情 報 保 護 學 會 誌
第22卷 第5號, 2012. 8

원전 계측제어시스템 사이버보안 기술동향

이 철 권*

요 약

원자력발전소(원전) 계측제어시스템은 원전을 안전하게 운전하기 위해 계측, 제어 및 보호, 감시 기능을 수행하는 설비로서, 2000년대에 들면서 아날로그 기술에서 컴퓨터와 데이터통신망을 기반으로 하는 디지털 기술로 변하고 있다. 디지털 기술의 도입은 원전에 많은 이점을 부여하였지만 한편으로는 최근 이란 핵시설 및 중국에서 발생한 사이버 사고를 통해 디지털 계측제어시스템이 사이버공격으로부터 취약함이 입증되었다. 이에 따라 사이버보안 기술을 도입하여 원전의 안전성을 확보하기 위한 방안이 요구되고 있다. 하지만 원전 계측제어시스템의 최상위 설계요건으로 요구되는 안전성 확보는 복잡한 기기검증 절차와 긴 시간이 요구되는 인허가 과정 등으로 인해 사이버보안 기술을 적용하는데 많은 어려움이 따른다. 본 논문에서는 원전 계측제어시스템의 특성을 살펴보고 현재 국내외에서 개발 및 적용중인 원전 사이버보안 기술동향을 소개한다.

Ⅰ. 서 론

원전 계측제어시스템(NPP I&C)은 원자력발전소 두뇌와 신경망에 해당하는 설비로서 계측, 제어 및 보호, 감시 기능을 담당하는 설비이다. NPP I&C는 2000년대로 들면서 전자기술의 발전에 따라 아날로그 장비에서 컴퓨터 및 데이터통신망 등의 디지털 장비로 교체되고 있으며, 건설중인 신규 원전의 경우 센서를 제외하면 아날로그 장비를 찾기 힘들 정도이다. 이러한 디지털 기술의 도입은 기존 아날로그 장비에서 고려되지 않았던 사이버공격에 대한 대비책을 필요로 한다.

〔그림 1〕 아날로그 및 디지털 원전 계측제어시스템

원전 NPP I&C는 외부와 폐쇄된 상태로 운전하도록 설계되므로 사이버공격은 불가능할 것으로 예상했으나, 최근 이란 핵시설을 공격한 Stuxnet Virus와 같은 지능형 지속위협(APT) 공격에 매우 취약함이 입증되었다. 한편 지금까지의 NPP I&C는 사이버공격에 대한 설계를 고려하지 않았으므로 비록 사이버공격의 성공가능성은 매우 낮다하더라도 일단 침투하기만 하면 대응이 불가능한 수준이다. 따라서 국내외 규제기관에서는 원전 사이버보안에 관한 규제지침을 발표하고 원전 건설 및 운영 사업자가 이를 준수할 것을 권고하였다[1,2]. 미국은 2001년 911 사건 이후 이에 대한 연구를 많이 수행하여 왔으나, 국내의 경우 2006년 후반에 들어서야 NPP I&C 사이버보안에 관한 연구 필요성을 인식하였다.

본 논문에서는 NPP I&C 사이버보안 기술동향을 분석하고, 예상되는 사이버공격에 대비하여 원전의 사이버보안 안전성 확보를 위해 필요한 기술을 설명한다.

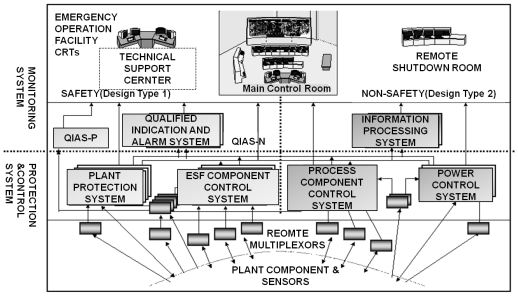
Ⅱ. 원전 계측제어시스템 사이버보안 현황

NPP I&C는 크게 원전 안전을 보장하기 위한 안전계통과 효율적인 전력생산과 관련한 비안전계통으로 구분되며, NPP I&C의 개략적인 구조는 [그림 2]와 같다. 안전계통은 원전 운전시 이상상태가 발생하면 즉시 원자

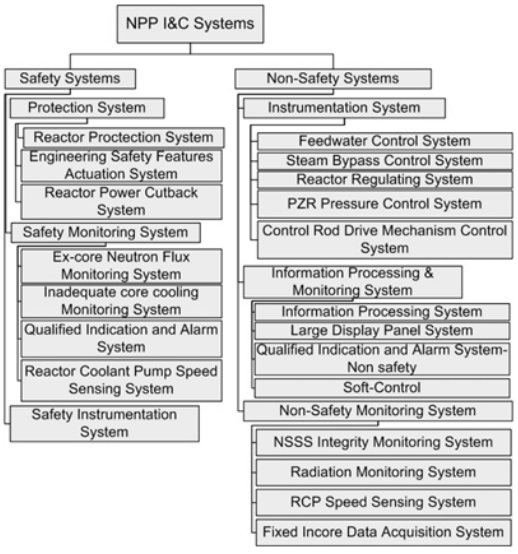
본 연구는 2010년도 지식경제부의 재원으로 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 원전기술혁신사업 연구 과제입니다. (No. 20101610100001E)

* 한국원자력연구원 계측제어.인간공학연구부 (cklee1@kaeri.re.kr)

로를 정지시키고 안전상태로 유지시키는 원전 고유한 시스템이다. 안전계통은 대부분 공급회사가 제한적인 원자력 전용의 장비를 사용하고 있으며, 이들은 예상가능한 모든 원전 사고상태에서도 운전이 가능하도록 설계된다. 비안전계통은 원전의 효율적인 운전에 필요한 제어계통 및 감시계통으로 구성되며, 일부 상용장비를 채택하고 있지만 많은 부분에서 원전 사업자가 요구하는 설계사양을 만족하도록 재설계되어 있다. NPP I&C를 구성하는 주요 계통들은 [그림 3]과 같다.



〔그림 2〕 원전 계측제어시스템 구조



〔그림 3〕 원전 계측제어시스템 종류

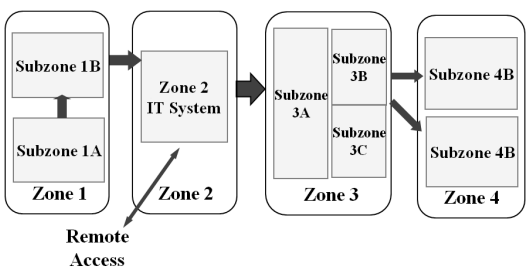
NPP I&C의 사이버보안 규제요건은 최초 안전계통만을 대상으로 하였으므로 안전계통에 대한 사이버보안 기술 적용방안을 연구해 왔다. 하지만 최근 미국 규제지침은 NPP I&C의 제어 및 감시계통을 포함하고 있으며, 나아가 원전 보안시스템 및 비상방재시스템으로 규제대상을 확대하여 사이버보안 기술적용을 요구하고 있다[3].

2.1 사이버위협 대응수준

전세계적으로 가동중인 원전은 외부망 차단을 통해 NPP I&C에 대한 원격 사이버공격이 가능한 접근경로를 원천 차단하고 있다. 또한, 신규원전의 경우 NPP I&C 설계과정에서 물리적 보안 및 접근통제 강화, 심층방어구조 적용 등을 통해 사이버보안에 대한 대비를 하고 있다. 그러나 현재 NPP I&C에 직접 적용가능한 사이버보안 기술이나 기기는 많지 않으며, 연구기관과 산업체가 이들 개발을 위한 관련 R&D를 추진중에 있다.

2.2 원전 계측제어시스템 사이버보안 등급

NPP I&C는 각 계통별로 부여된 안전등급을 고려하여 설계된다. 안전계통과 비안전계통 간에는 엄격한 독립성요건을 적용하여 비안전계통에서의 어떠한 기능손상이 안전계통으로 전파되지 않도록 하므로써 안전계통의 기능수행을 보장하고 있다.



〔그림 4〕 원전 계측제어시스템 사이버보안 등급

- Zone 1 : 보호계통 및 제어계통, Zone 2 : 감시계통 및 제어실
- Zone 3 : 원전 사무용 컴퓨터시스템, Zone 4 : 원전 Site 외부

규제지침은 NPP I&C 설계에 안전등급과 유사한 그림 4와 같은 사이버보안 등급을 적용하도록 권고하고 있다[4]. 즉, NPP I&C에 대한 보안성평가를 수행하여 계통별로 보안등급을 구분하고 보안등급에 따라 보안설계 요건을 차등화하여 NPP I&C 설계에 반영하므로서, 상대적으로 보안등급이 낮은 Zone은 높은 Zone으로 정

보를 전달할 수 없도록 경계설계하여 심층방호개념이 확보되게 한다.

2.3 관련 규제지침 및 법령

원전 사이버보안과 관련하여 발표된 국내외 규제지침 및 법령은 다음과 같다.

- 2005년 미국 NEI 04-04(Rev.00)
- 2006년 미국 Reg. Guide 1.152(Rev.02)
- 2007년 국내 KINS 내부지침 (GT-N27)
- 2009년 미국 10 CFR 73.54
- 2009년 국내 KINS 규제지침 8.22
- 2010년 미국 NEI 08-09(Rev.05)
- 2010년 미국 Reg. Guide 5.71
- 2011년 IAEA Tech. Guidances NSS-17
- 2011년 미국 Reg. Guide 1.152(Rev.03)

이 문서들은 계속해서 개정되고 있으며, 다음과 같은 필수지침을 포함한다.

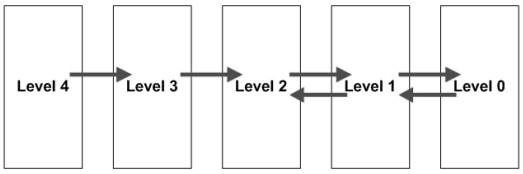
- 원전 수명주기 단계별 사이버보안 적용
- 안전한 개발환경 및 운영환경 확보
- 원전 운영시 주기적인 사이버보안성 평가

또한 미국규제지침 RG 5.71은 원전 사이버보안 적용을 위한 계획서 작성용 템플릿과 함께 사이버보안 기술적용을 위한 보안컨트롤들을 상세히 제시하고 있다. 그러나 보안컨트롤을 NPP I&C 설계에 반영하기 위해서는 시스템에서 요구하는 안전성요건과 사이버보안 설계요건 간의 연계를 해결하기 위한 노력을 필요로 한다.

Ⅲ. 원전 계측제어시스템 사이버보안 특성

일반적으로 산업제어시스템은 범용기술을 사용함으로써 IT 시스템과 같은 취약성을 내포할 수 있다. 하지만 NPP I&C는 다음과 같은 특징으로 IT 시스템의 취약성을 이용한 공격이 매우 어려울 것으로 예상된다.

⊙경계 정책 : NPP I&C는 안전계통과 비안전계통을 명확히 구분하여 비안전등급의 계통에서 안전등급의 계통으로 데이터 전송을 허용하지 않는다. 또한 NPP I&C는 외부 인터넷 망으로 부터의 연결점이 존재하지 않는다. [그림 5]는 IAEA 기술지침 및 미국 규제지침 RG 5.71의 심층방호 내용으로서, NPP I&C는 각 계통별로 보안등급을 구분하여 경계정책을 반영하여야 한다. 원전에서 NPP I&C는 대부분 보안등급이 3과 4로 부여되며 원격 접근이 허용되지 않는다.



〔그림 5〕 사이버보안 심층방호구조 요건

⊙어플리케이션 보안 정책 : 안전계통 어플리케이션 보안정책은 규정된 접근통제 정책에 따라 접근이 제한되며, 정상행위 수행 여부를 오랜 기간 검증을 통해 프로그램의 오류를 철저히 평가한다. 또한 개발된 소스코드에 대해 내부 구조를 철저히 분석하는 화이트박스(white box) 테스트 및 생명주기 단계별 확인 및 검증(Verification and Validation)를 수행함으로써 기능, 성능, 보안성, 신뢰성, 안전성을 종합적으로 검토하고 규제기관으로부터 인허가 승인후 기술을 반영한다. 따라서 이상동작을 하는 프로그램 또는 검증되지 않는 어플리케이션은 NPP I&C에 적용되지 않는다. 아래 내용은 어플리케이션 보안 정책을 만족하기 위해 반드시 수행되어야 하는 항목을 보여준다.

- 소프트웨어 취약성 분석 수행
- 소프트웨어 수명주기 단계별로 소프트웨어 V&V 및 안정성 분석
- 상용제품 도입에 따른 상용제품 인증 수행

⊙계통의 독립성 및 다중화 : NPP I&C는 각 계통이 독립성을 유지하도록 설계되며, 각 계통별로 안전성을 강화하기 위해 다중화가 적용된다. 즉, 한 계통에서 발생한 고장이 다른 계통으로 전파되기는 매우 어려우며, 각 계통내 한 채널에서 오작동이 발생하더라도 다중채널 구성으로 오작동을 보완하기 위한 장치들이 준비되어 있다. 특히, 디지털 장치의 고장에 대비하여 아날로그 장치를 이용한 다중화 설비가 제공되며, 이는 사이버 공격시 대응가능한 한 방편이 될 수도 있다.

⊙NPP I&C 전용장비 사용 : 원전 안전계통에 사용되는 PLC는 안전계통 및 안전관련 계통에 적용하기 위한 장비로써, 랙(rack), 버스모듈, 전원모듈, 프로세서모듈, 통신모듈, 디지털 입/출력모듈 등 안전계통 구성에 필요한 공급회사 전용장비이다. 이들은 범용기술을 최소화하고 인허가과정 및 상용인증을 통해 안전성을 검증함과 동시에 자체 개발 및 응용 기술을 적용하고 있

으므로 범용기술에서 알려진 사이버보안 취약성 활용이 용이치 않을 것이다. 사이버보안 관점에서 비교한 IT 시스템, SCADA 및 ICS, NPP I&C의 차이점은 [표 1]과 같다[5].

〔표 1〕 IT 시스템, SCADA 및 ICS, NPP I&C의 차이

구분	IT 시스템	SCADA 및 ICS	NPP I&C
성능 요건	- 비실시간 - 일관적인 응답 - 고성능 처리량 - 시간지연 수용가능	- 실시간 - 시간이 중요한 응답 - 적정한 처리량 - 시간지연 수용곤란	- 좌동
가용성 요건	- 재부팅 수용가능 - 시스템 작동 요건에 따라 가용성 결함 허용	- 공정 가용성 요건 때문에 재부팅 수용불가 - 정지는 수일/수주전 미리 계획 - 철저한 시험으로 높은 가용성 요구	- 재부팅 수용불가 - 연차보수 적용 - 최고 수준의 가용성, 기능성, 내환경시험 요구
위험 관리 요건	- 데이터 기밀성 및 무결성이 최대 목표 - 상대적으로 덜 중요한 내고장성, 순간적 정지는 중요하지 않음 - 중요 위험은 사업운영의 지연임	- 인명안전이 최우선, 다음으로 시설 보호 - 내고장성 필수, 순간적 정지 수용불가 - 중요한 위험은 규제 불만족, 인명, 장비, 생산의 손실임	- 좌동 - 원자로 안전성 및 핵물질 방호를 추가적으로 고려해야 함
시스템 구조 보안	- IT 자산 및 정보(저장된 혹은 전송되는)의 보호 - 중앙 서버는 보호가 요구됨	- 말단 클라이언트(예, 공정 제어기기와 같은 필드 기기)의 보호가 최우선 - 중앙서버의 보호도 중요	- 안전등급 순위를 고려한 보안 등급 설정 필요 - 보안위협의 안전성 위해도평가 필수
의도되지 않은 결과	- 보안 솔루션들은 대표적 IT 시스템 중심으로 설계됨	- 보안도구들이 ICS 동작을 방해하지 않는지 시험해야 함	- 보안기능이 시설의 안전성 및 성능에 악영향이 없도록 검증
상호작용 시간 중요도	- 상대적으로 덜 중요한 긴급 상호작용 - 필요에 따라 엄격한 접근 통제가 구현 가능함	- 사람에 대한 응답과 기타 긴급 상호작용이 중요함 - ICS에 대한 접근이 엄격히 통제되어야 하나 인간-기계 상호작용을 방해하지 않아야 함	- 좌동 - 안전계통 및 비안전계통 감시 및 제어 수단의 신호적 및 물리적 분리
시스템 운영	- 시스템이 대표적 OS에 맞게 설계됨 - 업그레이드는 자동화된 툴이 있어 손쉽게 이루어짐	- 보안 기능이 없는 변종 및 주문 제작형 OS 사용 - 소프트웨어 변경은 신중히 이루어짐. 특수한 제어 알고리듬, 하드웨어 및 소프트웨어 변경이 수반되므로 일반적으로 판매자에 의해 이루어짐	- 좌동 - 안전성/신뢰성 관련 업무 추가 - 규제기관의 심사/검사 필수
자원 제약	- 보안 솔루션과 같은 제3자 어플리케이션 추가를 지원할 수 있도록 시스템 자원이 충분함	- 시스템이 산업공정에 맞게 설계되어 보안 솔루션을 추가하기에 최소한의 메모리와 연산 능력 보유	- 좌동 - 다중화/다양성 설계에 대한 고려 필요
통신	- 표준 통신 프로토콜 - 국지적 무선 통신 기능을 가진 유선 통신 기반 - 대표적 IT 네트워크 사용	- 많은 독점적 및 표준 프로토콜 - 전용 유선 및 무선(radio 및 위성)을 포함한 여러 유형의 통신 매체 사용 - 복잡한 네트워크 사용, 때로는 제어 엔지니어가 필요함	- 좌동 - 무선 통신은 일반적으로 허용치 않음
변경 관리	- 소프트웨어 변경은 좋은 보안 정책과 절차 하에 시기 적절히 이루어짐. 절차는 종종 자동화됨	- 제어시스템의 무결성 유지를 보장하도록 소프트웨어의 변경은 철저히 시험되고 시스템에 점진적으로 이행됨. ICS 정지는 수일/수주전 계획되어야 함	- 좌동 - 안전성/신뢰성 평가 추가 - 변경에 대한 인허가 심사/검사 - 핵연료 교체주기에 맞춘 연차보수 시 변경
지원 관리	- 다양한 유형의 지원이 가능함	- 대부분 단일 판매자에 의해 지원됨	- 좌동
기기 수명	- 3-5년	- 15-20년	- 좌동
기기 접속	- 기기들이 보통 근거리에 위치하고 접근이 용이함	- 기기들이 고립되고 원격에 위치하며 접근하기에 과도한 물리적 노력이 요구될 수 있음	- 좌동

Ⅳ. 원전 계측제어시스템 사이버보안 연구현황

향후 예상가능한 원전사고 중 하나로 원전 사이버보안이 거론되고 있으며, 이에 따라 원자력산업에서 시급히 대비책을 강구해야 하는 현안중 하나로 인식되었다. 따라서 전세계 원자력산업 관련국에서는 이에 대한 R&D를 추진하고 있다.

4.1 국내 기술개발 현황

현재까지 NPP I&C 디지털장비의 국산화 및 원전 적용 경험을 보유한 국가는 많지 않다. 그 중 디지털 기술에 가장 발빠르게 대응하고 있는 국내 원자력 산업은 규제기관인 원자력안전기술원(KINS)과 한국원자력연구원(KAERI)을 중심으로 전문설계기관과 기기공급회사들과 협력하여 원전 사이버공격에 대응한 연구를 수행하고 있다. KINS는 교과부 지원으로 NPP I&C 사이버보안 인허가심사를 위한 평가기술을 개발하였으며, 원전을 운영하는 한수원과 한전 자회사인 설계회사 및 기기공급사는 신규원전에 사이버보안요건을 반영하기 위한 설계를 수행함과 동시에 가동원전에 대한 보안성 평가를 수행하고 원격 사이버공격으로부터 원전을 보호하기 위한 방안을 강구하였다. 이러한 몇 가지 국내 연구내용 예는 다음과 같다.

4.1.1 KNICS 안전계통 사이버보안 정책 연구

한국원자력연구원은 2001년부터 2008년까지 NPP I&C 국산화 (KNICS) 사업을 통해 안전계통 즉, 안전등급 제어기기, 원자로보호계통, 공학적안전설비기기제어계통을 국산화하는 과정에서 이들의 사이버보안 목표를 달성하기 위한 기준에 대한 연구를 수행하였다. 본 연구에서 보안정책, 데이터 정책, 악성 소프트웨어 방호, 플랫폼 보안, 통신 보안, 작업자 보안, 감사, 어플리케이션, 물리적 방호 정책을 제시하였으며, 이들의 적용방안에 대해서도 연구하였다.

4.1.2 원전 사이버보안 위험도 분석/평가시스템 개발

한국원자력연구원은 지식경제부(에너지기술평가원)의 지원을 받아 NPP I&C 사이버보안에 대한 규제지침을 분석하여 위험도 분석 및 평가도구를 개발하고 있다. 이는 NPP I&C 설계 및 개발과정에서 체계적으로 사이버보안 요건을 반영하고, 나아가 운영과정에서 사이버보안성을 유지하도록 기술적으로 지원하는 소프트웨어 도구이다. 이 도구는 NPP I&C 계통 및 기기설계 분석, 사이버보안 침투시험 결과 등의 데이터를 기반으로 하여, 미국 규제지침 RG 5.71 규제요건을 기준으로 평가를 수행한다.

4.1.3 NPP I&C 사이버보안 종합대책기술 연구

원자력안전기술원은 NPP I&C 사이버보안 워킹그룹을 통해 사이버보안 종합대책기술 보고서를 발간하였다. 연구내용은 미국 규제지침 RG 5.71에 기초하고 있으며, 디지털 컴퓨터 시스템, 통신설비 및 네트워크 분석, 심층방어 보호전략, 보안 통제, 운영 통제, 관리적 통제 등 사이버보안 프로그램의 수립과 이행 방법을 포함하고 있다[6].

이 외에도 국내에서는 정부주도로 KAERI와 국가보안기술연구소, 관련 산업체들이 참여하는 원전 사이버보안 기술개발을 위한 장기적인 R&D를 추진중에 있다.

4.2 국외 기술개발 현황

2002년 이후 가장 많은 R&D를 수행하고 있는 미국은 원전 사이버보안 대응을 위해 규제지침 및 법을 제정하였으며, 이를 근거로 신규 원전은 물론 가동원전에 대하여 2012년까지 상세이행 계획을 미국원자력규제위원회(NRC)에서 심사하고 있다. 또한 아이다호 국립연구소 (INL) 등 국가연구소에서는 Test-bed 및 비상대응팀(CERT)을 운용하고 있으며, 국가가 필요로 하는 전문인력 양성도 병행하고 있다[7]. 유럽에서도 국제원자력기구(IAEA)를 중심으로 프랑스와 독일, 영국, 노르웨이 등이 적극 참여하여 관련 연구를 진행중이며, 일본이나 중국 또한 자체적으로 대비책을 마련하고 있을 것으로 예상된다. 원전 사이버보안은 업무 특성상 연구결과가 공개되지 않기 때문에 참조할 수 있는 정보가 극히 제한적이므로 상세 연구내용이나 수준은 알 수 없고 단지 발표되는 단편적인 연구결과와 학술지의 논문을 통해 간접적으로 추정할 뿐이다.

Ⅴ. 원전 계측제어시스템 사이버보안 적용 방향

NPP I&C는 이미 외부망 차단 및 원격접속배제, 경계정책 및 어플리케이션 보안정책 적용, 계통의 독립성 및 다중화 설계, 장비의 특수성 등으로부터 사이버보안에 대한 기초적인 대응이 이루어지고 있다고 할 수 있다. 하지만 이러한 대응수준은 최근 Stuxnet 사례에서 볼 수 있듯이 공극(Air gap)을 극복한 신종 사이버공격으로부터 안전성을 장담할 수 없기 때문에 NPP I&C에 적용가능한 보안기술의 연구가 요구된다. 아래는 NPP I&C 사이버보안 강화를 위해 요구되는 필수기술에 대한 개발요건들이다[8].

- 사용자, 시스템 및 장비의 접근통제 기술
- 모니터링 기술 : HIDS 및 NIDS를 이용한 네트워크 모니터링 기술 적용
- 보안 이벤트 정의 및 기록
- 보안감사 기능
- 계측제어장비 식별 및 관리 기능

상기 보안기술은 NPP I&C에 악의적 사용자가 악의적 행위를 하기 위해 이미 내부에 침입을 시도할 때 이를 방지하거나 또한 침입이 성공하였을 때 이들의 침입을 파악하고 행위를 인지하기 위한 기술들이다. 하지만 이러한 기술들을 반영하기 위해서는 사용하고자 하는 보안장비 및 소프트웨어를 원전 규제기준 맞도록 개발하고 검증하여야 한다[9]. 즉, 보호하고자 하는 대상 장비들의 안전 및 보안 등급에 따라 개발과정에서 소스분석, 개발환경 통제, 상용 프로그램 사용시 상용제품인증 수행 등을 거치고, 이들 각각에 대한 V&V를 수행하여 인허가를 획득하여야 한다. 또한 적용되는 보안장비는 NPP I&C의 가용성을 보장함과 동시에 원전의 안전, 보안 및 비상방재 기능수행에 나쁜 영향을 주지 않아야 한다. 따라서 NPP I&C 사이버보안 기술을 개발하기 위해서는 다음과 같은 연구가 요구된다.

- 실제 시스템을 축소화 한 기기/계측제어계통/발전소를 포함하는 TEST-BED 구축을 통한 취약성 분석
- NPP I&C 컴포넌트 특성을 반영한 사이버침투시험 도구 개발
- 규제요건에 만족하는 모니터링 기술 개발
- 침투시험을 통한 계통별/컴포넌트별 영향성 분석
- 중요 자산에 따른 다중 보호 정책 및 기술 개발
- 주기적 사이버보안 시험 및 감사 절차 확립
- 사이버공격 대응 운전원 교육 및 훈련

Ⅵ. 결 론

본 논문에서는 NPP I&C 사이버보안 기술 동향에 대해 설명하였다. 디지털장비의 NPP I&C 도입은 현재 거의 완성된 수준이지만, 운전성 및 안전성 향상을 위해 향후 지금보다 더욱 지능화된 기기들을 적용하기 위한 연구들이 계속 진행될 것으로 예상된다. 이에 따라 고도화되고 다양한 NPP I&C 사이버보안 기술이 지속적으로 요구될 것이다. 또한 전자 및 정보산업의 기술발전을 반영하면서 동시에 국내 원전의 사이버보안 안전성을 확보하기 위해서는 관련기술의 개발과 함께 이들을 체계적으로 원전에 적용하기 위한 연구가 뒤따라야 한다. 이를 위해서는 연구기관과 한수원을 비롯한 설계사와 기기공급사의 원전산업, 국가 사이버보안 유관기관 및 IT 사이버보안산업의 융합연구가 절실히 요구된다.

참고문헌

[1] 한국원자력안전기술원, KINS/RG-NO 8.22, 계측제어계통의 사이버보안, 2007.

[2] 미국 NRC, R.G. 1.152, Rev. 02, Criteria for Use of Computers in Safety Systems of NPPs, 2006.

[3] 미국 R.G. 5.71, Cyber Security Programs for Nuclear Facilities, U.S. *Nuclear Regulatory Commission*, 2010.

[4] IAEA, Nuclear Security Series (NSS) No. 17, Tech. Guidance, “Computer Security at Nuclear Facilities”, 2011.

[5] 미국 NIST, SP800-83, Guide to Industrial Control Systems (ICS) Security, 2011.

[6] 한국원자력안전기술원, KINS/ER-199, 원전 계측제어계통 사이버보안 종합대책 기술보고서, 2011.

[7] 미국 US-CERT, Control System Security Program, http://www.us-cert.gov/control_system/ict_cert/.

[8] Jung-Woon Lee, Cheol-Kwon Lee, Jae-Gu Song, and Dong-Young Lee, “Cyber Security Considerations in the Development of I&C Systems for NPPs,” *The 2011 International Conference on Security and Management* (SAM2011), Las Vegas, Nevada, July 18-21, 2011.

[9] IEEE Standard 7-4.3.2-2010, Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, 2010.

〈著者紹介〉

이 철 권 (Lee, Cheol Kwon)
비회원
1980년 2월: 경북대학교 전자공학과 졸업
1985년 2월: 동아대학교 전자공학과 석사
2006년 8월: 충남대학교 전자공학과 박사
1985년 3월~현재: 한국원자력연구원 계측제어.인간공학연구부 근무
<관심분야> 원자력 계측제어, 원자력 사이버보안