

SMR 개발과 사이버보안

송 재 구*, 이 철 권**, 손 광 섭*, 이 영 준*

요 약

지금까지 원자력 산업은 국가의 전기수요 상당부분을 충족시키기 위해 대형 원전을 중심으로 건설하고 운영해 왔다. 그러나 대형 원전의 안전사고, 사용후 핵연료 처리 문제, 건설비 증가 등으로 세계 원자력 산업은 안전성을 향상시킨 소형모듈원전(Small Modular Reactor, 이하 SMR)의 개발에 주력하고 있다. 이에 본 논문에서는 SMR에 활용이 예상되는 최신 기술에 따라 증대되는 사이버보안 이슈와 관련 규제 동향에 관해 기술한다.

I. 서 론

세계는 에너지 안보뿐만 아니라 기후변화에 대처하기 위하여 탄소중립을 목표로 설정하고 에너지 분야에서의 다양한 변화를 시도하게 되었다. 이에 따라 탄소발생이 많은 화석연료를 사용하는 화력의 대안으로 태양광이나 풍력을 중심으로 하는 재생에너지 산업의 확대를 추구하였으며, 이에 국제적으로 많은 토론을 거쳐 원자력도 하나의 대안으로 채택되었다. 이러한 이유에는 재생에너지의 한계요건인 간헐성을 극복할 수 있는 대안으로 원자력이 국가의 필요한 에너지를 안정적으로 공급할 수 있는 것으로 평가되었기 때문이다. 또한, 원자력산업은 원자로를 발전 외에 담수나 큰 열에너지가 필요한 산업의 동력원으로 활용하기 위하여 안전성이 획기적으로 향상된 원자로를 개발하고자 관련 연구개발을 추진해 왔다. 이 결과로 SMR의 개발이 시작되었으며, 현재는 조기 상용화로 시장 선점을 위하여 국가별로 여러 개발사가 치열하게 경쟁하고 있다.[1]

최근 OECD NEA가 평가한 최적의 에너지믹스 산정 결과 탄소중립 실현을 위하여 재생에너지 비중이 증가할수록 재생에너지의 간헐성을 보완하기 위한 수단으로 저탄소 발전원인 원자력발전을 선정하였으며, 이 중에서도 대형원전 대비 탄력운전 성능이 우수한

SMR의 수요가 크게 증가할 것으로 전망하고 있다.[2]

이러한 SMR은 대형원전 대비 낮은 경제성을 보완하기 위해 자율운전, 원격운전등의 개념을 적극적으로 채택하고 있다. 그러나 이러한 혁신기술들의 활용은 기존 대형원전에서 경험하지 못한 사이버침해 발생 가능성을 증가시킬 수 있다. 이에 본 논문에서는 SMR 개발 따라 고려해야 할 사이버보안 내용과 규제현안에 대해 설명한다.

II. SMR 개발 개요

2.1. SMR 설계개념

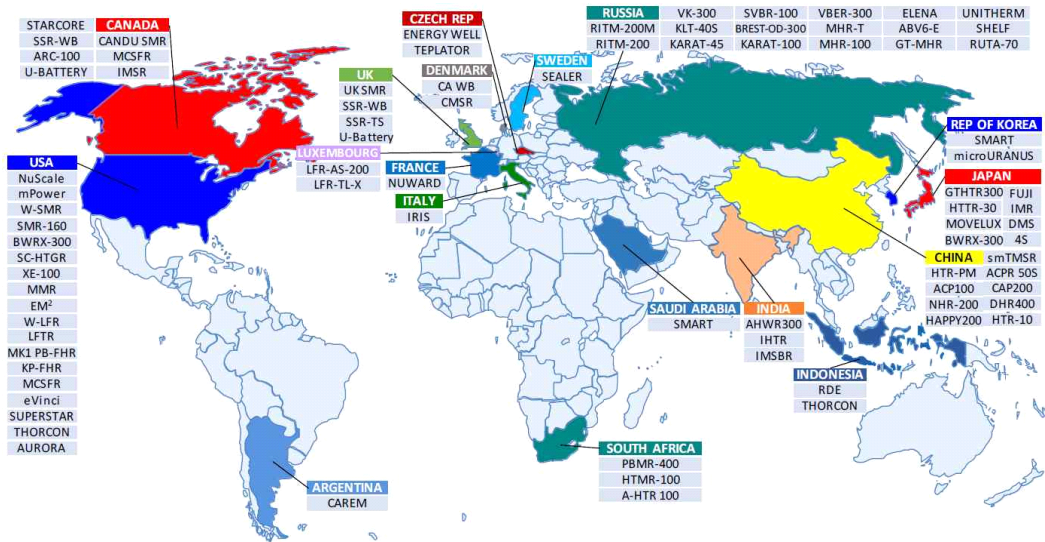
지금까지 원자력산업은 경제성이 유리한 대형원전 위주로 개발 및 운영되어 왔지만, 일부에서는 군사용이나 선박, 도서벽지 등에서 활용을 위하여 원자로 출력을 낮춘 중소형로(small and medium reactor)도 동시에 개발하여 왔다. 참고로 IAEA는 300MWe까지는 소형, 300~700MWe는 중형으로 정의하고 있다. 대부분의 중소형로는 대형원전에 비해 출력을 낮춘 형태로 개발되며, 원자로 등 주기가 하나의 원자로 용기에 내장되는 일체형원자로를 사용한다는 점 외에는 적용되는 세부기술에서는 큰 차이가 없다. 그러나 소형이라는 점에서 SMR과 혼용하여 불리고 있으나

본 논문은 한국원자력안전재단의 23년도 안전기술보고서 “SMR 사이버보안 기술 개발 및 규제체제 분석보고서와 SMR 물리적보안 기술 개발 및 규제체제 분석보고서”를 기반으로 작성되었습니다.

본 연구는 원자력안전위원회의 재원으로 한국원자력안전재단의 지원을 받아 수행한 원자력안전연구사업의 연구결과입니다. (No. 2202022)

* 한국원자력연구원 (책임연구원, jgsong@kaeri.re.kr, ksson78@kaeri.re.kr, yjlee426@kaeri.re.kr)

** 가천대학교 스마트보안전공 (연구교수, cklee100@gmail.com)



(그림 1) 세계 SMR 원자로 개발 현황(3)

modular(모듈식) 개념이 없다는 점에서 중소형로와 SMR이 차별된다. 최근 원전 산업을 주도하고 있는 SMR은 필요로 하는 곳에 필요한 만큼의 에너지를 공급할 수 있도록 소형의 원자로를 여러 개로 조합이 가능한 모듈식으로 설계한다. SMR은 송전망이 충분하지 않거나 외딴 지역의 소규모 전력망, 필요에 따라 용량의 점진적 추가가 필요한 복합발전단지, 해체된 석탄 화력 발전소 대신 유희부지 내 건설이 가능한 대체 발전원의 목적으로 개발한다. SMR은 원자로를 공장에서 생산하는 모듈조립 방식을 통해 건설공기 단축이 가능하며, 공장에서의 반복 생산을 통한 건설비 절감도 가능하다. SMR은 대형 원전사고가 발생하지 않도록 원자로를 지하나 수중에 건설하거나, 안전계통에 전기가 필요치 않도록 능동형 기기를 제거한 피동안전(passive safety) 개념을 도입함으로써 안전성을 획기적으로 향상시킨다.

2.2. SMR 개발현황

최근 대형원전 수요는 막대한 초기 투자비용에 대한 부담으로 인하여 기존의 원전 사용국 또는 국가 재정규모가 큰 원자력 도입 희망국의 신규 원전, 또는 기존 노후 원전을 대체하는 정도로 제한될 것으로 예상된다. 이에 따라 원자력 원천기술 보유국의 관심이 시장전망이 밝은 SMR로 전환되었으며, 미국, 영국, 러

시아, 중국 등을 중심으로 SMR 개발을 위한 컨소시엄을 구성하여 개발 및 상용화를 추진중에 있다. 2030년을 전후로 SMR이 본격 상용화될 것으로 전망되고 있으며, 그림 1과 같이 OECD 국가를 중심으로 2020년 기준 전 세계적으로 70개 이상의 SMR이 다양한 노형으로 개발중에 있다.[3]

2020년 5월 상업운전을 시작한 세계 최초의 부유식 원자력발전소인 러시아 아카데미 로모노소프는 35MW(e) SMR 2기로 에너지를 생산중이며, 또 다른 SMR은 CAREM(아르헨티나에서 개발한 30 MW(e) 일체형 가압 경수로)와 HTR-PM(중국에서 시운전 중인 211 MW(e) 고온 가스냉각 원자로)은 건설 또는 시운전 단계에 있다. 미국의 NuScale은 인허가심사 중에 있으며, 일본의 GTHTR300, 한국의 SMART, 중국의 ACP100 등은 개발중이다.

2.3. SMR 장점

SMR을 주요 개발사들은 다음과 같은 장점을 설명하고 있다.

- SMR의 여러 장점은 본질적으로 소형 및 모듈형 설계의 특성과 관련이 되며, 따라서 SMR은 설치공간이 작기 때문에 대형 원전에 적합하지 않은 장소에 건설 가능하다.
- 소형 및 모듈식 설계는 동일한 부지에 여러 개의

원자로 설치가 가능하다.

- SMR의 소형 및 피동안전 기능은 그리드가 작고, 원자력발전 경험이 적은 나라에서 수용을 용이하게 한다.
- 냉각수 확보에 대한 요건이 강하지 않으므로 원격지 건설 및 채굴 또는 담수화와 같은 특정 용도에도 적합하다.
- SMR은 설계의 단순성, 일체형 원자로의 반복 제조에 의한 경제성, 짧은 건설 기간 및 입지 비용 절감이 가능하다.
- 필요한 에너지 수요에 맞춰 원자로 모듈의 수를 탄력적으로(또는 유연하게) 선정할 수 있다.
- 사고발생 시 높은 수준의 피동 또는 고유(Intrinsic) 안전성을 가진다.
- 대형 원자로에서 요구되는 엄격한 많은 안전관련 요건들이 SMR 설계에 필요치 않다. 이는 일체형으로 설계되는 SMR은 대형 원자로 수준의 열저거 등 안전관련 공학적설비를 요구하지 않는다.
- 원자로 모듈이 지하에 건설되도록 설계하여 테러 등 외부 위협에 강하다.
- SMR 수명 종료 시 원자로 모듈 제거 또는 현장해체가 용이하다.

2.4. SMR 활용

1,000~1,600MWe 규모의 대형원전은 주로 전력생산용으로 원자력 이용국 및 전력 그리드가 큰 국가의 기저부하를 담당하는 역할이었지만, SMR은 원자력 이용국 및 전력 그리드가 작은 국가의 신규 발전원, 노후 화력발전 대체, 고립·해안·도서지역의 분산 발전 등의 발전원으로 활용될 수 있다. 또한 SMR은 소규모 전력망을 위한 발전원 외에 다음과 같이 다양한 산업적 활용이 가능하다.

- 산업공정의 열 및 난방
- 해수담수화
- 수소생산
- 선박, 우주선 (초소형원자로, micro-reactor)의 동력원, 등

III. SMR의 사이버보안 고려사항

규제기관 및 SMR 개발자가 논의한 결과, 지금까지 SMR의 사이버보안을 해결하기 위해 취한 접근방식은

아래와 같은 기존 경수로 원전의 접근방식과 다르지 않고, 원격지 건설이라는 특성 외는 특별히 다를 것이 없다는 것이 일반적인 견해이다. 원자력시설에서의 사이버공격은 시설에 물리적 피해를 입힐 수 있으므로 SMR 사이버보안 조치는 핵안보 및 시설의 안전성을 확보하기 위해 필수적으로 적용되어야 한다. 따라서 기존 경수로 원전과 마찬가지로 SMR 설계자는 설계 초기부터 폐로까지 사이버보안을 고려해야 하며, 디지털자산의 분류 및 사이버보안 심층방어 구조 설계, 사이버보안성 평가 및 보안조치 이행 방안의 개발, 사이버사건 대응방안 수립, 설계문서의 정보보안 등을 SMR 설계에 반영해야 한다. 이 외에 SMR 설계특성에 따라 사이버보안 고려가 요구되는 관련 기술들은 다음과 같다.[4]

- 자율운전
- 공급망 보안
- 원격 운전
- 새로운 디지털 I&C 기술 적용

IV. SMR의 사이버보안 규제현안

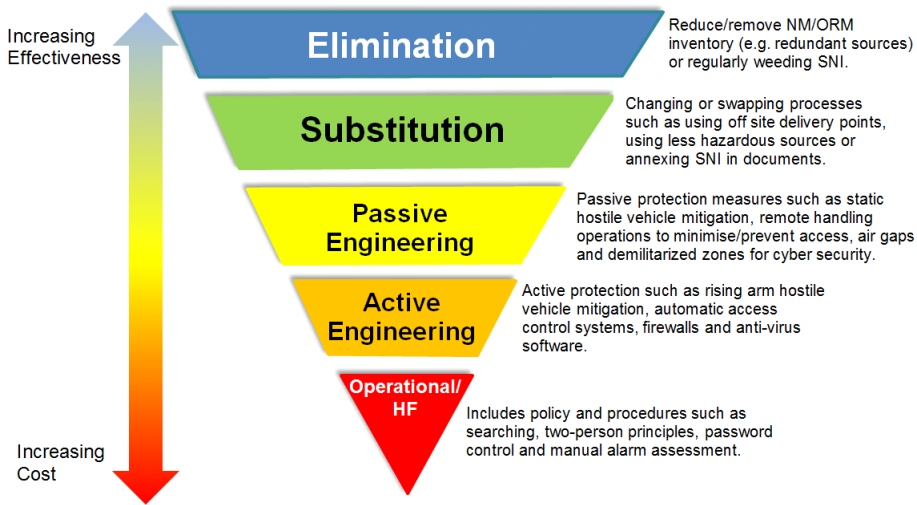
SMR의 설계특성에 따라 적용이 예상되는 새로운 기술들을 고려할 때 핵안보(보안시스템) 설계에서 기존 원전과는 많은 차이가 예상된다. 특히 사이버보안 설계에서 큰 변화가 예상된다. 이에 따라 SMR 개발과 함께 규제측면에서도 예상되는 규제현안에 대해 준비가 필요하다.

4.1. 사전 인허가제 (Pre-licensing)

SMR의 표준설계 (Standard Design) 과정에서 사이버보안 현안들이 설계에서 적절히 고려되는지를 사전에 검토하기 위해 도입되었다. SMR 개발에 대한 규제를 주도하고 있는 미국 NRC, 캐나다 CNSC, 영국 ONR의 규제체계를 분석한 결과, 규제기관이 사전 인허가제를 도입하여 개발 초기 단계부터 개발사들이 제기하거나 사안별로 예상되는 인허가 현안에 대한 검토 의견을 제시하여 개발사들에게 부담을 줄여주는 것과 동시에 인허가 획득까지의 기간을 줄이기 위한 절차를 도입하고 있다.[5]

- 미국 NRC : Pre-Application 프로세스 도입
- 캐나다 CNSC : 3단계 Vendor Design Review 도입
- 영국 ONR : 3단계 General Design Assessment

Security Hierarchy of Controls



(그림 2) 보안조치의 설계단계보안 계층구조(6)

프로세스 도입

- 국내 : 사전 인허가제 도입 추진중

4.2. 설계단계보안(Security by design)

“설계단계보안”은 설계 후 취약점을 보호하거나 완화하는 것이 아니라 원칙적으로 취약점을 줄이려는 접근방식으로, 악의적인 행위를 해결하기 위해 맞춤형 접근방식이나 설계를 통해 특정 위협을 완화하는 것이다. 이를 통해 고유보안(Inherent security) 설계가 가능하며, 고유보안은 다음을 통해 개선할 수 있다.[7]

- 핵물질 및 기타 방사성물질 또는 민감한 핵정보의 재고량을 줄이거나 더 이상 필요하지 않은 핵물질 및 기타 방사성물질 또는 민감한 정보를 제거
- 손상시 잠재적인 영향을 최소화하거나 없애기 위하여 핵물질 및 기타 방사성물질 또는 민감한 정보의 물리적 상태를 통제
- 엔지니어링, 관리 또는 기술적 보안조치를 적용하며, 이러한 수단들은 그림 2와 같은 계층적 보안 조치를 적용

4.3. 위험도정보 기반의 차등접근법(Risk informed graded approach)

원자력시설에는 광범위한 위협이 존재하므로 필요

한 분석의 깊이와 엄격성은 상당히 다를 수 있으므로 보안요건은 위협에 상응하는 방식으로 적용된다. 따라서 보안계획 또는 보안평가의 범위와 세부사항 (독립적인 평가 및 검증 포함)은 도난 및 사보타주 또는 민감한 핵정보 보유에 의한 분류에 상응해야 한다.[8]

차등접근 방식의 적용은 모든 적용 가능한 원칙과 모든 관련 위협을 종합적으로 고려하여 수행된다. 단편적인 원칙을 적용하여 위협관리 판단을 하기보다는 전체적인 보안 균형을 달성하는 데 우선순위를 두며, 차등접근법 방식이 적절하게 적용되었는지 판단할 때는 핵안보 위협 외에도 안전성 측면의 위협을 고려하고 적절한 균형을 달성했음을 정당화해야 한다.

4.4. 성능기반 평가 (Performance based evaluation)

미국이나 캐나다의 SMR 규제 접근방식의 최근 추세는 서술식(Prescriptive) 방식과 동시에 성능기반(Performance based) 방식의 규제를 병행하는 것이다. 이는 서술적 프로세스, 기술 또는 절차가 아닌 바람직하고 측정 가능한 결과에 초점을 맞춘 규제 접근방식으로, 성능기반 규제는 결과를 어떻게 달성할 것인지에 대한 구체적인 지침없이 정의된 결과를 도출한다. NRC에서 성능기반 규제조치는 적절한 안전여유를 보장하고 기관의 규제 개입 없이도 사업자가 안전을 개

선할 수 있도록 성능척도를 식별하는 데 중점을 두며, 현재 이 방법 적용을 위한 구체적인 예를 미국 NRC가 개발중에 있다.[9]

4.5. 심층방어 구조(Defensive architecture)

심층방어 구현의 중요한 측면은 억제(저지), 탐지, 지연, 평가, 대응, 접근 통제 및 내부자 위협 조치와 같은 다양한 보호 기능에 대해 복수 개 및 독립적인 방벽을 제공하는 것이다. 여러 장벽을 통합하는 심층방어는 공격이 성공하는 것을 방지하기 위해 설계되어야 하지만, 심층방어 수준의 적용은 핵안보, 특히 예방에 실패한 경우 보안 이벤트 완화의 토대가 된다.[10]

V. 결 론

세계 각국의 원자력산업은 경쟁적으로 SMR 개발을 추진하고 있지만, 설계정보 보호를 위해 설계개념 외에는 대부분의 내용을 제한적으로 공개하고 있다. 이러한 한계에도 불구하고 국내 SMR의 세계 수준의 기술 확보를 위해서는 각국의 SMR 기술개발 동향과 함께 규제기관의 사이버보안 규제 방향을 지속적으로 파악하고 이에 대한 이슈를 적시에 대응하기 위한 노력이 요구된다[11].

참 고 문 헌

[1] 과기부/산업부. 2021년도 예비타당성조사 보고서 혁신형 소형모듈원자로(i-SMR) 기술개발사업, 2021

[2] OECD/NEA. Small Modular Reactors_Challenges and Opportunities, Nuclear Technology Development and Economics, 2021

[3] IAEA. Advances in Small Modular Reactor Technology Developments 2020 Edition : A Supplement to IAEA Advanced Reactors Information System(ARIS), 2020

[4] WINS, WINS special report series - Security of Advanced Reactors, 2020

[5] CNSC, REGDOC-3.5.4: Pre-licensing Review of Vendor’s Reactor Design, 2018

[6] Rolls Royce, Rolls-Royce SMR Generic Security

Report, 2023

[7] SNL. US Domestic SMR Security by Design. SAND2021-0768, 2021

[8] Garcia et al., Regulatory Efforts for Cyber Security of Advanced Reactors, IAEA, 2022

[9] NRC, SECY-23-0021: Proposed Rule: Risk-Informed, Technology-Inclusive Regulatory Framework for Advanced Reactors, 2023

[10] IAEA. Computer security for nuclear security. NSS No. 42-G, 2021

[11] Jae-Gu Song, Cheol Kwon Lee, Jung Woon Lee, Kwang-Seop Son, Young Jun Lee, Considerations of Cyber Security for i-SMR, 2023 IAEA International Conference on Computer Security in the Nuclear World: security for Safety, Jun 2023

<저자소개>

송재구 (JAE-GU SONG)

2013년 3월~현재 : 한국원자력연구원 책임연구원
<관심분야> 원자력 계측제어 사이버보안, SMR 사이버보안, 기반시설 사이버보안



이철권 (Cheol Kwon LEE)

1985년 3월~2023년 11월 : 한국원자력연구원 책임연구원
2023년 11월~현재 : 가천대학교 스마트보안전공 연구교수
<관심분야> 원자력 계측제어 사이버보안, SMR 사이버보안, 기반시설 사이버보안



**손 광 섭 (KWANG-SEOP SON)**

2007년 12월~현재 : 한국원자력연구
원 책임연구원

<관심분야> 원자력 안전계통/제어기
기 설계, 원자력 계측제어/사이버보안
리스크 평가, 사이버위협 탐지

**이 영 준 (YOUNG JUN LEE)**

2006년 2월~현재 : 한국원자력연구
원 책임연구원

<관심분야> 원자력 계측제어 사이버
보안, SMR 사이버보안, 소프트웨어
확인 및 검증