SCADA 시스템과 정보망의 연동을 위한 위험분석 연구

김인중, 정윤정, 민병길, 박중길
국가보안기술연구소 취약성분석센터
e-mail:cipher@etri.re.kr

The Security Analysis Consideration for SCADA System with Information System

Injung Kim, YoonJung Jung, ByeongGil Min, JoonGil Park
Vulnerability Analysis Center, NSRI

요 약

최근 SCADA 시스템은 국가기반시설의 중요한 시스템으로 인식됨에 따라 사이버상의 침해사고 대응 및 복구대책이 요구되고 있다. 일반적으로 기존에는 SCADA 시스템 설계시 공정 절차에 따라 이식성, 확장성, 가용성, 유연성을 고려하였으나 최근 안전하고 신뢰성있는 시스템 운영을 위하여 보안에 많은 관심을 갖게 되었다.

본 논문에서는 SCADA 시스템에 대한 보안 설계에 필요한 위험분석 절차를 제시함으로써 사이버테러에 의하여 발생될 국가적 재난·재해를 사전에 예방하고자 한다.

1. 서론

SCADA(**S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition: 통합원격감시제어시스템)는 과거에 플랜트 및 공정제어를 위하여 정보수집, 처리, 분석 제어 및 송수신 기능들을 이용하여 원거리에 분산되어 있는 현장으로부터 데이터를 수집하고, 수집된 데이터를 바탕으로 생산·공정 등의 프로세스 상황들을 일정한 장소에서 종합적으로 감시하고 제어하기 위한 시스템으로 한정하였으나 최근 전력 송·배전, 송유관, 가스배관, 항공, 상하수도, 교통 등 국가기간시설에 이용되는 매우 중요한 시스템으로 인식되고 있다. 특히 SCADA는 업무의 효율성을 위하여 컴퓨터와 네트워크로 점차 구성[1]됨에 따라 오늘날 여러 가지 사이버공간상에 위협 및 침해요소들이 발생하기 시작하였다. 즉, 원격에서 펌프와 밸브와 같은 장치들에 대한 데이터 수집 및 제어가 가능하게 됨에 따라 SCADA망의 효율성과 편리성이 확대되는 것에 반하여 보안 위험은 계속 증가하게 되는 것이다[2].

실례로, 2003년 8월 미국 동부지역에 '소빅-F' 바이러스에 의하여 철도 신호 배차시스템이 마비되어 열차가 운행이 중단되는 사태와 2003년 1월 미국 오하이오주의 Davis-Basse 원자력발전소의 사설 컴퓨터 네트워크에 슬래머 웜이 침투하여, SCADA망이 방화벽으로 보호되어있음에도 불구하고 안전감시시스템이 5시간동안 정지된 사태 등으로 미루어 더 이상 SCADA 시스템이 안전하다고 볼 수 없는 상황에 이르게 되었다.

본 논문에서는 국내외 SCADA망에 대한 현황을 분석하고 이에 대한 보호대책 방안을 제시하여 안전하고 신뢰성있는 망운영이 가능하도록 한다.

2. 국내외 SCADA망 현황

현재 미국에서는 주요기반보호위원회(President's Critical Infrastructure Board)의 주관으로 2002년 9월에 사이버공간을 보호하기 위한 국가전략(National Strategy to Secure Cyberspace)을 발표[3]하면서 공유시스템의 보안 강화를 위한 중점 추진 과제 중 SCADA 시스템 보호체계 구축을 국가 현안으로 포함시켰으며, 국가기반시설의 핵심자산으로 수자원, 에너지, 교통, 정보통신등을 포함시켰다[4]. 이에따라 에너지성에서는 SCADA에 대한 사이버안전을 위하여 보안관리지침을 공표하였는데[5] 총 21개로 구성되어 있

으며 주요 내용은 다음과 같다.

SCADA 망의 보안을 증진시키기 위한 기술적인 행동 :

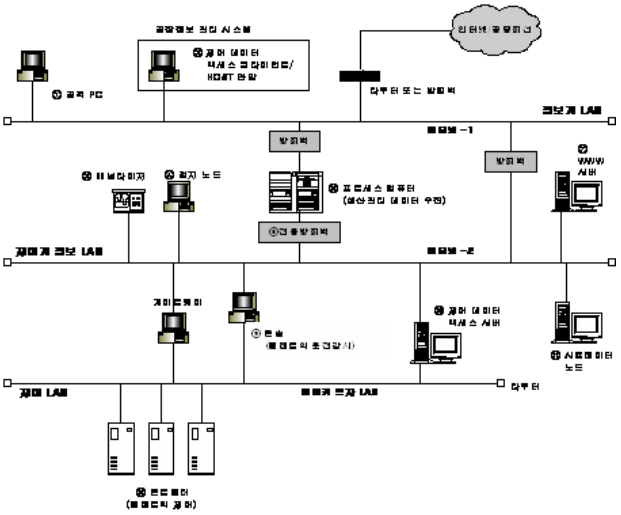
- o SCADA 망에 연결된 모든 접점에 대하여 파악하고 있어야 한다. 특히, 외부망, 인터넷망, 무선네트워크, 모뎀, 관리 업체등과의 접점으로부터 보호되어야 한다.
- o SCADA 망과 불필요한 연결은 제거한다.
- o SCADA 망과의 접점에 대하여 보안 평가를 통해 필요시 방화벽, IDS등 정보보호시스템을 도입한다.
- o 불필요한 서비스를 제거하거나 중단시켜 SCADA망을 견고하게 한다.
- o 시스템을 보호하기 위하여 특정 또는 비표준 프로토콜에 의지하지 않는다.
- o 장비 개발자 또는 시스템 공급자에 의하여 제공되는 보안관련 프로그램 및 제품을 적용한다.
- o SCADA망에서 백도어와 같은 악성 에이전트에 대항하기 위하여 강한 접근제어를 실시한다.
- o 내부와 외부에 침입탐지시스템을 도입하고 24시간 침입을 감시한다.
- o 보안과 관련된 행위를 식별하기 위하여 SCADA 장치와 망, 연동 망에 대한 기술적 감사를 수행한다.
- o SCADA 보안 평가를 위하여 SCADA 망과 연결된 모든 원격지를 점검하고 물리적 보안 조사를 실시한다.
- o 가능한 공격 시나리오를 만든 후 모의 침투를 수행하기 위하여 SCADA 공격팀을 만든다.

효과적인 사이버 보안 프로그램을 만들기 위한 관리적인 행동 :

- o 관리자, 시스템 운영자, 사용자를 위하여 보안 정책, 책임, 권한 등을 정확히 정의한다.
- o 네트워크 구조를 정리하고 민감한 정보 및 장비에 대하여 시스템을 인지한다.
- o 엄격하게, 연속적으로 위험관리 프로세스를 진행한다.
- o 종심방어의 기본 전략으로 망 보호전략을 세운다.
- o 사이버 보안 요구사항을 명확히 정의한다.
- o 효과적인 구성관리 프로세스를 수행한다.
- o 일상적인 자기 평가를 수행한다.
- o 시스템 백업과 재난 복구 계획을 수립한다.
- o 기관장 및 부서장의 보안 의식이 업무에 반영되도록 한다.
- o SCADA 시스템의 설계, 운영, 작동과 관련한 중요 정보를 다루는 요원들에게 보안교육 및 보안정보를 제공한다.

이와같이 미국에서는 SCADA에 대한 보안 및 재난재해 방지를 위하여 국가적 역량을 총 동원하고 있다.

일본의 경우 1996년부터 사이버테러 대책이라고 불리는 사회 중요 인프라 보안대책에 관하여 연구 수행하면서 대규모 플랜트의 취약성 조사, 네트워크 리스크 분석방법 개발, 플랜트 네트워크 보안대책 기술개발, Social Engineering 조사, 안정성검증 프레임워크 개발, 사이버테러 사고대응 계획 작성, 고신뢰성・고보안성 제어계에 대한 연구 등을 수행하였다[6]. 이때, 그림 1과 같은 네트워크 모델을 기본으로 테스트 시스템을 구축하여 DCS를 중심으로 한 제어계 네트워크 시스템에 있어서의 위협과 취약성 분석을 실험하였다.



[그림 1] SCADA 시스템에 대한 위험/취약성분석

시험결과 operation computer에서 사용하고 있는 OS에 따라 DCS를 세대별로 custom OS → UNIX → Windows NT로 분류했을 때 취약성은 세대가 새로울수록 증가하였으며, custom OS 베이스의 DCS라고 할지라도 제어계 네트워크 시스템에 침입한 경우, process control computer 등에 최신 OS가 존재할 경우, 그것이 공격의 대상이 되어 취약성이 노출

되며 그 취약성을 발판으로 DCS가 공격당할 가능성이 발견되었다. 특히 보안기능을 갖추지 않은 제어계 정보 LAN에 대해서는 게이트웨이 및 제어 서버에 대한 공격이 가능하였다.

국내 SCADA의 경우 모든 망은 폐쇄망 및 내부망으로 동작하고 있으므로 외부에 대한 공격으로부터 안전하다고 볼 수 있다. 하지만 최근들어 SCADA망에도 환경변화가 발생하고 있다.

- o PLC 등 제어시스템의 운영체제가 기존의 실시간 운영체제(RTOS)에서 Windows 기반 또는 Linux 기반의 제어 장치로 변화
- o 제어망에서 사용하던 Field BUS 프로토콜에서 신뢰성있는 TCP/IP 프로토콜로 변화
- o 폐쇠망으로 운영하던 제어망이 정보망과 연동하면서 인터넷과 직·간접적 연결가능성이 상존
- o 현장에서 시설의 제어하던 환경에서 중앙에서 원격관리 수행

이에 따라 보안 침해 요소 및 취약성이 증가하고 있으며 침해사고시 상상을 초월하는 피해 발생이 일어날 가능성이 상존하게 되는 것이다.

3. SCADA망 보안을 위한 위험분석

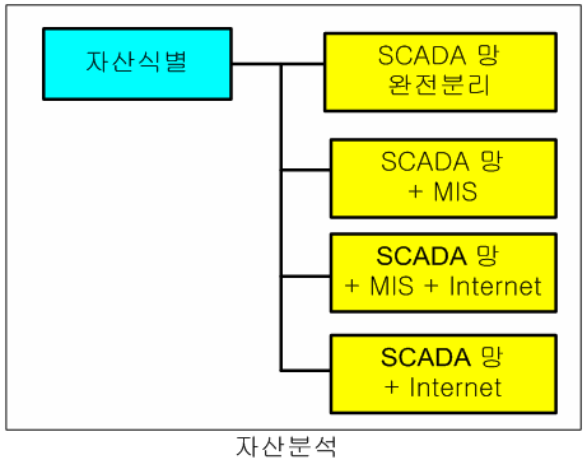
SCASA망에 대한 보안설계는 필요하나 기존의 시스템에 적용하기 위해서는 많은 어려움이 내포된다. 특히 정보보호시스템에 대한 구축을 위하여 기존 SCADA망 및 기기를 중지시킬 수 없다. 따라서, SCADA망에 대한 보안대책을 수립하기 전에 위험분석 또는 취약성분석을 실시해야 한다. 기존에 SCADA에 대한 위험 평가 기법으로 체크리스트법, 사고예상결과분석법, 위험과 운전분석(HAZOP), 이상위험도분석(FMECA), 결함수분석(FTA)등이 있으나 표 1과 같이 공정상에 고장, 사고등과 관련된 위험평가 기법이므로 사이버테러에 대처하기 위한 기법은 아니다[9]. 또한, 정보통신기반시설에 사용되는 GMITS[7], BS7799[8] 등을 사용하기 위해서는 제어망의 특성에 고려한 항목들을 추가로 개발해야 한다.

제안하는 위험분석은 먼저 SCADA망의 연결 정도에 따라 평가 수준을 정의한다. 그림 2에서와 같이 자산 분석은 4단계로 구분한다.

표1. SCADA 위험분석 기법

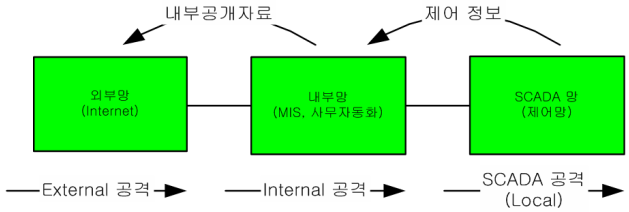
항 목	Check list	What-if	HAZOP	FMECA	FTA
사업초기	o	o			
상세설계					
위험의 일반적 이해	o	o			
위험의 철저한 분석			o	o	o
정량적 분석					o
간단히 알려진 기술	o	o	o		o
복잡하고 신기술			o	o	
제어 연동			o	o	
운전절차, 비공정조작			o	o	

먼저 SCADA망에 대한 자산식별을 통해 SCADA망이 정보망과 어느 수준으로 연결되어 있는 지를 분석한다. 완전 분리된 망인 경우 관리적인 보안대책으로도 가능하지만 내부 망과의 접점이 있는 경우에는 기술적인 보안대책이 필요하다. 특히 정보망 또는 SCADA망이 인터넷과 연결된 경우에는 접점을 통해 외부에서 공격하는 해킹까지도 고려해야 하므로 자산 분석이 정밀하게 이루어져야 한다. 다음으로 그림 3과 같이 위협 분석을 실시한다.



[그림 2] SCADA를 위한 자산분석 구분

최근에는 SCADA망에 대하여 경영측면에서 비용대 효과면에서 우수한 상용망 및 인터넷망을 선호하고 대국민 서비스를 지원하기 위하여 SCADA의 내부 공개자료 및 제어정보를 공개하고 있는 추세이다.



[그림 3] 네트워크 연결시 위협분석 구분

여기에서는 위협을 외부 공격, 내부 공격, SCADA(Local)공격으로 구분하여 정의한다. 외부와 연결되어 있는 경우 공격에 대한 보호 대책을 표 2과 같이 매트릭스 표를 만들어 운영한다.

보호대책 설계시 SCADA망에 대한 보안보다는 SCADA망과 정보망간의 연동 점에 대한 보안 설계가 가장 중요하다. 그림 4와 같이 연동 점에 SCADA망에 적합한 방화벽(Firewall), 보안 가드(Guard), 게이트키퍼(GateKeeper) 등을 설치하고, 데이터의 이상 유무를 파악하고 대응하기 위하여 침입탐지시스템(IDS), 침입방지시스템(IPS)를 도입한다.

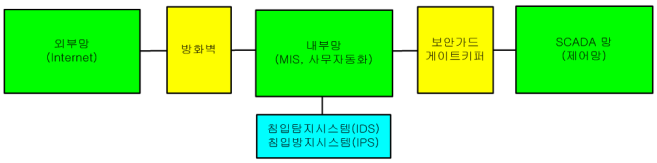


그림 4. SCADA 망에 대한 보안설계 구성도

4. 결론

현재 SCADA시스템에 대한 위험이 점차 현실화되어 가고 있다. 이에 대한 보안 솔루션을 제공하기 위해서는 다음과 같은 분야에 대하여 계속 연구가 이루어져야 한다.

- o 제어시스템을 위한 방화벽
- o 제어시스템을 위한 침입탐지시스템
- o 제어네트워크를 위한 암호화 장비
- o 운영체제를 위한 보안 RTOS
- o 보안 제어시스템 설계 기법
- o 보안관점에서 제어 프로토콜 분석
- o 보안관점에서 제어 표준 분석

사이버 공격을 통해 SCADA 시스템이 제어권을 잃게 된다면 지금까지의 재난 재해보다도 더 큰 국가적 위기가 발생할 것이므로 지금부터라도 기술적인 대비가 있어야 할 것이다.

참고문헌

[1] Yoshio, Hideki, Yoshiaki, Satoshi, Kuniaki, "Development of the Intranet-based SCADA for Power System", Power Engineering Societry Winter Meeting, 2000. IEEE.
[2] Jonathan Pollet, "Developing a Solid SCADA Security Strategy", Sensors for Industry Conference, 2002. 11.
[3] PCIPC draft paper, "National Strategy to secure Cyberspace", 2003. 2.
[4] PCIPC draft paper, "National Strategy for The Physical Protection of Critical Infrastructures and Key Assets", 2003. 2.
[5] DoE white paper, "21 Steps improve Cyber Security of SCADA Network", 2003. 4.
[6] 국가보안기술연구소 TM, "일본 중요인프라보호 활동 현황 분석", 2000. 11.
[7] ISO/IEC JTC1 TR 13335-1~5. 2000.1
[8] http://www.bsi-global.com, 1995.
[9] http://www.asp.co.kr/risk/method.php, 2003.

[표 2] 공격에 대한 보호대책 매트릭스

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