情報保護學會論文誌
第19卷 第6號, 2009. 12

SCADA 시스템의 안전성 확보방안에 관한 연구

김 영 진,† 이 정 현, 임 종 인‡
고려대학교 정보경영공학전문대학원

A Study on the Secure Plan of Security in SCADA Systems

Young-Jin Kim,† Jung-Hyun Lee, Jong-In Lim‡
Graduate School of Infomation Management and Security CIST, Korea University

요 약

전기, 가스, 교통 등 주요 기반시설을 감시 제어하는 SCADA 시스템은 보안관리 소홀로 제어권한이 공격자에게 절취당하거나 서비스를 하지 못할 경우 국가적으로 큰 손실과 혼란을 초래할 수 있다. 따라서 SCADA 시스템은 구축시 완벽한 보안대책을 함께 강구하고 사후 보안관리도 철저히 하여야 한다. SCADA 시스템은 일반 정보시스템과는 서비스 응답, 통신 프로토콜, 네트워크 구조 등에서 상이한 특성을 지니므로 SCADA 시스템의 특성에 맞는 보안구조 및 기술을 개발하고, 국가차원에서 보안관리를 위한 법적근거를 마련할 필요가 있다. 본 논문에서는 SCADA 시스템에 관한 보안취약요인을 분석하고 이를 토대로 사이버공격에 대한 SCADA 시스템의 안전성 확보방안을 모색해 보았다.

ABSTRACT

SCADA(Supervisory Control And Data Acquisition) systems are widely used for control and monitoring of critical infrastructures including electricity, gas and transportation. Any compromise in the security of SCADA systems could result in massive chaos and disaster at a national level if a malicious attacker takes the control of the system. Therefore, sound countermeasures must be provided when the SCADA systems are being developed as well as when they are being operated. Unlike general information processing system, SCADA systems have different service responses, communication protocols and network architectures and therefore a different approach should be applied to each SCADA systems that takes into consideration of each system's security characteristics and architectures. In addition, legal basis should be established to ensure the nationwide management of the systems security. This paper examines the vulnerabilites of SCADA systems and proposes action plans to protect the systems against cyber attacks.

Keywords: SCADA, security characteristics

I. 서 론

현대사회는 정보화 사회로서 우리의 생활에 필수불가결한 전력·가스·수도 공급 및 교통관리 등 대부분의 국가기반시설과 대규모 산업시설이 정보시스템을 기반으로 하는 SCADA 시스템에 의해 감시 운영되고 있다. SCADA(Supervisory Control and Data Acquisition) 시스템은 각종 센서들을 제어대상 시스템 및 네트워크에 설치하고, 관리자가 이를 통해 정보를 수집 분석하여 해당 시스템 및 네트워크를 감시 통제하고 필요한 조치를 할 수 있도록 구축된 것으로, 산업제어시스템(Industrial Control Systems, ICS), 분산제어시스템(Distributed Control Systems, DCS), 공정제어시스템(Process Control Systems, PCS) 등으로도 불린다[1].

이러한 SCADA 시스템은 대상 시스템이 정상적으로 운영되도록 직접적인 제어를 수행하므로 고도의 안전성이 요구된다. 만약, 잘못 조작되거나 악의적으로

접수일(2009년 7월 27일), 게재확정일(2009년 9월 8일)
† 주저자, yjkim243@korea.ac.kr
‡ 교신저자, jilim@korea.ac.kr

조작될 경우 국가적으로 큰 손실과 혼란을 초래할 우려가 있다[2]. 최근들어 SCADA 시스템은 정보통신 네트워크 형태로 다양한 전산시스템을 통해 정보를 수집 분석하고 제어명령을 수행하는 형태로 구성되고 있다[3]. 이로인해 SCADA 시스템을 위한 네트워크와 외부 네트워크 및 인터넷 등의 연결접점이 늘어나고, 그에 사용되는 전산시스템의 수가 증가함에 따라 보안취약성도 증가하고 있다. 또한, 이에 대한 체계적인 보안관리를 위한 법적기반도 미비하다.

따라서, 본 논문에서는 다양한 SCADA 시스템의 보안정책동향을 살펴본 후 SCADA 시스템에서 발생가능한 보안취약요인을 분석하고 이를 토대로 사이버 공격에 대한 SCADA 시스템의 안전성 확보방안을 제시해 보고자 한다.

II. SCADA 시스템의 구조 및 보안정책 동향

2.1 SCADA 시스템의 구조

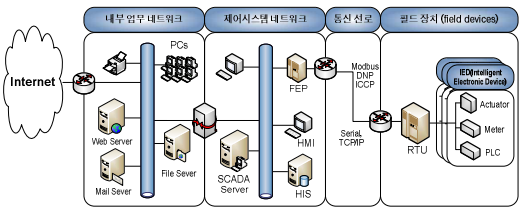
SCADA 시스템은 전력·가스·항공 등 활용되는 대상과 목적에 따라 네트워크 구성환경과 구조가 달라질 수 있지만 일반적인 구조는 다음 [그림 1]과 같다.

SCADA 시스템은 기본적으로 서버, HMI (human machine interface), 전단처리기 (front-end processor, FEP), 히스토리정보 서버 (history information server, HIS), 필드장치 (field devices) 등으로 구성된다[2].

① **SCADA 서버** : 필드장치에서 전송되는 계측정보를 수집·분석하고, HMI를 통해 내려진 제어 명령을 필드장치로 전달하는 장치

② **HMI** : 다양한 수집정보를 SCADA 시스템 사용자에게 제공하며, 사용자가 정보를 분석·판단하여 내린 제어명령을 각 필드장치에 전달

③ **FEP** : SCADA 서버와 다른 프로토콜을 사용하는 필드장치도 SCADA 서버와 통신할 수 있도록 프로토콜을 변환해 주는 역할을 수행



[그림 1] 일반적인 SCADA 시스템 네트워크 구조

[표 1] SCADA 시스템과 일반 정보시스템의 차이점

항목	SCADA 시스템	정보시스템
서비스 응답시간	실시간 응답 (서비스 지연 불허)	비실시간 또는 실시간 응답 (서비스 지연 허용)
가용성	서비스 중지 불허	서비스 중지 감내 가능
통신 프로토콜	전용통신 프로토콜 사용 (Modbus, DNP, ICCP 등)	TCP/IP 기반 통신 프로토콜
중요 보안 요구사항	가용성, 무결성	기밀성, 가용성
사고피해 파급효과	국가 사회적 손실 또는 혼란 야기	업무 불편 및 손실 발생

④ **HIS** : 제어기기와 SCADA 시스템의 상태정보 및 HMI를 통해 전달된 제어명령 등의 로그정보를 저장

⑤ **필드장치** : 대상 시스템의 다양한 상태신호 또는 정보를 SCADA 서버로 전송하고, SCADA 서버에서 전달된 제어명령을 해석하여 실제 제어대상 기기에 적합한 명령 신호를 보내는 장치들이며, 사용 환경에 따라 RTU (remote terminal units), PLC (programmable logic controllers), IED(intelligent electronic devices), PAC(programmable automation controller) 등으로 다양

SCADA 시스템 네트워크는 업무상의 필요에 따라 내부 업무네트워크와 연계된다[4]. SCADA 시스템 네트워크에서 내부 업무용 네트워크로 수집·분석된 정보를 전달하여 업무에 활용하도록 하고, 그 정보를 다시 외부기관으로 전송하거나 SCADA 시스템 네트워크와 외부기관 네트워크를 직접 연결하여 정보를 공유할 수 있다.

또한, SCADA 시스템은 일반 정보시스템과 여러 가지 면에서 상이한데, 그 차이점을 정리해 보면 [표 1]과 같다[5].

2.2. SCADA 시스템 관련 보안정책 동향

2.2.1 미국

2006년 에너지부는 에너지분야 SCADA 시스템 보안을 위한 로드맵을 발표했다[6]. 이는 에너지부, 국토

안보부, 캐나다 국가자원위원회가 공동 개발한 것으로 2015년까지 개발예정인 보안수준은 다음과 같다.

① SCADA 시스템의 운영기관이 보안현황을 실시간 모니터링 가능

② 차세대 SCADA 시스템은 보안기능을 내장하여 end-to-end 보안구조로 구현

③ SCADA시스템 네트워크가 외부공격에 자동 대응

④ SCADA 시스템 운영기관과 정부 합동 보안업무 수행환경 구축

2008년 3월 미국의 수자원 산업협회는 수자원분야 SCADA 시스템 보안을 위한 로드맵을 발표했다[7]. 이는 국토안보부와 수자원 산업협회가 공동으로 개발한 것으로 10년 이내 핵심기능의 손상없이 사이버 공격에 생존할 수 있는 SCADA 시스템을 개발, 운영하는 것을 골자로 하고 있다.

2009년 2월 미국의 국토안보부는 SCADA 시스템 보안협의를 위해 정부, 제조업체, 운영기관으로 산업제어시스템 협동워킹그룹(industrial control system joint working group)을 설립했고, 오바마 대통령은 미국의 사이버보안전략 재검토를 통해 국가기반시설에 대한 사이버 공격의 위험성을 정확히 파악할 것을 요구하는 등 정부차원에서 SCADA 시스템 보호에 많은 관심을 보이고 있다. SCADA 시스템 보안과 관련하여 올해 미국 국토안보부는 보안프로그램 개발을 위해 600만 달러를, 교통부는 항공분야 보안강화를 위해 1,200만 달러를, 에너지부는 보안기술 연구를 위해 2,500만 달러를 각각 투자할 계획이다.

2.2.2 한 국[8]

2001년 7월 정보통신기반보호법을 제정하여 SCADA 시스템을 비롯한 정보통신기반시설에 대한 국가차원의 보호체계를 구축하였다. 국가적으로 중요한 정보시스템 및 전자제어망을 주요정보통신기반시설로 지정, 취약점 분석·평가와 보호대책을 수립 시행하여 각종 전자적 침해행위를 사전에 예방하고 유사시 신속한 대응 및 복구를 하도록 한 것이 주요내용이다.

주요정보통신기반시설의 지정 대상은 사이버침해 발생시 국가안보와 국민생활에 중대한 영향을 미치는 국가안보·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템(SCADA)과 정보통신망으로 민간시설도 포함된다. 중앙행정기관의 장은 소관분야 정보통신기반시설 중에서 해당 관리기관이 수행하는 업무의 국가 사회적 중요성과 침해사고 발생시 국가안전보장과 경제 사회에 미치는 피해규모 및 범위, 침해사고의 발생가능성 및 복구의 용이성 등을 기준으로 주요정보통신기반시설로 지정할 수 있는데, 2009년 1월 현재 10개 중앙행정기관, 78개 관리기관, 109개 기반시설이 지정·관리되고 있으며 이 중 SCADA 시스템은 전력·가스분야 3개 시설이 지정되어 있다.

관계 중앙행정기관의 장은 매년 소관분야 주요 정보통신기반시설에 대한 다음연도의 보호계획을 수립, 정보통신기반보호위원회의 심의를 거쳐 시행하여야 하며, 관리기관은 신규 취약점 제거 및 경제적이고 실효성 있는 보호대책을 수립하기 위해 매 2년마다 정기적으로 취약점 분석·평가를 수행하고 있다.

III. SCADA 시스템에 대한 보안취약요인

3.1 법 · 제도적 취약요인[9]

SCADA 시스템은 일반 정보시스템과 통신 프로토콜, 서비스 응답시간 등 많은 면에서 차이가 있으나, 이의 구축, 운영 및 보호에 관한 법적근거가 미약하여 체계적인 보호가 이루어지지 않고 있다.

정보통신기반보호법은 제2조에서 동법의 적용대상인 “정보통신기반시설”을 전자적 제어·관리시스템 및 정보통신망이라고 정의하고 있어 SCADA 시스템을 보호대상에 포함하고 있으나, 법에 규정된 각종 보호체계와 방법·절차 등은 정보통신망의 보호에 치중하고 있고, 실제로 주요정보통신기반시설로 지정된 것도 일반 정보통신망이 대부분이다. 또한, 보호활동 내용도 SCADA 시스템을 위협하는 다양한 침해행위 중에서 해킹, 컴퓨터바이러스, 서비스거부공격(DoS) 등 “전자적 침해행위”로 한정하고 있어 SCADA 시스템의 체계적인 보호에는 한계가 있다.

또한, 주요정보통신기반시설로 지정된 SCADA 시스템의 관리기관이 매년 정부에 제출하는 보호대책의 심의기능을 가진 정보통신기반보호위원회도 시행 첫해를 제외하고는 모두 서면심의로 대체되는가 하면, ’08년에는 위원회의 위원장도 국무총리에서 국무총리실장으로 하향 조정되는 등 주요 정보통신기반시설 보호에 대한 국가·사회적인 관심도 낮은 편이다.

취약점 분석·평가시에도 주로 정보시스템과 동일한 점검방식과 보안도구를 사용하기 때문에 전력, 가스 등 SCADA 시스템의 특수성이 고려되지 않아 취약점을 효율적으로 발굴 개선할 수 있는지도 의문이다.

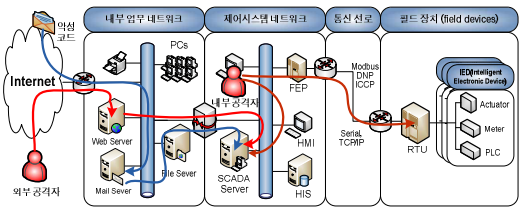
전자적침해행위가 발생한 경우에도 관리기관의 신고의무가 없어 신속한 원인규명과 재발방지대책 마련이 곤란함에 따라 동일한 사고가 다른 곳에서 재발할 가능성이 다분하다. 또한 중앙행정부처가 주요 정보통신기반시설을 자율적으로 지정토록 되어 있어 지정실적이 극히 저조한 데다 그중에서도 SCADA 시스템이 차지하는 비중은 더욱 낮은 실정이다.

이렇게 법적기반이 미약하다 보니 국가차원의 SCADA 시스템 보호노력 또한 미미하다. 국가정보원과 국가보안기술연구소를 중심으로 SCADA 보안정책과 기술연구를 수행하고 있고, 전력분야의 경우 정보공유분석센터(ISAC)를 설치, '전력IT 보안관리지침'을 수립·시행하는 등 다소 활발한 활동을 하고 있으나, 여타 분야는 그렇지 못한 것이 현실이다.

3.2 기술적 취약요인

SCADA 시스템의 보안위협은 발생위치에 따라 크게 두 가지로 나눌 수 있는데, 웹서버와 같이 공개된 서버를 통해 외부에서 침입하는 경우와 충분한 접근권한을 가지고 있는 내부자에 의해 발생하는 경우이다. [그림 2]는 SCADA 시스템에 대한 사이버 공격유형을 발생위치에 따라 다양하게 나타내고 있다.

또한, 대부분의 SCADA 시스템은 업무상 필요성 등으로 내부의 업무용 네트워크나 외부기관 네트워크와 연동하여 사용되고 있어[10] 다음과 같은 보안위협에 직면하고 있다.



[그림 2] SCADA 시스템 보안위협 발생원인 및 위치

3.2.1 외부 네트워크와 연동에 의한 보안위협

① 단일 네트워크 환경 : 다양한 내부 업무용 시스템이 연결된 네트워크에 SCADA 시스템을 연결하여 사용하는 경우로 내·외부의 모든 보안위협에 노출된다. 인터넷을 통해 SCADA 시스템 운용을 위한 서버, 터미널 장치 등에 다양한 형태의 사이버 공격이 가능하다. 각 시스템의 취약점을 이용한 직접 침투가 가능하며, 전자메일 등을 이용하여 악성코드의 전파도 가능하다. 또한 내부자는 SCADA 시스템의 권한을 쉽게 획득하여 임의로 조작할 수 있다.

② 서브넷으로 구분된 환경 : SCADA 시스템 네트워크와 내부 업무네트워크를 두개의 서브 네트워크로 구성한 후, 침입방지시스템(firewall)을 이용해 연결한 환경으로, 이 경우에도 적절한 접근제어를 하지 않을 경우 내·외부의 보안위협에 노출된다. 공격자는 우선 내부 업무네트워크의 시스템을 해킹한 후 다시 SCADA 시스템 네트워크를 해킹하여 권한을 획득할 수 있다. 또한 업무용 시스템이 웜, 바이러스에 감염될 경우 SCADA 시스템으로 쉽게 전이될 수 있으며, 내부자도 간단한 노력만으로 SCADA 시스템의 권한을 획득할 수 있다.

③ 망 분리 후 중계서버로 연동되는 환경 : SCADA 시스템 네트워크와 내부 업무네트워크를 완전히 분리된 별도의 네트워크로 만들고, 두 네트워크 사이에 중계 시스템을 두어 필요한 정보를 교환하는 환경으로, 이 경우에도 내·외부의 보안위협에 노출된다. 공격자는 내부 업무 네트워크의 한 시스템을 해킹한 후 그 시스템을 이용해 중계서버를 해킹하고, 다시 SCADA 시스템을 해킹할 수 있다. 또한 전자메일, 웹서비스, 파일전송 등을 통해 유입된 웜, 바이러스, 악성코드 등에 의해서도 피해를 입을 수 있다.

3.2.2 SCADA 시스템 내부 보안위협

SCADA 시스템 네트워크에는 다양한 시스템과 단말장치들이 연결되어 물리적으로 하나의 네트워크가 된다. 따라서 하나의 시스템 권한이 절취당하거나 악성코드에 감염될 경우 그 피해는 곧 전체 네트워크로 확산된다. 또한 내부 사용자는 하나 이상의 SCADA 시스템 구성요소에 접근할 수 있을 것이고, 이를 이용하면 보다 쉽게 전체 시스템을 공격할 수 있다.

3.2.3 시스템 취약성에 의한 보안위협

SCADA 시스템은 다양한 응용 프로그램과 전산장비 등이 통합된 하나의 솔루션이다. 각 응용 프로그램과 전산 장비들은 대부분 시스템 보안에 대한 큰 고려없이 개발되고 있다. 또한, 시스템에서 운영되는 서비스들 역시 보안 취약점을 내포할 수 있어 공격의 대상이 된다. 특히, rlogin, ftp, http 등의 경우 패스워

드 없이 손쉽게 접근이 가능하여 다양한 방법으로 관리자 권한을 획득할 수 있다. 또한, DNP, ICCP, Modbus 등 SCADA 시스템에서 사용되고 있는 통신프로토콜은 무결성이 보장되지 않아 공격자가 SCADA 시스템 통신회선에 접근만 가능하면 허위의 메시지를 생성하여 피해를 가할 수 있다.

IV. SCADA 시스템의 안전성 확보방안

4.1 SCADA 시스템에 맞는 보안관리 법적근거 마련

SCADA 시스템은 일반 정보시스템과 달리 피해 발생시 국가안보와 국민생활에 치명적인 영향을 미칠 우려가 있기 때문에 체계적이고 효율적인 보호를 위해서는 그에 맞는 별도의 법률이 마련되어야 한다.

SCADA 시스템에 대한 공격은 단순히 정보통신망을 통한 해킹 등 전자적 수단만을 사용하여 이루어지지 않고 시스템 관리자 매수를 통한 내부망 직접침투 등 사회공학적 방법과 물리적 침입을 결합한 보다 적극적이고 다양한 수법을 통해 이루어지는 경향이 있기 때문에 이에 대한 국가차원의 대비가 필요하다.

SCADA 시스템의 관리기관 뿐만 아니라 시스템 개발과 유지보수 및 경비보안을 담당하는 기관·업체까지도 법의 적용대상에 포함하여 시스템의 개발-구현-운영-폐기에 이르기까지 전 과정에 걸쳐 각 분야별로 보안대책이 수립·시행되도록 하여야 한다. 즉, SCADA 시스템 개발시 정부가 제시한 보안기준을 만족하고 전문기관의 안전성 확인을 거쳐야 하며, 운영과정에서 시스템 구성 변경이나 업무망 연동 등 보안취약점을 유발할 수 있는 각종 환경변화가 필요한 경우에는 시스템의 안전성을 확보할 수 있는 표준화된 방법과 절차가 준수되어야 한다. SCADA 시스템과 관련한 민감하고 상세한 자료는 인터넷이나 세미나·학회 등을 통해 무단 공개되지 않도록 보안관리 기준도 마련되어야 한다. SCADA 보호정책을 총괄하는 위원회는 대통령을 위원장으로 하고 장관급을 위원으로 구성하여 정책의 시행효과를 제고하는 한편, 전력·가스·수자원 등 분야별로 전문위원회를 두어 각 분야에 적합한 보호정책을 수립·시행할 수 있도록 하여야 한다. SCADA 시스템 취급인력에 대한 보안대책을 철저히 수립함과 동시에 특별수당 지급 등 혜택도 동시에 고려하여 전문인력을 양성 관리하여야 한다. SCADA 시스템의 침해사고를 실시간으로 감시, 대응책 강구를 위한 통합 보안관제체계를 구축하고 유사시 소방·경찰 등과 연계한 재난 및 범죄방지 대책도 함께 마련하여야 한다. 전문 연구기관을 지정하여 첨단 SCADA 시스템 보안기술을 연구·보급하도록 하는 한편, SCADA 시스템 보안표준을 마련하고 이를 준수한 관리기관이나 업체에 대한 각종 예산 및 세제혜택 등의 지원방안도 적극적으로 강구하여야 한다.

이와 관련, 현재 논의되고 있는 '지능형전력망촉진법' 제정안도 '지능형전력망촉진 및 보호에 관한 법률'로 변경하여 정부차원의 보호활동 내용이 포함되도록 하여야 할 것이다.

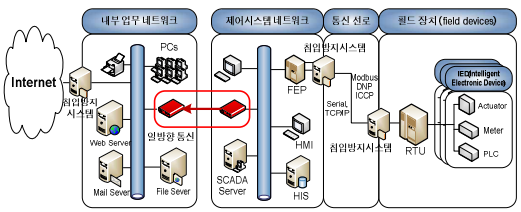
4.2 안전한 SCADA 시스템 구축방안

일반 정보시스템에 사용되는 보안제품은 SCADA 시스템에 필수적인 제어명령의 적시성(適時性) 및 실시간 응답성을 만족시키지 못하기 때문에 SCADA 시스템에 적합한 보안 아키텍처, 보안 통신프로토콜, 메시지 무결성 보장기법 등을 개발 적용하여야 한다.

4.2.1 외부 연동에 의한 보안위협 해소방안

SCADA 시스템 네트워크는 외부 네트워크 및 인터넷 등과 차단되도록 구축되어야 하나, 내부 업무에 따른 요구사항 등으로 실제 완벽한 분리나 차단이 불가능하다. 따라서 SCADA 시스템 구축단계에서 고려해야 할 세 가지 유형의 보안대책을 보안강도가 높은 순서에 따라 제시하고자 한다.

① 일방향 통신기술 적용 : 암호화 통신을 수행할 수 있는 일방향 통신장비를 SCADA 시스템 네트워크와 내부 업무네트워크 사이에 설치하고, 이를 통해 두 네트워크가 연동되도록 한다. 일방향 통신장비는 정보가 한 방향으로만 흘러 가도록 제한하는 시스템으로, [그림 3]은 일방향 통신기술이 적용된 SCADA 시스템 네트워크와 내부 업무네트워크 사이의 안전한 통신연결을 보이고 있다. 이 기술은 데이터 다이오드라는



[그림 3] 일방향 통신기술이 적용된 SCADA 시스템 네트워크

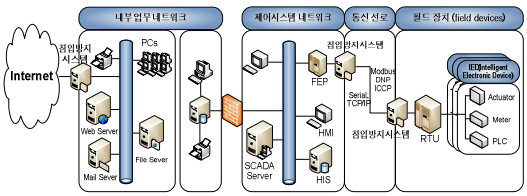
이름으로 1988년 호주 DSTO(Defense Science and Technology Organization)에서 처음 사용되었으며[11], 이후 미국의 NRL(Naval Research Laboratory) 에서 데이터 덤프, 보안저장 및 전달장치 등의 이름으로 연구되었다[12].

이 시스템을 도입할 경우 내부 업무네트워크의 데이터 및 공격자의 공격시도 등이 SCADA 시스템으로 전송될 수 없어 악성코드 및 바이러스의 전파가 불가능함에 따라 SCADA 시스템 네트워크를 안전하게 보호할 수 있다.

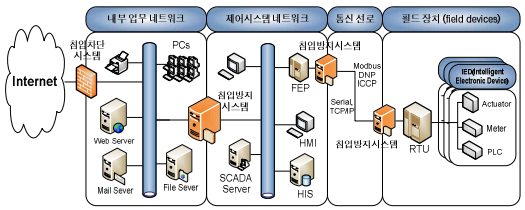
② 내부 업무 네트워크 구조변경 : 내부 업무네트워크의 구조를 업무에 따라 분리하여 이원화 운영하도록 한다. [그림 4]와 같이 SCADA 시스템에서 필요한 정보를 획득하여 업무를 수행하는 네트워크는 SCADA 시스템 네트워크와 연동되도록 구성하되, 다른 업무네트워크와는 완벽하게 차단되도록 하고 독립된 공간에 설치하여 제한된 인원만 출입을 허용하도록 하고, 시스템 및 네트워크 자체에 대한 접근권한 역시 필요한 인원에게 최소한의 수준으로 부여한다.

③ 침입방지시스템을 이용한 연결 : 침입방지시스템을 이용해 두 네트워크를 연결하는 것으로 가장 현실적인 방안이다. [그림 5]는 침입방지시스템이 외부 공격으로부터 SCADA 시스템 네트워크를 보호하는 모습을 보이고 있다. 내부 업무네트워크에서 SCADA 시스템 네트워크로 접근 및 정보전달 시도는 전부 차단하고, 반대방향으로 전달되는 자료는 허용하도록 구성한다. 이 방법은 전달 자료에 대한 패턴 검사를 통해서 악성코드, 바이러스 등을 조기 발견할 수 있고, 기밀자료가 유출되는 것을 탐지할 수도 있다.

이 방법은 반드시 침입방지시스템에 대한 보안성 검토를 거쳐야 한다. 침입방지시스템이 침입목표가 되어 집중공격을 받을 수 있고, 이로 인해 서비스 장애 상태에 빠질 수도 있으며, 버퍼 오버플로우 공격 등으로 관리자 권한이 절취당할 수 있는 취약성이 존재할 수 있기 때문이다.



[그림 4] 분리된 내부 업무 네트워크 구성



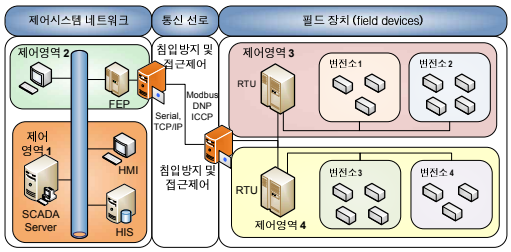
[그림 5] 침입방지시스템을 이용한 SCADA 시스템 네트워크 보안

4.2.2 SCADA 시스템 내부 보안위협 대처방안

SCADA 시스템 네트워크를 기능단위, 제어범위, 제어계층 등에 따라서 여러 개의 보안영역으로 구분하고, 각 영역에 대한 접근제어 목록을 구성하여 다른 영역사이의 정보흐름을 통제함으로써 내부에서 발생할 수 있는 제 2, 제 3의 공격을 차단하고, 내부자에 의한 공격시도도 차단할 수 있다. 또한, 각 영역 사이에는 침입차단장치나 보안게이트웨이 등을 설치하여 잘못된 접근시도나 비정상 트래픽, 취약한 프로토콜 등에 대해 사용제한을 할 수 있도록 한다.

[그림 6]은 각 보안 영역으로 구분되어 보호되고 있는 제어시스템 네트워크를 나타내고 있다.

또한 내부자에 의한 침입방지를 위해 각 사용자의 권한을 세분화하여 권한위주의 접근통제를 수행하고, 보안 운영체제를 도입하여 내부자에 의한 해킹시도를 미연에 탐지하고, 탐지결과에 신속하게 대응할 수 있는 보안관제체계를 구축해야 한다. 이 때, SCADA 시스템의 기능적 특징인 실시간 응답, 시리얼 통신, 무중단 요구, 결함허용(Fault Tolerance) 등을 고려하여 특화된 보안관제기술을 개발할 필요가 있다.



[그림 6] 영역별 접근통제가 적용된 안전한 SCADA 시스템 네트워크

4.2.3 시스템 및 서비스 보안취약성에 대한 대책

SCADA 시스템을 구성하는 각 서버, 클라이언트, 통신장치, 필드장치 등에는 다양한 보안 취약점이 존재할 수 있다. 따라서 주기적으로 보안 취약성을 분석하고 보호대책을 수정 보완하여야 한다.

또한 백신 및 침입탐지제품을 설치하고 지속적으로 보안업데이트를 하여 시스템 자체에 대한 보안관리를 수행한다. 이 때 사용하는 보안업데이트 서버는 외부 네트워크와 연계되지 않도록 하여야 한다. USB를 통한 악성코드 유입방지를 위해 보안 USB 메모리의 사용을 의무화한다. 이렇게 하면, 정보유출도 방지할 수 있는 이중 효과를 거둘 수 있다.

각 시스템에서 지원되고 있는 서비스중에서 보안 취약점이 공개되어 공격에 노출된 서비스와 평문 전송 및 패스워드 없이 사용할 수 있는 응용서비스들은 사용하지 않도록 한다. 특히, telnet & ftp (평문통신), rsh & rlogin(패스워드 없이 원격로그인) 등과 같은 취약한 서비스 사용은 지양(止揚)한다.

그리고, SCADA 시스템 내에서 소통되는 메시지 및 제어명령 등의 무결성과 기밀성을 보장할 수 있는 새로운 통신 프로토콜이 개발 및 적용되어야 한다. 현재 IEC (International Electrotechnical Commission) 에서 보안기능을 탑재한 DNP, ICCP 프로토콜의 국제 표준을 추진 중에 있다[13-15].

V. 결 론

최근 SCADA 시스템의 중요성과 사이버 공격으로 인한 대규모 피해발생 가능성이 크게 대두되고 있다. 미국을 비롯한 각국에서는 자국의 안보를 위해 SCADA 시스템에 대한 보안정책 및 기술개발에 앞장서고 있다. 본 논문에서는 최근의 이러한 동향을 살펴본 후 국가안보에 중대한 위협이 되는 SCADA 시스템의 사이버 공격에 대한 취약점을 분석하고, 이를 개선하기 위한 다양한 보안대책을 연구하였다.

또한, SCADA 시스템에 대한 사이버 공격은 국가간의 전쟁에서도 중요한 수단으로 간주되고 있다. 상대국가의 SCADA 시스템을 해킹하여 파괴시키거나 동작 불능으로 만들어 경제, 사회 등 국가 전반의 광범위한 피해유발과 대국민 혼란을 야기하고, 이를 통해 전력(戰力)을 감소시키는 것이 주요 목적이다.

따라서 국가차원에서 SCADA 시스템을 보다 안전하게 보호하여 국가안보를 공고히 함은 물론 국민들이 안정된 생활을 영위할 수 있도록 SCADA 시스템 보호를 위한 법, 제도를 조속한 시일내에 완비하고, 관련기술도 지속적으로 연구 개발하여야 할 것이다.

참 고 문 헌

[1] K. Stouffer, J. Falco, and K. Kent, “Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security,” NIST Special Publication 800-82, pp. 1-13, Sep. 2006.

[2] 김인중, 정윤정, 고재영, 원동호, “중요핵심기반시설(SCADA)에 대한 보안 관리 연구,” 한국통신학회 논문지, 30(8C), pp. 838-848, 2005년 8월.

[3] 김명수, 임용훈, 현덕화, 김충환, “전력자동화용 통신프로토콜 현황 및 분석,” 대한전기학회 하계학술대회논문집, pp. 2349-2351, 2003년 7월.

[4] 민병길, 김신규, 장문수, 서정택, “SCADA 시스템의 안전한 망 연동,” 한국사이버테러정보전학회 정보·보안논문지, 9(1), pp. 95-103, 2009년 3월.

[5] 이철수, “원방감시제어자료수집(SCADA) 시스템 보안성 강화 방안,” 국가사이버안전센터, Monthly 사이버 시큐리티, pp. 8-17, 2005년 12월.

[6] U.S. Department of Energy, U.S. Department of Homeland Security, “Roadmap to Secure Control Systems in the Energy Sector,” pp. 16-17, Jan. 2006.

[7] U.S. Water Sector Coordinating Council Cyber Security Working Group, “Roadmap to Secure Control Systems in the Water Sector,” pp. 21-33, Mar. 2008.

[8] 국가정보원, 방송통신위원회, “2008 국가정보보호백서,” pp. 99-103, 2008년 4월.

[9] 정보통신기반보호법, 법률 제8852호, 2008년 2월.

[10] J. Lee, H. Lee, and S. Kim, “Development Plan of Korean - Energy Management System,” Proc. of the 17th Conference of the Electric Power Supply Industry, pp. 1-3, Oct. 2008.

[11] N. Stevens and M. Pope, “An Implementation of an Optical Data Diode,” DSTO-TR-0785, DSTO Technical Report, May 1999.

[12] J.N. Froscher, D.M. Goldschlag, M.H. Kang, C.E. Landwehr, A.P. Moore, I.S. Moskowitz, and C.N. Payne, “Improving Inter-Enclave Information

Flow for a Secure Strike Planning Application," Proc. of 11th Computer Security Applications Conference, pp. 89-98, Dec. 1995.

[13] International Electrotechnical Commission, "Data and Communication Security - Profiles Including TCP/IP," IEC 62351-3, IEC Standard, pp. 6-9, Jan. 2007.

[14] International Electrotechnical Commission, "Data and Communication Security - Profiles Including MMS," IEC 62351-4, IEC Standard, pp. 6-15, Jan. 2007.

[15] International Electrotechnical Commission, "Data and Communication Security -Security for IEC 61850," IEC 62351-6, IEC Standard, pp. 6-12, Jan. 2007.

<著者紹介>

김 영 진 (Young Jin Kim) 학생회원
2009년 8월: 고려대학교 정보경영공학전문대학원 박사 수료
<관심분야> 정보보호 법·제도 및 정책, 정보보호제품 평가인증

이 정 현 (Jung Hyun Lee) 학생회원
2009년 12월: 고려대학교 정보경영공학전문대학원 박사 재학중
<관심분야> 정보보호법·제도 및 정책, 정보보호기술, 디지털 포렌식

임 종 인 (Jong In Lim) 종신회원
1986년 2월: 고려대학교 대학원 수학과 박사(암호학)
2000년 8월: 고려대학교 정보보호대학원/CIST 원장(센터장)
2004년 1월: 국가정보원 정보보호정책 자문위원
2005년 7월: 대통령 자문 전자정부 특별위원
2005년 12월: 국회 과기정위원회 정보통신 정책 자문위원
<관심분야> 정보보호기술, 정보보호정책, PET, 디지털 포렌식