디지털산업정보학회 논문지 제18권 제2호-2022년 6월
http://dx.doi.org/10.17662/ksdim.2022.18.2.039

원자로보호계통 사이버보안 연계 위협 분석 연구

정 성 민*·김 태 경**

A Study on Chaining Threat Analysis of Cybersecurity against Reactor Protection Systems

Jung Sungmin·Kim Taekyung

〈Abstract〉

The application of digital technology to instrumentation and control systems in nuclear power plants has overcome many shortcomings of analog technology, but the threat of cybersecurity has increased. Along with other systems, the reactor protection system also uses digital-based equipment, so responding to cybersecurity threats is essential. We generally determine cybersecurity threats according to the role and function of the system. However, since the instrumentation and control system has various systems linked to each other, it is essential to analyze cybersecurity threats together between the connected systems.

In this paper, we analyze the cybersecurity threat of the reactor protection system with the associated facilities. To this end, we quantitatively identified the risk of the reactor protection system by considering safety functions, a communication type, the use of analog or digital-based equipment of the associated systems, and the software vulnerability of the configuration module of the reactor protection system.

Key Words : Reactor Protection System, Cybersecurity, Nuclear Power Plants, Chaining Threat

Ⅰ. 서론

미국 원자력 규제위원회에서 사이버 공격(Cyber attack)은 컴퓨팅 환경 및 인프라를 교란, 비활성화, 파괴 또는 악의적으로 제어할 목적으로 사이버 공간을 통한 공격, 데이터의 무결성을 파괴, 통제된 정보를 훔치는 것으로 정의한다. 그리고 사이버보안(Cybersecurity)은 사이버 공격으로부터 사이버 공간 사용을 보호하거나 방어하는 능력으로 정의한다[1]. 원자력 발전소 시설의 사이버보안은 미연방규정집(Code of Federal Regulations)의 에너지와 관련된 10장(10 CFR)에서 규정하고 있다. 10 CFR73.54(a)의 세부 항목에서 사이버보안으로부터 보호해야 하는 관련 시스템을 안전 관련 시스템, 보안 시스템, 비상대응시스템, 그리고 기타 지원시스템으로 분류한다[2]. 원자력 발전소에 디지털 기술이 적용되면서 원자력 발전소를 구성하는 시스템에 관한 사이버보안의 연구가 중요하게 다루어지고 있다.

우리나라 원자력 발전소 중에 현재 건설이 진행 중인 신한울 1, 2호기와 신고리 5, 6호기는 주제어실을

* 명지전문대학 인터넷보안공학과 교수(제1저자)
** 명지전문대학 인터넷보안공학과 교수(교신저자)

포함하여 계측제어시스템이 대부분 디지털 설비로 교체되었다. 계측제어시스템에 디지털 기술의 적용은 아날로그 장비가 가지고 있던 부품 노후화에 따른 성능 저하, 불시 정지 발생 증가, 기기의 단종 문제 등 다양한 문제를 해결하게 된다[3, 4]. 하지만, 디지털 기반의 계측제어시스템은 아날로그 기반보다는 사이버보안 위협에 취약하다.

아날로그 기반의 계측제어시스템은 외부와 단절되어 운영됨으로 보안 강도를 어느 정도 유지할 수 있었고, 사이버보안에 대해 크게 고려할 필요가 없었지만, 디지털 기반의 계측제어시스템은 외부와의 연결되는 경로가 존재하게 되므로 외부에서의 다양한 사이버보안 위협에 쉽게 노출될 수 있다. 실제로 보안 관련 국제 학회에서 원자력 발전소를 포함한 산업제어시스템에 대한 사이버 공격에 대한 실증 및 논의가 계속해서 이루어지고 있다[5].

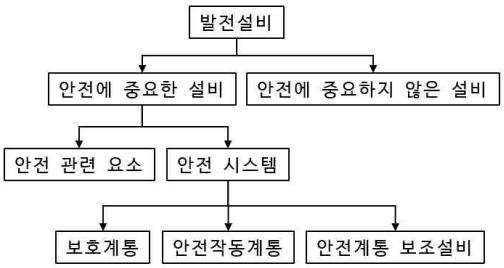
주요 안전 시스템인 원자로보호계통은 디지털 기반의 제어기기와 통신망을 사용하기 때문에 사이버보안 위협에 취약할 수 있으므로 사이버보안 위협을 분석하고 이에 대해 대비하는 것은 중요하다. 위협을 분석할 때 원자력 발전소 계측제어시스템은 여러 장비가 긴밀한 연계를 하고 있으므로 하나의 장비 각각의 관점에서 사이버보안 위협을 분석하는 것보다는 연계 설비의 전체적인 관점에서 사이버보안 위협을 분석하는 것이 효율적이다.

본 논문에서는 원자로보호계통의 주요 연계를 분석하여 사이버 위협을 정량적으로 확인한다. 2장에서는 원자력 발전소의 안전 및 비안전 시스템과 대표적인 안전 시스템인 원자로보호계통을 알아본다. 3장에서는 사이버보안 위협을 분석하기 위해 원자로보호계통의 구성과 기능을 정리한다. 4장에서는 가능한 사이버 공격에 대해 원자로보호계통과 연결된 설비의 연계 위협을 확인하고 5장에서 연구내용을 요약정리하였다.

Ⅱ. 원자력 발전소 안전 시스템

원자력 발전소의 안전 시스템은 가장 높은 등급의 안전을 보장해야 하는 시스템으로, 안전 시스템의 오작동은 방사능 유출 등 대규모 피해를 가져올 수 있으므로 사이버보안 위협에 대한 분석 및 대응은 중요하다[6].

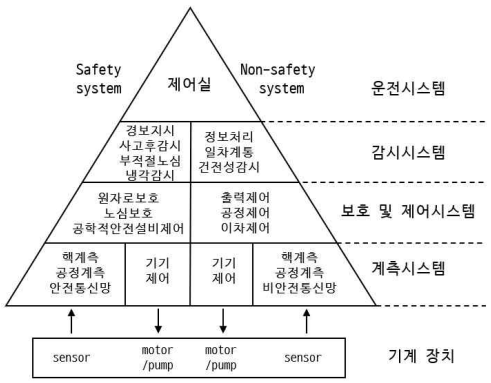
원자력 발전소 계측제어시스템에 대한 사이버보안을 강화하기 위해 한국원자력통제기술원은 KINAC/RS-019를 통해 원자력 시설의 안전, 보안, 비상대응 기능을 수행하는 디지털 설비를 필수 디지털 자산으로 정하였다. 그리고 필수 디지털 자산에 대하여 KINAC/RS-015 기술기준을 통해 심층 방호 전략을 적용하도록 기준을 제시하고 있다[7, 8].



<그림 1> 원자력 발전소 설비 분류

국제원자력기구(IAEA)에서는 원자력 발전소 시설에서 안전과 관련된 설비들은 <그림 1>과 같이 안전 시스템 아래 보호계통, 안전작동계통, 그리고 안전계통 보조설비로 나누고, 사이버보안의 대상을 원자력 시설의 기능적 구성요소를 이루는 계산, 통신, 설비 또는 기기 그리고 제어기기로 정의한다[9]. 이렇듯 국내외 규제기관은 여러 발행 문서를 통해 계측제어시스템에 대한 사이버보안을 강조하고 있다.

계측제어시스템은 안전 기능 수행 여부에 따라 안전 시스템과 비안전 시스템으로 나눌 수 있는데, <그림 2>는 계측제어시스템의 안전 및 비안전 시스템의 예를 보여준다[10].



<그림 2> 원자력 발전소 MMIS 개념

<그림 2>와 같이 계측제어시스템은 기능에 따라 보호, 제어, 감시, 그리고 계측 시스템으로 분류된다. 계측 시스템은 운영 관련 변수를 수집하고, 감시 시스템은 변수 정보를 운전원에게 제공한다. 제어 시스템은 안전해석에 따라 설정된 공정값을 바탕으로 원자로를 비롯한 관련 설비를 제어한다. 보호 시스템은 원자력 발전소의 안전 기능과 직접적으로 관련된 변수들을 실시간으로 감시하고, 변수가 정해진 안전 운전의 범위를 이탈하면 안전을 위해 원자로를 정지시키거나 공학적안전설비 작동신호를 발생시키는 기능을 수행한다[6].

여러 계통 설비 중에서 대표적인 보호 시스템으로 원자로보호계통(RPS, Reactor Protection System)은 안전과 관련된 기능을 수행하는데, 예상운전과도사건(AOO, Anticipated Operational Occurrence) 발생시에 원자로의 안전 제한치를 초과하지 않도록 원자로를 정지시키고, 제한사고 발생시에 사고를 완화하기 위해 공학적 안전설비 작동 계통을 보조하여 발전소를 안전한 상태로 만든다[11]. 원자로보호계통은 디지털 기반의 공정 논리 제어기기(PLC, Programmable Logic Controller)가 사용되는데, 공정 논리 제어기기는 원자력 발전소 운전을 위한 로직 및 시퀀스, 타이밍, 카운트 연산 등을 수행하기 위해 메모리와 중앙처리장치를 가진 전자장비이다. 또한 확장 모듈을 통해 공정 논리 제어기기 간, 혹은 다른 디지털 설비 간에 아날로그 및 디지털 기반의 통신을 지원하며, 펄스 카운터나 온도 입력 모듈도 지원한다. 따라서, 디지털 기반의 연산이나 통신 기술이 사용되므로 원자력 발전소 시설의 데스크톱 컴퓨터, 메인프레임 시스템, 서버나 네트워크 장비와 마찬가지로 사이버 공격의 성공 가능성을 고려해야 하고, 이를 사용하는 원자로보호계통의 사이버 공격에 대한 영향을 파악하기 위해 원자로보호계통의 기능 및 주요 연계를 파악해야 한다[12].

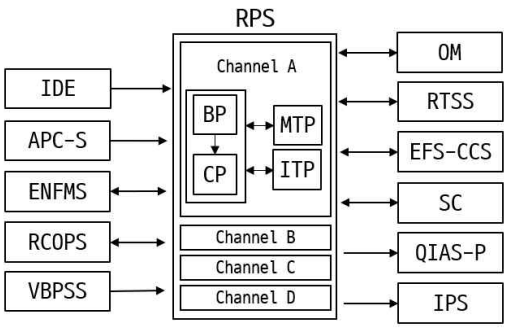
Ⅲ. 원자로보호계통 기능 및 구조

원자로보호계통은 디지털 기술이 적용된 공정 논리 제어기기와 통신망을 사용하므로 사이버 공격에 쉽게 노출될 수 있고, 안전 시스템이기 때문에 사이버 공격으로 인해 안전과 관련된 기능의 제대로 작동하지 못하거나 악의적으로 잘못된 공정값이 입력된다면 원자로가 의도하지 않은 상황에서 정지하거나 필요한 경우에 정지가 되지 않는 결과를 가져올 수 있다. 사이버 공격에 대한 시나리오를 작성하기 위해 먼저 원자로보호계통의 구성과 기능을 분석하고 물리적인 연계 사항을 파악해야 한다. 그리고 연계점에서 보안의 취약성을 정량적으로 분석하고, 분석된 결과를 바탕으로 사이버 공격의 대응책을 마련해야 한다.

원자로보호계통은 신뢰성을 위해 4채널로 구성되며, 각 채널은 입출력 모듈, 비교논리프로세서, 동시논리프로세서, 연계시험프로세서, 보수시험반 및 관련 하드웨어 장치로 구성된다[13]. 원자력 발전소의 안전 관련 변수는 계측 시스템을 통해 감시되는데, 안전 관련 변수의 값이 특정 설정값을 벗어나게 되면 비교논리프로세서(BP, Bistable Processor)는 트립

(Trip) 신호를 발생시킨다. 트립 신호는 채널 간 동시 논리프로세서(CP, Coincidence logic Processor)에 전달되는데, 동시논리프로세서는 트립 신호와 우회 신호 상태를 판단하여 원자로 정지를 결정한다. 원자로 정지를 위한 동시논리 트립 신호는 원자로정지차단기계통(RTSS, Reactor Trip Switchgear System)를 작동시킨다.

운전원모듈(OM, Operator Module)은 원자력 발전소의 주제어실에 설치되어 원자로보호계통 운전을 위한 원자로보호계통의 트립, 예비트립, 개시, 트립채널 우회 상태를 운전원에게 제공한다. 보수시험반(MTP, Maintenance and Test Panel)은 원자로 정지에 대한 우회 기능을 제공하며, 시험 및 유지보수를 위한 설비로 비안전 연계를 위한 기능을 수행한다. 연계시험프로세서(ITP, Interface and Test Processor)는 원자로보호계통의 상태를 감시하고, 보수시험반의 운전원 입력을 바탕으로 원자로보호계통에 대한 전반적인 시험을 수행하기 위한 관련 신호를 교환한다. 그리고, 공정 논리 제어기기의 응용프로그램은 응용프로그램 개발도구(IDE)를 사용하여 작성하는데, 응용프로그램 개발도구와의 연계도 중요한 부분이다. 만약, 응용프로그램 개발도구를 이용하여 공정 논리 제어기기에 잘못된 제어 논리가 업로드 된다면, 안전과 관련된 기능을 수행하는 데 문제가 될 수 있다.



<그림 3> 원자로보호계통 주요 연계

<그림 3>은 원자로보호계통과 물리적으로 연결되어 데이터를 송수신하는 주변 계통과의 연계 사항을 나타낸다[14-17]. 보조공정캐비닛(APC-S, Auxiliary Process Cabinet-Safety)은 가압기 압력이나 증기발생기 압력 및 수위를 원자로보호계통으로 송신한다. 노외중성자속감시계통(ENFMS, Ex-Core Neutron Flux Monitoring System)은 중성자속 신호를 원자로보호계통으로 송신하거나, 계통 관련 시험 신호를 수신한다.

노심보호계통(RCOPS, Reactor Core Protection System)은 원자로를 안전하게 운영하기 위해 국부출력밀도와 핵비등이탈율을 계산하여, 설정된 공정값을 벗어나는 경우 원자로 트립 신호를 원자로보호계통으로 송신하고, 계통 관련 시험 신호를 수신한다. 필수모선전원전원공급계통(VBPSS, Vital Bus Power Supply System)은 원자로보호계통에 전원을 공급한다. 원자로정지차단기계통은 원자로를 정지하기 위한 신호를 원자로보호계통에서 수신하고, 정지회로차단기(TCB, Trip Circuit Breaker) 상태 신호를 원자로보호계통으로 송신한다.

공학적안전설비-기기제어계통(ESF-CCS, Engineered Safety Feature- Component Control System)은 원자력 발전소 제한사고의 발생시 공학적 안전설비작동 신호를 원자로보호계통에서 수신하고, 계통 관련 시험 신호를 원자로보호계통으로 송신한다. 변수지시및경보계통(QIAS-P, Qualified Indication and Alarm System-PAMI)은 안전 관련 사고감시변수를 원자로보호계통에서 수신한다. 정보처리계통(IPS, Information Processing System)은 원자력 발전소의 상태 정보를 실시간으로 원자로보호계통에서 수신한다.

네트워크 관점에서 원자로보호계통은 통신을 이용하여 연계된 여러 계통과 데이터를 송수신하는데, 보조공정캐비닛, 노외중성자속감시계통, 노심보호계통, 그리고 원자로정지차단계통는 아날로그 기반의 배선

을 사용하기 때문에 사이버보안 위협에 대한 영향이 적다. 그러나 변수지시및경보계통, 공학적안전설비-기기제어계통, 정보처리계통(IPS, Information Processing System)은 디지털 기반의 통신망을 사용하므로 일반적인 정보시스템에 알려진 사이버보안 위협에 취약할 수 있다.

Ⅳ. 원자로보호계통 연계 위협 분석

원자력 발전소의 설비에 대한 사이버보안 위협의 정도를 정량적으로 분석하고자 할 때, 일반적으로 설비의 역할이나 기능에 따라 위협의 정도를 분석한다. 하지만, 하나의 계통은 또 다른 여러 설비 및 계통과 연계하여 작동하기 때문에, 하나의 설비에만 범위를 한정하여 사이버보안의 위협을 분석하기보다는 연계된 계통 및 설비를 같이 고려하여 사이버보안 위협의 정도를 분석해야 한다. 원자로보호계통의 사이버보안 관련 취약점을 정량적으로 분석하기 위해 위험(Risk)을 설비의 안전 기능 수행 여부에 따른 가용성(Availability), 아날로그 및 디지털, 단방향과 양방향 통신의 연계 위협(Threat), 원자로보호계통의 구성 모듈의 소프트웨어 관련 취약점(Vulnerability)을 다음과 같은 수식으로 표현한다[6].

$$R = A \times T \times V \quad (1)$$

안전 기능 수행 여부에 따라 원자력 발전소의 설비에 안전 등급 또는 비안전 등급을 부여하는데, 안전 등급은 중요도에 따라서 1, 2, 또는 3으로 분류하며 비안전 등급은 안전 등급에 해당하지 않는 설비에 부여한다[18].

안전 등급 설비의 경우 사이버 공격에 원자력 발전소에 미치는 영향은 비안전 등급의 설비에 비해 크다고 할 수 있다. KINAC/RS-019의 안전 관련 및 안전 중요 시스템 구분을 기준으로 <표 1>과 같이 안전 기능 수행에 따라 정량적인 점수를 부여한다.

<표 1> 설비의 가용성 기준

Level	Criteria	Value
High	연계된 설비가 안전 등급에 해당하여 가용성 침해시 원자력 발전소의 안전 기능에 중요한 영향을 미친다.	0.9
Medium	연계된 설비가 안전 등급은 아니지만, 안전 기능에 직접적인 영향을 줄 수 있어 가용성 침해시 원자력 발전소의 안전 기능에 부분적으로 영향을 미친다.	0.5
Low	연계된 설비가 비안전 등급에 해당하거나 안전 기능에 직접적인 영향을 주지 않으므로 가용성 침해시 원자력 발전소의 안전 기능에 미미한 영향을 미친다.	0.1

원자로보호계통과 연계된 외부 설비에 대해 안전 등급에 따라 <표 2>와 같이 중요도를 부여한다. 일반적으로 다른 안전 시스템과 마찬가지로 필수모선전원전원공급계통, 원자로정지차단시스템 설비는 기능적인 면에서 안전 기능에 미치는 영향이 다른 설비에 비해 적다고 할 수 있다. 운전자모듈, 보수시험반, 연계시험프로세서는 안전 기능에 부분적으로 영향을 미칠 수 있다고 할 수 있다. 또한, 주요변수지시및경보계통, 공학적안전설비-기기제어계통, 노심보호계통은 안전 등급에 해당하므로 중요도가 높고, 원자로의 정지 기능 수행에 관련이 있으므로 사이버 공격으로 원자력 발전소의 안전 기능에 잘못된 영향을 미칠 수 있다.

<표 2> 연계 설비의 가용성 분류

Asset	Impact	Asset	Impact
APC-S	High	ESF-CCS	High
ENFMS	High	Safety Console	Medium
RCOPS	High	QIAS-P	High
VBPSS	Low	OM	Medium
RTSS	Low	IPS	Low

다음으로 고려해야 할 사항은 설비 간의 연계 위협이다. 계측제어시스템은 다양한 설비가 같이 구성되어 운영되기 때문에 원자로보호계통 하나만으로 사이버보안 위협이 크거나 작다고 판단할 수는 없다. 원자로보호계통과 연계된 설비의 사이버보안 위협을 분석하여, 해당 설비와 원자로보호계통을 같이 사이버보안 위협의 정도를 판단해야 한다. 특히 하나의 설비가 사이버보안 위협이 작다고 해도, 여러 위협에 대한 취약점을 만들게 되면 이런 위협은 결합하여 원자로보호계통에 큰 영향을 미칠 수 있으므로 설비 간 연계 위협을 파악하는 것은 중요하다. <표 3>은 설비 간의 통신망의 종류에 따라 해당 계통으로 단방향 입력, 단방향 출력, 그리고 양방향으로 연계된 내용 및 아날로그와 디지털 사용에 대해 사이버보안 위협에 대해 정량적인 점수를 보여준다.

<표 3> 설비의 연계 위협 기준

Level	Criteria	Value
High	통신 방식 및 기반 기술에 따른 사이버 공격으로 연계 설비에 중요한 영향을 미친다.	0.9
Medium	통신 방식 및 기반 기술에 따른 사이버 공격으로 연계 설비에 부분적으로 영향을 미친다.	0.5
Low	통신 방식 및 기반 기술에 따른 사이버 공격으로 연계 설비에 미미하게 영향을 미친다.	0.1

<표 4>는 데이터를 주고받는 방향을 고려했을 때 원자로보호계통에서 연계된 설비의 방향, 혹은 반대 방향으로 사이버보안 위협에 따른 영향을 분석하였다. 일반적으로 필수모선전원공급계통은 아날로그 배선을 사용하고, 단방향 신호로 연계되므로 사이버 공격의 영향은 비교적 적다고 할 수 있다. 주요변수지시및경보계통과 정보처리계통은 원자로보호계통에서 단방향으로 데이터를 받으므로 양방향의 통신보다는 사이버보안 위협이 작다. 반면에 공학적안전설비-기기제어계통과 노심보호계통은 원자로보호계통과 양방향 통신을 하므로 사이버보안 위협으로 큰 영향을 받을 수 있다. 또한, 보수시험반이나 안전제어반은 디지털 기반의 장비를 사용하고, 원자로보호계통 간 송수신 데이터가 있으므로 사이버보안 연계 위협이 다른 설비보다 크다고 판단된다. 마지막으로 응용프로그램 개발도구는 원자로보호계통을 구성하는 공정논리 제어기기에 연결되어 응용프로그램을 업로드하기 때문에 원자로보호계통의 방향으로 사이버 공격의 영향은 비교적 크다고 판단된다.

<표 4> 연계 설비의 위협 분류

Asset	Impact	Asset	Impact
APC-S	Low	ESF-CCS	High
ENFMS	Low	Safety Console	High
RCOPS	Medium	QIAS-P	Low
VBPSS	Low	OM	High
RTSS	High	IPS	Low

위와 같은 하드웨어 부분 이외에 디지털 기반, 아날로그 기반을 고려하여 산업제어설비의 사이버보안 취약점을 기반으로 위협의 정도를 분석해야 한다. 미국 국토안보부(DHS)에서는 산업제어설비의 사이버보안 위협을 8개의 분야로 분류하고 소프트웨어와 관련된 취약성을 <표 5>와 같이 설명하였다[19].

<표 5> 산업제어설비 사이버보안 취약점

분류	사이버보안 취약점	결과
V1	입력값 검증	오류 및 가용성 저하
V2	잘못된 함수 사용	잘못된 결과값
V3	접근제어 적용	부적절한 권한 획득
V4	인증 수행	부적절한 인증 수행
V5	무결성 검증	악성코드 수행
V6	암호화 적용	기밀성 저하
V7	인증 정보 관리	인증정보 유출
V8	소프트웨어 관리	시스템 악용

해당 취약점은 원자로보호계통의 구성 모듈과 연계된 설비에 적용하여 사이버보안 위협에 대해 정량적으로 분석할 수 있다. 입력값 검증과 관련된 취약점(V_1)은 시스템 입력되는 데이터의 길이에 대한 검증이 부족한 경우에 발생한다. 이 취약점으로 제어 수행의 오류 및 가용성이 저하되는 결과를 가져오며 버퍼오버플로우나 서비스 거부 공격을 유발하게 된다. 안전하지 않은 함수 사용의 취약점(V_2)은 잘못된 출력값을 가져올 수 있는 함수를 사용할 때 발생하며, 시스템의 오류나 인증과 관련된 정보를 시스템에 그대로 저장하는 등의 문제를 가져온다. 허용, 권한 및 접근제어 취약점(V_3)은 잘못된 접근제어 수행으로 발생하여, 이 취약점을 이용하여 비인가자가 시스템의 데이터에 접근하거나 제어 명령을 실행할 수 있는 부적절한 권한을 획득할 수 있다. 부적절한 인증에 대한 취약점(V_4)는 인증 수행의 검증이 미흡한 경우에 발생하며, 공격자가 인증 과정을 우회하여 부적절한 권한을 획득할 수 있다. 불충분한 데이터 무결성 검증 관련 취약점(V_5)은 데이터의 무결성 검사가 부족하여 시스템내에서 악의적인 프로그램이 실행될 수 있게 된다. 암호화 적용과 관련된 취약점(V_6)은 보안 강도가 약하거나, 취약점이 알려진 암호 알고리즘 사용하는 경우에 발생하며, 공격자가 암호를 추측하거나 암호가 유출될 수 있게 된다. 인증 정보 관리와 관련한 취약점(V_7)은 인증 관련 중요 정보를 잘못된 방법으로 저장하는 경우에 발생한다. 이 취약점으로 인해 인증 정보가 쉽게 유출될 수 있다. 마지막으로 소프트웨어 보안패치와 관련된 취약점(V_8)은 시스템에서 보안 취약성에 대한 패치가 이루어지지 않고 최초의 기본 설정을 그대로 사용하는 경우에 발생하며 불필요한 서비스가 실행될 수 있다.

각 사이버보안 관련 소프트웨어 취약점을 원자로보호계통의 구성 모듈에 적용하여 사이버보안 위협의 정도를 분석한다. 원자로보호계통의 주요 소프트웨어 모듈은 비교논리, 동시논리 소프트웨어 및 보수시험반, 연계시험프로세서 소프트웨어가 있다. 그리고 공정 논리 제어기기에 제어 논리를 작성하고 저장하기 위한 응용프로그램 개발도구가 있다. 해당 소프트웨어가 원자로보호계통을 구성하는 각 모듈이 위의 소프트웨어 취약점으로 인해 원자로보호계통에 얼마나 영향을 줄 수 있는지 분석한다. <표 6>은 각 구성 모듈에 대한 소프트웨어 관련 사이버보안 취약성이 시스템의 오동작이나 정지에 미칠 수 있는 영향에 대한 기준을 나타낸다.

<표 6> 설비의 사이버보안 영향 기준

Level	Criteria	Value
High	취약성을 통해 설비가 시스템의 오동작이나 정지에 중요한 영향을 미친다.	0.9
Medium	취약성을 통해 설비가 시스템의 오동작이나 정지에 부분적인 영향을 미친다.	0.5
Low	취약성을 통해 설비가 시스템의 오동작이나 정지에 미미하게 영향을 미친다.	0.1

<표 7>은 원자로보호계통의 주요 구성 모듈의 소프트웨어 취약성 관련 사이버 위협 영향을 보여준다. 일반적으로 보수시험반, 연계시험프로세서, 비교논리 프로세서, 그리고 동시논리프로세서는 암호화 적용, 인증정보 관리, 소프트웨어 관리 취약점의 영향은 거의 없다고 판단된다. 입력 신호, 내부 채널간 교환되는 신호, 그리고 설비의 역할 등을 고려하여 각각의 취약점에 대해 그 피해 정도를 분석하였다. 특히, 응용프로그램 개발도구는 일반적인 컴퓨터에서 설치되기 때문에 대부분의 취약점에서 중요한 영향을 미치고 있다.

<표 8>은 원자로보호계통을 구성하는 모듈에 대하여 사이버보안 위험도를 분석하였다. 안전 기능과 관련된 연계 설비의 가용성과 주변 설비와의 연계 위협 그리고 소프트웨어 취약점의 사이버 공격 영향성을 이용하여 수식에 따라 위험도를 계산하였다.

<표 7> 원자로보호계통 사이버보안 영향 분류

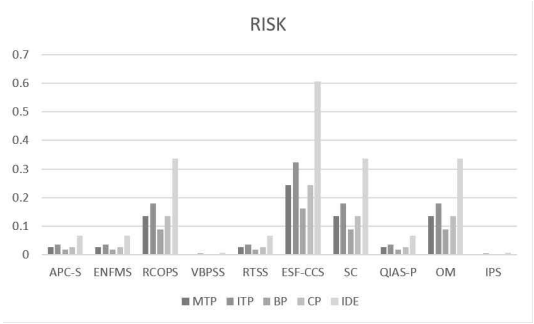
Module	V1	V2	V3	V4	V5	V6	V7	V8
MTP	L	L	M	M	H	L	L	L
ITP	M	M	M	M	H	L	L	L
BP	L	M	M	L	L	L	L	L
CP	H	M	L	L	M	L	L	L
IDE	H	H	H	M	H	M	M	H

<표 8> 원자로보호계통 구간별 위험도

Metric	MTP	ITP	BP	CP	IDE
APC-S	0.027	0.036	0.018	0.027	0.068
ENFMS	0.027	0.036	0.180	0.027	0.068
RCOPS	0.135	0.180	0.090	0.135	0.338
VBPSS	0.003	0.004	0.002	0.003	0.008
RTSS	0.027	0.036	0.018	0.027	0.068
ESF-CCS	0.243	0.324	0.162	0.243	0.608
Safety Console	0.135	0.180	0.090	0.135	0.338
QIAS-P	0.027	0.036	0.018	0.027	0.068
OM	0.135	0.180	0.090	0.135	0.338
IPS	0.003	0.004	0.002	0.003	0.008

원자로보호계통과 연계된 설비 중에서 공학적안전설비-기기제어계통, 노심보호계통 그리고 안전제어반, 운전원 모듈이 사이버보안에 대한 취약점으로 위험이 다소 높은 것으로 파악된다. 아날로그 기반의 설비인 필수모선전원공급계통이나 단방향의 정보처리계통의 경우는 사이버보안에 대한 영향이 매우 낮다고 할 수 있다.

<그림 4>에서 공학적안전설비-기기제어계통은 안전 등급으로써 원자로보호계통과 양방향 통신을 하고 있고, 디지털 기반의 설비이기 때문에 원자로보호계통과의 연계로써 위험도가 가장 높다. 관련하여 원자로보호계통에서 다음과 같은 사이버보안 위협을 고려해 볼 수 있다. 응용프로그램 개발도구에서 부적절한 입력값, 접근제어 취약점, 취약한 데이터 무결성 검증 등의 취약점을 이용한 사이버 공격으로 원자로보호계통에 잘못된 논리 제어를 업로드하거나, 사이



<그림 4> 원자로보호계통 위험도

버보안 위협이 연계시험프로세서를 통해 공학적안전설비-기기제어계통 또는 노심보호계통에 잘못된 정보 전달, 서비스 지연 등이 연계 설비의 시스템 오류를 유발하여 의도하지 않는 원자력 발전소 정지 또는 정지 불능의 상태를 유발할 수 있다. 따라서, 운영자는 이처럼 사이버보안 위협이 큰 연계 및 설비에 대한 사이버보안 강화를 고려해야 한다.

Ⅴ. 결론

원자력 발전소 계측제어시스템에 디지털 기술의 적용은 아날로그 기술의 많은 단점을 극복하게 하였지만, 이에 사이버보안의 위협도 그만큼 커지게 되었다. 특히 디지털 기반의 연계 설비는 사이버보안 취약점을 통한 다양한 공격 경로를 만들게 된다. 계측제어시스템은 안전 시스템과 비안전 시스템으로 나눌 수 있는데, 원자로보호계통은 예상운전과도사건 발생시에 원자로의 안전 제한치를 초과하지 않도록 원자로를 정지시키고, 제한사고 발생시에 사고를 완화하기 위해 공학적 안전설비 작동 계통을 보조하여 발전소를 안전한 상태로 만든다. 원자로보호계통에 디지털 기반의 장비를 사용하게 되면서, 이런 사이버보안 위협에 대한 대응은 이전보다 더 중요해졌다. 일반적으로 설비의 역할 및 기능에 따라 사이버보안

위협을 판단하게 되는데, 계측제어시스템은 다양한 시스템이 서로 연계되어 있으므로 사이버보안 위협과 관련하여 연계된 설비와 같이 그 위험을 분석하는 것이 중요하다.

원자로보호계통의 사이버보안 위협을 분석하기 위해 연계 설비에 대한 안전 기능 수행 여부에 따른 가용성, 원자로보호계통과 통신 형태 및 아날로그 및 디지털 기반에 따른 연계위협, 그리고 원자로보호계통 구성 모듈의 사이버보안 취약성 등을 고려하여 위험도를 정량적으로 확인하였다. 추후 연계 설비의 범위를 넓혀 원자력 발전소 계측제어시스템에서 설비간 연계에 따른 사이버보안 위협의 정도를 분석하고자 한다. 분석 결과는 운영자가 전체 설비의 위협 정도에 따른 중요 시스템을 판단할 수 있고, 적절한 대응을 마련하는 데 이용될 수 있다.

참고문헌

[1] U.S NRC, “Secure Network Design,“ Nuclear Regulatory Commission, NUREG/CR-7117, 2012.

[2] U.S NRC, “Protection of Digital Computer and Communication System and Networks,” 10CFR73.54, 2009.

[3] 이동일·류광기, “원자력 안전등급 제어기기의 통신망을 위한 통신보드 설계,” 한국정보통신학회, 한국정보통신학회 논문지, 제19권, 제1호, 2015, pp.185-191.

[4] 이성진, “가상화 기반 APR1400 MMIS 디지털 트윈 개발,” 대한전기학회 학술대회 논문집, 2021, pp.350-351.

[5] 우필성·김발호, “대규모 지능형 전력망의 사이버보안 위험성에 대한 평가 방법론,” 대한전기학회, 전기학회논문지, 제71권, 제3호, 2022, pp.477-487.

[6] 정성민·김태경, “다양성보호계통 사이버보안 연계 위협 분석 방안,” 디지털산업정보학회, 디지털산업정보학회 논문지, 제17권, 제1호, 2021, pp.35-44.

[7] 한국원자력통제기술원, “원자력 시설 등의 컴퓨터 및 정보시스템 보안 기술 기준,” KINAC RS-015, 2016.

[8] 한국원자력통제기술원, “원자력 시설 등의 필수 디지털자산 식별 기술기준,” KINAC RS-019, 2015.

[9] IAEA, “Computer Security Techniques for Nuclear Facilities,” Nuclear Security Series No. 17-T (Rev. 1), 2021.

[10] 김국헌·김태효·이성섭, 안전필수 시스템 제어설계, 한빛아카데미, 2021.

[11] 한국원자력안전기술원, 경수로형 원자력발전소 사용전(성능) 검사 지침서, KINS/GI-N03, 2018.

[12] 임준희·김휘강, “원자력발전소 디지털시스템 설계요건을 고려한 보안성 평가에 관한 연구,” 한국정보보호학회, 정보보호학회지, 제30권, 제2호, 2020, pp.59-63.

[13] 한국원자력연구원, SFR 원형로 NSSS 설계·검증, KAERI/RR-4306, 2017.

[14] 공명복·이상용, “ 디지털 원자로 보호시스템의 공통원인고장 분석에 관한 사례연구,” 대한산업공학회, 산업공학, 제25권, 제4호, 2012, pp.381-392..

[15] Seo-Ryong Koo, Seop Hur, Chang-Hwoi Kim, “Design Features of Reactor Protection System for SMART,” 2018 Spring Meeting of the KNS, Jeju, 2018.

[16] Han Gyu Kim, Woong Seock Choi, Se Do Sohn, “Design Improvement for the Reactor Trip Switchgear System for APR1400 Design Certification,” 2016 Autumn Meeting of the KNS, Gyeongju, 2016.

[17] Yanggyun Oh, Jinkwon Jeong, Changjae Lee,

Yoonhee Lee, “Fault-tolerant design for advanced diverse protection system,” Nuclear Engineering and Technology, Vol. 45, No. 6, 2013, pp.795-802.

[18] 원자력안전위원회고시 제2018-6호, 원자로시설의 안전등급과 등급별 규격에 관한 규정, 2018.

[19] DHS, “Common Cybersecurity Vulnerabilities in Industrial Control Systems,” 2011.

■ 저자소개 ■

정 성 민
Jung Sungmin

2020년 9월~현재
명지전문대학 교수
2014년 3월~2020년 8월
한국원자력연구원 선임연구원
2014년 2월 성균관대학교 전자전기 및 컴퓨터공학과(공학박사)

관심분야 : 산업시설보안, 제어시스템보안, 센서네트워크, 클라우드 컴퓨팅
E-mail : smjung@mjc.ac.kr

김 태 경
Kim Taekyung

2017년 9월~현재
명지전문대학 교수
2008년 3월~2017년 8월
서울신학대학교 교수
2006년 3월~2008년 2월
서일대학 교수
2005년 8월 성균관대학교 전자전기 및 컴퓨터공학과(공학박사)

관심분야 : 네트워크보안, IoT 보안, 개인정보보호, 클라우드 보안
E-mail : tkkim@mjc.ac.kr

논문접수일 : 2022년 6월 7일
수 정 일 : 2022년 6월 16일
게재확정일 : 2022년 6월 20일