정 보 보 호 학 회 지
제29권 제2호, 2019. 4

IAEA 주관 원자력시설 사이버사건 분석 및 대응능력 강화에 관한 국제공동연구

이 철 권*

요 약

이 글에서 IAEA 핵안보(정보보안) 부서의 원자력시설에 대한 사이버보안 활동과 함께 2016년부터 13개국 17개 기관이 협력하여 수행중인 “원자력시설 사이버사건 분석 및 대응 능력 강화에 관한 국제공동연구”에 대해 소개하고자 한다.

Ⅰ. 원자력 사이버보안 현황

디지털기술, 통신기술 및 소프트웨어기술의 발전에 따라 이들 기술을 기반으로 하는 정보, 금융, 방송, 통신 및 산업시설을 포함하는 국가기반시설은 해킹으로부터의 위험에 항상 노출되어 있다. 뿐만 아니라 뉴스를 통해 수시로 강대국 간의 사이버침해에 관한 설전이 들려오고 있는 가운데 언제부터인가 우리는 사이버보안이라는 용어에 익숙해져 있으며 또한 어떠한 형태로던 피해를 당하지 않기 위해 주의를 기울이고 있다.

원자력발전소(원전)나 핵물질을 보유하는 시설이 있는 국가는 원자력설비에 컴퓨터 기반의 디지털기술과 통신망이 널리 보급됨에 따라 2000년대로 접어들면서 사이버보안 필요성을 인지하게 되었으며, 2010년 이란의 핵시설에서 발생한 스턱스넷 침해사건 이후 사이버보안에 대한 대책을 적극적으로 강구하고 있다. 이 흐름의 중심에는 100여개의 원전을 운영하고 있는 미국과 함께 국제원자력기구(IAEA)가 있다. IAEA 사이버보안 담당부서는 원자력시설에 대한 사이버보안 지침들을 개발하여 170여개의 회원국에게 제공하며, 이 기술지침들을 기반으로 기술별, 수준별, 개최 범위별로 교육훈련 과정을 개발하여 원자력 종사자들을 대상으로 제공하고 있다. 또한 IAEA는 교육훈련 과정에 디지털계측제어설비에 대한 사이버보안 실무 (I&C Hands-on) 과정을 개발하여 종사자들의 사이버보안 인식 수준을 높이고자 노력하고 있다.

Ⅱ. 원자력 사이버보안과 IAEA 핵안보부서 사이버(컴퓨터)보안 활동

IAEA 핵안보부서(NSNS) 사이버(컴퓨터)보안 부서에서는 포괄적이고 리질리언트한(resilient) 컴퓨터 및 정보보안 프로그램을 개발하고 회원국에게 기술지침, 교육훈련, 관련 전문가 지원 등을 제공하며, 다음과 같은 업무를 수행하고 있다.

- ⊙ 전문가 회의 및 정보 교류 포럼 개최
- ⊙ 기술지침서 개발
- ⊙ 국제, 지역별 및 국가별 교육훈련 과정 개최 및 전문가 양성
- ⊙ 사이버사고 대응훈련 기술지원
- ⊙ 사이버보안 프로그램 개발 및 이행을 위한 주제별 전문지식 제공
- ⊙ 기타 지원활동(outreach)

〔그림 1〕 IAEA 사이버보안 활동

* 한국원자력연구원 원자력 ICT 연구부 (cklee1@kaeri.re.kr)
** 이 글에서는 IAEA 관련 기술지침서에 따라 컴퓨터보안과 사이버보안이 동일한 의미로 혼재되어 사용됨.

2.1. 원자력 사이버보안 지침 개발

회원국은 IAEA 사이버보안 지침을 기반으로 국가별로 원자력시설 인허가를 위한 규제지침을 개발하여 시설의 수명 전주기 동안 단계별로 필요한 기술을 개발하며, 나아가 필요한 보안조치를 취하고 있다[그림 2]. 국내에서도 가동중인 시설은 물론 건설중인 시설에 대해서도 규제지침을 만족하도록 사이버보안 기술을 적용하고 있다[1]. 이에 대해 원자력사업자는 (1)사이버보안 이행계획서를 작성하고, (2)해당시설에 대한 사이버보안성 평가 및 적절한 보안조치를 취하고 있으며, (3)사이버사건 발생시를 대비한 대응계획을 마련하고, (4)교육 및 훈련을 통해 종사자들이 신속하고 적절한 대응이 가능하도록 인식 및 대응 능력을 강화하도록 한다. 개발된 IAEA 기술지침은 IEC 등 국제표준과도 정보교류를 통해 이들이 사이버보안 요건 개발시 참고자료로 활용되고 있다[2].

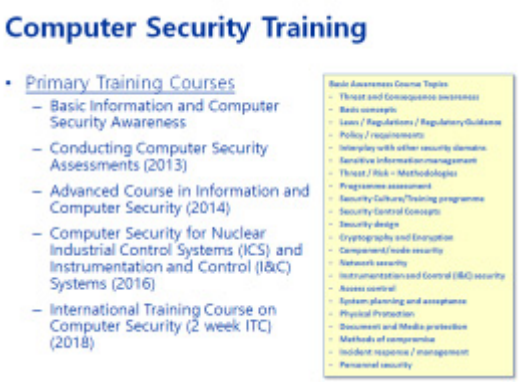
〔그림 2〕 IAEA 핵안보 기술지침서

2.2. 사이버보안 교육과정 개발

회원국의 사이버보안 이행 프로그램 개발 및 조치, 이들을 유지할 수 있도록 기술지원하기 위해 다음과 같이 다양한 교육 과정을 개발하였다.

- ⊙ 국제 과정 (International Training Courses)
- ⊙ 지역(대륙)별 과정 (Regional Training Courses)
- ⊙ 국가별 과정 (National Training Courses)
- ⊙ 국제 핵안보교육 네트워크 (INSEN)과 연계된 전문가 교육 과정

또한 교육과정은 교육수준별로 개최된다[그림 3].



〔그림 3〕 IAEA 사이버보안 교육과정

2.3. 핵안보 사이버보안 훈련 실시

핵안보 체제가 지속가능하도록 관할 당국과 운영자는 사이버보안을 포함하여 적절한 핵안보 제공 능력에 영향을 미치는 문제와 요인을 확인하고 다루어야 한다. 핵안보 훈련은 국가의 핵안보 체제 전반에 사이버보안의 효과적인 이행을 평가하고 구현된 사이버보안조치가 위협평가와 일치하는 수준의 보호대책을 제공하는지 확인하는 활동이다. 따라서 사이버조직은 핵안보 훈련을 실시하여 물리적보안과의 연합공격(Blended attack)을 포함한 사이버사건에 대한 대응 능력을 평가해야 한다.

관할 당국과 운영자는 참가자를 교육하고, 비상계획을 포함한 사이버보안 프로그램 (CSP)의 유효성을 검사하기 위해 주기적으로 사이버보안 훈련을 실시하며, 다른 보안훈련과 비상훈련이 함께 수행되도록 한다. IAEA는 사이버보안 훈련을 포함한 핵안보 훈련에 관하여 회원국을 지원한다.

2.4. 사이버보안 정보 공유

핵안보의 요소로서 사이버보안의 중요성은 충분히 인식되어왔다. IAEA 핵안보 계획서는 국가 및 시설 수준에서 예방과 탐지 및 대응을 지원하기 위해 컴퓨터보안 기능이 강화되어야 한다고 명시한다. 나아가 정보보안 사고는 직접 또는 간접적으로 원자력 안전 및 안보에 악영향을 줄 가능성이 있으므로 2013~2015년 IAEA 총회 결의안은 사이버보안 정보공유가 매우 중

요다고 언급하고 있다. 이를 위하여 핵안보부서는 정보 공유에 관한 기술지침을 개발 중에 있다.

2.5. 사이버사건 대응

컴퓨터 시스템 또는 컴퓨터 네트워크의 손상 발생시에 대비한 보호원칙은 예방에만 국한되어서는 안되며, 여기에는 또한 탐지 및 응답을 포함해야 한다. 따라서 원자력사업자는 물리적보안, 원자력 안전 및 핵물질 계량과 통제에 사용되는 시스템에 잠재적으로 영향을 줄 수 있는 컴퓨터보안 사고에 대응하기 위한 비상계획을 수립해야 한다. 대응은 직접 공격뿐만 아니라 그러한 시스템에 대한 정보수집 시도를 포함해야 한다.

IAEA는 포괄적인 컴퓨터사고 대응계획을 개발하는 회원국을 지원하기 위해 관련 기술지침을 개발하였다 [3].

Ⅲ. IAEA 주관 사이버사건 분석 및 대응능력 강화에 관한 국제공동연구

원전에서는 발생가능한 여러 안전 사고들에 대처하기 위하여 원전을 모사하는 시뮬레이터를 사용하여 운전원 및 사이버보안 종사자들을 대상으로 지속적 반복 훈련을 통해 대응능력을 강화하고 있다. 이와 유사한 개념에서 2016년 IAEA는 사이버침해 사건에 대한 운전원 및 종사자의 대응능력을 강화하기 위하여 사이버보안 훈련용 시뮬레이터를 개발하고 이를 R&D 및 교육훈련용으로 활용하는 계획을 수립하였다. 참고로 기존의 시뮬레이터는 안전과 관련한 운전원 훈련용으로 사이버보안과 관련해서는 활용이 불가능하다. 이를 위해 IAEA는 “원전 사이버사건 분석 및 대응능력 강화”라는 제목으로 국제공동연구 과제(CRP)를 제안하였고 13개 회원국에서 17개 기관이 이 국제공동연구 과제에 참여하고 있다.

3.1. 목적

이 공동연구의 목적은 원자력시설 안전 및 핵안보에 직접 또는 간접적으로 악영향을 미칠 수 있는 컴퓨터보안 사고의 예방 및 탐지, 대응에 관해 원자력시설에서 강화된 컴퓨터보안 기능을 지원하는 활동을 수행하는 것이다. 이를 위해 이 공동연구에서는 우수 사례, 보안기술, 사고분석 방법 및 원자력시설에서의 컴퓨터보안 사고에 대한 포렌식 활동을 포함한 대응을 위한 권고절차와 같은 주요 영역에 대해 연구하며, 연구결과는 핵안보 지침 및 훈련 개발을 위한 입력으로 활용될 예정이다.

3.2. 연구내용

연구내용은 사이버보안 사고 분석 및 대응을 강화하기 위한 (1)사이버보안 사고 인식 및 대응을 위한 운전원 지원, (2)사이버보안 사고 대응을 위한 분석 및 기술지원, (3)사이버보안 정보 교환, (4)사이버 포렌직의 4가지 주제에 관한 것이며, 각 주제별 상세 연구내용은 다음과 같다.

가) 원자력 안전 및 보안과 관련된 컴퓨터보안 사건에 대한 식별 및 대응 과정에서 운전원을 지원하는 기술 또는 기법을 연구, 개발 및 시연 : 원자력 안전 및 보안시스템의 복잡성으로 인해 원자력시설 내의 컴퓨터보안 사고를 탐지하고 분석하는 것이 어렵고 또한 기존 시스템에서 컴퓨터보안 사건 식별 및 조사를 지원하도록 설계되거나 분석된 적이 없다. 그러나 적시에 컴퓨터보안 사고를 식별하지 못하면 컴퓨터보안 사고대응이 효과가 없거나 지연될 수 있다. 그러므로 효과적인 사고대응을 위해서는 컴퓨터보안 사고 발생 즉시 탐지 및 분석하는 기술을 특성화해야 한다.

나) 멀웨어 탐지, 봉쇄, 제거 및/또는 시스템 기능의 복원을 지원 : 컴퓨터보안 사건분석 능력을 강화하여 사이버공격을 식별하고 특성화하기 위해 운영체계 포렌직 및 분석데이터를 수집할 수 있도록 필요한 조치가 이루어져야 한다. 사례로 (1)원자력시설에 능동적 또는 수동적 모니터링 장비를 설치, (2)능동적인 시험을 위한 매개변수 선정, 해당 응답기준 및 제한사항 개발, (3)허니팟, 허니닛(honeynets) 및 기타 적대행위 수집장치에 의한 기존 보안사고의 분석결과를 활용한다.

다) 핵안보 지원을 위해 협력체제로 통합될 수 있는 정보공유 소스 및 프레임 워크의 파악 : 전 세계적으로 컴퓨터보안 취약점의 악용과 잠재적 결과의 민감성으로 인해 정보교환은 금지되고 있다. 그러나 사이버공격에 대해 방어가 견고하고 대응이 효과적이기 위해서는 핵안보를 담당하는 국제 파트너들 간에 정보를 공유할 필

요가 있으므로 이 연구는 컴퓨터보안과 관련된 정보공유에 필요한 주요 요소와 프로토콜을 파악하는데 초점을 둔다. 정보공유 모델은 다른 산업 부문과 국가 프레임 워크 내에 존재하며 이 연구를 통해 이 체제가 핵안보에 어떻게 적용되고 이행될 수 있는 지를 조사한다.

라) 원자력시설 컴퓨터시스템에서 발생한 범죄 행위에 대한 포렌직을 수행한 사례 파악 : 원자력시설 컴퓨터시스템은 점점 더 통합되고 있으므로 컴퓨터시스템이 많이 사용될수록 공격대상 영역도 증가한다. 이러한 공격이 발생하면 공격의 목적, 동기, 전략 및 잠재적인 침입자를 식별하기 위하여 관련정보를 수집, 보존 및 분석하는 것이 중요하다. 이는 범죄 현장 및 디지털장치의 포렌직 분석을 통해서만 달성할 수 있다. 그러나 원자력시설에서 프로세스 제어시스템 구성 요소에 대한 디지털 포렌식의 증거 수집 및 분석은 새로운 영역이므로 이 연구에서는 원자력 안전 및 안보에 사용되는 시스템에서 컴퓨터보안 사고를 식별하고 수집하는 방법을 조사한다.

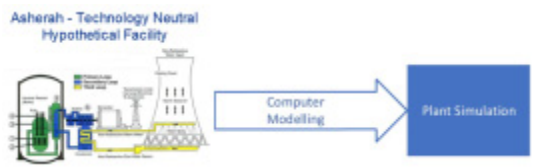
3.3. 개발 개요 및 참가 회원국/기관별 연구내용

3.3.1. CRP 개발 결과

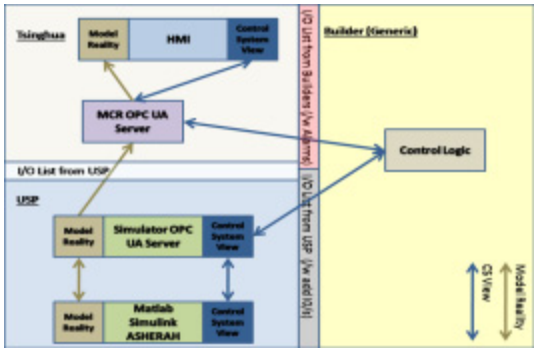
가상의 가압경수로(PWR) 모델/시뮬레이터를 개발하여 사이버공격이 원전에 미치는 영향성을 연구한다. 이 모델은 원전의 1차, 2차 및 3차 냉각 루프를 지원한다.

- ⊙ “Asherah”로 명명된 가상의 원전은 기존 PWR 설계를 기반으로 설계[그림 4]
- ⊙ 민감한 설계요소는 제거하고 다른 요소로 대체
- ⊙ 특정기술에 종속되지 않도록 설계
- ⊙ 모델은 HIL (Hardware in the Loop) 구조의 핵심

실제 산업에 사용되는 제어장비 (Siemens, ABB, Rockwell)를 가상의 원전(Asherah)모델/시뮬레이



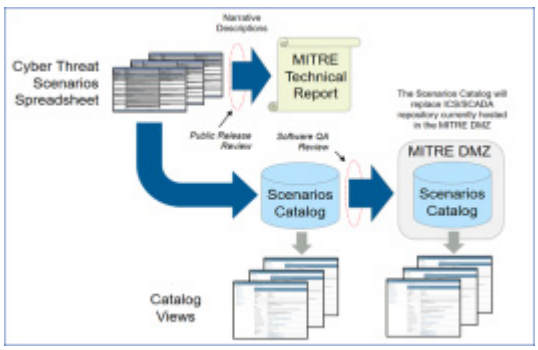
〔그림 4〕 Model/Simulator : Asherah NPP Simulator



〔그림 5〕 Coordination of Builders

터와 연계를 통해 기밀성, 무결성 및 가용성 (CIA)의 손상을 야기하는 취약점을 공격하므로써 사보타지의 결과를 결정한다〔그림 5〕. 또한, 위협 모델/시나리오를 개발하므로써 규제체제 (즉, DBT)에 대한 사례를 모사하기 위하여 테스트 Case를 개발한다〔그림 6〕.

이 시험결과를 바탕으로 컴퓨터보안 대책을 개발하므로써 원자력시설 기기 및 시스템에 대한 사이버공격을 방지하고 예방한다.



〔그림 6〕 Threat Modelers Activities

3.3.2. CRP 과제 구성 : 팀 역할

이 과제를 3개 그룹으로 역할을 나누어 수행한다.

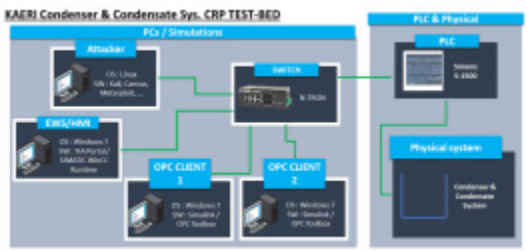
○ 설비/시스템 빌더 : 원자력 시스템의 모형 또는 시뮬레이터를 구축하는 팀 : 7개 기관 - AIT (Austria), University of Sao Paulo (Brazil), Otto von Guericke University Magdeburg (Germany), Korea Atomic Energy Research Institute (Korea), Canadian National Laboratory (Canada), University of Tenenssee Knoxville (USA), Tsinghua University (China)

○ 역량 제공 : 기 확보된 전문지식을 타 그룹으로 제공하는 조직 : 8개 기관 - CrySyS Labs (Hungary), CNEA (Argentina), Korean Institute of Nuclear Non-Proliferation and Control (Korea), Instituto Nacional de Investigaciones Nucleares (Mexico), National Centre for Nuclear Research (Poland), UL (USA), University of Massachusetts Lowell (USA), PAEC (Pakistan), GNRA (Ghana)

○ 위협모델 개발 : DBT, 시나리오 및 위협 전술, 기술 및 절차를 개발하는 조직 : 2개 기관 - Idaho National Laboratory (USA), MITRE (USA)

3.3.3. 시스템 빌더 연구 예

한국원자력연구원은 이 과제의 빌더그룹 중 하나로 참가하고 있다. 연구원은 PLC를 제어기로 사용하는 원전 2차계통 중 하나인 복수기 수위제어루프 Mock-up 및 복수계통에 대한 시뮬레이터(Simulink)를 개발하여 Asherah 시뮬레이터 (브라질 USP 개발) 및 제어실 HMI(중국 칭화대 개발)와 연계한다. 이 테스트베드를 통해 시나리오 기반의 사이버공격을 통한 다양한 사이버보안 시험 수행 및 사이버공격으로 인한 플랜트 영향성을 확인할 수 있도록 설계하였다[그림 7].



〔그림 7〕 복수기 및 복수계통 Testbed 구성도

Ⅳ. 향 후

이 연구과제는 지금까지 IAEA 사이버보안 부서에서 수행한 국제공동연구과제 중 규모 및 내용면에서 최대이다. 2016년 이후 이 과제에서는 다음의 내용을 수행하였다.

○ 시스템 빌더 및 역량제공 조직은 성공적으로 원전 모형 및 제어실 HMI를 개발.

○ 위협모델 개발자는 시스템 빌더 및 역량제공 조직을 위한 사이버위협 시나리오를 제공

○ 사이버보안 기술 (퍼징, 칼만 필터, 이상 탐지)이 개발되어 테스트베드에 시험 적용중

향후 나머지 연구와 함께 이 국제공동연구과제에서 개발된 모든 도구와 작성된 문서는 회원국이 교육 목적으로 사용할 수 있도록 개발될 예정이다.

참 고 문 헌

[1] KINAC/RS-015, “원자력시설의 컴퓨터 및 정보시스템 보안”, 한국원자력통제기술원, Dec. 2016.

[2] IEC-62645, “Nuclear power plants - Instrumentation and control systems - Requirements for security programmes for computer-based systems”, International Electrotechnical Commission, Aug. 2014.

[3] IAEA-TDL-005, "Computer security incident response planning at nuclear facilities", ISBN 978-92-0-104416-7, IAEA, June 2016.

〈저 자 소 개〉

이 철 권 (Lee, Cheol Kwon)

1980년 2월 : 경북대학교 전자공학과 졸업
1985년 2월 : 동아대학교 전자공학과 석사
2006년 8월 : 충남대학교 전자공학과 박사
<관심분야> 원자력 및 국가주요기반시설 사이버보안,