원전 사고연계 시스템의 사이버보안성 분석환경 개발방안에 관한 연구

변예은, 김현두, 김시원
한국원자력통제기술원
e-mail:hibye@kinac.re.kr

A Study on Establishment of Simulation Test Facility for Analysing Relativity of NPP Accidents

Ye-Eun Byun, Hyun-Doo Kim, Si-Won Kim
Korea Institute of Nuclear Nonproliferation and Control

요 약

2008년 미국 Hatch 발전소에서 제어시스템 소프트웨어 업데이트로 인한 비상정지, 2010년 이란 원자력시설에서 악성코드 스턱스넷(Stuxnet) 감염을 통한 원심분리기 1,000여개 파괴 등 원자력시설에 대한 사이버공격이 점차 증가하고 있는 상황에서 우리나라도 이와 같은 사고를 예방하기 위한 방안을 강구하여야 한다. 이미 우리나라 원자력시설에서 사용되는 시스템들이 아날로그 방식에서 디지털로 교체되고 있는 등 사이버공격에 용이하게 변화되고 있다.

이에 원전 사고연계 시스템들의 보안성을 평가할 수 있는 환경을 구축함으로써 사이버공격에 대한 보안대책 마련 및 근본적인 방어 체계를 수립하고자 한다.

1. 서론

2014년 한국수력원자력의 사이버사건, 2008년 미국 Hatch 발전소 제어시스템 소프트웨어 업데이트로 인한 비상정지, 2010년 이란 원자력시설 악성코드 스턱스넷(Stuxnet) 감염을 통한 원심분리기 1,000여개 파괴와 같이 국내외에서 원자력시설에 대한 사이버공격은 점차 증가하고 있다. 우리나라도 원자력발전소 계측제어시스템에 디지털 시스템을 반영하여 세계 최초로 100% 디지털화된 원자력발전소인 APR1400을 개발하고, 신규 건설원전인 신고리 3,4호기 등에 적용하는 등 사이버공격에 더욱 주의를 기울여야 하는 상황이다.

이러한 상황에서 핵물질의 불법이전 또는 원자력시설 및 핵물질의 사보타주를 야기하기 위한 전자적 침해행위에 대한 보안대책을 마련하고 근본적인 방어 체계를 수립해야 할 필요성 또한 증가하고 있다. 이에 복잡한 원자력발전소에서 사이버공격에 의해 어떠한 경로로, 어떠한 사고가 발생할 수 있는지를 평가하고 검증할 수 있는 시험환경 구축이 필요하다.

2. 핵심디지털자산 도출

'사이버보안 적용을 위한 시스템과 자산 식별(NEI 10-04)'와 '원자력시설등의 컴퓨터 및 정보시스템 보안 기술기준(KINAC/RS-015)'에서는 원자력시설에서 사이버보안 요건을 반드시 적용해야 할 대상으로서 SSEP(Safety, Security, and Emergency Preparedness) 기능을 수행하는 컴퓨터 및 정보시스템을 식별할 것과 침해를 당할 경우 해당 SSEP 기능에 악영향(Adverse Impact)을 줄 수 있는 지원 시스템 및 기기를 식별할 것을 요구하고 있다.

이에 '원자력시설등의 필수디지털자산 식별(KINAC/RS-019)'에서는 원자력사업자는 다음 기능들을 수행하는 컴퓨터 및 정보시스템(이하 '필수디지털자산(Critical Digital Asset)'이라 함)을 사이버공격으로부터 보호하여야 함을 요구하고 있다.

(그림 1) 원자력시설등의 필수디지털자산 식별 (KINAC/RS-019)

가. 안전 관련(Safety-related) 및 안전에 중요한(ITS, Important-to-safety) 기능

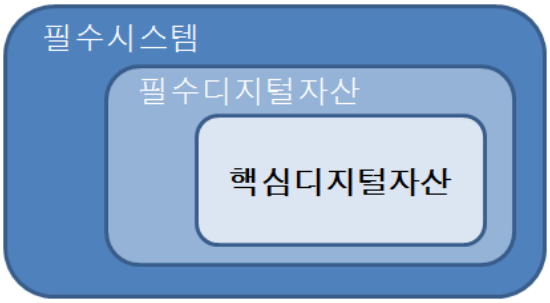
나. 보안(Security) 기능

다. 외부와의 통신을 포함한 비상대응(Emergency Preparedness) 기능

라. 침해를 받을 경우, 상기 기능에 악영향을 미치는 지원 시스템 및 지원 기기

이러한 필수디지털자산을 식별하기 위하여는 필수시스템(Critical System)을 먼저 식별하여야 하며, 이러한 필수시스템들은 디지털 또는 아날로그 시스템이 될 수 있다.

이와 같이 현재 규제 체계에서는 원자력시설 디지털자산의 70~80%인 필수디지털자산을 규제대상으로 하여 일괄 점검하고 있지만, 규제대상 내에서도 원전사고와 직접 관련된 핵심디지털자산(Vital Digital Asset)을 도출하여 취약점에 따른 대응책 마련이 필요하다. 다시 말해, 필수디지털자산은 원자력시설의 안전, 보안, 비상대응 기능을 수행하는 지원기기를 포함한 디지털자산이며, 핵심디지털자산은 사이버공격으로 인해 원전 사고를 직접 유발할 수 있는 디지털자산의 개념이다.



(그림 2) 필수시스템, 필수디지털자산, 핵심디지털자산의 관계도

이를 통해 효과적인 규제를 위해 사이버공격을 일으킬 수 있는 최신 위협에 따른 취약점을 분석하고 국내 보안기술 사례를 반영한 세부 보안요건 개발이 필요하다.

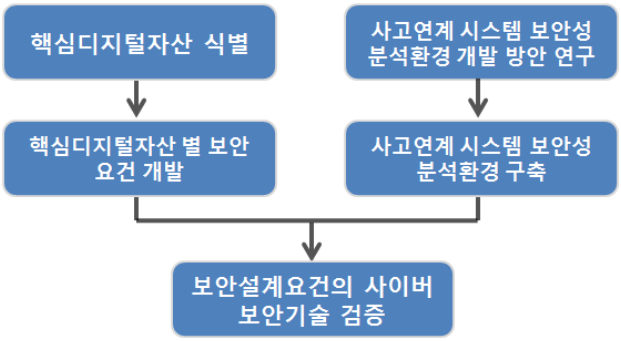
3. 국내외 시뮬레이터 현황

국내에서는 한국인터넷진흥원에서 사물인터넷, CCTV 등의 IT 환경에 특화된 시뮬레이터 외에도 제어시스템 테스트베드를 통하여 보안 취약점을 분석하고 대응방안을 연구하는 환경을 구축하여 제어시스템 보안 기술 및 연구를 진행하고 있으며, 국내 화력발전소에서도 운전 훈련용 시뮬레이터를 활용하고 있다. 특히, 제어시스템 분야 중에서도 원자력시설에 특화된 시뮬레이터 연구가 한국수력원자력, 한국원자력연구원 등에서 활발히 진행되고 있다. 원자력시설에 대한 모델링은 원전 계측제어시스템 개발과정이나 개발 후의 검증, 시스템 설치, 시운전, 운전원 교육 등 다양한 분야에서 활용되고 있으며, 현재에도 원자력발전소의 디지털 제어시스템 전 범위로 시뮬레이터를 개발하여 훈련 및 사전 운전을 위한 테스트베드로서 이용되고 있다.

국외에서는 2015년에 미국 에너지부에서 원자로 운영 능력 향상을 위해 지난 2010년 에너지 혁신 허브에서 시작된 첨단 경수로 시뮬레이션(Consortium for the Advanced Simulation of Light Water Reactors, CASL)의 5년 갱신 계획을 발표한 바 있다. 특히 원자로의 응용프로그램을 위한 가상환경(Virtual Environment for Reactor Applications, VERA)은 원자력 산업계에서 테스트를 위해 이용되고 있다. 또한, 2003년에 국가 SCADA 테스트베드(National SCADA Testbed, NSTB)를 설립하여 전력회사 및 정부 등을 중심으로 전력분야에 대한 테스트베드를 구축하였다. 또한, 일본에서는 제어시스템 사이버보안센터(Control System Security Center, CSSC)를 통해 SCADA 테스트베드를 구축하여 주기적인 취약점 분석 등을 수행하고 있다.

4. 원전 사고연계 시스템의 사이버 보안성 분석환경 개발

사이버보안 규제를 효과적으로 하기 위하여 규제대상 내에서도 원전 사고와 직접 관련된 핵심디지털자산을 도출하여 단계적 접근방식을 적용한 심층방호 규제요건을 적용할 수 있다. 이를 기반으로 핵심디지털자산 별 공격인자를 분석하여 보안요건을 개발할 수 있다. 또한, 앞서 살펴본 국내외 시뮬레이터 현황을 기반으로 사고연계 시스템 보안성 분석환경을 개발하기 위한 연구를 통해 대응방안을 분석하거나 보안기술을 검증할 수 있다.



(그림 3) 원전 사고연계 시스템의 사이버 보안성 분석환경 개발

5. 결론

IT 및 제어시스템 환경이 발전함에 따라 시뮬레이터나 테스트베드의 형태가 다양한 목적으로 사용되고 있다. 본 논문에서는 원전 사고를 일으킬 수 있는 핵심디지털자산을 식별하여 구축된 환경에 어떻게 적용을 시켜 원전 사고를 평가하고 검증할 수 있는지에 대해 알아보았다. 원자력시설에 대한 사이버보안 규제를 담당하고 있는 본 기관에서 보안성 분석 환경을 활용한다면 보다 효과적인 규제

및 심층적인 보안이 가능해질 수 있을 것이다. 이를 위해 향후 사고연계 시스템 보안성을 분석하기 위한 환경을 설계하기 위해 국내외 시뮬레이터 및 테스트베드에서 어떠한 점을 활용할 수 있는지 파악하고, 핵심디지털자산을 식별할 수 있는 방법론에 대한 연구도 필요하다.

참고문헌

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

[2] 한국원자력통제기술원 (2014), 원자력시설등의 컴퓨터 및 정보시스템 보안 기술기준(KINAC/RS-015)

[3] 한국원자력통제기술원 (2015), 원자력시설등의 필수디지털자산 식별(KINAC/RS-019)

[4] 한전전력연구원 (2015), 발전소 시뮬레이터 기술동향