정 보 보 호 학 회 지
제 30 권 제2호, 2020. 4

원자력발전소 디지털시스템 설계요건(Code & Standard)을 고려한 보안성 평가에 관한 연구

임 준 희*, 김 휘 강**

요 약

국내 원자력발전소는 1978년 웨스팅하우스 노형의 고리1호기부터 2019년 APR-1400 노형의 신고리3호기 준공까지 많은 기술의 발전을 이룩하였다. 과거와 비교하여 현재의 원자력발전소는 단순히 발전용량만 증가한 것이 아니라, 안전에 대한 요구가 반영되어 발전하였다. 첫째, 미국 TMI 사고, 우크라이나 체르노빌 사고, 일본 후쿠시마 사고를 겪으며 자연재해, 인적실수 등에 관한 강화된 대책이 적용되었다. 둘째 미국 Browns Ferry 원전 정지, Hatch 원전 정지, 이란 핵시설 스턱스넷 공격 등을 겪으며, 사이버위협에 대응하기 위한 사이버보안 규제요건이 원자력발전소에 적용되었다. 그러나 사이버보안 규제요건과 원자력발전소 설계요건이 상충하는 부분이 일부 존재한다. 본 논문에서는 원자력발전소 사이버보안 규제요건과 상충하는 설계요건(Code&Standard)을 분석하여, 사이버 보안관점에서 요구되는 보안 조치사항을 도출하였다.

Ⅰ. 서 론

예전 원자력발전소는 아날로그 계측제어시스템(I&C)으로 설계되었으나, 최근에 상업 운전을 시작한 APR-1400 노형의 경우 대부분이 디지털로 설계되었다. 원자력발전소의 제어시스템이 디지털로 변화됨에 따라 사이버침해라는 새로운 위협이 대두되게 되었다.

일반적으로 원자력발전소 제어시스템은 외부와 연결이 되지 않은 독립된 망으로 구성되어 안전한 것으로 인식됐다. 그러나 2010년 이란의 원자력시설(원심분리기)이 스턱스넷에 감염되어 피해를 봤다. 이때 부셰르 원자력발전소도 스턱스넷에 감염이 되었으나, 근무하는 직원 PC만 감염시켰을 뿐, 원자력발전소 운전에 영향을 주지는 못했다. 이는 원전에 적용된 심층방호 전략에 의해 스턱스넷에 의한 사이버 공격을 막아낼 수 있었다. 원자력발전소에는 만약의 사고를 대비하여 여러 안전장치를 겹겹이 설치하여 실제 사고 시 방사능 유출을 방지하고 있다.

원전 사이버보안에도 이러한 심층방호 개념이 적용된다. 중요한 설비 순서대로 높은 등급에 배치하고 낮은 등급과의 통신에는 단방향 통신만을 하도록 규정하고 있다. 이를 통해 낮은 등급의 시스템이 사이버 공격 때문에 침해를 받더라도 늪은 등급 시스템에 악영향을 끼칠 수 없도록 방어하는 개념이다. 그러나 이러한 심층방호 개념에서 원전 설계요건(Code & Standard)과 상충하는 부분이 발생한다.

따라서, 본 논문에서는 원전 설계요건(Code& Standard)과 사이버보안 규제요건을 분석하여 불일치사항을 확인하고, 사이버보안 관점에서 심층방호 전략을 적용하기 위해 고려해야 할 사항을 제시하는 데 의의가 있다.

Ⅱ. 심층방호 개념

원자력발전소의 안전설계는 4가지 기본 개념을 가지고 있다. 다중성, 독립성, 다양성 그리고 심층방호이다. 특히 이 4가지 기본 개념에서 심층방호는 원자력 안전의 핵심개념이라고 말할 수 있다. 미국 원자력안전위원회(NRC)에서는 심층방호를 “방사선 또는 위험 물질 방출 사고들을 예방하고 완화할 수 있도록 원자력시설을 설계하고 운전하기 위한 접근법”으로서 “잠재적인 인적실수나 기계적 고장을 보상하기 위하여 하나의 방어수단에만 의존하지 않고 다수의 독립적인 방어단계를 제

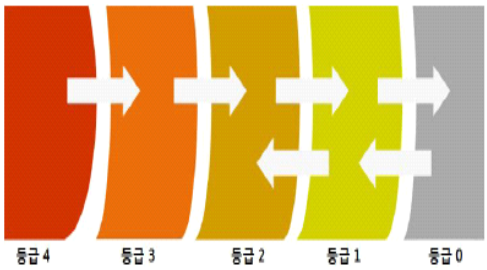
* 고려대학교 정보보호대학원 사이버보안학과 (대학원생, ijh0726@korea.ac.kr)
** 고려대학교 정보보호대학원 사이버보안학과 (교수, cenda@korea.ac.kr)

공하는 것이 핵심"이며 "접근제어, 물리적 방벽, 다중성·다양성을 지금 핵심 안전 기능과 비상대응조치가 포함된 것"으로 설명하고 있다. [1]

국제원자력기구(IAEA)에서는 사이버보안 심층방호를 "핵 안보 위협으로부터 대상을 보호하기 위한 조치와 시스템의 연속적인 계층의 조합"으로 정의하며 컴퓨터 시스템 침해가 발생하기 전에 실패하거나 실패해야 하는 일련의 연속적이고 독립적인 보호 수준의 조합을 통해 구현된다고 설명하고 있다. [2]

미국 원자력안전위원회에서는 "심층방호 구조는 5가지의 사이버보안 등급으로 구성"되며 다음과 같은 특징을 포함한다고 설명하고 있다. [3]

- 안전 및 보안 기능은 가장 높은 등급(4등급)에 배치하여 낮은 등급으로부터 보호
- 안전에 중요한 기능(비 안전), 비상대응기능은 최소 3등급에 배치
- 4등급에서 3등급, 3등급에서 2등급 통신은 물리적으로 단방향이 되도록 구성하여, 3등급에서 4등급으로 및 2등급에서 3등급으로 통신 되는 것을 금지



〔그림 1〕 사이버보안 심층방호 구조

Ⅲ. 안전설계 개념

국내 원자력발전소는 1980년대 한국형 원자력발전소부터 계측제어시스템(I&C)에 디지털을 도입하였다. Relay나 Solid State를 이용한 아날로그 제어방식에서 Microprocessor를 이용한 디지털 방식으로 변화됨에 따라 신호방식도 Hardwired에서 Data Communication 방식으로 변화되었다. 이와 같은 제어방식 변화에 따라 기존 아날로그 원자력발전소는 안전설계에 IEEE-603(Critical for Safety System for Nuclear Power Generating Station)를 적용하였으나, 디지털발전소는 IEEE 7-4.3.2(Standard for Digital Computer in Safety System of Nuclear Power Generating Station)를 적용한다.

3.1. IEEE 7-4.3.2 통신 독립성

IEEE 7-4.3.2에서는 통신 독립성을 요구하고 있다. 통신 독립성이란 "원자력발전소 계측제어시스템(I&C) 설계요건 중에 안전시스템 채널 간 통신 또는 안전시스템과 비 안전시스템 간의 통신 시 적용되는 것으로, 통신할 경우, 물리적으로 분리된 기기를 사용하여야 하고, 타 채널 또는 비 안전시스템의 기기가 안전시스템의 기능을 저해하지 않아야 한다는 독립성 요건을 만족하기 위한 하나의 필요조건"을 말한다. 안전과 비 안전시스템 간의 주된 통신기준은 다음과 같다.

- 안전 기능을 수행하는 장치는 안전 기능 처리를 방해할 수 있는 handshaking 또는 인터럽트 수행금지
- 수신된 데이터와 전송된 데이터는 안전 기능을 수행하는 컴퓨터의 이미 결정된 위치에 분리되어 저장되며, 이미 결정된 메모리 위치는 데이터 수신 또는 전송을 위해서만 사용
- 이미 정의된 데이터 집합들만 수신 안전계통에 의해서 처리되어야 하며, 인식할 수 없는 데이터는 정의된 설계에 따라 수신 계통에 의해 식별되고 처리되어야 함
- 안전 프로세서의 운전에 영향을 미칠 수 있는 명령 들이 아닌 데이터 집합들만이 전송되거나 처리될 수 있음. 모든 외부 신호들은 안전논리의 정상 순서에서 작동 안전논리에 따라 처리되는 데이터로 취급되어야 함. 안전논리 또는 논리 순서 영역을 변경할 수 있는 명령들은 허용되지 않음
- 안전 기능을 지원하는 데 필요한 통신은 전용 매체를 이용하는 일대일(Point to Point) 통신
- 통신 프로토콜은 메시지 데이터의 유효성과 적시성이 프로토콜에 포함되고 그것이 수신자에 의해 적절히 처리될 수 있도록 설계
- 안전계통 소프트웨어는 안전계열이 작동되고 있는 경우 변경으로부터 보호됨
- 안전계통 소프트웨어 형상은 주기적 자동 또는 수동 감시시험을 지원하기 위해 변경 또는 수정요구 금지

위와 같은 통신기준을 고려하여 IEEE 7-4.3.2

Annex E(통신 독립성)에서는 표 1과 같이 안전시스템과 비 안전시스템 간의 세 가지 통신방식이 제시된다.

〔표 1〕 IEEE 7-4.3.2 Annex E(독신 독립성) 통신방식

구분	통신방법	사이버보안 요건
안전 → 비 안전	One-way Path	충족
안전 ⇄ 비 안전	Two-way Path	위배
안전 ↔ 비 안전	One-way Path	위배

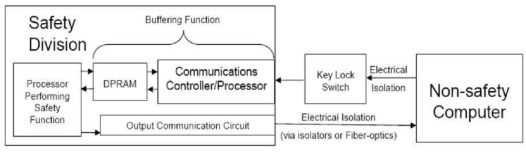
3.2. 안전과 비 안전 One-way Path

안전에서 비 안전으로 단방향 통신 경로를 구성하는 물리적 링크는 필요에 따라 전기적 격리와 통신 격리를 제공할 수 있다. 전기적 격리는 광 또는 Fuse 등으로 수행된다. 접속(또는 해제) 경로가 안전시스템에 악영향을 주지 않기 위해 broadcast 경로는 완전히 단방향으로 구성된다. 따라서 이 방식은 사이버보안 심층방호 요건을 충족하는 방식이다.

3.3. 안전과 비 안전 Two-way Path

이 방식은 두 개의 통신 경로를 이용하여 두 시스템 간의 양방향 통신을 허용한다. Two-way Path 방식을 사용하기 위해서는 안전시스템은 Buffer Circuit이 필요하다. Buffer Circuit은 DPRAM과 통신 제어기로 구성이 되는데, 비 안전시스템에서 전송된 데이터를 수신하고 분석하여 통신 프로토콜에 따라 오류 검사를 수행한다. 또한, 메시지 변질과 비 안전 컴퓨터 오작동의 영향으로부터 안전 기능을 수행하는 프로세스를 보호하는 기능을 수행한다.

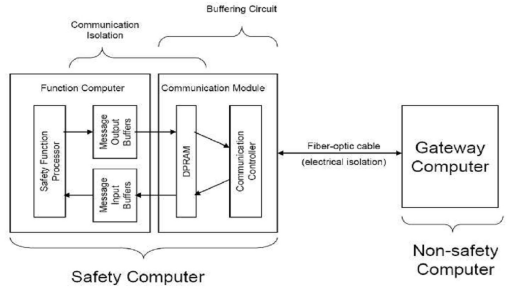
그러나 사이버보안 관점에서 비 안전(3등급)에서 안전등급(4등급)으로의 데이터 흐름은 규제요건을 만족하지 못한다.



〔그림 2〕 Two-way Path

3.4. 안전과 비 안전 One-Way Path

안전에서 비 안전 양방향 통신방식(One way)은 하나의 통신 경로를 이용하여 두 시스템 간의 양방향 통신을 허용한다. 이 방식은 하나의 안전시스템과 비 안전시스템 간의 양방향 통신을 허용하되, 버퍼 회로로서 통신 제어기와 DPRAM을 포함하는 분리된 통신 모듈을 사용한다. 비 안전시스템 메시지는 통신 모듈로 전송되고, 통신 프로토콜의 요구된 오류 검사, 적시성 확인 및 메시지 검증이 수행된 후, DPRAM으로 전송된다. 즉, 비 안전시스템으로부터 변조된 메시지가 전송될 경우, 버퍼 회로에서 사전에 검증함으로써, 안전시스템에 영향을 줄 수 없도록 설계되어 있다. 그러나 이 방법 역시, 비 안전(3등급)과 안전(4등급) 간의 양방향 통신을 함으로써 사이버보안에 어긋난다.



〔그림 3〕 One-way Path

Ⅳ. 적용방안

원자력발전소 심층방호의 목적은 “사이버 공격(Cyber Attack)부터 설계기준위협(Design Base Threat, DBT)에 이르기까지 필수디지털 자산(CDA)을 보호”하는 것이다. 따라서 원자력발전소의 보안성 평가를 위해서는 먼저 국가에서 정한 설계기준위협이 어떻게 설정되어 있는지 확인이 필요하다. 관련 법규에 따르면 설계기준위협(Beyond DBT)을 초과하는 위협은 원자력발전소 사업자의 조치범위를 넘어서는 것으로 국가에서 위협에 대해 방어하게 되어 있다. 따라서 원자력발전소 보안성 평가를 위해서는 먼저 위협의 범위를 설정해야 한다.

그다음 보호해야 하는 시스템 및 자산을 식별한다. 현재 사이버보안 규제기준인 RG 5.71에서는 명확한 식

별기준을 제시하고 있지 못하다. 예를 들어, 원자력발전소의 과도상태 발생 시 상태정보를 제공하는 시스템을 안전에 중요한 시스템으로 식별하도록 요구하고 있으나 원자력발전소에는 수많은 과도상태가 존재한다. 모든 정상범위에서 약간 벗어난 상태를 모두 과도상태로 간주한다면, 발전소 내 모든 시스템은 보호 대상이 된다. 따라서 명확한 기준을 수립하여 보호해야 할 시스템과 자산을 식별하고, 통신 연결성 분석을 통해 심층방호 요건에 따라 등급을 부여(안전:4등급, 비 안전:3등급)한다.

식별된 시스템과 자산은 설계요건에 따라 양방향 통신으로 구성되어 사이버보안 요건과 불일치한 부분이 발생할 수 있다. 불일치 시스템도 설계요건에 따라 통신 독립성이 확보되었으며, 양방향 통신인 경우에도 충분한 보안 조치가 적용되었다.

설계요건과 사이버보안 규제요건을 맵핑한 결과, 다음과 같이 심층방호 전략을 위해 요구되는 사이버 보안 조치를 도출하였다.

〔표 2〕 안전설계 통신요건 분석결과

가) Buffer Circuit를 구성하여 비 안전 시스템으로부터 안전시스템을 보호하는가?
• 비 안전시스템으로부터의 안전시스템 악영향 방지 • 메시지 변조, 오류 등을 확인 • Priority Logic에 의하여 악영향 발생 시 안전기능에 방해 금지
나) 물리적, 전기적 격리를 통하여 시스템이 독립적으로 설계되었는가?
• 사이버침해가 발생한 경우, 타 안전시스템으로 전파되지 않도록 격리
다) Handshake, Ready to Receive, 메시지 응답 등의 부적절한 수신을 금지하고 있는가?
• 프로토콜 취약점 악용 방지
라) IP 또는 MAC 주소를 잠금하고 있는가?
• 네트워크 접근통제 시행
마) 정보의 무결성(Integrity)을 검사하는가?
• 메시지 변조, 오류 등을 확인

〔표 3〕 사이버 보안 조치 매핑결과

설계요건	사이버 보안 조치
가	**〔1.3.4, 자원사용 우선권〕** 우선순위가 높은 프로세스가 낮은 프로세스에 의해 방해되는 것을 방지하기 위해 우선순위에 따라 자원의 사용을 제한하도록 설정
나	**〔1.1.12, 네트워크 접근통제〕** 물리적 혹은 논리적 네트워크 분리 **〔1.1.15, 안전하지 않은 연결〕** 필수디지털 자산을 설치 혹은 변경 시에 공급자가 해당 필수디지털 자산에 원격접근이 불가능하도록 모뎀 등을 구성 **〔1.1.19, 외부시스템의 사용〕** 외부에서 높은 보안등급에 있는 필수디지털 자산에 접근 불가 보장
다	**〔1.1.13, 안전하지 않은 프로토콜 제한〕** 보안 조치가 미흡한 네트워크 프로토콜을 사용할 때에는 해당 네트워크로의 불법적인 접속을 방지하기 위한 추가적 보안 조치 이행 **〔1.1.13, 안전하지 않은 프로토콜 제한〕** 네트워크 프로토콜에서의 명령이 필수디지털자산의 보안상태를 낮추지 못하도록 구성
라	**〔1.1.12, 네트워크 접근통제〕** MAC 주소 잠금 **〔1.1.12, 네트워크 접근통제〕** 정적 테이블 주소 유지 **〔1.3.5, 전송 무결성〕** MAC 주소 잠금을 통한 중간자 공격 및 가짜 기기가 네트워크에 추가되는 것을 예방
마	**〔1.3.5, 전송 무결성〕** 정보의 수신 시 해당 정보가 전송 도중 변경이 없었음을 보장하기 위해 암호화를 구성해야 하며, 동 조치가 어려울 때 대안적인 물리적 조치 강구 **〔1.3.5, 전송 무결성〕** NAC 장비 등을 통한 중간자 공격 및 인가되지 않은 기기가 네트워크에 추가되는 것을 예방

V. 결 론

디지털 자산을 식별할 때, 안전계통의 통신 연결성 분석을 통해 심층 방호에 어긋나는 통신 연결 구간을 확인하였다. 그다음 안전설계요건의 통신 독립성 분석을 통해 요구되는 사항을 확인하였고, 확인된 결과와 보안 조치사항을 맵핑하여, 심층방호 전략에 충족되는 보안 조치사항들을 도출하였다.

사이버보안 규제요건에서는 원자력발전소 물리적 방호를 위한 침입 탐지시스템, CCTV 등의 보안시스템도 안전시스템과 같은 4등급에 배치하도록 요구되고 있다. 그러나 보안시스템 설계요건을 제시하고 있는 IEEE 692(Security System for Nuclear Power Generating Stations)에서는 안전설계처럼 통신 요구사항이 제시되지 않았다. 3등급에 배치되는 기타계통(비 안전시스템, 보안시스템, 비상대응시스템) 시스템에도 별도의 통신 연결을 위한 기준은 제시되지 않는다. 따라서 기타계통의 통신 위배 사항 발생 시, 안전설계 요건을 분석하여 도출된 보안 조치사항들을 적용하여 취약점을 완화·제거하는데 활용될 수 있을 것으로 기대된다.

참 고 문 헌

[1] U.S NRC, Cyber Security Programs for Nuclear Power Facilities, NRC Regulatory Guide 5.71, January. 2010.

[2] KINAC, “원자력시설의 컴퓨터 및 정보시스템 보안”, KINAC/RS-015, 2016.

[3] IEEE, “Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations”, IEEE 7-4.3.2, 2010.

[4] KEPIC, "안전계통 디지털 컴퓨터", ENB 6370, 2015.

[5] “원전, 사이버 공격에 안전한가?”, 에너지신문, 2015년 5월 18일 수정, 2020년 4월 6일 접속, http://www.energy-news.co.kr/news/articleView.html?idxno=33814

〈저자소개〉

임 준 희 (Jun Hee Lim)

정회원

2020년 3월 : 고려대학교 사이버보안학과 석사과정

2011년 3월~2012년 12월 : 한전KDN 전력IT연구원

2013년 1월~현재 : 한국수력 원자력 사이버보안부

<관심분야> 계측제어 시스템, 제어시스템 보안,

김 휘 강 (Huy Kang Kim)

종신회원

1998년 2월 : KAIST 산업경영학과 학사

2000년 2월 : KAIST 산업공학과 석사

2009년 2월 : KAIST 산업 및 시스템공학과 박사

2004년 5월~2010년 2월 : 엔씨소프트 정보보안실장. Technical Director

2010년 3월~현재 : 고려대학교 정보보호대학원 교수

<관심분야> 온라인게임 보안, 네트워크 보안, 네트워크 포렌식