, 무선통신 등에 관련된 항목들이 다수 존재한다. 본 논문에서 제안하는 방법과 같이 원전 디지털 계측제어시스템에 적합한 사이버보안 요구사항 식별을 위해 다양한 요구사항 항목에서 적합한 요구사항 항목을 선별하여 요구사항 항목을 작성하는 제안방법이 적합한 것으로 확인되었다. 하지만 사이버보안 위협과 위험도 평가 시 원전 디지털 계측제어시스템의 중요한 특성인 안전성 측면이 고려되지 않았다. 안전성 측면을 고려하기 위해 논리적 아키텍처 개발단계에서 노드와 인터페이스 식별 시 해당 노드나 인터페이스가 안전 기능이나, 안전에 관련된 노드 및 계통과의 관계성을 가지는지 여부를 파악하여 안전성을 평가한다. 그리고 원전 디지털 계측제어시스템에 발생 가능한 사이버보안 위협을 식별하기 위해서 침투테스트가 필요하다고 판단된다. 하지만 계측제어시스템의 경우 IT환경과 차이점이 많기 때문에 직접적인 침투테스트보다는 대상 시스템과 유사한 테스트베드를 구성하여 침투테스트를 수행하여야 할 것이다.

V. 결 론

원전 디지털 계측제어시스템의 경우 점차 아날로그에서 디지털화가 되어 가고 있고 그 범위 또한 점차 넓어 질 것이다. 이에 따라 원전 디지털 계측제어시스템의 사이버보안 강화를 위한 다양한 기술개발이 필요하며, 점차 원자력 발전소 전체를 강화 할 수 있는 사이버보안 기술의 개발도 필요할 것이다.

본 논문에서는 원전 디지털 계측제어시스템의 사이버보안 강화를 위한 사이버보안 기술 개발 체계를 제안하고 제안방법을 공학적 안전설비 기기제어계통에 적용 하여 제안 방법의 적합성과 문제점을 파악하고 보완방법을 제시하였다. 그리고 이를 통해 운영 원전 또는 개발 원전에 현재 필요한 사이버보안 기술을 식별하고 개발 할 수 있는 기반을 마련하였다. 향후 연구로 위협의 정량적 산정방법과 사이버보안 기술 식별 시 적용성 평가방법에 대한 연구가 진행되어야 할 것이다.

References

[1] Cheol-kwon Lee, "Trend of technology of instrumentation and control system in nuclear power plants," Review of KIISC, 22(5), pp 28-34, Aug. 2012.

[2] In-Soo Koo, Kwan-Woong Kim, Seok-Boong Hong, Geun-Ok Park, and Jae-Yoon Park, "Digital asset analysis methodology against cyber threat to instrumentation and control system in nuclear power plants," The Journal of Korea Information and Communications soci-

ety, 6(6), pp.839-847, Dec. 2011.
〔3〕 Nicolas Falliere, Liam O Murchu a, and Eric Chien, "W32.Stuxnet Dossier," Version 1.4, Symantec Security Response, February 2011.
〔4〕 Dong-Hoon Kim, "Concept of KNICS Development," The proceedings of KIEE, 52(9), pp.24-32, Sep. 2003.
〔5〕 KINS, "instrumentation and control system," RG chapter 8, KINS, 2011.
〔6〕 US NRC, "Cyber Security Programs for Nuclear Power Facilities," NRC Regulatory Guide 5.71, January. 2010.
〔7〕 US NRC, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," Regulatory Guide 1.152, Rev. 03, June. 2010.
〔8〕 Nuclear Energy Institute, "Cyber Security Plan for Nuclear Power Reactors," NEI 08-09 ,January. 2010.
〔9〕 IAEA, "Computer Security at Nuclear Facilities," IAEA Nuclear Security Series N0.17, 2010.
〔10〕 KAERI, "Development of digital reactor safety systems: Development of network protocol for the integrated safety system," KAERI, 2007.
〔11〕 KAERI, "Development of digital reactor safety system - Production of the digital reactor safety systems," KAERI, 2004
〔12〕 Ministry of Trade, Industry and Energy, "Development of digital reactor safety system," Ministry of Trade, Industry and Energy, 2008
〔13〕 KAERI, "Development of digital reactor safety system - Design support for ESF-CCS," KAERI, 2008.
〔14〕 Louis Marinos, ENISA, "ENISA Threat Landscape 2013," European Network and Information Security Agency, 2013.
〔15〕 US.ICS-CERT, http://ics-cert.us-cert.gov/ics-archive
〔16〕 Gunhee Lee, Jungtaek Seo, and Eung-ki Park, "Smart Grid Security Threats and Security Requirements Analysis," Review of KIISC, 21(7), pp 7-17, Nov. 2011.
〔17〕 National Institute of Standards and Technology, "Special Publication 800-53," National Institute of Standards and Technology, August. 2009
〔18〕 National Institute of Standards and Technology, "Special Publication 800-82," National Institute of Standards and Technology, June. 2011
〔19〕 International Organization for Standardization, "Information technology - Security techniques - Information security management systems - Requirements," ISO/IEC 27001:2005, International Organization for Standardization, 2013.
〔20〕 KISA, "G-ISMS specification of information protection measures," KISA, 2013
〔21〕 KISA, "ISMS certification criteria of detailed inspection items," KISA, 2013.
〔22〕 Ministry of Security and public Administration, "Information and Communication Security business rules," Ministry of Security and public Administration, 2009.
〔23〕 Ministry of Security and public Administration, "Critical information and communication infrastructure vulnerability assessment, evaluation criteria," Notice No. 2012-54, Ministry of Security and public Administration, 2012.
〔24〕 Korea Communications Commission, "Information Security Management Guidelines," Directive No.109, Korea Communications Commission, 2012.

〈저자소개〉

사 진

정 만 현 (Manhyun Chung) 정회원
2006년 2월 동국대학교 컴퓨터공학부 졸업
2009년 2월 고려대학교 정보경영공학대학원 석사
2012년 8월 고려대학교 정보보호대학원 박사수료
2012년 9월 ~ 현재 : 한국전자통신연구원 부설연구소 연구원
〈관심분야〉 정보보호, 원자력보안, 제어시스템보안, 침입탐지시스템

사 진

안 우 근 (AHN WOO GEUN) 정회원
2011년 2월 : 고려대학교 컴퓨터·통신공학부 졸업
2013년 2월 : 고려대학교 컴퓨터·전파통신공학과 석사
2013년 1월~현재 : 한국전자통신연구원 부설연구소 연구원
〈관심분야〉 정보보안, 제어시스템, 취약점 분석

사 진

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

사 진

서 정 택 (Jungtaek Seo) 종신회원
1999년 2월 : 충주대학교 컴퓨터공학과 졸업
2001년 2월 : 아주대학교 컴퓨터공학과 석사
2006년 2월 : 고려대학교 정보보호대학원 정보보호공학 공학박사
2000년 11월 ~ 현재 : 한국전자통신연구원 부설연구소 책임연구원/부장
2011년 11월 ~ 현재 : 고려대학교 정보보호대학원 겸임교수
〈관심분야〉 스마트그리드 보안, 제어시스템 보안, 원자력 사이버보안, 취약성 분석평가, DDoS 공격 탐지 및 대응