디지털산업정보학회 논문지 제16권 제1호-2020년 3월
http://dx.doi.org/10.17662/ksdim.2020.16.1.099

원전 안전계통의 사이버보안 위협 및 대응

정 성 민*

Cybersecurity Threats and Responses of Safety Systems in NPPs

Jung Sungmin

〈Abstract〉

In the past, conservative concepts have been applied in terms of the characteristic of nuclear power plants(NPPs), resulting in analog-based equipment and closed networks. However, as digital technology has recently been applied to the design, digital-based facilities and communication networks have been used in nuclear power plants, increasing the risk of cybersecurity than using analog-based facilities. Nuclear power plant facilities are divided into a safety system and a non-safety system. It is essential to identify the difference and cope with cybersecurity threats to the safety system according to its characteristics. In this paper, we examine the cybersecurity regulatory guidelines for safety systems in nuclear power plant facilities. Also, we analyze cybersecurity threats to a programmable logic controller of the safety system and suggest cybersecurity requirements be applied to it to respond to the threats. By implementing security functions suitable for the programmable logic controller according to the suggested cybersecurity requirements, regulatory guidelines can be satisfied, and security functions can be extended according to other system requirements. Also, it can effectively cope with cybersecurity attacks that may occur during the operation of nuclear power plants.

Key Words : Cybersecurity Requirement, Regulatory Guide, Programmable Logic Controller

Ⅰ. 서론

원자력 발전소는 우라늄의 핵분열 때 나오는 에너지를 이용하여 증기를 생산하고, 이 증기의 힘으로 터빈을 돌려서 전기 에너지를 만든다. 원자력 발전소를 구성하는 다양한 시스템 중에서 계측제어시스템은 인간의 신경망과 같은 역할을 하며 발전소의 설비들이 안전하게 운영될 수 있도록 계측, 감시, 제어, 보호의 기능을 수행한다. 계측제어시스템은 시스템의 기능과 규제 등급에 따라 안전계통과 비안전계통으로 나뉜다[1, 2]. 안전계통은 원자력 발전소의 안전을 보장하기 위해 계통의 중요도에 따른 등급을 바탕으로 설계되고 제작되어야 한다.

일반적으로 계측제어시스템은 아날로그 기반 설비와 폐쇄적인 통신망을 사용했기 때문에 최소한의 보

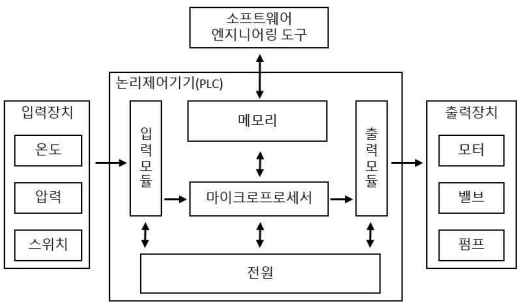
* 한국원자력연구원 선임연구원

안 요구사항을 만족할 수 있었고, 사이버보안 위협도 크지 않았다. 이후 디지털 기술이 발전하고 아날로그 장비의 노후화, 부품 단종에 따른 유지보수의 어려움 등의 문제에 따라 디지털 기반의 설비와 통신망의 사용이 원자력 발전소의 계측제어시스템에 점차 확대되었다. 이것은 계측제어시스템의 운영에 대한 효율성을 높일 수 있었지만, 기존 아날로그 기반의 설비에 비해 사이버보안 위협이 증가하게 되었다[2, 3]. 원자력 시설에서의 사이버보안 위협은 정보시스템의 사이버보안 위협과는 구분되어야 하고 효율적으로 보안 위협에 대응하기 위해 계측제어시스템에 대한 이해를 바탕으로 시스템의 개발 및 설계 단계부터 설비에 필요한 보안 요건을 도출해야 한다[4, 5].

본 논문에서는 원자력 시설을 위한 규제지침과 사이버보안 위협을 살펴보고 계측제어시스템을 구성하는 설비인 안전등급 논리제어기기를 위한 사이버보안 요건을 제시한다. 2장에서 규제 지침에서 정의하고 있는 필수디지털자산에 해당하는 안전등급 논리제어기기를 알아보고 원자력 시설을 위한 규제 지침인 RG 5.71과 RS-015를 살펴본다. 3장에서는 사이버보안 요건을 도출하기 위해 고려되어야 할 사항, 논리제어기기의 사이버보안 위협, 그리고 적용이 제외되어야 하는 보안 조치에 대해 알아본다. 4장에서는 보안 조치를 만족하기 위해 위협과 제외 사항을 바탕으로 논리제어기기에 적용되어야 하는 보안 요건을 도출한다.

Ⅱ. 원전 사이버보안 규제 지침

원자력 발전소는 계측, 감시, 제어, 보호 기능과 관련하여 다양한 계통으로 이루어져 있다[6]. 계측계통은 압력, 온도, 수위, 방사능 등과 같은 원자력 발전소의 상태 정보를 현장에 설치된 센서를 통해 수집하고, 감시계통은 운전원이 상태 정보를 실시간으로 확인할 수 있도록 주제어실의 다양한 설비를 통해 수집된 정보를 제공한다. 제어계통은 계측 및 감시계통을 통해 수집된 상태 정보를 바탕으로 원자력 발전소를 안전하게 운전할 수 있도록 각종 설비를 제어한다. 마지막으로 보호 계통은 발전소의 안전과 관련된 변수들을 지속해서 감시하고, 변수가 정해진 안전 운전 범위를 벗어나면 원자로를 정지시키거나 공학적안전설비작동 신호를 발생시킨다[7].



<그림 1> 논리제어기기 하드웨어 구조도

원자력 발전소의 보호계통은 현장에서 계측된 정보를 수집하고 제어로직의 결과에 따라 발전소 설비를 제어하기 위해 안전등급의 논리제어기기 (PLC, Programmable Logic Controller)를 사용한다[8, 9]. 논리제어기기는 원자력 발전소와 같은 가혹한 환경을 견딜 수 있도록 만든 소규모 컴퓨터이다. 소프트웨어 엔지니어링 도구를 이용하여 논리제어기기의 제어로직을 작성하고 논리제어기기에 다운로드한다. <그림 1>은 논리제어기기의 하드웨어 구조를 나타내며 논리제어기기는 마이크로프로세서, 메모리, 입출력 모듈, 그리고 전원으로 구성되어 있다.

계측제어시스템에 논리제어기기와 같은 디지털 기반의 설비와 관련 통신망이 사용되면서 사이버보안의 위협이 증가하였고 이에 규제 기관에서 원자력 시설에 대해 사이버보안 규제 지침의 적용을 요구하고 있다. 하지만 기존에는 사이버보안에 대한 요구가 크지 않았다. 따라서 계측제어시스템에 구현된 보안 기능은

제한적이고 규제 지침에서 제시하는 모든 보안 조치를 만족할 수 없다. 또한, 규제 지침은 많은 기술적, 운영적, 관리적 보안 조치 세부항목을 제시하는데, 정보시스템 관점에서 고려되어야 할 사항과 발전소의 운영환경에서 고려되어야 하는 사항까지 다루고 있으므로 규제 지침을 그대로 계측제어시스템에 적용하는 것은 어려움이 있다. 따라서 계측제어시스템이 보안 조치를 만족할 수 있는 보안 기능을 구현하기 위해서 계측제어시스템을 개발 및 설계하는 단계부터 필요한 보안 요건을 고려해야 한다. 이를 위해 사이버보안 관련 규제 지침을 살펴보고 계측제어시스템의 구성 설비인 논리제어기기의 사이버보안 위협을 논의한다.

<표 1> RG 5.71 항목 및 세부항목 개수[8, 11]

분류	항목	세부
Security Controls (Appendix B)	Access Controls	23
	Audit and Accountability	12
	CDA and Communications Protection	22
	Identification and Authentication	9
	System Hardening	5
Operational Controls (Appendix C)	Media Protection	6
	Personnel Security	2
	System and Information Integrity	11
	Maintenance	3
	Physical and Environmental Protection	9
	Defensive Strategy	-
	Defense-in-Depth	-
	Incident Response	8
	Contingency Planning	7
	Awareness and Training	10
	Configuration Management	9
Management Controls (Appendix C)	System and Service Acquisition	6
	Security Assessment and Risk Management	3
Total	18	145

미국 원자력규제위원회 (NRC)에서 발행한 RG 5.71은 미국연방법 10CFR73.54에서 설명하고 있는 원자력 시설의 사이버보안 적용과 관련한 법규에 대해 해당 내용을 구체화한 규제 지침이다[10]. RG 5.71은 원자력 발전소를 구성하는 설비 중에서 안전, 보안, 및 비상대응에 해당하는 기능을 수행하는 디지털 자산을 필수디지털자산으로 분류하고, 필수디지털자산을 위한 기술적, 운영적, 그리고 관리적 보안 조치를 제시하고 있으며, 보안 조치는 <표 1>과 같이 18개 항목 아래 145개의 세부항목으로 이루어져 있다[8, 11].

국내에서는 한국원자력통제기술원(KINAC)에서 원자력 시설에 대한 사이버보안 업무를 담당한다. 한국원자력통제기술원은 원자력 시설 중에서 사이버보안이 적용되어야 할 디지털 자산 식별을 위해 RS-019를 발행하고, 사이버보안 규제 지침으로써 RS-015를 발행하였다. RS-015는 국내 원자력방호방재법령과 관련 고시, 그리고 국제기구의 여러 규제 지침을 바탕으로 원자력 시설이 이행해야 할 보안 조치를 정리하였다[12, 13]. RS-015는 RG 5.71과 같이 기술적, 운영적, 그리고 관리적 보안 조치를 부록으로 기술하고 있으며, 총 13개 항목 아래 101개의 세부항목으로 구성되어 있다[14]. RS-015는 RG 5.71에 제시하고 있는 보안 조치의 항목은 대부분 다루고 있지만, 저장매체 보호, 방어전략, 심층방호, 사고대응, 그리고 비상계획에 대한 항목은 부록에서 다루지 않는다. 다음 장에서는 안전등급의 논리제어기기에 대한 사이버보안 고려사항과 사이버보안 위협, 그리고 보안 조치 중에서 논리제어기기에서는 고려하지 않아도 되는 보안 조치를 살펴본다.

Ⅲ. 논리제어기기의 사이버보안 위협

3.1 사이버보안 요건 도출시 고려사항

원자력 발전소의 계측제어시스템에서 논리제어기기 및 소프트웨어 엔지니어링 도구와 같은 디지털 기

반의 기기와 통신망이 사용되기 때문에 사이버보안 위협에 효율적으로 대응해야 한다. 계측제어시스템을 위한 사이버보안 요건을 도출하기 위해서는 다음과 같은 사항을 고려해야 한다[13, 15, 16].

첫째, 기존의 규제 지침을 분석하여 계측제어시스템의 설계 단계에서부터 적용할 수 있도록 필수적인 보안 요건을 도출해야 한다. 미국 원자력규제위원회(NRC)의 RG 5.71와 한국원자력통제기술원(KINAC)의 RS-015의 규제 지침은 대부분 상위 수준의 내용을 다루고 있기 때문에 계측제어시스템에 그대로 적용하기 어렵다. 또한, 계측제어시스템은 안전계통과 비안전계통으로 구분되고 계통 간의 연계가 복잡하므로 사이버보안 대응을 위해서 계통 등급과 연계 등을 분석하여 실제 기술적으로 적용이 가능한 보안 요건이 도출되어야 한다.

둘째, 정보시스템과 계측제어시스템의 보안의 목적의 차이를 바탕으로 적절한 보안 요건을 도출해야 한다. 정보시스템은 기밀성과 무결성을 우선 고려해야 하지만 계측제어시스템은 안전성과 가용성이 우선 고려된다. 기밀성과 무결성을 보장하기 위해 계측제어시스템에 암호화를 적용하는 경우에 암호화 처리를 위해 발생하는 부하 때문에 응답시간이나 신뢰도에 영향을 준다면 암호화는 사용되어서는 안 된다. 논리제어기기와 소프트웨어 엔지니어링 도구의 특징을 고려하고 안전성과 가용성이 우선되는 보안 요건이 필요하다.

셋째, 기존의 정보시스템의 사이버보안 위협을 분석하여 계측제어시스템을 위한 사이버보안 요건을 도출해야 한다. 정보시스템에서 사이버보안 위협이 되는 버퍼오버플로우, 경계검사 취약, 명령어 삽입 공격, 널 포인트 사용, 접근제어 미흡, 권한 상승 문제, 인증 우회, 중간자 공격, 인증 정보 노출, 하드 코딩, 잘못된 네트워크 형상이나 보안 장비의 우회 같은 취약점이 계측제어시스템에도 보안 위협이 될 수 있다.

3.2 논리제어기기의 사이버보안 위협

계측제어시스템의 구성 설비인 안전등급 논리제어기기를 위한 사이버보안 요건을 도출하기 위해 논리제어기기에 대한 주요 사이버보안 위협을 정리한다.

3.2.1 인증 및 접근제어

논리제어기기는 사용자가 작업을 위해 소프트웨어 엔지니어링 도구를 통해 접근하거나 다른 장치들이 연결될 수 있다. 사용자나 다른 장치의 인증 우회나 인증 부재는 사이버보안 취약점이므로 논리제어기기에서 인증 우회나 인증 부재를 방지해야 한다. 그리고 접근제어를 위해 논리제어기기에 사용자나 기기별로 접근 권한이 설정되어야 하고 각각의 권한이 남용되지 않도록 해야 한다.

3.2.2 로깅

보안 사고에 적절한 대응을 할 수 있도록 사용자의 접근, 논리제어기기 내의 제어로직의 생성, 변경 및 삭제, 네트워크 구성 변경 등과 같이 논리제어기기의 상태에 대한 로깅 기능을 구현해야 한다. 로깅 기능의 부재는 사이버보안 공격에 대한 탐지를 늦추고, 시스템에 대한 공격을 쉽게 만든다.

3.2.3 무결성 검증

논리제어기기 내부의 제어로직 변조는 기기의 오작동을 일으킬 수 있다. 초기 제어로직의 설치 혹은 제어로직의 업그레이드 패치 등의 과정에서 소프트웨어 엔지니어링 도구를 통해 제어로직을 논리제어기기에 다운로드하는 경우 변조를 방지하기 위해 무결성을 확인할 수 있는 기능이 구현되어야 한다.

3.2.4 암호화

논리제어기기에 사용자가 로그인하는 경우나 안전계통의 제어를 위한 데이터를 송수신하는 경우에 로그인 정보 및 제어 데이터는 암호화를 사용하여 기밀성을 보장해야 한다. 암호화 기능을 사용하는 경우 기밀성을 보장할 수 없는 취약한 암호 알고리즘이나 표준이 아닌 암호화 알고리즘은 금지해야 한다. 특히, 안전계통에서 암호화를 통해 기기 간의 기밀성을 유지하는 것이 필요한 경우 가용성을 위배하지 않도록 성능에 대한 영향성 평가가 이루어져야 한다.

3.2.5 프로그램 형상

논리제어기기에 접근이 가능한 소프트웨어 엔지니어링 도구에서 실행되는 프로그램의 불필요한 초기 서비스는 실행을 막고, 보안 설정을 확인하여 필요하지 않은 네트워크 통신 포트는 비활성화한다. 논리제어기기에서 기본적인 설정 변경을 확인할 수 있어야 한다.

3.2.6 저장매체 관리

논리제어기기 및 소프트웨어 엔지니어링 도구에는 이동식 저장매체를 연결할 수 있는 포트가 제공될 수 있다. 이동식 저장매체가 계측제어시스템에 연결되는 경우 정상적으로 허가된 저장매체인지 확인하는 기능과 적절한 접근제어를 통해 불필요한 권한에 따른 사용을 방지할 수 있어야 한다.

3.2.7 입력값 검증 미흡

원자력 발전소를 안전하게 제어하기 위해서 현장의 계측 정보나 사용자의 설정치 등의 다양한 데이터가 논리제어기기로 입력된다. 이때 입력되는 데이터의 경계검사가 미흡하면 버퍼오버플로우 등의 취약점이 발생할 수 있다. 그리고 공격자가 논리제어기기 운영체제의 명령어에 악의적인 코드나 명령어를 삽입하는 명령어 공격을 통해 사용자가 의도하지 않은 작업을 실행시킬 수 있다.

3.2.8 네트워크 설계

안전계통 네트워크의 보안 경계를 정의하고 제어망과 정보망을 분리해야 한다. 방화벽의 부재나 잘못된 설정으로 인해 제어망과 정보망 사이를 인증 절차 없이 접근하는 경우 사이버보안 취약점이 된다. 또한, 안전계통과 비안전계통의 보안 등급이 다른 두 네트워크 사이에서는 송수신되는 데이터가 보안 등급이 높은 네트워크에서 낮은 네트워크로만 단방향으로 통신이 이루어지도록 한다.

3.2.9 보안장비 구성

계측제어시스템에 방화벽 등의 보안장비를 구성하는 경우 보안장비 규칙의 잘못된 설정이나 탐지할 수 없는 통신 프로토콜의 사용은 장비의 우회와 같이 사이버보안의 위협이 될 수 있다. 논리제어기기를 위한 독자적인 프로토콜을 사용하는 경우에 검증이 충분히 이루어진 프로토콜을 사용하고, 논리제어기기는 보안장비와의 안정적인 운용을 위해 충분한 확장성을 가져야 한다.

3.2.10 비안전한 코드 사용

계측제어시스템의 논리제어기기를 설계하는 과정에서 소프트웨어와 관련하여 검증을 통해 결과물에 보안상의 결함이 없도록 해야 한다. 제어로직에 널 포인터 역참조나 안전하지 않은 함수를 사용하는 경우는 해당 오류에 대한 예외처리 기능이 구현되어야 한다.

3.3 보안 조치 제외사항

논리제어기기의 보안 기능의 구현을 위한 최소한의 보안 요건을 도출하기 위해 불필요한 조치는 제외해야 한다. RG 5.71 규제 지침의 보안 조치 중에서 다음에 해당하는 항목은 적용하지 않는다.

3.3.1 운영 요건

보안 조치 중에서 정책과 절차의 개발, 배포, 검토 활동이나 운영단계에서 고려되어야 할 인적 행위와 관련된 조치들은 논리제어기기에서 구현되어야 할 보안 기능과 관련이 없으므로 설계 및 개발 단계에서 고려되어야 할 사이버보안 요건이 아니다.

3.3.2 기술 제한

기술 제한 항목은 보안 조치 중에서 논리제어기기에 기술적으로 적용이 불필요한 항목을 말한다. 무선통신, 웹, DNS, 그리고 공개키 등의 기능은 논리제어기기에서 사용하지 않거나 구현 불가능하므로 해당 보안 조치는 고려하지 않는다.

3.3.3 계통 적용

계측제어시스템에는 역할에 따라 여러 계통이 있고 하나의 계통은 논리제어기기와 산업용 컴퓨터로 구성된다. 시스템 공지, 접속 기록 공지, 그리고 타임스탬프 등의 보안 조치는 상위의 계통 수준에서 사이버보안 위협에 대응해야 하는 것이 적절하기 때문에 논리제어기기를 위한 보안 요건 항목에서는 고려하지 않는다.

3.3.4 요건 통합

인증이나 암호화와 같이 보안 조치에서 여러 세부 항목에서 중복으로 다루고 있는 부분에 대한 요건을 하나로 통합하여 기술해야 한다.

다음 장에서는 규제 지침을 만족하기 위해 사이버보안 위협과 제외사항을 고려한 논리제어기기에 필수적으로 구현되어야 할 보안 요건에 대해 정리한다.

Ⅳ. 논리제어기기의 사이버보안 요건

4.1 기술적 보안 요건

기술적인 보안 조치는 필수디지털자산에 적용되어야 할 기술적인 방법이나 도구 등에 관련한 보안 조치를 의미한다. 이전 장에서 살펴본 주요 보안 위협 중 인증 및 접근제어, 로깅, 무결성 검증, 암호화, 그리고 프로그램 형상과 관련하여 해당 위협에 대응하기 위해 논리제어기기에서 고려되어야 할 사이버보안 요건을 정리한다. 그리고 정리된 요건 중에서 운영 요건, 기술 제한, 계통 적용 그리고 요건 통합 부분에 해당하는 보안 조치는 제외한다. <표2>는 보안 조치를 만족하기 위한 논리제어기기를 위한 기술적 보안 요건을 보여준다.

<표 2> 기술적 보안 요건

분류	세부항목	개수
접근제어	계정 관리, 접근 이행, 정보 흐름 이행, 기능 분리 및 최소 권한, 세션 잠금, 활동 감시, 네트워크 접근 통제, 비안전 프로토콜 제한	8
감사 및 책임	감사 기록, 로그 저장 용량 감사 대상 기록의 분석	3
필수디지털장치 및 통신	공유자원, 전송 무결성, 암호화 사용, 서비스 비인가 원격 개시, 보안 매개변수의	6

보호	전송, 이질성/다양성	
식별 및 인증	사용자 식별 및 인증, 패스워드 요구 사항, 장치 식별 및 인증, 인증 기호 관리, 암호 모듈 인증	5
시스템 강화	불필요한 서비스 제거	1

4.1.1 접근제어

① 계정 관리

논리제어기기의 자원 및 기능에 대한 접근 권한을 설정하고 기능과 책임에 맞는 권한을 부여해야 한다. 논리제어기기에 대한 권한은 최소한 관리자, 개발자, 사용자 3가지로 분류해야 한다.

② 접근 이행

관리자는 제어기기에 대한 최상위 권한을 갖고, 개발자는 개발 및 유지보수와 관련된 작업 수행의 권한을 가져야 한다. 그리고 사용자는 논리제어기기의 상태만을 확인할 수 있는 권한을 가져야 한다.

③ 정보 흐름 이행

논리제어기기간 또는 논리제어기기와 소프트웨어 엔지니어링 도구 간에는 기존에 정의된 데이터만 송수신해야 한다.

④ 기능 분리 및 최소 권한

계정에 따라 접근이 가능한 논리제어기기의 기능은 분리되어야 하고 각 계정은 다른 계정의 기능을 수행할 수 없어야 한다.

⑤ 세션 잠금

논리제어기기에 로그인 이후 일정 시간 내에 사용자의 작업 활동이 없으면 세션을 종료해야 한다.

⑥ 활동 감시

논리제어기기의 감사 자료 생성을 위해 계정의 접속 기록, 계정의 생성, 변경 및 삭제, 제어로직의 변경 내용을 감시해야 한다.

⑦ 네트워크 접근 통제

논리제어기기와 소프트웨어 엔지니어링 도구의 연결에는 네트워크 접근 통제가 수행되어야 한다.

⑧ 비안전 프로토콜 제한

논리제어기기 네트워크에 안전성이 검증되지 않는 프로토콜은 사용하지 않아야 한다.

4.1.2 감사 및 책임

① 감사 기록

논리제어기기는 감사를 위한 로그를 저장하는 기능을 보유해야 한다.

② 로그 저장 용량

논리제어기기는 로그를 저장하기 위한 충분한 크기의 내부 저장 공간을 확보해야 한다.

③ 감사 대상 기록의 분석

논리제어기기는 로그 데이터를 소프트웨어 엔지니어링 도구로 송신할 수 있어야 한다.

4.1.3 필수디지털장치 및 통신 보호

① 공유자원

논리제어기기 간에 또는 연계되는 다른 기기 간에 자원은 공유되지 않아야 한다.

② 전송 무결성

논리제어기기 간, 논리제어기기 내부 모듈 간 또는 논리제어기기와 소프트웨어 엔지니어링 도구 간 송수신 되는 데이터는 출발지와 목적지 종단간 상호 확

인할 수 있는 기능을 구현해야 한다. 또한 출발지와 목적지 종단간의 인증을 위해 유효한 주소와 송수신 테이터의 유효한 순서를 확인 및 검사할 수 있는 기능을 구현해야 한다.

③ 암호화 사용

논리제어기기의 안전기능 및 성능을 고려하여, 암호화가 불가능한 경우를 제외하고 송수신 데이터에 암호화를 적용해야 한다.

④ 서비스 비인가 원격 개시

논리제어기기에 원격접속 기능을 구현하지 않아야 한다.

⑤ 보안 매개변수의 전송

논리제어기기 간 또는 논리제어기기와 소프트웨어 엔지니어링 도구 간 송수신되는 인증 관련 보안 매개변수는 기밀성이 보장되어야 한다.

⑥ 이질성/다양성

논리제어기기의 중요 모듈은 가용성을 보장하기 위해 이중화로 구성해야 한다.

4.1.4 식별 및 인증

① 사용자 식별 및 인증

논리제어기기에서 수행되는 작업은 단계별 인증 기능을 구현해야 한다. 소프트웨어 엔지니어링 도구의 접근을 위한 인증과는 별도로 논리제어기기의 접근을 위한 인증이 수행되어야 한다.

② 패스워드 요구 사항

소프트웨어 엔지니어링 도구를 통해 논리제어기기에 접근시 신뢰성 있는 인증방법을 사용해야 하며 인증시 사용하는 패스워드는 충분한 보안 강도를 유지해야 한다.

③ 장치 식별 및 인증

논리제어기기에 비인가 노드의 물리적 또는 논리적 연결을 방지하는 기능을 구현해야 하고 다른 논리제어기기 및 소프트웨어 엔지니어링 도구를 식별할 수 있는 기능과 유효성을 확인할 수 있는 기능을 구현해야 한다.

④ 인증 기호 관리

논리제어기기의 인증 정보는 기밀성을 유지해야 한다.

⑤ 암호 모듈 인증

논리제어기기에서 사용하는 암호화 알고리즘은 충분한 보안 강도를 유지해야 한다.

4.1.5 시스템 강화

① 불필요한 서비스 제거

논리제어기기의 운영체제 등의 응용 프로그램은 실제로 사용되는 기능만을 포함해야 하며, 불필요한 기능은 제거해야 한다.

4.2 운영적 및 관리적 보안 요건

운영적 보안 조치는 기술적인 방법보다는 인적 요소에 의해 이루어지는 사이버보안 활동에 대한 조치를 말하고, 관리적 보안 조치는 대부분 위험 관리나 사이버보안 정책에 관한 내용이다. 운영 요건, 기술 제한, 계통 적용, 그리고 요건 통합에 해당하는 보안 조치는 제외하고 사이버보안 위협 중 저장매체 관리, 입력값 검증 미흡, 네트워크 설계, 보안장비 구성, 그리고 비안전한 코드 사용에 대한 위협에 대응하기 위한 보안 요건을 선별한다. <표3>은 보안 조치를 만족

하기 위한 운영적 및 관리적 보안 요건의 세부항목을 보여준다.

<표 3> 운영적 및 관리적 보안 요건

분류	세부항목	개수
저장매체 보호	저장매체 접근	1
시스템 및 정보 무결성	악성코드 방지, 감시도구 및 기술, 정보 입력 제한	3
물리적 보호	물리적 보호	1
심층방어	심층방어	1
비상계획	비상계획	1
형상관리	형상관리	1
시스템 및 서비스 획득	시스템 및 서비스 획득	1

4.2.1 저장매체 접근

논리제어기기에 연결 가능한 저장매체는 허가된 사용자만이 접근할 수 있도록 접근제어를 지원해야 한다.

4.2.2 시스템 및 정보 무결성

① 악성코드 방지

논리제어기기는 악성코드 방지를 위해 무결성을 확인하여 제어로직을 다운로드하는 경우에 변조를 확인하여야 한다.

② 감시도구 및 기술

논리제어기기의 안전성과 성능 범위 내에서 보안 위협에 대한 탐지 및 방지 기능이 고려되어야 하고, 자가진단 기능을 통해 보안 영향 감지 방안이 마련되어야 한다.

③ 정보 입력 제한

논리제어기기 외부로부터의 입력은 고정된 크기 및 지정된 형식으로만 수신되도록 설정해야 한다. 논리제어기기 외부로부터의 입력은 유효성에 대한 검사를 수행해야 한다. 또한, 제어기기 외부로부터는 데이터의 입력만 가능해야 하며 시스템 명령의 입력은 수행하지 않아야 한다.

4.2.3 물리적 보호

논리제어기기의 장치연계를 위한 포트 중에서 불필요한 포트는 물리적으로 폐쇄되어야 한다.

4.2.4 심층방어

논리제어기기 네트워크망에서 안전 및 비안전, 제어망 및 상태망은 단방향 게이트웨이를 이용하여 물리적으로 분리해야 하며, 분리된 네트워크 간에는 독립성을 보장해야 한다.

4.2.5 비상계획

논리제어기기의 설정 정보와 네트워크 구성 정보 등을 백업할 수 있어야 한다.

4.2.6 형상관리

논리제어기기는 내부의 인터페이스 모듈, CPU, 전원 등의 시스템의 구성품의 목록을 확인하고 비인가 장치의 접근을 탐지할 수 있는 기능이 구현되어야 한다.

4.2.7 시스템 및 서비스 획득

논리제어기기의 입출력 데이터에 대한 버퍼오버플로우 검증을 수행해야 한다. 또한, 논리제어기기의 제어로직에서 사용되는 모든 함수는 해당 기능과 사용 변수에 대하여 검증되어야 한다. 제어로직에서 널 포인터를 예외 처리할 수 있는 기능이 구현되어야 한다.

Ⅴ. 결론

원자력 시설을 위한 사이버보안 규제 지침에 따라 운영 중인 원자력 발전소의 사이버보안을 평가한다. 하지만 기존 계측제어시스템은 보안에 대한 고려가 부족했기 때문에 보안 기능이 제한되어 규제 지침에서 제시하는 모든 보안 조치를 만족하기는 어렵다. 따라서 규제 지침을 만족하기 위해서 계측제어시스템의 개발 및 설계 단계부터 보안 기능을 설계하고 구현해야 한다. 보안 기능을 구현하기 위해 규제 지침의 내용을 모두 적용할 수 있지만, 규제 지침에서 다루고 있는 보안 조치가 기술적인 부분을 포함하여 정책, 절차, 그리고 인적 요소까지 다양하게 다루고 있으므로 이 보안 조치를 그대로 계측제어시스템에 적용하는 것은 어렵다.

본 논문에서는 계측제어시스템을 구성하는 설비인 논리제어기기의 개발 및 설계 단계부터 적용되고 구현되어야 할 보안 요건을 선별하였다. 계측제어시스템의 논리제어기기에 필요한 최소한의 보안 요건은 RG 5.71의 145개의 세부항목 중에 32개에 해당한다. 32개의 보안 요건을 고려하여 기능이 구현된다면 논리제어기기 수준에서의 보안 조치를 만족할 수 있다. 선별된 보안 요건은 개발자가 계측제어시스템의 보안 기능을 설계하고 구현하는데 적절하게 적용할 수 있고, 시스템 설계에 따른 인허가 과정에서 보안 기능 구현에 대한 근거로 참고할 수 있다. 또한, 구현된 보안 기능을 이용하여 원자력 발전소 운영 단계에서 예상되는 사이버보안 위협에 효율적으로 대응할 수 있을 것이다.

참고문헌

[1] 정성민·박기용, “계측제어시스템 사이버보안 요건서 고려사항,” 디지털산업정보학회 공동학술대회, 서울, 2016, pp.27-29.

[2] 정만현·안우근·민병길·서정택, “원전 디지털 계측제어시스템 사이버보안 기술 체계 수립 방법 연구,” 한국정보보호학회, 정보보호학회논문지, 제24권, 제3호, 2014, pp.561-570.

[3] 김도연, “원전 계측제어계통의 안전 네트워크 설계 및 평가를 위한 보안 기준,” 한국전자통신학회, 한국전자통신학회 논문지, 제9권, 제2호, 2014, pp.267-272.

[4] U.S. NRC, “Criteria for Digital Computers in Safety Systems of Nuclear Power Plants,” Regulatory Guide 1.152, 2006.

[5] 정성민·박기용, “계측제어시스템 개발을 위한 사이버보안 요구사항,” 디지털산업정보학회 공동학술대회, 서울, 2017, pp.34-37.

[6] Jung-Woon Lee, Cheol-Kwon Lee, Jae-Gu Song, and Dong-Young Lee, "Cyber Security Considerations in the Development of I&C Systems for Nuclear Power Plants," The 2011 International Conference on Security and Management(SAM'11), Las Vegas, USA, 2011.

[7] 원자력안전위원회규칙 제24호, “원자로시설 등의 기술기준에 관한 규칙,” 2020.

[8] 정성민·박기용, “계측제어시스템을 위한 기술적 보안 요건 적용,” 디지털산업정보학회 공동학술대회, 서울, 2018, pp.69-72.

[9] Sadegh vosough and Amir vosough, "PLC and its Applications," International Journal of multidisciplinary Sciences and Engineering", Vol.2, No.8, Nov, 2011.

[10] U.S. NRC, “Protection of Digital Computer and Communication Systems and Networks,” 10 CFR 73.54, 2009.

[11] U.S. NRC, “Cyber Security Programs for Nuclear Facilities,” Regulatory Guide 5.71, 2010.

[12] 한국원자력통제기술원, “원자력시설등의 필수디지털자산 식별 기술기준,” KINAC RS-019, 2015.
[13] 한국원자력통제기술원, “원자력 시설 등의 컴퓨터 및 정보시스템 보안 기술기준,” KINAC RS-015, 2016.
[14] 정성민·박기용, “원전 계측제어시스템에 적합한 운영적 및 관리적 보안 요건,” 디지털산업정보학회 공동학술대회, 서울, 2019, pp.175-178.
[15] 이철권, “원전 계측제어시스템 사이버보안 기술동향,” 한국정보보호학회, 정보보호학회지, 제22권, 제5호, 2012, pp.28-34.
[16] DHS, “Common Cybersecurity Vulnerabilities in Industrial Control Systems,” 2011.

■ 저자소개 ■

정 성 민
Jung, Sungmin

2014년 3월~현재
한국원자력연구원 선임연구원
2014년 2월 성균관대학교
전자전기컴퓨터공학과 (공학박사)
2008년 2월 성균관대학교
전자전기컴퓨터공학과 (공학석사)
2005년 2월 성균관대학교 정보통신공학부
(공학사)

관심분야 : 원자력보안, 제어시스템보안, 센서네트워크
E-mail : smjung@kaeri.re.kr

논문접수일 : 2020년 3월 10일
수 정 일 : 2020년 3월 16일
게재확정일 : 2020년 3월 18일