정보산업동향

원자력발전소 계측제어계통사이버보안 적용 동향

정광일·이준구·박근옥 (한국원자력연구원)

목 차 »

1. 서 론
2. 원전 적용 규제지침 및 산업표준 동향
3. 원전 계측제어계통 사이버보안 적용
4. 국내 규제기관의 최근 동향
5. 결 론

1. 서 론

최근 원자력발전소(이하 원전)는 점차 디지털화된 기기 및 통신망을 채택하여 사용하고 있다. 특히 원전의 두뇌 및 신경망에 해당하는 계측제어계통의 경우, 디지털화가 빠르게 진행되고 있다. 현재 계측제어계통 중에서 특정 계통의 설계상의 요건에 따른 아날로그 기기 사용 및 수동 스위치 사용 등과 같은 특이한 경우를 제외하고는 거의 모든 계측제어계통 기기 및 통신수단이 디지털화되고 있고 자동화되고 있다. 그러나 이러한 디지털화가 가속됨에 따라 비안가된 기기 또는 사용자가 디지털 기술의 본질적인 취약성을 악용하여 원전의 운전 및 운영에 위협을 주고 있다. 원전의 환경은 다른 일반 상용 환경 및 산업환경과는 다르게 원전의 고유 특성, 즉 안전성, 신뢰성, 보안성, 결정론성, 검증성, 격리성 등을 만족해야하며, 이를 만족하지 못할 경우 경제사회 및 일반대중에게 많은 위협 요소를 가질 수 있다. 원전 계측제어계통에서 사이버 상의 보안 문제는 새로운 취약성을 이용한 공격 등으로 인하여 대응책 미비 및 공격 주체를 찾을 수가 없어 어떠한 피해를 입었는지조차 파악할 수 없는 큰 문제점을 가지고 있다. 특히 원전의 경우 일반 상용 IT 시스템과는 다르게 실시간성, 운전특성, 침해특성 및 위험관리 목표 등 여러 면에서 특성이 다르므로(표 1), 이러한 사이버위협으로 인하여 원전의 가동이 멈출 수 있고, 심지어 크나큰 재앙을 일으킬 수 있는 안전-필수 인프라(safety-critical infrastructure)이다. 따라서 원전에서 사이버 위협에 대응한 사이버보안 기술 적용이 중요한 과제로 떠올랐다.

현재 원전에서의 사이버보안 기술의 적용에 대해서는 많은 연구가 진행되고 있고, 규제기관 및 산업표준 기관 또한 이와 관련하여 새로운 규제지침 및 산업표준을 제시하고 있다. 그러나 이러한 규제지침 및 산업표준에서는 절차적, 기술적 사항을 일부 제시하고 있으나, 구체적인 방법적

〈표 1〉 일반 IT 시스템과 원전계측제어 시스템의 특성

구분	IT 시스템	원전 계측제어 시스템
실시간성	비 실시간성	실시간성
지연 특성	시간 지연 일부 허용	시간 지연에 민감
전송대역폭	고대역폭/고성능 처리	낮은 대역폭/적정 처리 용량
응답시간 특성	응답성능 중요	응답 시간 중요
운전 특성	운전정지에 둔감	운전정지에 민감
시스템 설계 특성	짧은 생명주기(5~10년)	긴 생명주기(원전수명 60년)
고장 특성	복구 용이	복구 어려움
침해 특성	정보노출, 경제적 영향	대중 보건 및 자연환경 영향
유지보수 특성	잦은 소프트웨어 및 네트워크 구조 변경	품질보증절차에 따른 엄격한 유지 보수
보안특성	기밀성/무결성	기밀성/무결성/가용성
위험관리 목표	데이터의 기밀성/무결성	원전의 안전, 인간/자연환경의 안전

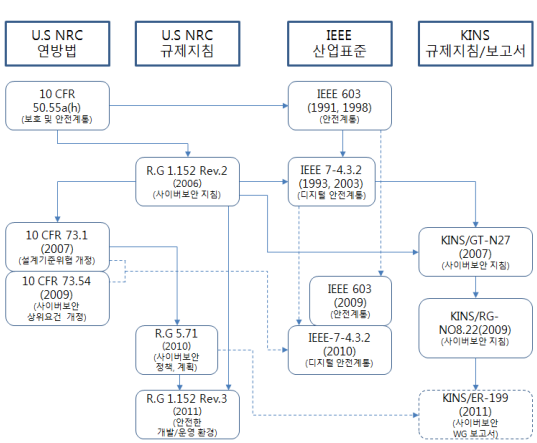
및 행정적 사항을 제시하지 못하고 있는 실정이다. 또한 위에서 제시한 바와 같이, 원전에 일반 IT 사이버보안 기술을 적용하는 경우 원전의 검증성 및 결정론성을 만족하여야 한다. 즉, 원전에 적용된 사이버보안 기술은 검증을 통하여 그 기능이 정확하게 동작함을 보임은 물론이고, 신뢰성, 안전성, 실시간성 및 결정론성을 저해하지 않음을 보여야만 한다. 또한 원전에 사이버보안 기술 적용으로 인하여 원전 특성 및 기능성을 저해하지 않아야 한다.

그러나 원전에 대한 사이버 위협 및 공격사례는 현재 세계 각국에서 다양하게 보고되고 있다. 2003년 미국 데이비스 베시(Davis-Besse) 원전의 컴퓨터 네트워크에 슬래머웜이 침투하여 부지 내 네트워크에 대량의 데이터가 전송되어 원전 정보망이 영향을 받게 되었다. 이에 따라 안전변수지시계통과 발전소 컴퓨터 계통의 운전이 정지되는 침해 사고가 발생하였다. 이는 보안 요구사항을 무시하고 보안 특성에 대한 인식의 부족이 원인이 된 사고였다. 또한 2007년 DHS (Department of Homeland Security)는 사이버 공격 시험을 통하여 실제 원전의 디젤발전기를 정지시킬 수 있었으며, 2008년 미국 회계감사원은 미국 최대 국립전력회사인 TVA사 제어시스템을 모의 해킹하여 발전소 제어시스템에 침투할 수 있었다. 2010년 스턱스넷(Stuxnet) 바이러스는 원전의 제어시스템을 침투하여 이란의 나탄즈 원자력 원심분리기의 일부 기능을 마비시키는 공격사례가 있었다. 이러한 공격사례들을 통하여 원전은 사이버 해커들이 고의로 공격하고자 하면 위협 및 침해받을 수 있는 다양한 루트가 존재함을 알 수 있다. 이로 인하여, 원전관련 규제기관 및 산업표준 기관은 원전에 작용할 수 있는 요건, 규제지침 및 산업표준을 잇따라 내놓거나 수정 및 개정하고 있다. 원전 운영자 및 설계자들은 이러한 원전관련 요건, 규제지침 및 산업표준에 따라서 운영 및 설계하여야 한다.

2. 원전 적용 규제지침 및 산업표준 동향

국내 원전에서 많이 적용되는 규제지침으로는 미국의 원전 규제기관인 미국 원자력 규제위원회(U.S NRC : U.S Nuclear Regulatory Commission)에서 발행한 10CFR(Code of Federal Regulatory) 및 Regulatory Guide(이하 R.G)가 있으며, 국내 원전 규제기관인 한국원자력안전기술원(KINS : Korea Institute of Nuclear Safety)에서 발행하는 각종 규제지침과 관련 보고서가 있다. 또한 원전에 많이 적용되는 산업표준으로서 IEEE에서 발행하는 표준문서가 있다. 따라서 본 절에서는 위의 규제기관 및 산업표준에서 사이버보안 관련 주요활동을 생산된 문서를 통하여 간략히 정리하였다.

10CFR50.55a(h)는 원전에서 사용하는 안전계통(safety system)의 보안(security)이 중요하며, 계통설계에 고려되어야 함을 기술하고 있다[1]. 이러한 내용을 승인하고 반영하여 IEEE Std. 603(1998년)은 안전계통 설계에 “control of access” 보안 요건을 통해 안전계통 소프트웨어 및 하드웨어에 대한 물리적/전자적 접근을 통제하기 위한 규제지침을 기술하였다[6]. IEEE 7-4.3.2(2003년)는 디지털 안전계통에 대한 상세 요건을 제시하고 있으며, 2003년까지만 해도 보안 요건을 제시하고 있지 않았다[7]. 이후 U.S NRC에서 R.G 1.152(2006년) "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"을 통하여 원전에서 디지털 안전계통을 설계할 때 생명주기(life cycle)에 따라 사이버보안을 적용하여 설계하여야 한다는 사이버보안 지침을 정의하고 기술하였다[4]. 10 CFR 73.1은 2007년 개정을 통하여 사이버보안 상위요건을 수립하였다[2]. 국내에서도 국외의 사이버보안 규제 활동에 발맞추어 KINS에서 KINS/GT-N27 “원자로시설 계측제어계통의 사이버보안 기술지침”을 제시하였으며, KINS/RG-NO8.22 “원전 계측제어계통의 사이버보안”을 통하여 KINS/GT-N27을 일부 수정하고 사이버보안의 원전 적용을 공고히 하였다[8,9]. U.S NRC는 2009년 10CFR 73.54의 개정을 통하여 10CFR 73.1의 사이버보안 상위요건에 따른 사이버보안 활동에 대한 내용을 반영하여 개정하였다[3].



(그림 1) 원전 관련 규제지침 및 산업표준

이와 같이 원전 계측제어계통의 디지털화에 따른 사이버위협에 대한 취약성을 보완하기 위하여 많은 활동이 조금씩 적용되어 왔으며, 결국 2010년 U.S NRC는 10 CFR 73.54 사이버 요건을 만족하기 위한 지침으로써 새로운 규제지침으로 R.G 5.71을 추가하였다[5]. 이 규제지침은 어떤 시스템을 원전에 적용하기 위해서는 적용되는 사이버보안 계획, 정책을 비롯하여 설계, 구현, 시험, 설치, 운영 등 각 생명주기 단계별로 적용되어야 할 기술적/관리적/행정적 조치 사항을 상세하게 기술하고 있다. 또한 R.G 5.71은 사이버보안 계획서에 대한 템플릿을 부록 A에서 제시하고 있으며, 이를 기반으로 현재 주요 가동원전 및 설계중인 원전이 원전 계측제어계통 설계 시에 사이버보안 정책, 계획, 이행활동 수립 등에 참조 및

활용되고 있다. IEEE 7-4.3.2(2010년)는 위에서 간략히 설명한 10CFR 73.1(2007년), 10CFR 73.54(2009년), R.G 1.152(2006년)의 사이버보안 내용을 반영하여 5.9 “접속제어”절을 통하여 물리적보안 및 사이버보안에 대한 내용 및 생명주기에 따른 보안 요건을 제시하고 있다. R.G 1.152는 2011년 개정을 통하여 원전에 적용되는 디지털 시스템 설계 및 구현시 개발환경에 대한 보안 요건을 추가하였으며, 생명주기에서 설치단계부터 폐기단계까지 적용되는 요건을 삭제하였다. IEEE 7-4.3.2도 R.G 1.152의 요건을 참조한다면 추후 이러한 부분이 개정이 될 것으로 예상된다. (그림 1)은 위에서 언급한 규제지침 및 산업표준의 관계도를 보여준다.

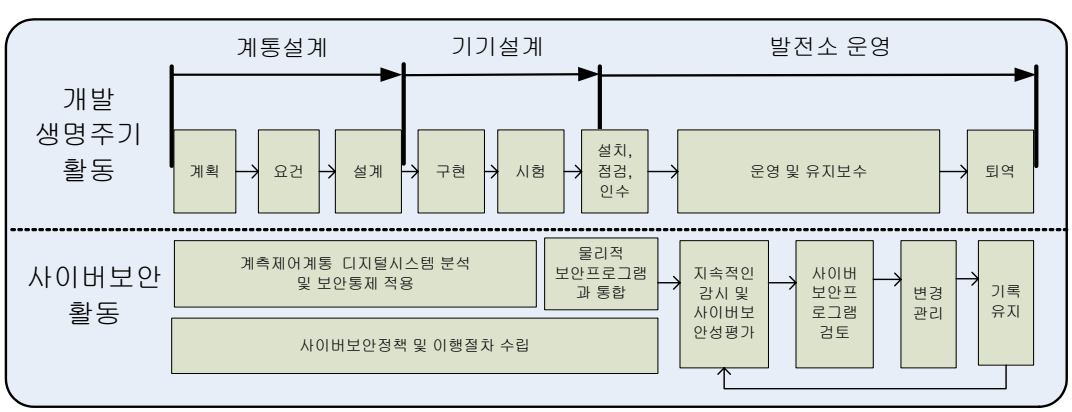
3. 원전 계측제어계통 사이버보안 적용

원전 계측제어계통의 사이버보안 위협으로부터 효과적으로 보호하기 위해서는 (그림 2)와 같이 계측제어계통의 개발단계에서부터 실제 발전소에 설치되어 운영되는 동안에 걸쳐 보안정책수립, 지속적인 보안성 평가, 검토 및 유지관리가 이루어져야 한다. 현재 원전 계측제어계통은 R.G 5.71의 요건에 따라 안전 및 안전에 관련된 기능을 수행하는 시스템 또는 기기를 필수계통으로 분류하며, 필수계통은 사이버위협 또는 공격에 의해 기능수행에 영향을 받지 않게 설계되도록 요구되어지고 있다. 본 절에서는 이러한 사이버보안 요구에 따라 원전 계측제어계통 설계에 적용되는 대상 분류, 방법 및 절차에 대해서 기술한다.

3.1 사이버보안 대상

원전 계측제어계통의 사이버보안 대상은 미국 원자력규제위원회의 R.G 5.71에 근거하여 계측제어 계통의 안전 및 안전에 관련한 기능을 수행하는 시스템 또는 기기를 필수계통으로 분류하고, 필수계통중 디지털 기술을 사용하거나 안전에 영향을 주는 디지털 시스템을 필수 디지털 자산으로 분류한다. 다음과 같은 기능을 수행하는 시스템 및 기기가 필수디지털자산으로 볼 수 있다.

1) 안전 및 정상 출력 운전 기능을 수행하는 기기나 계통
2) 안전 및 정상 출력 운전 기능에 영향을 미치는 기기나 계통
3) 1)항과 2)항의 기능을 지원하는 기기나 계통
4) 1)항, 2)항 및 3)항의 기기나 계통의 보안 기능을 수행하는 기기, 계통 및 통신망



(그림 2) 원전 계측제어계통 사이버보안 활동 예시

3.2 사이버보안성 평가 절차 및 심층방호 설계

원전 계측제어계통의 사이버 위험 평가는 위험식별과 위험평가의 두 단계로 구성한다. 사이버 위험 평가를 위한 초기 자료인 자산 분석은 필수디지털자산 식별과 필수디지털자산에 대한 가치평가인 필수디지털자산 분석 평가 단계로 구성한다. 필수디지털자산 분석 결과는 사이버 위험식별과 위험평가 수행 단계의 입력으로 사용한다. 위험식별 단계는 1) 위험 자산 식별, 2) 사이버 위험 식별, 3) 현재의 보안 통제 식별, 4) 취약점 식별, 5) 영향성 식별로 구성하며, 위험평가 단계는 1) 자산 손상으로 인한 결말(consequence) 평가, 2) 사이버 사고 가능성 평가, 3) 사이버 위험 평가 등으로 구성한다.

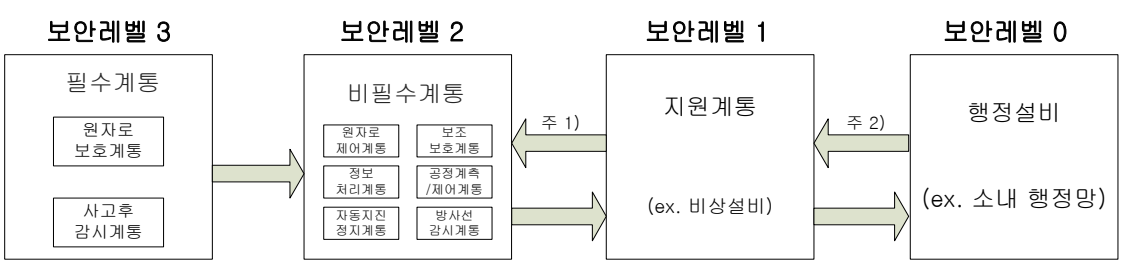
심층방호(Defense-in-Depth) 보호 전략은 사이버공격에 대응하고 사이버공격으로 인한 피해를 완화하고, 복구를 위한 총체적 보호 전략이다. 심층방호 보호 전략의 심층방호 구조는 방벽으로 보호하는 다중의 계층 구조로서 단일 보호 방벽의 훼손 또는 단일 보안 통제의 무력화가 원자력발전소의 안전 및 안전 관련 기능에 손상을 주지 않는다. 원전 계측제어계통의 심층방호 모델의 사용 예시는 (그림 3)과 같다.

3.3 사이버보안 자산 평가 및 보안수준 할당

원전 계측제어계통의 자산평가는 (그림 4)와 같이 영향성 분류기준에 따른 영향성 평가, 보안수준 할당 및 보안수준에 따른 요건 적합성활동으로 구성된다. 원전 계측제어계통은 영향성평가 결과 및 자산식별 결과에 따라 심층방호 모델의 보안수준을 정의하며 각 계층의 보안수준을 정의하여 각 보안수준에 필요한 상위수준의 요건을 마련하고, 이에 따른 계통의 요건적합성을 평가한다. (그림 3)의 심층방호 모델의 사례와 같이, 보안수준은 네 개의 보안수준, 즉 보안수준3, 보안수준2, 보안수준1 및 보안수준1으로 분류하며, 보안수준3이 가장 상위의 보안수준이다.

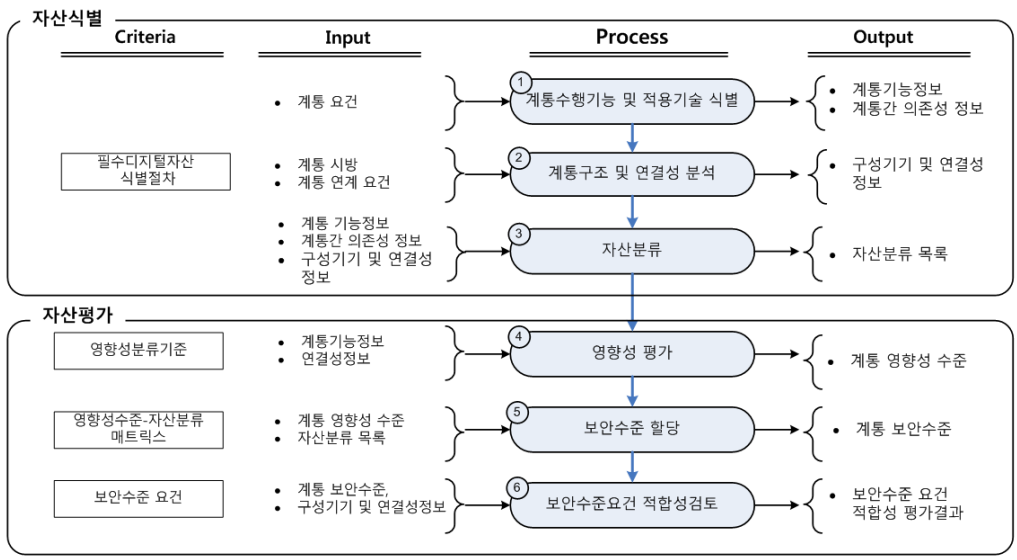
4. 국내 규제기관의 최근 동향

원전에서 사이버보안을 적용하기 위해서는 원전 설비에 대한 규제기관의 상위 사이버보안 규제 지침이 중요하며, 운전운영자, 설계자 및 연구자는 이에 따른 충실한 사이버보안 이행이 중요하다. 국내 원전 규제기관인 KINS는 원전에서 사이버보안 적용을 위하여 2010년부터 원전 계측제어계통 분야에 실질적으로 적용 및 활용 가능한 근거를 개발하기 위하여 원전 운영자, 설계자, 연



주 1) 하위레벨로부터의 데이터는 영향성 평가 및 침입방지시스템 또는 침임탐지시스템을 통하여 허용됨.
주 2) 하위레벨로부터의 데이터는 침입방지시스템 또는 침임탐지시스템을 통하여 허용됨.

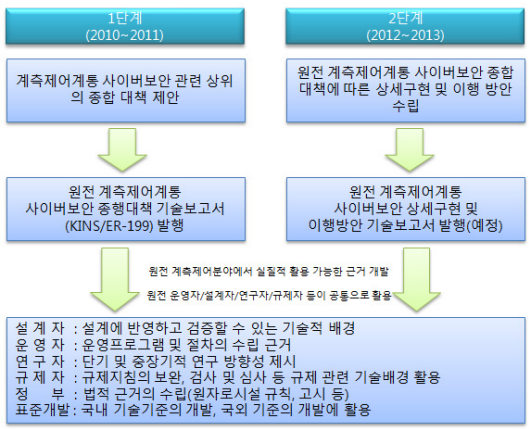
(그림 3) 원전 계측제어계통 심층방호 모델 예시



(그림 4) 원전 계측제어계통 자산 식별 및 자산 평가 절차 예시

규자 등과 워킹그룹(WG-NICCS : Working Group on Nuclear I&C Cyber Security)를 구성하여 연구가 진행되고 있다. 현재 1단계의 주요 활동 및 연구 활동은 KINS/ER-199 보고서로 작성하였다[10]. 이 보고서를 통하여 사이버보안 활동 이행의 필요성 및 사이버보안활동에 대한 조직적인 체계의 필요성에 대해서 언급하였으며, 설계자, 운영자, 및 연구자들을 위하여 원전 계측제어계통에 활용가능한 근거문서를 개발하려고 노력하고 있다. 현재 WG-NICCS는 R.G 5.71을 사이버보안 주요 규제지침으로 정의하고 분석 중에 있다. 최근 2012년 8월에는 WG-NICCS 2단계 3차 회의가 개최되었으며, KINS는 최근의 규제동향에 대해서 발표하였다[11].

KINS는 교과부 고시인 “원자로시설 등의 기술기준에 관한 규칙”에 최근 규제 동향에 따라 사이버침해행위와 사이버보안 대책에 대한 정의를 추가하고 주요 계측제어계통에 대한 사이버보안 대책의 수립 및 이행에 관한 항목을 신설 또는 수정하였다. 또한 원자로 시설의 안전과 물리적 방호의 연계에 대해서 통합적으로 검토되어야 하고, 원자로 시설의 변경이 있을 시 안전과 물리적 방호에 미치는 부정적 영향이 없는지 사전에 평가가 수행되어야 함을 “원자로시설 등의 기술기준에 관한 규칙”에 추가하려고 진행중이다. 이외에 KINS는 신울진 1,2호기 계측제어계통의 사이버보안 이행계획에 대한 적합성 평가, 신고리 3,4호기 운영단계에서의 사이버보안 적합성 평가를 수행를 수행하고 있다. 이외에 가동중 원전에 대해서는 충분한 법적 요건을 마련 후에 진행할 계획이다. WG-NICCS의 2단계 연구활동은 (그림 5)와 같이 “원전 계측제어계통 사이버보안 상세구현 및 이행방안 기술보고서”로 예정되어 있으며, 지속적인 회의를 통하여 설계자, 운영자, 연구자 및 규제자 간에 사이버보안 관련 이행활동 및 동향에 대한 정보를 공유하면서 원전 사이버보안 관련 조직적인 체계를 마련하고, 구체적인 사이버보안 관련 규제지침을 확립하고자 노력 중에 있다.



(그림 5) WG–NICCS 워킹그룹 추진 체계[11]

5. 결 론

원전에서 사이버위협 및 테러 등과 같은 사이버보안 공격으로 인한 원전의 가동정지 또는 원전의 예기치 않은 이상 동작은 전력수급 문제 뿐만 아니라 더 나아가 경제사회 및 자연환경에 막대한 영향을 줄 수 있다. 현재 원전을 포함한 전력망에 대한 공격시도는 지속적으로 증가하고 있으며, 차후 사이버전에서는 이러한 전력망에 대한 공격이 제 1 공격목표가 될 것이라고 한다[12]. 따라서 원전에서 사이버보안 관련 대응 활동이 더 박차를 가하여 원전의 안전성을 시급히 확보하여야 한다. 최근 국내외 원전 관련 규제기관 및 산업표준기관에서 제시하는 규제지침 및 산업표준에 따른 사이버보안 정책, 계획 및 대응방안에 따라 사이버보안 관련 활동이 진행되고 있다. 현재 가동중, 건설중 및 설계중인 원전에서 이러한 사이버보안 관련 지침 및 표준에 따라 사이버보안 취약성을 분석하고 대응방안을 모색하고 있으며, 이에 따른 이행계획을 수립하고 행동을 취하고 있다. 최근 국내에서 설계중인 원전은 개념설계에서부터 구현 및 시험단계까지 사이버보안 취약성을 사전에 분석하고, 취약성을 보완한 후 이를 다시 설계단계에 반영하고 이에 따른 사이버보안 취약성 분석을 재수행하도록 내부적인 설계공정을 요건화하는 등 사이버보안 관련 요건을 충실히 이행하고 있다[13]. 그러나 전술한 바와 같이 원전에서 사이버보안 관련 활동은 이제 시작단계에 있다고 볼 수 있으며, 앞으로 원전 사이버보안 관련 활동에서 아래와 같은 사항이 고려되고 보완하기 위한 연구가 진행된다면 좀 더 안전한 원전을 설계, 건설 및 운영할 수 있을 것이다.

1) 원전의 관련 기기는 보통 설계수명을 30~60년으로 설계하므로, 한 번의 사이버보안 정책, 계획, 이행 계획의 수립보다는 주기적인 정책, 계획, 이행 계획의 변경이 필요하다. 사이버보안 공격루트 및 공격 방법은 디지털 기반의 취약성을 이용하여 다양화되고 있고, 한번 공격 대상이 정해지면, 그 공격대상은 알지 못하는 사이에 공격이 진행되거나 또는 정보를 수집한 후에 수집된 정보를 기반으로 다른 2차, 3차 공격이 이루어질 수 있다. 따라서 모든 원전은 항상 사이버보안 관련 동향에 주의를 기울여야 하며, 주기적인 정책, 계획, 이행 계획 및 이행 활동의 변경 및 갱신을 통하여 사이버 취약성을 감소시키고, 사이버보안 공격에 대비하여야 한다.

2) 향후 원전에서 사이버보안 기술이 더욱 더 주목을 받을 것으로 예상되며, 사이버 위협 및 테러에 대비하기 위한 많은 연구가 진행되어야 한다. 현재 원전 계측제어계통에서 사용되는 기기 및 통신망은 상용의 기기 및 통신망을 원전 요건에 맞도록 검증성, 신뢰성 및 결정론성 등의 요건에 적합하도록 수정하거나 일부 변경하여 사용하고 있는 실정이다. 향후 비공개된 기기 및 비공개된 통신망에 대한 연구가 더 진행되어야 할 것이다. 특히 원전 계측제어제어계통에서 모든 정보

를 전송하는 통신망 측면에서 원전 계측제어계통 전용의 통신망 개발 등을 통하여 사이버 위협 및 테러에 좀 더 적극적으로 대비하는 것도 좋은 대응방안으로 판단된다.

3) 원자력 발전소는 그 상황, 크기 및 용도에 따라 다양한 형태로 존재로 존재한다. 예를 들면, 가동중인 원전, 건설중인 원전, 설계중인 원전, 또는 대형원전, 중소형 원전, 소형원전 또는 발전용 원자로, 연구용 원자로, 다목적 원자로 등 다양하게 존재한다. 이러한 원전 형태에 따라 동일한 사이버보안 정책, 계획, 기술 및 전략을 적용시키는 것은 무리가 있을 것이다. 예를 들어 가동중인 원전에 지침이 새롭게 나올 때마다 그 지침을 적용시키기 위해서 원전 운영을 중단 시킨다면 국내 전력 수급에도 많은 영향을 미칠 수 있다. 따라서 원전의 상황, 크기 및 용도에 따라 사이버보안 정책 및 적용 수준도 달리 하는 단계별 접근 전략(graded approach)이 필요하다.

4) 원자력발전소는 수많은 기기 및 계통으로 구성된다. 현재 원전에 사이버보안을 적용시키기 위해서 원전 기기 및 계통의 전문가와 일반 IT 사이버보안 전문가와의 교류 및 협력을 통해서 사이버보안 활동이 이루어지고 있다. 그러나 원전은 수많은 기기 및 계통으로 이루어져 일반 IT 전문가가 단기간 내에 원전을 모두 이해하고 이에 따른 사이버보안 대응 전략을 수립하기가 쉽지 않다. 따라서 원전 기기 및 계통을 잘 알고 있고 또한 사이버보안 분야에도 전문적인 지식을 보유한 인력 교육이 절실히 필요하며, 이러한 인력들이 각 원전에 적절히 배치 및 원전 계측제어계통 설계에 활용되어야 할 것이다.

5) 현재 원전관련 규제기관 및 산업표준 기관들도 등도 최근 들어서야 사이버보안 관련한 규제지침 및 산업표준을 제시하고 있다. 그러나 사이버보안 관련한 규제지침 및 산업표준에 대한 내용이 앞서 2장에서 살펴본 바와 같이 계속적으로 바뀌고 있는 실정이고, 서로 참조하여 관련 요건을 수정 및 개정하고 있으며, 끊임없이 진화하고 변화하는 새로운 사이버위협 및 보안 요건에 대한 부분은 자세히 기술하고 있지 못한 실정이다. 따라서 추후 명확한 사이버보안 정책, 계획, 이행계획, 기술적, 관리적 및 행정적인 사항에 대해서 좀 더 구체적으로 수정 및 개정이 되어야 하고, 새로운 구체적인 지침이 추가되어야 할 것이다.

참고문헌

[1] 10 CFR 50.55a(h), Code and Standards - Protection and Safety System, U.S. NRC.

[2] 10 CFR 73.1, Physical Protection of Plants and Materials - Purpose and Scope, U.S. NRC.

[3] 10 CFR 73.54, Protection of Digital Computer and Communication Systems and Networks, U.S. NRC.

[4] Regulatory Guide 1.152, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants, U.S. NRC.

[5] Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities, U.S. NRC.

[6] IEEE Std. 603, Standard Criteria for Safety Systems for Nuclear Power Generating Stations.

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

[8] KINS/GT-N27, 원자로시설 계측제어계통의 사이버보안 기술지침, KINS, 2007년.

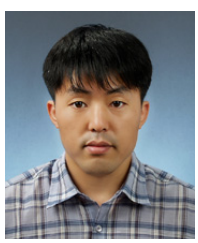
[9] KINS/RG-NO8.22, 원전 계측제어계통의 사이버보안,, KINS, 2009년.

[10] KINS/ER-199, 원전 계측제어계통 사이버보안 종합대책 기술보고서, KINS, 2011년.

[11] 원전계측제어 사이버보안 워킹그룹 활동 및 KINS 사이버보안 동향(2단계 3차회의) 발표자료, WG-NICCS, 2012년.

[12] 서정택, 이철원, 스마트그리드 사이버보안 동향, 한국정보처리학회지, Vol.17, No.2, pp.37-45, 2010년.
[13] 구인수, 김관웅, 박근옥, 원자력발전소의 디지털 계측제어시스템의 사이버보안을 위한 디지털 자산분석 방법, 한국전자통신학회논문지, Vol.6, No.6, pp.839-848, Dec., 2011년.

저 자 약 력



정 광 일
이메일 : hisunny@kaeri.re.kr

- 1997년 전북대학교 전자공학과(학사)
- 1999년 전북대학교 대학원 전자공학과(석사)
- 2003년 전북대학교 대학원 전자공학과(박사)
- 2003년~2004년 한국표준과학연구원
- 2004년~현재 한국원자력연구원 연구로공학부 책임연구원
- 관심분야 : 계측제어계통, 사이버보안, 유무선 통신

이 준 구
이메일 : jklee@kaeri.re.kr

- 1998년 충남대학교 전기공학과(학사)
- 2000년 충남대학교 대학원 전기공학과(석사)
- 2011년 충남대학교 대학원 전기공학과(박사수료)
- 2000년~현재 한국원자력연구원 연구로공학부 선임연구원
- 관심분야 : 계측제어계통, FPGA 설계, 사이버보안

박 근 옥
이메일 : gopark@kaeri.re.kr

- 1986년 경기공업개방대학 컴퓨터공학과(학사)
- 1993년 충남대학교 대학원 전산학과(석사)
- 2006년 공주대학교 대학원 전산학과(박사)
- 1987년~현재 한국원자력연구원 연구로공학부 책임연구원
- 관심분야 : 인간공학, 계측제어시스템, 인간기계인터페이스, 사이버보안, 소프트웨어 V&V