원전 사이버보안 현황 및 안전성 확보를 위한 중장기 R&D 전략

박 치 용
한국에너지기술평가원 전략기획본부 기술기획팀 원자력PD

1. 개 황

원자력발전(이하 원전)은 핵분열에 의해 발생한 에너지를 변환 이용하여 전기를 생산하는 것이다. 원전은 핵분열 반응에 의한 질량결손이 직접 에너지로 변환되어 방출되므로 일반 화학에너지에 비해서 효율이 매우 커서 1kg의 우라늄은 260만t의 석탄, 혹은 91만ℓ의 석유에 해당하는 에너지를 발생시킨다.

사이버보안은 사이버 환경에서 네트워크를 통해 연결된 조직, 사용자 자산을 보호하기 위해 사용되는 기술적 수단, 보안 정책, 개념, 보안 안전장치, 가이드라인, 위기관리 방법, 보안 행동, 교육, 훈련, 모범사례, 보안 보증, 보안 기술들의 집합으로 정의한다.

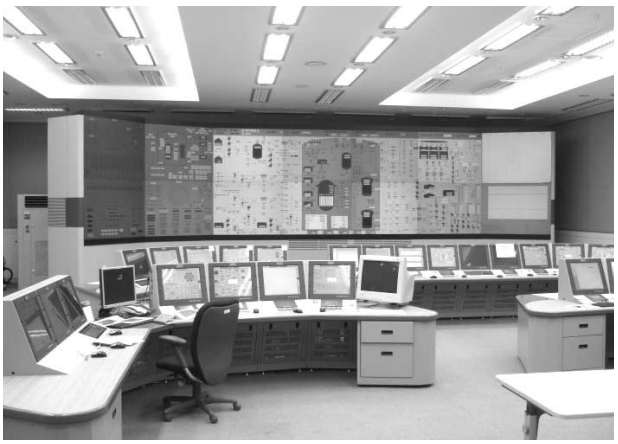
금융이나 지식산업 등 IT 기술을 사용하는 산업에서 사이버공격으로 컴퓨터시스템이 해킹당하거나 기능 마비를 일으켜 경제적 손실을 초래함에 따라 사이버 보안의 중요성이 대두되었다.

2. 원전 사이버보안의 연구배경, 침해사례 및 필요성

원전 사이버보안(NPP-CS[1])은 원전 계측제어계통과 사이버보안이 합쳐진 개념이다. 원전 계측제어계통은 원전 계통 또는 기기/장비로부터 각종 데이터를 취득, 분석, 처리하여 제어함으로써 원전의 안전한 운전을 담당하는 중추 신경계 역할을 수행한다. 그동안 아날로그 기술 기반의 원전 계측제어계통은 2000년대 들어 디지털 기술이 적용되기 시작하여 APR-1400부터는 전체 계측제어계통의 디지털화가 추진되어 원전에 디지털 기술을 적용함에 따라 사이버보안의 중요성도 높아지고 있다.

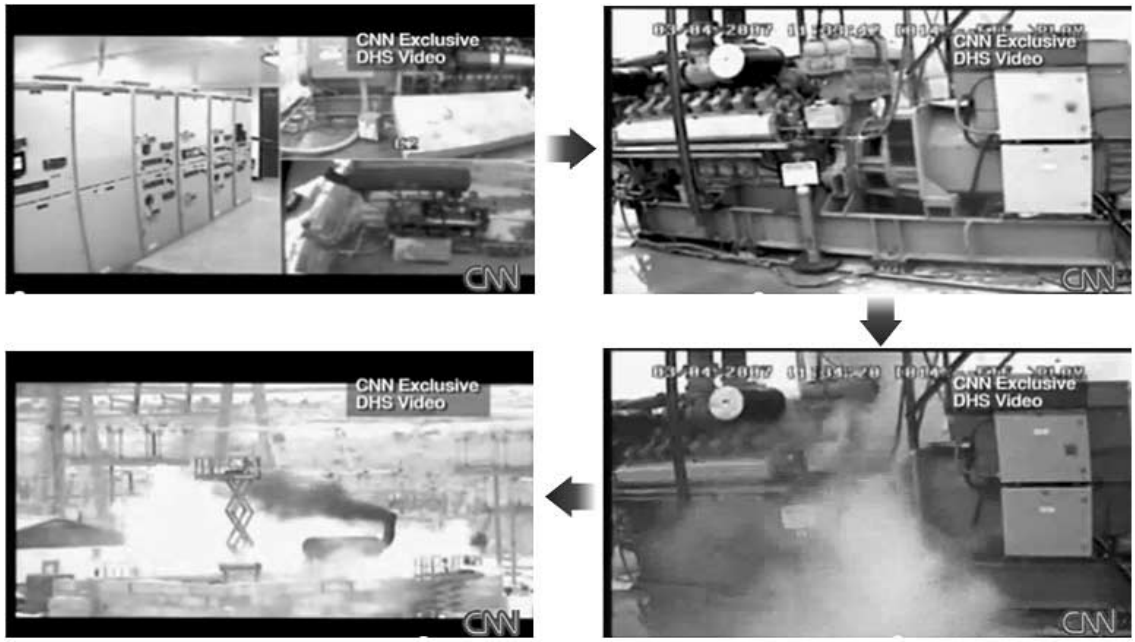
국가 주요기반시설인 원전은 물리적으로 분리된 전용망을 사용하고 있어 안전성이 고려되고 있으나, 만에 하나 사이버공격 사고로 원전 계측제어계통의 기능이 마비된다면, 원전의 정상운전은 물론 공공의 안전까지 위협당할 수 있다. 2010년 이란 핵시설의 주요 기반시설에 대한 스턱스넷[2] 공격 이후, 국가 주요 기반시설에 대한 체계적인 사이버보안 대책수립이 요구되고 있다.

스턱스넷, 듀큐[3]와 같은 APT[4] 공격으로 인해 물리적으로 분리된 전용망을 사용하는 원자력 제어시스템이라도



[그림 1] 아날로그 및 디지털 원전 계측제어계통

1) NPP-CS : Nuclear Power Plant Cyber Security
2) 스턱스넷(Stuxnet) : 이란 핵시설의 Siemens社 산업용 제어기기인 PLC(Programmable Logic Controller)를 감염시켜 오작동을 유발하기 위한 목적으로 개발된 바이러스
3) 듀큐 : Duqu, 스턱스넷과 유사한 구조의 바이러스지만 스턱스넷이 제어시스템의 파과가 목적이었다면 듀큐는 설계문서 등 핵심 정보를 수집하여 유출하는 것이 목적
4) APT : (Advanced Persistent Threat), 지능형 지속 위협



[그림 2] CNN 방송이 보도한 모의 사이버공격에 의한 발전기기 파괴 영상

사이버 공격 가능성이 지속적으로 제기되고 있는 상황이다. 미국 국토안보부와 아이다호 국립연구소(INL)에서 실시한 Aurora 취약점에 대한 사이버 공격은 발전기 자체의 보호메커니즘의 취약점을 공격하여 발전기를 파괴하였다.

원전 사이버보안 기술은 그 자체가 보안대상이기 때문에 선진기술의 도입이 어렵고, 원전 사이버보안 기술을 외국에 의존할 경우 국산 디지털계통 상세설계 내용의 유출이 불가피하여 보안성 유지에 허점이 발생할 가능성이 존재한다. 또한 계측제어계통의 설계변경 및 유지보수와

[표 1] 원전 제어시스템 침해 사례

사례	위협(위협원)	대비책
Davis-Besse 원전 슬래머 웜 감염	인터넷을 통한 제어시스템 침해 (악성코드)	사이버보안 예방, 강화기술 연구개발
Browns Ferry 원전 가동중지	대용량 네트워크 트래픽 발생으로 인한 기능 상실(PLC)	안전한 원전 제어시스템 관리, 테스트베드 구축
Hatch 원전 가동중지	검증되지 않은 S/W 업데이트 (업데이트 파일)	안전한 원전 제어시스템 관리, 테스트베드 구축
Stuxnet	인터넷을 통한 제어시스템 침해 이동저장장치(USB)를 통한 제어시스템 침해(적대적 국가, 악성코드)	사이버보안 예방, 강화기술 연구개발
Duqu	정보 유출(악성코드)	사이버보안 예방, 강화기술 연구개발
원자력분야 해킹 시도	인터넷을 통한 제어시스템 침해 시도 (적대적 국가)	사이버침해사고 분석 및 대응기술 개발

관련하여 사이버보안대책 수정이 필요할 경우 이를 해결하기에는 기술적, 시간적 문제가 발생할 것이다. 따라서 국내 자체적인 기술의 확보가 필요하며 이를 위해 국내 기술개발이 절실하다.

국내 원전산업에서 노력하고 있는 APR1400 및 OPR1000 수출에도 새로운 사이버보안 인허가 요건의 만족을 요구받고 있는 상황이므로 원전 사이버보안 요건을 독자 기술로 만족시켜 수출경쟁력을 증대시킬 필요가 있다. 원전 계측제어계통은 설계 및 개발과정에서부터 발전소 설치, 운전, 유지보수 및 폐기에 이르기까지 체계적으로 사이버보안 기술을 적용해야 한다. 이러한 원전 사이버보안 기술을 확보하기 위해서는 체계적이고 중장기적인 전략을 수립과 관련기술의 개발이 필요하다.

3. 원전 사이버보안기술 국내 · 외 현황

원전 안전성 확보를 위해 국내 · 외적으로 규제기관에서 원전 사이버보안에 대한 규제지침 개발 및 규제대상 범위 확대가 이루어지고 있으며, 이에 상응하는 원전 사이버보안 구현은 물리적 격리 및 전략 이행 계획수립 등으로 이루어지고 있다.

지속적으로 보편화되어 가는 사이버 공격기술에 대해서는 산업계 보안기술의 적용으로 이루어지고 있으나, 디지털화가 진행 중인 원전에 대한 고도화된 특정 대상 공격에 대해서는 첨단 기술개발을 통해 선제적 대응 기술개발 노력이 필요하다. 미국의 경우, 기존 원전은 계측제어계통이 아날로그 시스템이 대부분이고 디지털 기술이 적용되는 신규원전에 대한 건설이 활발하지 않음에도 불구하고, 사이버보안에 대한 필요성을 인식하고 원전 적용을 위한 기술개발이 활발히 진행 중이다.

국내에서는 원전 디지털 안전계통을 국산화하는 과정을 통하여 개발되는 계통에 대한 취약점 분석이 수행된 바 있다. 다른 나라에 비해 신형원전 개발과 신규원전 건설 그리고 원전 해외수출이 활발한 국내에서는 사이버보안에 대한 체계적인 연구를 위하여 기술체계 분석 및 방향 설정을 수립한 후에 원전 특성에 맞는 기술개발 추진이 필요한 실정이다.

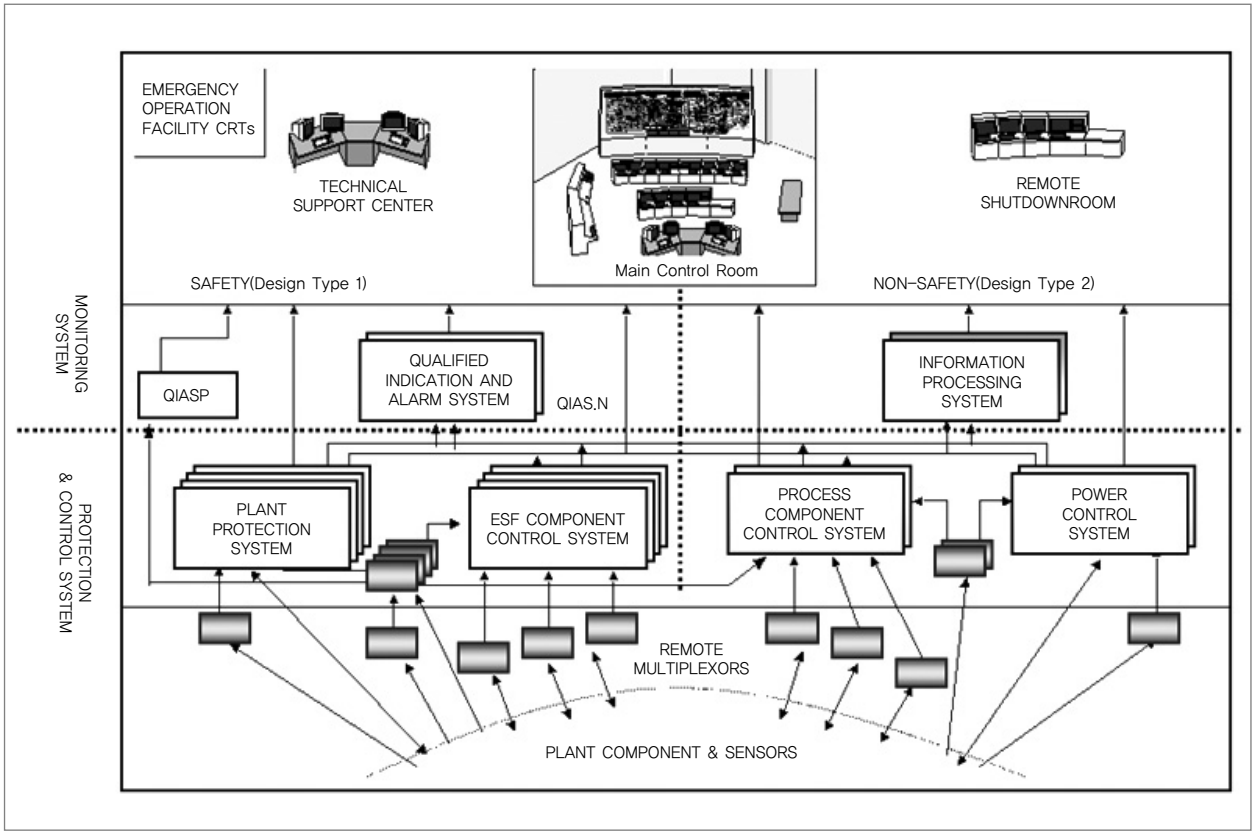
4. 원전 사이버보안 특성 및 적용대상

가. 원전 사이버보안 특성

원전 계측제어시스템의 사이버보안은 SCADA[5] 또는 ICS[6]가 가진 특성을 대부분 그대로 가지면서 다음과 같은 추가적인 특성을 가진다.

- 원자력 규제요건에 따른 심층방어설계의 적용
  - 엄격한 접근통제 및 원격접속 배제
  - 계통/기기의 안전 및 보안등급에 따른 단방향 통신
- 방사능 누출에 대비한 높은 안전성 및 신뢰성 요구
  - 원전 전용설비 적용
  - 원전 요건을 만족하는 가용성과 신뢰성, 혹독한 환경시험 요구
  - 주기적인 기기 시험
- 유지보수 특성
  - 핵연료 교체주기를 고려한 계획예방 정지
- 원전 규제 전문기관 존재

5) SCADA: Supervisory Control And Data Acquisition, 집중 원격감시 제어시스템 또는 감시 제어 데이터 수집시스템
6) ICS: Industrial Control System, 산업 제어시스템



[그림 3] APR-1400 원전 계측제어시스템 구조

나. 원전 사이버보안의 적용대상

국산 디지털기기가 적용된 한국형 원전(APR1400) 및 디지털 기술, 기기 또는 계통이 적용되고 상세설계 내용의 확보가 가능한 가동 중 원전의 다음과 같은 시스템에 적용한다.

- 계측제어계통(I&C systems)
- 보안시스템(Security Systems)
- 비상방재시스템(Emergency Preparedness Systems)
- 손상 시 이들 시스템 기능에 악영향을 미치는 지원 시스템(Support Systems)

비안전계통, 설계정보 저장장치 등 산업시설측면에서도 사이버보안 적용이 요구된다.

5. 원전 사이버보안 기술 시장 전망

호기당 원전 사이버보안 적용 비용 100억 원을 예상하여, 현재 가동 중인 해외원전 430기의 교체수명을 20년 정도로 보고 20%를 수주하는 가정을 적용하여 매년 평균 수출시장규모를 산정하였다. 이와 함께 국내의 경우 2030년까지 적어도 한번 이상 MMIS 설비를 교체해야 하므로 매년 1기 이상 설비교체를 예상하면 다음과 같은 시장규모가 예상된다.

국외 : (신규원전 4기 + 가동원전 4기) X (MMIS 공급가격)
1,000억 원 X (기여도) 10% = 800억 원/년
국내 : (신규원전 1기 + 가동원전 1기) X (MMIS 공급가격)
1,000억 원 X (기여도) 10% = 200억 원/년

6. 추진 방향 및 중장기 R&D 추진전략

가. 주요 추진방향

중장기적으로 사이버보안을 정착시키기 위해서는 정책 및 제도, 연구개발 및 인력양성이 동시에 진행되어야 하며 각 내용은 다음과 같이 구성된다.

- 정책/제도 : 원전 특화 사이버 보안기술 도출 및 기술 개발 추진체계, 원전 사이버보안 정책 수립, 원전 사이버 보안 프로그램 및 이행지침 수립
- 연구개발 : 원전 취약점 분석 및 보안대책 수립, 안전한 원전 운영을 위한 사이버보안 기술 연구개발(예방, 탐지, 대응, 분석 및 강화)
- 인력양성 : 원전 사이버보안 전문가 양성, 원전 사이버 보안 교육훈련

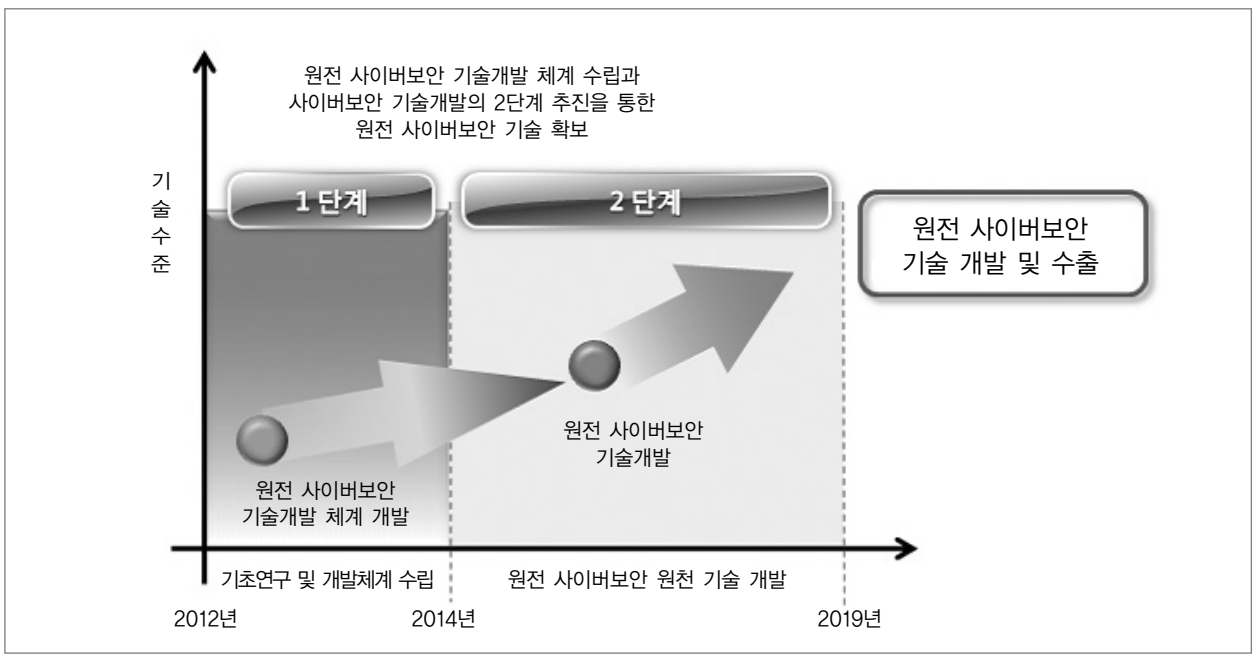
나. 추진전략 및 체계

원전 사이버보안 정책/제도 정비 및 사이버보안 기술 개발 체계를 수립하는 체계수립의 1단계와 1단계를 통하여 도출된 사이버보안 기술 과제를 개발하는 사이버 보안 기술개발의 2단계에 의한 체계적 원전 사이버보안 접근전략이 요구된다.

- **1단계 원전 사이버보안체계 수립** : 2014년까지 원전 사이버보안 현황분석, 정책 · 제도 정비 및 원전 사이버 보안 가이드라인 개발, 원전 사이버 보안 기술개발 체계 수립
- **2단계 원전 사이버보안기술 개발** : 1단계를 통하여 도출된 사이버보안기술 항목을 연구 · 개발하여 원전의 안전성을 확보하고, 원전 사이버보안 기술 개발 및 수출 기반 마련

원자력안전법에 의거, 관련 인허가요건에 따라 원전 사이버보안기술 개발이 요구된다.

- 안전등급 계통에 적용되는 기술은 엄격한 인허가 요건 준수
- 비안전등급 계통에 적용되는 기술은 산업시설 보호에서 요구되는 수준으로 검증



[그림 4] 원전 사이버보안 추진전략

설계생명주기 단계별 사이버보안기술 적용지침에 따라 설계, 개발, 운영에 따른 사이버보안 기술개발이 필요하다.

- 사이버보안 기술개발 과정에서의 보안성 확보 및 원전운영 중 사이버침해로부터의 보안 안전성 확보 방안
- 원전운영에 따른 주기적 사이버보안평가, 형상관리 및 감시 지침 개발

추진체계는 원자력 전문 연구기관, 보안기술 전문 연구기관, 원자력 운영 및 규제기관간의 협력을 통한 원전 사이버보안 체계수립과 보안기술 개발항목 도출 및 추진일정을 수립하여 국가적인 사이버 안전성 확보 체계를 구축한다.

7. 기대효과

원전 사이버보안 중장기 R&D의 성공은 안전성 향상, 경제성 제고 그리고 타 산업으로의 파급효과와 같은 다음과 같은 기대효과가 예상된다.

- 원전 사이버보안의 체계적이고 일관된 기술 개발 및 적용은 원전의 안전성, 신뢰성 및 가동률 향상에 기여
- 원전산업 전체에 사이버보안기술 적용을 통해 안전성 향상 및 긍정적인 사회인식 기여
- 사이버 공격에 의한 원전 불시정지와 복구로 인한 경제적 손실 방지
- 원전에 적용된 사이버보안 기술을 일반산업으로 파급하여 국가 주요 기반시설 전반의 사이버보안 강화 기대

'위기는 곧 기회'라는 말이 있듯이 후쿠시마 원전 사고는 많은 인명과 재산 피해를 초래했고, 원전시장의 르네상스 훈풍이 오기가 무섭게, 원전시장의 위축을 가져왔다. 하지만 과거 TMI 사고나 체르노빌 사고 발생 시에도 우리나라는 원전을 멈추지 않는 투자를 지속함으로써 원전의 기술자립을 이루어 냈다.

이럴 때 일수록 원자력분야 R&D에 과감한 투자가 필요하며, 원전 사이버보안 기술은 그 자체가 보안대상이기 때문에 선진기술의 도입이 어렵다. 또한 원전 사이버보안 기술을 외국에 의존할 경우 국산 디지털계통 상세설계 내용의 유출이 불가피하여 보안성 유지에 허점이 발생할 가능성이 존재하기 때문에 원전 사이버보안 R&D에 중장기적인 투자가 요구된다. 이와 함께 최신 기술 협력을 통한 시너지 창출 및 개발이 필요한 원자력 특화 사이버보안기술 도출이 필요하다.

현실적이고 실질적인 보안대책 수립 및 실용성 높은 사이버보안기술 도출과 일정 수립, 공동연구 및 워킹그룹의 운영을 통하여 원자력분야 전문가 및 학계의 다양한 의견을 수렴하는 것이 필요하다. 또한 전문 인력 육성과 원전 사이버보안 기술 인력의 저변 확대가 가능하도록 정기적으로 활발한 연구 활동을 통한 긴밀한 협력도 요청되고 있다.

따라서 지식경제부, 원전 전문 연구기관, 보안기술 전문 연구기관, 원전 전문 설계기관, 원전 운영 및 규제기관 등 전문가들의 공통된 노력을 통해 원전 사이버보안이 철저히 수행됨으로써 전방위적인 원전 산업발전 및 연관 분야의 시너지 효과가 창출되길 기대해본다. KEA

[참고문헌]

1. 박치용 외 산학연 전문자문위원단, 원전 사이버보안 안전성 확보를 위한 중장기 R&D 전략보고서, 한국에너지기술평가원(2012년.07월)