원자력시설의 무선통신 사이버보안을 위한 접근통제 방안 연구

김상우*
*한국원자력통제기술원
kjoey@kinac.re.kr

A Study on Access Control for Wireless Communication at Nuclear Facilities

Sangwoo Kim*
*Dept. of Nuclear Security, Korea Institute of Nuclear Non-proliferation And Control

요 약

최근 4차 산업혁명과 더불어 센서 네트워크와 같은 최신 무선통신 기술들의 기반시설 적용을 위한 연구들이 활발하게 이루어지고 있다. 원자력시설 또한, 보안 및 비상대응 시스템에 무선통신을 적용하기 위한 연구들이 진행되고 있으며, 미국과 UAE의 경우 이미 원자력시설에 무선통신을 적용하여 사용하고 있다. 그러나 무선통신의 경우, 물리적인 네트워크 접근 경로가 존재하지 않기 때문에 통신 경로에 대한 접근통제가 불가능하며 광범위한 지역에 네트워크를 설치하는 경우 중계 단말 수량의 증가로 인한 접근통제 취약점이 발생할 가능성이 있다. 이와 같은 무선통신의 특성 때문에 원자력시설의 필수디지털자산에 무선 네트워크를 적용 시 현재의 통신 경로 접근통제 등의 유선 통신을 기준으로 작성된 접근통제 규제기준으로는 무선통신에 대한 접근통제를 이행하기에는 부족함이 있다. 이에 본 논문에서는 무선 네트워크 접근통제를 위한 규제 기준 개선안을 제시한다.

1. 서론

최근 4차 산업혁명이 이슈화됨에 따라 기반시설에도 주파수 통신을 활용하는 센서 네트워크와 같은 최신 기술을 도입하기 위한 연구들이 활발하게 이루어지고 있다. 원자력시설 또한, 무선통신 적용을 통해 비용 절감 및 효율 극대화를 위한 노력들이 지속적으로 이루어지고 있으며, 실제 미국의 경우 원자력발전소의 비상대응, 비안전 시스템 등에 무선통신을 활용하고 있다[1, 2, 3]. 국내 원자력시설의 필수디지털자산에 무선통신을 적용하기 위해서는 원자력시설의 컴퓨터 및 정보시스템 보안 기준인 KINAC/RS-015에 따라 디지털자산에 대한 기술적·운영적·관리적 보안조치를 반드시 수행해야 한다[4]. 그러나 무선 주파수를 대기 중으로 방사하는 무선통신의 특성 상 규제기준에서 요구하는 통신경로 접근통제, 네트워크 접근통제의 수행이 불가능하다. 이에 본 논문에서는 무선통신의 특성을 고려한 원자력시설 무선통신 장비에 대한 접근통제 규제 요건을 제안한다.

2. 국내 규제 기준 현황

국내 원자력시설의 필수디지털자산은 KINAC/RS-015에 따른 기술적·운영적·관리적 보안조치를 적용해야 한다. 기술적 보안조치에서는 원자력시설에 대한 무선통신 사용은 원칙적으로 금지하고 있으나, 필요시 보안성 평가 및 규제기관의 승인 후 사용하도록 하고 있다. 네트워크를 사용하는 필수디지털자산들은 반드시 기술적보안조치인 네트워크 접근통제와 운영적 보안조치인 통신경로 접근통제를 적용해야 한다. 그러나 운영적 보안조치의 통신경로 접근통제의 경우, 물리적 형태가 존재하는 유선 통신을 기준으로 작성되어 무선 네트워크를 사용하는 장치에는 해당 보안조치를 적용하기 어렵다. 네트워크 접근통제 또한 망 분리를 통해 원격에서 네트워크의 물리계층에 접근하는 것이 불가능한 상태를 기본 전제로 하고 있기 때문에 현재 명시된 보안조치 만으로는 원자력시설의 무선통신에 대한 규제에 활용하기에는 부족함이 있다[5].

3. 원자력시설 무선통신 접근통제 규제 기준 제안

2장에서 제시한 현재 규제기준의 무선통신 적용시 발생 가능한 문제점을 해결하기 위해 본 논문에서는 기존의 규제기준 일부 항목을 수정/보완한 원자력시설의 무선통신을 위한 접근통제 규제 기준을 제안한다.

<표 1> 무선통신 네트워크 접근통제 규제기준 제안

네트워크 접근통제	
기존	원자력사업자는 다음이 수행되도록 보장한다. 가) MAC(Media Access Control) 주소 잠금 나) 물리적 혹은 논리적 네트워크 분리 다) 정적 테이블 주소 유지 라) 패스워드 등 중요정보 전송 시, 암호화 마) 모니터링
추가 항목	바) 네트워크 장비 및 무선통신 장치는 초기에 서로를 식별하고 인증하여야 함 사) 무선 네트워크 구성 이전에 접근통제를 위해 허용 가능한 기기 목록을 작성 및 보유 아) 무선 네트워크 구성 이전에 접근통제를 위해 인가된 주파수 호핑 알고리즘 및 네트워크 ID 사용 자) 무선통신 시스템 설계 및 설치 시 무선 네트워크 접근통제 정책의 미적용 구간이 발생하지 않도록 장치의 설치 위치 및 개수 등을 지정하고 문서화

표 1은 기존 KINAC/RS-015에 존재하는 원자력시설의 필수디지털자산을 위한 네트워크 접근통제 규제기준에 무선통신 네트워크에 대한 접근통제를 위한 항목을 추가한 것이다. 무선통신 네트워크의 주파수가 방사되는 대기에 대한 접근통제는 불가능함으로 우선 주파수 접근 후 실제 네트워크 통신 사용하기 전의 인증 과정을 추가하여야 한다. 또한 네트워크 활용 시 쉽게 구입이 가능한 상용기기로 쉽게 접근이 불가능하도록 특화된 주파수 호핑 알고리즘 또는 네트워크 식별자를 통해 비인가 장비의 네트워크 접근을 통제해야 한다.

<표 2> 무선통신 통신경로 접근통제 규제기준 제안

통신 경로 접근통제	
기존	원자력사업자는 필수디지털자산 통신케이블 및 장비에 대한 물리적 접근을 통제하고 문서화하여야 한다.
신규	원자력사업자는 무선통신 사용 시 방호구역 외부에서는 통신 접근이 불가능 하도록 주파수 범위 및 중계기 설치 구역을 제한하고 문서화해야 한다.

표 2는 기존 KINAC/RS-015의 통신 경로 접근통제 항목과 무선통신을 위한 신규 규제 항목이다.

기존 규제기준은 표 2와 같이 통신케이블이 존재하는 유선 통신을 대상으로 적용 가능한 기준이기 때문에 유선통신에는 적용이 불가능 하다. 이에 상기 규제 기준에 준하는 무선 통신 네트워크의 물리계층에 대한 접근을 통제하기 위해 위와 같은 신규 항목을 제시하였다.

(그림 1) 무선통신 통신 경로 접근통제 적용 예시

본 논문에서 제시하는 무선통신 통신경로 접근통제를 적용할 경우 그림 1과 같이 무선통신 범위는 방호 구역 내부로 한정될 것이다. 방호 구역은 원자력시설의 물리적방호 규정에 따라 기본적인 물리적 접근통제가 이루어지고 있으며, 이에 따라 무선통신 경로에 대한 접근통제를 만족할 수 있다.

4. 결론

최근 원자력시설의 무선통신 사용 요구 및 연구가 증가함에 따라 사이버보안 규제에 대한 필요성도 증가하고 있다. 이에 본 논문에서는 현재의 원자력시설에 대한 사이버보안 규제기준에 따른 보안조치를 무선통신 장치에 적용하였을 경우 접근통제와 관련하여 발생 가능한 문제점을 도출하였다. 도출된 문제점을 해결하고자 네트워크 접근통제를 위한 추가 항목과 무선통신 경로 접근통제를 위한 신규 항목을 제안하였다. 본 연구는 원자력시설에 무선통신을 적용하고자 하는 연구자들과 규제기준을 개발하고자 하는 규제자를 위한 선행 연구로 활용이 가능하다. 또한, 상기 항목들이 실제 규제 기준에 반영 될 경우, 원자력시설의 무선통신 설치로 인해 발생 가능한 신규 공격 경로에 대한 접근통제를 기대할 수 있다.

참고문헌

[1] 고도영, 이재곤, 임재현 & 김만우. "원전 기기상태감시 무선기술 적용 타당성 조사". 대한기계학회 춘추학술대회(2017)

[2] Deng, Zhiguang, et al. “Application Analysis of Wireless Sensor Networks in Nuclear Power Plant.” International Symposium on Software Reliability, Industrial Sagety, Cyber Security and Physical Protection for Nuclear Power Plant. Springer, Singapore, 2019.

[3] Electric Power Research Institute, ”implementation guideline for wireless networks and wireless equipment condition monitoring”, 2009, TR1019186.

[4] 송동훈, et al. "원자력시설 사이버보안 강화를 위한 관리적 보안조치 검증 방법론 연구." 한국통신학회 학술대회논문집 (2018): 1048-1049.

[5] KINAC/RS-015, “원자력시설의 컴퓨터 및 정보시스템 보안”, 2016