원자력 발전소 디지털 시스템의 보안 요구 사항

김진*, 김장성*, 강영두**, 김광조*

*한국정보통신대학교, 공학부

** 한국원자력안전기술원, 계측제어팀

Security Requirements of Digital Systems in Nuclear Power Plants

Zeen Kim*, Jangseong Kim*, Youngdoo Kang**, Kwangjo Kim*

*Information and Communication University (ICU)

**Korea Institute of Nuclear Safety (KINS)

요 약

원자력 발전소 시스템은 기존의 아날로그 방식에서 점차 디지털화 추세에 있으며, 앞으로 전반에 걸쳐 디지털화가 이루어질 것으로 전망된다. 이는 정보기술의 발전과 더불어, 유지 보수에 대한 경제적 잇점을 동시에 갖추고 있기 때문이다. 이러한 디지털화는 종래에 없었던 새로운 보안 취약점을 발생시키고 있으며, 이를 위한 보안 방식은 IT분야와는 달리 심각하게 고려되지 않은 실정이다.

2001년 9.11 테러 이후 각종 사회 기반 구조에 대한 보안 인식이 강화되면서, 에너지 분야에 있어서도 물리적 공격 뿐 아니라 통신망을 통한 사이버 공격에 대한 부분도 심각하게 고려되고 있다. 이에 최근 미 NRC, IAEA, 국내의 KINS와 같은 원자력 관련 기관들은 원전의 디지털 계측 제어 시스템에 대한 보안의 필요성을 인식하고, 보안 규제 지침 및 보안 가이드라인을 발표했거나, 준비 중에 있다.

본 논문에서는 국가기반구조 중의 하나인 원자력 발전소에서의 침해 사례 및 각국의 동향을 조사하고, 보안 규제 및 보안 가이드라인에서 고려해야만 하는 디지털 시스템에 대한 보안요구사항을 제시한다.

I. 서론

전력시설, 가스 파이프라인, 교통시스템, 정유시설, 상하수도 등 국가주요기반구조에 대한 공격의 결과는 일상생활의 불가능으로부터 국가의 존폐에 이르는 막대한 손실을 가져다 줄 수 있다. 이러한 주요기반구조에 대한 보안은 2001년 9.11 사건 이후 더욱 강력히 요구되었으며, 이를 위한 연구가 국내외에서 다양하게 수행되었다. 이들 연구의 공통된 특징은 세부적인 보안 요소 기술의 안전성 분석과 같은 기술적 보안 기능 뿐 아니라, 보안을 위한 교육은 물론, 피해시의 대처 방법에 이르는 일반적인 보안 생명주기 전반에 걸쳐 진행되었다는 점이다.

본 연구는 이러한 주요기반구조 중 원자력 발전소의 보안 문제에 대해서 논한다. 원자력 발전은 국내 전기 생산의 약 40퍼센트 이상을 차지할 만큼 중요한 시설이다. 현재 정보기술의 발전 및 비용 효율성 측면에서의 잇점때문에 원자력 발전소의 내부 시스템도 아날로그 방식에서 점차 디지털화 되어가는 추세에 있다. 이러한 시점에서 본 연구는 원자력 발전소의 디지털 화에 있어서의 재문제를 살펴보고, 이를 위한 대책은 논의하고자 한다.

본 논문의 구성은 다음과 같다. 먼제 II 장에서는 각종 원전 시스템에서 발생한 사이버 피해 사례와 보안 대책 동향을 살펴본다. III 장에서는 원전 시스템의 사이버 보안 문제를 살펴보고, 이를 대비하기 위한 보안 대책을 고려한다. 마지막으로 IV 장에서 결론과 함께 논문을 마무리한다.

II. 피해 사례와 보안대책 동향

1. David-Besse 원전의 사이버공격

지난 2003년, 미국 오하이오의 데이비드 베스 핵 발전소는 슬래머 웜의 침입으로 인하여 5시간 동안 안전 감시 시스템이 멈춰있었다. 이는 방화벽으로 보호되고 있는 시스템에서 일어난 일이었기 때문에 더욱 충격이 컸다. 이 시스템을 복구하는데 6시간이 소요되었다. 이 문제는 슬래머웜에 감염된 기기를 이용하여 유지·보수를 한 것이 원인이었다. 이를 통해서 폐쇄망으로 구성된 네트워크라 하더라도 유지, 보수, 모니터링을 위해 잠시라도 외부망과 연결 가능하거나, 혹은 외부망에서 사용되던 기기의 삽입은 심각한 보안 위협으로 작용할 수 있게 됨을 확인할 수 있었다. 이 사건은 원자력 발전소 사이버 보안의 필요성을 인지시킨 중요한 사건이었다.

2. Aurora 프로젝트 [1]

올해 3월 미 국토안보부는 아이다호 국가지정 연구실에서 원전에 대한 사이버 공격 실험을 수행하였다. Aurora로 명명된 이 프로젝트에서, 사이버 공격을 통해서 원전의 운행주기를 변경할 수 있었고, 결국 발전기가 멈추게 되는 결과를 확인할 수 있었다. 구체적인 공격 방식은 기밀로 분류되어 알려지지 않았지만, 사이버 보안이 원전에 미치는 영향을 충분히 인식시킬 수 있는 실험이었다. 이 공격은 발전기의 가동을 정지하는 수준의 공격이었지만, 실제 계측 제어 시스템에 접근이 가능해진다면 원자력 발전소의 원자로와 같은 1차 계통의 안전 역시 위험해질 수밖에 없다.

3. IAEA 대응 동향 [2]

IAEA (International Atomic Energy Agency)는 원전 시스템의 디지털화에 따르는 보안문제를 심각하게 고려하여 보안 기술문서를 작성 중에 있다. 이를 위한 기술 모임에는 국내의 전문가를 포함하여 정보보호 분야, 원자력 연구 분야, 전산 분야, 규제 및 법령 분야의 전문 인력으로 구성되어 있으며, 이들은 각자의 분야의 최신 동향 및 원전 시스템으로의 적용에 대한 기술 회의를 다수 개최하였다. 2007년 내에 최종 가이드라인을 작성 예정으로 진행 중이다.

4.KINS 규제 지침 (안) [3]

한국원자력안전기술원은 디지털 계측 제어 시스템에 대한 사이버 보안 문제를 인식하고, 규제 지침을 현재 작성 중에 있다. 이 규제지침은 디지털 계측 제어 시스템에서의 안전과 정상운전의 보장을 위한 것이며, 모든 수명 주기에 걸친 기밀성, 무결성, 가용성의 만족을 목적으로 하고 있다. 최초의 지침에서는 원전의 안전, 비안전 부분의 구분없이 보안 규제를 하려던 것에서 현재의 수정본에서는 안전계통에 대해서만 사이버 보안을 적용하도록 규제 지침의 작성 과정 중에 있다. 또한 규제 입장에서의 사이버 보안에 관한 연구를 수행하여 가능성 수준과 영향성 수준을 기반으로 한 사이버 보안 위험수준을 제시하였다 [4].

본 작업은 2007년 내에 최종 규제 지침을 확정할 것으로 보이며, 과학기술부 고시로 추진할 예정으로 있다.

5.NRC 규제 방안 [5]

US NRC (Nuclear Regulatory Commission) 는 2006년 초 원전 계측 제어 시스템에 대한 사이버 보안 규제 가이드의 제 2차 수정본을 공지했다. 이 문서에서 NRC는 디지털화에 따른 보안 취약점에 대한 대책 사항을 충실히 수행할 것을 명시하고 있으며, 일반적인 보안 가이드로 세부적인 사항은 각 관련 기관에서 보안 생명주기에 따라서 진행해야 함을 언급했다.

III. 원전 시스템 보안 문제와 대책

1.시스템 구성

원전의 시스템을 안전도와 관계하여 구분하면 안전 관련 시스템, 비안전 시스템의 두 가지로 구성할 수 있다. 안전 시스템은 원자로 및 발전설비를 자동으로 초기화할 수 있는 계측 제어 장치 및 그 관련 장치, 비상 발전기 동작을 위한 계측 제어 장치, 발전설비 제어 시스템, 경보 시스템을 포함한 제어실 계측 제어, 접근 제어 시스템 등으로 구성되며, 비안전 시스템은 사무 자동화 과련 및 이메일, 외부 웹페이지 등과 같은 외부 접속 관련 시스템 등을 뜻한다.

이러한 시스템들은 그 특성에 따라서 차별화된 수준별 보안을 고려해야만 한다. 아래의 (그림 1)은 원전의 정보시스템의 구성을 간단히 표현한 것이다.

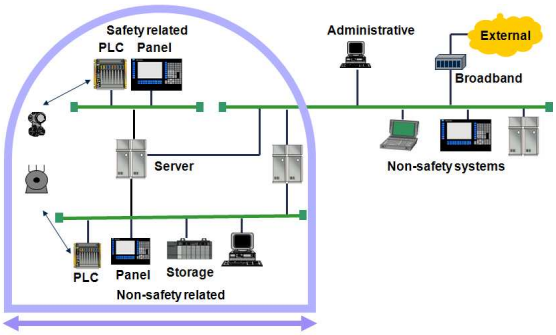

그림 1: 원자력발전소의 구성 시스템

2. 주요 보안 위협 및 보안 요구사항

원전 시스템은 국가 주요 기반 구조의 하나로, 그 내부의 디지털 시스템이 내 외부의 공격에 의해 침해받았을 때, 심각한 피해를 야기시킨다. 예측 가능한 원전 사이버 시스템에서의 주요 보안 위협 다음과 같다.

- 제어 망을 통한 정보의 흐름을 지연, 차단하여 제어 시스템 사업자에 대한 네트워크 가용성을 거부함으로써 제어 시스템 운영을 붕괴시킴
- 제어 시스템 사업자에게 거짓 정보를 발송하여 무단 변경을 은폐하거나 시스템 사업자의 부적절한 조치를 초래함.
- 제어 시스템 소프트웨어를 변경하여 예측할 수 없는 결과를 초래함
- 안전 시스템의 운영을 방해함.
- 프로그래머블 논리 제어장치, 원격 단말 장치, 분산제어시스템 제어장치에 저장된 지시사항을 무단 변경, 예를 들어 경고 임계치 변경, 공정의 조기 셧다운 명령, 혹은 제어 장비를 불능하게 함
- 통신망을 통한 공격 뿐 아니라 물리적 피해에 따르는 시스템의 안전성 침해

이러한 위협 요소에 대한 안전성을 보장하기 위한 보안 요구사항을 정리하면 다음과 같다.

- 기밀성 : 보호되어야 할 정보는 모든 수명주기 동안 오직 인가된 대상에게만 제공 또는 교환되어야만 하고, 비인가된 대상에게 노출되어서는 안됨
- 무결성 : 구성 하드웨어 및 소프트웨어의 정보가 완벽, 정확, 정당함을 보장하고, 인가되지 않은 변경 및 실수나 고의에 따른 변경이 없을을 보장
- 가용성 : 정당한 사용자가 언제든지 원하는 정보를 이용하고 정상적인 기능을 수행할 수 있음
- 인증 및 인가 : 정당한 사용자의 정보시스템의 작동을 위한 정보의 확인 및 해당 사용자의 시스템 접근 가능 수준을 판단함
- 생존성 : 시스템의 공격, 고장 등으로부터 해당 시스템의 기능을 일정 수준이상 유지할 수 있도록 지원함

이러한 보안 요구사항들은 각각의 시스템의 안전 요구 수준에 따라 적절히 보안 강도를 조절하여 적용되어야만 한다. 다만, 그 적용은 전체 발전소 동작의 수명주기에 걸쳐 진행되어야만 한다.

3. 추가 보안 고려 사항

미국은 주요 국가 기반 구조에 대한 보안 로드맵을 분야별로 보고한 바 있으며, 원전과 관련된 부분으로는 미 에너지부에서 2006년 1월 발표한 에너지 분야 제어시스템의 보안 로드맵 [6]이 있다. 이외에도 영국의 국가기반시헌 보호 조정센터에서는 SCADA (Supervisory Control And Data Acquisition, 원방감시제어시스템) 에 대한 각종 가이드라인을 제정 배포하였으며, 일본의 경우도 경제산업성에서 사회 주요 기반 시설에 대한 보안 대책의 연구 중 하나로 발전소의 취약성 및 네트워크 보안 대책, 안전성 검증 프레임워크, 사이버 사고 대응 계획들에 대한 연구를 수행하고 있다.

2절에서 언급한 보안 요구사항과 더불어 원전의 디지털 계측 제어 시스템에 있어서 특별히 추가적으로 요구되는 보안 고려 사항을 정리하면 아래와

같다.

1) 연결성 향상

디지털화 된 계측 및 제어 시스템은 점차 원전의 내부 시스템에 연결되고 일반 운영 플랫폼에 의존하며 인터넷을 통해 접속할 수 있다. 이러한 변화는 운용성을 개선하지만, 계측, 제어 시스템 보안 기능에 대한 개선이 동시에 이루어지지 않았기 때문에 심각한 취약성도 초래할 수 있다.

2) 상호의존성

기반시설 간의 높은 상호의존도는 한 분야의 고장이 타 분야로 확산될 수 있다. 공격자들은 사이버 시스템을 공격하여 이들이 제어하는 실제 시스템에 대한 폭포수 효과를 초래함으로써 광범위한 경제 피해를 유발할 수 있다.

3) 복잡성

실시간 제어에 대한 수요는 시스템의 복잡성을 증대시켰다. 제어 시스템에 대한 접근이 허용되는 사용자의 수가 늘어났고, 내부망과 제어 시스템이 상호 연결되며, 기반시설간의 상호의존도는 증가되었다. 정보기술 시스템 담당자와 계측, 제어 시스템 운영 담당자의 훈련 및 관심사가 현격한 차이를 나타냄으로써 이들 두 핵심 그룹간의 네트워크 보안을 조율하는 것이 필요하다.

4) 레거시 시스템

구형 레거시 시스템은 보다 독립된 형태로 운영될 수 있지만, 암호 정책과 보안 관리가 불충분하고 데이터 보호 메커니즘이 부재하며 정보 링크는 스누핑, 중단, 차단되기 쉽다. 이렇게 불안정한 레거시 계측, 제어 시스템은 서비스 수명이 대단히 길며, 문제가 완화되지 않는다면 수년 동안 계속해서 취약한 상태를 유지할 것이다.

5) 시스템 접근성

인터넷 사용을 제한해도 계측, 제어 시스템은 상호 연결된 전산망에 내재되어 있는 바이러스, 웜, 해킹과 같은 취약점에 전부 노출된다. 뿐만 아니라, 제어 채널은 내부적으로 상용 통신 시설을 통과하는 무선 혹은 임대회선을 사용하기 때문에 데이터나 제어 메시지의 위조에 대한 보호책이 전무한 상태이다. 또한 레거시 시스템은 하청업체 및 정비 업체에 대한 연결을 경유하는 백도어 접속을 허용하는 경우가 많다. 이를 방지하기 위한 기술이 요구된다.

IV. 결론

원전 시스템은 국가 주요 기반 구조의 하나로, 사이버 공격을 통한 발전 정지와 같은 2차계통의 문제 뿐 아니라 원자로와 같은 1차 계통까지 영향을 미칠 수 있으며, 이 경우 국민의 생존까지 위협하게 된다. 정보기술의 발전에 따라 원전의 시스템 역시 점차 디지털화의 추세에 있으며, 이 때문에 발생하는 다수의 공격과 피해가 예측된다. 본 고에서는 국내외의 관련 동향을 조사 분석 하고, 원전의 사이버보안을 위한 구성 시스템의 분류및 수준별 보안 방법과 함께 기존의 보안 시스템의 적용 시 특별히 고려해야할 사항에 대해 정리했다.

본 고의 결과가 향후 원자력발전소의 디지털 시스템 보안기술의 정책 수립 및 실제 현장 적용 시 참고가 될 수 있을 것으로 기대하며, 이를 위한 대책 기술 및 정책 개발을 향후 연구로 남겨둔다.

참고문헌

[1] http://article.joins.com/article/cnn_e/article.asp?total_id=2896348

[2] IAEA Technical Meeting in Idaho on Cyber Security rev 5, 621-12-TM-29279, Oct.17-20, 2006.

[3] 강영두, 디지털 계측제어 계통 사이버 보안에 대한 규제 방향, NSIC 2007 발표자료집, 2007.

[4] Y. Kang, C. H. Jeong, and D. I. Kim, "Regulatory Approach on Digital Security of I&C Systems in Nuclear Power Plants," Transactions of the Korean Nuclear Society Autumn Meeting, 2006.

[5] NRC Regulatory Guide 1.152, Rev. 2 , Jan. 2006.

[6] U.S. Derpartment of Energy, Roadmap to Secure Control Systems in the Energy Sector, Jan. 2006.