情報保護學會論文誌
第18卷 第1號, 2008. 2

산업제어시스템 정보보안 감리 프레임워크 연구

이 철 수
경원대학교 소프트웨어 대학

Information security auditing Framework in Industrial control system

ChulSoo Lee
Kyungwon university

요 약

정보기술의 발전은 비즈니스 환경의 변화는 물론 대형 산업 시설의 자동화에 많은 변화를 가져왔다. 전력, 수자원, 에너지, 교통, 통신, 등은 국가의 안보와 국민 생활의 안정 그리고 국가 경제발전의 기반을 형성하는 국가의 주요 기반시설이며 이들 모두 산업제어 시스템에 의해 통제되고 있다. 또 비즈니스 환경의 변화는 조직의 모든 시스템을 통합하고 있어 경영정보시스템과 산업제어 시스템의 통합이 이루어지고 있다. 이에 따라 산업제어 시스템의 표준화와 개방형 시스템으로 전환이 이루어지고 있어 더욱 보안의 중요성이 커지고 있다. 제어시스템 보안에 대한 연구가 기술, 관리, 환경 등 다양한 분야에서 추진되고 있다. 그럼에도 제어시스템 감사에 대한 연구는 아직 미약하다.

정부는 최근 정부 및 주요 공공 시스템에 대한 정보시스템 감리를 의무화 하여 안정성, 효율성, 효과성을 평가하고 있다. 또 주요정보통신기반시설에 대해서는 취약점 분석을 하고 그 개선 작업을 하도록 의무화하고 있다. 그럼에도 제어시스템에 대한 감리를 하지 않고 있고 제어시스템에 대한 보안 아키텍처나 감리 프레임워크도 준비되어 있지 않다. 본 연구는 제어시스템 감리를 위한 정보보안 아키텍처와 정보보안 감리 프레임워크를 제시하여 감리의 기반을 마련하였다.

ABSTRACT

Information technology have led to change the automation of large industrial control system as well as business system and environments. Industrial control system(ICS) is vital components of most nation's critical infrastructures such as electricity, natural gas, water, waste treatment, transportation and communication that are based of national security, safety of citizen and development of national economy. According to the change of business environment, organizational management pushed integration all of the system include MIS and ICS. This situation led to use standard information technologies for ICS, this transition has been to expose ICS to the same vulnerabilities and threats that plague business system. Recently government obliged owners of the public information system to audit for safety, efficiency and effectiveness, and also obliged the owners of national infrastructure to improve their system security as a result of vulnerability analysis. But there doesn't prepare a security architecture and information security auditing framework of ICS for auditing. In this paper, I suggested the security architecture and information security auditing framework for ICS in order to prepare the base of industrial system security auditing.

Keywords : industrial control system(ICS), SCADA, Security architecture, auditing Framework

접수일: 2007년 9월 21일; 채택일: 2007년 11월 12일
† 주저자, csl100@kyungwon.ac.kr

Ⅰ. 서 론

산업제어시스템(ICS: Industrial control system)이란 광범위 한 지역에 분산되어 설치된 센서, 제어기, 로봇 등을 유무선으로 연결하여 자동제어 하는 발전된 공장 자동화 기술을 의미하며 DCS(Distributed control system), PCS(process control system), SCADA(supervisory control and data acquisition) 시스템 등으로 부르기도 한다. 이 논문에서는 주로 SCADA 시스템으로 부르기로 한다.

이들 시스템에 대한 사이버 보안의 중요도를 인식하기 시작한 것은 미국의 9·11 테러 이후 국가주요 기반시설들이 모두 이들 제어 시스템에 의해서 운영되고 있어 사이버 공격을 받거나 침해를 당할 경우 국가안보와 국가경제, 국민생활의 안정에 막대한 피해를 주게 된다는 것을 인식한 이후이다. 미국을 비롯한 선진국들은 국가 주요기반시설을 보호하기 위한 노력의 일환으로 SCADA 시스템에 대한 보안 대책을 연구하고 있다. 우리나라도 2000년에 "정보통신기반보호법"을 제정하여 국가주요정보통신시설을 지정하고 매년 취약점을 분석하고 개선대책을 수립하여 시행하도록 하고 있다.

정보기술의 발전과 경영 환경의 변화는 조직의 정보시스템의 통합을 추진하고 인터넷을 통해 고객 서비스를 강화하게 되었다. 이로 인해 지금까지 독립된 영역으로 운영되던 SCADA 시스템이 일반 비즈니스 시스템과 연동되고 통합되는 추세에 있다. SCADA 시스템은 지금까지 특정한 업체에서 제공하는 하드웨어, OS, 통신 프로토콜을 중심으로 구축 운영하여 왔다. 그러나 연동과 상호운영은 개방형 시스템으로 전환을 가져왔고 일반 비즈니스 시스템에서 사용하는 하드웨어, OS, DB, 통신 프로토콜로의 표준화를 추진하고 있다. 이러한 사항은 지금까지 노출되지 않았던 SCADA 시스템의 취약점을 노출하는 결과를 가져오고 있고 일반 비즈니스 시스템과의 연결은 알려진 취약점을 SCADA 시스템에 부가하는 결과를 가져오게 되었다.

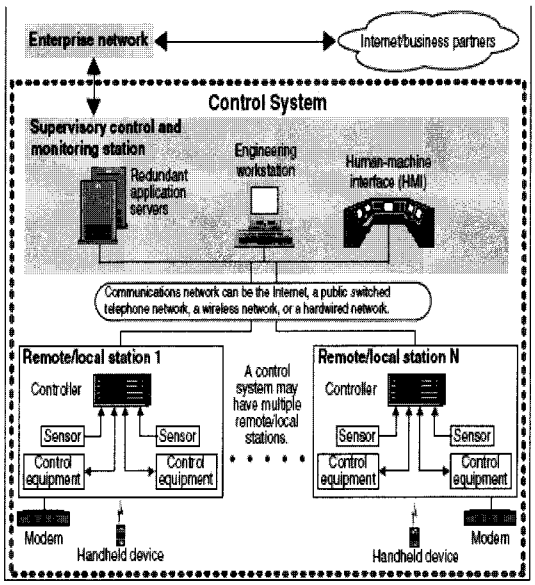
SCADA 시스템에 대한 환경변화는 보안 기능 강화를 위한 연구를 촉진하게 되었다. 일반 비즈니스시스템과 SCADA 시스템의 특성의 차이에서 발생하는 구성과 운영에 관한 위험분석, 보안통제 요구분석, 보안 대책이나 도구 등에 대한 기술개발과 보안 시스템 구현이나 운영에 대한 감사 방법의 필요성 등이 추진되고 있는 중요한 연구 분야이다.

본 연구에서는 SCADA 시스템에 대한 특징과 기능을 살펴보고 SCADA 시스템에 적합한 보안 아키텍처를 제시하고 SCADA 보안 시스템을 구축하거나 구축되어 운영되는 SCADA 보안시스템에 대한 감사를 하기 위한 프레임워크를 제시하여 이를 정보통신 기반시설의 보안 감사에 적용하는 근간을 마련하고 이를 시행하기 위해 필요한 향후 연구 방안을 제시하였다.

Ⅱ. SCADA 시스템 보안 관련 연구

SCADA 시스템의 일반적인 구성은 [그림 1]에서와 같이 비즈니스 영역, 제어 영역, 필드영역으로 구분되고 각 영역은 내부의 장비들을 연결하기 위한 내부 네트워크로서 전사적 네트워크, 제어 네트워크, 필드 네트워크가 있고 각 영역의 장비를 연결하고 있다. 또 영역과 영역의 연결을 위한 네트워크로서 PSTN, 인터넷, 무선 등으로 구성되어 있다.

비즈니스 영역과 전사적 네트워크는 개방형 IT 기술을 적용하고 있으나 제어영역은 일부만 개방형 IT 기술을 적용하고 그 외의 부분은 생산업체 고유의 하드웨어, OS와 통신 프로토콜을 사용하고 있다. 통신 프로토콜은 100여 가지로 매우 다양하며 기기나 기능의 호환성이 없어 주 생산업체들을 중심으로 표준화를 추진하고 있다.



[그림 1]. SCADA 시스템 일반구성

〔표 1〕. IT 시스템과 SCADA 시스템 차이

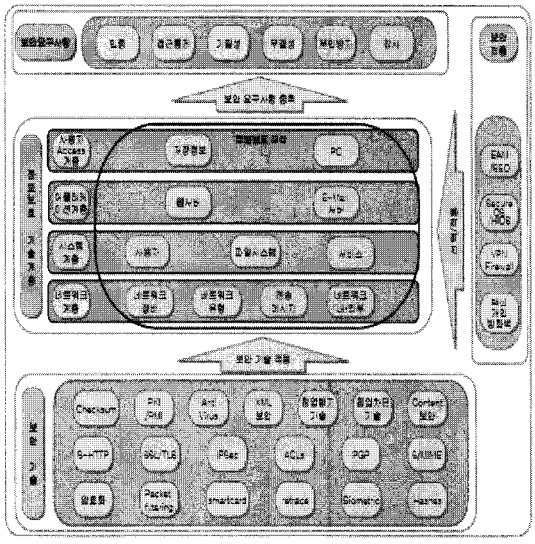
분류	IT 시스템	SCADA 시스템
성능 요구	**Non-real-time Response must be consistent High delay** 허용	**Real-time Response is time-critical High delay** 불허용
가용성 요구	rebooting 허용, 가용성의 결핍을 허용	rebooting 불허용, 계획된 가동정지, 높은 가용성 요구
위험관리 요구	자료의 비밀성과 무결성 순간적인 가동중지 허용(감내 시스템 불급) 위험영향은 비즈니스 운영의 지연	프로세스 가용성 순간적인 가동 중지 불허(감내 시스템 중요) 위험영향은 인명, 시설, 생산의 손실.
보안핵심	IT 자산 및 정보 중앙서버 보호.	필드 장치에 대한 보호
기존도구	대표적인 IT 시스템을 대상으로 설계	SCADA운영을 보증하도록 설계되지 않음
시간 의존 상호작용	**Less critical emergency interaction** 강력한 접근 통제 제한이 해당 등급에 적용	**Response to human and other emergency interact** 엄격한 접근 통제되지만 사람과 기계의 상호작용 방해 없음
시스템 운영	개방형 운영체제 사용하도록 설계 갱신이 자동화된 도구로 즉시 처리	개별 제작된 운영체제를 사용 소프트웨어변경은 하드웨어와 다른 소프트웨어, 제어 알고리즘변경 수반
자원 제한	시스템이 보안 솔루션 등 제 3자 응용 사용이 가능하게 충분한 자원을 사용할 수 있게 규격화	시스템이 보안기술 추가를 지원하기 위해 최소의 기억장치와 컴퓨팅 능력만 허용, 본래 기능에 한정
통신	표준 통신 프로토콜 지역적인 무선 능력을 가진 유선 네트워크가 기본 대표적인 IT 네트워킹을 시행	많은 생산자 통신 프로토콜이 존재 전용선, 위성, 라디오를 포함한 통신미디어사용 네트워크가 복잡하고 제어 전문 엔지니어가 필요
변경관리	소프트웨어 변경이 보안정책과 절차의 실현에 맞게 바로 적용 가능 절차가 자동화	소프트웨어 변경은 무결성 유지를 위해 시스템 전반의 우선 시험 후 점진적 전개 필수 시험을 위한 운영정지는 일별/주별로 계획 후 실시
관리지원	다양한 지원형태가 허용된다.	서비스 지원이 단일 생산자에 의해서만 가능
요소 생명주기	주문에 대한 생명주기가 3-5년	주문에 대한 생명주기가 15-20년
요소 접근	요소들이 지역에 있고 접근용이	요소들이 독립되어 원격지에 있어 접근을 위해 광범위한 물리적 노력이 요구됨

SCADA 시스템과 관련된 보안연구는 비즈니스 IT 시스템과의 차이에서부터 출발하고 있다. 특성의 차이를 비교한 것이 [표 1]이다.

SCADA 시스템에 관한 보안관련 연구는 세 방향으로 나누어서 추진되고 있다. 가장 활발한 연구가 진행되고 있는 분야로서 SCADA 시스템에 대한 보안 요구를 설정하는 것이다.

시스템의 특성 차이로 인해서 SCADA 시스템에 기존의 보안 솔루션이나 도구들의 적용 방법에 대한 연구와 SCADA 시스템 환경에서의 통합된 보안 기술 적용 방법 등에 관한 연구들이 진행되고 있다. 나아가서 산업제어 시스템 일반에 적용되어야 할 보안 프로파일에 관한 연구와 보안 지침이 연구 되고 있다. 이 보안 지침은 개별 보안 제품에 관한 사항이 아니고 SCADA 시스템에 적용되어야 할 일반적인 보안요구로서 계속 발전되어야 할 내용들이다.

두 번째는 정보보안 아키텍처에 관한 연구이다. 보안은 전사적 정보기술 아키텍처에 포함된 하나의 분야로 고려되었다. 그러나 최근에 보안의 중요성이 인식되면서 IT정보보안 아키텍처로 독립된 연구가 진행되고 있다. 미 국방성은 분산정보시스템에 대한 추상적인 구조적 관점을 사용자 영역과 네트워크 영역으로 나누고 각 영역에서 제공되어야 할 보안 서비스와 보안 통제에 관한 관계를 도식하여 가장 일반적인 보안 아키텍처를 제시하고 있다. 우리나라에서는 정부와 공공부문의 정보시스템을 대상으로 [그림 2]에서와 같이 정보보안 기술



〔그림 2〕. 정보보안 기술 아키텍처

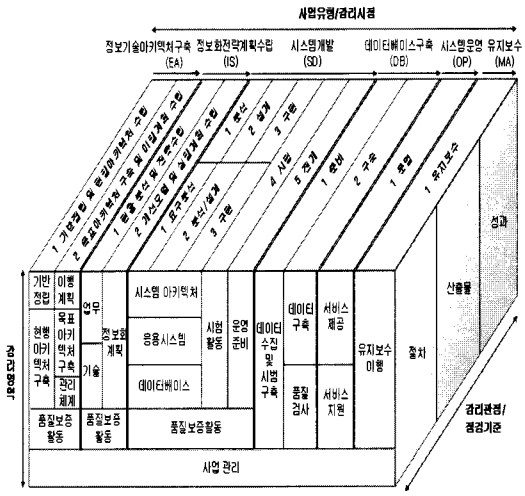
아키텍처를 제시하고 있다. 이 아키텍처는 보안 요구사항과 보안 기술계층 그리고 해당되는 보안 기술과 보안제품에 관한 관계를 나타내고 있어 보안 기술에 관한 사항만 제시하여 일반적인 적용에 한계를 나타내고 있다.

최근의 보안 아키텍처는 조지아택 대학에서 적용하고 있는 것과 같이 아키텍처 자체를 그대로 web에 적용하여 대화형으로 사용자들에게 필요한 정보와 활동을 수행할 수 있도록 구성하고 있다. 특히 보안에 대한 활동주기를 중심으로 일상적인 억제 활동, 탐지활동, 예방 및 대응 활동으로 나누어서 사용자가 직접 보안 활동에 참여하도록 구성하고 있다. SCADA 시스템에 관한 정보보안 아키텍처는 아직 마련되지 못하고 있어 본 연구에서 이를 제시하였다.

세 번째 연구 분야가 정보보안 시스템의 감사에 관한 연구이다. 정보보안에 대한 감사는 정보시스템 감사의 일환으로 이루어져 왔고 정보보안 시스템 자체에 대한 감사는 아직 초기 단계에 있다. 단지 보안 제품에 대한 평가제도로서 ITSEC, TESEC, CC 등이 국제적으로 시행되고 각 제품에 대한 프로파일들이 연구 개발 되고 있어 제품으로서의 정보보안 요구와 필요한 통제요소들의 만족여부를 검증하고 있다. 또 조직의 ISO17799나 ISO27001에 의한 정보관리체계의 시행 등으로 보안을 고려하여 왔다. 그러나 사이버 공간에 대한 위협이 커지고 그들에 대한 정보보안 시스템이 구체적으로 요구되어 지고 미국의 경우 Sarbanes-Oxley Act가 제정되어 조직의 내부통제에 대한 검증을 공식적으로 요구하게 되어 정보보안 시스템에 대한 감사가 조직 경영에 필수적인 사항이 되었다.

미국은 민간분야에서는 ISACA가 CobIT를 기반으로 정보시스템 감사를 추진하여 왔고 공공분문은 NIST가 중심이 되어 정부와 공공기관의 정보시스템에 대한 보안통제와 관련하여 800 series를 개발하여 보급하고 있다. 이러한 것들은 정부기관의 보안에 직접 적용되어야 할 기준이다. OMB의 Circular A-130, A-123의 안전성 요구사항은 이러한 기준의 준수여부를 감사하고 이를 의회와 대통령에게 보고하도록 규정하고 있다. 또 국가 주요 기반시설에 대한 정보시스템 보안감사의 필요성을 제기하고 관련 제도와 기법 등에 관한 연구를 하고 있다.

국내에서는 정보시스템 감리에 관해 정보시스템 감리기준이 제정되어 감리를 수행하고 있다. 정보시스템의 다양성과 전략계획 수립, 개발, 운영, 유지관리 등 사업의 유형에 따른 감리영역과 감리 점검 기준 등을 연구하여 정보시스템 감리 프레임워크를 [그림 3]과 같이 제시하고 있다.



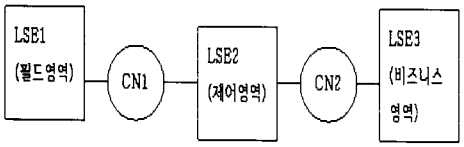
〔그림 3〕. 정보시스템 감리 프레임워크

보안 분야는 별도의 사업 영역으로 구분하지 않고 있으며 감리점검 기준의 산출물 영역에 보안성, 무결성, 안정성에 관한 점검 항목이 포함되어 있다. 그러나 보안이 모든 정보시스템 환경의 기본 요구가 되고 있고 정보인프라가 됨으로써 본 연구에서 정보시스템 보안감리 프레임 워크를 제시하여 보안 감리를 위한 기반이 되게 하였다.

Ⅲ. SCADA 시스템 정보보안 아키텍처

정보보안 아키텍처의 목표는 첫째, 조직의 경영전략 및 사업수행 목표를 달성하기 위한 정보보안 목표와 이를 달성하기 위한 정보보안 요구와 서비스를 도출하고, 둘째, 조직의 정보보안 목표를 제시하고 정보보안에 대한 공통 언어를 설정하고 일관성을 유지하고 중복을 배제하여 정보보안을 구현하며, 셋째, 관리적, 물리적, 기술적 대책을 포괄하는 전반적 관점에서 정보보안을 구현하고, 넷째 정보보안 아키텍처의 개발과 운영을 통해 조직의 정보보안 수준을 높이고 정보보안 문화를 정착시키는데 있다.

SCADA 시스템의 보안 아키텍처도 목표는 동일하다. 단지 비즈니스 시스템과 구성, 기능, 시스템의 기술사양, 시스템의 특성 등의 차이로 인한 보안 요구와 서비스가 다를 수 있다. 본 논문에서 대상으로 하는



〔그림 4〕. SCADA 시스템 보안 범위

SCADA 시스템은 분산구조를 가지고 전사적인 비즈니스 시스템과 연동이 되면서 전사적인 플랜트 운영 및 관리를 할 수 있는 시스템으로 정의 한다. 보안 아키텍처를 구성하기 위해 이를 기능과 특성의 차이가 있는 영역별로 [그림 4]와 같이 구분하고 각각의 구성과 특성을 아래와 같이 정의한다.

- LSE1(필드영역): 지역 통신네트워크와 장비들로 구성된다. 지역 통신 네트워크는 산업용 LAN이나 무선 혹은 필드버스 등으로 연결된다. 구성될 수 있는 장비로서는 RTU, PLC와 같은 자체 처리능력을 가진 장비와 센서, 제어기와 같은 단순 기능만 가진 것도 있다. 대부분이 저장 용량이 적고 처리 능력이 떨어져 암호화, 다수 계정의 확보 등이 불가능하고 최소한의 자료만 저장할 수 있다. 각각의 장치들은 고장이나 계획되지 않은 가동 중단이 되어서는 안 된다.
- LSE2(제어 영역): 일반적으로 산업용 LAN 혹은 필드버스 등으로 연결된다. PLC, RTU, HMI, 응용서버, historian, 제어서버 등으로 구성된다. PLC, RTU 등은 제한된 저장 용량으로 암호화, 다수계정 등을 적용하기 어렵다. 그 외의 시스템은 비즈니스 IT 기술적용이 가능하며 특히 제어서버는 가용성이 중요하여 고장이나 계획되지 않은 가동 중단이 돼서는 안 된다.
- LSE3(비즈니스 영역): LAN으로 연결된다. 구성될 수 있는 장비로서는 workstation, PC, 응용서버, DB서버, 메일서버 등 일반적인 비즈니스 시스템들로 구성되며, 외부와의 접속을 위해 인터넷 등에 연결된다. 대부분이 개방형 표준 시스템으로 구성되며, 일반적인 보안 서비스 구현에 제한사항이 없다.
- CN1:제어 영역과 필드 영역을 연결하는 통신 네트워크로서 PABX, router, 무선 인터페이스 장치, 등으로 구성된다. 회선의 구성은 WAN, 전용선, 전화선 등으로 구성되며 데이터와 아날로그 자료의 송수신이 요구될 수 있다. 일반 비즈니스 통신 프로토콜을 적용하기 어렵다.
- CN2: 제어 영역과 비즈니스 영역을 연결하는 통신 네트워크로서 router, 교환기 등으로 연결된다. 일반 비즈니스 프로토콜을 적용할 수 있다.

이상과 같이 정의한 각 영역이 SCADA 시스템의 보안 대상이며 이들은 그 구성과 특성이 다르기 때문에

〔표 2〕. 보안서비스/보안통제

서비스/통제		FD	CD	BD	CN1	CN2	비고
지원	식별/명칭	적용	적용	적용	적용	적용	객체/주체/자원
	암호키 관리	비적용	부분적용	적용	부분적용	적용	속도/저장능력우선(제어장비)
	보안관리	필드환경에 따라 적용	적용	적용	적용	적용	정책과 계획 연속계획 인적/물리적 보안
	시스템 보호	모듈화 권한 최소화	적용	적용	권한 최소화	적용	악성코드/패치 변경/구성관리
예방	보호된 통신	가용성 최우선	가용성 최우선	적용	적용	적용	암호통신/VPN VLAN/내장 web
	인증	계정 제한	계정 제한	적용	부분적용	적용	모든 주체/네트워크/프로세스
	권한 부여	기준값 변경	원격 접근	적용	적용	적용	주체/객체/자원
	접근 통제	MAC	MAC/RBAC	RBAC			모든 객체/자원
	부인 방지	비적용	적용	적용			
	프라이버시 처리	비적용	적용	적용	부분적용	적용	
	모니터링	적용	적용	적용	적용	적용	실시간/경보
복구	감사	log안함	제어자료 log	모든 log	방화벽	방화벽	감사 목적 추가 log
	탐지/봉쇄	즉시 교체	장비 없음	적용	장비 없음	적용	LDS/IPS/ESM
	완전성 증명	비적용	부분적용	적용	부분적용	적용	포랜식/통제도구
	복구	즉시 교체	복구/교체	복구	복구/교체	복구	침해이전으로 복구

보안 요구가 다르며 그에 따라 적용되는 보안 기술과 관리 방법도 달라질 수밖에 없다. 각각의 영역에서 요구되는 보안 서비스/보안 통제를 도식하면 [표 2]와 같다.

이러한 보안 요구와 통제를 대상별로 구분하여 적용할 수 있도록 보안아키텍처를 구성하되 반드시 고려되어야 할 상호관계를 가진 보안 요소들로서 아래의 세 영역으로 나누어 상호관계를 표현하였다.

3.1. 보안 서비스와 통제요구

보안서비스 모델은 달성하고자 하는 보안 목표를 이루기 위해 요구되는 보안통제를 기능요소로 나누고 그들의 상호관계를 나타낸 것으로 지원, 예방, 복구로 구분하고 각각에 대한 통제는 가용적일 수 있으나 여기서는 아래와 같이 나누었다.

- 지원은 대부분의 정보기술 보안에 기초가 되는 포괄적인 서비스로서 (1)식별과 명칭 (Identification and naming): 주체와 객체 모두에 대한 식별이 필요하다. 사용자, 프로세스, 정보자원에 대한 유일한 명칭과 그의 식별, (2)암호키 관리: 암호 기능이 여러 서비스에 구현될 때 이에 대한 안전한 관리는 필수적인 사항, (3)보안관리: 시스템에 대한 보안 기능이 특정하게 구현되고 운영상에 변경이 일어날 경우 보안관리 기능이 필요, (4)시스템보호: 시스템의 설계와 구현이 품질과 관련된 것으로 예를 들면 권한의 최소화, 프로세스 분리, 모듈화, 계층화, 객체의 재사용 등의 기능 적용
- 예방은 공격으로부터 보안 침해를 예방하기 위한 서비스로 (1)보호된 통신: 분산 환경에서 신뢰할 수 있는 통신 능력이 필요하고 이는 전송 간에 비밀성, 무결성, 가용성이 보장된 것을 의미한다. 이를 보장하기 위한 보안 기능의 구현이 필요, (2)인증: 주체의 식별과 식별된 주체의 신분에 대한 증명, (3)권한부여: 주어진 시스템에서 허가된 행동의 부여와 관리, (4)접근통제: 주체에 대한 특별할 프로세스에 접근을 허가하기 인한 인증 절차이다. 이는 접근통제 의사결정의 진위여부는 물론 보안수준 결정의 적정여부도 함께 지켜져야 한다. (5)부인방지: 시스템 책임은 보낸 사람이 보낸 정보를 부인할 수 없고 받은 사람이 받은 정보를 부인할 수 없도록 하는 능력이 중요하다. (6)처리 프라이버시: 정부나 민간 모두에서 시스템에서 사용되는 개인의 프라이버시에 대한 관리가 필요하다. 개인에 의해서 시스템에서 수행되는 처리에 대해 프라이버시의 손실 방지는 중요하다.
- 탐지와 복구는 예방에 대한 도구가 완전할 수 없기 때문에 보안 침입을 탐지하고 그들의 영향을 줄이는 활동으로 (1)감사: 보안 감사는 보안침해의 사후 탐지와 복구에 핵심요소, (2)침입탐지와 봉쇄: 안전하지 못한 사항의 탐지는 초기 대응의 가장 효과적인 방법이며, 탐지된 공격의 억제나 봉쇄는 기본적인 보안 기능. (3)완전성의 증명: 보안 목표의 손상여부에 대한 증명은 목표를 보호하기 위한 통제 요구의 손상여부 판단이 필요하고 이는 해당 통제를 시행하기 위한 도구나 방법의 작동여부와 관련이 있다. 이런 일련의 고장들에 대한 설정과 구현이 필요하고 , 포괄적인 포랜식 도구나 기능이 필요, (4)사고 이전의 상태로의 복구: 침해사고가 발생 하였을 때, 시스템은 사고 이전의 안전한 상태로 반드시 복구되어야 한다.

3.2. 보안대상과 적용기술

보안의 대상이 되는 시스템과 네트워크를 나타내는 것으로 여기서는 비즈니스 영역(LSE3), 제어영역(LSE2), 필드영역 (LSE1)과 그들을 연결하는 두 계층의 네트워크를 포함한다. 또 대상이 되는 보안 기술은 [표 2] 보안대상이나 네트워크의 특성과 보안 통제 요구에 따라서 서로 다르게 적용되어야 한다. 논문에 제시한 아키텍처에서는 IT 보안기술 항목을 제시하였지만 그대로 필드영역이나 제어영역에 적용될 수는 없다. 또 네트워크 보안 기술도 CN1과 CN2에서 동일하게 적용될 수 없다. CN1의 경우 자체 지역네트워크도 산업용 LAN을 사용하고 있어, 통신 프로토콜도 다르며, 운영체제 등의 기술 사양이 다르고, 무선망을 이용한 필드장비와의 직접적인 연결을 하고 있어 이를 고려한 통신 보안 기술이 적용되어야 한다.

3.3. 보안환경 및 관리

SCADA 시스템은 광범위한 지역에 분산되어 설치되어 운영되고 있는 것이 일반적이다. 따라서 하나의 시스템으로 연결되어 구축 운영되고 있다고 해도 각 영역, 특히 필드 장비들의 운영환경은 다를 수가 있고 적용된

기술도 다를 수 있다. 따라서 이에 적정한 보안 관리와 운영이 필요하다. 보안 관리는 일반적인 보안관리 프로세스인 체계 및 계획의 수립, 구현, 운영 및 점검, 보안 평가의 단계를 거치면서 수행된다. 각 단계에서 필요한 활동들이 모두 포함되어야 하며 준수되어야할 법규나 규정, 지침 표준들이 포함되어야 한다.

이상의 사항을 상호 유기적으로 영역별 특성에 따라 적용할 수 있도록 SCADA 시스템 정보보안 아키텍처를 도식한 것이 [그림 5]이다.

Ⅳ. SCADA 시스템 보안 감리 프레임 워크

SCADA 시스템보안 감리 프레임워크를 구성하기 위해서 먼저 일반 정보시스템 보안 감리 프레임워크를 설정하여야 한다. 실제로 SCADA 보안 감리와 일반 정보시스템 보안 감리의 프레임워크는 동일 할 것으로 판단된다. 단지 시스템 구성과 가능, 통신 프로토콜 등이 다르기 때문에 발생하는 위협이 다르고 이에 대응하기 위한 보안 대응 방법이 다를 수 있다. 프레임 워크를 위해 고려하여야 할 분야가 1)사업의 유형, 2) 감리 영역, 3) 감리관점/감리기준이다.

보안 사업의 유형을 규정하기 위해 먼저 사업을 행하고 있는 현상을 파악해 보자. 정보보안 제품은 응용 시스템 운영 환경이 되는 기본 인프라에 맞추어 보안 통제 요구를 만족시키는 제품을 전문업체가 개발한다. 이러한 제품의 개발이 적합한 보안기능을 수행하며 적합한 개발 원칙에 따른 개발 여부에 대해서는 보안제품 평가제도가 실행되고 있다. 그러므로 정보보안 시스템 구현은 평가받은 제품을 선정하여 해당 보안기능을 정보시스템에 적용하는 결과가 된다. 이때 선정된 보안제품의 기본 인프라 및 프로토콜이 정보시스템 환경과 다를 경우 이를 수정 보완하여 맞추는 작업이 필요하다. 이러한 과정은 보안시스템 구현 생명주기 동안에 수행되는 과정이다. 따라서 보안 감리의 대상으로 보안제품을 개발하는 과정을 포함시키는 것은 합당하지 않다.

정보시스템 정보보안 구축 사업은 기존 시스템이나 신규 시스템을 구축 운영하고 있는 조직에서 정보시스템의 보안을 구현하기 위한 방법으로 조직의 정보시스템에 대한 위험 및 취약점 분석을 하여 이를 기초로 위험과 취약점을 줄이기 위한 방법으로 보안도구를 선정

[그림 5]. SCADA 시스템 정보보안 아키텍처

하고 이의 설치는 보안 제품을 판매한 보안업체가 주도하여 온 것이 일반적인 방법이었다. 그러나 이런 방법의 보안시스템 구성은 일관된 보안 정책의 부재와 위험수준의 수용 범위 등에 대한 원칙이 없고 조직의 비즈니스 정책과 목표의 달성에 대한 보안 요구에도 부합하지 못하여 정보시스템 보안에 크게 기여하지 못하고 있는 것이 현재의 실정이다. 따라서 정보시스템 보안에 관련된 사업을 전사적 보안정책 및 보안 계획 수립을 별도의 사업으로 시행하고 이러한 계획에 근거하여 정보시스템 보안대책을 구현하는 사업을 수행하여 구현된 보안 시스템을 운영/관리하는 것을 구분하여 별도의 사업으로 추진하는 것이 적정할 것으로 판단한다. SCADA 시스템도 동일한 사업 영역으로 구분하는 것이 적정하다고 판단하였다.

1)전사적 보안 정책 및 보안계획 수립 사업: 조직 전체의 정보보안 정책 및 계획을 수립하여 정보보안 시스템을 구현하기 위한 사업으로 전반적인 과정은 ISO/IEC 17799 혹은 27001의 정보보안 관리체계에서 요구하는 11개의 핵심통제 요구에 대한 점검과 그에 해당하는 대응 방안을 정책과 계획에 수용하는 것으로 정책 수립을 위한 업무 현황분석, 위험분석, 기술과 제도분석 단계와 그를 바탕으로 정보보안 계획을 수립하는 단계로 각 단계를 감리 영역으로 설정하였다.

2) 정보보안 시스템 구현 사업: 정보보안 전문업체가 조직의 위협을 제거하기 위한 통제 요구에 의해서 보안 제품이나 장비 혹은 서비스를 조직의 정보시스템에 설치하는 사업으로서 체계 및 계획의 수립, 구현, 운영과 점검, 평가의 단계로 구분하여 감리 영역을 설정하였다.

3) 정보보안 시스템 운영 사업: 정보보안 시스템 운영은 조직의 시스템운영과 함께 이루어진다. 따라서 정보보안에 대한 운영 개념을 정립하여야 한다. 여기서는 보안 시스템 운영을 조직의 정보시스템 운영을 위해 제공되는 보안 서비스의 제공과 지원, 업무 연속성의 확립, 시스템 모니터링과 감사, 사고대응과 복구의 영역으로 구분하였고 감리도 해당 영역을 대상으로 하도록 설정하였다.

대상이 되는 감리 영역에 대해서 보안 감리의 관점과 보안 감리기준을 정해야 한다. 정보시스템 감리에서의 감리관점은 사업을 추진하기 위한 절차(process)가 적정한지를 살펴보고 적정한 절차를 거쳐서 추진할 때에 생성된 산출물(product)이 목적한 대로 생성되었는지를 확인하며 최종 결과로서 성과(performance)를 측정하고 있다. 정보보안 감리의 관점도 이와 동일하여야 할 것으로 판단하였다. 그러나 산출물에 있어서는 보안 시스템 구축 사업과 정보시스템 구축 사업의 목적이 상이하기 때문에 이를 고려하여 산출물의 세부 항목을 설정하였다. 상세한 내용을 살펴보면 아래와 같다.

- 절차(process): 사업에 대한 각종 관리 활동 및 구축/운영 절차의 수립과 절차의 준수여부에 대한 적정성을 검토한다.
  - 계획의 적정성(plan reasonability): 사업수행 계획, 인력 운영계획 등 각종 계획 수립 적정성
  - 절차 적정성(process reasonability): 개발/운영/유지보수 절차 수립의 적정성, 위험/일정/품질/형상/인력/변경관리 절차 등의 수립 적정성
  - 준수성(compliance): 각종 계획의 준수 적정성, 위험/일정/품질/형상/인력/변경관리 등 절차 및 활동준수 적정성
- 성과(performance): 궁극적인 사업의 성과 목표 및 기대효과의 달성 가능성 및 달성 여부에 대한 검토
  - 실현성(realizability): 구체성, 실현가능성, 투자대비 효과성, 성과 목표 달성, 시스템 사용 가능성 등에 대한 검토
  - 충족성(sufficiency): 임무/기술적 요건 만족, 성과 목표 달성, 과업범위 충분성 등에 대한 검토
- 산출물(product): 적정한 구축/운영 절차를 통하여 생산된 개발 산출물(문서, 기능 등)과 정보보안 시스템, 보안 서비스 및 지원 방법 등이 목표로 하는 보안 서비스나 보안 통제의 충족여부를 검토
  - 편의성(usability): 사용의 편의성, 운영 편의성, 학습성에 대한 검토
  - 효율성(efficiency): 정보지원(인력, 서버 등)활용의 효율성, 업무 효율성, 응답시간 신속성, 시스템 확장성, 기술발전 부합성에 대한 검토
  - 준거성(compliance): 산출물 관련 기준/절차/표준/법/제도의 준수여부 검토
  - 일관성(consistency): 분석성, 변경성, 현행화, 추적성, 유지보수성 등에 대한 검토
  - 가용성(availability): 효과적인 운영 유지를 위해 시스템의 가용에 직접적으로 영향을 주는 서비스이다. 효과적인 유지는 허가되지 않은 변경의 방지, 허가된 접근에 의해서 달성되며, 임무의 효과적인 달성은 침입탐지, 완전성, 손실의 방지, 침해 발생 시 신속한 복구 등의 상호 작용에 의해서 달성된다. 따라서 관련 요소들과의 관계가 정립되어 있는 지를 검토
  - 무결성(integrity): 무결성 서비스를 위해서는 가용성 서비스에서 요구된 인증과 접근 통제 등의 통제요구가 만족되어야 한다. 무결성의 유지나 복구는 가용성 유지가 근본이기 때문이다. 따라서 가용성에 관련된 통제요구의 관계정립과 기능의 수행 여부를 검토
  - 비밀성(confidentiality): 비밀성은 한번 상실되면 복구될 수 없다. 통신상의 노출방지, 허가된 접근, 프라이버시 보호 등의 통제 요구가 만족되어야 하며 그들의 상호관계가 정립되었는지를 검토

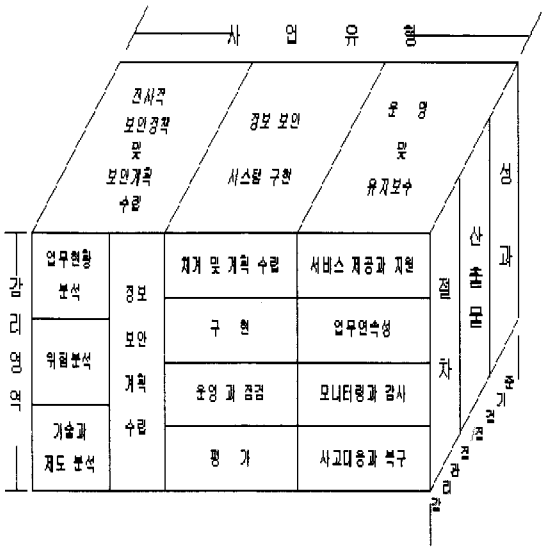
- 책임성(accountability): 사용자 활동에 대한 책임성 유지는 감사와 부인방지 서비스에 의해서 수용된다. 접근 통제도 사용자 활동의 기록에 중요한 역할을 한다. 그들의 상호관계 정립여부와 기능을 검토
- 보증(assurance): 보증은 보안 목표가 바르게 만족하게 달성되었는지에 대한 신임의 기본이다. 따라서 보증은 예방을 위한 접근 통제와 인증, 지원을 위한 시스템 보호(최소 권한 부여, 객체의 재활용, 프로세스 분리 등)와 보안 관리, 복구를 위한 통제요구들과 그들의 관계 정립여부와 그들을 어떻게 마련하였는지 여부를 검토하는 것이 중요하다.

특히 SCADA 시스템과 같은 분산 시스템에서는 보안 서비스가 논리적 물리적으로 만족되어야 하고 시설이 설치되어 있는 영역(domain)의 설정과 그들을 연결하고 있는 네트워크에 대한 보안 서비스가 보증되어야 한다. 또한 분산시스템에서는 운영체제 보안, 다계층 분산 보안서비스, 사용자 응용과 클라이언트-서버보안 서비스 등을 만족 시켜야 한다. 시스템 보증은 복잡한 기술 솔루션의 적용을 피하고, 신뢰도가 높은 요소들을 사용하며, 사고의 확장을 제한 할 수 있는 구조를 가지며, 운영 환경에서의 통합기술과 비기술적 대응 방안의 장점을 구현함으로서 신뢰도를 높일 수 있다. 따라서 기본적인 통제요구 이외에도 그러한 요소들을 구현하여 기능이 수행되는 지를 검토하여야 한다.

설명한 감리 사업의 유형과 감리 영역 그리고 감리관점/감리기준을 하나로 구성하여 SCADA보안감리 프레임워크를 도식하면 [그림 6]과 같다.

Ⅳ. 결 론

SCADA 시스템은 전력, 가스, 수자원, 철도 등의 실시간 제어를 필요로 시스템에 적용하고 있어 대형의 플랜트나 국가 주요 기반시설에 적용하고 있다. 정부나 정부 산하기관들의 정보시스템에 대한 감리를 의무화 하면서도 그들 시스템의 정보보안에 대해서는 정보시스템 아키텍처의 일부로만 취급을 할 뿐 별도의 대책을 마련하기 위한 방법론이 연구된 것이 없다. 본 연구에서 제시한 SCADA 시스템 정보보안 아키텍처는 정부 및 민간 분야의 정보보안 정책이나 계획 수립의 근간이 될 수 있을 것으로 판단된다. 또한 SCADA 시스템을 운영하고 있는 조직에 대한 보안 감사는 국가안보 측면을 고려하여 반드시 강화되고 매년 시행되어야 한다.



〔그림 6〕. SCADA 보안 감리 프레임워크

본 논문에서는 이를 위해 SCADA 시스템을 구축 운영하는 조직의 정보보안 정책을 수립하기 위한 아키텍처를 제시하였고, SCADA 정보보안 프레임워크를 제시하여 사업 유형별로 감리를 할 수 있는 방법을 제시하였다.

향후 연구되어야 할 과제는 일반 비즈니스 시스템과 SCADA 시스템에 대한 감리기준에 관한 연구를 하여야 할 것이다. 일반 비즈니스 시스템에 대한 통제요구나 보안 서비스 요구는 관리적, 기술적, 환경적인 분야에서 제시되어 있지만 SCADA 시스템에 대해서는 아직 그러한 요구가 제시되어 정보보안 제품의 사양으로 적용할 수 있도록 되어 있지 못하다. 따라서 관련 연구가 조속히 수행되어야 할 것이며, 그에 따른 감리 기준에 관한 연구가 있어야 할 것이다.

참고문헌

[1] 정보시스템 감리 발전 방향, 한국전산원 1998,6
[2] 공공부문 정보보호 아키텍처 구성 방안 연구, 한국전산원 2004
[3] 정보시스템보안감리 프레임워크 발전 방향 연구, 한국전산원, 2003
[4] 정보시스템 감리점검해설서, V2.0. 한국전산원,

2007, 2
[5] SPP-ICS(system protection profile- Industrial control systems) version 1.0, NIST, 2004
[6] spice & CMMI, 경영정보학회 S/W management 연구회, 정호원, 2004, 4
[7] CobiT 4.0 한글판 한국정보시스템감사통제협회, 2006
[8] ANSI/ISA-TR99.00.01-2004, Security Technologies for Manufacturing and Control Systems, ISA, 2004
[9] ANSI/ISA-TR99.00.02-2004 Integrating Electronic Security into the Manufacturing and Control Systems Environment, ISA, 2004
[10] DOD technical architecture framework information management Volume 6, Department of Defense Goal Security Architecture, Version 3.0, April 1996
[11] Draft-SP800-82 Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security, NIST, September, 2006
[12] Critical Infrastructure Protection : Challenges and Efforts to Secure Control Systems, GAO-04-354, GAO, 2004
[13] perspectives on the future of control system security, Jeff Dagle, PE, SANS process control & SCADA security summit 2006, march 3 2006

〈著者紹介〉

이 철 수 (Lee ChulSoo) 정회원
소속 : 경원대학교 소프트웨어 대학(software collage of Kyungwon university)
1975-1977 : KAIST 전산과 석사
1977-1981 : KAIST 전산과 박사
1982-1993 : (주) 데이콤
1993-1998 : 한국전산원
1999-2000 : 한국정보보호원
2000-2002 : 정보통신대학교
2003- 현재 : 경원대학교
<관심분야> 정보보호 정책, 침해사고 대응기술