원자력발전소의 필수디지털 자산 식별 및 보안 조치 현황 분석

김상우* · 신익현** · 권국희** · 변예은**

*한국원자력통제기술원

Analysing Current state of Identifying Critical digital assets And Cyber security control for Nuclear Facility

Sangwoo Kim* · Ick-Hyun Shin** · Kook Heui Kwon** · Ye eun Byun**

*Korea Institute of Nuclear Nonproliferation and Control

E-mail : kjoey@kinac.re.kr, ihshin@kinac.re.kr

요 약

최근 원자력발전소를 대상으로 하는 사이버위협이 급증함에 따라 원자력사업자는 원자력시설의 컴퓨터 및 정보시스템이 사이버공격에 대해 적절히 보호됨을 보장하여야하며 특히 사이버공격에 노출될 경우 핵물질 불법이전 및 공공안전에 악영향을 끼칠 수 있는 필수 계통에 대한 보호가 필요하다. 본 논문에서는 이를 위해 원자력발전소를 대상으로 하는 사이버위협 현황을 조사하고, 원자력시설의 필수 계통과 그에 포함된 필수디지털자산들을 식별 방법과 그에 따른 사이버보안 조치를 수행하는 국내·외의 국내 원자력 시설에 적합한 필수 계통 식별 및 보안조치 방법을 분석한다.

ABSTRACT

Currently as cyber threats grow up targeting nuclear power plants(NPP), licensees must guarantee that computer and information systems of nuclear facilities can be adequately protected against cyber attack. Especially critical system that cause illegal transfer of nuclear material and adverse impact to public safety need protecting. In this paper, we surveying the cyber threat examples targeted at NPP, and taxonomy the method of cyber security for NPPs in korea through analyzing the methodology to identify critical system and address cyber security controls for nuclear facilities.

키워드

Nuclear facility, Cyber attack, Cyber Threat, CDA, Security controls

Ⅰ. 서 론

최근 원자력발전소의 디지털기술 적용에 따라 실제 원자력 발전소를 대상으로 하는 사이버 위협 또한 증가하고 있으며, 사업자는 국민의 안전을 위해 원자력시설 내부의 필수디지털자산이 사이버위협으로부터 보호됨을 보장하여야한다. 보호가 필요한 필수디지털자산 식별을 위해서는 먼저 디지털자산을 포함하는 필수계통에 대한 식별이 필요하다. 본 논문에서는 원자력시설의 필수계통 및 필수디지털 자산 식별과 식별된 자산에 대한 보안조치 방법론의 국내외 연구현황을 조사하고, 이를 통해 국내 원자력시설의 사이버보안을 위한 연구 방향을 제시한다.

Ⅱ. 본 론

본 장에서는 원자력시설을 대상으로 한 사이버 공격 사례와 이를 방어하기 위한 국내·외의 보호가 필요한 필수디지털자산 식별을 위한 연구 동향 및 그에 따른 사이버 보안조치 현황을 분석한다.

2.1 사이버 공격 사례

원자력발전소에 디지털 설비가 도입된 2000년대 이후 원자력발전소를 대상으로 하는 사이버공격 사례는 꾸준히 증가하고 있다. 2003년 1월, 미국의 데이비스 베씨 원전을 감염시킨 슬래머 웜의 등장 후 그해 8월 미국 북동부의 원전의 블래

스터웝 감염에 따른 정전사태가 발생하였다. 이후 2010년 이란의 핵시설 및 중국의 주요기반시설에 대한 스턱스넷의 공격으로 원자력 발전소를 대상으로 한 사이버공격이 국가적인 무기로 사용될 수 있다는 것이 증명되었다. 또한 2014년 1월 주변국인 일본의 몬주발전소가 악성코드에 감염으로 인한 주요 정보가 유출이 보고된 그 해 12월 국내에서도 원자력 사업자인 한국수력원자력에 대한 해커의 사이버공격 및 원전 가동중지 협박이 있었으며, 이를 통해 원자력시설을 대상으로 한 사이버테러는 더 이상 가상의 위협이 아닌 현실이 되었음을 확인할 수 있다. 이러한 사이버위협으로부터 국민의 안전을 보장하기 위해 원자력시설의 필수 계통의 식별 및 이에 대한 보안조치가 시급한 현실이다.

2.2 필수 계통 및 디지털 자산 식별

현재 미국의 경우 원자력규제위원회(이하 NRC)의 규제지침에 근거하여 RG 5.71에 따라 계측제어 계통의 안전 및 안전에 관련된 기능을 수행하는 시스템(SSEP) 또는 기기를 필수 계통으로 분류하며, 현재 국내·외에서 필수 계통의 식별 및 분류를 위한 연구가 활발하게 이루어지고 있다[1, 2]. 미국의 NEI의 '사이버보안 규정에 의한 시스템 및 자산 식별'에서는 원자력 발전시설의 SSEP 기능을 포함하거나 이를 지원하는 계통을 [표 1]과 같이 5가지 항목으로 분류하며, 아래 항목 중 한 가지 이상 관련된 계통을 보호가 필요한 필수 계통으로 식별한다[3].

표 1. SSEP 시스템 항목 분류

시스템 명	기능
Safety Related (SR)	원자로 정지 시 안전한 상태 유지를 위한 기능, 피폭의 원인이 될 수 있는 사고의 방호 또는 완화 기능 등을 포함하는 안전에 중요한 시스템
Non-Safety Related /Important-to-Safety (NSR/ITS)	직·간접 적으로 불시의 원자로 정지 또는 운전 중단의 결과를 초래할 수 있는 원자로 이외의 시스템
Security (SEC)	기기들인 안전에 중요한 시스템, 설계기준위협에 포함된 사보타주 행위를 탐지, 평가, 완화 및 차단 기능 등의 보안 시스템
Emergency Preparedness (EP)	핵 비상사건으로부터 공공의 안전을 위한 보호기재를 포함하는 비상 준비 시스템
Support	위 시스템들을 보조 또는 지원하는 지원 시스템

국내에서는 한국원자력연구원이 사이버 위험평가와 자산분석 절차와 계측제어 계통의 심층방어모델에 따라 원자로 계측제어설계의 사이버보안 적합성을 분석하기 위한 계측제어계통의 디지털 자산 분석 방법론을 제안하였으며, 현재도 관련된 연구가 꾸준히 진행되고 있는 중이다[1]. 또한 대한민국의 원자력 시설 등의 방호 및 핵물질 운반 등을 규제하는 한국원자력통제기술원(KINAC)의 '원자력시설 등의 컴퓨터 및 정보시스템 보안 기술기준'에서는 원자력사업자에게 원자력시설 내 모든 운영시스템, 기기, 통신시스템, 네트워크, 지원시스템 등에 대한 초기영향분석을 수행하여, 원자력시설의 SSEP 기능에 악영향을 미치는 시스템을 판별하고, 이들을 필수시스템으로 분류하도록 요구하고 있으며, 이러한 필수 시스템 식별 절차를 [그림 1]과 같이 도식화 하고 있다[4].

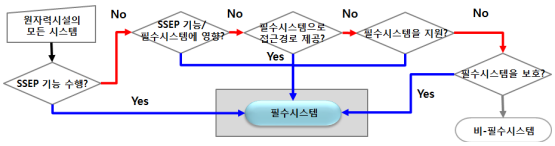

그림 1. 필수 시스템 식별 절차

2.3 필수 디지털 자산 사이버 보안조치

미국에서는 NRC의 규제지침 5.71의 사이버 보안 계획에 따라 사업자에게 계측제어 계통의 SSEP 기능과 관련된 기기를 사이버공격으로부터 보호하기 위한 보안조치를 요구하고 있으며, 국내에서는 KINAC의 원자력시설 등의 컴퓨터 및 정보시스템 보안 기술기준에서 기술적, 운영적, 관리적 보안조치로 분류된 101가지 보안 조치를 토대로 사업자의 보안조치 현황을 규제하고 있다.

또한 미국에서는 사업자가 모든 필수디지털자산을 대상으로 NRC의 규제지침 의거한 보안조치 전부를 수행하는 부담을 경감하기 위해 NEI 13-10 사이버보안조치 평가를 통해 필수디지털자산들을 분류하고 그에 따른 보안조치 및 대안조치 수행을 제안하고 있다.

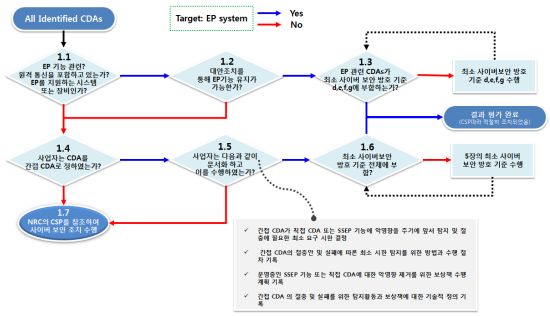

그림 2. CDA 결과 평가

사이버보안조치 평가에서는 우선 모든 필수디지털자산을 SSEP기능에 직접적인 연결 또는 악영향 가능 여부를 판단하여 직접 및 간접 디지털 자산으로 분류한다. [그림 2]는 이후 모든 필수디지털자산을 대상으로 EP기능 관련 결과 평가를 수행하는 절차이다.

결과 평가 종료 후 필수디지털자산들은 적용되는 보안조치 및 대안조치에 따라 [표 2]와 같이 RG 5.71에 따른 사이버보안 조치가 필요한 직접 디지털자산, 그림2 1.5의 대안 조치 와 [표 3]의 최소 사이버 보안 방호 기준 일부 적용하는 직접 디지털자산, 대안 조치 와 최소 사이버 보안 방호 기준을 적용하는 간접 디지털 자산 이렇게 세 가지 항목으로 식별하고 있으며, 사업자의 보안조치 효율성을 높이기 위해 각 항목 별로 적합한 최소 보안조치를 적용방법을 제시하고 있다[5].

표 2. 결과평가에 따른 보안조치 등급 분류

항목 1	대상	RG 5.71에 따른 사이버보안 조치가 필요한 EP와 관련 없는 직접 디지털 자산
	보안조치	RG 5.71 CSP의 101가지 보안조치 적용
항목 2	대상	최소 사이버 보안 방호 기준 일부 적용하는 직접 디지털자산
	보안조치	RG 5.71의 “Addition and Modification of Digital Assets” 적용
		[그림 2] 1.5의 대안조치 문서화, 수행 및 담당자 훈련
		[표 3]의 최소 사이버 방호 기준 d, e, f, g적용 - 10 CFR 50.47의 a,b,c,d 4가지 항목 적용
항목 3	대상	대안 조치 및 최소 사이버 보안 방호 기준을 적용하는 간접 디지털 자산
	보안조치	RG 5.71의 “Addition and Modification of Digital Assets” 적용
		[그림 2] 1.5의 대안조치 문서화 및 수행
		[표 3]의 최소 사이버 방호 기준 a, b, c, d, e, f, g적용 - 10 CFR 50.47의 a,b,c,d 4가지 항목 적용

NEI 13-10은 현재도 진행 중인 연구로 Rev.1에서는 비상 대응기능만을 대상으로 한 자산 분석과 대안조치 방법론을 제시하였다. 차후 이에 대한 연구가 완성 될 경우 모든 필수디지털자산에 대한 동일한 보안조치가 아닌 각 필수디지털자산의 특성에 따른 단계별 보안조치 적용이 가능하며 국내 원자력시설의 사이버보안조치 효율성 증대 및 사업자 및 규제기관의 업무 경감을 위한 연구를 위해서도 귀중한 참고자료가 될 것이다.

표 3. 최소 사이버보안 방호 기준

항목	보안 조치
a.	NEI 08-09의 Appendix E에 따른 간접 CDA 식별
b.	간접 CDA와 상호관계에 있는 자산은 무선 인터넷 통신 기능 소유 불가
c.	간접 CDA와 상호관계에 있는 자산은 다른 기기로부터 독립, 분리되어 있어야 함
d.	간접 CDA의 보호를 위해 휴대용 미디어 장치와 모바일 기기의 사용은 NEI 08-09의 D1.19에 따라 조치
e.	간접 CDA 변경 시 NRC의 ‘사이버보안조치’ 4.5에 따라 디지털 자산의 추가 또는 변경 전에 이에 대해 평가
f.	간접 CDA의 영향을 받는 장비는 장비운용가용성 및 기능에 대한 주기적인 검사 수행
g.	NRC의 ‘사이버보안조치’에 따른 모니터링 및 평가

III. 결 론

현재 해외뿐만 아니라 국내에서도 국가 중요기반시설인 원자력 발전소를 대상으로 하는 사이버 위협은 꾸준히 증가하고 있다. 이에 따라 본 논문에서는 사이버공격 시 핵물질의 불법이전 및 사보타주가 발생 가능한 필수 계통 식별 방법과 보안 조치 현황과 사업자의 필수디지털자산에 대한 보안조치 시 사업자의 시간과 인력 부담을 경감시키기 위한 필수디지털자산의 분류 방법론을 분석하였다.

향 후 이와 같은 필수디지털자산의 기능 및 특성에 따른 단계별 식별 방법들을 활용하여 국내에 원자력시설에 적합한 자산분류기준과 그에 따른 체계적인 자산분석 절차에 대한 연구가 필요하다.

참고문헌

[1] 구인수, 김관웅, 홍석붕, 박근옥, & 박재윤. (2011). 원자력발전소의 디지털계측제어시스템의 사이버보안을 위한 디지털 자산분석 방법. 한국전자통신학회 논문지, 6(6), 839-847.

[2] Regulatory Guide 5.71, “Cyber Security Programs for Nuclear Facilities”, US-NRC, 2010.

[3] Identifying Systems and Assets Subject to the Cyber Security Rule, NEI 10-04, 2012

[4] KINAC/RS-015.01, 원자력시설등의 컴퓨터 및 정보시스템 보안 기술 기준, 한국원자력통제기술원, 2014

[5] Cyber Security Control Assessments, NEI 13-10 Rev1, 2014