중요핵심기반시설(SCADA)에 대한 보안 관리 연구

정회원 김 인 중*, 정 윤 정*, 고 재 영*, 원 동 호**

A Study on the Security Management for Critical Key Infrastructure(SCADA)

InJung Kim*, YoonJung Chung*, JaeYoung Koh*, Dongho Won** ***Regular Members***

요 약

전력, 가스, 상하수도, 고속전철 등 국가에서 관리하는 중요핵심기반시설은 대부분 SCADA(Supervisory Control and Data Acquisition) 시스템으로 관리, 운영되고 있다. 최근 이러한 시설들이 사이버 테러 및 해킹, 바이러스 등에 의하여 원격 조작 및 통제되는 경우 심각한 위험에 빠질 수 있다. 따라서, 중요핵심기반시설에 대한 종합적인 정보보호 관리기법을 수립해야 할 시점에 이르게 되었다.

본 논문에서는 자산, 위협/취약성, 위험도 계산 등의 위험분석 프로세스를 기반으로 정보보호대책(기밀성, 무결성, 가용성) 및 장애처리를 포함한 보안관리 기법을 제안하고자 한다. 이를 위하여 미국, 일본 등 중요핵심기반시설에 대한 정보보호 관리 현황을 알아본다.

Key Words : SCADA, Risk Analysis, Asset, Vulnerability, Threat

ABSTRACT

Most of the national critical key infrastructure, such as power, piped gas and water supply facilities, or the high-speed railroad, is run on the SCADA system. Recently, concerns have been raised about the possibility of these facilities being attacked by cyber terrorists, hacking, or viruses. Thus, it is time to adopt the relevant security management techniques.

This paper attempts to propose such security management techniques, including information protection measures and troubleshooting, based on a risk analysis process concerning assets, threats/vulnerability, and hazards, and to examine the security management status of critical key infrastructure in the U.S. and Japan.

Ⅰ. 서 론

최근 첨단 정보통신기술의 급격한 발전으로 철도, 전력, 발전소, 댐 등 대규모 플랜트 시설들이 제어시스템으로 구축되어 있으나 점차 정보시스템화 되어 가고 있다. 제어시스템은 민감한 프로세스와 물리적 기능을 제어하고 감시하기 위하여 많은 기간시설과 산업에서 사용하고 있는 컴퓨터 기반의 시스템으로 일반적으로 제어시스템은 필드로부터 운영된 데이터와 센서측정 결과를 모으고, 정보를 표시하고, 지역/원격 장비를 순차적 제어 명령을 수행한다. 제어시스템 기반의 대규모 플랜트 네트워크는 국가에서 중점관리하고 있으며 중요핵심기반시설로 지정되어 운영되고 있다. 이러한 시설들의 공통점은 장치마다 상호 또는 외부 기기와 연결하여 각각의 장치에 대한 원격 접근과 제어가 가능하고, 여러 명

* 전자통신연구원 ({cipher, yjjung, jykoh}@etri.re.kr)
** 성균관대학교 전기전자및컴퓨터공학부(dhwon@dosan.skku.ac.kr)
논문번호 : KICS2005-05-025, 접수일자 : 2005년 5월 31일

령 및 조작을 할 수 있도록 양방향 통신서비스 환경을 구축하고 있다. 이러한 환경을 DSC(Distributed Control System) 및 SCADA(Supervisory Control and Data Acquisition)라고 한다. 여기서, DSC는 제어시스템의 일종으로 작은 지역에서 하나의 프로세서나 플랜트에 적용을 의미하고, SCADA는 제어시스템의 일종으로 광역, 분산된 동작을 수행하는 플랜트 등에 적용하는 일반적으로 분산제어시스템을 포함하는 광의의 용어로 사용한다.

본 논문에서는 중요핵심기반시설중에서 정보시스템화 되어가고 있는 SCADA 시스템에 대한 사이버 침해 및 공격에 따른 위협으로부터 시스템을 보호하고 이에 대한 보안 관리 방안을 제시함을 목적으로 한다. 현재 대부분의 국가는 SCADA 시스템을 폐쇄망으로 운영하고 있고, 벤더 고유의 운영체제 및 프로토콜을 사용하므로 사이버 공격과 관련해서 안전하다고 할 수 있다. 하지만 향후 비용 대 효과 면을 극대화하거나 보호해야 할 시설이 중요하지 않다고 판단되는 경우 인터넷 또는 상용망에 연결하여 운영하는 시도가 발생 할 것이다. 이렇게 되면 국가가 운영하고 있는 모든 정보를 대국민들이 같이 공유할 수 있는 장점이 있으나 해커의 공격으로부터 치명적인 피해[1]가 발생할 수 있다. 그림 1은 일반적인 제어시스템의 구성도[2]이다.

기존의 중요핵심기반시설은 현장 제어, 전용회선, 실시간 운영체제, 전용 프로토콜, 단말 PLC 등을 사용하여 해커로부터 독립적이고 안전한 운영이 가능하였다. 하지만 경영합리화를 통하여 중요핵심기반시설들이 중앙집중식 원격 관리, TCP/IP 네트워

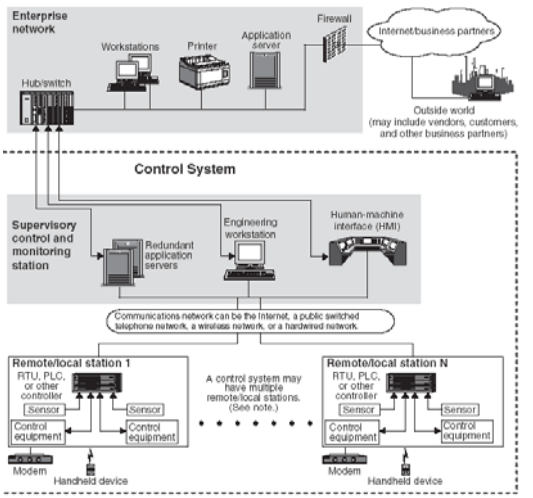

그림 1. 제어시스템의 전형적 구성요소

표 1. 제어망과 정보망간의 비교

	제어망(SCADA)	정보망(MIS)
운영체제	실시간 OS(RTOS) 자체 OS	범용 OS (Windows,Linux)
주전산기	메인프레임	서버
단말기	PLC	PC
네트워크	폐쇄망	개방망/제한망
프로토콜	FieldBUS Industrial Ethernet	TCP/IP
특징	Time Critical	Data Critical
운영 주체	전기/전자 직종	전산/컴퓨터 직종
구축	일괄적으로 진행	순차적으로 진행

크 기반의 프로토콜, 범용 운영체제(Windows, Linux)를 탑재한 PC등을 사용하기 시작하게 되면 점차 안전성이 떨어지고 보안취약점이 증가하기 시작하게 된다[2]. 제어망과 정보망에 대한 비교는 표 1과 같다.

현재까지는 기존의 폐쇠망의 인프라 구조를 바탕으로 SCADA 시스템을 운영하고 있지만 향후 시스템이 노후화되고 새로운 시스템이 구축되는 경우 상호 연동에 따른 취약점 및 위협이 발생하게 되며 이러한 위험은 해커로부터 자유롭지 못하게 된다. 최근 테러의 경향을 보면 점차 SCADA 시스템에 대한 공격으로 집중화되고 있으며 한번 피해가 발생하면 대규모 인명피해 및 국가적 이미지에 엄청난 실추시키게 되는데, 해커의 소행은 고도화 지능화됨에 따라 사이버테러에 대한 대비가 무엇보다도 중요하다. 특히, 사용자의 부주의에 의한 바이러스/웜 유포는 공격의 주체가 불분명하여 대응 및 복구에 대한 한계를 드러나게 한다. 지난 2005년 5월 러시아 모스크바에서 발생한 전력설비에 대한 화재 및 테러로 인하여 모스크바 반경 200Km이내의 모든 정보시스템 및 기반시설을 마비시키는 일이 발생하였으나 정전에 대한 원인 분석이 제대로 이루어지지 못했다. 그리고, 이슬람계 국제 테러조직 알카에다가 최근 한국을 공격 대상으로 지목함에 따라 사이버 테러 가능성이 점차 높아지고 있다[29].

지금까지는 정보망에 대한 위험분석/관리는 활발하게 이루어졌지만 SCADA 시스템에 대해서는 개방형 모델이 아니므로 관련 연구에 상대적으로 소홀하였다. 하지만 SCADA 시스템이 점차 보편화되고 광역화되면 이에 대한 연구가 필요로 하게 된다. 향후 SCADA 시스템은 여러 지역이 널리 분포되어 있으므로 타 시스템과의 연동이 필수적이다. 그림 2와 같이 위성망, CDAM/TDMA망, 유선/무선망, 전

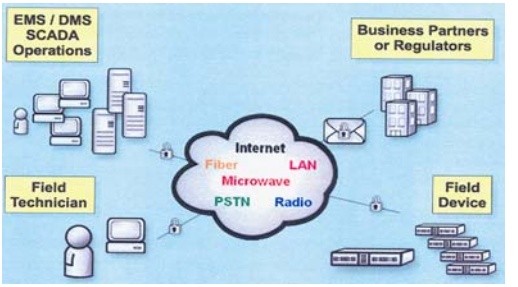

그림 2. SCADA시스템의 연동 분석

화망 등을 복잡하게 운영 관리하고 있으며 이로 인하여 운영자 및 관리자조차도 응용업무의 흐름이 어떻게 진행되고 있는지를 파악하지 못하는 경우가 발생한다.

Gartner사가 2004년 1월 발표한 보고서[26]는 철도, 전력망, 발전소, 댐 등이 중요한 인프라 요소의 접속에 사용되고 있는, SCADA 시스템에 대하여 심각한 취약성을 지적하고 있다. 즉, SCADA 시스템은 IP 기술의 발전에 따라 취약성이 더욱 더 높아지고 있으며 2005년부터 발생될 국가적인 사이버 전의 주 공격 대상이 될 것으로 예측하고 있다. SCADA 시스템은 원래 폐쇄망으로 운영되고 있었기 때문에, 원격으로 접속하는 해커로부터의 공격으로부터 안전하게 관리 될 수 있었다. 하지만 이러한 시설들은 경영 합리화에 따라 인터넷에 연결되고 TCP/IP프로토콜을 사용하는 범용 제어기의 도입되게 된다면 해킹 도구를 이용한 공격[16]에 치명적인 피해가 발생할 우려가 점차 높아지는 것이다.

이에 따라 미국에서는 2003년 2월 "안전한 사이버 공간을 위한 국가 전략"[10]을 발표하였다. 이 전략은, 미국의 경제, 방위, 산업 전반으로 중요한 서비스에 있어서 정보 시스템/네트워크의 사이버 보안에 대한 미국 정부의 정책이 제시되고 있다. 여기에는 사이버 공간에 대한 보호전략의 추진하기 위하여 NIAC(National Infrastructure Assurance Council)를 설치하는 것과 동시에, 정보 시스템 관련의 공공기관이나 민간기업과의 협력 체제를 강화해야 한다는 것이 주요 내용이다. 이를 위하여 SCADA 시설에 대한 보호대책 및 추진 방향은 다음과 같이 제시하고 있다.

① 정부와 민간과의 관계는 디지탈 제어 시스템(DCS)과 감시제어 데이터 수집(SCADA) 시스템의 보안을 강화하기 위해서 신기술의 개발을 실시한다. DCS/SCADA 시스템에 의존하고 있는 파이프라인 및 전력망의 경우 인터넷 접속에 대한 위험을 상세하게 조사하여 24개월 이내에 보안 인증을 실시하는 등, 적절한 조치를 취해야 한다. DCS/SCADA 시스템을 사용하는 타 시설도 같은 보안 대책을 실시하는 것을 고려해야 한다. 에너지성에서는 SCADA 시설의 보호 대책 가이드[9]를 제시하고 있다.

② 대통령 중요 인프라 보호 위원회는, 단기(1~3년), 중기(3~5해), 및 장기(5년 이상)의 IT 보안 연구를 포함한 연방 정부의 연구개발 프로그램에 대해, 과학기술 정책국(OSTP)의 협의한다. 2004년도 이후에 있어서의 연방 정부 자금에 의한 단기의 IT시큐러티 연구개발에는, 과학기술 정책국 및 R&D 위원회가 명확하게 한 우선 프로그램을 포함해야 하는 것이다. 기존의 우선 사항으로서는, 침입 검출, 인터넷 인프라 보안(BGP, DNS등의 프로토콜을 포함), 어플리케이션의 보안, 서비스의 거부, 통신 비밀 보전(SCADA시스템의 암호화 및 인증 포함), 고도의 보증 시스템, 및 보안 시스템 구성 등을 들 수 있다.

③ 정부와 민간과의 관계는 각자 사이버적·물리적인 상호 의존을 명확하게 한다. 또, 국토 안전 보장 전략으로 제안되고 있는 각종 시스템 및 계획에 대하여 취약성을 줄이기 위한 방안을 수립한다.

다음으로 2004년 5월 전략에 대한 세부 실행 계획서[27]를 만들었다. 이 계획서에는 인터넷의 취약성 평가의 처리를 2004년 중에 실시하고, 중요 인프라의 취약성 평가는 2005년부터 예정하고 있다. 또한 카네기 멜론 대학의 미국 컴퓨터 긴급 대응 팀(US-CERT)은 국가적인 사이버침해에 대한 종합적인 대응 임무를 수행하기 위하여 연방 컴퓨터 침해사고 대응 센터(FedCIRC)를 흡수했다. 본토안보국의 사이버 보안국은, 아직 24시간 체제의 대응 센터를 설치하지 않지만, 인터넷이나 그 외의 공공의 네트워크와는 분리된, 데이터와 음성의 네트워크인 중요 인프라 경고 정보 네트워크(CWIN : Critical Infrastructure Warning Information Network)의 확대를 계획하면서 12.8백만달러(약 1,536억원)의 예산을 반영하였다. 여기에는 정부기관간의 정보 공유를 위한 제한시설 사용시 보안투명성, 전자 문서의 인증, 제한시설에서 배포되는 자료에 대한 보안 대책, 정보분석/공유센터의 개선, 무선 보안 네트워크,

사이버 공격의 추적에 관한 연구 등을 포함하고 있다.

이러한 국가기관의 보안정책에 따라 외국에서는 국가기간시설에 대한 취약점 및 위협에 대한 연구[18][19][20]가 활발하게 이루어지고 있으며 특히 테스트베드를 운영[13]하면서 새로운 운영체제 및 프로토콜에 관한 연구도 병행하여 수행 중에 있다.

Ⅱ. 국내외 정책 동향

본 장에서는 국내외적으로 추진하고 있는 정부 정책 동향에 대해 살펴봄으로써 각국의 정책 추진 방향 및 특징에 대해서 알아보고자 한다.

2.1 미국 기관

SCADA 시스템에 대한 중요성을 인식한 가장 큰 사건으로 2003년 8월 14일 미국 북동부 정전사고를 들 수 있다. 이기간 동안 미국과 캐나다 주민 500만명이 고생을 했으며 미국 경제에 약 80억달러의 피해를 입게 되었다. 미 정부는 이러한 정전 사고시 사이버 공격이 동시에 발생하는 경우 더 큰 피해를 발생할 수 있을 것으로 판단하고 향후, 제어망에 대한 성능 개선 시 사이버 보안을 고려하여 설계[14]하도록 하였다. 이를 위하여 SCADA 시스템의 사이버 보안에 대한 2개 범주를 정하였다.

- 비즈니스 정보 및 프로세스의 비밀성과 무결성
- SCADA 시스템을 위한 국가적 보안

2.1.1 PDD63

국제적 테러리스트의 공격으로 부터 국가기간시설의 보호하기 위하여 대통령 명령으로 제정된 법률로써 되었다. 여기에는 정부와 개인이 할 역할과 교통, 상수도, 가스 저장시설 및 생산시설, 화학, 공장, 전력 등에 대한 보안 대책 방안 등을 제시하고 있다.

2.1.2 Operation Liberty Shield

미국 시민과 시설에 대한 보호를 위하여 제시된 국가 계획이다. 여기에는 사람과 상품의 원활한 흐름을 유지하기 위하여 화학시설, 석유화학시설, 핵시설, 전력전송망, 교량, 지하철 등 핵심기반시설과 핵심 자산에 대한 보호등을 포함하고 있다. 역시, 테러리스트 공격, 사이버 테러리즘, 해킹, 정부 지원 사이버전쟁에 대한 계속적인 감시를 포함하고 있다.

2.1.3 에너지성(DOE)[9]과 국가 표준기술국(NIST)

이 두기관은 SCADA시스템과 제어망에 대한 취약점을 점검하기 위하여 테스트 베드를 제작하여 운영하고 있다.

2.1.4 EPA : Environment Protection Agency

국토안보국의 국가전략에 의하여 설립된 기관으로 두 개의 주요기간시설 수자원과 화학공장을 담당하고 있다. 이 기관은 이러한 기간시설에 대한 자산을 분석하고 취약성을 줄이는 사업을 벌이고 있다. 최근 이기관은 중소형 수자원 공사에 대한 보안과 경비강화에 많은 지원을 해주고 있다. 이러한 행동은 2002년 "공공위생보안과생화학테러에대한보호및대응에관한법"(Public Health Security and Bioterrorism Preparedness)에 의거 취약성 분석, 보안 교육, 위급시 대체 요령 등을 알려주고 있다.

2.1.5 미국 화학분야 사이버 보안 전략

기관간의 상호 연동되는 제어 시스템 및 정보에 대하여 안전하게 유지하기 위하여 사이버 보안 위험 관리 및 제거 방안을 제시하고 있다.

2.1.6 미국 석유 연구소(API)

미국 에너지성과 다른 국가기관과의 밀접한 관계를 가지고 있으며 파이프라인, 터미널, 정련, 시추소 등에 대한 취약점 분석을 위하여 "석유 시설에 대한 보안 가이드라인"을 제시하였다. 2003년 5월 API와 국가 석유 및 정제시설 연합회는 "석유 및 석유화학 시설을 위한 보안 취약점 분석 방법론"을 발표하였다.

2.1.7 ISA의 SP99

제어시스템 보안을 목적으로 하는 위원회로 보안 프로세스의 개선과 제어시스템에 대한 방어[4]를 심의하고 있다. SP99 위원회는 4개의 소 분과를 가지고 있으며 2003년 가을 기술 문서[5]를 제시하였다. 이 문서에는 제어시스템 보안을 위하여 간단한 조치사항이 나타난다.

- ISA dTR99.00.01- 제어시스템과 제조를 위한 보안 기술
- ISA dTR99.00.02- 제어시스템 환경과 제조의 집중화된 전자 보안
- ISA dTR99.00.03- 제어시스템 보안과 제조를 위한 테스트,기록, 척도

2.1.8 북미 전기 신뢰성 평의회(NECR) 사이버 보안 긴급 법률 1200[12]

2003년 8월 채택된 이 법률에는 최소한의 사이버

보안을 위하여 구현해야 하는 가이드라인이 정해져 있다. 2004년에 표준화가 될 것으로 예상되며 전력 시설, 관련 지사, 분배망 등에 적용될 것이다.

2.1.9 국토안보국

이 기관은 광역 기반시설에 대한 보안을 위하여 각종 지침 및 절차를 제시한다. 이 지침들은 이전의 부서에서 제시된 내용들을 수정 보완하여 미국을 좀 더 안전하게 유지할 수 있도록 한다.

이외에도 식품 및 마약행정국(Food and Drug Administration), 국가안전국(NSC), 국립과학재단(NSF), 국립학술원(National Academies), 정보 기술연구개발분과, 북미전기신뢰성위원회, 전력연구소, 광전력 시스템위원회, 석유 파이프라인 산업회, 가스기술연구소, 미국가스협회, 화학분과 사이버보안 프로그램 등에 관련 연구를 수행하고 있다.

2.2 미국의 연구기관

미국에서는 SCADA와 관련된 연구소 및 실험실이 많이 있다. 특히 이중에서 PNNL 연구소와 Sandia 연구소가 주요 연구 기관이다.

2.2.1 Idaho 국립공학환경연구소

국가 SCADA 시스템 테스트베드를 운영 중에 있으며 제어시스템 취약성과 보안 대책을 수립하기 위한 연구를 진행 중에 있다. 이 테스트 베드는 컴퓨터 제어, 통신, 필드 시스템에 대한 여러 가지 가능성을 분석하고 새로운 표준과 프로토콜을 개발하는 데 도움을 준다.

2.2.2 북태평양 국립연구소(PNNL)

DOE에서 설립하였으며 전기전력 연구소와 함께 전력분야의 사이버 보안을 연구하고 있다. 1996년에 발표된 주요 인프라 보호대책에 대한 대통령 명령에 대한 기술적 지원, 1997년 여러 연구소과 공동 취약성분석 프로그램, 1998년 DOE의 주요 인트라 보호 대책팀 참여, 2000년 북미 전기 신뢰성 기구(NERC)의 주요 인프라 보호 포럼 지원 등을 하고 있다. 특히, 제어시스템의 보호를 위하여 여러 관계 업체 및 기관과 공동 협력하고 있다.

2.2.3 Sandia 국립 연구소[6]

최근 6년 동안 주요 인프라에 대한 제어시스템 보안을 위한 여러 활동을 수행하였다. 연구원들은 대부분 전력, 가스, 석유, 교통, 수자원, 핵발전, 산업체에 대한 제어시스템의 취약성 분석과 위험 분석 방법론 등을 연구하고 있다. 제어시스템에 대한 취약성을 인식하기 위하여 보안 프로그램, 교육, 위협 시나리오 등을 개발하고 있으며 여러 사이버보안 훈련을 실시하고 있다. 역시 통신프로토콜에서 정보보안을 포함한 표준 작업등을 연구하고 있다.

2.2.4 Snadia의 SCADA 보안 개발부서

이 부서에서는 SCADA 시스템 설계, 시스템, 장비에 대한 보안을 개선하기 위하여 여러 테스트를 수행하고 있다. 역시 침입 탐지, 암호화/인증, 보안 프로토콜, 시스템과 장비의 취약점 분석, 보안 구소 설계, 분석 등을 통해 제어시스템이 강화될 수 있도록 하는 기술 및 정책을 연구하고 있다.

2.2.5 Argonne 국립 연구소(ANL)

DOE에 의하여 설립되었으며 석유와 가스시설에 대한 취약점분석을 실시하고 있다. ANL은 업체와 사용자로부터 상이한 제어시스템 운영체제에 대한 정보를 수집하여 데이터베이스화하고 있다. 이를 통하여 해당 취약점을 평가한다. 또한 이연구소는 여러 제어시스템의 문제점과 영향, 이로 인한 요구사항과 해결방안을 분석하고 있다.

2.2.6 Los Alamos 국립 연구소

Sandia와 공동협력을 하면서 국가 인트라 시뮬레이션 및 분석을 수행하고 있다. 특히 전기와 가스 전력 분야에 중점 수행 중에 있으며 국토안보국의 임무를 지원하고 있다.

2.2.7 프로세스제어시스템 사이버보안 포럼 (PCSCSF)[3]

이 기관은 KEMA 컨설팅과 LogON 컨설팅사가 주관하여 만든 포럼으로 효율적인 제어시스템의 운영을 위하여 사이버 보안에 대한 연구를 수행하고 있다. 주요 포럼 내용은 공격, 위협, 취약성, 최적의 실행, 교육, 해결방안 등을 토의하며 워크샵과 세미나를 수행하고 있다.

2.2.8 KEMA와 CERT/CC

KEMA 컨설팅과 카네기멜론대 CERT/CC는 E-CERT와 관련한 정책을 수립하는 기관으로 국가 주요기간시설, 영향분석, 산업체와 정보교류를 통해 제어시스템상의 사이버 보안 침해와 관련한 정보를 수집하고 분석한다. 취약성과 침해에 대한 관리방안을 수립하며 제어 시스템 개발업체와 함께 공동으로 연구를 수행하고 있다. 전력분야에 중점으로 컨

설팅 및 연구하며 결과를 에너지성과 국토안보국에 제공하고 있다.

2.3 일 본

일본은 1997년 9월부터 대규모 플랜트 망에 대하여 악의 있는 침입자에 의한 데이터의 변조와 파괴에 의한 플랜트의 폭발과 정지등의 장해발생 가능성과 그것에 대한 대응책을 연구[28][22]하고 있다. 이를 위하여 일본정보처리진흥사업협회(IPA)에서 고신뢰성/고시큐리티 제어 시스템의 연구를 통산 산업성 위탁 사업으로 실시하여 이에 대한 취약점 및 위협 사례를 분석[25]하였다.

2.4 국내 현황

인터넷 강국의 우리나라는 현재 인터넷이용률이 세계 최고수준이 65%를 이용하고 있다. 그러나 인터넷을 기반으로 하는 사이버 해킹 공격은 급격히 증가하여 국내 해킹 바이러스 신고 접수는 2001년 5,333건에서 2002년 15,192건, 2003년 26,179건으로 폭발적으로 증가[32]하고 있다. 다만, SCADA 시설의 경우에는 폐쇄망으로 안전하게 운영 관리되고 있으므로 이에 대한 사이버 테러는 발생할 가능성이 없으나 이에 대한 연구는 이루어져야 할 것이다.

2.4.1 NCSC[32]

2002년 1.25 인터넷 대란 이후 국가정보원을 중심으로 국가사이버안전센터(NCSC)를 설립하여 국가 사이버 테러 대응을 위한 정책수립, 국가 사이버 테러 예방 활동, 침해사고 발생시 긴급 대응 조사 및 복구지원 등을 수행하고 있으나 주요정보통신기반시설 및 정보통신망과 관련되어 임무를 수행하고 있다.

2.4.2 국가안전보장회의 위기관리센터[37]

국가 안전보장회의(NSC) 위기관리센터는 국가 위기 관련 업무를 종합해 체계적이고 신속하게 관리하기 위하여 대형 재난 및 재해로부터 군사적 충돌까지 국가 위기를 종합적으로 관리하고 있는 곳이다. 여기에서는 국가위기관리 기본지침을 만들고 위기 위형별 대응 프로그램을 개발하며 사이버 테러에 대한 대응 등 광범위한 네트워크 구성하고 있다.

2.4.3 사이버안보조정회의[36]

국가기간망에 대한 사이버테러 대응을 위한 국가정보원(NIS)의 “사이버안전센터”, 민간부분 사이버테러 대응기구로 한국정보보호진흥원(KISA)의 “인터넷침해사고대응지원센터”, 그리고 군 주요 정보체계 보를 위한 “국방정보전대응센터”등에 대한 상호의견을 조정할 비상설 총괄기구이다. 이 회의에서는 사이버테러 관련 정보를 수집해 보고하는 최상위 대응 기구의 역할을 수행한다.

2.4.4 국가정보원[31]

국내 각종 보안기관, 연구소, 컴퓨터침해사고대응팀(CERT), 정보공유분석센터(ISCA)등에 대한 조정 통제를 수행하고 있다.

2.4.5 소방방재청[30]

재난관련 업무체제의 일원화를 통한 정책심의 및 총괄조정 기능을 수행하며 안전관리 체제를 확립하고 있다. 또한 재난 예방에 대한 인식제고 및 예방투자 강화를 수행하고, 안전의식 제고를 위한 대국민 홍보등 예방활동을 수행하고 있다.

2.4.6 비상기획위원회[35]

국가안전을 위태롭게 하는 비상사태발생시 효율적으로 대처하기 위한 평시 준비 업무를 수행한다. 이를 위하여 비상 대비 계획, 국가 동원, 비상대비 사업, 비상대비 훈련 등을 실시하고 있다.

2.4.7 산업정보보안학회

산업시설에 대한 정보보안 및 이에 관련되는 학문연구[21], 산학활동, 국제 교류 증대를 위하여 국내 산업 및 전자상거래에 대한 정보보안, 보안 산업 경쟁력 강화, 정보보안 정책 및 기술 연구등을 수행하고 있다.

2.4.8 국가보안기술연구소[34]

국가기관 정보시스템 및 주요정보통신기반시설에 대한 보안진단 및 점검을 정기적으로 수행하고 있다. 현재 주요정보통신기반시설에 대한 취약점분석 평가를 통해 분석된 자료를 토대로 국가기간시설에 대한 취약점 및 위협에 대한 기초 연구를 수행 중에 있다.

Ⅲ. 보안 요구사항

SCADA 시스템은 이기종의 유무선 네트워크와 다양한 프로토콜의 혼재로 기존 인터넷 등에서 발생되는 보안 취약성외에도 추가적으로 고려해야 할 보안취약성[15]이 많이 존재한다. 제어시스템의 다양한 기기들은 인터넷과 연결로 사이버 공격의 대상

이 될 수 있으며, 더욱이 시스템에 대한 조정 및 제어가 가능하므로 보안 측면에서 고려해야 할 보안 요구사항은 더욱 복잡해지고 다양화[23]되고 있다. 또한, Ethernet, LON, ProfiBUS, CAN, AS-I, InterBUS 등 다양한 기술[24]이 사용되고 있으나 대부분은 보안 취약성에 대한 연구가 이루어지고 있지 않다.

3.1 시스템 보안

3.1.1 PLC, 장치 인증

불법 장치의 사용을 방지하기 위하여 제어망을 사용하는 경우 장치에 대한 인증 과정이 필요하다. 현재까지 장비 인증은 제대로 이루어지고 있지 않으므로 새로운 장치의 도입 시 이에 대한 기술적 정책적 연구가 필요하다.

3.1.2 사용자 인증

제어망에서는 장치 인증 외에 장치를 사용하는 사람의 신원확인을 위한 사용자 인증 기능이 반드시 필요하다. 제어망에서 생체인식, 패스워드, 인증서, 스마트카드등 다양한 사용자 인증 기술의 활용이 가능하겠지만, 장치의 낮은 성능을 고려하여 사용자 인증 기술의 활용 및 적용성이 검토되어야 한다.

3.1.3 장치간의 인증

안정된 제어시스템을 구현하기 위해서는 기본적으로 장치간의 상호인증이 요구된다. 장치간의 인증이 어려운 경우에는 방화벽 등은 앞단에 설치하여 운영하는 방안을 고려할 수 있다.

3.1.4 암호화

제어시스템의 주요정보를 해커가 읽거나 변조하지 못하도록 암호화해야 한다.

3.1.5 사용자 투명성

기존에 제어시스템을 사용하는 과정과 새로운 보안 시스템을 도입하는 경우가 차이가 없어야 한다.

3.1.6 가용성

제어망에 보안대책을 세워서 가용성이 상실하게 되면 더 큰 위험을 갖게 된다. 따라서 가용성이 허용되는 범위 내에서 보안 대책을 세워야 한다.

3.1.7 기타

제어망의 보안을 위해서는 기존의 보안대책과의 연동이 가능하도록 설계해야 하며, 보안으로 인하여 제어시스템이 불안해지는 경우가 발생하면 안된다.

3.2 보안 관점

SCADA 시스템에 대한 보안 문제[7][8]를 해결하고 발전하기 위해서는 다음과 같은 항목을 고려해야 한다.

- 제어시스템을 위한 사이버 보안의 기술은 무엇인가?
- 어떤 종류의 사이버 공격이 제어시스템에 영향을 미칠 것인가?
- 상호 연동되는 네트워크의 인터페이스는 어떻게 구성할 것인가?
- 제어시스템의 물리적 보안은 어떻게 보증할 것인가?
- 기관의 자산에 대한 보안을 위하여 직원들에 대한 교육 및 훈련을 어떻게 할 것인가?
- 업무의 연속성이 보안 대책 수립 이후에도 보증되는가?
- 산업체와 정부기관간에 연구가 공동으로 이루어지고 있는가?
- 표준 및 규정이 제정되었는가?
- 대부분의 기관이 사이버 보안 표준에 만족하고 있는가?
- 어떤 기관이 제어망을 위한 사이버 보안에 책임을 질 것인가?
- 어떤 평가가 최적의 보안과 만족을 달성했다고 할 수 있는가?

Ⅳ. SCADA 시스템의 보안 관리

먼저 현 대상시설에 대하여 보안에 대한 수준을 사전한 분석을 통하여 보안서비스 및 연동서비스 현황을 분석한다. 이를 통하여 어느 수준의 보안 대책이 되어 있는 지를 분석하게 되는 데 본 보고서에서는 그림 3과 같이 SCADA 시스템에 대한 위험성능분석 모델(Capability model)을 제시한다.

일반적으로 SCADA 시스템에 보안 솔루션이 없는 경우에 곡선 1과 같이 시스템이 독자망인 경우에 가용성 및 기밀성에 대하여 안전하다고 볼 수 있지만 무결성은 보장하지 못한다. 특히, 인트라넷 이상인 경우에는 가용성조차 장담할 수 없다. 따라서 위험분석 결과 A 지점인 경우 SCADA 시스템은 불안전하다고 볼 수 있다. 안전성을 확보하기 위하여 독자망으로 설계할 수 있지만 이 경우 회선비용 및 유지 관리에 많은 어려움이 발생하게 된다. 따라서 보호 솔루션을 SCADA 시스템에 적용함으

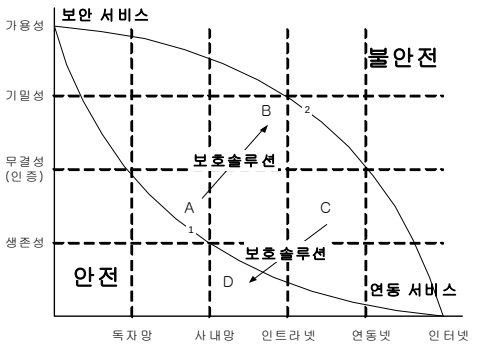

그림 3. SCADA의 성능 분석 모델

로써 곡선을 2와 같은 분포로 만들게 되면 위험분석 결과가 B지점인 경우에도 안전한 시스템이라고 볼 수 있게 된다.

따라서, 인트라넷으로 운영한다고 해도 기밀성을 유지하는 SCADA 시스템이 가능하게 된다. SCADA 시스템에 대한 보안 수준을 확인한 후 안전성을 어느 정도 확보할 것인가는 성능 분석 모델을 통하여 제시한 후 다음 프로세스로 진행한다. 반대로 C지점에 위치한 시스템 모듈에 대하여 D 위치로 이동하게 하여 SCADA 시스템을 안전하게 할 수 있다. 이 경우에는 대부분의 시스템 모듈들이 안전하면서 일부 모듈이 취약한 경우에 사용하는 것이 좋다.

SCASA 시스템에 대한 보안설계는 필요하나 기존의 시스템에 적용하기 위해서는 많은 어려움이 내포된다. 특히 정보보호시스템에 대한 구축을 위하여 기존 SCADA 시스템 및 기기를 중지시킬 수 없다. 따라서, SCADA 시스템에 대한 보안대책을 수립하기 전에 위험분석 또는 취약성분석을 실시해야 한다. 기존에 SCADA에 대한 위험 평가 기법으로 체크 리스트법, 사고예상 결과 분석법, 위험과 운전분석(HAZOP), 이상 위험도분석(FMECA), 결함 수분석(FTA)등이 있으나 표 2와 같이 공정상에 고장, 사고등과 관련된 위험 평가 기법이므로 사이버테러에 대처하기 위한 기법은 아니다[9]. 또한, 정보통신기반시설에 사용되는 GMITS[7], BS7799[8] 등을 사용하기 위해서는 제어망의 특성에 고려한 항목들을 추가로 개발해야 한다. 제안하는 보안관리는 먼저 SCADA망의 연결 정도에 따라 평가 수준을 정의한다. 그림 4에서와 같이 자산 분석은 4단계로 구분한다.

먼저 SCADA망에 대한 자산식별을 통해 SCADA 망이 정보망과 어느 수준으로 연결되어 있는 지를 분석한다. 완전 분리된 망인 경우 관리적인 보안대책으로도 가능하지만 내부 망과의 접점이 있는 경

표 2. SCADA의 위험분석 기법

항 목	Check list	What -if	HAZ -OP	FME -CA	FTA
사업초기	o	o			
상세설계					
위험의 일반적 이해	o	o			
위험의 철저한 분석			o	o	o
정량적 분석					o
간단히 알려진 기술	o	o	o		o
복잡하고 신기술			o	o	
제어 연동			o	o	
운전절차, 비공정조작			o	o	

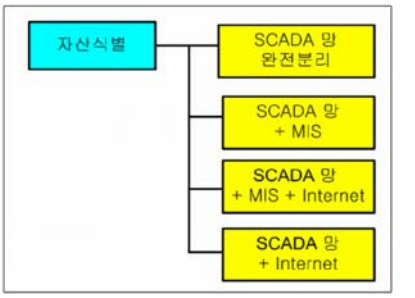

그림 4. SCADA 시스템을 위한 자산분석

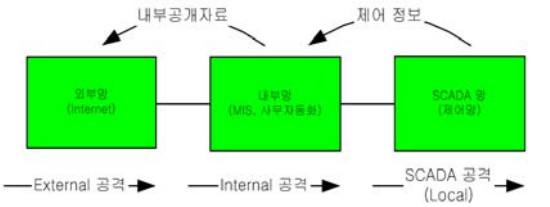

그림 5. 네트워크 연결시 위협분석 구분

우에는 기술적인 보안대책이 필요하다. 특히 정보시스템 또는 SCADA 시스템이 인터넷과 연결된 경우에는 접점을 통해 외부에서 공격하는 해킹까지도 고려해야 하므로 자산 분석이 정밀하게 이루어져야 한다. 다음으로 그림 5와 같이 위협 분석을 실시한다.

여기에서는 위협을 외부 공격, 내부 공격, SCADA (Local)공격으로 구분하여 정의한다. 외부와 연결되어 있는 경우 공격에 대한 보호 대책을 표 3과 같이 매트릭스 표를 만들어 운영한다.

보호대책 설계시 SCADA망에 대한 보안보다는 SCADA망과 정보망간의 연동 점에 대한 보안 설계가 가장 중요하다. 그림 6과 같이 연동 점에 SCADA 망에 적합한 방화벽(Firewall), 보안 가드(Guard), 게이트키퍼(GateKeeper) 등을 설치하고, 데이터의 이상 유무를 파악하고 대응하기 위하여 침입탐지시스템(IDS), 침입방지시스템(IPS)를 도입한다.

표 3. 공격에 대한 보호대책 매트릭스

번호	종류	내용	영향	위험도	빈도수	허용시간	보호대책
1	외부공격	DoS 공격	SCADA 시스템 정지	5	0.1	1시간	공격 IP에 대한 차단을 위한 방화벽 설치
2	외부공격	바이러스 및 웜 유포	SCADA 시스템 정지	5	0.3	6시간	실시간 업데이트 바이러스 서버 구축
3	내부공격	운영 데이터에 대한 유출 및 절취	기관 이미지 실추	3	0.1	24시간	운영자에 대한 보안교육 및 훈련 실시
4	내부공격	MIS 서버 파일 삭제	복구에 따른 부대비용 발생	2	0.3	2시간	서버에 대한 접근제어 강화
5	Local 공격	SCADA 시스템의 유압 계측기 파손	관련 작업 불가	1	0.6	15분	예비 부품 확보 및 응급조치반 가동

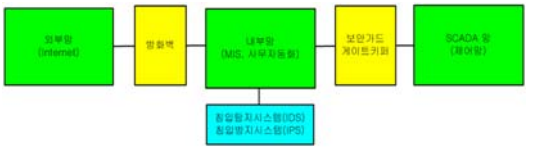

그림 6. SCADA 망에 대한 보안설계 구성도

V. 결 론

SCADA 시스템에 대한 중앙 집중화 및 자동화가 이루어지는 상황에서 안전성을 확보하는 방안이 선행 연구되어야 한다고 본다. 이는 개인의 경제 손실 이외에 국가적인 피해 및 생명까지도 위협받을 수 있기 때문이다. SCADA 시스템에 대한 보안 관리는 매우 어려운 작업이다. 보안 대책을 제시한다고 해도 실제 운영 중인 시스템을 정지시키고 작업을 수행할 수 없으며 또한 해당 취약성을 해결하였다고 할지라도 새로운 취약점이 발견되거나 및 보안관리 방안을 새로 정립해야 한다. 따라서, 기존의 SCADA 시스템에 대해서는 관리적 보안대책을 통해 강화해 나가고 이후 새로운 SCADA 시스템을 구축하는 과정에서 기술적 보안대책을 고려한 설계 방안이 최적의 보안 솔루션이라고 볼 수 있다. 이를 위하여 보안 조직을 정비하고, 보호지침을 만들며, 비상시 재난대비 훈련을 통해 침해사고 예방 및 대응 복구가 실시간으로 해결될 수 있도록 해야 한다. 그러기 위해서는 반드시 보안 관리를 통한 침해 및 피해 영향을 파악하고 있어야 한다.

이제는 정보보호 패러다임의 변화로 인하여 정보통신 환경에서 중요핵심기반시설에 대한 위협 요소에 대한 분석 및 보안관리가 요구되고 있다. 불특정 시스템에 대한 공격으로 중요핵심기반시설에 피해가 발생한다면 일반인들도 공격에 의한 피해 대상이 되는 것이다. 사이버 공격 기술의 보편화로 인하여 공개된 툴을 이용하여 누구든지 해킹 시도 가능하고 중요핵심기반시설에 대한 대규모/ 광역화로 사회적 기능 마비가 발생할 수 있으므로 정보시스템 단위의 정보보호 방식에서 통합 정보보호 방식으로 전환되어야 할 것이다.

참 고 문 헌

[1] 국가정보원, "2004 국가정보보호백서", 2004.

[2] GAO, "Critical Infrastructure Protection : Challenge and Efforts to Secure Control Systems," http://www.gao.gov, Mar. 2004.

[3] PCSCS, "2004 Proposal: Process Control System Cyber Security Forum - An Infrastructure Industry Forum and Initiative," http://www.pcscs.org, 2004.

[4] Jonathan Pollet, "Safety Considerations for SCADA/DCS Cyber Attacks," ISA-The Instrumentation Systems, and automation Society, 1. Nov. 2003. http://www.isa.org

[5] Dale Peterson, "Intrusion Detection and Cybersecurity," ISA-The Instrumentation Systems, and automation Society, http://www.isa.org, 1. May. 2004.

[6] Jason Stamp, John Dilinger, William Young, "Common Vulnerabilities in Critical Infrastructure Control Systems," White paper, Sandia National Laboratories, http://www.sandia.gov, 2003.

[7] 김인중, 정윤정, 민병길, 박중길, "SCADA 시스템과 정보망의 연동을 위한 위험분석 연구," 한국정보처리학회 춘계학술대회논문집, 2004. 5.

[8] 김인중, 정윤정, 박중길, 원동호, "상호연동 기반의 SCADA시스템에 대한 보안위험분석 프로세스," 한국통신학회 하계학술대회논문집, 2004. 7.

[9] The Office of Energy Assurance for the U.S. DoE, "21 Steps to improve Cyber Security of SCADA Networks," 19, Sep. 2002. http://oea.dis.dis.gov/documents/21StepsBooklet.pdf

[10] White House, "the National Strategy to Secure Cyberspace," Feb. 2003. http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf

[11] Dana A. Shea, "CRS report for Congress - Critical Infrastructure: Control Systems and the Terrorist Threat," Congressional Research Service, July 14, 2003. http://www.usembassy.it/pdf/other/RL31534.pdf

[12] NERC board, "Renewal of Urgent Action

Cyber Security Standard", June 2, 2004. http://www.nerc.net
[13] Ron Derynck, "Securing Critical Industrial Networks," Verano white paper, 2004. http://www.verano.com
[14] White House, "The Physical Protection of Critical Infrastructures and Key Assets," Feb. 2003.
[15] 바다란, "Critical Alert for Cyber Terror - Security for Nation Infrastructure(SCADA & DCS), White paper. 2002년 10월.
[16] Ron Derynck, "Cyber-Security and System Integrity for Transportation Networks," Verono White paper, 2004.
[17] Jonathan Pollet, "Developing a Solod SCADA Security Strategy," Sicon02, Nov 2002.
[18] Zhaoxia Xie, G. Manimaran, A.G. Phadke, Virgilio Centeno, "An Information Architechure for Future Power Systems and Its Reliability Analysis," IEEE Trans. Power Systems, VOL. 17, No3, AUG. 2002.
[19] Ebata, Y. Hayashi, H. Hasegawa, Y. Komatsu, S. Suzuki, K., "Devekoment of the Internet-based SCADA for Power System," Power Engineering Society Winter Meeting, 2000. IEEE.
[20] Hamoud, G. Chen, R.-L. Bradley, I. "Risk assessment of power systems SCADA," Power Engineering Society General Meeting, 2003, IEEE.
[21] 한국산업정보보안학회, 산업정보보안정책세미나 및 추계학술대회논문집, 2003년 11월 20일.
[22] 博之, 田中, 克巳 岡, 文一, "Requirements for high reliability and high security plant control system," White paper Information-technology Promotion Agency, http://www.ipa.go.jp, 2000.
[23] 김인중, 정윤정, 민병길, 박중길, "SCADA 시스템 보안을 위한 기술연구," 국가보안기술연구소 기술문서. 2004. 6.
[24] 박장환, "필드버스 입문," 도서출판 동서, 2000. 1.28.
[25] 일본정보처리추진기구, "일본 전력의 중요 인프라시설 방어연습에 관한 조사보고서," 2004. 8.
[26] David L. Fraley, "Cyberwarfare: VoIP and Convergence Increase Vulnerability,"Gartner Report, 13 January 2004. http://www.gertnder.com
[27] William New, "Reports shows holes in cybersecurity plan", Daily berifing, June 21, 2004. http://www.govexec.com/story_page.cfm?articleid=28790&printerfriendlyVers=1&
[28] Douglas, Edward, "The status report on the US preparation for measures against cyber terrorism," http://www.ipa.go.jp, 2000.
[29] 연합뉴스, "보안업계, 알카에다 사이버테러 대비 강화", 2004년 10월.
[30] 소방방재청, http://www.nema.go.kr
[31] 국가정보원, http://www.nis.go.kr.
[32] 국가사이버안전센터, http://www.ncsc.go.kr
[33] 국가사이버안전센터, "국가사이버안전메뉴얼", 2004.
[34] 국가보안기술연구소, http://www.nsri.re.kr
[35] 비상기획위원회, http://www.epc.go.kr
[36] 디지털타임즈, 국가사이버테러대응체계가동, 2003. 12.16.
[37] 국가정보원, 국가사이버안전메뉴얼, 2004.

김 인 중 (InJung Kim) 정회원

1992년 2월 충남대학교 전자공학과(석사)
1992년~2000년 국방과학연구소 선임연구원
2001년~현재 성균관대학교 전기전자및컴퓨터공학부 박사과정
2000년 2월~현재 국가보안기술연구소 선임연구원
<관심분야> 정보보안, 네트워크 보안, 위험분석, 보안관리

정 윤 정 (YoonJung Chung) 정회원

1997년 2월 성균관대학교 정보공학과 졸업
1999년 2월 성균관대학교 정보공학과(석사)
1999년 하나로정보통신 연구원
2000년 11월~현재 국가보안기술연구소 선임연구원
<관심분야> 정보보안, 네트워크 보안, 위험분석, 보안관리

고 재 영 (JaeYoung Koh) 정회원

1998년 8월 전북대학교 공과대학 전자공학과(박사)
1984년~2000년 국방과학연구소 선임연구원
2000년 2월~현재 국가보안기술연구소 책임연구원
2004년~2005년 국가정보보안협의회 사무국장
2005년 6월~현재 통일부 자문위원
<관심분야> 정보보안, 전산망보안, 위험분석, 보안정책

원 동 호 (Dongho Won) 정회원

1976년~1988년 성균관대학교 전자공학과(학사, 석사, 박사)
1978년~1980년 한국전자통신연구원 전임연구원
1988년~2003년 성균관대학교 교학처장, 전기전자및컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장.
1996년~1998년 국무총리실 정보화추진위원회 자문위원
2002년~2003년 한국정보보호학회장
현재 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장, (정통부지정 ITRC) 정보보호인증기술연구센터 센터장
<관심분야> 암호이론, 정보이론, 정보보안관리