정 보 보 호 학 회 지
제26권 제4호, 2016. 8

산업제어시스템 보안 표준화 동향

나 재 훈*, 나 중 찬**

요 약

초기의 산업제어시스템은 독립적인 네트워크를 구성하고 있어서 외부 네트워크와는 분리되어 있어 안전하다는 의견을 갖고 있었으나, 악성코드에 의한 우회적 공격이 발생함으로 단순 공극(Air-gap) 정책으로는 대처하는 것에는 한계가 드러났다. 또한 정보통신(ICT: Information & Communication Technology) 기술의 발달로 산업제어네트워크는 비즈니스, 정보공유 그리고 유지보수를 위하여 외부 네트워크와 연결이 필요하게 되었다. 이로 인하여 ICT의 보안 취약점도 전수되는 상황이 되었다. 그러나 산업제어시스템은 독립적인 플랫폼과 제어기술로 구축되어 있어서, ICT의 기 개발된 보안 메카니즘이 그대로 적용될 수 없다는 것이 문제로 인식되고 있다. 산업제어시스템 보안을 위하여 단품의 보안 제품이나 서비스로 대응하는 것으로는 보안강도를 충족하지 못하는 것이 일반적이며, '심층 방어' 체계를 구축하여 종합적이고, 체계적인 보안 대책이 필요하다. 이와 상응하여 산업제어시스템 영역에 최적의 보안 수준을 유지하기 위하여 장비의 호환성을 제공하기 위하여 표준화 필요성이 대두되고 있으며, 이에 현재 진행되고 있는 표준화 동향을 분석한다.

Ⅰ. 서 론

산업제어시스템 이라는 용어는 산업생산 영역에서 사용되고 있는 여러 형태의 제어시스템이라는 용어가 일반화된 것이다[1]. 산업제어시스템은 보통 SCADA (Supervisory Control And Data Acquisition), DCS (Distributed Control Systems), 그리고 PLC (programmable logic controllers)와 같은 제어시스템을 포함하며, 전력, 수자원, 석유, 가스, 교통과 같은 산업에서 보편적으로 활용되고 있다. 원격지에서 수신된 데이터를 기반으로, 자동화되거나 운영자에 의한 관리 명령은 원격지의 밸브나 차단기의 개폐와 센서로부터 데이터를 수집, 그리고 현장의 알람상태를 모니터를 하는 제어 장비들에게 전달될 수 있다.

산업 제어시스템은 주요 기반시설을 포함하며, 사이버 공격으로 인해 기능이 마비되면 국민의 생명, 생활, 재산, 국가 경제에 중대한 영향을 끼쳐 국가경제에 혼란 초래할 수 있으며, 일반 ICT (Information Communication Technology) 시스템과 비교해 볼 때 폐쇄성, 자원의 특수성, 운용 가용성 등의 측면에서 차이점이 있다[2].

본 논문에서는 산업제어시스템 보안을 위하여 ICT와 비교하여 산업제어시스템에서는 무엇을 목표로 하고 있으며, 이러한 목표를 위하여 국내외 기술들의 현황과 국외 표준화 동향을 소개하고자 한다.

Ⅱ. 산업제어시스템 보안

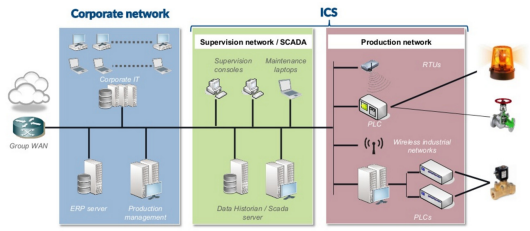
2.1. 산업제어시스템 구조

산업제어시스템은 산업 공정을 운영 또는 자동화하기 위하여 사용되는 장비, 시스템, 네트워크 그리고 제어로 구성되어 있다. SCADA 네트워크는 관리 목적으로 운영을 위한 데이터와 그리고 공정관리를 위한 제어 능력을 제공하기 위하여 ICS (Industrial Control System)와 소통을 하는 시스템 또는 네트워크가 된다. 자동화는 계속적으로 진화하고 또 점점 중요한 위치를 차지하게 되었으며, 산업제어시스템(ICS)/SCADA의 사용은 널리 보급되고 있다.

산업제어시스템의 전통적인 구조는 인터넷과는 파이

본 연구는 미래창조과학부의 정보보호핵심원천기술개발사업의 일환으로 수행되었음.[R0126-15-1095. 사이버물리시스템에서의 물리적 단방향 보안 게이트웨이 개발]
* 한국전자통신연구원 CPS보안연구실 (jhnah@etri.re.kr)
** 한국전자통신연구원 CPS보안연구실 (njc@etri.re.kr)

어월을 이용하거나, 아니면 공극(Air-gap)으로 분리가 되어있다. 그림 1에서 산업제어시스템은 하부구조의 생산라인에서 작업공정의 상태를 알 수 있도록 센서가 존재하며, 이러한 센서로 부터 데이터를 수집하여 상위 관리 사이트로 전달을 한다. 데이터는 관리서버에 지속적으로 저장되면서 현황판에 작업공정을 실시간적으로 상황을 알리며 정책에 의하여 사전 정의된 작업이면 조건에 따라 바로 다음 작업공정 지시가 하부 작업 네트워크로 전달되어지고, 액츄레이터를 통하여 작업공정의 조치가 이루어진다. 이러한 작업을 위하여 하부구조에는 현장 사이트들이 독립된 형태로 구성되어 있으며 이들 현장 사이트들을 상하 및 상호 통신을 위하여 SCADA가 교량역할을 한다.



〔그림1〕 산업제어시스템 구성도

2.2. ICT와 산업제어시스템과의 비교

초기 산업제어시스템은 릴레이, 카운터 및 타이머 배치를 통한 하드웨어 형태로 구현하였으나, 프로그램이 가능한 집적회로 및 마이크로프로세서의 등장으로 PLC 제어기 형태로 발전되었다. 현재 산업제어시스템 설비들은 상호연결성과 원격접근성 향상을 위한 ICT 기술 적용으로 보안 취약점 발생 가능성이 증대되는 단점을 가지게 되었다. 아래 표1은 일반 ICT 시스템과 산업제어시스템은 많은 차이점을 가지고 있어 보안관리체계 구축에 대하여 ICT와는 다른 접근방법을 고려 하여야 함을 보이고 있다[1]. 즉, 산업제어시스템은 ICT (Information & Communication Technology)와 같이 정보를 획득하는 것에 주력을 하는 것이 아니고, 획득한 정보를 가지고 기반 설비를 제어하는 것이므로, 시스템의 정지는 재산상의 피해는 물론 안전에 큰 문제를 일으킬 수 있으므로 허용되지 않다.

〔표 1〕 ICT와 산업제어시스템의 차이점

구분	ICT	제어시스템
요구성능	비 실시간	실시간
가용성	재시동 허용, 가용성 편차 허용	재시동 불허, 계획된 정지, 고 가용성
보호대상	정보	필드 장치, 프로세스
시스템운영	표준 OS 사용	전용 OS 사용
생명주기	단기〔3~5년〕	장기〔15~20 년〕
통신 프로토콜	TCP/IP 기반	전용프로토콜
SW변경관리	보안정책에 따라 자동적용	사전 시험 후 점진적 적용, 계획된 정지 시기에 적용
접근 용이성	지역에 국한, 접근 용이	넓은 영역에 퍼짐, 물리적 접근 노력 필요
보안솔루션	일반 ICT 시스템 대상 솔루션	사전 시스템 영향성/가용성 평가
파급효과	제한적 피해	재산 수준의 사회/경제적 피해
자원 제한	추가SW설치가능	백신,IDS등의 설치 어려움
A/S 지원	다양한 지원	단일 벤더지원

2.3. 산업제어시스템 관련 보안사고(Incident)

산업제어시스템과 관련하여 발생된 사건, 사고는 다음과 같다.

- 퇴사한 직원이 무선 네트워크를 이용하여 호주 퀸즈랜드의 폐수처리 제어 시스템을 해킹하여 오작동 유발, 세 달 동안 총 46차례 해킹하여 80만 리터의 폐수 무단 방출 (‘00)
- 미국 오하이오 주 데이비스-베시(Davis-Besse) 원자력발전소가 내부는 방화벽으로 보호되고 있었지만 설계사의 회사 네트워크에서 발전소로 원격 접속이 가능한 허점을 이용하여 슬래머 웜(Slammer Worm)에 감염. 원전 비안전 계통 신호 이상이 발생하여 원자력발전소 가동 중지(‘03)
- 슬래머 웜에 의한 스카다(SCADA) 시스템 감염으로 8시간 동안 해양 설비 플랫폼(Offshore Production Platform) 가동 중단. 생산 중단 및 재가동으로 약 1,200만 달러의 손실 발생(‘04)

- 다임러크라이슬러(DaimlerChrysler)의 미국 공장 시스템에서 사용 중인 마이크로소프트(Microsoft)의 Windows 2000 서버와 XP가 조톱 웜(Zotob Worm)에 감염되어 자동차 제조 공장 13곳 모두 1시간 가량 운영 중단(‘05)
- 이란 나탄즈(Natanz) 우라늄 농축시설 시스템의 유지보수를 위한 데스크톱이 유지보수 업체 직원의 실수로 스턱스넷에 감염되면서 IR-1 타입 원심 분리기 1,000여개 고장 및 교체(‘10)
- 미국 일리노이주 스프링필드 외곽의 상수도 시설에 원격 접속이 가능한 점을 악용한 해킹으로 제어 펌프에 장애 발생(‘11)
- 사우디아라비아의 정유회사인 아람코(Aramco)가 샤문(Shamoon)이라는 이름의 악성코드 감염으로 네트워크 마비(‘12)
- 카타르에서 두 번째로 큰 LNG 생산 시설인 라스가스(RasGas)가 알 수 없는 악성코드 공격에 의해 네트워크 마비(‘12)
- 스카다 시스템 업체 텔벤트(Telvent) 제품에 악성코드가 삽입(‘12)
- 마약 및 총기 밀수에 악용할 목적으로 벨기에 앤트워트항 콘테이너 관리 시스템 해킹(‘13)
- 전쟁 대피소로 사용되는 이스라엘 카멜(Carmel) 터널 개폐 장치 해킹으로 악성코드 감염, 이틀간 엄청난 교통 혼잡 발생(‘13)
- 일본 몬주 원자력발전소 내부 작업자가 동영상 재생 프로그램을 업데이트하던 도중 악성코드에 감염, 42,000개 이상의 직원 개인 정보 노출(‘14)

〔표 2〕 국내외 산업제어시스템 보안사고

연도	발생국	내용	비고
2003	미국 오하이오주 Davis-Besse 발전소(원자력)	감시시스템 바이러스 감염으로 5시간 운영중단	악성코드
2005	다임러크라이슬러 (제조)	운영체제 감염으로 공장 13곳 1시간 운영중단	악성코드
2007	미국 LA 교통시스템 (교통)	내부자에 의한 시스템 침해	내부자
2007	미국	전직 직원이 TCCA	악성코드
	캘리포니아 운하 (수자원)	운하 제어시스템에 악성프로그램 설치,운하 운영 마비, 5,000만 달러 이상 손실	
2008	폴란드 트램 (교통)	14세 소년이 TV 리모컨을 개조하여 트램 교차로 불법 조작, 4대의 트램 탈선 및 12명 부상	리모콘
2008	터키 송유관 (에너지)	석유송유관 카메라 통신 소프트웨어 취약점을 이용해 네트워크 침투,알람 관리 네트워크 장애 발생 및 석유 압력 변조로 폭발 사고 유도	해킹
2009	러시아 수력발전 (수자원)	수력발전 댐의 터빈 제어시스템 장애, 전기 터빈 폭발, 75명 사망	해킹
2009	미국 전력망 (전력)	Conficker 웜 제어시스템 감염 1천 2백만 컴퓨터 감염	악성코드
2009	러시아 Sayano-shushenskaya 댐 (수자원)	제어시스템 문제로 발전기 터빈 폭발	장애
2010	이란 우라늄 원심 분리기 (원자력)	스턱스넷 감염으로 원심분리기 1,000개 감염	악성코드
2011	미국 상수도 시설 (수자원)	원격접속으로 일리노이주 상수도 시설 시스템 침투, 펌프 작동 시스템 파괴	해킹
2012	사우디 아람코 (석유)	악성코드 감염, 네트워크 마비	악성코드
2012	카타르 LNG 생산시설 (가스)	악성코드 감염, 네트워크 마비	악성코드
2012	미국 휴스턴 상수도 (수자원)	제어시스템에 미공개 악성코드 감염	악성코드
2012	이란, 수단, 시리아 등 (기반시설)	주요 중동국가의 컴퓨터에 침입하여 중요 데이터 유출・파괴	해킹
2012	미국 전력 (전력)	전력시설 터빈 제어시스템 악성코드 감염, 3주간 운영 중단	악성코드
2013	이스라엘 터널 개폐장치(교통)	악성코드 감염으로 교통혼잡 발생	악성코드

연도	발생국	내용	비고
2013	한국 방송/금융 (방송/금융)	방송 및 금융 등 다수의 기업 전산망이 악성코드로 인한 시스템 파괴 등 장애 발생, PC 및 시스템 4만8천여 대 피해	악성코드
2014	일본 원자력 발전소 (원자력)	후쿠이현 몬주 핵발전소 내 관리자PC 바이러스 감염, 교육 훈련보고서, 조직변경의 홍보 메일 등 사내데이터 유출	악성코드
2014	한국수력원자력 (원자력)	e-메일 통한 악성코드 감염, 도면유출	악성코드
2014	독일 철강 (철강)	독일 철강회사의 용광로 제어시스템에 장애 발생	장애
2015	우크라이나 전력 (전력)	악성코드 인한 정전사태	악성코드

2.4. 주요 취약점

의도적 또는 비의도적인 행위로 주요 기반시설의 시스템 운영을 방해하는 활동에 대한 우려가 증대되고 있지만 현재의 파이어월, IDS (Intrusion Detection System), IPS (Intrusion Prevention System) 등의 ICT 보안 제품은 외부 네트워크 경계 영역에 집중되어 있어 내부 인트라넷인 산업제어시스템에서 발생되는 문제에 대하여는 적절한 대응에는 한계가 있다. 또한 내부자 위협을 포함하여 침투경로가 다양해지고 있는 상황에서 제어망의 경우에도 경계망 보안에 초점이 맞춰져 있어 내부 행위분석 방안이 미약하다.

제어시스템 및 프로토콜은 고유 프로토콜 기술로 기존 제어시스템 동작에 대한 공개 정보가 없었기 때문에 초기부터 해커의 침입에 대한 대책을 고려하지 않았다. 그리고 외부와 통신하지 않거나, 전용망 및 사설망을 사용하여 두 지점간의 통신을 사용하는 폐쇄적인 구조이기 때문에 기존에는 보안을 고려하지 않는 경향이 있었다.

산업제어시스템의 기술적 보안 취약점은 플랫폼과 네트워크와 같이 2가지 측면에서 분석 할 수 있다[1].

- 플랫폼의 취약성:
  - 보안취약점이 발견된 이후에도 운영체제 및 벤더 소프트웨어의 패치가 개발되지 않음
  - 운영체제 및 응용프로그램의 패치가 유지되지 않음
  - 전방위적 시험 없이 운영체제 및 응용프로그램의 패치가 구현됨
  - 기본 구성을 사용함
  - 필수적인 구성이 저장되지 않거나 백업되지 않음
  - 휴대용 장치의 보호되지 않은 데이터
  - 적절한 패스워드 정책의 부족
  - 패스워드를 사용하지 않음
  - 패스워드 노출
  - 부적절한 접근제어 방법 적용
  - 멀웨어 방어 소프트웨어의 미설치
  - 최신의 멀웨어 방어 소프트웨어 또는 정의 파일을 사용하지 않는 경우
  - 전방위적 시험 없이 구현된 멀웨어 방어 소프트웨어 사용

- 네트워크 취약성:
  - 네트워크의 보안구조가 빈약한 경우
  - 데이터 흐름제어를 적용하지 않은 경우
  - 빈약하게 구성된 보안장비의 사용
  - 네트워크 장비의 구성 파일을 저장 및 백업하지 않은 경우
  - 암호화하지 않은 패스워드 전송
  - 네트워크 장비에 계속 존재하는 패스워드
  - 부적절한 접근제어를 적용한 경우
  - 보안 경계가 정의되지 않은 경우
  - 방화벽이 설치되지 않았거나 부적절하게 구성된 경우
  - 제어네트워크에서 비 제어 트래픽을 사용한 경우
  - 제어네트워크가 아닌 영역에서 제어네트워크 서비스를 사용한 경우

Ⅲ. 산업제어시스템 보안 표준화

각 산업별로 특성을 갖으며 기술 발전을 해오던 제어시스템은 점점 규모도 방대하여지고 산업이나 사회에 중요한 역할을 담당하게 되면서 보안 사고에 대한 조치에 대한 필요성이 인식되고, 호환성과 상호운용성에 대한 인식이 높아지고 있다. 15년에서 20년 가까이 장비를 운용하게 되면 부품이나 장비를 교체하게 되는데 벤더가 사라진 경우에는 극단적인 경우에는 전 공정라인에 걸쳐 장비를 대치해야 하는 난감한 상황이 벌어질 수 있다. 이것은 보안 관점에서 뿐만 아니라 사업의 지속성 측면에서도 개선되어야 할 문제점이다. 만약 제어

시스템이 이러한 교체/패취 체계가 안 되어 있다면 지금부터라도 레거시망을 포함하여 제어시스템의 가용성을 보장하면서 보안 메커니즘 운용하는 정책을 계획하는 것이 필요하다.

산업제어시스템 관련 보안 표준은 산업제어시스템이 산업계에 존재해온 기간만큼의 역사성을 갖는다. 국제표준 보다는 산업계의 필요에 의한 사실적 표준단계로부터 시작되었으며, 이러한 표준이 국제표준기구에 상정(Transportation)되어 국제표준으로 격상된 표준의 예라 하겠다. 산업제어시스템 보안 관련 표준은 표 3에서 보는 것과 같이 크게 미국의 NIST와 IEC의 표준으로 대분될 수 있다. NIST의 SP 800-82 문서와 건강,안전, 환경을 보호하기 위하여 제어시스템에 대한 사이버 리스크를 약화하기 위한 ISA99 (IEC 62443)가 대표적인 표준이다.

〔표 3〕 국외 산업제어시스템 보안표준 목록

표준명	내용
AGA 12-1	Cryptographic Protection of SCADA Communications Part 1: Background, Policies and Test Plan
AGA 12-2	Cryptographic Protection of SCADA Communications Part 2: Retrofit Link Encryption for Asynchronous Serial Communications
ANSI/ISA-99	Security for Industrial Automation and Control SystemsTerminology, Concepts, and Models
FIPS 140-2	Security Requirements for Cryptographic Modules
CIDX	(This document was moved from Chemical Industry Data Exchange (CIDX) to the American ChCouncil in 2006) "Guidance for Addressing Cyber Security in the Chem
ISO 27001	This standard will be replaced by ISA 99, "Manufacturing and Control System Security, Part 2: Establishing a Manufacturing and Control System Security Program." Interna
ISO 27002	techniques - Information security management systems - Requirements," First edition, October 15, 2005.
IEC 62351	Power systems management and associated information exchange-Data and communications security
IEEE 1402	Guide for ElectriSubstation Physical and Electronic Security
ISA 99.00.01-2007	Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models
ISA 99.00.02-2007	Security for Industrial Automation and Control Part 2: Establishing n Industrial Automation and Control System Security Program
ISA 99.00.03-2007	Security for Industrial Automation and Control Part 2: Establishing n Industrial Automation and Control System Security Program
ISA 99.02.01-2009	Security for Industrial Automation and Control Part 3: Operating an Industrial Automation and Control System Security Program
NERC CIP	Establishing an Industrial Automation and Control Systems Security Program
NIST SP 800-40 R2	Creating a Patch and Vulnerability Management Program
NIST SP 800-53	Recommended Security Controls for Federal Information Systems-Information Security
NIST SP 800-61	Computer Security Incident Handling Guide
NIST SP 800-82	Guide to Industrial Control Systems (ICS) Security
NIST SP 800-83	Guide to Malware Incident Prevention and Handling
NIST SP 800-86	Guide to Integrating Forensic Techniques into Incident Response
NIST SP 800-92	Guide to Computer Security Log Management

NIST의 SP 800-82 문서는 SCADA와 DCS, 그리고 PLC와 같은 제어시스템에 대한 보안 지침을 제공하는 문서이다. SCADA는 중앙통제의 데이터 수집과 제

어관리를 이용하여 산재되어 있는 자산을 제어하는 시스템이고, DCS는 공장과 같이 근거리 지역의 생산시스템을 제어하며, PLC는 특정 응용이나 조정을 위한 독립장치의 제어에 사용된다. 본 문서는 산업제어시스템의 보안 목표로 가용성, 무결성 그리고 기밀성의 순서대로 우선순위를 설정한다. 그리고 산업제어시스템 구현을 위한 주된 보안 목표로서는 다음과 같은 것을 포함한다.

- 산업제어시스템의 네트워크와 네트워크 동작에 대한 논리적 접근을 제한
- 산업제어시스템의 네트워크와 장비에 대한 물리적 접근을 제한
- 산업제어시스템의 개별적 컴포넌트들을 공격으로부터 방어
- 부정적 조건에서 이웃하는 장비나 네트워크에 문제를 발생하지 않도록 기능을 관리
- 사고발생시 빠르게 시스템을 회복

NIST 800-82의 주된 보안 개념은 이러한 목표를 추구하면서, 네트워크를 분할 및 격리하여 심층방어 정책을 구축하는 것을 권고한다. 문서의 구성은 2절에 산업제어시스템의 개요와 보안을 위한 중요성과 합리성을 설명하며, 3절에 산업제어시스템과 IT간의 차이점과 위협, 취약점 그리고 사고에 대하여 설명하며, 4절에는 3절의 취약점과 연계된 리스크를 약화하기 위한 산업제어시스템 보안 프로그램을 설명하고, 5절에 네트워크 분할과 함께 네트워크 구조에 보안을 결합하는 것을 권고하고 있다[1].

ISA99 (IEC 62443) 표준은 ANSI에서 바로 채택이 될 수 있도록 양식과 규정을 준수하여 작성되었으며, 북미의 150 기업과 기관이 참여하여 작성 하였으며, IEC의 표준으로 부분적으로 표준화가 완료되었고, 또 진행중에 있다. ISA99 위원회가 어떤 목표로 표준화를 진행했는가를 이해하기 위해서는 위원회의 워킹그룹 구성을 살펴보는 것이 도움이 된다. 아래 표3은 산업제어시스템 보안을 기반으로 워킹그룹이 구성되었음을 보이고 있다.

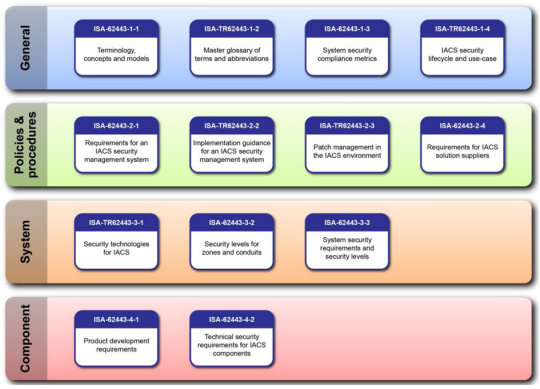
ISA-62443 산업표준 시리즈는 그림2와 같이 4개의 범주로 분류되어 개발되고 있다[3].

- 일반: 모든 시리즈의 근간이 되는 것이며 표준과 기술 보고서에 적용되는 용어 및 개념 정의 표준
- 정책과 절차: 사이버보안을 위한 정책과 절차의 조직적 측면의 표준
- 시스템: 시스템 설계와 능력(기능)을 포함하는 사이버 보안의 시스템 레벨의 기술적 측면의 표준
- 컴포넌트: 개발 프로세스와 컴포넌트 능력(기능)을 포함하는 컴포넌트 레벨의 기술적 측면의 표준

〔표 4〕 국외 산업제어시스템 보안표준 목록

이름	주제	내용
WG 1	Security technologies	Provides general guidance on the applicability of specific technology in the IACS environment
WG 2	Security Program Definition and Operation	Responsible for developing ISA-62443-2-1, Requirements for an IACS Security Management System, including alignment with ISO 27001
WG 3	Terminology, Concepts and Models	Responsible for developing ISA-62443-1-1, Terminology, Concepts and Models. This standard establishes the basis for the 62443 series.
WG 4	Technical Requirements	Responsible for several standards and reports in the ISA-62443 series that defined specific technical requirements for IACS security.
WG 5	Committee Leadership	Includes leaders of each active work group. Purpose is directing committee activities in support of the co-chairs.
WG 6	Patch Management	Provides guidance in the area of patch management in the form of technical report ISA-TR62443-2-3.
WG 7	Safety and Security	Establishes and maintains liaison relationships required for addressing issues at the intersection of IACS security and process

이름	주제	내용
		safety.
WG 8	Communications and Outreach	Primarily responsible for developing and delivering materials needed to educate and share news about committee activities.
WG 9	Wireless and Security	Establishes and maintains liaison relationships required for addressing issues at the intersection of IACS security and wireless communications.
WG 11	IACS Security for the Nuclear Sector	Provides specific guidance on matters related to cybersecurity in the nuclear sector.



〔그림 2〕 ISA-62443 표준 시리즈

Ⅳ. 결 론

본 논문에서는 산업제어시스템의 보안의 주요 이슈를 살펴보았다. 이미 독립적으로 구축이 된 제어네트워크를 현실적으로 최상의 보안 대책을 세우는 것은 풀기 쉽지 않은 난제에 속한다. 그러나 서비스와 제어의 질을 높이기 위하여 ICT의 기술을 융합화 하는 것이 추세이며, 이러한 추세에 따라 ICT의 보안 이슈가 전이되는 것은 당연한 결과로 인식되고 있다.

이러한 상황에서 모든 취약점을 동등한 보안수준으로 대책을 세우는 것은 비현실적으로 판단되며, 현재 일어나고 있는 사고와 관련하여, 즉 공격분석을 통한 보안 대책을 세움에 있어서, 악성코드에 의한 공격, 그리고 내부자에 의한 공격이 대부분을 차지하고 있음을 보안 사고 기록을 통하여 확인하였다.

이러한 분석의 결과 망분리 정책이 실현되었고, 이에 따른 장비들이 출시되어 있는 것은 대응이 현실적으로 잘 이루어지고 있다고 사료된다. 그리고 NIST SP 800-82 규격이나 IEC 62443 시리즈에서 레거시 망을 고려한 표준안이 제시가 되고 있으며, 요구되어지는 보안수준을 위하여 점진적 제어시스템이 진화하도록 기술적 내용들을 담아주고 있다는 것은 고무적인 것으로 판단되며, 가용성을 고려한 보안패치를 위한 구조와 메커니즘이 망분리 정책과 더불어 우선적으로 조치를 할 수 있는 기술로 주목받고 있다.

그러나 장비의 보안 패치가 이루어지지 않은 상태의 제로데이 공격이 산업제어 시스템에서는 아주 효과적인 공격 방법이 되고 있으므로, 가용성 보장을 위하여 장비의 정지가 제한적으로 허용되고 있는 상황에서 적시에 보안 패치가 이루어지지 않은 장비와 게이트웨이들이 존재하게 되는 운영상(정책상)의 문제점이 있다. 우선 경계에 접한 보안게이트웨이들의 보안수준을 유지하는 것이 급선무라고 판단이 되며, 독립 네트워크의 제어계의 장비들의 펌웨어를 가용성을 보장하면서 패치를 하는 방안에 대하여 기술과 표준 개발이 병행하여 진행되어야 할 공개 이슈라고 사료된다.

참 고 문 헌

[1] Guide to Industrial Control Systems (ICS) Security, June 2011, NIST SP 800-82.

[2] 차영태, 조병훈, 나중찬, 산업제어시스템 보안기술 동향과 산업전망, Vol. 13-6, 2013년.

[3] Security for industrial automation and control systems, Sep. 2012, IEC 62443.

〈저 자 소 개〉

나 재 훈 (Jae Hoon Nah)
종신회원

1985년 2월 : 중앙대학교 컴퓨터공학과 졸업
1987년 2월 : 중앙대학교 컴퓨터공학과 석사
2005년 2월 : 한국외국어대학교 정보공학 박사
1987년~현재 : 한국전자통신연구원 정보보호연구본부 전문위원/책임연구원
2009년~현재 : ITU-T SG17 Q7 Rapporteur
2011년~2012년 : 한국정보보호학회 학회지 편집위원장
<관심분야> CPS보안, IoT보안, P2P, IPTV, 웹메쉬업 보안

나 중 찬 (Jung Chan Na)
종신회원

1986년 2월 : 충남대학교 계산통계학과 학사
1989년 2월 : 숭실대학교 전자계산학과 석사
2004년 2월 : 충남대학교 컴퓨터과학과 박사
1989년2월~현재 : ETRI CPS보안연구실실장/책임연구원
<관심분야> 제어시스템보안, 펌웨어 보안 취약성