국가 기반시설 사이버 보안기술 동향

이철원
[illegible]

최근, 전력 송·변전, 석유 및 가스 파이프라인, 상수도 및 하수처리 등을 감시·제어하는 원방감시제어시스템에 대한 사이버 보안 위협이 점차 증가하고 있다. 미국을 비롯한 여러 나라에서는 원방감시제어시스템 사이버 보안 노력에 많은 노력을 기울이고 있다. 본고에서는 원방감시제어시스템의 보안 위협 및 보안동향을 소개하고 우리나라의 국가 기반시설을 보호하기 위한 향후 추진과제를 제안한다.

주제어: 원방감시제어시스템, 국가 기반시설, 보안 위협, 보안기술

I. 개요

국가 기반시설이라 함은 에너지·통신·교통·금융·의료·수도 등 국가기반체계의 보호를 위하여 계속적으로 관리할 필요가 있다고 인정되는 시설 중 다른 기반시설이나 체계 등에 미치는 연쇄효과, 둘 이상의 중앙행정기관의 공동대응 필요성, 재난이 발생하는 경우 국가안전보장과 경제·사회에 미치는 피해규모 및 범위, 재난의 발생가능성 또는 그 복구의 용이성을 고려하여 지정된 시설을 말한다(행정안전부, 2007).

또한, 2001년 제정된 정보통신기반보호법에서는 "정보통신기반시설이라 함은 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어관리시스템 및 정보통신망을 말한다"라고 규정하고 있다. 동 법에서는 정보통신기반시설중 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을「주요정보통신기반시설」로 지정할 수 있도록 규정하였다. 주요정보통신기반시설로 지정되기 위한 요건으로는 정보통신기반시설을 이용한 업무의 국가사회적 중요성, 정보통신기반시설에 대한 의존도, 다른 정보통신기반시설과의 상호연계성, 침해사고가 발생할 경우 국가안전보장과 경제사회에 미치는 피해규모 및 범위, 침해사고의 발생가능성 또는 그 복구의 용이성 등을 고려하여 지정하고 있다(행정안전부, 2008). 2007년 12월 기준으로 101개 시설이 주요정보통신기반시설로 지정되어 관리되고 있으나, 대부분의 지정시설이 통신 및 금융 분야에 치우치고 있는 형편이다.

그러나 첨단 정보통신기술이 다양한 분야에 접목됨에 따라 지금까지 물리적 보안에만 주력해왔던 분야에 대한 보안 관심사가 높아지고 있다. 전력 생산·분배, 댐 운영, 가스 생산·유통, 수자원 관리 및 대규모 플랜트 시설들을 제어하는 시스템이 첨단 정보통신기술을 활용함에 따라, 점차 개방화·표준화되어 가고 있다. 同 시설 및 석유화학 플랜트, 대규모 산업 플랜트, 공장 자동화설비 제어를 위하여 사용 중인 시스템을 원방감시제어시스템(SCADA, Supervisory Control And Data Acquisition), 분산제어시스템(DCS, Distributed Control System), 공정제어시스템(PCS, Process Control System) 등이라 하며 통칭하여 제어시스템이라 한다. 제어 시스템은 민감함 프로세스 및 물리적 기능을 원격 감시 및 제어하는데 사용되는 컴퓨터 기반 시설, 시스템, 장비를 통칭하는 것으로, 현장 시설에서 센서 측정치와 운영 데이터를 수집·처리하여 로컬 혹은 원격 장비에 제어 명령을 전달하는 시스템을 의미한다. 이러한 제어시스템은 에너지

기반시설 및 대규모 산업 플랜트의 중추신경 역할을 수행하고 있으며, 만약 제어시스템이 외부로부터 사이버 공격을 당한다면 국가안보, 국가경제 및 공중 보건·안전에 중대한 결과를 초래할 수 있다. 이와 같은 제어시스템은 지금까지 전용 통신망 사용, 벤더 독자의 고유 운영체제 사용 등으로 인하여 외부로부터 사이버 침해위협에 안전하다고 여겨져 왔다.

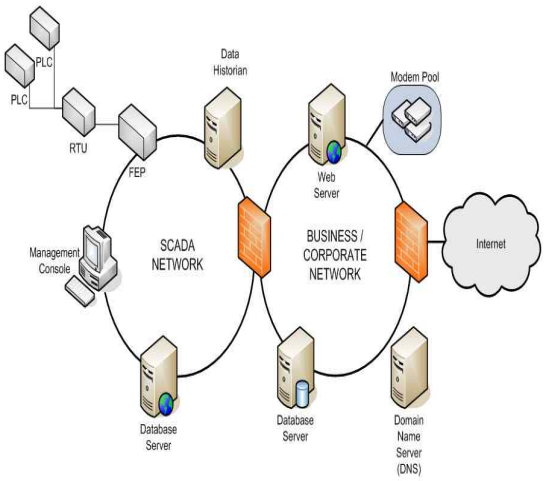
하지만 최근 국외에서 수집된 사이버 침해사례 및 同 시설의 개방화·표준화 추세를 고려해 보면 특정집단의 후원을 받는 잠재적 위협세력에 의한 해킹·사이버테러 등의 사이버 위협에 안전할 수 없다고 판단된다. 미국의 경우, 불순세력에 의한 제어 시스템 침투 및 파괴 가능성이 매우 높다고 인정하여 제어 시스템의 취약점을 식별하고 효과적인 대책을 세우기 위한 민·관 합동의 다양한 노력을 진행하고 있다.

본 고에서는 국가기반시설 중 에너지, 운송, 수자원 및 대규모 산업 플랜트의 운용 핵심 설비인 제어시스템을 외부의 위협으로부터 보호하기 위하여 보안 위협 및 피해사례를 소개하고, 미국의 제어시스템 보안기술개발 로드맵과 최신 보안기술을 소개하여 제어시스템 보안정책 수립에 도움을 주고자 한다.

II. 제어시스템 보안 위협

오늘날 사용되고 있는 대다수 제어 시스템은 보안에 대한 관심이 낮았던 시대에 설계되었다. 이러한 시스템은 비교적 격리된 환경에서 운용되며 주로 독점 소프트웨어와 하드웨어, 통신 기술에 의존하였다. 과거 제어시스템은 가용성(availability) 및 무결성(integrity)을 매우 중요시 하는 시스템으로 정보보호를 위하여 엄격한 보안정책을 적용하였다. 우선 제어시스템에 대한 접근 권한이 없는 사람들로부터 네트워크를 보호하기 위하여 엄격한 격리 정책을 적용하였다. 작업 공간에 대한 물리적 격리는 물론 통신망에 대해서도 전기적 연결을 금지하였다. 외부와 연결되지 않은 독자 네트워크를 유지하면서 Modbus, DNP3와 같은 제어시스템 전용 프로토콜을 사용하였다.

그러나 오늘날에는 에너지 기반구조의 확장, 시장경쟁 체제 도입 등으로 인하여 제어시스템과 경영시스템간 상호 연동 필요성 및 제어시스템간 연계를 위한 상호운용성이 강조되었다. 그 결과, 윈도우나 UNIX와 같은 표준 운영체제의 사용, 인터넷이나 공중 전화망, 유·무선 네트워크와 같은 일반 통신 기술도 널리 사용되고 있다. 다음의 <그림 1>은 오늘날의 전형적인 제어시스템 구성도이다.



<그림 1> 전형적 제어시스템 구성도

현 에너지 제어 시스템의 심각한 보안 문제점을 야기하는 요인은 제어시스템의 상호 연결로 인한 접속점의 증가, 시스템 복잡도 증가, 기반시설간 상호의존도 증가, 아웃소싱 및 외국 제품에 대한 의존성 증가, 시장 구조조정, 범용 운영체제 및 플랫폼의 사용 확대 등을 꼽을 수 있다.

대표적인 제어시스템 취약점 사례는 다음과 같다(이철수, 2006).

- 제어시스템 및 전사적 네트워크의 보안 취약점에 대한 패치 불이행
- 전사적 네트워크와 제어시스템 연동으로 인한 외부 공격통로 제공
- 제어시스템 개발 시 생성된 시험계정의 존치로 인한 공격통로 제공
- 다이얼업 모뎀을 위한 접근 경로 존재
- 무선통신의 사용 증가
- 방화벽의 부적절한 보안정책
- 침입을 탐지하고 사고를 분석할 수 있는 도구의 부재

- 제어시스템에 사용되는 소프트웨어 취약점에 대한 분석 부족
- 제어시스템 내 전송되는 데이터의 평문 전송
- 상용화된 소프트웨어나 표준화된 네트워크 기술 사용
- 제어시스템은 신뢰할 수 있는 사용자가 사용한다고 가정

  * 캐나다 브리티시컬럼비아대학교에 의하면, 불만있는 내부자, 전직 고용원에 의한 사고가 15%를 차지(1998~2001년중)

- 제어시스템은 성능을 고려한 설계로 원격접속, 이중 네트워크 인터페이스, 무선 네트워크 접속, 버퍼오버플로우, 도스 공격 등에 대한 H/W 및 S/W적 취약점 내재
- 언더그라운드 해커회의인 「TOORCON 7」에서 해커가 SCADA를 해킹 대상으로 하고 있음을 발표하는 등 9.11 이후 제어시스템이 해커의 관심대상으로 부상

아래의 <표 1>은 미국의 NSTAC(National Security Telecommunication Advisory Committee)에서 각각 1997년도와 2005년도 제어시스템의 변화에 따른 취약성을 분석한 결과이다(Paul Oman & Matt Phillips, 2007). 1997년과 비교할 때 더 심각해진 사항으로 인터넷 연결 및 무선네트워크 사용, 상용망의 적용 등을 들 수 있다. 이러한 문제는 기존 문제점보다 더 심각한 취약성을 안게 되며, 피해발생시 시스템 전체가 마비될 수 있는 가능성을 상존한다.

<표 1> 1997년 및 2005년 제어시스템 취약점 점검 결과 비교

취약성	1997년	2005년
취약한 패스워드의 사용	○	○
디폴스 패스워드의 미변경	○	○
로그인 계정의 공유	○	○
불충분한 경고 표시	○	○
해킹 위협에 대한 무관심	○	○
보안정책의 부재	○	○
안전하지 않은 모뎀 접근	○	○
침입탐지	○	○
인터넷 연결	×	○
무선 네트워크의 사용	×	○
상용 통신회사 회선 사용	×	○

상기와 같이 제어 시스템이 보안 취약점을 가지게 되면서 제어 시스템에 대한 다음과 같은 공격들이 가능하게 되었다.

- o 제어 네트워크를 통한 정보의 흐름을 방해하여 제어 시스템의 운용을 방해
- o RTU(Remote Terminal Unit)나 PLC(Program Logic Controller) 제어기에 있는 경보 임계값을 불법적으로 변경하거나 제어장비에 대한 불법적인 명령을 실행
- o 제어시스템 운영자에게 그릇된 정보를 전송하여 운영자에 의해 부적절한 행동을 초래
- o 제어시스템 소프트웨어를 수정하여 예측할 수 없는 결과를 초래하게 하는 행동
- o 안전한 시스템 운용을 방해하는 행동

실제로 나타난 제어시스템에 대한 사이버 침해 징후 및 사례는 여러 분야에서 감지되고 있다. 사이버 침해 징후의 대표적 예로, 2002년 아프가니스탄 전쟁 중 알카에다의 기지로 보이는 곳에서 알카에다 조직원의 소유로 보이는 노트북에서 사이버테러에 이용될 수 있는 소프트웨어와 미국 내 댐의 설계도를 발견되었다. 이 밖에도 대표적으로 발생한 사례는 다음과 같다.

- o 2003년 8월 First Energy의 SCADA 시스템 경고 프로세서 고장으로 Northeast Power Blackout
- o 공격자가 백업 컴퓨터의 모뎀을 경유, SRP 소유 컴퓨터에 불법적으로 접근하여 1994년 아리조나주 피닉스의 수력 전기 제공사업자(SRP)에 사이버 침해 사고 발생
- o 2개월 동안 무선 전송기를 이용하여 하수도 처리 제어시스템에 46회 침입하여 특정 하수 처리시설의 데이터를 변경하여 근교 강 및 공원에 처리되지 않은 264,000 갤런의 하수 방출(호주 Maroochy Shire Sewage Spill 사례)
- o 2003년 8월 Sobic 컴퓨터 바이러스가 미국 동부 전역의 기차 신호시스템 마비하여 10대의 Amtrak 기차가 최대 4-6시간 정도 지연
- o 2003년 1월 Davis-Besse 원자력발전소 MS SQL 서버가 슬래머웜에 감염되어 전력감시 프로세스 컴퓨터 마비

o 2005년 12월, Taum Sauk Water Storage 댐이 수십억갤론의 물을 방류하는 치명적 사고 발생

o SCADA시스템이 제어 및 모니터링 기능을 제대로 수행하지 못함으로써 발생한 Bellingham, Washington Gasoline Pipeline 사고로 '99년 6월, 237,000 갤론의 기름이 16개 파이프라인에서 새어나와 화재 발생

o 원자력 발전소의 가동 중단원인이 "공정제어 네트워크의 플랜트내에 과다 트래픽"인 것으로 조사된 Browns Ferry 원자력 발전소 침해사고(NRC 보고서)

* 노후화된 네트워크 기반시설의 설계일 수도 있지만, 위조 트래픽으로 인한 프로토콜 스택 에러로 인한 장애일수도 있다고 지적

o 유럽네트워크정보보안연구소(ENISA, European Network and Information Security Agency)는 2007년 3월에 에스토니아가 사이버 공격을 받아 은행, 온라인 방송 등 네트워크 기반시설에 많은 피해가 발생한 것으로 보고

o 미국 국토안보부는 2007년 3월 4일 사이버 해킹을 통해 발전기에 과부하가 걸리도록 유도하여 발전기의 밸브가 파손되어 전력 발전기가 장애를 발생할 수 있다는 시험 비디오를 공개(idaho 국립 연구소에서 실시)

o 미국 CIA는 2008년 1월에 미국외 지역에서 인터넷을 통한 침입으로, 정전사태 등 피해가 발생하는 등 국가주요기반시설에 대하여 사이버 공격이 발생한 증거를 가지고 있다고 발표

상기와 같은 제어시스템에 대한 보안 위협을 방지하기 위해서는 다양한 보안대책이 강구되어야함에도 불구하고 현존하는 보안대책은 제어시스템보다는 일반 IT에 적합한 보안대책에 초점이 맞추어져 있다. 일반적으로 제어시스템용 보안대책을 강구하기에 앞서 제어시스템과 일반 IT 시스템의 차이점을 파악하고(<표 2> 참조), 이에 대한 대응 방법의 차이도 분명하게 인식하는 것이 필요하다. 일반적인 대응방법의 차이는 다음과 같다.

<표 2> 정보시스템과 제어시스템간의 차이

내용	정보시스템	제어시스템
신뢰성	업무시간에 한정 사소한 장애 허용 필드상에서 사전 시험	24*7*365 운영 장애 허용 불가 필드적용전 QoS 점검
위험 영향 요소	기밀성, 무결성, 가용성	인명, 생산물, 장비
위험 관리	기능 장애시 재부팅 실시	재난 분석 핑료 장애에 강한 설계
정보	지연은 수용	지연에 민감

o 위험관리 목표의 차이: 생활의 손실이나 공공의 건강에 대한 위험을 방지

o 구조적 보안 초점의 차이: RTU(Remote Ter- minal Unit)나 PLC(Program Logic Controller) 제어기가 중앙 서버보다 더 중요

o 가용성 요구의 차이: 제어처리는 연속성이 요구

o 의도하지 않은 결과: 제어 시스템에 통합된 모든 보안기능은 취약점이 없어야 함

o 대응 시간의 중요성: 일반적인 정보시스템과는 달리 시스템과 사람간의 대응 시간이 매우 중요

o 반응 시간 요구의 차이: 제어시스템은 정보전달에 지연이 허용되지 않기 때문에 반응시간이 중요

o 자원 제한: 제어시스템과 그들의 실시간 운영체제는 대표적인 IT 보안기술을 포함할 수 있는 충분한 컴퓨팅 자원이 부재

o 정보 무결성: 제어시스템에서 입력되는 정보는 매우 중요하므로 제어시스템 운영을 위해 고의적인 악성정보를 제거하기 위한 예측은 매우 중요

o 통신: 제어시스템 환경에서 사용되는 통신 프로토콜과 매체는 일반적인 환경과 상이

o 소프트웨어의 갱신: 시기적절한 보안패치의 어려움

불행한 것은 제품 및 기술 아웃소싱 증가 및 상용제품에 대한 의존성 증가, 경영망과 제어망의 상호연결의 지속적인 증가, 실시간 기업 정보에 대한 수요 증가, 차세대 전기 그리드 개발, 정보 기술 및 통신 기능의 컨버전스 증가, 인터넷 프로토콜(IP) 기반 통신 이용 증대, 무선 통신 의존도 증가 및 첨단 사이버 공격 성능 향상 및 공격 도구의 정교화 등으로 인하여 향후에도 제어시스템을 위협하는 침해사례는 끊임없이 증가할 것으로 예측된다.

III. 제어시스템 보안 기술 동향

국가기반시설 특히 제어시스템에 대한 보안이 향후 국가안보의 초석임을 인지한 미국은 에너지부(DOE)와 국토안보부(DHS)를 중심으로 제어시스템 보호에 많은 노력을 기울이고 있다. 백악관은 2003년 초 발표한 「사이버스페이스 보안을 위한 국가 전략」에서 DHS와 DOE가 업계와 제휴하여 "... DCS/SCADA 보안을 강화하기 위한 최우수 실무 및 신기술을 개발하고, 보호대상 DCS/SCADA 관련 시설을 결정하며, 同 시설의 단기 사이버 보안 개선을 위한 우선 계획을 수립" 하도록 요구하였다. 또한 HSPD-7(대통령명령 7호) 에서는 DHS와 공동으로 에너지 분야의 취약성 평가 촉진, 사이버 공격 예방 및 완화를 위한 위험 관리 전략 수립 등을 요구하였다(Bush, 2003). 지금까지 진행된 미국의 주요 노력을 살펴보면 다음의 <표 3>과 같다.

<표 3> 미국의 제어시스템 보안 활동 현황

활동	선도 조직	범위	주요 활동 및 행사
공정제어 시스템 포럼(PCSF)	국토안보부(DHS)	안전한 제어 시스템의 국제 설계, 개발, 배치	• PCSF 창립회의 • 초대 국제 표준 조정 회의
공정 제어 보안 요구사항 포럼(PCSRF)	국립표준기술원(NIST)	산업 공정 제어 시스템 보안 요구사항	• 산업 제어 시스템을 위한 시스템 보호 프로파일 1.0버전 공개
정보 기반시설 보호 연구소(I3P)	Dartmouth College, 국토안보부, NIST	국가 사이버 보안 R&D 조정 프로그램	• I3P SCADA 보안 연구 프로젝트 • 석유 및 가스 기반시설 제어 시스템 보안
국제 전력 인프라 보증 (IEIA) 포럼	호주/캐나다/뉴질랜드/영국/미국 이해관계자 및 정부 기관의 협력	전력 기반시설 보호 계획	• 주요 기반시설 보호에 대한 미국-호주 쌍무 토의 • 북미 이해관계자 회의
국립 SCADA 테스트 베드	에너지부(DOE), 아이다호(INL) 및 Sandia 국립 연구소(SNL)	SCADA 기반시설 시험, 취약성 평가, 표준 개발	• NSTB 가동(2004년) • ICCP 보안을 위한 검토 및 시험 기구 • SCADA 레퍼런스 모델 개발(1단계) • SCADA/EMS 제품에 대한 사이버 취약성 평가
제어 시스템 보안 센터	국토안보부(DHS), INL, US-CERT	제어 시스템 사이버보안을 위한 시험 및 정보 센터	• 전력 분야 사이버 보안 표준 및 지침 비교 • 설치된 제어 시스템에 대한 사이버 취약성 평가 • 위험 분석도구 개발
미국가스협회(AGA) 12 지침	AGA, 가스기술연구소(GTI), NIST	SCADA 통신을 위한 암호화 지침	• AGA 12, 파트 1 및 2 업무 지침 공개 • AGA 12, 파트 3 및 4 개발중
ISA-SP99	ISA-SP99 위원회	안전한 제어 시스템 조달 및 이행 기준 제공	• ANSI/ISA-TR99.00.01-2004, 제조 및 제어 시스템 보안 기술(2004) 등

본 장에서는 미국의 제어시스템 보안을 위한 대표적 활동인 제어시스템 보안로드맵 및 기타 보안기술을 소개한다.

1. 제어시스템 보안 로드맵

미 정부의 제어시스템 보안 로드맵은 "10년 이내에, 핵심 기능의 손실 없이 의도적인 사이버 공격에서 생존할 수 있는 핵심 애플리케이션을 가진 제어 시스템을 설계, 설치, 운영 및 유지한다."라는 비전하에 작성되었다. 同 로드맵은 현재의 제어시스템 보안 문제뿐 아니라 새로운 사이버 위협에 대한 보안대책도 고려하였다. 즉, 제어시스템에 대한 기존의 위협과 새롭게 대두되고 있는 위협에 대처하기 위하여, 다음과 같은 전략적 프레임워크 및 목표를 골격으로 로드맵이 작성되었다(DOE & DHS, 2006).

- 보안실태의 측정 및 평가: 10년 이내에 에너지 자산 소유자들이 제어 시스템의 완전 자동화된 보안 상태 감시 완비
- 보호 대책의 개발 및 통합: 레거시 시스템을 위한 보안 솔루션 개발 및 10년 이내에 빌트인, 단대단(end-to-end) 보안을 제공하는 차세대 제어 시스템

으로 구형 레거시 시스템을 대체
- 침입 탐지 및 대응: 10년 이내에 제어 시스템 침입 시도에 대한 대응조치 및 개선 조치를 자동으로 수행하는 제어 시스템 네트워크를 운영
- 지속적 보안기능 개선: 향후 10년 동안, 에너지기반시설 소유자는 정부 및 제어시스템 이해관계자와 협력하여 보안 강화를 촉진

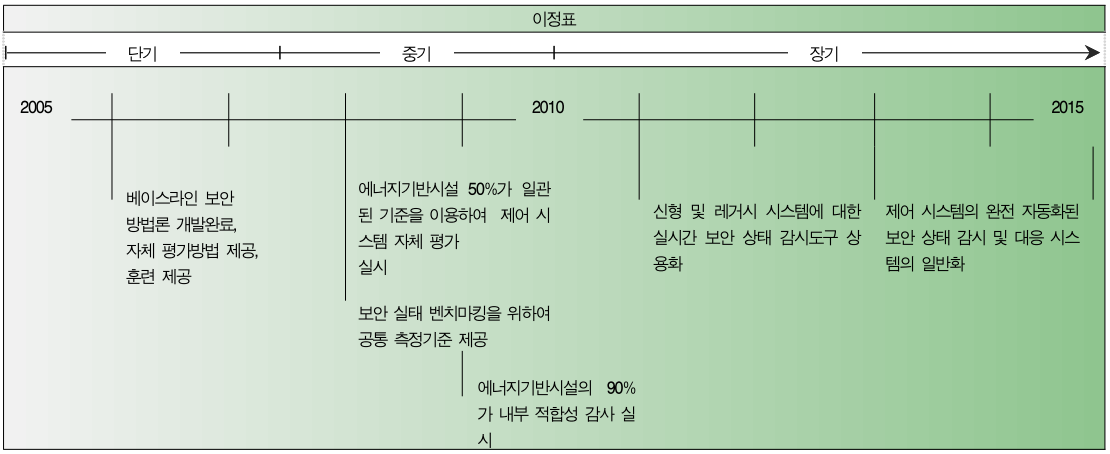
상기에서 제시한 목표 달성을 위하여 제어시스템 보안 로드맵은 반드시 극복해야 할 분명한 과제를 제시하고 있으며, 시간별 이정표에 따른 예상 성과물 및 이를 달성하기 위한 우선적으로 시행하여야 할 일련의 솔루션을 식별하고 있다.

1) 제어시스템 보안실태 측정 및 평가

에너지 기반시설 소유자는 제어 시스템, 제어시스템 컴포넌트 및 컴포넌트간 연계에 대한 보안 실태를 이해함으로써 적절한 시정 조치를 결정할 수 있다. 이를 위하여 정적이며 실시간적 보안 상태를 측정 및 평가할 수 있는 도구와 기술, 방법론뿐만 아니라 믿을 수 있고 널리 사용되는 보안 측정기준이 필요하다. 보안 실태 측정 및 평가를 위한 도전 과제와 로드맵을 <표 4>에 제시하였다.

<표 4> 제어시스템 보안실태 측정 및 평가 로드맵

목표 : 보안 실태 측정 및 평가	
도전과제	• 기술진과 경영진이 널리 이해하거나 수용하지 않는 위험 요인 • 위험 분석 성능을 제한하는 불충분한 보안 측정기준 • 명확한 측정 스펙이 부족한 기존 표준 • 보안 상태 측정 및 평가를 위한 일관된 측정기준의 부재 • 위험 측정을 위한 도구 및 기술 부족 • 사이버 취약성 평가를 위한 표준 부재 • 위협의 입증 및 정량화의 어려움 • 자산 소유자의 지적재산권 보호의 어려움



제어시스템 보안실태 측정 및 평가 로드맵 달성을 지원하기 위한 다양한 과제 중 우선적으로 해결하여야 하는 과제로,(<표 5> 참조) 취약성 평가, 보호 대책의 우선순위를 설정할 수 있는 위험 평가 도구의 개발을 단기적으로 요구하고 있다. 중기적으로 제어 시스템의 보안실태를 측정하기 위한 명확하고 일관된 측정기준을 요구하며, 제어시스템 보안에 필수적인 베이스라인 보안 요구사항을 확립하도록 요구하고 있다. 장기적으로 보안 상태 감시 및 개선을 완전 자동화 시스템을 개발을 촉구하고 있다.

<표 5> 보안상태 측정 및 평가 로드맵 달성을 위한 우선식별 과제

선별된 우선순위	
전략적 위험 규명	• 위협 및 공격 정보에 대한 정보공유 환경 조성
레거시 시스템	• 위협, 취약성, 결과를 비교하는 위험 매트릭스 작성 • 위험 분석 및 타당한 조치 결정
보안도구 및 실무	• 자체 평가 실시 도구 개발을 위한 기금 조달 노력 • 사이버 공격 및 대응 시뮬레이터 설치 및 평가 • 보안 실태를 위한 명확하고 간결한 측정에 대한 컨센선스 개발 • 취약성 평가 방법론, 보안 대책 우선순위 설정을 위한 프레임워크, 소요 비용 정당화 방법을 포함하는 위험 평가도구 개발
제어 시스템 구조	• 기초, 중간, 고급 보안상태 유지를 위해 시스템 수명 사이클 전반에 걸친 규정된 베이스라인 보안 요구사항 개발 • 자동 보안 상태 및 대응 지원 시스템 개발

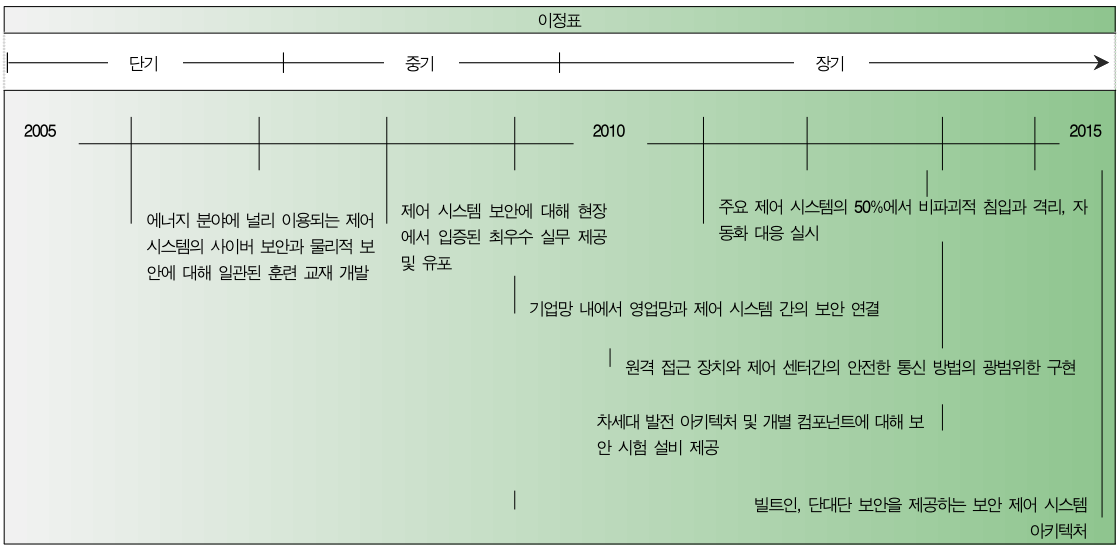
2) 보호대책 개발 및 통합

보안 문제가 식별되면, 알려진 보호 대책을 적용하고 새로운 수요에 따른 보안 솔루션을 개발할 수 있다. 레거시 시스템의 경우 보호대책은 알려진 보안 취약점을 해결하기 위한 패치, 조직 내 전 직원을 대상으로 교육 및 훈련, 시스템 성능을 저하시키지 않는 범위 내에서 보안 기술의 개선 등이 있다. 하지만 가장 효과적인 것은 보안성을 가진 플러그인플레이, 차세대 제어시스템 구조 설계 등을 통해 빌트인, 단대단 보안의 종심방어를 수행하는 것이다.

<표 6> 보호대책 개발 및 통합 로드맵

목표 : 보호 대책의 개발 및 통합

도전 과제	• 위험 증가로 이어지는 개방적이고 유연한 제어 • 제어 시스템의 취약성을 크게 증가시킬 수 있는 SCADA와 기업망간의 연결 • 레거시 시스템의 보안 업그레이드는 과 비용 및 시스템 성능 저하 초래 • 판매업체가 아닌 제3자 제공 하드웨어 및 소프트웨어의 알려진 기술 취약점 • 신기술을 위한 표준화 시험 계획 및 업그레이드는 널리 이용되지 않음 • 노드 수의 증가에 따라 복잡성도 기하급수적으로 증가 • 업체가 참조하는 구체적 요구사항이나 표준이 없음



선별된 우선순위

레거시 시스템

- 침입을 방지하고 비용 효과적인 견고한 SCADA 암호화 솔루션 개발
- SCADA와 영업망 연결을 위한 최우수 실무 식별
- 보안 솔루션 적용이 가능하도록 레거시 통신 성능 개선

보안도구 및 실무

- 변전소와 통제 센터의 물리적 보안 및 사이버 보안을 위한 최우수 실무 규명
- 운영 시스템의 24/7 가동에 영향을 주지 않는 패치 기술 개발
- 제어 시스템 환경에 적합한 견고한 운영 시스템 개발
- 사이버 보안과 물리적 보안을 위한 장비, 구조 및 프로세스를 시험할 수 있는 국가 SCADA 테스트 베드 유지

제어 시스템 구조

- 시험 아키텍처를 포함한 보안 시험 설비 및 지침 개발
- 보안기능이 갖춰진 플러그 앤 플레이 컴포넌트 개발
- 호스트에 대한 영향을 최소화하는 방화벽, 침입 탐지, 바이러스 방지 솔루션을 포함하는 비용효과적인 게이트웨이 보안 솔루션 개발

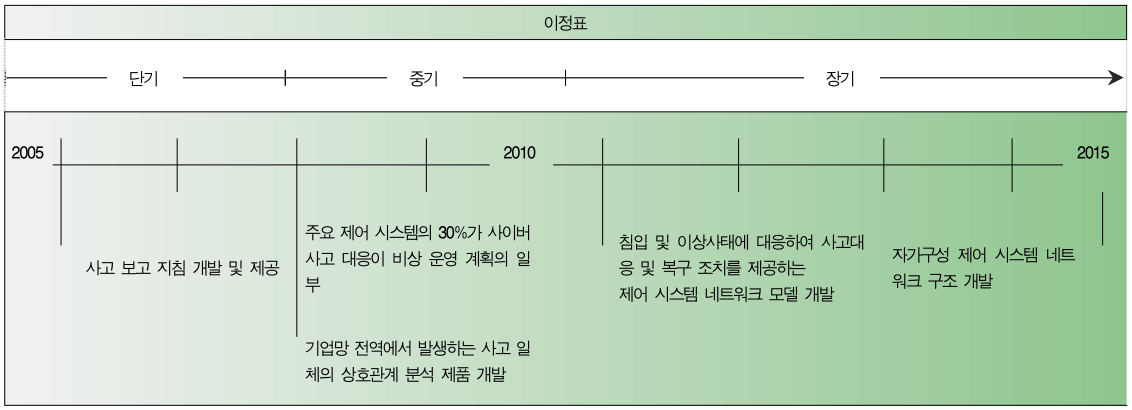
3) 침입 탐지 및 대응

제어시스템에 대한 사이버 공격 도구가 점차 정교화 됨에 따라 제어시스템은 모든 상황에서 완벽한 보안성을 제공할 수 없다. 그러나 제어시스템은 침입을 탐지하고, 이상 작동을 분석하며, 시스템 무결성을 감시하고, 보안 사건을 관리하며, 감사 추적을 포함하는 자동화된 침해 사고 보고 프로세스를 가지고 있어야 한다. 장기적으로 침입에 대응하여 사고 대응 및 복구 조치를 자동화 할 수 있는 네트워크를 구성하는 것이 바람직하며, 이를 위한 로드맵이 다음의 표에 제시되어 있다.

<표 7> 침입탐지 및 대응을 위한 로드맵

목표 : 침입 탐지 및 대응 전략 이행

도전 과제	• 시험과 검증을 거친 보안도구의 부족 • 비상사태 시 신속하게 대응할 수 있는 능력에 영향을 주는 보안 대책 • 정교한 해킹 도구와 자원의 증가



선별된 우선순위

전략적 위험 규명

- 업계의 승인을 거친 사고보고 지침 및 최우수 실무 식별
- 에너지 업계가 정보 공유와 사고 보고를 촉진시킬 수 있는 비밀정보 사용 허가

보안도구 및 실무

- 사고 대응 절차 및 도구 개발 및 훈련 제공
- 보다 견고한 애플리케이션을 위해 네트워크와 호스트에 적응하는 침입방지시스템 개발
- 보안사건 관리도구 개발
- 사고보고 및 연관성 분석을 위한 시각화 도구를 포함한 자동화 보안 정보 수집 도구 개발

제어 시스템 구조

- 자동 보고 기능이 있는 감사추적시스템과 제어 시스템 침입 탐지 시스템/침입방지 시스템 개발
- 이상 활동을 탐지 및 보고할 수 있는 메커니즘을 갖춘 센서 및 센서 시스템 개발 및 배치
- 자동화 보안 상태 및 대응 지원 시스템 개발

4) 지속적 보안개선 활동 유지

제어시스템 보안 필요성이 강력하게 제기됨에 따라 에너지 업계와 정부 공히 제어 시스템 보안을 개선하기 위한 방법을 고민하고 있다. 그러나 同 분야의 보안이 전통적인 IT 보안과 상이하므로, 제어시스템 보안을 개선하기 위한 지속적인 자원의 투입, 공정한 인센티브, 관련 당사자간의 긴밀한 협력 등이 요구된다. 또한, 정부와 에너지 업계는 각자의 역할 및 책임을 정하여 제어시스템 개선을 위한 노력을 수행해 나가야 한다. 미국 정부는 지속적으로 제어시스템 보안을 개선하기 위해 해결하여야 하는 도전 과제를 다음과 같이 선정하였다.

- 기업 내에서 보안 필요성을 해결하기 위해 제공되는 자원의 제한
- 전문지식의 부재, 고비용, 기업의 타성으로 인하여 기술 변화가 억제
- 제어 시스템 보안 위험에 대한 제한된 지식 및 이해
- 정부와 업계 단체 간에 위협 및 사고 정보 공유 부족
- 정부와 업계 간에 효과적인 보안 중심 파트너십 확립의 어려움
- 정부 기관간의 조율 부재로 혼동과 비효율을 초래

상기 도전 과제를 해결하기 위한 중요과제로는 다음과 같은 것이 있다.

- 안전한 데이터 교환 및 통신을 위한 표준 및/혹은 규제조치 개발
- 업계의 주요 기반시설 정보의 보호를 보장하여 정보 공유를 촉진
- 에너지기반시설 소유자와 운영자와 공동으로 사이버 보안 위협 및 현안을 논의할 수 있는 단일 연방기관 식별
- 기업 사례 강화에 도움이 되는 보안대책 이행의 인센티브 및 이익에 대한 분석
- 제어 시스템 보안 분야 투자에 대한 적절한 인센티브 조성
- 제어 시스템 보안 컨소시엄 결성

이상으로 제어시스템 보안을 위한 전략적 프레임워크와 이에 따른 로드맵을 살펴보았다. 10년 이내에 핵심 어플리케이션에 대한 제어시스템 안전성을 확보하는 것은 매우 어려운 과제이지만, 비전을 달성하기 위하여 업계, 정부, 기타 관련 기관과의 협력이 무엇보다도 중요하다.

2. 주요 제어시스템 보안기술

제어시스템 보안을 위하여 국립연구소이외에도 학계 및 산업체에서도 활발히 연구에 참여하고 있다. 본 절에서는 대표적 보안기술을 연구분야를 소개한다.

1) 통합보안서비스와 포렌직

통합 보안서비스는 안전한 제어 네트워크 구축, 모니터링, 인증 등으로 구분되며, 포렌직은 침해사고 대응 및 사고 흔적 수집 및 분석에 대한 기술이다. 을 들 수 있다. 통합 보안서비스 기술을 개발하기 위하여 현재 국외에서 연구되고 있는 분야는 메시지 모니터링, 프로토콜 기반의 보안 솔루션 개발, 보안 터널링 연구 등이 있다. 장기적으로 관점에서 미들웨어 개발 및 키 관리 연구가 포함될 수 있다.

제어시스템의 트래픽은 매우 단순하며 예측이 가능한 데이터 구조이다. 특히 제어신호의 경우에는 크기가 작으므로 암호화의 효과도 적다. 따라서 사고 발생시 포렌직을 통한 사고 사례를 분석하고 재발 방지 노력을 경주해야 하므로 포렌직 기술개발은 매우 중요하다. 현재 연구되고 있는 포렌직의 구조는 제어시스템의 주요 제어기기 및 네트워크 단에 에이전트를 설치하고 각종 정보를 데이터 웨어하우스에 저장을 하고 사고 발생시 포렌직과 관련된 최적화된 정보를 제공하기 위한 구조연구가 진행중이다.

2) 제어시스템의 취약점 및 보안 연구

제어시스템 보안 취약점 연구는 제어시스템이 주오 사용하는 TCP/IP 상의 Modbus 프로토콜의 취약점 및 DNP3 프로토콜 취약점 및 보안 연구가 주류를 이루어 진행되고 있다.

제어시스템에서 가장 많이 사용되고 있는 프로토콜이 Modbus로 이 프로토콜의 특징은 기존 IP 프로토콜과 달리 마스터/슬래이브 방식을 사용하고 있으며, 마스터에서 패킷을 슬래이브에게 전송하면, 슬래이브는 응답을 하는 방식을 사용한다. modbus의 헤더 4바이트의 정보를 이용하여 TCP/IP 헤더를 만들어 일반 TCP/IP 네트

워크를 이용할 수 있다. 제어시스템 내 링크 계층 프로토콜로 TCP/IP를 사용하게 되면서 시스템 설계가 효율적이면서 유연성이 뛰어나게 되나 제어기기 내에 TCP/IP 스택을 올려야 하므로 복잡성과 자원 할당 문제를 고려해야하는 관계로 프로그램 구조가 복잡해진다(Edmonds, Papa & Shenoi, 2007). 특히, 보안 문제를 고려해야 한다. 일반적으로, Modbus 프로토콜을 이용하는 장비는 데이터에 대한 이상 유무를 확인하기 2바이트의 에러 확인 바이트를 사용한다. 최근 이 2바이트의 에러 확인 바이트는 해쉬 함수를 이용하여 무결성을 보장하기 위한 디지털 서명 정보로 이용하는 연구가 진행되고 있다.

데이터의 무결성 만으로는 TCP/IP 프로토콜 자체의 취약성을 이용한 해킹으로부터 제어시스템을 보호할 수 없다. 해커가 TCP/IP 프로토콜의 취약성을 이용하여 마스터(서버)를 공격하여 접근 권한을 획득한 후, Modbus 메시지에 대한 해쉬 처리 과정을 방해하는 경우 메시지의 변조가 가능하게 된다. 결국 메시지의 변조는 제어시스템을 통제할 수 있게 되는 것이며 제어시스템의 기능을 마비시키거나 가동을 중지시킬 수 있게 된다. 이와 관련한 취약점분석도구가 개발되고 있는 데, Modbus 프로토콜을 사용하고 있는 시스템에 테스트 사례 발생기를 통해 제어기기의 오동작 가능성을 분석한다(Dutertre, 2007). 테스트사례발생기에 의하여 발생되는 각종 테스트 결과를 분석하여 제어기기가 오동작 및 해킹으로 인한 장애 발생을 최소화 할 수 있도록 한다. 또한 위협을 상태 머신(State Machine)으로 나타내는 경우, 여러 가지 위협 경로 및 제어 장치의 상태들을 파악하는 데 도움이 된다. 상태 다이아그램(State Diagram)을 이용하여 자동화도구를 개발할 수 있다.

DNP3(Distributed Network Protocol)는 제어시스템에 적합하게 만들어진 표준 Communication Protocol이다. 이는 RTU, IED(Intelligent Electronic Device), 매스터와 슬래이브간의 정보처리 프로토콜이다. DNP 3 프로토콜에 대한 해킹 공격을 방지하기 위하여 송신자의 신원확인 및 메시지의 무결성에 대한 연구가 진행 중이다.

3) 제어시스템 접근통제 연구

제어시스템에서 사용하는 방화벽은 권한을 가지지 않은 자가 권한이 부여되지 않는 자료에 불법적으로 접근을 시도할 때 이를 차단하기 위하여 접근 통제기법을 사용한다. 일반적인 접근 통제기법은 제어시스템과 같이 복잡하고 단순한 제어신호에 대하여 적합하게 규칙을 설정하기 매우 어렵다. 현재 주목할 만한 연구는 접근통제 규칙을 도식화하여 분석할 수 있도록 구성함으로써 접근과 관련된 우회, 통과, 오설정에 따른 허용 등을 분석할 수 있도록 하는 것이다(Cunningham, 2007). 현재 EMERALD IDS는 제어시스템 보안 전문회사인 DigitalBond사의 제어시스템용 접근제어 규칙을 사용하면서 각종 제어프로토콜에 대하여 감시를 수행할 수 있도록 개발되어 있다.

이밖에도 제어기기에 사용되는 플랫폼에 안전성을 보장하는 별도의 플랫폼을 탑재하여 제어기기간의 상호 운영시 안전성을 보장하는 연구, 프로그램 취약성을 해결하기 위한 방안으로 소스코드에 대한 분석을 수행하고 문제점을 검출해 줄 수 있는 자동화된 기법에 대한 연구가 진행되고 있다.

Ⅳ. 결론

미국, 일본, 영국 등 세계 각국은 자국 기반시설의 중추신경계를 구성하는 제어시스템에 대한 사이버 위협을 방지하기 위한 많은 노력을 기울이고 있다. 특히, 미국은 미국 에너지부 산하 샌디아 연구소에 SSDL(SCADA Security Development Lab.)을 설립하고 신뢰성이 보장되는 SCADA 시스템을 위한 다양한 연구를 진행 중이다. 또한, 자체 Red Team을 구성하여 SCADA 시스템의 취약성을 분석하고 있으며, 보안기능이 가미된 차세대 제어시스템 연구에도 많은 투자를 하고 있는 실정이다. 미국 상무부 산하 국립표준기술원(NIST)에서도 「Homeland and Industrial Control Security」 그룹을 중심으로 제어시스템 보안에 대한 연구를 진행하고 있으며 관련업체, 연구기관 등으로 구성된 PCSRF(Process Control Security Requirement Forum)을 이끌어가며 ISA(Instrumentation Systems and Automation Society)와 협력하여 관련 표준화 연구를 진행 중이다.

선진 외국의 상기와 같은 움직임은 우리에게 시사해주는 바가 매우 크다 하겠다. 즉, 우리나라도 제어시스템의 안전성 강화를 위한 보안 기술을 연구하고 개발하여

향후 아니 지금 일어나고 있을지도 모르는 제어시스템에 대한 사이버 위협 제거 노력을 하여야 한다. 제어시스템 전용 암호 알고리즘 개발하고, PLC(Programmable Logic Controller) 전용 침입차단시스템을 개발하며, 제어시스템용 사용자 인증, 암호 통신 프로토콜 개발, 제어시스템 전용 위험분석 도구 등을 연구해 나가야 한다. 병행하여 제어시스템의 핵심 설비인 PLC의 취약성을 분석할 수 있는 시험 suite 개발하고, 제어 시스템용 사이버 위협 관제기술을 개발에 투자하여야 할 시기이다.

정부에서는 국가정보원, 지식경제부, 국토해양부 등이 중심이 되어 범 국가적인 제어시스템 안전성 강화 프로그램을 마련하여 추진하여야 한다. 또한 정부부처, 한국전력, 전력거래소 등 유관기관, 대규모 산업 플랜트를 운영하는 민간기업, 관련 연구기관 등이 참여하는 협의체를 설립하여 제어시스템 보안 관련 정보를 공유하고, 사이버 위협에 공동 대처할 수 있는 기반을 마련하는 것이 필요하다고 판단된다.

제어시스템에 대한 사이버 보안, 이제는 시작하여야 할 때이다.

<참고문헌>

▷ 이철수. 2006. 정보망과 제어망간의 연동 취약점에 관한 연구.

▷ 행정안전부. 2007. 재난및안전관리기본법.

▷ 행정안전부. 2008. 정보통신기반보호법.

▷ Bush, President George W. 2003. *Homeland Security Presidential Directive 7: Critical infrastructure identification, prioritization, and protection*. Washington, DC. www.whitehouse.gov/news/ releases/2003/12/20031217-5.html.

▷ Cunningham Robert. 2007. Securing Process Control Systems of Today and Tomorrow. *Proceedings of First Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection. March 18-21.*

▷ DOE & DHS. 2006. *Roadmap to Secure Control Systems in the Energy Sector*.

▷ Dutertre Bruno. 2007. Formal Modeling and Analysis of the Modbus Protocol: Automated Test-Case Generation for Modbus. *Proceedings of First Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection. March 18-21.*

▷ Edmonds Janica, Mauricio Papa & Sujeet Shenoi. Security Analysis of Multilayer SCADA Protocols: A Modbus TCP Case Study. *Proceedings of First Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection. March 18-21.*

▷ Oman Paul & Matt Phillips. 2007. Implementing and Testing a Custom IDS for Substation and Process Control Systems. *Proceedings of First Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection. March 18-21.*

▷ Rodrigo ChandíaCenter. 2007. Security Strategies for SCADA Networks. *Proceedings of First Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection. March 18-21.*

李哲源: 아주대학교에서 컴퓨터공학 박사를 수료하고, 현재 ETRI 부설연구소 연구부장으로 재직 중이다. 주요 관심분야는 국가 기반시설 보호, 컴퓨터 및 네트워크 보안분야이다(cheolee@ensec.re.kr).