원자력 산업에서의 인공지능 도입에 따른 규제 동향 연구

장은지*, 이현주
*한국원자력통제기술원

*ejchang@kinac.re.kr

A Study on Regulatory Status on using Artificial Intelligence in Nuclear Industry

Eunji Chang*, Hyunjoo Lee
*Korea Institute of Nuclear Nonproliferation and Control

요 약

본 논문은 원자력 산업에서 인공지능(AI) 기술 도입에 따른 규제 방향을 고찰하고, 원자력시설의 사이버보안 규제에 어떻게 반영할 수 있는지 분석하였다. 미국 원자력규제위원회(NRC) 및 유럽연합(EU)에서 발표한 AI 관련 규제 사항을 중심으로, 원자력 산업에서 AI 활용의 자율성 수준에 따른 규제 단계를 제시하였다. 이를 통해 국내 원자력시설에 AI를 도입할 때 고려할 수 있는 사이버보안 규제 체계 수립의 기초를 제공하고, 단계별 규제 접근법을 통해 효율적 규제 방안을 모색할 수 있음을 제안한다.

Ⅰ. 서 론

미국의 차세대 원자로를 위한 디지털 트윈 기술 프로젝트인 Generating Electricity Managed by Intelligent Nuclear Assets (GEMINA) 프로젝트에서는 인공지능(AI) 기술을 사용해 원자력 발전의 경제성을 높이고 유지보수 비용을 줄여 탄소배출 없는 전력망 구축을 목표로 한다. 그러나 AI 의 도입은 새로운 사이버보안 위협을 초래할 수 있고, 특히 원자력발전소는 여러 오류들이 동시에 발생하였을 때 큰 사고로 이어질 수 있기 때문에 AI 도입으로 인하여 발생할 수 있는 새로운 사이버보안 위협에 따라 추가로 필요한 규제 방향을 검토할 필요가 있다. 본 논문은 미국의 원자력규제위원회(NRC) 등 해외 규제기관의 인공지능 사용에 대한 규제 입장 및 연구기관의 연구 결과를 기반으로 원자력 시설에서 AI 를 사용하게 되었을 때 참고할 수 있는 규제 방안을 소개하고 향후 국내 원자력 시설의 AI 도입을 위한 사이버보안 규제 체계 수립 시 참고할 수 있는 규제 관점을 제시한다.

Ⅱ. 본 론

국내 원자력시설의 사이버보안 규제 업무는 한국원자력통제기술원 (KINAC)에서 “원자력시설 등의 방호 및 방사능 방재 대책법” 제 45 조에 의거, 원자력안전위원회로부터 위탁 받아 수행하고 있다. KINAC 은 원자력시설의 사이버보안 규제를 위하여 SSEP(Safety, Security, and Emergency Preparedness) 기능을 수행하거나 해당 기능에 악영향을 미치는 시스템을 식별하고 그에 따라 보안조치를 적용하도록 사업자에게 요구하고 있다.[1] 따라서 원자력시설에 AI 기반 시스템을 적용하기 위해서는 AI 가 SSEP 기능을 수행하는지 여부를 확인해야 한다. 또한 AI 의 활용이 원자력 시설의 의사결정에 있어 어떠한 역할을 하는지에 따라 SSEP 기능 혹은 해당 기능에 악영향을 미치는지 결정된다고 할 수 있기 때문에 AI 의 자율성 수준에 따른 규제 정도 구분을 결정해야 할 것이다.

2023 년 미국 원자력규제위원회 (Nuclear Regulatory Commission, NRC)는 NUREG-2261 “Artificial Intelligence Strategic Plan: Fiscal Years 2023-2027”[3]을 통해 AI 가 원자력시설에 적용될 시 준비해야 할 전략과 계획을 제시하고 있다. NRC 는 다양한 수준의 AI 및 AI 의 활용 정도에 따라 단계에 맞는 적절한 규제 요건을 수립할 것을 제시한다.

표 1. 원자력 시설에서의 AI 활용 수준에 따른 레벨 정의

AI 의 자율성 수준	원자력 시설에서의 AI 활용 정도
레벨 1: 인사이트 (AI 의 도움을 받는 사람의 의사결정)	시스템의 AI 통합은 플랜트 안전/보안 및 제어에 영향을 미치지 않는 최적화, 운영 지침 또는 비즈니스 프로세스 자동화에 사용됨
레벨 2: 협업 (AI 의 의사를 기반으로 하는 사람의 의사결정)	플랜트 안전/보안 및 제어에 영향을 미칠 수 있는 알고리즘의 권장 사항을 사람(운전원 등)이 검토하고 실행하는 시스템
레벨 3: 운영 (사람이 감독하는 AI 의사결정)	플랜트 안전/보안 및 제어에 영향을 미칠 수 있는 결정을 알고리즘이 내리고 사람의 감독 하에 운영을 수행하는 시스템
레벨 4: 완전 자율 (사람의 개입없이 AI 가 의사결정)	플랜트 안전/보안 및 제어에 영향을 미칠 수 있는 사람의 개입이나 감독에 의존하지 않고 알고리즘이 운영, 제어 및 지능형 적응을 담당하는 시스템

국내 원자력시설 사이버보안 규제의 핵심은 해당 시스템의 SSEP 기능 수행 여부와 의존성에 따라 악영향이 있는 경우를 식별하는 것이다. 레벨 1 수준에서 AI 를 도입할 경우, SSEP 기능 수행을 하지 않고 SSEP 기능을 수행하는 시스템과의 연결성에 대한 확인이 필요할 것이다. 사례로, 현재 한국원자력연구원에서 내부 규정에 대한 질의응답을 위해 챗봇 형태의 자체 언어모델을 개발하고 있다.[2] 이러한 운영 지침 또는 비즈니스 프로세스 자동화에 사용되는 시스템에 대해서는 해당 시스템이 SSEP 기능에 영향을 미치지 않는다는 가정 하에 규제 범위에서 제외될 수 있다.

레벨 2 수준부터는 SSEP 기능에 영향을 미칠 수 있는 수준으로, 현행 사이버보안 규제 범위에 포함될 확률이 높을 것이다. 원자력시설에서의 AI 사용에 대한 규제는 안전, 안보 측면에서 다양하고 엄격하게 적용되겠지만 사이버보안 규제 관점에서만 본다면 AI 는 일종의 소프트웨어로 볼 수 있다. 따라서 국내 원자력시설 사이버보안 규제기준에 따라 활용되는 AI 시스템이 필수시스템인지를 구분하여 해당되는 보안조치를 적용하여야 할 것이다. 구체적인 사이버보안 규제 요건에 대해서는 EU 인공지능법(이하, AI 법)에서 요구하는 사이버보안 요건을 참조할 수 있다.[4]

AI 법에서는 전기 공급과 같은 중요한 인프라의 안전구성요소로 활용되는 AI 시스템을 고위험 영역으로 구분하고, 사이버보안 관점에서는 데이터 보호 취약점 관리 등 시스템 무결성에 대한 요구를 하고 있다. AI 법에서 고위험 영역에 요구하는 사이버보안 원칙은 다음과 같다.

1. AI 에 대한 사이버보안 요구사항은 AI 모델 자체가 아닌 시스템 전체에 적용되어야 한다. 예를 들어 AI 모델 외에도 AI 를 구동하는 인터페이스, 센서, 데이터베이스, 네트워크 통신 구성 등 여러 유형의 구성요소를 포함하여야 한다. 이는 보안조치를 적용하여야 한다.
2. AI 시스템과 구성요소에 대한 사이버보안 리스크 평가를 수행해야 한다. 시스템이 설계된 방식을 고려하여 적절한 사이버보안 리스크 완화 조치를 결정할 수 있다.
3. 기존 사이버보안 조치와 AI 에 대한 조치를 결합하여 적용해야 한다. 심층보안(security-in-depth) 및 설계기반보안(security-by-design) 등의 엄격하고 복잡한 시스템에 대한 사이버보안 접근 방식을 모델로 삼고 시스템 수준에 따라 AI 에 특정한 조치가 아닌 범용적으로 사용된 보안조치로 해결될 수 있다.
4. 최신 AI 시스템은 보안의 복잡성과 기술적 과제가 남아있기 때문에 사이버보안 측면에서 문제가 해결되지 않는다면 고위험 영역에서는 AI 를 사용하는 것이 적절하지 않다.

미국의 국립표준기술연구소(NIST)에서도 AI 시스템을 설계, 개발, 도입하는 조직을 위한 가이드 문서인 'AI 위험관리 프레임워크 1.0'을 발간하였다.[5] 동 문서에도 위와 유사한 내용을 일부 언급하고 있다. 본 논문에 언급된 내용을 참고하여 국내 원자력시설에 AI 도입 시에 적절한 사이버보안 규제 체계를 수립할 수 있을 것이다.

Ⅲ. 결 론

인공지능 도입은 원자력발전소의 운영 효율성을 높이고 안전성을 강화하는 데 중요한 역할을 할 수 있지만, 원자력발전소의 특성상 높은 수준의 안전이 요구되는 분야에서는 인공지능과 같은 신기술 도입에 한계가 존재할 수 밖에 없다. 미국은 2021 년도부터 원자력사업자와 AI 관련 워크샵 등을 진행하고 있다. 우리나라도 새로운 기술 활용을 위해 신속한 규제 방안 마련을 위한 대책이 필요하다. 특히 자율운전기술의 도입을 고려하고 있는 소형모듈원자로(SMR) 개발이 진행 중인 바, 관련 규제 기준을 신속히 수립하여 설계 시에 반영할 필요가 있다. 본 논문에서 언급된 내용은 국내 원자력시설에서의 AI 사이버보안 규제 방안을 마련할 때 참고할 수 있을 것이다. 특히 단계별 규제 접근법을 통해 규제 효율성을 높일 수 있을 것이라고 예측된다. 향후 AI 도입에 대한 규제 개발의 측면으로, 국제표준과 미국, 캐나다, 유럽 등에서 선진적으로 도입한 규제 기준 등의 동향을 지속적으로 추적하여 구체적인 기술기준을 수립하고 규제 체계에 적절하게 반영할 필요가 있다.

참 고 문 헌

[1] 한국원자력통제기술원, KINAC/RS-015 Rev.2 "원자력시설의 컴퓨터 및 정보시스템 보안," 2023.

[2] 유용균, "원자력 분야의 인공지능 활용," 2023, (https://horizon.kias.re.kr/25980).

[3] European Commission, "Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts," 2021.

[4] Nuclear Regulatory Commission, NUREG-2261 "Artificial Intelligence Strategic Plan: Fiscal Years 2023-2027," 2023.

[5] National Institute of Standards and Technology (NIST), "Artificial Intelligence Risk Management Framework (AI RMF) 1.0," 2023.