Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.6, Dec. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.6.1539

분석적 방법을 적용한 원전디지털자산 취약점 평가 연구*

김 인 경,† 권 국 희‡
한국원자력통제기술원

A Study on Vulnerability Assessment for the Digital Assets in NPP Based on Analytical Methods*

In-kyung Kim,† Kook-heui Kwon‡
Korea Institute of Nuclear nonproliferation And Control

요 약

원자력 발전소의 디지털화로 인한 사이버위협 노출로 보다 확고한 사이버보안 체계 구축 필요성이 대두되고 있으며 주기적인 취약점 분석 및 평가를 통한 적합한 보안대책 정립이 필요하다. 그러나 원전시스템은 안전성을 최우선으로 둔 특성 및 취약점 분석을 위한 제반사항 구축에 많은 비용 및 시간 등이 필요하여 기존의 취약점 분석 환경 및 분석 도구를 적용하는데 어려움이 있다. 이에 본 연구에서는 원전디지털자산 취약점 분석 시 고려해야 할 사항 및 일반적인 취약점 분석 방법들을 비교하여 기존의 취약점 분석 방법의 한계점을 보완하는 원전디지털자산에 적합한 취약점 평가 방법에 대해 제시하고 시범 적용한 결과를 기술하고자 한다.

ABSTRACT

The necessity of establishing a more secure cyber security system is emerging to protect NPP against cyber attacks as nuclear facilities become increasingly reliant on digital system. Proper security measures should be established through periodic analysis and evaluation of vulnerabilities. However, as Nuclear facilities has safety characteristics as their top priority and it requires a lot of time and cost to construct regarding the activities for vulnerability analysis, it is difficult to apply the existing vulnerability analysis environment and analysis tools. In this study, We propose a analytical vulnerability assessment method to overcome the limitations of existing vulnerability analysis methods through analysis the existing vulnerability analysis methods and the issues to be considered when applying the vulnerability analysis method.

Keywords: Nuclear digital assets, Control system cyber security, Vulnerability assessment

I. 서 론

원자력 발전소의 디지털화로 인해 정밀한 운영과 편의성 및 효율성은 증가하였으나 사이버위협에 노출되면서 사이버보안에 대한 필요성이 대두되고 있다. 특히, 기존 원자력 발전소는 설계 당시에 기본적인 보안조치에 대한 요건을 고려하지 않았고, 2010년 이란의 나탄즈 원전의 스턱스넷 공격으로 에어갭(air-gap)상태에서도 바이러스에 감염되는 사례를 통해 사이버공격에 안전하지 않음이 드러났으며[4] 사이버공격이 방어체계를 회피하는 방법으로 진화하고 있기에 보다 확고한 사이버보안 체계 구축이 필요하다. 이에 사이버보안 위협에 신속하게 대응하고 사이버보안 강화를 위해 시스템의 주기적인 취약점 분석 및 평가를 통하여 적합한 보안대책 정립에 대한 지속

Received(07. 24. 2018), Modified(1st: 10. 12. 2018 2nd: 10. 19. 2018)Accepted(10. 13. 2018)
* 본 연구는 원자력안전위원회의 재원으로 한국원자력안전재단의 지원을 받아 수행한 원자력안전연구사업의 연구결과입니다. (No. 1605007)
† 주저자, ikkim@kinac.re.kr
‡ 교신저자, vivacita@kinac.re.kr(Corresponding author)

적인 연구가 필요한 실정이나 현재 원자력 발전소의 사이버보안 적용은 도입단계이며 원전시스템은 IT 시스템과의 폐쇄성, 자원의 특수성 등의 차이로 기존의 취약점 분석 및 평가 방법의 적용에 어려움이 있다. 또한 취약점 분석을 위한 제반사항 구축에 많은 비용 및 시간이 필요하여 원전에 적합한 차별화된 취약점 분석 가이드 및 보안성 평가 프레임워크가 적용되어야 한다. 이에 본 연구에서는 원전디지털자산의 취약점 분석 시 고려해야 할 사항 및 일반적인 취약점 분석 방법에 대해 분석하여 기존의 취약점 분석 방법의 한계점을 보완하는 원전디지털자산에 적합한 취약점 분석 방법을 제시하고자 한다.

II. 취약점 분석 방법 개요

2.1 원전디지털자산 취약점 분석 시 고려사항

초기 원전디지털자산은 대부분 물리적으로 독립되어 있고, 기본적인 오류 검출 및 정정 기능을 이행하는 하드웨어와 소프트웨어 및 통신 프로토콜을 기반으로 했으나 점차 개방적이고 표준화된 시스템으로 전환하면서 IT 및 네트워크 관련 기술들을 반영하는 단계로 발전하고 있다. 이러한 변화는 운영자 및 관리자에게 IT 기술의 편의성을 제공하지만 성능, 신뢰성 및 안전성 요건에만 집중한 설계로 IT에서 가지는 사이버위협에 노출되었고 일반적인 IT자산의 보안문제를 해결하기 위한 대책이 적용되고 있다. 원전디지털자산은 IT자산 간에 동작 및 위험 측면, 성능 등의 차이로 IT와는 다른 보안 특성을 갖기 때문에 원전 환경에 맞는 사이버보안과 운영 전략을 신중하게 적용해야 한다. 원전시스템은 높은 처리 성능이 필수적이지는 않지만 응답시간이 중요하므로 기준 시간 내에 처리해야 하며 가동 중단을 허용하지 않고 높은 안전성이 요구되기에 가용성, 무결성, 기밀성의 우선순위의 보안목적을 갖는다. 원전디지털자산 취약점 분석 시 고려해야 할 원전디지털자산의 일반적인 특성은 다음과 같다.

- 실시간성 : 높은 처리 성능이 필수적이지 않지만 응답시간이 중요하므로 기준 시간 내에 처리해야 한다.
- 가용성 : 가동 중단을 허용하지 않고 높은 안전성을 위하여 다중화된 시스템이 필요하다.
- 위험관리 : 방사능으로부터의 인명 안전이 최우선으로 고장 허용(Fault Tolerance) 시스템이 필수적이며 위험발생 시 환경 파괴, 인명피해, 장비 및 생산 손실의 영향을 받는다.
- 보안설정 방향 : 중앙서버와 프로세서를 직접적으로 제어하는 컨트롤러의 보호가 중요하다.
- 물리적 상호작용 : 밸브, 펌프와 같은 장치에 연결되어 있어 상호작용 할 수 있으며 보안 기능이 물리적 처리를 방해하지 않도록 해야 한다.
- 시스템 운영 환경 : 대부분의 시스템에서 보안 기능이 구현되어 있지 않으며 운영 시스템은 보안 솔루션들과 별도로 설치되어 있다. 시스템 내 소프트웨어 및 어플리케이션의 업그레이드가 힘들고 공급 업체에서 지원하지 않는 버전의 소프트웨어 사용 시 패치가 없을 수 있다.
- 자원 한계 : 보안 기능 적용 시 필요한 자원이 제약되어 있거나 없을 수 있으며 공급 업체와의 계약으로도 호환되는 보안 기능을 설치할 수 없을 수 있다.
- 통신 : IT와는 다르거나 독점적인 프로토콜과 통신 매체 사용으로 새로운 보안 솔루션의 개발이 필요할 수 있다.
- 변경 및 관리 : 소프트웨어와 하드웨어 변경으로 인한 시스템 정지 시 미리 계획되어야 하며 철저한 사전 테스트가 이루어져야 한다. 관리 지원은 하나의 공급 업체에 의해 이루어지고 타 업체의 다양한 상호 운용 지원이 어렵다.
- 접근 통제: 주로 원격지에 격리되어 있으며 물리적 접근성에 대한 보안 수준이 높다.
- 시간 결정적 응답 시간 : 긴급상황 발생 시, 운영자와의 상호작용, 시스템에 대한 응답시간이 중요하므로 관리자의 인증과정과 같은 보안 기능으로 인하여 요구되는 처리시간을 초과하지 않아야 한다.

2.2 일반적인 취약점 분석 방법

원전디지털자산에 적용 가능한 일반적인 취약점 분석 방법은 분석 환경 및 분석 도구에 따라 다음과 같이 분류할 수 있다.

2.2.1 분석 환경

□ 현장 가동 시스템

실제 대상 시스템의 가동 중 또는 주기시험 기간

을 이용한 취약점 분석을 수행할 수 있는 환경으로 원자력발전소는 주기별 계획예방정비 기간을 통하여 가동 중단 후 안전점검 및 유지보수 등을 수행하고 있으며 주기시험 기간을 이용해 침투테스트 및 모의해킹, 취약점 분석 도구와 같은 기술적 방법을 적용하여 취약점 분석을 수행할 수 있다. 가동 또는 주기시험 중의 실제 시스템을 직접적으로 이용한 취약점 분석은 점검결과의 신뢰성은 높지만 발전소 및 시스템에 대한 영향성이 크기 때문에 발전소 및 시스템의 영향 분석, 시스템에 대한 데이터 백업과 복구 방안 등의 수행 계획 등이 요구되어 현장 가동 시스템에 직접 기술적 방법을 적용한 취약점 분석의 실행은 현실적으로 어려움이 많다.

□ 모사 시스템

대상 시스템에 대한 시뮬레이션이나 테스트베드를 구축한 취약점 분석을 수행할 수 있는 환경으로 테스트베드 등의 모사 시스템에 모의해킹 및 침투테스트, 취약점 분석 도구와 같은 기술적 방법을 적용한 취약점 분석은 발전소나 시스템에 영향을 주지 않고 시스템의 취약점을 파악할 수 있는 장점을 보유하나 테스트베드 구축을 위한 비용 및 시간과 유사성 검증에 어려움이 있으며 구축된 테스트베드에 제한된 범위만을 수행할 수 있는 단점이 존재한다.

Table 1. Comparison of environment for vulnerability analysis

	On-site operation system	Simulation system
Scope	- Technical - Operational - Management - Physical	Limited technical scope for the building system
Understand status	Difficult to grasp the status at all times (Identified only during periodic testing)	Limited technical scope for the building system
System influence	High	None
Reliability	High	Medium
Direction of security setting	Immediate and realistic security measures can be presented	Possible directions for additional security measures on technical requirements
Review of results	Re-perform Vulnerability Analysis	Comparative analysis and confirmation with on-site operation system
Other action	- Analysis impact of plants and systems - Data backup and recovery for system	- Cost and time required to build - Similarity verification with on-site operation system required

2.2.2 분석 도구

□ 침투테스트 및 모의해킹

침투테스트 및 모의해킹은 시스템에 침투하여 취약점을 찾아내서 공격을 시도하여 침투가능성을 검토하는 방법으로 신뢰성은 높지만 취약점 정보 수집보다는 취약점을 이용해 시스템에 악의적인 영향을 줄 수 있는 사이버 공격의 영향성 추정에 초점이 맞추어지기에 취약점 식별 방법으로는 어려움이 있다. 또한 원전디지털자산은 알려진 취약점 정보가 많지 않기에 침투테스트 방법의 일부로 쓰이는 공격트리 설정을 통한 시나리오 구성에 한계가 있다.

□ 취약점 분석 도구(취약점 스캐너)

시스템 스캐너, 네트워크 스캐너, DB 스캐너와 같은 취약점 분석 도구는 시스템의 중요도에 따라 다양한 도구를 적용할 수 있고 시스템 및 네트워크 자원에 대한 종합적인 점검기능을 제공하여 점검결과를 기초로 취약점에 대한 보안조치 적용이 용이하다. 취약점 분석 도구는 취약점 데이터베이스가 핵심으로 운영체제, 프로토콜 등과 같은 분류를 통한 취약점 정보가 필요하다. 현재 취약점 분석 도구는 공개 툴을 포함하여 최신 취약점 정보를 업데이트한 신뢰성 높은 다양한 툴이 많지만 상용화된 IT 제품의 취약점을 기반으로 하여 원전의 특성에 맞게 개발된 원전

디지털자산에 적용에 어려움이 있다. 또한 취약점 도구 자체가 해킹도구로 사용될 수 있고 취약점 도구 자체의 성능, 안전성에 따라 결과에 대한 신뢰성 판단에 한계가 있다.

□ 정적 분석 도구

정적 분석은 프로그램을 실행하기 위한 환경 구축 필요 없이 프로그램을 실행하지 않고 프로그램 텍스트를 정적으로 분석하여 취약 요소를 찾아낼 수 있으나 코드 진단 규칙 보유 수준이 점검 신뢰성에 영향을 미치며 소프트웨어의 소스코드 취약점 분석으로만 활용 가능하여 취약점 분석 범위에 한계가 있다. 원전시스템은 개발단계에서 보안수준이 높기에 소스 확보에 대한 현실적 어려움이 있으며 오탐율이 높은 편으로 광범위한 취약점 분석 방법으로는 부족하다.

□ 퍼징

퍼징 테스트는 침투테스트 전문가나 소스 확보 없이 이해하기 쉽고 단순하며 자동화하기 쉬운 장점이 있지만 장시간 소요되며 소프트웨어의 취약점 점검만 가능하여 운영환경 및 관리적 측면의 취약점 분석의 한계가 있다. 또한 원전시스템에서는 독점적인 프로토콜의 사용으로 프로토콜 특성을 반영한 별도의 퍼징 기술이 필요하다.

□ 점검 체크리스트

점검 체크리스트는 현장에서 하나씩 확인하고 O/X를 체크하거나 상/중/하 등급으로써 취약점을 진단하는 과정으로, 설문형식을 통한 기본적으로 확인할 수 있는 문항을 만들어 현재 보안 수준을 진단할 수 있다. Fig.1은 [5]에서 제공하는 취약점 분석·평가 기본항목 중 원전에 적용할 수 있는 제어시스템의 기술적 분야 점검 체크리스트이다. 원전시스템은 성능 및 기능의 요건으로 인한 기본적인 보안조치의 적용이 어려울 수 있고 해당 취약점에 대한 보안조치를 대체 할 수 있는 기능을 가질 수 있기에 취약점에 대한 보안조치의 확인보다는 원전시스템의 요건, 성능 및 기능 등의 분석을 통한 종합적인 취약점 평가가 필요하다. Fig.1과 같은 취약점 점검 체크리스트에서 제공하는 질문은 취약점에 대한 포괄적 범위의 현황분석, 보안관리 정책 및 절차, 보안조치의 유무 등만을 확인할 수 있으며 원전시스템의 특성을 고려한 취약점에 대한 보안조치 시 영향성 판단, 대체가능한 기능, 세부적인 보안현황 파악 등이 힘들

Table 2. Comparison of tools for vulnerability analysis

	Penetration Testing and Ethical Hacking	Analysis Tools (vulnerability scanner, static analysis tool, fuzzing)	Checklist
Scope	- Technical(S/W, Network) - Operational - Management - Physical - Structural	- Technical(S/W, Network)	- Operational - Management - Physical - Structural
Reliability	High	Medium	Low
Usability of Results	Identify vulnerabilities that could cause actual attacks	Identify potential vulnerabilities	- Understand basic security measures within a comprehensive scope - Binary directions such as only adding functions can be presented
Other Action	Configuring attack scenarios	- Cost and time required to develop technical tools - Performance and safety analysis of vulnerability tool itself	Compliance and effectiveness analysis for inspection items

* Since this figure is nationalized as a checklist provided by public notice in [5], the author has translated it in English in accordance with the paper format.

Scope	ID	Vulnerability Checklist	Level
Account Management	C-1	Account for control system operation and management is not shared with other users	H
	C-2	ID / PW, connection path, certificate, etc. are not hard-coded	H
	C-3	Operate control system, log in account for management, save log records	H
Patch Management	C-4	Establish procedures such as the latest updates to the control system and tests to safely apply security patches	H
Access Control	C-5	Operator rights of the control system operator are restricted to a limited range and command	H
	C-6	The control system is physically separated from the business network and the Internet network	H
	C-7	Establishment of physical unidirectional environment for data linking with the outside of the control network to fundamentally block intrusion into the control network	H
	C-8	Limit external network connections such as wireless Internet, tethering, and external wired network connections to the control network	H
	C-9	Disconnect and connect to unauthorized systems on the control network	H
Security Management	C-10	Create control system diagrams, operation manuals, emergency procedures, etc. and keep them up-to-date	H
	C-11	Prohibits the use of USB in the control system, and controls the use of removable storage media such as USB	H
	C-12	Apply countermeasures to prevent forgery and falsification of control commands	H
	C-13	Apply preventive measures against control command replay attack	H
	C-14	Separate access rights to control system developers, operators, and administrators	H
	C-15	Control system, vendor default and no vulnerable services	H
	C-16	When inputting an abnormal specific value into the input window of the control program, a predefined error message is output so that system important information is not exposed	H
Security Management (Selection)	CS-17	Are information security policies and guidelines established for control systems separate from those for information systems?	M
	CS-18	s it not possible to configure the control system and the control device without an unauthorized person or an authentication process?	M
	CS-19	Has the control system and operating system removed other functions and services for control purposes only?	M
	CS-20	Does it limit the range of parameters available for control commands and safe control in operation?	M
	CS-21	Have you built a test bed or test environment to test the safety of the control system, new system introduction, patches and modifications?	M
	CS-22	Is the control network subdivided into each sub-network, and the communication between the network and the system necessary for the control system operation is restricted?	M

Fig. 1. Vulnerability analysis and assessment criteria - control system checklist

고 특히 기술적인 범주는 취약점에 대한 정보만 제공하여 기술적 방법 적용 없이 근본적인 취약점 분석 및 평가 방법으로는 한계가 있다.

III. 원전디지털자산 분석적 취약점 평가 방법

3.1 분석적 취약점 평가 방법 개요

원전시스템은 안전성을 최우선순위로 둔 특성 및 취약점 분석을 위한 환경 구축에 많은 비용 및 시간이 필요하여 실제 가동 시스템이나 테스트베드 구축을 통해 기존 취약점 분석 도구를 적용하는데 어려움이 있으며 침투테스트 및 모의해킹, 기술적 분석 도구 활용 시에는 사전 관련 취약점 정보 및 보안 수준이 높은 개발자의 소스 등 분석 도구 적용을 위한 제반사항이 필요하다. 이에 본 장에서는 상기 방법들을 보완할 수 있는 분석적 취약점 평가 방법을 제시하고자 한다.

분석적 취약점 평가 방법은 대상 시스템에 대한 기능 및, 성능, 하드웨어 및 소프트웨어 구성, 구현 및 운영 사항, 운전 환경 등에 대한 자료 및 정보 분석을 통해 자산의 취약점을 평가하는 과정으로 실제 또는 모사 시스템와 비교하여 현실적 제한 없이, 대상 시스템에 대한 자료의 분석을 통하여 취약점을 파악할 수 있어 효율적이고 광범위한 평가가 가능하다. 운영 시스템에 영향을 미치지 않고 테스트베드의 구축을 위한 비용이 소요되지 않으며 자료 분석을 통한 빠른 취약점 파악으로 선행 보안조치를 적용할 수 있으며 기술적 범위뿐 아니라 관리적, 물리적, 구조적 문제점이 있는지에 대한 파악이 가능하여 침투 시나리오 및 점검 체크리스트 구성 시 참고자료로 활용할 수 있다. 다음 Table3은 2장에서 분석한 분석 환경 및 분석 도구와 비교한 분석적 취약점 평가 방법에 대한 개요이다.

Table 3. Overview of analytical vulnerability assessment method

	Analytical Vulnerability Assessment
Scope	- Technical - Physical - Operational - Structural - Management
System Influence	None
Reliability	Medium
Understand status	- Security measures for vulnerabilities - Alternative function - Factors to consider when securing a vulnerability
Direction of security setting	Provide direction of security measures from multiple angles
Usability of Results	- Comparable analysis and verification with On-site operation system and simulation system - Configure Penetration Scenario and Checklist - Available for reference of analysis tool development
Other Action	None

3.2 프로세스

본 연구에서의 분석적 취약점 평가 방법에 대한 단계 별 분석 내용은 다음과 같다.

1) step0. 자산 분석

대상 자산에 기본적인 자료 및 정보 수집 단계로 대상에 적용 가능한 취약점을 식별하기 위해 대상의

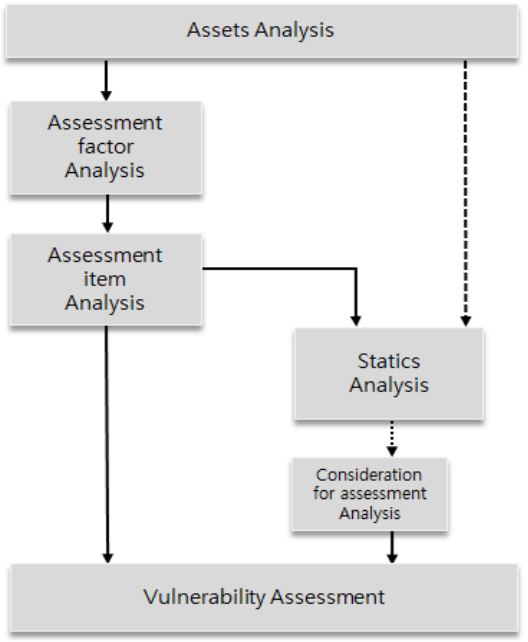

Fig. 2. Processes of analytical vulnerability assessment method

일반적인 특성, 구성모듈, 플랫폼 등의 분석을 수행한다. 본 단계에서의 상세 분석 범주는 다음과 같다.

- 대상 자산이 가지는 고유의 성질이나 대상 자산의 특정한 속성
- 대상 자산의 운영체제, 프로그램 등 대상 자산의 상세한 구성 요소
- 대상 자산을 포함한 시스템의 네트워크 구조, 네트워크 장비 등 대상 간 네트워크 정보
- 대상 자산을 구현한 프로그램 언어
- 대상 자산에서 사용하는 프로토콜, 통신 방향 등 통신 방법
- 대상 자산이 가지는 기본적인 기능
- 대상 자산의 표준화 규격

2) step1. 평가 요소 분석

step0의 분석 결과를 통하여 원전디지털자산의 평가 요소 도출 단계로 공개되거나 알려진 취약점에 대해 대상 자산에 적용가능 여부를 파악하여 보안조치에 대한 점검이 필요한 취약점 유형들을 분석한다. 본 단계에서의 상세 분석 범주는 다음과 같다.

- 대상 자산의 OS, 어플리케이션 등을 포함한 소프트웨어 및 대상 자산을 포함한 시스템의 네트워크에서의 설계 및 구현 상에 있을 수 있는 기술적 취약점 유형
- 대상 자산에 대한 설정, 유지보수 등 운영 및 관리 상에 있을 수 있는 운영적 및 관리적 취약점 유형
- 대상 자산이 속해있는 환경의 통제 및 감시, 기기 등 물리적인 속성의 물리적 및 구조적 취약점 유형

3) step2. 평가 항목 분석

step1에서 도출한 원전디지털자산 평가 요소를 평가하기 위한 평가 항목 도출 단계로 평가 요소인 취약점 유형의 속성 및 특성에 대한 분석을 통하여 적용할 환경, 기본적인 점검방법, 필수적 또는 기본적인 보안조치, 발견된 사례 등의 분석을 통하여 평가할 항목들을 도출한다.

Scope	Technical	**Assessment factor**	Permissions, Privileges, and Access Controls
Detailed Assessment Factor	Access Controls		
Description	Improper authentication and access control in possible execution paths can damage the device or allow access and execute unauthorized data		
Main Assessment Item	• Whether the system is closed when the login attempt fails • Whether the connection is closed after a given working time • Whether to terminate the session if it has not been used for a certain period of time • Whether authentication retry attempts are restricted		
Detailed Item Example	• Ensure that system startup and functionality can be accessed with default privileges • Check if file upload is possible with remote control • Check whether the file can be read or overwritten using the protocol without host login • Check for backdoor account • Determine whether network file systems have restricted security settings • Ensure that the attacker can access the host when the authorized administrator runs the system • Check whether the database is access control based on records, not users		
Applied Environment	OS, Engineering Software, Network device		

Fig. 3. Step3 Example of configuration for vulnerability assessment item

4) step3. 현황 분석

step2에서 도출한 평가 항목에 대한 평가 준비 단계로 step0를 참조하여 평가 요소 별 주요 특징, 적용환경, 보안환경 등 대상자산에 대한 현황을 분석한다. 본 단계에서의 상세 분석 범주는 다음과 같다.

- 대상 자산이 적용되어 있는 물리적 환경, 연계 방식 등 환경적 특성
- 대상 자산의 보안조치에 관한 현황 파악

- 적용 가능한 취약점 관련 대상 자산의 속성
- 자산의 속성 및 환경에 의해 취약점 평가 시 고려야 할 사항 도출

5) step4. 평가

step3 결과를 고려하여 step2에서 도출한 평가 항목에 대한 평가를 수행하는 단계로 평가 기준을 정립하고 해당 항목에 대한 기능 미사용 및 적절한 보안조치 적용, 보안조치 부재 시 대체가능한 기능 여부, 악의적인 공격 시도 시 위험성 여부 등에 대한 종합적인 판단을 수행한다.

IV. 시범 적용

본 장에서는 원전디지털자산 중 원전 안전계통에 사용하기 위하여 엄격한 품질체계 및 검증 과정을 통하여 원전의 안전기능에 적용한 제어기인 안전등급 PLC를 대상으로 본 연구에서 제시한 취약점 평가 방법을 적용한 결과를 제시한다.

4.1 자산 분석

안전등급 PLC는 높은 신뢰성과 고도의 안전성을 확보하기 위해 규제지침 및 기술 표준에 따라 개발되며 step1에서 분석한 결과 중 일부는 다음 Table4와 같다.

Table 4. Basic information of Safety class PLC

Scope	Description
Characteristics	- Real time System - Safety Class 1E - Fault-Tolerance
Language	- C, LD/FBD
Function	- Cyclic Redundancy Check - Diagnosis
Configuration	- Process Module - Communication Module - Bus Module - I/O Module - Power Module - Engineering S/W
Communication	- Communication-Network : Profi-bus - Communication-Datalink : RS-232, RS-422
Related Standards	- Reg. Guide 1.89 - 10CPR50. App. B - IEEE 323 - IEEE 344

4.2 평가 요소 및 평가 항목

본 절에서는 안전등급 PLC 취약점 평가를 위해 산업제어시스템 사이버보안 취약점 리스트 [1], [2], [3] 분석을 통하여 안전등급 PLC에 있을 수 있는 취약점 요소들을 Table5와 같이 도출하고 필수적이거나 기본적으로 점검해야 할 주요 평가 요소별 평가 항목 결과를 기술한다.

4.2.1 기술적 평가 요소 별 평가 항목

기술적 범주에서는 소프트웨어, 프로토콜 및 통신, 시스템 및 네트워크 장비, 보안기능 및 장비 등을 대상으로 주요 평가 요소에 관련한 보안요건, 기능, 보안조치 등의 반영여부를 평가하여야 하며 상세한 평가 항목은 다음과 같다.

□ 부적절한 입력값 검증
- 메모리 고정 할당 또는 입력 길이 점검 논리 여부
- 입력변수 경계검사 및 처리 논리 보유 여부
- 입력변수의 매개변수에 대한 유효성 검사 여부
- 허용 목록에 따른 입력 매개 변수 상태 확인 여부
- 변수화된 쿼리 또는 저장된 절차를 사용한 SQL 쿼리 사용 여부
- 클라이언트에서의 유효성 중복 검사 수행 여부

□ 비안전한 코드 사용
- 검증된 함수와 표준함수를 사용 여부
- 인증절차에 취약한 해쉬 알고리즘 사용 여부
- 변조될 가능성이 있는 모든 포인터에 대해 사용되기 전 건전성 검사 논리 보유 여부

□ 부적절한 인증
- 단계별 인증 기능 보유 여부
- 모든 통신 채널 및 소프트웨어와 시스템과 연결되는 다른 장치들의 인증 여부

□ 허용, 권한 및 접근 통제
- 로그인 시도 실패 시 시스템 폐쇄 여부

Table 5. Main assessment factor of Safety class PLC

	Main Assessment Factor	Detailed Assessment Factor
Technical	Improper Input Validation	Buffer overflow, Lack of Bounds Checking, Command Injection, Path Traversal, Dos Attack
	Insecure Code	Use of Insecure Functions, Use of Insecure 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
	Insufficient data integrity	Absence of Data Integrity Check
	Communication and Protocols	Use of Plain text, Use of public protocols, Use of insecure protocols, MITM Attack
Operational and Management	Permissions, Privileges and Access Controls	Account Management, Password Management, Identification and Authentication Management
	Maintenance	Patch Management, Insufficient Documentation
	Incident Response	Insufficient Audits and Assessments, Backup and Restore, Log Management, Real time Detection of security incident
	Configuration and Settings	Third Party and Proprietary S/W, Unnecessary Service, Default Setting
	Network Management	Network Design, Network Segmentation, Firewall, Security Perimeter
Physical and Structural	Environment Settings	Physical protection, Environment Controls, Physical Port for Media interfaces
	Hardware	RPI&EMP, Spare component, Redundancy of critical system, Removable media Management

- 주어진 작업 시간 후에 접속 종료 여부
- 일정 시간 동안 미입력시 세션 파기여부
- 암호화를 통한 인증 관련 정보의 보호 기능 여부
- clear-text 및 plain-text로 보내지는 자격 증명 여부
- 권한의 남용 관리의 적절성 여부
- 높은 등급의 권한이 필요한 시스템 관리의 적절성 여부

□ 불충분한 데이터 무결성 검증
- 클라이언트와 서버에서의 인증절차 중복 수행 여부
- Checksum 및 Hash와 같은 전송 중 데이터의 무결성 확인 방법 사용 여부
- 데이터의 전송 또는 저장 시 충분히 검증된 암호화 기법 수행 여부

□ 통신 및 프로토콜
- 데이터의 전송 또는 저장 시 충분히 검증된 암호화 기법 수행 여부
- 공개 프로토콜 사용 여부 및 보안 기능 보유 여부
- 원전 전용 프로토콜에 대한 보안 기능 보유 여부
- 포트넘버, IP주소, 통신방향, 통신 내용에 따른 패킷 필터링 여부
- 통신 채널의 양 끝단을 인증하는 절차 수행 여부

4.2.2 운영적 및 관리적 평가 요소 별 평가 항목

운영적 및 관리적 범주에서는 계정 및 인증 관리, 운영 및 개발 환경 관리 등 사이버 보안 정책에 관한 수립 및 관리 여부를 평가하여야 하며 주요 평가 요소에 대한 상세한 평가 항목은 다음과 같다.

□ 허용, 권한 및 접근 통제
- 기능별로 다른 계정 부여 여부
- 계정 타입별 최소한의 권한 부여 여부
- 시스템 설계와 실행 권한의 분리 여부
- 인증 및 식별 정책 개발, 배포, 주기적 검토 및 업데이트 여부
- 패스워드 암호화 여부 및 복잡도 보유 여부

□ 유지보수
- 필요한 패치 테스트 환경 보유 여부
- 패치로 인한 변경사항들의 포괄적인 회귀 테스트 수행 여부
- 시스템의 기능성, 보안 보장성, 적시성을 고려한 패치관리 여부
- 악성코드 방지를 위한 소프트웨어 설치 및 업데이트 여부
- 보안 정책 및 정책의 공식화 및 문서화 여부
- 자산 목록 존재 여부
- 입출력 매체 관리의 적절성 여부

□ 비상대응
- 보안 감자 및 평가의 주기적 수행 여부
- 백업 정보의 관리 여부
- 로그 관리 기능 여부
- 침입탐지/방지 기능 보유 여부
- 실시간 로깅 및 보안감지 기능 여부

□ 구성 및 설정
- 독점 소프트웨어 사용 여부
- 중요 정보의 공유파일 저장 여부
- 불필요한 기능의 확인 및 제거 여부
- 제3자 어플리케이션의 관리 여부
- 보안 기능의 미사용 또는 비활성화 여부
- 기본적으로 설정된 기능에 대한 변경 여부

□ 네트워크 관리
- 네트워크 물리적 혹은 논리적 분할 여부
- 제어망과 비제어망의 물리적 분할 여부
- 네트워크망 구조 보안 적절성 여부
- 안전과 비안전 네트워크간 연결 장비의 보안 적절성 여부
- 네트워크 장비의 직접적인 접근과 관리자 기능을 제한하기 위한 접근 제어 여부
- 네트워크 구성의 일치성 여부

4.2.3 물리적 및 구조적 평가 요소 별 평가 항목

물리적 및 구조적 범주에서는 시스템의 안전성 및 신뢰성 만족을 위해 외부 환경에 대한 검증된 장비 사용 및 물리적 보호 장치가 적절하게 잘 취해였는지에 대한 평가가 필요하며 주요 평가 요소에 대한 상세한 평가 항목은 다음과 같다.

□ 환경설정
- 공조시스템의 적절성 여부
- 물리적 보호 장치의 적절성 여부
- 휴대용 저장매체 목록 및 관리 여부
- 주요 장치의 이중화 여부
- 매체인터페이스 포트의 물리적 접근에 대한 보안 적절성 여부
- 다중 NIC(랜카드 등)에 대한 구성관리 기능 및 NIC 불법 장착에 대한 탐지 기능 여부

□ 기기검증
- 무선 주파수(RPI)와 고출력전자기파(EMP) 검증 여부
- Spare 부품의 적절성 여부

4.3 현황 분석

안전등급 PLC는 원전 안전 계통에 사용하기 위하여 엄격한 품질체계 및 검증 과정을 통하여 원전의 안전기능 적용에 대한 허가를 획득한 제어기로서 제품마다 기능, 성능 등 특성에 다소 차이는 있으나 일반적으로 하드웨어와 소프트웨어로 구성되어 적용 목적에 따라 유연하게 구성, 처리하는 장점을 갖고 있다. 본 절에서는 안전등급 PLC 취약점 평가 전 고려해야 할 설계적 특성 및 적용 환경에 대해 제시한다.

4.3.1 설계적 특성

□ Software

안전등급 PLC의 소프트웨어는 운영체제, 엔지니어링 개발 도구 및 응용소프트웨어로 분류할 수 있으며 관련된 주요 특성은 다음과 같다.

- 모든 소프트웨어는 개념설계 단계, 계획단계, 요구사항 단계, 설계단계, 구현단계, 검증단계의 모든 개발 생명주기에 걸쳐 안전 요건에 대한 확인 및 검증이 수행된다. 즉, 소프트웨어에 잠재 가능한 안전 위험 요소들은 이러한 확인 및 검증과정에 의하여 제거된다.

- 운영체제는 경성 실시간(Hard Real-Time) 스케줄링 방식을 사용하며, 상용 운영체제를 원전에 적합하도록 수정한 독자적 운영체제를 적용한 소프트웨어를 사용한다.
- 운영체제는 제어기 각 모듈 및 프로그램 실행과 관련한 전반적인 상태를 진단할 수 있는 자가진단(diagnosis) 기능을 수행한다.
- 통신 프로토콜은 토큰패싱과 같이 결정론적 방식을 사용하며 응용수준의 프로토콜은 독자적으로 개발한 소프트웨어를 사용한다.
- 안전등급 PLC의 모든 소프트웨어는 형상관리 시스템을 통하여 관리되며 엔지니어링 도구와 안전등급 PLC연결을 위한 인증이 요구된다.

□ Network

안전등급 PLC에 적용되는 통신은 일대일 데이터 링크, 다대다 네트워크 통신망 및 직렬통신의 3가지 종류로 분류되며 관련된 주요 특성은 다음과 같다.

- 모든 통신은 데이터량, 메모리, 송수신 주소 등이 고정되고 주기적으로 전송하며 전송권한이 결정론적인 방식을 사용한다.
- 안전등급 PLC와 엔지니어링 개발 도구 간에는 RS-232의 직렬통신 방식을 사용한다.
- 데이터 통신에는 주소, CRC와 함께, 순차적(Sequential) 번호를 송신하여 패키지의 분실을 체크한다.
- 데이터 통신모듈은 CRC 오류, 송수신 실패 등과 같은 기본적인 진단기능을 보유한다.

□ Hardware

안전등급 PLC는 전자기파, 온도, 습도 내진 등에 대한 기기검증을 수행하고 해당 기준을 만족하며 다음과 같은 특성을 보유한다.

- 안전등급 PLC의 기본 작동 기능은 Key 스위치로 보호되며, 모든 장치는 기기검증에 의하여 환경적 위해성에 영향을 받지 않는다.
- 프로세서 모듈, 전원 모듈, 통신 모듈과 같은 주요 구성모듈은 이중화로 구성된다.

4.3.2 적용 환경

안전등급 PLC이 적용되는 원전 안전계통은 그 특성으로 인하여 물리적 환경 또는 연계 방식이 제한적이다. 따라서 취약점 분석 시, 디지털자산이 갖고 있는 특성 뿐만 아니라 이들이 적용되는 환경을 고려하여 평가해야 하며 주요 특성은 다음과 같다.

- 디지털장치의 특성으로 인한 다량 손실을 방지하기 위하여 채널 내부의 다중화를 고려한다. 채널 내부의 다중화는 안전등급 PLC의 물리적인 다중화 또는 PLC 내부 프로세서의 다중화 방식을 사용한다.
- 다중화 채널 간에는 물리적으로 분리되고, 전기적으로 격리되며 통신 독립성이 유지된다.
- 안전계통은 정보처리계통(IPS) 등의 비안전계통으로 단방향 통신에 의한 송신 기능만 존재하며 비안전계통으로부터의 수신 연계를 갖지 않는다.
- 안전계통의 구성 장치는 Key-Lock에 의하여 보호되는 캐비닛 내부에 장착된다.
- 안전계통의 작동은 안전성 분석에 의하여 요구된 수행 응답시간을 만족해야 하므로 고유 기능 이외의 부가적인 기능은 응답시간 요건을 만족할 수 있는 범위 내에서 수용될 수 있다.

4.4 평가 결과 예시

본 연구에서 제시한 항목은 최종 장비의 사용 환경 및 시스템의 설정 상태에 따라 결과가 달라질 수 있으며, 총 64개의 항목 중 대상 자산인 안전등급 PLC에 적용되는 사항은 60개, 관련 기술을 사용하지 않거나 구조가 존재하지 않는 등으로 해당사항이

Table 6. Result of vulnerability assessment for safety class PLC

Unit : Number

		T	O/M	P/S
Applicable	S	16	24	7
	CR	5	5	1
N/A		3	1	0
Total		26	30	8
		64		

* S : Secure
CR : Complement-Requiring
** T : Technical
O/M : Operational and Management
P/S : Physical and Structural

Table 7. Example of vulnerability assessment for Safety class PLC

Assessment factor	Detailed Assessment factor	Design Features and status of the Safety Controller	Assessment
Technical			
Improper Input Validation	Buffer overflow	- Any external input function is not possible while online - Validating function for Input value exists - Verified in accordance with nuclear coding standard NUREG/CR-6463(4.1.1.5 Utilizing Memory-Related Functions with Boundary Checking, 4.1.1.9 Proper Array Indexing) during software V&V process	S
	Lack of Bounds Checking		S
	Command Injection	- Disable of external command - There is no OS Command interface to execute by command line - Fixed only task by engineering tools - There is no database SQL query interface	N/A
	Path Traversal	- There is no file system concept to use external support path specification	N/A
	Dos Attack	- Fixed type for transmission data, scan time, task number and etc. - Provide the function for prevent Dos attack on external interface	S
Operational and Management			
Permissions, Privileges, and Access Controls	Account Management	- There are separate administrator and developer accounts on the Engineering software - Administrator account can delete, create, and modify the user account and the encryption information of the PLC. - Separate login required to connect to PLC	S
	Password Management	- Password are encrypted and provide the function to force them to have sufficient length and complexity - The length and complexity of passwords are limited to two characters sets and eight length	CR
	Identification and Authentication Management	- The configuration file of Engineering software is restricted by encryption - Establish and implement procedure for identifying when installing application software - It need to be review through operational management process	S
Physical and Structural			
Environment Set	Physical protection	- The cabinet-key Lock, Serial port are physically closed - The cabinet is designed to reflect the locking device and the building must have an ID card for access.	S
	Physical Port for Media interfaces		S

없는 사항은 4개의 항목으로 분석되었다. 이에 본 연구에서는 평가 항목에 대하여 안전등급 PLC 적용 여부 및 대응 고려사항이 존재하는지에 대한 검토를 통하여 설계 요건, 표준에 따른 검증, 해당 요소에 대한 적절한 보안조치 등으로 인해 취약점이 없다고 판단된 결과를 양호(Secure)라 분류하였으며, 해당 요소에 대한 보안조치 부재 및 미흡, 대체 기능 부재 등으로 악의적인 공격 시도 시 위험이 있을 수 있으며 이에 대한 보안조치가 요구된 항목과 본 연구의 시점에서 관련된 보안 기술이 도입되고 있는 중이거

나 검증이 진행되고 있는 사항 또한 보완필요(Complement-Requiring)로 분류하여 판단하였으며 정량적인 그 결과값은 Table6과 같다.

또한 Table7은 각 범주 별 일부 상세 평가 요소에 대한 평가 결과 예시이며, 각 범주 별 주요 현황 분석은 다음과 같다.

□ 기술적 보안성

소프트웨어는 설계 및 안전 요건에 대한 확인 및 검증 과정에서 무결성 보장을 위한 검증을 수행하고 있으며 부적절한 입력값 검증 , 비안전한 코드 사용으로 인한 취약점은 제거되었을 것으로 판단된다. 또한 로그인 시, 일정횟수 이상 실패, 접속 후 일정 시간 미 입력 및 통신 시 등에는 로그아웃, 세션을 종료하는 기능을 보유하여 적절한 접근통제를 하고 있으나 중요한 데이터 유출 방지를 위한 데이터 암호화 기능이 권장된다.

□ 운영적 및 관리적 보안성

일반적으로 개발자 계정과 관리자 계정으로 나뉘어 통제되고 있지만 두 계정의 정확한 기능 범위에 대한 구분 확인이 필요하며 패스워드 관리에 있어서 복잡성 강화가 요구된다. 네트워크 관리에 있어서는 원전디지털계측제어 시스템은 폐쇄망으로 운영되어 웹 어플리케이션을 사용하지 않고 원격접속이 불가하여 이에 관련된 취약점은 존재하지 않는 것으로 판단된다.

□ 물리적 및 구조적 보안성

원자력 시설 계측 제어시스템은 높은 안전성 및 신뢰성 만족을 위하여 구조적으로 제한적인 특성을 갖으며 하드웨어 사용에 있어서 엄격한 가용성/기능성/내환경 시험을 적용하고 적절한 공조시스템을 설계에 반영하였기에 물리적 및 구조적인 취약점은 없다고 판단된다.

V. 결 론

원전 시스템은 기존의 IT 시스템과의 폐쇄성 및 보안 우선순위 등에서 많은 차이가 있으며 실시간성 및 가용성 등과 같은 원전 고유의 특성으로 인해 실제 운용 시스템 및 모사 시스템 구축을 통한 침투테스트 및 모의해킹, 취약점 분석 도구와 같은 기존의 취약점 분석 방법의 적용에 어려움이 있고 제반사항 구축에 많은 비용 및 시간이 필요하다. 이에 본 연구에서는 기존의 취약점 분석 방법의 한계점을 보완하는 원전시스템에 적합한 분석적 취약점 평가 방법 및 시범 적용한 결과를 제시하여 본 연구에서 제시한 방법의 적용성 및 실효성을 확인해보았다.

본 연구에서의 분석적 취약점 평가 방법은 자산 분석, 평가 요소 및 평가 항목 분석, 현황 분석을 통해 대상 자산의 특성 및 요건, 환경적 사항을 고려하여 대상 시스템에 대한 보안성에 대해 다각도로 평가하는 과정으로, 평가 결과를 통해 빠른 취약점 파악으로 선행 보안조치를 적용할 수 있으며 또한 향후 침투시나리오 및 점검 체크리스트 구성 시 참고자료로 활용될 것으로 기대된다.

References

[1] National Institute of Standards Technology(NIST), 800-82(rev2) “Guide to Industrial Control Systems (ICS) Security”, May. 2015.

[2] Department of Homeland Security (DHS), “Common Cyber security Vulnerabilities in Industrial Control Systems”, May. 2011.

[3] Department of Energy/Idaho National Laboratory(DOE/INL), “Vulnerability Analysis of Energy Delivery Control Systems”, Sep. 2011.

[4] National Institute of Standards Technology(NIST). 800-53(rev.4) “Recommended Security Controls for Federal Information Systems and Organizations”, Apr. 2013.

[5] Ministry of Science and ICT, “The Analysis and Evaluation Standards for Information and Communication Infrastructure, vol. 2013, no. 37, Oct. 2013.

[6] International Atomic Energy Agency (IAEA), Nuclear Security Series No. 13, “Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities” (INFCIRC/225/Revision 5), Jan. 2011.

[7] International Atomic Energy Agency (IAEA), "Nuclear Security Series No. 17, Computer Security at Nuclear Facilities", Dec. 2011.
[8] Korea Institute of Nuclear Nonproliferation And Control(KINAC), KINAC/RS-015, "Regulatory Standard on Computer Security of Nuclear Facilities", Dec. 2016.
[9] Korea Institute of Nuclear Nonproliferation And Control(KINAC), KINAC/RS-019, "Regulatory Standard on Critical Digital Assets of Nuclear Facilities", Dec. 2015.
[10] U,S.Nuclear Regulatory commissio(U.S.NRC), Regulatory Guide 5.71(R.G 5.71), "Cyber Security Programs for Nuclear Facilities", Jan. 2010.
[11] U,S.Nuclear Regulatory commissio(U.S.NRC), Regulatory Guide(R.G) 1.152(Rev.3), "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants", Jul. 2011.
[12] U,S.Nuclear Regulatory commissio(U.S.NRC), 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks", Mar. 2009.
[13] Nuclear Energy Institute(NEI), NEI 10-09(rev.0) "Addressing Cyber Security Controls for Nuclear Power Reactors", Sep. 2011.
[14] U,S.Nuclear Regulatory commission(U.S.NRC), NUREG/CR-6847, "Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants", Oct. 2004.
[15] Nuclear Energy Institute(NEI), NEI 08-09(Rev.6), "Cyber Security Plan for Nuclear Power Reactors", Apr. 2010.
[16] K. J. Cha, J. H. Ahn, Y. M. Kim, and Y. G. Kwon, "A Study of PLC System Vulnerability Checklists in Nuclear Power Plants", Transactions of the Korean Nuclear Society Autumn Meeting, Oct, 2012.
[17] Lee Cheol Kwon, "Nuclear Power Plant Instrumentation and Control Systems Cyber Security Technology Trends," Journal of The Korea Institute of information Security & Cryptology, vol. 22, no. 5, pp. 28-34, Aug. 2012.
[18] D. W. Kim, B. G. Min, H. D. Park, and S. W. Park, "PLC -Based Control System Vulnerability Analysis Method", Journal of The Korea Institute of information Security & Cryptology, vol. 25, no. 5, pp.26-36, Oct. 2015.
[19] Choi Myeonggil Choi, "A Study on Security Evaluation Methodology for Industrial Control Systems", Journal of The Korea Institute of information Security & Cryptology, vol. 23, no. 2, pp. 287-298, Apr. 2013.
[20] B. G. Min, W. G. Ahn, J. T. Seo, "Vulnerability Analysis Method according to Cyber Security Threat Change", Journal of The Korea Institute of information Security & Cryptology, vol. 24, no. 1, pp. 7-12, Feb. 2014.
[21] Kim Do Yeon, "Vulnerability Analysis for Industrial Control System Cyber Security", Journal of The Korea Institute of electronic communication sciences, vol. 9, no. 1, pp. 137-142, Jan. 2013.
[22] Park Sang-Hyung, "An Empirical Study of the Method of Vulnerabilities Analysis on Instrumentation & Control System for Nuclear Power Plant", PH.D. Thesis, Graduate School of Soongsil University,

Jun. 2011.
〔23〕 Kang Young doo, "A Study on Cyber Security Assessment Methodology of Instrumentation& Control Systems for Nuclear Power Plants", PH.D. Thesis, Graduate School of Chonbuk National University, Feb. 2010.
〔24〕 J. G. Song, J. W. Lee, G. Y. Park, K. C. Kwon, D. Y. Lee, and C. K. Lee. "An Analysis of Technical Security Control Requirements for Digital I&C Systems in Nuclear Power Plants". Nuclear Engineering and Technology, Vol.45, No.5, Mar. 2013.
〔25〕 U,S.Nuclear Regulatory commission(U.S.NRC), NUREG/CR-6463, "Review Guidelines on Software Language for Use in Nuclear Power Plants Safety Systems", Jun. 1996.
〔26〕 Chatham House, "Cyber Security at Civil Nuclear Facilities", Sep. 2015.
〔27〕 Department of Homeland Security (DHS), "NCCIC/ICS-CERT FY 2015 Annual Vulnerability Coordination Report", 2015.
〔28〕 National Cybersecurity and Communications Integration Center(NCCIC), "ICS-CERT Annual Assessment Report", 2016.
〔29〕 M. Holt, A. Andrews, CRS Report RL34331, "Nuclear Power Plant Security and Vulnerabilities", Jan. 2014.
〔30〕 National Cyber Security Center(NCSC), " Checklist security of ICS/SCADA systems(Take organisational and technical measures)", May. 2016.

〈저자소개〉

김 인 경 (In-Kyung Kim) 정회원
2015년 2월: 고려대학교 수학과 석사
2017년 5월~현재: 한국원자력통제기술원 사이버보안실 전문연구원
〈관심분야〉 제어시스템 보안, 기반시설 보안, 사이버보안 평가

권 국 희 (Kook-heui Kwon) 정회원
2008년 2월: 경북대학교 컴퓨터공학과 학사
2012년 9월: 아주대 정보전산학과 석사
2018년 8월: 충남대 컴퓨터통신 및 보안 박사과정 수료
2007년 11월~2011년 8월: 한국전력기술 원자력계측제어실 선임기술원
2011년 9월~현재: 한국원자력통제기술원 사이버보안실 선임연구원/실장
〈관심분야〉 정보보안, ICS 보안, 개발단계 보안, Risk 평가