디지털산업정보학회 논문지 제17권 제1호-2021년 3월
http://dx.doi.org/10.17662/ksdim.2021.17.1.035

다양성보호계통 사이버보안 연계 위협 분석 방안

정 성 민*·김 태 경**

An Analysis Measure for Cybersecurity linked Threat against Diverse Protection Systems

Jung Sungmin·Kim Taekyung

〈Abstract〉

With the development of information technology, the cybersecurity threat continues as digital-related technologies are applied to the instrumentation and control system of nuclear power plants. The malfunction of the instrumentation and control system can cause economic damage due to shutdown, and furthermore, it can lead to national disasters such as radioactive emissions, so countering cybersecurity threats is an important issue. In general, the study of cybersecurity in instrumentation and control systems is concentrated on safety systems, and diverse protection systems perform protection and reactor shutdown functions, leading to reactor shutdown or, in the worst case, non-stop situations. To accurately analyze cyber threats in the diverse protection system, its linked facilities should be analyzed together. Risk analysis should be conducted by analyzing the potential impact of inter-facility cyberattacks on related facilities and the impact of cybersecurity on each configuration module of the diverse protection system. In this paper, we analyze the linkage of the diverse protection system and discuss the cybersecurity linkage threat by analyzing the availability of equipment, the cyber threat impact of the linked equipment, and the configuration module's cybersecurity vulnerability.

Key Words : Diverse Protection System, Cybersecurity, Non-safety system, Nuclear Power Plants

Ⅰ. 서론

4차산업 혁명아래 정보통신기술의 발달은 인공지능, 사물인터넷, 클라우드, 그리고 빅데이터 등 지능과 정보기술의 융합으로 새로운 서비스를 만들고 우리에게 많은 이익을 가져다주었지만, 반대로 이것을 이용한 사이버 위협이 계속되면서 사이버보안 연구의 중요성은 더욱 커지고 있다. 특히, 국가 중요기반시설인 원자력 발전소가 사이버 공격의 목표가 되고 있는데, 이란의 부셰르 원자력 발전소의 원심 분리기의 가동을 중단시킨 2010년 스틱스넷 공격에서부터 2014년 일본 몬주 원전 해킹 시도, 2015년 해커 그룹

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

의 한국수력원자력 관련 자료 해킹, 2015년 우크라이나 발전소 공격에 따른 대규모 정전 등 원자력 발전소에 대한 사이버 공격은 계속되고 있다[1-3].

원자력 발전소는 발전 단가가 일반 화력이나 수력 발전소에 비해 낮고 친환경적이지만, 사이버 공격은 정보의 변경이나 유출뿐만 아니라, 방사능 유출 등에 따른 대규모 피해를 발생시킬 수 있으므로 사이버 공격으로부터 원자력 발전소를 보호하는 것은 중요하다. 원자력 발전소의 계측제어시스템은 방사능의 안전과 관련된 사고에 대비하기 위해 비안전 시스템과 안전 시스템으로 구성되어 있다[4]. 최근 원자력 발전소의 사이버보안에 대한 논의가 활발하게 이루어지고 있지만, 대부분 안전 시스템에 집중되어 있거나 일반적인 정보시스템의 위협을 가정하고 있다. 원자력 발전소의 비안전 시스템 중에서 다양성보호계통은 원자력 발전소의 정지 및 보호 기능 수행과 관련이 있으므로 사이버 위협을 예측하고 영향을 분석하는 것은 중요하다.

본 논문에서는 다양성보호계통의 사이버 위협을 분석하고 사이버 위협 시나리오를 확인한다. 2장에서는 원자력 발전소의 계측제어시스템과 대표적인 비안전 시스템인 다양성보호계통을 알아본다. 3장에서는 사이버 위협에 대처하기 위해 다양성보호계통 사이버보안 취약성, 구성 및 기능에 대해 정리한다. 4장에서 예측되는 사이버 공격에 대해 다양성보호계통뿐만 아니라 연계되는 설비의 위협을 확인하고 5장에서 연구내용을 요약하였다.

Ⅱ. 계측제어시스템

원자력 발전소의 설비는 안전 등급과 비안전 등급으로 나뉘는 데 안전 등급은 원자력 안전 기능에 따라 원자로 시설의 설비에 부여한 등급을 말하며 안전 등급 1, 2 및 3으로 분류한다. 또한, 비안전 등급은 안전 등급 1, 2 또는 3에 속하지 아니하는 원자로 시설의 설비에 부여한 등급을 말한다. 안전 등급 설비는 비안전 등급의 설비에 비해 설비의 신뢰성에 대한 높은 검증이 요구된다[5, 6]. 원자력 발전소 계측제어시스템은 원자력 발전소의 사고를 방지하고 사고 결과를 완화하여 원자력 발전소의 정상적인 운전을 위해 계측, 감시, 제어 기능을 수행한다. 원자력 발전소 계측제어시스템의 대표적인 안전 및 비안전 시스템은 <표 1>과 같다[7].

<표 1> 원자력 발전소 계측시스템 분류

분류	안전 시스템	비안전 시스템
계측	PI, Ex-Core	PI, Ex-Core
감시	QIAS-P	QIAS-N, IPS, NIMS
제어	ESF-CCS, RSS	P-CCS, CEDMCS, RPCS
보호	RPS, ESFAS, CPCS	DPS

안전 및 비안전 시스템을 구성하는 계측제어시스템은 그 기능에 따라 각각 계측시스템, 감시시스템, 제어시스템, 보호시스템으로 분류한다. 계측시스템은 압력, 온도, 수위, 방사능 등 원자력 발전소의 운영에 따라 변하는 상태 정보를 현장에 설치된 계측기나 센서를 통해 실시간으로 수집한다. 감시시스템은 운전원이 원자력 발전소의 운전 상태를 실시간으로 확인하여 조치할 수 있도록 주제어실의 다양한 모니터링 설비를 통해 계측시스템에서 수집한 정보를 시각적으로 제공한다. 제어시스템은 계측 시스템과 감시시스템을 통해 현장에서 수집한 안전 변수 등 공정값을 바탕으로 원자로, 제어봉구동장치, 급수, 터빈증기 우회 등 각종 설비를 제어한다. 안전해석을 통해 각 변수에 대해 설정치가 정해지고 이것은 제어를 위한 기준이 된다. 보호시스템은 안전 변수들을 실시간으로 감시하고, 변수의 값이 정해진 안전한 운전 범위에 해당하는 설정치에 미달하거나 초과하게 되면 운영 중인 원자로를 안전하게 정지시키거나 필요한 경우

에 공학적안전설비작동 신호를 보내 안전 설비를 작동하게 한다[8].

원자력 발전소는 다른 분야와는 달리 보수적인 기술을 적용함에 따라 계측제어시스템은 디지털 기술보다는 아날로그 기술이 사용되었고 제어망은 인터넷과 연결되지 않은 분리된 망을 이용하였다. 이런 이유로 일반적인 정보통신 시스템과는 달리 사이버 공격에 대한 가능성이 매우 적었고 원자력 발전소를 설계할 때 사이버보안에 대한 고려도 부족했다. 그러나 정보통신 기술의 발전은 원자력 발전소의 시스템에도 적용되어 디지털 기반의 제어기기, 통신망, 소프트웨어 등 정보통신 관련 디지털 기술이 사용되면서 원자력 발전소에서 사이버 공격의 성공 가능성을 완전히 배제하기는 어려워졌다[9].

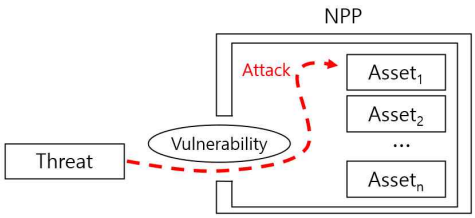
최근 사이버보안 연구의 대부분은 원자력 발전소의 정지 및 보호 기능과 밀접한 관련이 있는 발전소보호계통(PPS, Plant Protection System)과 같은 안전 시스템에 집중되어 있다. 하지만 비안전 시스템 중에서 다양성보호계통(DPS, Diverse Protection System)은 그 기능에 따라 원자력 발전소를 정지시킬 수 있는 기능이 있다. 따라서 사이버 공격의 영향으로 다양성보호계통의 제어시스템을 조작하거나 물리적으로 오류를 일으켜 정지를 위한 구간에서 제대로 동작하지 않는다면 큰 사고가 발생할 수 있다.

다양성보호계통은 10CFR50.62의 설계요건을 만족하기 위해 원자로가 정지되어야 하는 조건일 때 정지되지 않는 정지불능 예상과도상태(ATWS, Anticipated Transient Without Scram)에 대한 위험을 완화할 수 있도록 원자력 발전소의 안전 변수를 입력받아 원자로정지 및 터빈정지와 보조급수 작동 기능을 수행한다[10]. 이를 위해 다양성보호계통은 센서 출력부터 최종 작동까지 안전 등급인 발전소보호계통과 독립적이며 다양성을 갖춘 설비로 구성한다. 다양성보호계통은 비안전 등급의 두 개의 채널로 구성되며 예상운전사건(AOO, Anticipated Operational Occurrence)의 조건에서도 정상적으로 작동해야 하고 내진범주 II에 따른 물리적인 건전성을 유지해야 한다. 그리고 발전소보호계통과의 독립성을 만족하기 위해 비안전 등급의 필수모선전원공급계통(VBPSS, Vital Bus Power Supply System)의 전원을 사용하고 안전 시스템과 전기적, 물리적으로 격리되어 설치한다[11, 12].

Ⅲ. 다양성보호계통 사이버보안 위협

3.1 다양성보호계통 취약성

취약성은 <그림 1>과 같이 사이버 공격의 도구로 외부의 위협이 목표로 하는 시스템에 악의적인 영향을 줄 수 있도록 하는 도구가 되고, 위협은 목표로 하는 시스템에 악의적인 영향을 주는 사이버 공격을 의미한다[13].



<그림 1> 취약성

다양성보호계통은 디지털 기반의 제어기기와 통신망을 사용하기 때문에 사이버 위협에 취약하고, 안전 시스템인 발전소보호계통과 다양성을 위하여 설계된 계통이기 때문에 사이버 공격으로 인해 구성요소의 기능 수행이 지연되거나 악의적으로 조작된 변수가 입력된다면 원자로 정지 및 정지 불능과 같은 잘못된 결과를 가져올 수 있다. 다양성보호계통의 사이버 위협에 대비하기 위해 다양성보호계통을 포함한 계측

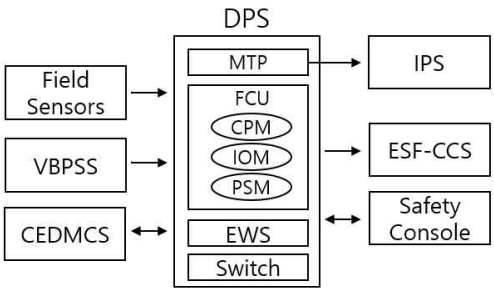
제어시스템을 대상으로 침투 시험을 통해 취약성을 확인하는 것이 필요하지만 오동작에 따른 피해가 클 수 있으므로 직접 해당 자산을 대상으로 침투 시험을 수행하는 것은 어렵다. 따라서 사이버 위협을 효율적으로 분석하기 위해 테스트베드를 통해 다양한 사이버 취약성에 대해 정량화된 사이버 위협을 확인해야 한다[14].

테스트베드와 관련하여 사이버 위협 시나리오를 작성하기 위해 다양성보호계통의 구성과 기능을 분석하고 다양성보호계통과 물리적 또는 논리적으로 연결된 다른 계통과의 연계 사항을 파악해야 한다. 그리고 보안에 취약한 부분을 확인하고 위험을 정량화하여 분석된 결과를 바탕으로 사이버 위협의 대응을 마련해야 한다.

3.2 다양성보호계통 구성 및 기능

다양성보호계통은 두 개의 다양성보호계통 캐비닛과 EWS(Engineering Workstation System)로 구성된다. 다양성보호계통은 비안전 등급 제어기(FCU, Field Control Unit)를 이용하는데, 캐비닛에는 비안전 등급 제어기를 포함하여 보수시험반(MTP, Maintenance and Test Panel), 전원공급장치(PDU, Power Distribution Unit), 그리고 제어망, 정보망을 위한 스위치로 구성된다.

비안전 등급 제어기는 제어 신호 및 정보 신호의 입력과 출력을 처리하고, 원자로정지를 위해 비교논리 기능과 동시논리 기능을 수행한다. 비교논리 기능은 입력된 안전 변수를 바탕으로 고정된 설정치와 비교하여 원자로 정지를 결정하거나 외부로부터 주어진 상태를 사용하여 원자로 정지를 결정한다. 동시논리 기능은 두 개의 채널 중 다른 채널로부터의 결정된 정지신호를 받아 2/2 동시논리를 적용하여 최종 원자로 정지를 결정한다. 또한, 비안전 제어기는 신호처리, 논리 수행, 이중화, 시각 동기, 이벤트 처리, 감시, 그리고 진단 기능을 수행한다. 신호 처리 기능은 아날로그 및 디지털 신호를 구분하여 처리 및 신호 정보의 업데이트 주기를 설정하고, 논리 수행 기능은 제어기에 프로그래밍 언어 및 프로세스 모듈에 로딩된 논리를 수행하는 주기를 결정한다. 이중화 기능은 CPU나 입출력 이중화를 지원하여 절체되는 조건 및 수행 시간을 확인하고, 시각 동기 기능은 네트워크를 통해 내부적으로 연계된 장비의 시간 동기화를 수행한다. 이벤트 처리 기능은 내부적으로 발생하는 이벤트에 대해 전송주기 및 방식, 처리 용량 등을 확인하고 감시 기능은 내부 통신망을 감시하여 데이터의 전송 경로, 크기, 전송 속도 등을 확인한다. 마지막으로 진단 기능은 하드웨어 및 소프트웨어에 대해 전원, 통신, CPU, 입출력 모듈 등의 상태를 진단 확인하는 기능이다.



<그림 2> 다양성보호계통 주요 연계 사항

<그림 2>는 다양성보호계통과 물리적 또는 논리적으로 데이터를 주고받는 다른 계통과의 주요한 연계 사항을 보여준다[7, 14]. 네트워크 관점에서 다양성보호계통은 제어망과 정보망을 분리하고 메인망과 백업망으로 이중화하여 송수신되는 신호의 신뢰성을 확보하였다. 네트워크를 이용하여 여러 계통과 단방향 또는 양방향으로 데이터를 송수신하는데, 현장 센서(Field sensor), 제어봉구동장치제어계통(CEDMCS, Control Element Drive Mechanism Control System),

그리고 필수모선전원공급계통과 같은 일부 구간은 단방향 통신망이나 아날로그 실배선을 사용하기 때문에 사이버 위협에 대한 영향이 적다. 그러나 다양성보호계통이나 공학적안전설비-기기제어계통(ESF-CCS, Engineered Safety Feature- Component Control System)의 경우는 디지털 기반의 제어기기와 통신망을 사용하고 스위치, 안전제어반(Safety console), 보수시험반, 그리고 정보처리계통(IPS, Information Processing System)의 자산은 디지털 서버와 컴퓨터, 디지털 기반의 통신망을 사용으로 사이버 위협에 취약할 수 있다.

Ⅳ. 다양성보호계통 연계 위협 분석

다양성보호계통의 취약점을 분석하기 위해 구성 자산에 대해 먼저 위험(Risk)을 자산의 가용성(Availability), 연계 위협(Threat), 사이버 취약성(Vulnerability)을 수식 (1)과 같이 정의한다.

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

일반적으로 산업제어시스템은 기밀성이나 무결성보다는 가용성이 우선순위가 높다. 따라서 다양성보호계통의 주변 구성 자산이 가용성의 침해를 받는 경우 원자력 발전소에 얼마나 영향을 줄 수 있는지 <표 2>와 같이 정량적인 점수를 부여한다.

<표 2> 자산의 중요도 기준

Level	Criteria	Value
High	가용성 침해시 원자력 발전소의 정지에 중요한 영향을 미친다.	0.9
Medium	가용성 침해시 원자력 발전소의 정지에 부분적으로 영향을 미친다.	0.5
Low	가용성 침해시 원자력 발전소의 정지에 미미하게 영향을 미친다.	0.1

다양성보호계통과 연관된 자산에 대해 디지털화 여부, 이중화 구성, 명령 입력 수단을 고려하여 원자력 발전소의 영향을 분석하면 <표 3>과 같다. 현장 센서나 필수모선전원전원공급계통과 같은 자산은 구성과 기능에서 원자력 발전소의 정지에 미치는 영향이 다른 자산에 비해 미미하다. 그리고 보수시험반이나 정보처리계통은 발전소 정지에 부분적으로 영향을 미칠 수 있다. 마지막으로 제어봉구동장치제어계통, 공학적안전설비-기기제어계통, 그리고 안전제어반은 원자로의 정지와 직접적인 연관이 있으므로 가용성의 침해로 원자력 발전소의 정지 기능에 큰 영향을 미칠 수 있다.

<표 3> 원자력 발전소에 대한 자산의 영향

Asset	Impact
Field-Sensor	Low
VBPSS	Low
CEDMCS	High
MTP	Medium
IPS	Medium
ESF-CCS	High
Safety Console	High

다음으로 고려해야 할 사항은 자산 간의 연계 위협이다. 하나의 자산에 대해 사이버 위협의 가능성이 작다고 해서 전체적인 시스템에 대한 사이버 위협 또한 낮다고 할 수 없다. 낮은 사이버 위협을 결합하였을 때 큰 영향을 미칠 수 있기 때문에 자산간 연계 위협에 대해 분석하는 것은 중요하다.

<표 4>는 사이버 공격이 성공하였을 때 자산 간의 제어망, 정보망의 사용 여부, 통신망 종류, 디지털 혹은 아날로그 신호 연계 등을 확인하여 사이버 공격의 영향으로 해당 자산과 연결된 다른 자산에 미치는 영향을 분석하여 자산의 연계된 자산 간의 사이버 위협에 대해 정량적인 점수를 부여하였다.

<표 4> 자산의 연계 위협 기준

Level	Criteria	Value
High	사이버 공격의 영향으로 해당 자산과 연결된 자산에 중요한 영향을 미친다.	0.9
Medium	사이버 공격의 영향으로 해당 자산과 연결된 자산에 부분적인 영향을 미친다.	0.5
Low	사이버 공격의 영향으로 해당 자산과 연결된 자산에 미미하게 영향을 미친다.	0.1

다음으로는 <표 4>의 기준에 따라 다양성 보호계통에서 연계된 자산의 방향, 혹은 반대 방향으로 사이버 공격에 따른 영향을 분석하였다. 일반적으로 현장 센서나 필수모선전원공급계통의 경우는 아날로그 실배선으로 이루어져 있으므로 양단의 사이버 공격으로 인한 영향은 미미하다고 할 수 있다. 정보처리계통은 다양성보호계통과 보수시험반을 통해서 데이터를 주고받기 때문에 양단의 사이버 공격의 영향은 부분적이다. 단방향의 통신망 사용으로 제어봉구동장치제어계통이나 공학적안전설비-기기제어계통의 경우는 다양성보호계통이 사이버 공격으로 큰 영향을 받을 수 있는 자산이나, 반대의 경우 제어봉구동장치제어계통이나 공학적안전설비-기기제어계통이 다양성보호계통에 미미한 영향을 줄 것으로 판단된다. 마지막으로 보수시험반이나 안전제어반의 경우 디지털 기반의 컴퓨터나 기기를 사용하고, 다양성보호계통 간 송수신 데이터가 있으므로 연계되는 사이버 위협이 양단에 모두 크다.

<표 5> 연계된 자산의 사이버 공격 영향성

Asset	From DPS (DPS → Asset)	To DPS (Asset → DPS)
Field-Sensor	Low	Low
VBPSS	Low	Low
CEDMCS	High	Low
MTP	High	High
IPS	Medium	Medium
ESF-CCS	High	Low
Safety Console	High	High

마지막으로 다양성보호계통을 구성하는 모듈에 대해 사이버 위협을 분석해야 한다. 미국 국토안보부(DHS)에서는 산업제어시스템의 사이버 위협을 분류하고 소프트웨어 관련 취약성을 제안하였다[15]. <표 6>은 미국 국토안보부에서 제안한 산업제어시스템의 일반적인 소프트웨어 취약성으로 원자력 발전소의 다양성보호계통을 구성하는 자산에도 적용할 수 있다. 일반적으로 다음과 같이 8가지 취약성에 대해 논의한다.

<표 6> 원자력 발전소 설비 소프트웨어 취약성

Classification	Security Vulnerability
V_1	Improper Input Validation
V_2	Poor Code Quality
V_3	Permissions, Privileges, and Access Controls
V_4	Improper Authentication
V_5	Insufficient Verification of Data Authenticity
V_6	Cryptographic Issues
V_7	Credentials Management
V_8	ICS Software Security Configuration and Maintenance

① 부적절한 입력값 검증

부적절한 입력값과 관련된 취약점은 버퍼 오버플로우나 경계검사 부족 등 입력값 크기에 대한 검증이 부족해서 잘못된 결과가 발생하는 경우이다. 서비스 거부(DoS) 공격도 여기에 해당하며 시스템에 대한 서비스 처리가 지연되는 경우가 발생한다.

② 안전하지 않은 코드 사용

보안에 취약한 함수를 사용하는 경우에 시스템에 인증 정보를 저장하거나, 널포인터의 역참조 문제가 발생한다.

③ 허용, 권한 및 접근제어 취약점

시스템의 접근제어가 제대로 수행되지 않으면 비

인가자의 데이터 접근 및 실행을 할 수 있으며 부적절하게 권한을 실행하여 공격자가 권한 상승으로 시스템에 접근할 수 있다.

④ 부적절한 인증 취약점

인증과 관련하여 인증 과정이 없거나 관리가 미흡한 경우로 인증을 우회하여 권한에 한 적절한 검증 없이 시스템에 접근이 가능해지거나 권한 노출 및 데이터의 유출 가능성이 있다. 이 취약점은 중간자 공격이나 ARP 스푸핑을 가능하게 한다.

⑤ 불충분한 데이터 무결성 검증

데이터에 대한 무결성 검사가 부족하면 외부에서 다운로드 받은 데이터에 대한 오류를 확인하기 어렵고 시스템에서 검증되지 않은 악의적인 프로그램이 수행될 수 있다.

⑥ 암호화 적용

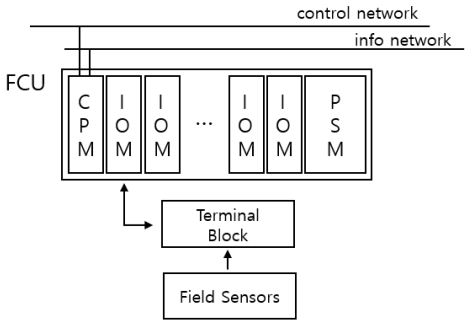
보안 강도가 약한 암호 알고리즘 사용하여 암호 추측 가능 및 암호 유출의 우려가 있다. 그리고 중요한 데이터를 평문으로 보내는 경우 데이터가 유출될 수 있으며 자체 프로토콜에 보안 기능이 부족한 경우 사이버 위협에 취약하다.

⑦ 인증 정보 관리

응용 프로그램이 인증과 관련된 중요 정보를 인증되지 않은 방법으로 보관하거나 소스 코드 내에 인증 관련 정보를 저장하는 경우에 사이버 위협에 취약하다.

⑧ 소프트웨어 보안패치

시스템에서 보안 패치가 이루어지지 않고 기본적인 설정을 그대로 사용하여 시스템 내에서 불필요한 서비스가 실행하는 경우 실행되는 서비스 및 응용 프로그램이 공격자에 의해 악용될 수 있다.



<그림 3> FCU 구성

각 취약성은 다양성보호계통의 구성 모듈에 적용하여 영향을 분석한다. 다양성보호계통은 비안전 제어기, 제어망과 정보망을 위한 스위치, 그리고 전원공급장치로 이루어져 있고 비안전 제어기는 세부적으로 CPU 모듈(CPM), 입출력 모듈(IOM), 그리고 전원공급모듈(PSM)로 이루어져 있다. 그리고 다양성보호계통의 제어로직 설계 및 계통 시스템의 구성 및 설정, 디버깅 기능, 시스템 상태감시 기능 등을 수행하는 EWS이 있다. <그림 3>은 비안전 제어기의 구성요소를 보여준다.

다양성보호계통을 구성하는 각 모듈이 해당 소프트웨어 취약성으로 인해 원자력 발전소에 어느 정도 영향을 줄 수 있는지 정해야 한다. <표 7>은 각 구성요소를 대상으로 사이버 취약성이 시스템의 오동작이나 정지에 미치는 영향을 기준으로 정량적인 수치를 나타낸다.

<표 7> 자산의 사이버영향 기준

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

<표 8>은 비안전 제어기 각 구성 요소의 소프트웨어 취약성 관련 사이버 위협 영향을 나타낸다. 전원공급모듈은 일반적으로 사이버 위협에 대해 미미한 영향을 보인다. EWS과 CPU 모듈이 사이버 공격에 중요한 영향을 보이고, 입출력 모듈과 스위치의 경우 부분적인 영향을 미치는 것으로 판단된다. 최종 연계 위협에 대해 분석을 하는 경우에 해당 구성요소에 대한 사이버 취약성의 영향성을 전체적으로 판단하기 위해 평균값을 이용한다.

<표 8> 다양성보호계통 사이버보안 영향성

Module	V_1	V_2	V_3	V_4	V_5	V_6	V_7	V_8
CPU Module	H	M	M	H	L	H	M	M
I/O Module	H	M	M	L	H	L	L	L
PSM	L	L	L	L	L	L	L	L
EWS	M	M	H	H	M	L	H	H
Switch	L	L	H	H	L	L	L	M

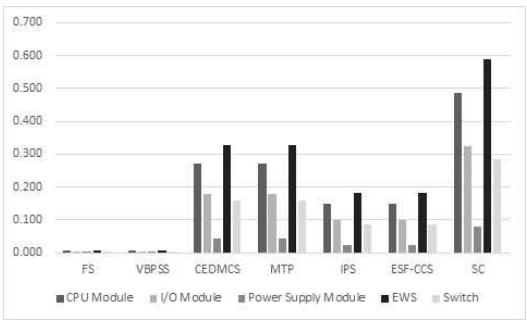
<표 9>는 다양성보호계통에 예상되는 사이버 공격에 대해 구성 요소별로 가용성, 연계 위협 그리고 사이버 공격 영향성을 이용하여 식 (1)에 따라 개별적인 위험도를 계산하고 각 구간에 대해 양방향으로 연계된 자산에 대한 위험의 평균값을 적용하여 구간별로 사이버보안 영향성을 적용하여 구간별 위험도를 계산한 값이다.

<표 9> 다양성보호계통 구간별 위험도

Metric	Field-Sensor	VBPSS	CEDMCS	MTP	IPS	ESF-CCS	Safety Console
CPM	0.006	0.006	0.270	0.270	0.150	0.150	0.486
IOM	0.004	0.004	0.180	0.180	0.100	0.100	0.324
PSM	0.001	0.001	0.045	0.045	0.025	0.025	0.081
EWS	0.007	0.007	0.328	0.328	0.182	0.182	0.590
Switch	0.004	0.004	0.158	0.158	0.088	0.088	0.284

다양성보호계통과 연계된 안전제어반의 경우 CPU 모듈, 입출력 모듈과 EWS 간에 사이버보안 관련 위험이 다른 구간들보다 크다고 할 수 있다. 공학적안전설비-기기제어계통이나 정보처리계통의 경우는 CPU 모듈과 EWS 간에 사이버 위협이 크다고 판단된다. 보수시험반과 제어봉구동장치제어계통은 EWS 간 사이버 위협이 매우 컸으며, 현장 센서나 필수모선전원공급계통의 경우는 아날로그 사용의 특성상 사이버 위협이 그리 크지 않다고 판단된다.

<그림 4>와 같이 각 구간의 위험값을 비교하면 안전제어반과 다양성보호계통의 EWS의 연계 부분이 가장 높았고, 따라서 이 부분이 사이버 위협이 제일 크다고 판단할 수 있다. 또한 EWS의 관점에서 다른 연계 사항들과의 위험을 보면 보수시험반 및 제어봉구동장치제어계통의 구간에서 위험이 큰 것을 알 수 있다.



<그림 4> 다양성보호계통 구간별 위험도

따라서 다음과 같은 시나리오의 경우에 다양성보호계통에서 가장 큰 사이버 위협이 될 수 있다. 접근제어 취약점, 부적절한 인증 취약점, 인증 정보 관리, 그리고 소프트웨어 보안패치가 미흡하여 사이버 공격으로 다양성보호계통을 구성하는 EWS가 오동작을 일으킨다. EWS 오동작은 안전제어반과의 사이버 위협에 대한 결합으로 위험이 더욱 커지고, 제어봉구동장치제어계통과 보수시험반과 같은 연계 자산에 사

이버 위협을 통한 시스템 오류 및 서비스 지연을 일으킨다. 결국 원자력 발전소는 정지 또는 정지 불능 상태가 되면서 큰 피해를 가져올 수 있다.

Ⅴ. 결론

최근 원자력 발전소 계측제어시스템의 사이버 위협에 대비하기 위해 다양한 연구가 진행되고 있다. 계측제어시스템은 안전과 비안전 시스템으로 구분되는데, 비안전 시스템 중에서 다양성보호계통은 원자력 발전소를 정지시킬 수 있는 보호 기능이 있다. 따라서 사이버 공격의 영향으로 다양성보호계통의 구성 모듈을 조작하거나 물리적으로 오류를 일으켜 정지를 위한 구간에서 제대로 동작하지 않는다면 큰 피해를 가져올 수 있다.

다양성보호계통의 사이버 위협을 분석하기 위해 사이버보안 취약성을 확인할 수 있는데, 다양성보호계통만을 분석하는 방법보다는 다양성보호계통의 연계를 분석하고 연계되는 설비가 원자력 발전소에 미치는 영향의 정도를 판단한다. 그리고, 연계되는 장비와 다양성보호계통 간에 위협을 분석하여 위험을 전반적으로 분석 판단해야 한다. 본 논문에서는 다양성보호계통과 연계되는 장비 간의 위협 분석을 통해 안전제어반과 다양성보호계통의 구성요소인 EWS 간의 위험이 제일 크다는 것을 확인하였고 구간별로 위협이 되는 요소를 분석하고 대응책을 마련할 수 있도록 정량적인 정보를 제공하였다.

추후 해당 영향성을 분석하는 경우 사용자의 경험에 의존하는 위험 정도의 오차를 줄일 수 있도록 일반적인 정보통신 분야에서 기검증된 취약성 정량화 방법을 활용하여 계통별로 최적화된 사이버보안 대응 방안을 마련하고자 한다.

참고문헌

[1] 송동훈·임현종·김상우·류진호·신익현, “사이버보안 위협평가를 통한 원자력시설 등 중요시설 대상 최신 사이버 위협 사례 분석 연구,” 한국정보보호학회, 정보보호학회지, 제28권, 제2호, 2018, pp.51-60.

[2] Seungmin Kim, Gyunyoung Heo, EnricoZio, Jinsoo Shin, Jaegu Song, “Cyber attack taxonomy for digital environment in nuclear power plants,” Nuclear Engineering and Technology, Vol. 52, No. 5, 2020, pp.995-1001.

[3] 엄익채, “핵심기반시설 사이버 보안 평가 모델링 기법 연구,” 한국디지털정책학회, 디지털융복합연구지, 제17권, 제8호, 2019, pp.105-113.

[4] 정성민, “원전 무선 센서 네트워크에 적합한 클러스터 헤드 체인 라우팅 프로토콜,” 디지털산업정보학회, 디지털산업정보학회 논문지, 제16권, 제2호, 2020, pp.61-68.

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

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

[7] KHNP, “APR1400 Design Control Document,” NRC ADAMS, 2018, pp.7.1-43

[8] Jungwoon Lee, Cheolkwon Lee, Jaegu Song, and Dongyoung 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.

[9] 권기춘, “원전 계측제어시스템 현재와 미래,” 대한전자공학회 ICS´ 2016 정보 및 제어심포지엄 논문집, 서울, 2016, pp.46-62.

[10] USNRC, “Section 50.62 Requirements for

Reduction of Risk from Anticipated Transients without Scram(ATWS) Events for Light-Water-Cooled Nuclear Power Plants", 10CFR50, 1996.

[11] 한국원자력안전기술원 규제기준, "제8장 계측제어계통," KINS/RS-N08.00, 2015.

[12] 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.

[13] 강동주·이종주·이영·이임섭·김휘강, "전력 SCADA 시스템의 사이버 보안 위험 평가를 위한 정량적 방법론에 관한 연구," 한국정보보호학회, 정보보호학회논문지, 제23권, 제3호, 2013, pp.445-457.

[14] 정성민, "원전 다양성 보호계통 사이버보안 테스트베드 설계," 한국정보처리학회, 2020온라인 춘계학술발표대회 논문집, 제27권, 제1호, 2020, pp.292-294.

[15] 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 정보전자과 교수
2005년 8월 성균관대학교 전자전기 및 컴퓨터공학과(공학박사)

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

논문접수일 : 2021년 3월 3일
수 정 일 : 2020년 3월 10일
게재확정일 : 2021년 3월 17일