정 보 보 호 학 회 지
제24권 제3호, 2014. 6

특수 제어망의 정보보호 관리체계 제안

하 기 웅*, 민 남 홍, 황 희 성, 임 채 호**

요 약

SCADA 시스템은 독립적인 폐쇄된 환경에서 운영되는 산업 제어 시스템이다. 국가기간시설에 주로 이용되는 이 시스템에서 문제가 발생할 경우, 그 문제는 대재앙으로 확산될 수 있다. 최근에는 이 시스템들이 폐쇄된 환경에서 개방형으로 바뀌어가는 추세로 변화하고 있기 때문에, 정보망과는 다른 특징을 가진 제어 시스템에 대한 분석과 그에 대한 보안성 강화가 필요한 시점이 오고 있다. 본 논문에서는 현 시점의 국내외 정보망 및 제어 시스템에 대해서 어떠한 정보보호 관리체계가 적용되고 있는지 분석하고, 제어망의 특수한 성질에 근거하여 현 관리체계에 대한 한계점을 설명한다. 그리고 정보망과는 다른 제어 시스템만의 특징을 바탕으로 국내 제어 시스템에 대한 새로운 관리체계 방안에 대해서 부분적으로 제안한다.

Ⅰ. 서 론

SCADA(Supervisory Control And Data Acquisition) 시스템이란 폐쇄된 환경에서 운영되는 ICS(Industrial Control System)이다. 일반적으로 국가 시스템에서 많이 사용되고 있으며, 그 외에 중요한 기반 시설이나 제어 시설에도 사용되고 있다.

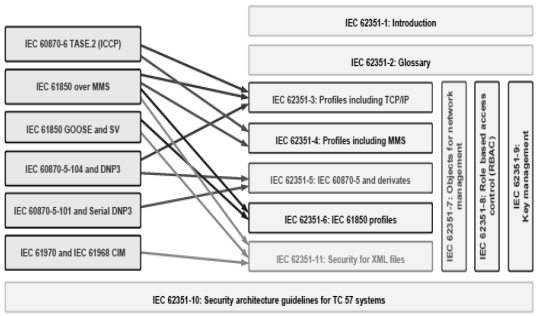
〔그림 1〕 제주도 Smart Grid 실증 단지

최근에는 이러한 시스템이 개방형으로 바뀌어가는 추세로 바뀌고 있다. 그 예로 국내에서는 [그림 1]과 같이 제주도에 Smart Grid 실증 단지를 구축하여 Smart Grid 연구를 활발하게 진행하고 있다. 이 사업은 기술 개발 성과의 실증과 그에 대한 비즈니스 모델을 개발하는데 그 목적이 있으며 IT, 에너지 등 170여 개 민간 기업이 참여하고 있다. 그리고 2013년까지 총 2400여 억 원을 투입한 대규모 사업이다. 이 사업의 내부에는 실시간 요금, 전기 차 충전, 신재생 실증 등이 포함되어 있다.[1]

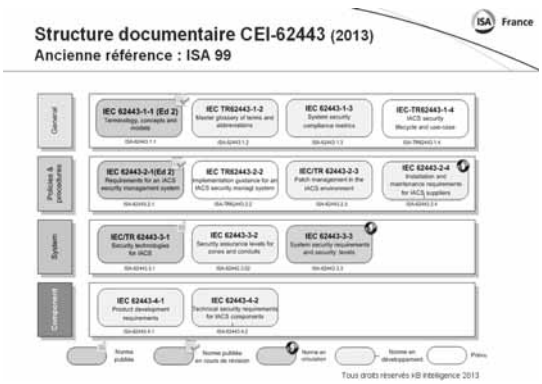
이렇게 ICS가 개방형으로 바뀌어가면서, 전력망에 대한 보안이 점차적으로 부각되고 있다. 기존의 환경에서는 그 필요성이 드러나지 않아 보안에 대해 많은 투자를 이루지 않았기 때문에, 만약 이대로 개방형이 진행된다면 이 시스템은 심각한 보안 이슈를 가지게 된다. 이미 해외에서는 각 국가들이 제어 시스템에 대한 보안 체계를 구축하고 그에 대한 대응방안을 모색하고 있으며, 미국에서는 SP 800-82 등의 문서 형태로 발표하였으며 [그림 2]와 [그림 3]과 같이 국제적으로는 IEC 62351, IEC 62443 등의 제어 시스템 보안 이슈를 포함한 규격 문서를 발행하였다.

국내에서는 국제적으로 제일 잘 알려진 정보보호 관리체계인 ISO 27001로 제어 시스템에 대해서 보안 인

* 동국대학교 국제정보대학원 정보보호학과 (hkw342@naver.com)
동국대학교 국제정보대학원 정보보호학과 (vvipmin@gmail.com)
동국대학교 국제정보대학원 정보보호학과 (heediyo@gmail.com)
** KAIST 정보보호대학원 (chlim@kaist.ac.kr)



〔그림 2〕 IEC 62351의 구성도



〔그림 3〕 IEC 62443의 구성도

증을 진행하고 있다. 하지만 제어 시스템은 기존의 정보 시스템과는 다른 분명한 차이점이 존재한다. 따라서 정보 시스템과 제어 시스템 사이의 차이점을 기반으로 하면서 국내 시스템 환경에도 적합한 새로운 인증이 필요하다.

본 논문의 목적은 K-ISMS을 기반으로 하여 미국 NIST 표준을 참고로 통제항목 추가 기준을 설립하여, 국내 제어 시스템에 대한 새로운 정보보호 관리체계 방안을 제안하는 것이다.

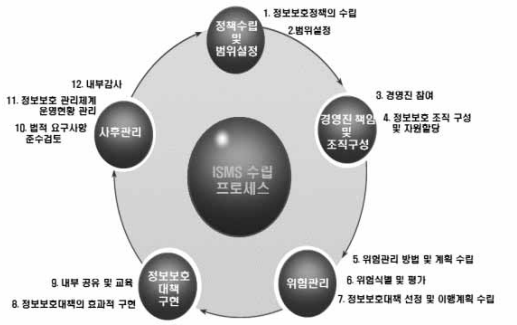
본 논문은 다음과 같이 구성한다. 2장에서는 국내외 정보망과 제어망의 정보보호 관리체계 현황을 살펴보고 서로 비교한다. 3장에서는 정보망과 제어망의 차이점을 분석하고, 국내에서 적용하고 있는 현 관리체계의 한계점과 피해 사례를 분석하여 국내 제어 시스템 정보보호 관리체계의 개선사항을 분석한다. 4장에서는 정보보호 관리체계를 도출하는 방법을 설명하고, K-ISMS와 NIST 표준을 비교 분석하여 K-ISMS와 NIST 표준을 기반으로 평가 기준을 도출하여 최종적으로 국내의 제어 시스템 정보보호 관리체계를 제안한다. 그리고 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 정보망과 제어망의 ISMS 비교

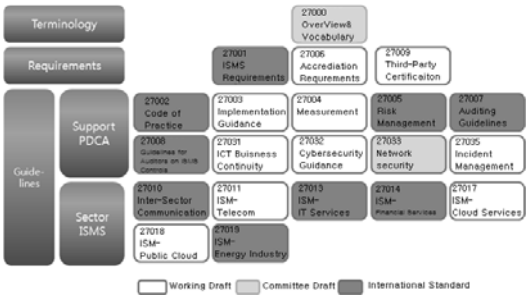
2.1 K-ISMS[2]

국내 대표적인 정보망 정보보호 관리체계로는 한국인터넷진흥원에서 주관하는 ISMS 인증제도가 있다. ISMS 인증제도는 정보보호의 주요 목적인 기밀성, 무결성, 가용성을 실현하기 위한 절차와 과정을 체계적으로 수립 및 문서화하고 지속적으로 관리 및 운영하는 시스템에 적합한 정보보호를 위해 정책 및 조직을 수립, 위험 관리, 대책 구현, 사후 관리 등의 정보보호 관리과정을 통해서 구현된 여러 정보보호 대책들이 유기적으로 통합된 체계에 대해 제 3자의 인증기관인 KISA가 객관적이고 독립적으로 평가하여 기준에 대한 적합성 유무를 보증해주는 제도이다.

ISMS 인증심사 기준은 2002년에 제도를 도입한 후 2013년에 개정기준을 공표하였으며 [그림 4]와 같이 정보보호 관리과정 5개 분야 12개 통제사항, 정보보호 대책 13개 분야 92개 통제사항 총 104개 통제사항으로 구성되어 있다. 즉, ISMS 인증을 받기 위해서는 인증기준을 만족하여야 한다. 이 기준은 2013년 2월 18일 이후로 적용되며 중복/유사기준 통합, 실효성 없는 기준 삭제, 신규 기술 및 정보보호 트렌드 등을 고려하여 구 기준 137개 통제사항에서 104개 통제사항으로 개정하였다.



〔그림 4〕 ISMS 정보보호 관리과정 요구사항



〔그림 5〕 ISO 27001 패밀리 시리즈

2.2 ISO 27001

국제적인 표준 정보망 정보보호 관리체계로는 ISO 27001이 있다. ISO 27001이란 정보보호 관리체계 요구사항(Information Security Management System Requirements)으로 정보보호 관리체계에 대해 국제 인증 시 요구사항을 정의하고 있다. ISO 27001은 정보보호 관리체계에 대한 국제적인 표준이기 때문에 전 세계 선진 기업이 합의한 Best Practice를 활용해 자사에 적용할 수 있게 된다.[3]

ISO 27001 인증은 자사의 정보보호 관리체계 업무에 대해서 제 3자 인증기관에 의해 적합성을 인증 받는 제도이다. 현재 정보보호 분야에서 가장 권위 있는 국제 인증 규격으로 과거 영국 표준인 BS7799를 기반으로, 지난 2000년에는 Part 1(실행지침) 부분을 국제 표준인 ISO 17799로 전환하고 2005년에 Part 2(규격) 부분을 ISO 27001로 전환하였다. 그리고 뒤이어서 2007년에 ISO 17799를 ISO 27002로 바꾸어 발표하였다.

ISO 27000 시리즈 또한 올해인 2013년 9월에 개정판이 발행되었다. 절차는 정보보호 PDCA(Plan-Do-Check-Act) 모델 4단계, 구조는 14개 분야 114개 통제사항으로 구성되어 있다. 즉 ISO 27001 인증을 받기 위해서는 위의 인증기준을 만족하여야 한다. 이 기준은 기존의 국제 표준에 대해 지난 3여 년 간의 개정 작업을 통해서 조직의 외주관리 통제 및 운영보안 통제 등을 새롭게 추가한 버전이며 구기준 133개 통제사항에서 114개 통제사항으로 개정하였다.[4]

2.3 SP 800-53 APPENDIX I[5]

미국의 대표적인 정보망 정보보호 관리체계로는 NIST에서 발행한 SP 800-53 문서가 있다. SP 800-53은 연방 정보보안 관리법 (FISMA : Federal Information Security Management Act)에서 정의한 표준을 충족시키는 규격을 제공하는 7개의 NIST 발간물 중 하나로, 2005년 12월에 의무사항이 된 연방 정보처리 표준 200(Federal Information Processing Standard 200), 연방 정보시스템에 대한 최소 보안 통제장치(Minimum Security Controls for Federal Information System)를 어떻게 구현할 것인가에 대해 자세히 설명하고 있다.

SP 800-53에는 위험 관리 프레임워크인 RMF(Risk Management Framework) 보안 라이프 사이클을 [그림 6]과 같이 도입하고 있다. 구체적으로 그 사이클은 "1. 정보 시스템 분류, 2. 보안 통제 선택, 3. 보안 통제 구현, 4. 보안 통제 평가, 5. 정보 시스템 승인, 6. 보안 통제 감시"의 6단계로 이루어진다. 보안 통제에 관한 세부적인 구조는 SP 800-53에서 단계적으로 기술하고 있다. 이 문서는 선택할 수 있도록 하는 권고수준의 표준 가이드라인이다. 이 가이드라인은 강제사항이 아니지만 미국의 주요한 기반 시설을 구성하는 조직들이 이 지침을 따라줄 것을 권장하고 있다. 2013년 4월에 발간된 rev4는 총 18개 분야 256개 통제사항으로 구성되어있다.

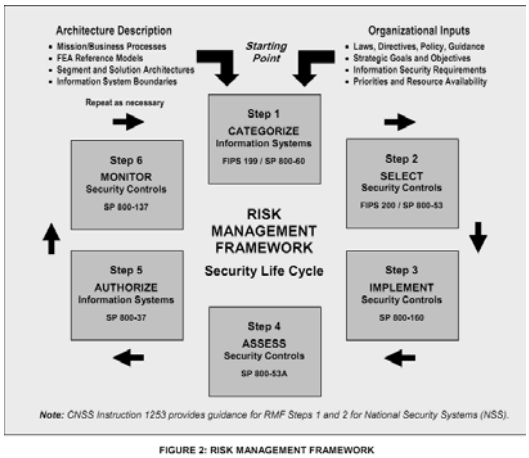


FIGURE 2: RISK MANAGEMENT FRAMEWORK

〔그림 6〕 Risk Management Framework

2009년 8월에 발표된 SP 800-53 rev3 최종 버전에는 SP 800-53의 통제 기준을 산업 제어 시스템에 적용한 예가 Appendix I에 나와 있다. 정식 명칭은 ICS Supplemental Guidance이며, 16개 분야 64개 통제사항

〔표 1〕 국내외 정보보호 관리체계 비교

	K-ISMS:2013	ISO 27001:2013	NIST SP 800-53 APPENDIX I
담당기관	한국인터넷진흥원(KISA)	국제표준화기구(ISO/IEC)	미국국가표준기술원(NIST)
관리과정	1.정보보호정책 수립 및 범위설정 2.경영진 책임 및 조직 구성 3.위험관리 4.정보보호 5.사후관리	PDCA 모델 1.ISMS 수립 2.구현 및 운영 3.모니터링 및 검토 4.유지 및 개선	RMF 보안 라이프 사이클 1.정보 시스템 분류 2.보안 통제 선택 3.보안 통제 구현 4.보안 통제 평가 5.정보 시스템 허용 6.보안 통제 모니터링
통제항목 구조	13개 분야	14개 분야	16개 분야
통제항목 분류	정보보호 정책 정보보호 조직 외부자 보안 정보자산 분류 정보보호 교육 인적 보안 물리적 보안 시스템개발 보안 암호 통제 접근 통제 운영 보안 침해사고 관리 IT 재해복구	정보보안 정책 정보보안 조직 자산 관리 인적자원 보안 물리적 및 환경적 보안 통신 보안 접근 통제 정보시스템 취득 개발 및 유지보수 정보보안 사고 관리 업무연속성 관리 준수 공급자 관계 암호 통제 운영 보안	접근 통제 (AC) 인식 및 훈련 (AT) 감사 및 책임추적성 (AU) 보안평가 및 승인 (CA) 구성 관리 (CM) 비상대응 계획 (CP) 식별 및 인증 (IA) 사고 대응 (IR) 유지보수 (MA) 매체 보호 (MP) 물리적/환경적 보안 (PE) 계획 (PL) 위험 평가 (RA) 시스템 및 서비스 인수 (SA) 시스템 및 통신 보호 (SC) 시스템 및 정보 무결성 (SI)
세부 통제항목	104개	114개	64개
특징	국내 표준 정보보호 관리체계	국제 표준 정보보호 관리체계	미국 산업 제어 시스템 및 조직에 대한 보안통제 권고항목
발표년도	2013년	2013년	2009년

으로 재구성되어있다. 본 논문에서는 rev3의 Appendix I를 참고하였다.

2.4 국내외 정보보호 관리체계 비교

앞에서 살펴본 정보보호 관리체계들은 각각의 관리 절차와 통제 항목을 가지고 있다. K-ISMS와 ISO27001에서 설명하고 있는 정보 시스템에 관한 통제 항목, 그리고 NIST RMF와 SP 800-53 APPENDIX I 파트에서 적용하고 있는 산업 제어 시스템에 관한 통제 항목은 [표 1]에서 비교하였다.

Ⅲ. ISMS의 개선사항 분석[6]

3.1 정보망과 제어망의 차이점 분석

현재 우리가 사용하고 있는 제어망 시스템은 전용망 및 공중망, Desktop-Computing 또는 인터넷이 산업에 통상적으로 사용되기 이전부터 개발된 것들이 대다수이다. 이러한 제어망 시스템은 요구사항을 만족하기 위해 성능, 안정성, 유연성, 신뢰성을 바탕으로 설계되었다. 대부분의 제어망 시스템의 경우 외부 네트워크와 물리적으로 떨어져 있고, 전용 하드웨어와 전용 소프트웨어 그리고, 오류 검출 및 정정 기능을 가지고 있는 통신프로토콜을 사용한다.

〔표 2〕 정보(IT) 시스템과 제어 시스템의 차이점〔6〕

분류	정보망	제어망
성능 요구	비 실시간, 지속적 응답, 고속 처리량, 지연 및 지터 허용	실시간, 신속한 응답, 적당한 처리량 허용, 지연 및 지터는 불허용
가용성 요구	재부팅 허용, 시스템 운영 요구사항에 따라 가용성 결함 허용	재부팅 불허용, 높은 가용성 요구, 여분의 시스템 필요, 계획된 가동 정지, 철저한 사전 배치 테스트
위험관리 요구	데이터 기밀성과 무결성이 가장 중요, 고장방지의 중요도 낮음(일시적인 가동 중지 허용), 비즈니스 운영 지연이 최대 위험 요소임	인명의 안정성이 가장 중요, 고장방지 필수(일시적인 가동 중지 불허용), 규정의 불이행, 환경의 영향, 인명 및 장비 혹은 생산 능력의 손실이 최대 위험
보안 구조	IT 자산 및 저장/전송되는 정보 보호, 중앙 서버 보안	제어장치와 PLC 같은 필드 장치 보호, 중앙 서버 보안
보안 솔루션	통상적인 IT시스템을 대상으로 설계	제어시스템 운영을 침해하지 않도록 보안 툴(off-line) 테스트 필요
시간 민감성	비상사태 시 상호작용에 덜 민감. 보안 정도에 따라 시스템에 대한 엄격한 접근 통제 적용 가능	비상사태 시 사람 혹은 다른 상호작용에 대한 대응이 매우 중요, 시스템에 대한 접근이 엄격히 규제되어야 함(그러나 HMI와 상호작용을 방해해서는 안 됨)
시스템 운영	일반적인 운영체제 사용하도록 설계. 갱신은 자동화된 도구를 이용해 쉽게 가능 일반적인 OS를 사용하도록 설계. 자동화된 도구를 사용하여 쉽게 갱신 가능	특화된 운영체제와 표준 운영체제 사용(흔히 보안 기능 결여), 소프트웨어 변경은 세심한 주의 필요(보통 벤더에 의해 수행) 특화된 OS와 표준 OS사용(보안 기능 부족), S/W 변경은 주의 필요(벤더에 의해 수행)
자원 제약성	보안 솔루션과 같은 제3자 애플리케이션의 추가를 지원하는 충분한 자원 이용가능	프로세스에 최적화된 설계로 보안 기능 추가를 위한 메모리 용량 및 컴퓨팅 자원 제한 존재
통신	표준 통신 프로토콜. 주로 지역 무선 기능을 가진 유선 네트워크 사용. 통상적인 IT 네트워크 기반으로 구축	통상적인 표준 통신 프로토콜. 다양한 형태의 유무선 사용, 복잡한 네트워크로 전력시스템에 대한 전문성이 요구
변화관리	소프트웨어의 변경은 보안정책과 절차에 따라서 주기적으로 실시 (자동화 도구를 사용)	소프트웨어의 변경은 제어시스템의 무결성을 보장하기 위해 단계적으로 실시 (대부분이 지원되지 않은 OS를 사용하여 패치 불가)
관리지원	다양한 형태의 지원 가능	단일 벤더를 통해서만 지원 가능
시스템 생명주기	짧은 생명주기 (3~5년)	긴 생명주기 (15~20년)
컴포넌트 접근성	근거리에 설치되어있어 접근이 용이	원거리에 설치되어 있고, 고립되어 있어 접근이 어려움

하지만 오늘날 시스템이 그물망처럼 연결되어 있는 환경에서 요구되는 보안통신기능은 많이 부족한 상태이다. 제어망 시스템은 통계적인 성능 및 장애를 고려하여 설계하기 때문에 가용성, 신뢰성, 유지보수성이 설계 시 가장 중요한 사항이었던 반면, 사이버 보안 대책에 관한 필요성은 전혀 예상하지 못했다. 제어망 시스템의 전용 솔루션을 일반적으로 사용하고 있는 IP기반의 디바이스가 대체하고, 연결성 및 원격접속기능을 증진시키기 위해 IT솔루션들을 채택하고, 산업 표준 컴퓨터, OS, 네트워크 프로토콜 등을 사용하여 구현되기 때문에 점점 IT시스템과 비슷해지기 시작했다.

이러한 통합으로 기존 제어망 시스템과는 다른 새로운 IT 능력을 지원해 주지만, 이로 인하여 제어망 시스템이 새로운 형태의 위협에 노출이 되며, 침해에 대한 가능성도 점차 증가하였다. 기존 IT시스템에 보안 이슈를 해결하기 위해 보안 솔루션이 설계되었지만, 제어망 시스템에 보안 솔루션을 적용하기 전에는 각별한 주의가 필요하다. 기존의 환경과 다른 경우에는 제어망 시스템에 맞게 설계된 새로운 보안 솔루션을 필요로 한다. 제어망 시스템의 침해는 결국 인간의 생명을 위협하게 되고, 생산성에 손실이 가며, 이에 따른 경제적인 타격을 주게 되고, 나아가 국가 경제에 악영향을 끼치게 된다.

〔표 3〕 정보(IT) 시스템과 제어 시스템 보안 특성의 차이점〔7〕

분류	정보시스템	제어시스템
중요 보안 요구사항	기밀성, 무결성, 가용성 순	가용성, 무결성, 기밀성 순
백신	공통적이고 광범하게 시행됨	흔하지 않고, 각각의 조건이 다르기 때문에 효과적인 설치가 불가능함
패치	계획적, 정기적으로 패치 실시	비계획적, 비정기적, off-line 시스템 상에서만 패치 실시. 특정 벤더에 의존
보안 인식	개인 및 공공 부문에 중간 정도	물리적 보안을 제외하고 보안인식이 낮음
보안 시험/감사	보안 프로그램에 대한 시험/감사	정치에 대한 일시적 시험
물리 보안	안전	원격/무인 안전

〔표 4〕 과거와 현재 제어시스템의 차이〔6〕

	과거 제어시스템	현재 제어시스템
동작환경	독립적인 시스템으로 구축 및 운용	인터넷과 같은 개방형 망을 통하여 외부시스템과의 연계 및 통합
연결 방식	전용선으로 연결	인트라넷이나 인터넷과 연동
운영체제	실시간 OS, 임베디드 OS	범용 OS (Windows, Linux)
시스템 형태	메인프레임 사용	워크스테이션, PC, 이동/무선 매체
프로토콜	필드버스, ICCP 등의 프로토콜	TCP/IP, 무선 프로토콜

또한, 제어망 시스템은 1년 내내 작동할 수 있도록 운영되어야 한다. 하지만. 제어망 시스템의 설계 및 운영 시 목표로 하는 안정성 및 효율성이 보안과 충돌하게 된다. 한 예로, 긴박한 상황 시에 패스워드로 인증을 요구하는 절차가 방해가 되어서는 안 된다.

이렇듯 제어망 시스템은 IT 시스템과는 다른 위험과 우선순위를 가진다. 제어망 시스템과 IT시스템의 접목이 갈수록 증가하고 있는 추세이지만, [표 2]와 같이 제어망 시스템과 IT시스템에는 운영되는 환경과 요구사항, 그리고 기술적인 특성 측면에서 많은 차이가 존재한다. 또한 [표 3]은 제어망 시스템과 IT시스템의 보안 특성의 차이점을 나타낸 표이다. 제어 시스템에 가장 적절한 보안 방안을 찾기 위해서는 본 논문에서 제시하는 특성과 차이점에 대해서 잘 이해해야 한다.

3.2 현 관리체계의 한계점 및 피해사례 분석

3.2.1 한계점

과거에 폐쇄된 환경에서 운영되던 제어시스템들은 현재 개방된 환경으로 넘어가고 있다. 업무효율성, 경쟁력 강화, 경영 합리화 등으로 인터넷 같은 외부 망과 연동되는 것이다. [표 4]는 현재 기준이 반영되고 있는 시스템을 나타낸다.

이와 같이 제어 시스템이 지속적으로 정보망과 접목됨에 따라 제어시스템을 구축·운영하는 산업제어시설들에 대한 사이버 침해 위협이 점차적으로 증가 하고 있다. 제어시스템에 대한 사이버 보안 위험을 증가시키는 요인들은 다음과 같다.

1) 알려진 취약성을 가진 기술과 프로토콜의 채택

산업시설은 비용 감소와 성능 향상을 위해 전용 OS에서 범용 OS로, 그리고 TCP/IP 같은 일반적인 네트워크 프로토콜 사용으로 전환하고 있다. 표준 프로토콜과 기술의 사용은 경제·기술적 측면에서 이익을 가져다주지만, 이러한 기술들은 이미 알려진 취약점을 가지고 있기 때문에 널리 이용 가능하고, 해킹 툴에 취약하다.

2) 다른 네트워크와의 연결접점의 증가

정보관리, 운영 및 비즈니스 관련 요구사항으로 인해

〔표 5〕 제어 시스템의 피해사례〔6〕

발생년도	목표물	피해사례
2000년	호주 Queensland 오폐수 제어시스템	퇴사직원이 무선네트워크를 이용하여 해킹, 악성코드를 설치. 3달 동안 총 46번 해킹을 통하여 80만 리터의 오폐수를 무단 방출함
2003년	미국 오하이오 주 Davis-Besse 원자력발전소	Slammer Worm이 침투하여 생산용 시스템이 6시간 동안 작동되지 않음
2005년	미국 Daimler Chrysler	제어시스템이 Zotob Worm 감염으로 인해 생산시스템 가동 중단으로 1400만 달러의 피해를 입음
2008년	TVA사 발전소 제어시스템	모의 해킹하여 침투에 성공함

기업IT 시스템과 연결된다. 많은 기관들은 외부에서 산업제어시스템 관리자와 기술 엔지니어가 제어시스템을 모니터링하고 제어할 수 있도록 원격 접속 채널을 구축하고 있다. TCP/IP FTP XML로 스테이션과 장치들에 데이터를 전송하기 위해 WAN(Wide Area Networks)과 인터넷을 사용한다.

3) 안전하지 않은/위험한 연결의 증가

시스템 유지업무의 편리성을 위해 시스템 공급 시 원격접속을 제공한다. 패스워드는 보통 특정 벤더의 모든 시스템에 동일하게 제공되기 때문에 더 위험하다. 제어시스템에서 무선 통신의 사용이 증가하고 있고, 통신 시 인증이나 암호화가 제공되지 않아 제어 시스템에 불법적인 접근 및 데이터 조작을 가능케 한다. 이질적인 시스템들의 통합 복잡성으로 인해 제어 시스템 엔지니어들은 흔히 보안 위험에 대해 인식하지 못한다.

4) 제어시스템에 대한 기술적인 정보의 노출

산업시스템의 설계, 유지보수, 상호연동과 통신에 대한 공개 정보를 인터넷을 통해 손쉽게 얻을 수 있다. 접근 가능한 정보를 이용하여 제어시스템에 대한 많은 지식을 가지지 않은 공격자도 자동화된 공격 툴이나 공장 초기 패스워드를 이용하여 제어시스템에 불법적으로 접근할 수 있다.

3.2.2 피해 사례

2010년 국가 주요산업제어시설을 대상으로 공격하는 'Stuxnet'이 등장하여 본격적으로 사이버전의 위협이 부각되고 있다.

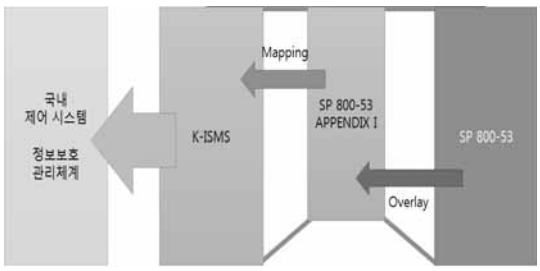
Stuxtnet은 기간망에 쓰이는 시설을 파괴한다는 점에서 사이버 공격을 무기화한 최초 사례로 알려져 있다. 전 세계 10만대 PC가 Stuxnet에 감염된 것으로 파악되었으며, 실제로 이란 원자력핵발전소의 20%를 중단시켜 수개월간 이란의 핵무기 개발을 지연시켰다.

Stuxtnet을 시작으로 향후 산업기반 시설 등의 특정 목표를 대상으로 한 위협이 증가할 것으로 예상된다. [표 5]는 Stuxtnet 이전에 발생한 산업제어시설에 대한 보안침해 사고를 나타낸다.

Ⅳ. 국내 제어망을 위한 정보보호 관리체계

4.1 설계 방법론

미국에서는 대표적인 통제 항목 리스트 지침서인 SP 800-53을 산업 제어 시스템에 오버레이(Overlay)해서 도출한 변경 항목들이 APPENDIX I에 나와 있다. 본 논문은 국내 제어 시스템의 정보보호 관리체계 도출을 위해서 미국에서 적용한 오버레이 방법과 유사하게 적용한다.



〔그림 7〕 국내 제어망 통제 항목 도출 방법

국내에서는 SP 800-53과 같은 특정 시스템에 대해 오버레이를 적용한 사례가 존재하지 않기 때문에, 본 논문에서는 〔그림 7〕과 같이 APPENDIX I를 토대로 K-ISMS의 항목 중 해당하는 부분의 내용을 제어 시스템에 맞게 변경하는 작업으로 항목을 도출한다.

4.2 매핑을 통한 비교 분석

매핑은 대상 정보보호 관리체계인 K-ISMS, NIST SP 800-53 APPENDIX I, ISO 27001에 대해서 진행한다.

〔표 6〕 전체적인 통제 항목의 매핑

K-ISMS	NIST SP800-53 (부록 I)	ISO 27001
정보보호 정책	-	보안정책
정보보호 조직	접근 통제 (AC), 인식 및 훈련 (AT), 비상대응 계획 (CP), 위험 평가 (RA), 시스템 및 통신 보호 (SC)	정보보안 조직
외부자 보안	접근 통제 (AC), 인식 및 훈련 (AT), 구성 관리 (CM), 사고 대응 (IR), 계획 (PL), 시스템 및 서비스 인수 (SA)	인원 보안
정보자산 분류	위험 평가 (RA)	자산 관리
정보보호 교육	-	인원 보안
인적 보안	-	인원 보안
물리적 보안	인식 및 훈련 (AT), 비상대응 계획 (CP), 유지보수 (MA), 매체 보호 (MP), 물리적/환경적 보안 (PE)	물리적/환경적 보안
시스템개발 보안	접근 통제 (AC), 구성 관리 (CM), 식별 및 인증 (IA), 위험 평가 (RA), 시스템 및 서비스 인수 (SA), 시스템 및 통신 보호 (SC), 시스템 및 정보 무결성 (SI)	정보시스템 취득 및 개발, 유지보수
암호 통제	-	정보시스템 취득 및 개발, 유지보수
접근 통제	접근 통제 (AC), 구성 관리 (CM), 식별 및 인증 (IA), 유지보수 (MA), 물리적/환경적 보안 (PE), 시스템 및 서비스 인수 (SA), 시스템 및 통신 보호 (SC)	접근 통제
운영 관리	접근 통제 (AC), 인식 및 훈련 (AT), 감사 및 책임추적성 (AU), 보안평가 및 승인 (CA), 구성 관리 (CM), 비상대응 계획 (CP), 매체 보호 (MP), 위험 평가 (RA), 시스템 및 서비스 인수 (SA), 시스템 및 통신 보호 (SC), 시스템 및 정보 무결성 (SI)	통신 및 운영 관리
전자거래 보안	-	통신 및 운영 관리
보안사고 관리	사고 대응 (IR), 시스템 및 정보 무결성 (SI)	보안사고 관리
검토, 모니터링 및 감사	접근 통제 (AC), 감사 및 책임추적성 (AU), 식별 및 인증 (IA), 계획 (PL), 시스템 및 통신 보호 (SC)	법규 준수
업무연속성 관리	비상대응 계획 (CP), 위험 평가 (RA)	사업 연속성 관리

먼저 해당 정보보호 관리체계에 대해서 [표 6]과 같이 전체적인 통제 항목의 매핑을 진행한다. SP 800-53에 대해서는 ICS에 대한 내용을 오버레이한 APPENDIX I를 기반으로 하고 있기 때문에, 기존의 NIST 800-53에 비해서 항목 수가 적음을 알 수 있다. 또한 이번에 새로 개정된 ISO 27001과 K-ISMS에 대해서 아직 확립된 비교 기준이 없기 때문에 매핑은 기존의 버전으로 진행하였다.

다음으로 항목에 대해서 세부적인 매핑 진행을 보여준다. 본 논문에서 모든 항목에 대한 매핑 진행 과정을 보여줄 수 없으므로, [표 7]과 [표 8]과 같이 전체 통제 항목 중 K-ISMS 통제 항목 번호 11번에 해당하는 '운영관리' 항목에 대해서 세부적인 매핑 테이블을 보여준다.

〔표 7〕 K-ISMS 11.1/11.2 항목의 세부적인 매핑

K-ISMS		NIST SP800-53 (부록 I)		ISO 27001	
11. 운영관리				A.10 통신 및 운영관리	
11.1 운영 절차와 책임				A.10.1 운영 절차 및 책임	
11.1.1	운영절차의 문서화			A.10.1.1	문서화된 운영절차
11.1.2	정보자산의 변경관리	CM-3 CM-4 CM-5	구성 변경 통제 보안 영향 분석 변경을 위한 접근제한	A.10.1.2	변경관리
11.1.3	직무분리	AC-5	직무분리	A.10.1.3	직무분리
11.1.4	개발과 운영환경의 분리			A.10.1.4	개발, 테스트, 운영설비의 분리
11.1.5	외부 운영설비 관리				
11.2 시스템운영				A.10.3 시스템 계획 및 인수	
11.2.1	시스템도입				
11.2.2	시스템인수	CA-2 CM-3 CM-4	보안 평가 구성 변경 제어 보안 영향 분석	A.10.3.2	시스템 인수
11.2.3	성능관리				
11.2.4	용량관리	AU-5 CP-2	감사 처리 장애에 대한 응답 보안 평가	A.10.3.1	용량 관리
11.2.5	백업 및 복구관리				
11.2.6	장애관리				
11.2.7	로그관리				
11.2.8	보안시스템 운영				

〔표 8〕 K-ISMS 11.3/11.4/11.5/11.6 항목의 세부적인 매핑

K-ISMS		NIST SP 800-53 (부록 I)		ISO 27001	
11. 운영 관리				A.10 통신 및 운영 관리	
11.3 네트워크 운영				A.10.6 네트워크 보안관리	
11.3.1	네트워크 운영대책	AC-17 AC-18 SC-7 SC-19 SC-23	원격 접속 무선 접속 경계 보호 VoIP 세션 신뢰성	A.10.6.1	네트워크 컨트롤
11.3.2	인터넷 접속관리	SC-10 SC-22 SC-23	네트워크 연결해제 이름/주소 변환 서비스에 대한 구조 및 권한 설정 세션 신뢰성	A.10.6.1	네트워크 컨트롤
11.3.3	원격운영관리	AC-17 SC-9	원격 접속 전송 기밀성	A.10.6.1 A.10.6.2	네트워크 컨트롤 네트워크 서비스 보안
11.4 매체 및 문서관리				A.10.7 매체 처리	
11.4.1	매체 취급 및 보관	MP-5	미디어 전송	A.10.7.1 A.10.7.3	이동식 매체 관리 정보 처리 절차
11.4.2	매체의 폐기			A.10.7.2	미디어 처분
11.4.3	시스템 문서의 보안			A.10.7.4	시스템 문서 보안
11.5 악성소프트웨어 통제				A.10.4 악성 코드 및 모바일 코드 보호	
		SI-3	악성 코드 보호	A.10.4.1	악성코드 통제
11.6 원격컴퓨터 및 원격작업					

4.3 정보보호 관리체계 평가 기준 도출

본 절에서 통제내용을 전부 다루기에는 한계가 있으므로, K-ISMS의 일부 통제항목에 대해서만 다루기로 한다.

제어시스템에서 가장 중요한 것은 안전이다. 따라서 안전과 보안의 상호의존성을 고려해야 한다. 또한, 일반 정보시스템과는 다르게 제어시스템은 가용성을 가장 우선시하므로, 기능이 완전하게 동작하지 않는 것을 대비하여 예비 대책을 제공해야 한다.

이를 바탕으로 NIST SP 800-53 문서의 APPENDIX I를 참고하여 K-ISMS에 접목시킬 수 있는 통제내용을 [표 9]에 제시하였다.

〔표 9〕 K-ISMS에서 ICS 내용을 추가한 새로운 운영관리 부분 통제항목

통제목적	통제사항	변경한 통제내용
11.1 운영절차와 책임	11.1.2 정보자산의 변경관리	정보시스템 관련 자산들을 조사하고, 모든 변경사항들을 반영할 수 있는 공식적인 관리 책임 및 절차를 수립해야 할 때, 제어시스템은 안전과 보안의 상호의존성을 고려해야 하고, 구성변경과 액세스 제한에 대한 보상 컨트롤을 추가해야 한다.
	11.1.3 직무분리	부주의에 의한 또는 고의적인 시스템 오용의 위험을 감소시키기 위해 직무를 분리하고, 제어시스템에서 역할을 나눌 수 없을 때, 조직은 보안과 감사를 증가시키는 등의 보상컨트롤이 필요하다.
11.2 시스템 운영	11.2.2 시스템인수	새로운 정보시스템의 설치 또는 업데이트에 따른 인수기준을 확립하고, 평가 범위를 설명하는 보안 평가 계획을 개발한다. 구성 변경을 제어하고, 보안 영향을 분석하며, 안전과 보안의 상호 의존성을 고려해야 한다. 또한, 시스템은 이 기준에 의해 테스트를 한 후 인수하여야 한다.
	11.2.4 용량관리	용량계획을 수립하여 조직에서 용량 요구사항을 충족시켜 적정선의 용량을 확보하고, 이에 따른 관리방안을 수립하여 주어진 용량을 최적으로 사용할 수 있도록 용량관리를 해야 한다. 비상계획 시 조직은 장애발생 시 시스템의 상태 변수를 복원하기 위한 지침을 확립해야 한다. 또한, 감사처리장애에 대한 응답을 명확히 해야 하고, 별도의 정보 시스템 감사 기능을 제공해야 한다.
11.3 네트워크 운영	11.3.1 네트워크 운영대책	제어시스템 네트워크 운영 보안 유지를 위해 직무 분리, 접근권한 통제, 원격접속/무선접속 설비 관리, 네트워크 분리를 위한 책임 및 절차, 높은 감사 조치, VoIP 기술의 사용, 세션의 신뢰성 등을 포함한 대책을 수립하여야 한다. 제어 시스템이 이 대책의 어떤 부분 또는 전체를 수립할 수 없을 때, 조직은 제어시스템 전용 지침에 따라 메커니즘 또는 절차를 수립하여야 한다. 기술의 사용은 이것이 제어시스템의 운영 성능에 악영향을 주지 않는지 신중하게 검토하고 검증한 후 결정해야 한다.
	11.3.2 인터넷 접속관리	제어시스템에서 인터넷 망과 접속 시 침입차단시스템과 침입탐지시스템 등을 통해 접근통제 및 모니터링을 수행하여야 한다. 제어시스템이 안정성, 성능, 신뢰성에 대한 심각한 악영향 때문에 네트워크 연결을 종료할 수 없는 상황 또는 통신 세션의 신뢰성을 보장할 수 없는 상황에서 조직은 제어시스템 전용 지침에 따라 적절한 통제를 수행해야 한다.
	11.3.3 원격운영관리	제어시스템 네트워크를 통해 시스템을 운영하는 경우, 일반적으로 제어시스템 정보에 대한 접근은 내부의 특정 터미널에서만 할 수 있도록 제한해야 한다. 또한 조직은 적절한 고장 모드를 선택해야 한다. 외부에서 네트워크를 통하여 시스템을 관리할 경우에는 사용자 인증, 암호 및 접근통제 기능을 설정하여야 하며, 제어시스템 보안 목적은 전형적으로 가용성, 무결성, 기밀성 순서의 우선순위를 따르므로 암호의 사용은 시스템 운영 성능에서 보안 요구사항과 잠재적인 영향을 신중하게 검토한 후 결정해야 한다.
11.4 매체/문서 관리	11.4.1 매체 취급 및 보관	제어시스템에서 허가되지 않은 유출이나 오용으로부터 정보를 보호하기 위해 매체의 취급 및 보관에 대한 절차를 수립하고 운영할 때, 제어시스템이 매체 전송 시 암호화 메커니즘을 지원하지 않는 상황에서 조직은 제어시스템 전용 지침에 따라 물리적인 보안 대책과 같은 통제를 수행해야 한다.
11.5 악성소프트웨어 통제		바이러스 등의 악성 소프트웨어로부터 제어시스템을 보호하기 위해 악성 소프트웨어들을 예방하고 탐지, 대응하는 대책을 수립해야 한다. 이 대책은 그것이 제어시스템의 운영 성능에 악 영향을 주지 않는지 신중하게 검토 및 검증 한 후 결정되어야 한다. 조직이 중앙 집중적으로 악성 소프트웨어 보호 메커니즘을 관리할 수 없는 상황인 경우, 제어시스템 전용 지침에 따라 적절한 통제를 수행해야 한다.

Ⅴ. 결론 및 향후과제

산업 제어 시스템이 개방형으로 바뀌어가는 추세에 따라 전력망에 대한 보안도 점차 부각되고 있다. 해외에서는 이미 여러 국가들이 제어 시스템에 대한 보안 관련 이슈를 중점적으로 연구하고 보안 체계를 구축하고 있다. 하지만 국내에서는 아직 일반적인 정보 시스템에 대응하는 정보보호 관리체계로 제어 시스템에 대해서 인증을 진행하고 있다. 정보 시스템과 제어 시스템은 시스템의 특징에서 분명한 차이점이 존재함을 본 논문에서 제시하였다.

본 논문은 국내외 정보망과 제어망에서 사용되고 있는 여러 가지 종류의 정보보호 관리체계를 알아보았다. 또한 K-ISMS을 기반으로 미국의 SP 800-53을 산업 제어 시스템에 오버레이를 적용한 부록 I를 참고하여 국내 제어 시스템에 대한 변경된 정보보호 통제항목 기준을 설립하는 방안을 설명하였고, 그에 대한 결과를 도출하였다.

하지만 본 논문은 미국의 오버레이 예시를 국내 환경에 적용시킨 예이므로 예비 모델에 불과하다. 또한 2013년에 새롭게 등장한 ISO 27001과 K-ISMS 환경에 적용하지 않았기 때문에 앞으로 발전하게 되는 분야에 사용하기에 다소 부족하다. 따라서 향후 새로운 ISO 27001과 K-ISMS 환경에 맞추어서 오버레이 방법론을 기반으로 좀 더 발전된 제어 시스템 정보보호 관리체계에 대한 연구가 필요하다.

본 논문을 통해서 일반적인 정보 시스템과 다른 제어 시스템에 대한 특별한 정보보호 관리체계가 필요함을 인지하고, 그에 대한 맞춤형 정보보호 관리체계가 마련되어 제어 시스템에 특화된 인증과 관리제도가 확립되기를 바란다.

참 고 문 헌

[1] 제주 스마트 그리드 실증단지, “스마트 그리드 추진 동향” http://smartgrid.jeju.go.kr/contents/index.php?mid=0102

[2] KISA, “ISMS 인증기준 세부점검항목”, 2013. 05. http://www.kisa.or.kr/jsp/common/downloadAction.jsp? bno=48&dno=114&fseq=1

[3] 보안뉴스, “국내외 정보보호 관리체계 인증현황 및 준비방법”, 2007.02 http://www.boannews.com/know_how/view.asp?page=52&gpage=51&idx=1191&numm=866&search=title&find=&kind=03&order=ref

[4] 산업통상자원부, “정보보안관리체계(ISMS) 국제표준 2.0 시대 예고”, 2013. 10.

[5] NIST, “Security and Privacy Controls for Federal Information Systems and Organizations”, SP 800-53 Revision 3, 2009. 08.

[6] 권정옥 외 1인, “산업제어시스템의 보안 관리방안에 관한 연구”, Samsung SDS Journal of IT Services, 2011. 09.

[7] 전용희, “스마트 그리드의 취약성, 특성, 설계 원칙 및 보안 요구사항 분석”, 정보보호학회지, 2010. 06.

[8] NIST, “Guide to Industrial Control System(ICS) Security”, SP 800-82, 2008. 09.

[9] KISA, “ISMS 인증제도 소개” http://isms.kisa.or.kr/kor/intro/

[10] 김기철 외 1인, "K-ISMS 기반의 한국형 스마트 그리드 정보보호 관리체계 평가 기준 제안", 정보보호학회논문지, 2012. 12.

[11] 권상은, “실시간 보안수준 측정을 위한 정보보안 관리 모델 연구”, 석사학위논문, 정보보호대학원, KAIST, 2013.

[12] 임효식, “주요 보안 요소 중심의 금융기관 사고 대응 프로세스 개선안 연구”, 석사학위논문, 정보보호대학원, KAIST, 2014.

[13] “정보보안관리체계(G-ISMS) 기반의 KISTI 정보보안 관리 모델 연구”, KISTI, 2012.

〈저 자 소 개〉

하 기 웅 (Gi-Ung Ha)
학생회원

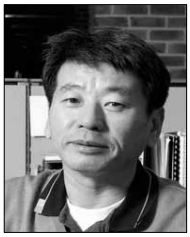
2012년 2월 : 동아대학교 컴퓨터공학과 졸업
2013년 3월~현재 : 동국대학교 정보보호학과 석사과정
관심분야 : 네트워크보안, 제어시스템보안, 침입탐지시스템

민 남 홍 (Nam-Hong Min)
학생회원

2013년 2월 : 동국대학교 컴퓨터공학과 졸업
2013년 3월~현재 : 동국대학교 정보보호학과 석사과정
관심분야 : 정보보호, 제어시스템보안, 접근제어

황 희 성 (Hee-Sung Hwang)
학생회원

2013년 3월~현재 : 동국대학교 정보보호학과 석사과정
관심분야 : ISMS, 정보보호, 취약점 분석



임 채 호 (Cha-Ho Lim)
종신회원

1986년 : 홍익대학교 전산학과 졸업
2001년 : 홍익대학교 전자계산학과 박사
2006년~2009년 : NHN(주) 보안실 실장, 연구센터 수석
2009년 : 한국정보보호학회 부회장
2010년 8월~현재 : KAIST 사이버보안연구센터 연구부소장
2011년 2월~현재 : KAIST 정보보호대학원 연구교수
관심분야 : 인터넷 보안, 정보보호 위험 관리, 정보보호 관리 및 정책