*Journal of The Korea Institute of Information Security & Cryptology* ISSN 1598-3986(Print)
VOL.29, NO.6, Dec. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.6.1425

# 원자력발전소 디지털 제어기의 사이버보안 기능 적합성 시험방법 연구*

송 재 구,†‡ 신 진 수, 이 정 운, 이 철 권, 최 종 균
한국원자력연구원

# Research of Cyber Security Function Test Method for Digital I&C Device in Nuclear Power Plants*

Jae-gu Song,†‡ Jin-soo Shin, Jung-woon Lee,
Cheol-kwon Lee, Jong-gyun Choi
Korea Atomic Energy Research Institute

요 약

디지털 제어기 적용의 확대로 원자력 시설에 대한 사이버보안 이슈가 대두되었다. 이에 대처하기 위해 공표된 국내 원자력 시설에 대한 사이버보안 기술기준 RS-015에서는 원자력 시스템 개발자에게 보안 기능의 적용과 아울러 알려진 취약점 분석, 보안 기능에 대한 시험 및 평가를 요구하고 있다. 이를 위해서는 원자력 사이버보안 기술기준에 따른 보안 기능 적합성 시험 절차 및 방법 개발이 필요하다. 본 연구에서는 RS-015의 기술적, 운영적, 관리적 보안조치에 대한 세부항목을 분류하여 기기 수준에서 요구되는 보안 요건을 도출하고 기기에 구현되는 보안 기능이 보안 요건을 만족하는지를 시험하는 절차와 방법을 개발하였다. 본 논문에서는 보안 기능 적합성 시험 절차 및 방법 개발을 위한 과정을 설명하고 개발된 시험사례를 제시한다.

ABSTRACT

The expanded application of digital controls has raised the issue of cyber security for nuclear facilities. To cope with this, the cyber security technical standard RS-015 for Korean nuclear facilities requires nuclear system developers to apply security functions, analyze known vulnerabilities, and test and evaluate security functions. This requires the development of procedures and methods for testing the suitability of security functions in accordance with the nuclear cyber security technical standards. This study derived the security requirements required at the device level by classifying the details of the technical, operational and administrative security controls of RS-015 and developed procedures and methods to test whether the security functions implemented in the device meet the security requirements. This paper describes the process for developing security function compliance test procedures and methods and presents the developed test cases.
**Keywords:** Security Test, Digital I&C, Nuclear Power Plant

## I. 서 론

기반 시설에 대한 사이버 위협 증가와 함께 2010년 미 원자력 규제 위원회(NRC)의 RG5.71 규제 지침의 발표로 시작된 원자력 사이버보안 규제는 우리나라의 규제 기준 RS-015의 공표로 이어졌으며

Received(09. 03. 2019), Modified(1st: 10. 11. 2019, 2nd: 10. 23. 2019), Accepted(10. 29, 2019)
* 본 연구는 산업통상자원부(MOTIE)와 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 연구과제입니다. (No. 20171510102100)
† 주저자, jgsong@kaeri.re.kr
‡ 교신저자, jgsong@kaeri.re.kr(Corresponding author)

이에 따라 원자력 시설 운영 기관은 보안성 평가와 함께 다양한 보안 조치를 이행하기 위해 노력 중에 있다. 하지만 기존 운영 중인 원자력 시설 대부분은 아날로그 시스템으로 운영 중이며, 디지털화된 일부 시스템 또한 자원의 한계로 기술적 사이버보안 적용에 어려움이 따른다.

이에 운영 기관들은 운영 및 관리적, 대안적 조치를 주된 사이버보안 대응 방안으로 고려해 왔다. 하지만 노후화된 계측제어시스템의 기기 교체와 성능 개선 요구에 따라 디지털 제어기 적용 가능성이 높아짐과 동시에 기술적 사이버보안 강화를 위한 보안 기능 적용이 요구되고 있다.

특히, 최신 디지털 계측제어시스템이 적용된 한국형 원전 APR1400(Advanced Power Reactor 1400) 모델로 개발된 신고리 5,6 호기는 사이버보안 강화 요구에 따라 비안전 계통을 중심으로 다양한 보안 기능이 추가 검토되고 있다.

또한, 해외 PLC(Programmable Logic Controller) 제작사와 보안 전문 업체는 강화되고 있는 원자력 시설 사이버보안 규제를 만족하기 위해 보안 기능을 내재한 제어기를 개발하고 있다[1,2,3,4,5]. 국내의 경우 한국형 원전 APR1400 주요 디지털 제어기 국산화를 성공한 제작사를 중심으로 2017년부터 제어기 성능 향상과 함께 사이버보안 강화를 위한 기능 개발 연구를 진행 중으로 사이버보안 기능 적용에 따라 원자력 규제에 근거한 사이버보안 기능 시험 방법이 필요하다.

이에 본 논문에서는 원전 디지털 계측제어기에 추가되는 사이버보안 기능을 시험하기 위해 규제 기준에 따른 사이버보안 기능 요건 적합성 시험 방법을 제안한다.

## II. 사이버보안 규제 지침 및 보안 시험 현황

본 장에서는 원자력 시설에 적용되는 제어기의 보안 기능 시험 방법 도출을 위해 국내외 규제 지침 및 기술기준을 살펴보고, 정보보호제품 및 정보통신 시설에 대한 사이버보안 시험 및 평가 현황을 알아본다.

### 2.1 원자력 시설에 대한 사이버보안 지침 및 평가현황

국내 원자력 시설에 대한 물리적 방호, 사이버보안 규제를 담당하는 한국 원자력 통제기술원(KINAC)은 2014년 KINAC/RS-015 "원자력 시설 등의 컴퓨터 및 정보시스템 보안 기술기준"을 발표하고 사이버 공격의 대상이 되는 필수 디지털 자산에 대해 운영적, 관리적, 기술적 사이버보안 조치를 적용 및 이행하도록 하고 있다[6]. 특히, 개발자 보안 테스트 항목을 통해 모든 보안 요건을 만족하는지 테스트 및 평가하도록 하여, 시스템에 알려진 취약점 및 악성코드가 없음을 보장하도록 명시하고 있다.

미 NRC는 2010년 원자력 시설에 대한 사이버보안 프로그램을 통해 원전 운영 기관에서 디지털 자산을 사이버 공격으로부터 보호하기 위해 규제 가이드를 발표하고 이를 기반으로 현 미국의 원자력 시설에 대한 사이버보안 규제를 이행하고 있다[7].

미국 국립 표준 기술연구소(NIST)는 산업 제어 시스템을 대상으로 보안 요구 사항 및 위험 분석에 따른 보안대책을 설명한 SP 800-53을 발표했다[8]. 본 문서는 미국 규제 기준인 RG5.71에 원자력 시설에 요구되는 보안 통제 항목 참고 자료로써 활용되고 있다.

국제원자력기구(IAEA)는 원자력 시설에 대한 사이버 요건을 기술한 Nuclear Security Series No.17 Computer Security at Nuclear Facilities를 발표함으로써, 원자력 시설에 대한 악의적 행위로부터 중요한 디지털 자산의 보안 및 안전을 보장하기 위해 권고사항 및 이행에 관한 기술 지침 제공하고 있다[9].

이와 같이 사이버보안 이슈에 대응하기 위해 국내외 주요 원자력 관련 기관에서 기술 가이드 문서를 개발하여 활용하고 있다. 규제 대상 운영사는 규제 문서들의 요건에 따라 적합한 규제 준수 방법을 제안하여야 한다. 이에 NEI(Nuclear Energy Institute)는 미국 내의 규제 대상자인 원전 개발, 운영사들을 대표하여 규제 준수를 위한 가이드 문서를 개발하였다. 대표적으로 사이버보안 대상 자산 식별 방법, 사이버보안 평가 방법에 대한 가이드를 개발하고 규제 기관인 NRC와 지속적인 협의를 통해 합리적인 규제 수준을 도출하고자 노력하고 있다[10,11].

이러한 국내외 원자력 주요 기관들의 노력에도 원자력 발전소에 적용되는 제어기 수준에서 요구되는 보안 기능에 대한 적합성 시험을 위한 기준이 제시된 사례가 없다.

원자력 안전 등급 소프트웨어의 경우 생명주기에 따라 검증 및 확인(V&V) 활동을 수행하여 소프트

웨어 검증 절차를 이행하고 있다. 검증 방법으로 인허가 적합성 검토와 IEEE Std. 1012 요건에 따라 소프트웨어 요구 사항에 대한 시스템 요구 사항을 양방향으로 추적하는 추적성 분석과 페이건 인스팩션 그리고 정형 검증 등을 수행한다[12,13].

사이버보안 기능 적합성 시험 역시 소프트웨어 검증에서 수행하는 규제 요건에 대한 추적성 분석과 같이 양방향 추적 작업과 함께 사이버보안 기능의 적합성 시험을 위한 절차와 기준이 필요하다. 이를 통해서 사이버보안 기능에 대한 검증 및 확인 내용이 안전 등급 소프트웨어와 함께 향후 원자력 검증 활동에 필수 항목으로 포함될 필요가 있다.

### 2.2 국내 사이버보안 시험 및 검증 현황

정보보호제품은 안전성과 신뢰성 검증을 위한 평가인증 제도를 도입하여 24종의 보안 제품군에 대하여 인증 제도를 운용 중에 있다[14]. 평가 인증 제도는 정의된 제품군이 만족해야 하는 명세를 정의함으로써 모호한 요구 사항을 제거하고 시험이 가능한 수준에서 일관성 있는 시험을 지원함으로써 공공기관에 적용되는 제품에 대한 보안성을 보증하고 있다.

보안성 보증 제도를 활용하여 원자력 시설에 적용되는 제어기에 추가되는 보안 기능을 검증하기 위해서는 대상 제어기기가 평가대상 정보보호시스템으로 분류되어야 한다. 하지만 제어기 본래의 목적이 보안 기능에 해당하지 않고, 정보보호시스템 대상 제품군에도 포함되지 않아 평가를 위한 명세부터 별도 개발이 필요하다.

한국정보통신기술협회의(TTA)는 산업 제어시스템의 보안 요구 사항을 정의하기 위한 기준으로 “산업 제어시스템 보안 요구사항”을 발표하였다[15,16,17,18]. 이를 통해 현장장치, 제어, 운영 등 3계층으로 구분하고 각 보안 요구사항 정의를 위한 기준을 제시하고 있다. 본 문서는 기반 시설에 대한 환경을 우선 고려한 가이드로 보안 기능에 대한 시험을 위해 상위 수준에서 고려되어야 하는 항목을 제시하고 있다. 따라서 특정 제어기기에 적용된 보안 기능을 시험하기 위해서는 기기별, 보안 기능별 세분화된 시험기준 개발이 추가로 요구된다.

## III. 사이버보안 기능 적합성 시험방법

본 장에서는 원자력 사이버보안 기술기준 문서인 RS-015를 기준으로 연구된 사이버보안 기능 적합성 시험 방법을 설명한다.

적합성 시험방법 설명을 위해 제어기 수준의 요건 도출부터 시험사례를 개발하기 위한 절차는 그림 1과 같다. RS-015를 기준으로 제어기 수준에서 요구되는 사이버보안 요건을 분석(A) 한다. 본 연구에서는 요건 도출 분석을 위해 J.G. Song[19]이 제안한 원자력 사이버보안 요건 도출 방법을 활용하였다.

구체적으로 시험대상 기기에 대한 공격 벡터와 장치의 적용 환경을 고려하여 가능한 사이버 공격 방법을 식별하고자 하였다. 대상 기기에 접근하기 위해 발생하는 일반적인 접근 경로 및 방법을 NEI18-08의 Attack Pathway and Attack Vector Discussion에 근거하여 아래 5가지 항목으로 정의하였다[20].

(1) 주요 디지털 자산 간 직접 연결된 통신(Wired network connection) : 주요 디지털 자산 간 직접 연결된 통신은 대상 디지털 자산 사이에 정보를 송/수신하기 위해서 직접 연결된 모든 통신 환경을 고려한다. 구체적인 예로써 DNP3, RS-485 및 RS-232C 와 같은 제어 기기 간의 통신 프로토

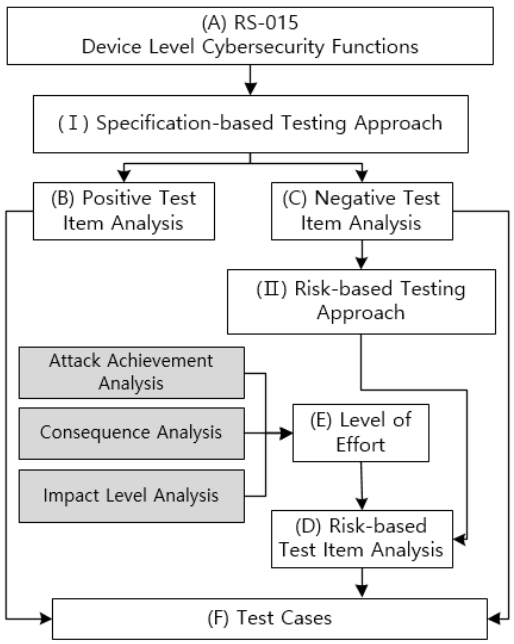


Fig. 1. Development procedure for cyber security function test cases

콜을 이용한 접근 가능 여부를 분석한다.

(2) 무선통신을 이용한 접근 가능성 (Wireless network connection) : 주요 디지털 자산이 무선 통신을 지원하는 물리적 모듈을 포함한 경우 이를 통한 접근 가능 여부를 분석한다.

(3) 접근 가능한 매체 및 미디어 (Portable Media and Mobile Devices (PMMD) connection) : 주요 디지털 자산의 개발, 설치 및 유지 보수 시 사용하는 USB, CD 등의 매체와 오실로스코프, 노트북 등의 엔지니어링 장치 등을 이용한 접근 가능 여부를 분석한다.

(4) 공급망 (Supply chain access) : 설계, 개발, 납품, 설치, 운영 단계에서의 발생하는 프로그램 개발 및 수정, 펌웨어 업데이트, 하드웨어 추가 등을 통한 접근 가능 여부를 분석한다.

(5) 물리적 직접 접근 (Physical access) : 내/외부 사용자가 직접 대상 장치에 접근하는 것으로 내부자 위협 또는 비 인가된 사용자의 직접 접근 가능 여부를 분석한다.

그림 2는 자산 간 연결 가능한 유/무선 통신, 매체 및 미디어, 공급망 그리고 물리적 직접 접근이 가능한 사용자에 대한 5가지 공격 벡터가 주요 디지털 자산에 어떻게 연관되는지를 보여준다.

이와 더불어 대상 제어기의 적용 환경을 고려한다. 원전 디지털 제어기의 필수 요구 기능과 대안적 보안 통제 적용 가능 여부를 확인하기 위해 아래 4가지 항목을 추가 고려함으로써 제어기 자체의 보안 기능의 중요성을 분석한다.

(1) 자산의 물리적 방호 현황

(2) 공극(Air gap)을 포함하여 독립된 시스템 간의 정보가 연계되는 구간 확인 (유지 보수 정보, 운영 관리 정보 등 매체를 통한 정보의 이동)

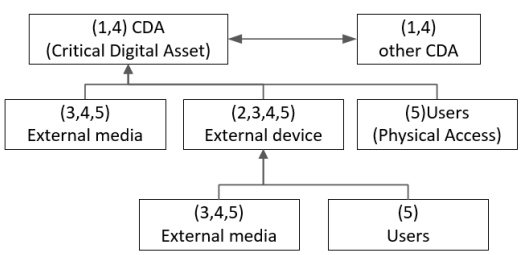


Fig. 2. Elements of Attack Vectors to a Target Critical Digital Asset(CDA)

(3) 미디어, 유지 보수 장치 관리 현황

(4) 자산에 대한 유지 보수 정책 (자산에 유지되는 보안 기준, 현 상태 이외의 통신 연결 및 다른 데이터의 입출력 불가, 자산의 형상변경 불가 등)

RS-015에서는 기술적, 운영적, 관리적 보안조치에 대해 접근제어, 감사 및 책임, 시스템 및 통신의 보호 등 총 13개의 주요 사이버보안 항목으로 구분하고, 이 사이버보안 항목들에 대해 세부항목 101개의 요건을 제시하고 있다. 원전 디지털 제어기의 사이버보안 기능 적합성 시험을 위하여 101개의 제시된 요건을 총 377개의 상세 요구 사항으로 분류하고, 각각의 상세 요구 사항에 대해 제어기에서 기능적으로 구현이 필요한지 정성적 평가를 수행한다. 구현이 필요한 것으로 식별된 요구 사항에 대해서는 적합성 시험 방법으로 Specification-based Testing Approach(Ⅰ) 및 Risk-based Testing Approach(Ⅱ)를 적용하여 구체적인 시험 항목을 도출한다. Specification-based Testing Approach(Ⅰ)은 사이버보안 요건 및 설계 사양서를 기준으로 명시된 보안 기능이 정상적이고 신뢰적으로 작동하는지에 대한 시험항목을 식별한다. Specification-based Testing Approach는 Positive 시험항목 분석(B)과 Negative 시험항목 분석(C)으로 구분된다. Positive 시험항목 분석을 통해서는 대상 장비의 보안 기능이 보안 요건에 부합하도록 구현되어 있는지 정상적인 정보를 입력하여 정상적인 결과가 나오는지 시험하는 Positive 요건 시험항목을 도출한다. Negative 시험항목 분석을 통해서는 보안 요건에 대한 Negative 요건을 설정하고 대상 시스템에 정상적이지 않은 정보의 입력 또는 비정상적인 조작을 통한 보안 기능의 안전성과 신뢰성을 시험하는 Negative 요건 시험항목을 도출한다. 다음으로 이렇게 도출된 Positive 및 Negative 요건 시험항목에 대해 Positive 및 Negative 요건에 대한 시험사례(F)를 생산한다. Risk-based Testing Approach(Ⅱ)은 일반적으로 취약성 점검 시험, 침투 시험, Fuzzing 시험 등을 포함한다. Risk-based Testing Approach(Ⅱ)를 통한 시험항목 도출을 위해 Negative Test 시험항목 분석(C) 결과를 기반으로 Risk-based 시험항목 분석(D)을 수행한다. Negative 요건 시험항목에 대하여 공격자가 공격 대상에 대해 취득할 수

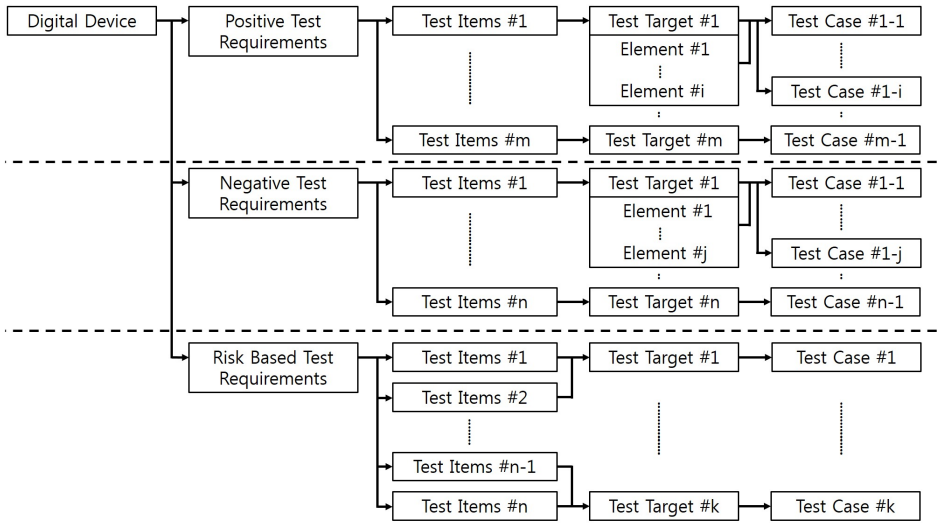


Fig. 3. Test case relationship between test targets, items, and requirements

있는 공격 효과를 식별하고(Attack Achievement Analysis), 사이버 공격으로 인해 기기에 초래되는 결과를 예상하여(Consequence Analysis) 기기에 초래되는 결과가 궁극적으로 발전소에 파급되는 영향의 수준을 분석한다(Impact level Analysis). 시험항목에 대한 시험의 난이도(E)는 시험자의 역량에 따라 정량적 평가가 어려운 한계로 시험 시 요구되는 예상 시간을 산정함으로써 시험의 난이도를 반영한다. 본 연구에서는 표 1과 같이 NESCOR의 Guide to Penetration Testing for Electric Utilities Version 3에서 정의한 시험 난이도 산정 기준 시간을 활용하였다.

이러한 Risk-based 시험항목 분석(D) 결과와 시험의 난이도(E) 분석을 근거로 중요도가 높은 시험항목들에 따라 난이도가 상대적으로 낮은 시험 방법을 우선 채택하여 Risk-based 요건에 대한 시험사례(F)를 개발한다. 최종적으로 도출되는 시험항목, 시험대상, 시험사례의 관계는 그림 3과 같다.

적합성 시험방법에 대한 요건도출 및 시험사례 개발 절차에 따라 Specification-based Testing Approach(Ⅰ)를 통해 m 개의 Positive 시험항목과 n 개의 Negative 시험항목이 식별된다. 또한 식별된 각각의 시험항목에 따라 별도의 시험사례가 개발 된다. 반면 Risk-based Testing Approach (Ⅱ)를 통해 개발되는 Risk-based 시험항목은 Negative 시험항목과 같지만 모든 시험항목이 각각의 시험대상 및 시험사례를 갖지는 않는다. 이는 권한 관리, 암호화, 계정 정보 보호 등의 여러 시험항목이 계정에 대한 취약성 시험 하나의 사례로 평가될 수 있기 때문이며, 시험사례를 구성하는 공격 시나리오와 평가자의 역량에 따라 차이가 발생할 수 있다.

Table 1. An estimated level of effort [21]

| Level of Effort | Number of Hours |
|---|---|
| Low | 1-4 |
| Medium | 5-16 |
| High | 17-40 |
| Extremely High | 41+ |

## Ⅳ. 사이버보안 기능 적합성 시험방법 분석 사례

본 장에서는 제안된 사이버보안 기능 적합성 시험방법에 따라 도출된 시험사례를 설명한다. 원자력 시설에 보안 위협이 될 수 있는 내용을 제외하고 일반화한 시험항목을 PLC를 기준으로 분석한 사례를 설명한다.

### 4.1 Positive 시험사례 도출

Positive 시험은 보안 요건에 따라 개발된 기능에 대한 정상작동을 확인하는 시험으로 보안 기능에서 의도한 범위 안의 정보를 입력한 결과를 확인하는 시험이다. 표 2는 RS-015의 계정관리 요건 중 "주어진 업무를 수행하는 데 필요한 만큼의 제한된 접근

Table 2. Example of positive test target for PLC security function

| Test Item Code | Test Targets |
|---|---|
| AC-00-01 | 1. Engineering tool has an account management function for PLC<br>2. Login account of PLC is divided into two types (Admin, Engineer) |
| AC-00-04 | Check below functions when PLC authentication function fails<br>1. Communication status is not available within (one) minute after (three) times of PLC authentication failure.<br>2. If PLC authentication fails (three) times in engineering workstation with engineer authority, communication is not possible within the (one) minute. |

제한을 각 계정에 부여" 항목에 대해 시험이 필요한 대상 장치인 PLC와 엔지니어링 도구에 요구되는 시험대상을 정의한 예로 계정 기능 유/무, 사용자 계통의 권한 분리 기능, 제어기의 무차별 인증 시도 대응 기능 등을 시험대상으로 선정하고 있음을 보여준다. 표 3은 표 2의 AC-00-01 시험항목 코드를 기준으로 요구되는 시험사례를 정의한 내용으로 관리자의 인증정보, 권한 등을 통해 확인되어야 하는 결과를 각각 입력 정보와 예상 결과를 정의하고 실제 시험을 통해 도출된 결과와 예상되는 결과의 비교를 통해 시험 결과의 성공/실패 여부를 판단할 수 있도록 정의된 템플릿을 보여준다.

### 4.2 Negative 시험사례 도출

Negative 시험은 Positive 시험의 연장선으로 Positive 시험에서 의도한 정보를 벗어난 값을 입력함으로써 개발한 보안 기능의 작동 상태를 확인하는 시험이다. 예를 들어 기기의 요건이 0~10의 정수 값을 넣어 동작을 수행한다면 Positive 시험의 입력 정보는 0에서 10 사이의 정수 값을 입력하는 시험을 수행하는 것이며, Negative 시험은 0에서 10 사이의 정수 외의 정보(예를 들어 음수 값, 혹은 소수 값 등)를 입력하여 시험을 수행한다. 따라서 Positive 시험과 동일한 항목을 기준으로 의도한 정보를 벗어난 값을 입력 정보로 정의하여 시험사례 만든다.

표 4는 비인가된 사용자의 정보를 입력하거나, 권한이 없는 사용자의 접근으로 허가되지 않은 기능의 접근 가능성을 확인하기 위해 정의된 Negative 시험사례로 정의된 예를 보여준다.

### 4.3 Risk-based 시험사례 도출

Risk-based 시험은 개발된 보안 기능에 대한 잠재적 위험을 확인하기 위한 시험으로 침투시험 등을 통해 보안 기능의 유효성을 확인하는 시험이다. 다른 시험과 달리 Risk-based 시험은 투입되는 인력과 자원에 따라 무수한 시험이 가능하다는 특징이 있다. 이에 시험 범위 및 우선순위를 선정하기 위한 분석이 요구된다. 대상 제어기와 적용되는 보안 기능의 우선순위를 선정하기 위해서 다음 3단계의 분석 절차를 수행한다.

1) 공격 취득 대상 분석 : 공격 시나리오에 따라 공격자가 확보할 수 있는 자원, 행위 등을 정성적으로 분석한다. 공격자가 취득할 수 있는 대상은 "엔지니어링 도구 사용 권한 획득", "계정 DB 작동 불

Table 3. Example of positive test case for PLC security function

| Test case No. | Accounting Separation | | | Pass/Fail |
|---|---|---|---|---|
| | Input | Expected Results | Test Result | |
| 01 | 1. ID and password of administrator account<br>2. Run account management | Confirm that run account management functions | | (O/X) |
| 02 | Check permissions by administration and engineering account | Confirm that the login account privilege is divided several types (e.g., Admin, Engineer) | | (O/X) |

Table 4. Example of negative test case for PLC security function

| Test case No. | Accounting Separation | | | Pass/Fail |
|---|---|---|---|---|
| | Input | Expected Results | Test Result | |
| 01 | 1. Undefined ID and password / ID and password of Engineer account<br>2. Run account management | Confirm that can not access account management functions | | (O/X) |
| 02 | ID and password of Administrator account | Administrator account does not run the engineering software. It can be run only in an engineering account | | (O/X) |

능, 또는 인증 오류 유발", "제어기 내의 정보 삭제", "통신 패킷 변조" 등과 같은 수준의 결과로 도출하게 된다.

2) 영향성 분석 : 영향성 분석은 기기 가용성, 무결성, 기밀성 분석을 통해 보안 기능이 정상 작동하지 않을 때 기기 수준에서부터 계통, 발전소 수준에 미치게 되는 영향을 분석하게 된다.

표 5는 원자력 복수 계통(Condenser System)에 적용되는 PLC를 대상으로 영향성 분석을 수행한 예를 보여준다. 분석 대상이 되는 기기에 대하여 기기의 기능 및 역할을 정의(Step 1) 하고, 이에 대한 가용성, 무결성, 기밀성 측면에서의 보안 기능 분석을 수행(Step 2) 하여, 분석된 결과에서의 사이버 공격이 발생했을 시 계통 수준에서 미치는 영향 및 발전소 수준에서 미치는 영향(Step 3)을 분석한 결과를 보여준다.

3) 시험 중요도 식별 : 원자력 발전소는 안전계통이 발전소 운영과 별도로 이상상태 발생 시 자동 발전소 정지로 유도하도록 설계되어 있다. 따라서 본 연구에서는 사이버 공격으로 인한 정보 유출, 기능 상실 보다 조작된 정보를 제공하여 이상 상태로 유도하는 경우를 가장 위험한 상황으로 고려한다.

중요도 식별은 공격자가 취득 대상 분석의 결과와 영향성 분석 결과를 취합하고 최종 제어신호 변조 공격과 관련된 보안 기능 여부를 최종 검토하여 시험의 중요도를 그림 4와 같이 높음/중간/낮음으로 구분한다.

Table 5. Example of consequence analysis for digital device

| Consequence Analysis for A Digital Devices | | | | |
|---|---|---|---|---|
| Digital Assets | Step 1 | Step 2 | Step 3 | |
| | Type of Interaction | Digital Compromise | Potential Consequence to Critical System | Consequence to Plant |
| PLC | Controls parameter: Control equipment function based on an internal algorithm for the condenser system | Confidentiality: Digital information could be intercepted and read | None.<br>No system is impacted. Information for the condenser system could be read | No safety, security, emergency preparedness or continuity of power consequences |
| | | Integrity: Digital signals or set-points could be corrupted so that operation of equipment function is not executed | Failed.<br>Loss of control function is failure of Condenser Physical System function (Ex: Water level in condenser system) | Moderate impact for continuity of power consequences |
| | | Availability: Loss of availability in multiple instrument channels could result in denial of control for equipment | Failed.<br>Loss of control function is failure of Condenser Physical System function (Ex: Water level in condenser system) | Moderate impact for continuity of power consequences |

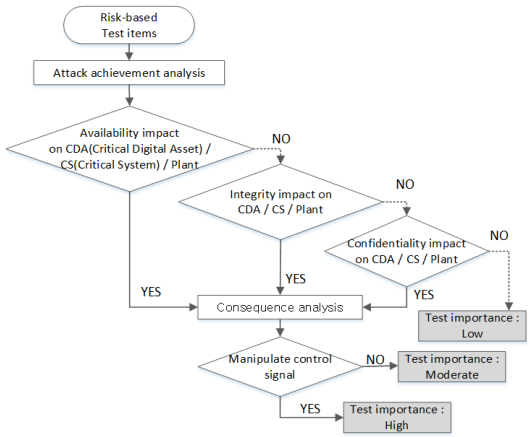


Fig. 4. Test importance level analysis procedures

표 6는 Risk-based 시험항목 중 PLC의 구성 정보를 인증 없이 변경 가능함을 시험하는 항목(AC-00-19-PT)의 예를 보여준다.

표 6의 해당 항목은 계정관리 항목으로 취약할 경우 제어기기의 가용성, 무결성, 비밀성 모두에 영향을 미치게 되며, 제어신호 변조가 가능한 상태까지 연관된다. 따라서 해당 시험항목의 중요도는 "높음"으로 분류된다. 시험의 난이도는 직접 제어기로의 접근하기 위한 임베디드 보드 접근 시도, 엔지니어링 도구를 통한 접근 시 요구되는 응용프로그램, 암호화, 제어기의 운영체제 분석 등이 요구된다. 이에 정성적 분석을 통해 최소 소요시간이 17-40 시간으로 "높음"으로 산정하였다.

표 7은 평가항목에 대한 평가대상으로 정의한 항목의 예로 제어기의 설정 정보를 포함하는 파일의 암호화 우회 시도, 제어기의 엔지니어링 도구의 인증 및 제어기 접근 시 인증 우회 시도, 물리적 접근을 통한 설정 정보 추출 및 분석 등을 포함한다.

표 8은 표 7의 AC-00-19-PT 시험대상에서 정의된 설정 정보 암호화 및 변조에 관련된 시험사례로 계정 관련 데이터 파일의 위치 파악 및 해당 파일 암호화 여부, 비인가된 사용자가 악의적 파일 접근 및 변경 여부에 대해 확인해야 하는 항목을 입력 정보로 정의하고 검사 결과 성공/실패를 판단하기 위해 정의한 예상 결과 항목을 보여준다.

Table 6. Example of risk-based test item for PLC security function

| Test Item Code | Test Item |
|---|---|
| AC-00-19-PT | Confirm that PLC configuration change is impossible without authentication |

Table 7. Example of risk-based test target for PLC security function

| Test Item Code | Test Target |
|---|---|
| AC-00-19-PT | 1. Configuration file encryption and changeability test<br>2. Authentication bypass of engineering workstation + Attempt to access and change control device configuration information<br>3. Hardware hacking using physical I/O interface |

## 4.4 시험사례 활용 결과 분석

본 논문에서 제안한 디지털 제어기의 사이버보안 기능 적합성 시험방법을 원전 주요 제어기기인 PLC

Table 8. Example of risk-based test case for PLC security function

| Test Case No. | Input | Expected Results | Test Result | Pass/Fail |
|---|---|---|---|---|
| 01 | Identify account-related data files in the engineering software installation folder | Unable to identify the account-related data file | | (O/X) |
| 02 | Unauthorized access to account-related data files | Unable to access account-related data files without authentication | | (O/X) |
| 03 | Confirm that authentication information protection | Authentication information encryption | | (O/X) |

평가에 활용한 결과 제어기기의 특성에 따라 국내 사이버보안 기술기준 RS-015에서 요구하는 보안 기능 항목을 파악할 수 있었다.

시험사례 도출을 위해서는 기기 제작사와의 협력이 필수적으로 요구되며, 제작사의 개발 자료에 근거한 시험대상 식별 및 사례 도출의 중요성을 확인할 수 있었다.

상세 시험사례 정의를 통해 Positive, Negative 시험의 경우 평가자의 역량과 관계없이 일관된 평가가 가능하였으며, 개발된 보안 기능에 연관된 기술기준 항목 준수 여부를 쉽게 판단할 수 있었다. 결과적으로 사이버보안 규제 요건에 대한 추적성 분석과 함께 적합성 시험 절차와 기준으로 활용 가능함을 확인하였다.

Risk-based 시험은 원자력 발전소 계통, 사이버보안, 제어기기 개발자 등 전문가 그룹 협의에 근거하여 중요도, 시험의 난이도 분석을 통해 요구되는 필수 시험항목, 시험대상, 시험사례 정의가 가능하였다. 다만 시험사례 평가 시 평가자의 역량에 따라 일관된 시험 결과가 도출되지 않는다는 한계가 있음을 확인하였다.

본 연구는 원자력발전소의 계측제어시스템의 핵심이 되는 주요 디지털 제어기기인 PLC를 대상으로 수행된 연구로 발전소에 도입된 서버 등과 같은 IT 장비의 보안 기능 적합성 평가를 위해 기존 IT 사이버보안 검증기술을 활용한 시험사례 개발이 추가로 요구된다.

## V. 결 론

원자력 시설에 대한 사이버보안 규제 이슈와 다양한 디지털 제어기의 적용에 따라 사이버보안 기능을 제어기 수준에서 적용하기 위한 노력이 진행 중이다. 이에 추가되는 보안 기능 적합성 확인을 위한 시험 방법이 요구되고 있다.

이에 본 연구에서는 원자력 시설에 적용되는 디지털 제어기를 대상으로 국내 사이버보안 기술기준에 따라 보안 기능의 적합성 시험방법을 제안함으로써 원자력 시설에 사용되는 기기에 반영된 사이버보안 기능 검증시험의 기반을 마련하고자 하였다.

원자력 시설에 적용되는 수많은 디지털 제어기에 대해 일관성 있는 평가 기준을 마련하기 위해 본 연구에서 제안하는 시험방법을 이용하여 다양한 디지털 제어기의 시험사례를 지속해서 개발할 예정이다.

## References


[1] Schneider-electric, "NERC CIP compliance for the power generation industry, Developing a comprehensive program to comply with NERC CIP cyber security requirements," https://www.schneider-electric.com/en/download/document/PAS_63680_CPM16120/ (accessed Aug. 2019).

[2] ISA Security, "Schneider Electric achieves industry-first ISA Secure® Level Two Security Development Life cycle Assurance certification," https://www.isasecure.org/en-US/News-Events/Schneider-Electric-achieves-industry-first-ISASecu (accessed Aug. 2019).

[3] SANS, "Waterfall for NRC Compliance with regard to NIST 800.53 and 800.82: Using Waterfall's Unidirectional Security Solution to Achieve True Security & NRC Compliance Ver. 1.4," https://www.sans.org/cyber-security-summit/archives/file/summit_archive_1493758233.pdf (accessed Aug. 2019).

[4] SIEMENS, "Security with SIMATIC-S7 controllers," https://support.industry.siemens.com/cs/document/77431846/security-with-simatic-s7-controllers?dti=0&lc=en-WW (accessed Aug. 2019).

[5] LogRhythm, "LogRhythm Support for NRC RG. 5.71," White paper - Compliance Support for NRC RG 5.71. LogRhythm Inc. Jul. 2014.

[6] Regulatory Standard 015, "Regulatory standard on computer security of nuclear facilities," KINAC, Oct. 2014.

[7] Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities," U.S. Nuclear Regulatory Commission, Jan. 2010.

[8] NIST SP800-53A Revision 1, "Guide for assessing the security controls in federal information systems," National

Institute of Standards and Technology, Jun. 2010.
[9] IAEA Nuclear Security Series No.17, "Computer security at nuclear Facilities," International Atomic Energy Agency, Dec. 2011.
[10] NEI 13-10 Revision 5, "Cyber Security Control Assessments," Nuclear Energy Institute, Feb. 2017.
[11] NEI 08-09 Revision 6, "Cyber Security Plan for Nuclear Power Reactors," Nuclear Energy Institute, Apr. 2010.
[12] IEEE Standard 1012-2016, "IEEE Standard for System, Software, and Hardware Verification and Validation," Institute of Electrical and Electronics Engineers, Sep. 2017.
[13] K. C. Kwon, J. S. Lee, and E. Jee, "Application and Analysis of the Paradigm of Software Safety Assurance for a Digital Reactor Protection System in Nuclear Power Plants," KIISE Transactions on Computing Practices, vol. 23, pp. 335-342, Jun. 2017.
[14] ITSCC, "Korea IT Security Evaluation and Certification Scheme," https://itscc.kr/svc/svc/openPage.do?pageId=010200 (accessed Aug. 2019).
[15] TTA.KO-12.0307-part1, "Security Requirements for Industrial Control System - Part 1: Concepts and Reference Model," Telecommunications Technology Association, Jun. 2017.
[16] TTA.KO-12.0307-part2, "Security Requirements for Industrial Control System - Part 2: Field Device Layer," Telecommunications Technology Association, Jun. 2017.
[17] TTA.KO-12.0307-part3, "Security Requirements for Industrial Control System - Part 3: Control Layer," Telecommunications Technology Association, Jun. 2017.
[18] TTA.KO-12.0307-part4, "Security Requirements for Industrial Control System - Part 4: Operation Layer," Telecommunications Technology Association, Jun. 2017.
[19] 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 System in Nuclear Power Plants," Nuclear Engineering and Technology, vol. 45, pp. 637-652, Oct. 2013.
[20] NEI 18-08, "Portable Media Scanning Stations / Kiosk cyber Security Controls Evaluation Template," Nuclear Energy Institute, Aug. 2018.
[21] J. Searle, G. Rasche, A. Wright, S. Dinnage, "Guide to Penetration Testing for Electric Utilities Revision 3," National Electric Sector Cybersecurity Organization Resource, 2016.

## 〈저자소개〉

송 재 구 (Jae-gu Song) 정회원
2006년 2월: 한남대학교 멀티미디어학과 졸업
2008년 2월: 한남대학교 멀티미디어학과 석사
2011년 8월: 한남대학교 멀티미디어학과 박사
2013년 3월~현재: 한국원자력연구원 선임연구원
〈관심분야〉 사이버보안, 원자력 계측제어

신 진 수 (Jin-soo Shin) 정회원
2012년 2월: 경희대학교 원자력공학과 졸업
2013년 8월: 경희대학교 원자력공학과 석사
2017년 8월: 경희대학교 원자력공학과 박사
2018년 9월~현재: 한국원자력연구원 박사후연구생
〈관심분야〉 정보보호, 사이버보안, 원자력공학

이 정 운 (Jung-woon Lee) 정회원
1979년 2월: 한양대학교 기계공학과 졸업
1981년 2월: 한국과학기술원 기계공학과 석사
1990년 5월: University of Iowa Biomedical Engineering 박사
1990년 11월~현재: 한국원자력연구원 책임연구원
〈관심분야〉 산업제어시스템 사이버보안

이 철 권 (Cheol-kwon Lee) 정회원
1980년 2월: 경북대학교 전자공학과 졸업
1985년 2월: 동아대학교 전자공학과 석사
2006년 8월: 충남대학교 전자공학과 박사
1985년 3월~현재: 한국원자력연구원 책임연구원
〈관심분야〉 원자력 계측제어, 원자력 사이버보안

최 종 균 (Jong-gyun Choi) 정회원
1994년 2월: 한양대학교 원자력공학과 졸업
1996년 2월: 한국과학기술원 원자력공학과 석사
2001년 8월: 한국과학기술원 원자력공학과 박사
2001년 9월~현재: 한국원자력연구원 책임연구원
〈관심분야〉 원자력공학, 안전성평가, 원자력사이버보안