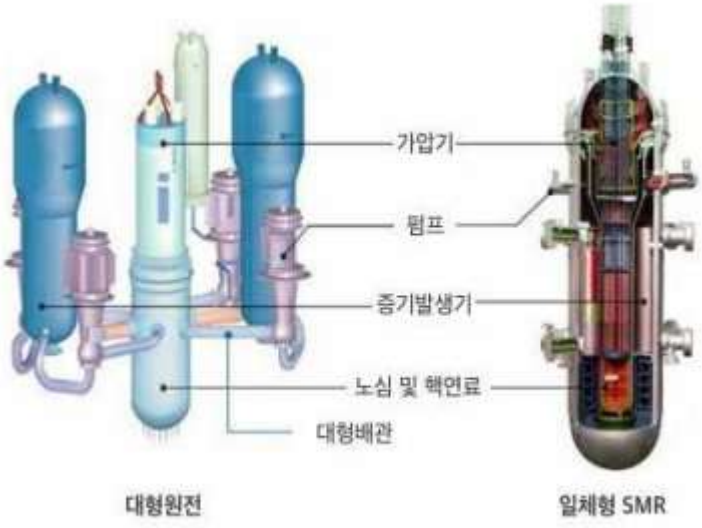
Ⅰ. SMR 개요

전 세계적으로 에너지 안보와 기후변화에 대응하기 위해 탄소중립 목표를 설정하고 에너지 분야에서 다양한 변화를 시도하고 있다. 이에 따라, 탄소 배출이 많은 화석연료 기반 화력 발전의 대안으로 태양광 및 풍력을 중심으로 하는 재생에너지 산업이 확대되고 있으며, 원자력 발전도 국제 논의를 통해 대안으로 부각되었다. 원자력 발전은 재생에너지의 한계인 간헐성을 극복하고 국가에 필요한 에너지를 안정적으로 공급할 수 있는 대안으로 평가받고 있다. 그러나 원자력 발전소는 후쿠시마 원전 사고처럼 치명적인 사고가 발생할 경우, 막대한 인명 피해와 환경 파괴를 초래할 수 있는 위험성을 안고 있다. 이에 따라 원자력 산업은 단순한 전력 생산을 넘어, 안전성이 향상된 차세대 원자로 개발을 목표로 연구개발을 추진하고 있다. 이러한 배경 속에서 소형모듈원전(Small Modular Reactor, SMR) 개발이 본격화되면서, 세계 각국에서 조기 상용화를 목표로 시장 선점 경쟁이 치열하게 진행되고 있다.

SMR은 공장 제작형 모듈 기술을 이용한 전기출력 300MWe 이하 원자로이다[1]. 국제 원자력 기구(International Atomic Energy Agency, IAEA)는 300MWe 이하인 원자로를 소형원자로로 분류하며, 700MWe 이하인 원자로를 중형원자로로 분류한다. 10Mwe 이하일 경우에는 초소형 원자로(Micro Modular Reactor, MMR)으로 분류한다. SMR은 모듈형 제작 방식, 저용량, 표준화로 인해 건설 기간을 3년 이하로 축소시킬 수 있으며 건설 비용을 낮출 수 있다. 설계 상 모듈 형태는 연결 부위에서 방사능이 방출될 가능성을 낮추며, 피동형 안전설계를 적용하여 인간의 개입 없이 자동으로 냉각할 수 있어 안전성이 높다. 또한, 대규모 냉각수를 필요로 하지 않아 오지에 설치될 수 있으며, 부하 추종 운전이 가능함에 따라 재생에너지를 보완하는 기능을 수행한다[2]. [그림 1]과 [표 1]은 대형원전과 SMR을 비교한 것이다.



<자료> 서울시 녹색산업지원센터, 2024 녹색산업 인사이트 insight 소형모듈원자로(SMR), 2024.09.

[그림 1] 대형원전과 일체형 SMR의 비교

[표 1] 대형원전과 SMR 비교

구분	대형원전	SMR(소형모듈원전)
안전성	체르노빌, 후쿠시마 등 대형사고 발생 이력이 있음	소형화, 피동형으로 사고 발생위험을 낮춤
운영 탄력성	대용량 출력이 고정됨 (기저부하)	Scalable & 부하추종운전이 가능함 (분산전원 및 신재생에너지 백업 전원으로 활용 가능성)
건설 Risk	현장작업의 비중이 높음 (건설비 Risk ↓)	공장작업의 비중이 높음 (건설비 Risk ↑)
응용 분야	발전용	담수, 수소생산, 정유, 선박추진용

<자료> 에너지경제연구원. 2021.10.22 『세계원전시장 인사이트』, p.6. 그림 재인용

SMR은 기존 대형원전에 비해 안전성, 경제성, 유연성 측면에서 여러 가지 장점을 갖는다. 피동 안전 시스템과 단순화된 일체형 설계를 적용하여 배관 파단 사고 등의 가능성을 최소화할 수 있다. 또한, 모듈형 설계를 통해 다수의 모듈을 동시에 또는 단계적으로 설치할 수 있어 시공 작업을 크게 줄일 수 있다.

SMR은 대형원전에 비해 절반 이하의 부지에서도 건설이 가능하며, 안전성이 강화됨에 따라 주변 대피 구역을 최소화할 수 있어 기존 화력발전소 부지에도 도입이 가능하다. 또한, 태양광 및 풍력과 같은 신재생에너지의 간헐성을 보완하기 위해 부하 추종 운전(Load Following) 기술을 적용하여 출력 조절이 가능하다. 뿐만 아니라, SMR은 전력 생산뿐만 아니라 수소 생산, 공정열 활용, 지역 난방, 해양 탐사 등 다양한 용도로 활용될 수 있도록 설계된다.

이처럼 SMR은 차세대 원자로로서, 작은 규모와 높은 안전성을 바탕으로 다양한 이점을 제공할 것으로 기대된다. 그러나 SMR의 상용화가 본격적으로 이루어질 경우, 이들 시스템에 대한 사이버공격의 위험성도 증가할 가능성이 있다. 특히, SMR은 원격 운전 및 자동화 기술 활용을 고려하고 있기 때문에, 시스템에 대한 공격자의 접근 가능성이 높아질 수 있다. 이러한 취약점이 악용되면 전력 공급의 안정성에 심각한 영향을 미칠 뿐만 아니라, 원자력 사고로 이어질 수 있다. 따라서 SMR 개발과 도입에 앞서 사이버보안의 중요성을 더욱 강조해야 하며, 국가 에너지 안보와 공공 안전을 보호하기 위해 반드시 설계 초기 단계에서부터 사이버보안 대책을 고려해야 한다. 사이버보안은 단순한 기술적 방어를 넘어 SMR의 신뢰성과 안전성을 보장하는 필수 요소이며, 이를 통해 SMR의 성공적인 상용화와 시장 경쟁력 확보가 가능할 것이다.

II. 해외/국내 SMR 사업 추진 현황

현재 북미, 유럽을 중심으로 전세계 70여개 업체가 SMR을 경쟁적으로 개발 중이다. 미국은 SMR 기술과 관련하여 가장 앞섰다고 평가받으며, NuScale Commission 社, Terra Power 社, X-Energy 社 등 여러 개발사가 독자적인 노형 설계의 모델을 개발 중이다. 이에 미국 원자력규제기관(Nuclear Regulatory Commission, NRC)는 NuScale Commission 社에서 개발한 SMR에 대해 표준설계인증을 승인하였으며, 미국 서부지역의 전력공급을 비영리 기반으로 하는 Utah Associated Municipal Power System(UAMPS) 지역 공공기관의 자금을 활용하여 Idaho 주에 Nuscale 발전소를 2026년까지 건설할 계획임을 발표하였다[3].

<자료> 에너지경제연구원. 2021.10.22『세계원전시장 인사이트』, p.6. 그림 재인용

[그림 2] Nuscale SMR 개념도

러시아는 국영기업인 Rosatom 社를 중심으로 기술개발을 추진하고 있으며, 설계사인 OKBM 社는 다양한 전기 출력 규모의 총 5개 해상용 SMR을 보유하고 있으며, 선박・산업용 MMR을 포함하는 17개의 SMR 모델을 개발 중이다[4].

중국은 경제 분야 국가최고계획인 '국가5개년발전계획'을 토대로 중국의 대표 경수형 SMR인 ACP100 연구개발을 비롯하여 SMR 관련 지원정책을 수립하였으며, 이후 지속적으로 일관된 국가전략 및 범정부적 접근방식을 채택하고 있다.

캐나다는 연방정부의 'SMR 로드맵', '국가 행동계획'을 기반으로 SMR 개발 및 배치를 지원하고 있으며, SMR 연구개발 및 실증을 위해 4년간 2960만 캐나다 달러의 예산을 투입하여 SMR 배치에 집중하고 있다. 또한, 캐나다 온타리오 주에서

는 캐나다 최초로 SMR 건설 프로젝트를 추진 중이다.

유럽 국가 중 대표적으로 영국과 프랑스에서 SMR 사업 지원을 가속화하고 있으며, 영국은 원자력산업협의회(Nuclear Industry Council)를 중심으로 SMR 개발 및 상용화를 지원하고 있다. 프랑스는 '프랑스 2030' 계획에서 SMR 계획을 포함하는 원자력 부문에 2030년까지 10억 유로 투자를 발표하는 등의 SMR 개발에 집중하고 있다.

대한민국도 SMR 사업에 대한 추진을 가속화하고 있는 것은 마찬가지이다. 국내에서는 한국원자력연구원, 한국전력기술, 한국수력원자력 등이 대표적으로 SMART(System-integrated Modular Advanced Reactor), BANDI-60, 혁신형 SMR(i-SMR)과 같은 기술들을 개발 중이다.

[표 2] 주요 국내 기관의 SMR 프로젝트 현황

기관명	모델	현황
한국원자력연구원	SMART 100MWe 경수로	▪ 세계 최초 SMR 표준설계인증 획득('12) ▪ 사우디아라비아와 2기 건설 고려 MOU 체결('15), 관련 기술개발협력 협정 체결('19)
한국전력기술	BANDI-60 60MWe 해상부유식 가압경수로	▪ 한국조선해양과 공동으로 부유식 해상원전 바지선을 설계하여 미국선급협회로부터 원칙 승인을 받음 ▪ 개념설계를 마치고 기본설계 진행중
한국수력원자력	i-SMR	▪ 표준설계 개발 추진 중, '28년까지 표준설계인가 획득 후 '30년대 글로벌 시장 진출 목표

<자료> 서울시 녹색산업지원센터, 2024 녹색산업 인사이트 insight 소형모듈원자로(SMR), 2024.09.

또한, 국내 주요 기업인 두산에너빌리티, 삼성중공업, 현대건설, SK그룹 등은 미국의 주요 SMR 개발 기업들과 공동 투자·연구, 설계·제작, 건설 등 다양한 분야에서 협력하며 프로젝트를 추진하고 있다.

국내에서는 SMR 사업에 대한 정책 또한 활발히 추진되고 있다. 2022년에는 한국

형 녹색분류체계에 원전을 포함하였으며, 시장 조기 선점을 목표로 i-SMR 개발 완료 계획을 수립하고 관련 정책을 추진하고 있다. 또한, 2024년 6월에는 '차세대 원자력 확보를 위한 기술 개발 및 실증 추진방안(안)'을 발표하여, SMR을 비롯한 차세대 원자로 기술 개발과 시장 주도권 확보를 위한 지원 방향을 제시하였다.

[표 3] 한국의 SMR 관련 정책

시기	정책	내용
'21.12	제6차 원자력진흥종합계획('22~'26) 의결	▪ 기본방향으로 'SMR 신시장 개척과 원전 수출시장 확장' 제시 ▪ 4대 목표 12대 정책방향 중 하나로 '4. 선도적 기술혁신과 정책지원으로 미래 원전시장 선점' 제시, 기술혁신에 i-SMR 개발 포함
	제6차 원자력연구개발 5개년 계획('22~'26) 발표	▪ '원자력시장 체제개편에 대비한 연구개발 본격 추진' 명시 ▪ 원자력 R&D 5대 분야 중 하나로 SMR 선정, 주요 내용으로 혁신형 SMR 표준설계 및 기술검증을 통한 핵심기술 확보, 미래성장동력 발굴을 위한 SMR 원천기술 개발, 원자력 에너지효율 혁신 명시
'22.10	12대 국가전략기술 발표	▪ 차세대 원자력을 포함시켜 국가전략기술 프로젝트로 추진
'23.7	'혁신형 소형모듈원전(i-SMR) 기술개발사업' 공식 출범	▪ 글로벌 시장에서 경쟁할 수 있는 안전성·경제성을 갖춘 i-SMR(모듈당 170MWe)을 개발, '28년까지 표준설계인가 획득을 목표로 23~28년간 3,992억 원 투자 예정
'24.2	'2024 원자력안전위원회 주요정책 추진계획' 발표	▪ 안전성 확보를 위한 규제기반 선제적 마련의 일환으로 예산 67억 8000만원 확보('23년 대비 대폭 증액)), 「SMR 규제연구 추진단」 운영으로 검증기술 마련 속도
'24.6	'차세대 원자력 확보를 위한 기술개발 및 실증 추진방안(안)' 발표	▪ 세계 차세대 원자로 시장 대응을 위해 총 예산 2조 4,810억 원(국비 1조 6,490억원, 민간 8,320억원) 규모로 민·관 합동으로 기술개발 및 실증까지 지원

<자료> 서울시 녹색산업지원센터, 2024 녹색산업 인사이트 insight 소형모듈원자로(SMR), 2024.09.

현재 SMR은 개발 단계의 기술로, 상용화된 사례는 단 3기에 불과하지만, 전 세계적으로 시장 확장에 대한 기대가 높아지고 있다. 특히 미국, 러시아, 중국을 중심

으로 18개국에서 70여 개의 SMR 설계 및 개발이 진행 중이다. 우리나라 정부는 아직 SMR 기술 개발 단계에 머물러 있으며, 실증 단계에는 진입하지 못한 상황이다. 그러나 우리나라 정부는 2024년 6월에 '차세대 원자력 확보를 위한 기술 개발 및 실증 추진방안(안)'을 발표하여, 제도적 기반을 마련할 계획이다.

III. 기존 원전 및 SMR 사이버보안 위협

기존의 대형원전이 점차 디지털화된 기기 및 통신망을 채택함에 따라, 비인가된 기기 또는 사용자가 디지털 기술의 본질적인 취약성을 악용하여 원전의 운전 및 운영에 위협을 주는 사례가 잇따라 발생하고 있다[5]. 대표적인 원전 대상의 사이버공격 사례는 2010년대 초반에 발생한 Stuxnet 공격 사건이다. 해당 공격에 활용된 Stuxnet 악성코드는 이란의 부셰르 원자력 발전소와 나탄즈 우라늄 농축 시설 핵 개발용 원심분리기를 제어하는 EWS(Engineering Workstations) 및 PLC(Programmable Logic Controller) 제어시스템을 감염시켜 파괴하였다[6]. 이는 원전 시설이 사이버공격의 현실적 위협에 직면하고 있음을 보여주는 대표적인 사례다. 이 외에도 원전 시설을 대상으로 하는 사이버공격 사례는 [표 4]와 같다.

[표 4] 원전 시설 대상 사이버공격 사례

발생 시기	발생 국가	내용
2003	미국	Davis Besse 원전의 Slammer Worm 공격
2006	미국	Brown Ferry 원전의 제어통신망 과부화 공격
2008	미국	Hatch 원전 제어 S/W Upgrade 후 불시 정지
2010	이란	Stuxnet 악성코드 감염
2014	일본	문주 Malware 공격
2014	대한민국	한국수력원자력 사이버위협
2016	독일	Ramnit, Conflicker 악성코드 감염
2019	인도	Dtrack 악성코드 감염

대한민국에서도 원전 시설을 겨냥한 사이버공격 사례가 발생한 바 있다. 대표적인 예로 2014년 ‘한국수력원자력 해킹 사건’을 들 수 있다. 이 사건에서 공격자는 고리 원전과 월성 원전을 대상으로 사이버공격을 감행하였으며, 한국수력원자력 임직원 10,799명의 개인정보를 외부로 유출시켰다. 뿐만 아니라, CANDU 제어 프로그램 자료, 원전 설계도, 원자력발전소 수민 방사선량 평가 프로그램 파일 등과 같은 민감한 정보까지 유출된 것으로 알려지면서, 대한민국 원전 보안의 취약성

이 드러나 큰 논란을 불러일으켰다. 특히, 해당 사이버공격은 국가 주요 인프라인 원전 시설을 겨냥한 것으로, 공격자는 지속적이고 공개적인 협박을 통해 사회적 불안을 조성하고 국민들의 불안 심리를 자극했다. 이러한 점에서, 해당 사건은 단순한 사이버공격을 넘어 국민 안전을 위협하는 사이버테러의 성격을 띠었다고 볼 수 있다. 이러한 사이버위협은 단순한 정보 유출을 넘어 원전의 안전성과 직결될 수 있으며, 최악의 경우 핵물질 유출과 같은 중대한 사고로 이어질 가능성이 있다. 이를 바탕으로 해외/국내에서는 원전에 대한 사이버보안에 대한 중요성이 대두되었다.

기존의 대형원전 조차 반복적이고 정교한 사이버공격의 대상이 되고 있는 상황에서, 상대적으로 디지털 기술의 의존도가 높은 SMR은 더욱 큰 사이버위협에 직면할 가능성이 크다. SMR은 기존 원전의 경제성을 보완하기 위해 자율 운전 및 원격 운전과 같은 디지털 기술을 적극 채택하고 있으며[7], 이에 따라 사이버보안 위협 및 취약성이 더욱 증가할 수 있다.

이에 미국 샌디아 국립 연구소(Sandia National Laboratories)는 SMR을 포함하는 4세대 원자로(Generation IV Reactors)의 구현 및 개발 단계에서 사이버-물리적 위험 관리 체계의 중요성을 강조하며, 4세대 원자로에 대한 주요 사이버-물리적 위험 요소를 [표 5]와 같이 식별하였다[8].

[표 5] SMR을 포함하는 4세대 원자로 대상 주요 사이버-물리적 위험 요소

사이버-물리적 위험 요소	내용
하드웨어 공급망	설계부터 배송까지 다양한 위협이 존재하며, 마더보드(Motherboards)에 악성 부품 삽입 등과 같은 사이버침해 사례 발생 가능
소프트웨어 공급망	PLC(Programmable Logic Controller) 프로그램에 대한 공급망 위험 및 취약점 발생 가능
서비스 공급망	외부 서비스 공급업체로부터 공급받은 장비에 대한 위험 및 취약점 발생 가능
자율 운전	머신러닝 및 인공지능 활용에 대한 위험 및 취약점 발생 가능
고급 원자로 운영 기술 아키텍처	원자력발전소의 구조적 결함에 따른 취약점 발생 가능

외부 보안 운영	원격 보안 작업을 수행하는 원자로에 대한 사이버침해 발생 가능(예: 물리적 보안 시스템(Physical Protection System) 무력화 등)
현장 보안 운영	철저하지 않은 사이버보안 계획 및 문화에 따른 사이버침해 발생 가능
원격 운전	원격 통신 연결 손실, 안전 및 보안을 위한 제어시스템 간의 상호작용에 대한 사이버침해 발생 가능

1. SMR 대상 사이버-물리적 위험요소에 대한 파급 영향: 공급망

SMR의 설계 및 운영에 필요한 다양한 부품, 소프트웨어 및 시스템은 다수의 공급망을 통해 제공된다. 공급망을 통해 유입된 악성코드나 결함이 원자로 제어시스템에 삽입되는 경우, SMR의 안전성을 위협하는 요소로 작용할 수 있다. 특히, 공급망 공격(Supply Chain Attack)은 시스템의 초기 설계 단계부터 내재된 취약점을 확대시킬 수 있으며, 이는 원자로 운전 중단이나 방사능 누출과 같은 심각한 사고의 원인이 될 수 있다.

2. SMR 대상 사이버-물리적 위험요소에 대한 파급 영향: 자율 운전

SMR에 대한 자동화 기술 활용이 증가함에 따라 외부 위협이 커지고 있으며, 이에 따른 사이버공격의 위험도 고려해야 한다. 특히, 자동화 시스템이 공격을 받을 경우 즉각적인 대응이 어려워 원자로 운전이 정상적으로 관리되지 못하는 상황으로 이어질 수 있다. 따라서, 원자로의 안전성을 확보하기 위해 자동화 기술에 대한 사이버보안 대책이 필수적으로 마련되어야 한다.

3. SMR 대상 사이버-물리적 위험요소에 대한 파급 영향: 원격 운전

SMR은 원격 운전 시스템을 활용한 원자로 제어를 고려함에 따라, 운영 효율성을 극대화할 수 있는 장점을 갖지만, 동시에 외부 공격자가 원자로 시스템에 접근할 위험도 내포하고 있다. 원격 운전 시스템은 네트워크를 통한 통신에 의존하기 때문에, 외부에서 사이버공격을 통해 원전 시설에 무단 접근하고 제어할 가능성이 존재한다. 공격자가 원자로 시스템에 무단으로 접근할 경우, 시스템 오류가 발생하거나 원자로 운전에 영향을 미칠 가능성이 있다. 이에 따라 운영 안정성이 저하되고,

적절한 대응이 이루어지지 않을 경우 추가적인 문제로 이어질 수 있다.

이러한 SMR 사이버보안 위협은 그 파급영향이 매우 크기 때문에, 원전 시설의 안전성을 유지하기 위해서는 보안 위협에 대한 철저한 인식과 대응이 필수적이다. 사이버공격이 성공할 경우, 그로 인한 피해는 단순히 기술적 차원을 넘어 사회적 신뢰와 환경적 안전에도 심각한 영향을 미칠 수 있다. 특히, SMR은 원격지에 설치되는 특성상 사이버공격에 더욱 취약할 수 있으며, 보안이 소홀할 경우 단순한 운영상의 문제가 아니라 국가 에너지 안보와 공공 안전까지 위협하는 심각한 결과를 초래할 수 있다. 따라서 SMR의 설계 및 개발 단계에서부터 사이버보안 위협을 철저히 인식하고, 이에 대한 강력한 보안 조치를 반영하는 것이 필수적이다.

IV. SMR 사이버보안을 위한 고려 사항

기존의 원전 시설에 대한 사이버보안을 고려할 때 설계 기반 위협(Design Basis Threat, DBT) 개념이 중요한 역할을 한다. DBT는 원전 시설을 보호하는 데 필요한 위협 수준을 정의하며, 내/외부 위협을 모두 고려한다. SMR의 사이버보안을 해결하기 위한 접근 방식은 기존 경수로(Light-water reactor, LWR)와 크게 다르지 않다. 따라서 SMR 설계자는 기존 경수로 원전과 마찬가지로 설계 초기부터 폐로까지 DBT 기반의 사이버보안을 반드시 고려해야 한다. 이를 위해 SMR의 사이버보안 조치를 이행할 구체적인 방안을 개발하고, 설계 문서 보안 및 공급망 사이버보안을 포함한 종합적인 대응이 필요하다. 또한, SMR의 설계 특성에 따라 공급망 보안, 자율운전, 새로운 디지털 I&C 기술, 원격 운전 등 다양한 사이버보안 요소가 고려되어야 한다.

1. 공급망 보안 사이버보안 고려사항

SMR의 설계 및 구성은 컴퓨터 기반 시스템에 의존하여 관리되는 프로세스를 포함하며, 제조, 모델링 및 시뮬레이션 등 디지털 정보에 대한 전반적인 보안 대책이 필수적으로 요구된다. 공급망 공격은 안전, 보안 및 신뢰성에 영향을 미칠 수 있으며, SMR의 제작 및 유지보수에 중요한 요소로 작용할 수 있다. 이러한 위험에 대응하기 위해서는 설계, 건설, 운영 및 폐로의 각 단계에서 관련된 인력과 조직이 신뢰할 수 있고 안정적인지 확인해야 한다[9]. 또한, 품질 관리와 사이버보안을 통합하는 관리 및 조달 절차에 대한 신뢰성 및 안정성 검토도 필요하다. 이는 신뢰할 수 없는 공급업체의 사용을 방지하고, 자산의 기밀성, 무결성 및 가용성을 보호하는 데 필수적이다. 또 다른 중요한 고려사항은 민감하고 기밀로 간주되는 설계 문서를 철저히 보호해야 한다는 것이다. 설계 보안 문서를 사이버공격으로부터 보호하는 조치는 공급망 관리에서 반드시 포함되어야 한다. 이를 위해 미국 국립표준기술연구소(NIST)에서 발간한 ‘시스템 및 조직을 위한 사이버보안 공급망 위험관리 지침(NIST 800-161)’과 미국 원자력 규제 위원회(NRC)에서 발간한 ‘공급망 리스크 관리 전략’을 참고할 수 있다.

2. 자율 운전 사이버보안 고려사항

SMR의 자율 운전 기능을 구현하기 위해 적용 가능한 머신러닝 및 인공지능 알고리즘에 대해 사이버공격 가능성을 고려해야 한다. 특히, 머신러닝과 인공지능 알고리즘을 활용하는 경우 발생할 수 있는 대표적인 사이버공격은 적대적 공격이 있다. 적대적 공격은 딥러닝의 심층신경망 모델에 적대적 교란(Adversarial Perturbation)을 적용하여 시스템의 오분류를 유발하는 방식이다[10]. 적대적 공격의 종류는 [표 6]과 같다.

[표 6] 적대적 공격 종류

종류	내용
회피 공격 (Evasion Attacks)	인공지능이 잘못된 의사결정을 하도록 손상된 데이터를 주입하는 공격
중독 공격 (Poisoning Attacks)	공격자가 인공지능 모델의 학습 과정에 관여하여 인공지능 시스템 자체를 손상시키는 공격
탐색적 공격 (Exploratory Attacks)	모델 전도 공격(Model Inversion Attack)과 API(Application Programmable Interface)를 통한 모델 추출 공격(Model Extraction via APIs) ※ 모델 전도 공격: 인공지능 모델의 학습에 사용된 데이터를 추출하는 공격 기법 ※ 모델 추출 공격: 공개된 API가 있는 학습 모델의 정보를 추출하는 공격 기법

이러한 적대적 공격에 대해 대응하기 위한 보안 조치 예시로는 가능한 모든 적대적 사례를 학습 데이터에 포함하여 머신러닝 및 인공지능 모델을 훈련시키는 적대적 훈련(Adversarial training)이 있다[11]. 이는 모델을 훈련하는 단계에서 예상 가능한 공격 데이터를 입력하여 모델의 저항성을 강화하는 방식이다. 또한, 적대적 공격을 탐지하고 차단하는 방법에 대한 연구도 활발히 진행되고 있으며, 이러한 보안 조치들은 SMR 개발 단계부터 고려될 수 있어야 한다.

3. 새로운 디지털 I&C 기술 사이버보안 고려사항

새로운 디지털 I&C 기술에 활용되는 OPC 통합 아키텍처(OPC-UA), TSN(Time Sensitive Network), 다중 통신 등 최신 표준들이 SMR에 적용됨에 따라, 안전 기준을 충족하도록 보안성 평가 방안을 마련해야 한다. 또한, SMR의 동적 동작을 모니터링하기 위한 무선기술, 스마트 센서 등에 대한 보안 조치 방안이 필요하다. 이에 대해 구현가능한 보안 조치 방안 예시로는 무선 통신 및 OPC-UA, TSN 네트워크에 전송되는 데이터에 대한 암호화를 통한 기밀성 및 무결성 보호 방안이 있으며, WPA3(Wi-Fi Protected Access 3), VPN(Virtual Private Network) 등과 같은 고급 무선 보안 프로토콜을 사용하여 무단으로 데이터가 변조되는 것을 방지할 수 있다.

4. 원격 운전 및 무선통신 사이버보안 고려사항

SMR은 원자로의 작동을 모니터링하고 감독할 외부 제어실 및 조직에 운전 데이터를 지속적으로 제공하도록 설계된다. 특히, SMR이 설치되는 지역이 외진 곳에 위치하는 경우가 많아, 기존의 유선 통신망을 구축하기 어려운 상황에서는 무선 통신이 필수적인 역할을 한다. 하지만 이러한 원격 접속 및 무선통신을 활용한 SMR 운영은 기존의 원격 접속 취약점을 활용한 사이버 침해를 일으킬 수 있다. 실제로 원격 접속 취약점을 통한 산업제어시스템(Industrial Control System, ICS) 대상 사이버공격 사례는 [표 7]과 같이 보고된 바 있다[12, 13].

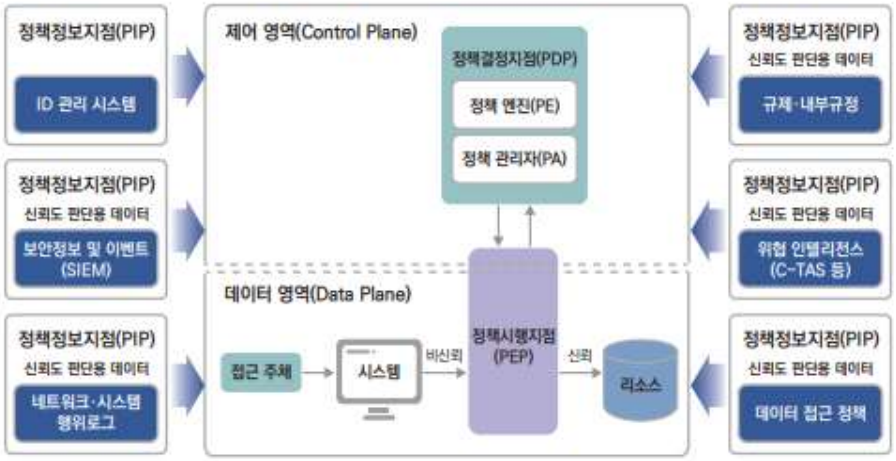
[표 7] 원격 접속 취약점을 통한 산업제어시스템 대상 사이버공격 사례

사이버공격 사례	내용
우크라이나 전력망 사이버공격(2016)	Crashoverride 악성코드를 활용한 RTU(Remote Terminal Unit) 프로토콜의 취약점 악용 공격
미국 올즈마 수처리시설 사이버공격(2021)	원격 접속 소프트웨어 취약점을 활용한 사이버공격

이러한 원격 접속 취약점 활용 공격에 대응하기 위해서는 제로트러스트 아키텍처를 기반으로 하여 원격 및 무선통신을 통해 송수신되는 정보의 기밀성, 가용성 및 무결성 확보 방안을 고려할 수 있다.

SMR에 제로트러스트 아키텍처 보안 모델을 적용하기 위해서는 다양한 보안 기법

을 적용해야 한다. 먼저, 다단계 인증(Multi Factor Authentication, MFA)과 원자로 운전 및 관련 정보 접근에 대한 최소 권한 제한을 설정한다. 또한, 사용자와 기기에 대해 일관된 통합 인증을 수행하고, 세밀한 접근 제어 및 모니터링을 강화한다. 마지막으로, 외부 통신에는 전용선과 암호화를 적용하여 네트워크 보호 기법을 구현할 수 있다. 이를 통해 SMR을 구성하는 내부 디지털 자산에 대한 공격 가능성 및 위험을 완화·관리함으로써 자산을 보호할 수 있다.



<자료> 과학기술정보통신부, 제로트러스트 가이드라인 2.0, 2024. 12.

[그림 3] 제로트러스트 아키텍처 보안 모델 및 논리 구성 요소

4. 안전-안보연계(SSI) 및 3S(Safety, Security, Safeguards) 통합을 통한 사이버보안 고려사항

원자력 안전 및 핵 안보 연계(Nuclear SSI)는 핵물질, 방사성 물질, 관련 시설 및 활동의 안전과 보안에 영향을 미치는 안전 및 보안 권고사항에 대해 필요한 조치를 개발하고 이를 구현하는 과정이다. 이 과정은 보안이 안전을 저해하지 않고, 안전이 보안을 방해하지 않도록 하며, 두 가지가 상호 시너지를 낼 수 있도록 안전 및 보안 대책을 조화롭게 설계하고 실행하는 것을 의미한다[14]. SMR의 기술적 특성상 자동화 시스템의 활용이 증가함에 따라, 안전 기능을 수행하는 시스템과 보안 기능을 수행하는 시스템 간의 고도화된 통합이 필요하다. 이를 위해 두 시스템 간

의 상호 악영향을 방지하고, 사이버공격을 포함한 악의적인 공격에 대한 제어 복원력을 지원할 수 있는 혁신적인 I&C 기술 개발이 필수적이다. 또한, SMR에 대한 SSI 및 안전조치를 고려한 3S 통합 설계를 통해 안전, 보안 및 안전조치 기술을 디지털, 네트워크, 4차 산업 기술을 기반으로 통합할 수 있다. 개발 초기 단계에서부터 안전, 보안 및 안전조치를 종합적으로 고려해야 하며, 일부 SMR은 혁신적인 안전조치 및 검증 방법의 구현이 요구된다.

5. 설계 단계 보안(Security by Design, SBD)

SBD는 설계 단계에서 사이버보안 정책을 적용하여 설계 및 구매 과정에 사이버보안 요건을 반영하고, 소프트웨어 개발 과정에서는 SDOE(Secure Develop and Operation Environment) 요건을 적용하는 개념이다. 이는 물리적 보안 수단에 의존하기보다는 근본적으로 보안 위험을 줄이기 위해 시스템 설계 단계에서부터 보안을 내재화하는 방식이다. SMR에 SBD 개념을 적용하여 보안 조치를 구현하면 운영 중에 보안 기술 적용 비용을 절감할 수 있으며, 안전 요건 개발 초기부터 보안 요건을 동시에 검토함으로써 안전과 보안을 통합할 수 있다. 또한, 설계자는 안전 및 보안에 관한 규제 요건을 설계 초기부터 고려하여 인허가 절차를 원활하게 진행할 수 있다.

6. 위험도정보 기반의 차등접근법(Risk Informed Graded Approach)

기존의 원전 시설에서는 광범위한 위험에 대한 분석의 깊이 필요성에 따라 보안 요건을 차등 적용하는 방식을 채택하고 있다. SMR 설계에서도 마찬가지로, 적용 가능한 모든 보안 원칙과 관련 위험을 종합적으로 고려하여 보안 요건을 설정할 수 있다[15]. 단편적인 원칙을 적용하여 위험 관리 판단을 내리기보다는 전체적인 보안 균형을 달성하는 데 우선순위를 둔다. 이러한 접근 방식이 적절하게 적용되었는지 판단할 때는 핵안보 위험뿐만 아니라 안전성 측면에서의 위험도 고려하여 적절한 규제를 달성했음을 정당화해야 한다. SMR의 경우, 기존 원전의 보안 원칙을 기반으로 보다 효율적이고 체계적인 보안 설계가 요구되며, 안전성과 보안을 동시에 고려하는 종합적인 접근이 필요하다.

7. 심층방호(Defense-in-Depth) 전략

심층방호 전략은 억제(저지), 탐지, 지연, 평가, 대응, 접근 통제 등의 보호 기능을 통해 내부자 위협을 포함한 다양한 위협으로부터 방어하기 위해 복수의 독립적인 방벽을 제공하는 전략이다. 이는 미국 원자력규제위원회(Nuclear Regulatory Commission, NRC)의 Regulatory Guide 5.71(원자력시설을 위한 사이버보안 프로그램) 지침과 한국 원자력통제기술원(Korea Institute of Nuclear Nonproliferation and Control, KINAC)에서 발간한 RS-015(원자력시설의 컴퓨터 및 정보시스템 보안) 지침에서도 명시된 개념으로, 원전 시설의 사이버보안을 강화하기 위한 핵심 원칙 중 하나로 강조되고 있다. 심층방호는 공격의 성공을 방지하도록 설계되어야 하지만, 동시에 예방 조치가 실패할 경우 보안 사건을 완화할 수 있는 기반을 마련하는 역할도 한다. SMR에 심층방호 전략을 효과적으로 구현하기 위해서는 적용 방안을 면밀히 검토해야 하며, 이를 위해 NIST 프레임워크(Executive Order 13636에 따른 NIST Framework) 지침을 참고하여, SMR을 구성하는 모든 디지털 구성 요소에 대한 기준선(Baseline) 보안 조치를 적용하는 방안을 고려할 수 있다.

Ⅴ. 결론

현재 SMR은 기존 대형원전에 비해 안전성, 경제성, 유연성 측면에서 여러 장점을 갖추고 있어, 전 세계적으로 설계, 개발, 실증에 이르기까지 활발히 연구·추진되고 있다. 또한, SMR은 기존 대형원전보다 설계가 단순하여 운영 및 유지보수 측면에서는 유리하다. 그러나 이러한 단순화된 설계로 인해 기존 원전처럼 다양한 설비를 다중적으로 설치하는 데에는 한계가 있다.

특히, SMR은 자율운전 및 원격 운영 기술을 고려하고 있어, 기존 원전에서 적용하던 제어시스템 독립망 운영 및 단방향 시스템을 이용한 연계 등의 보안대책을 그대로 적용하기 어려울 수 있다. 따라서, SMR의 자율운전 및 원격운전 기술과 관련하여 보안조치를 설계 단계부터 철저히 반영해야 한다.

최근 우리나라는 프랑스를 제치고 체코 신규 원전 사업 입찰에 성공하는 등, 원자로 설계 및 건설 분야에서 세계적인 기술력과 경쟁력을 입증하고 있다. 이에 따라 국가정보원은 원전 수출을 지원하고 미국·유럽연합 등 주요국의 사이버보안 정책을 준수할 수 있도록 국가 원자력시설 생애주기별 보안 내재화 지침을 발표하였으며, 이를 통해 국제 수준의 보안 요구사항을 제시하고 있다.

우리나라는 SMR 강국으로 부상하기 위해 SMR 사업단을 중심으로 i-SMR 설계 및 개발을 진행하고 있다. 이에 따라, SMR 사업단은 설계 및 개발 과정에서부터 국제 수준의 사이버보안 요구사항을 충족하기 위해 보다 적극적으로 대응해야 하며, 이에 따른 준비와 투자가 필요하다. 향후 SMR 수출 및 글로벌 경쟁력 확보를 위해 체계적인 보안 강화 노력이 요구된다. 4차 산업혁명 시대에도 우리나라가 원자력 강국으로서의 위상을 강화하고 국제적 신뢰를 높이기 위해, SMR 설계 및 개발 초기 단계부터 SMR의 안전성과 더불어 사이버보안 체계를 철저히 구축하는 것이 필수적이다.

◓ 참고문헌

[1] 한국수력원자력(주), “SMR 기술 개발”, https://www.khnp.co.kr/central/contents.do?key=1930.

[2] 삼일회계법인, “SMR(소형모듈원자로)의 무한한 가능성과 전략”, 2024.

[3] 이정익, KAIST 원자력 및 양자공학과, “소형모듈원전(SMR)의 도전과제와 국내외 동향”.

[4] 한국원자력연구원, “소형모듈원자로(SMR) 해외 기술새발 동향”, 2022-02호, 2022.

[5] 정광일 외 2인, “원자력발전소 계측제어계통사이버보안 적용 동향”, 정보처리학회지, 2012.

[6] 신익현 외 1인, KINAC 사이버보안실, “세계를 선도하는 국내 원전 사이버보안을 책임진다.”, 피플스토리.

[7] 송재구 외 4인, “SMR 개발과 사이버보안”, 정보보호학회지, 2023.

[8] Sandia National Labarotaries, “Cyber-Physical Risks for Advanced Reactors”, 2021. 09.

[9] Raphael Daguay, “Small Modular Reactors and Advanced Reactor Security: Regulatory Perspectives on Integrating Physical and Cyber Security by Design to Protect Against Malicious Acts end Evolving Threats”, International Journal of Nuclear Security, 2020. 12.

[10] KISEC 연구리포트, “적대적 공격 종류”, https://www.kisec.com/rsrh_rpt_det.do?id=221, 2020.

[11] LG CNS, “머신러닝 보안 취약점! 적대적 공격의 4가지 유형”, https://www.lgcns.com/blog/cns-tech/ai-data/9616/, 2020. 02.

[12] DRAGOS, “Crashoverride: Analysis of the Threat to Electric Grid Operations”, 2017. 06.

[13] LSTE, “Security Incident at Oldsmar Water Treatment Plant and Lessons Learned”.

[14] 백민, 한국원자력연구원, “원자력 안전-보안 연계 관리 개선방안”, KNS 춘계 학술발표회, 2021.

[15] Garcia Ismael 외 2인, “U.S.A Regulatory Efforts for Cybersecurity of Small Modular Reactor/Advanced Reactor”, IAEA, 2022.