정 보 보 호 학 회 지
제24권 제5호, 2014. 10

산업제어시스템 보안성 평가·인증 동향 분석

손 경 호*

요 약

본 논문에서는 전력, 가스, 수도, 교통 시스템 등의 국가주요기반시설 및 산업분야에 널리 사용되는 산업제어시스템(ICS;Industrial Control System)에 대한 보안표준 및 보안요구사항을 살펴보고, 이를 충분히 만족하고 정확하게 구현되었음을 시험·평가를 통해 인증하는 평가·인증 체계에 대해 살펴본다. 특히 미국을 중심으로 활발히 진행 중인 ISASecure®EDSA 인증 프로그램에 대해 상세히 분석하고, 국내에 이를 적용하기 위한 방안에 대해 제안하고자 한다.

Ⅰ. 서 론

최근, 다양한 산업분야 및 우리의 실생활에 널리 사용되고 있는 산업제어시스템(ICS, Industrial Control System)는 제조, 발전, 가공 등의 산업시설 뿐만 아니라 전력, 자원운송 등 주요정보통신 기반시설 및 빌딩, 공항 등의 시설에 적용된 시스템을 말하며, 원격에 있는 설비를 제어하기 위해 설비 정보를 수집함과 동시에 제어 명령을 설비에 전달하는 기능을 가진다. 이런 산업제어시스템은 감시 제어 데이터 수집시스템이라고 불리는 SCADA(supervisory control and data acquisition systems), 분산 제어시스템인 DCS(Distributed control systems), PLC(Programmable Logic Controllers) 및 센서 등 다양한 구성요소 및 유형들로 이뤄져 있다.[1]

기존의 산업제어시스템들은 제어용 컴퓨터 내장기기와 독자적인 통신프로토콜이 적용되어 외부에서 분리 독립된 구성으로 구축·운영 되어 왔지만, 최근, ICS는 업무 효율화와 다양한 분야 적용을 위해 일반 업무용 시스템 망과 연계하기 위해 IT 및 인터넷 기술을 이용하게 되었으며, 이로 인해 ICS에도 범용 표준기술이 적용되고 개방화가 빠르게 진행되고 있다.[2]

이런 상황에서 기존 인터넷망에서의 보안 사고에 대한 위협이 산업제어시스템으로 확산되었고, 2010년 스턱스넷(Stuxnet) 공격이 발생됨에 따라 산업제어시스템의 정보보호에 대한 관심이 더 높아지고 있다.[3,4]

이런 추세와 더불어 미국을 중심으로 한 자동화표준단체인 ISA(International Society of Automation)는 ICS를 구성하는 제품 및 시스템의 보안요구사항을 정의하고 이를 표준으로 주도함과 동시에, ICS를 구성하는 SCADA, DCS, PLC 등의 장치에 대한 보안성을 시험·평가하고, ICS를 운영하는 조직의 정보보호 관리체계를 심사하는 ICS의 안전성을 확보하기 위한 ICS 평가인증 제도에 대한 개발을 본격화하고 있다.[5,6]

본 논문에서는 산업제어시스템(ICS)을 운영하는 조직에 대한 보안인증과 ICS 주요 구성요소에 대한 보안성 평가·인증 동향을 분석하고자 하며, 2장에서는 산업제어시스템과 관련된 보안표준 및 보안요구사항을 분석하고, 3장에서는 산업제어시스템에 대한 각국의 평가·인증 동향을 분석하고, 4장에서는 미국을 중심으로 활발히 진행중인 ICS 보안성 평가·인증제도인 ISASecure 프로그램을 상세히 분석한다. 결론으로는 향후 ICS 보안성 평가·인증에 대응하기 위한 대책을 논하고자 한다.

Ⅱ. 산업제어시스템 보안표준 및 보안요구사항

앞서 언급한 바와 같이 ICS에 대한 정보보호 필요성이 점차 증대됨에 따라 ICS의 보안솔루션 도입이 가속화 되었으며, 기존 보안솔루션을 ICS환경에 적합하도록 변경 및 적용한 새로운 ICS 보안솔루션이 필요하게 되었다. 이처럼 ICS 보안위협에 대응하기 위한 관리적, 기술적, 물리적 보안대책이 ICS에 구현되면서 기술적 수단에 대한 검증(Verification & Validation)과 관리적·

* 한국인터넷진흥원 정보보호산업단 (khson@kisa.or.kr)

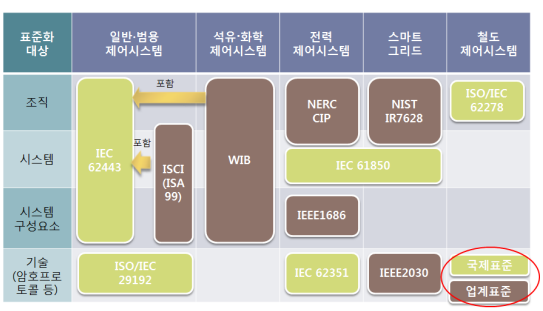
물리적 보안대책에 대한 정보보호 관리체계 운영에 대한 이슈가 발생하였다. 특히, 미국을 중심으로 ICS에 대한 정보보호 대책을 수립하고 구현하기 위해 ICS 보안기술 및 보안요구사항을 정립하고 이러한 보안요구사항을 충분하고 정확하게 구현하였는지 평가하여 ICS 구성요소에 대한 신뢰성을 보장하고자 하는 움직임이 활발하게 진행되고 있다.[7-10]

본장에서는 ICS 관련 보안표준 및 보안요구사항 들의 범위를 개괄적으로 살펴보고자 한다.

2.1. ICS 보안표준·요구사항 범위

지금까지 제안되고 있는 기준·표준·보안요구사항들은 범위(조직, 시스템, 장치·디바이스), 대책(운용·관리적 대책, 기술적 대책), 업종분야(범용, 각 업계 고유), 이용자(사업·운용자, 시스템개발자, 장치·디바이스 개발자) 등에 따라 차이를 보이고 있다.[11-17]

- IEC 62443 : INDUSTRIAL NETWORK AND SYSTEM SECURITY
- ISCI : ISA Security Compliance Institute Society Interest Group
- WIB :Werkgroep Instrument Beoorderling
- NERC CIP : North American Electric Reliability Corporation, Critical Infrastructure Protection Standards
- NIST IR7628 : Guidelines for Smart Grid Cyber Security
- ISO/IEC 62278 : Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS)
- ISO/IEC 29192 : Information technology- Security techniques-Lightweight cryptography
- IEC 61850 : design of electrical substation automation
- IEC 62351 : Security for Power systems management and associated information exchange
- IEEE 1686 : IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities
- IEEE 2030 : Smart Grid Interoperability Standards

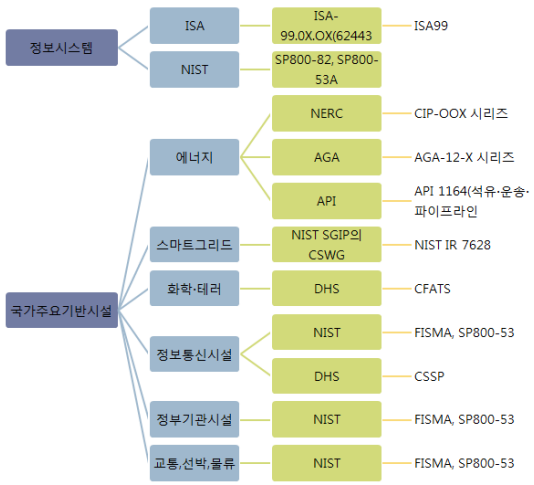


〔그림 1〕 ICS 보안 표준·보안요구사항 영역

특히, 미국 ISA의 표준기구인 ASCI(Automation Standards Compliance Institute) 산하에 ISCI(ISA Security Compliance Institute Society Interest Group)를 구성하고 ICS에 대한 보안이슈를 다루기 위해 ISA-99.0X.0X 시리즈를 개발하였다. ISA-99 시리즈는 ICS 환경에 적합하도록 보안요구사항 및 위험분석에 따른 보안대책을 특성화하여 업계표준으로 제정되었으며. ISA-99 시리즈가 IEC 표준문서의 토대가 됨에 따라 ISA-99시리즈 명칭을 ISA-62443로 변경하였다. 또한 국제 표준화 기구인 IEC TC65/WG10은 ISA 99시리즈를 토대로 ICS에 대한 보안기술 및 보안관리 체계를 국제 표준화하였다. 다만 ISA 99표준은 조직에 대한 정보보호에 관한 이슈를 다루지 못하였기 때문에 IEC TC65/WG10은 네덜란드 정유업체 단체가 제정하여 유럽 업계표준인 WIB 시리즈 중에서 조직에 대한 정보보호 내용을 참고하여 이에 대한 국제표준 (IEC62443) 초안을 마련하였다. 또한, 미국 NIST는 SP800-82에서 ICS 기본개념 및 구성요소에 대해 정의하고, 이들에 대한 정보보호 개념을 IT정보보호 기술과 비교하면서 IT 전문가들이 ICS를 이해할 수 있도록 가이드를 제시하고 있다.

특히, 국가주요 기반시설의 정보보호관련 표준 중 에너지와 관련된 북미 전기안전협회(NERC, North American Electric Reliability Corporation)가 제정한 CIP(Critical Infrastructure Protection Standards) 표준과 석유·운송·파이프라인 관련 API Standard 1164(Pipeline SCADA Security, Second Edition) 표준이 많이 활용되고 있다. 전력(스마트그리드)과 관련된 분야에서는 SGIP-CSWG (Smart Grid Interoperability Panel-Cyber Security Working Group)에서 2010년 8월에 NISTIR 7628을 발표하였다.

이외에도 미국은 아래 그림과 같이 국가 주요 기반시설의 정보보호를 위해 다양한 주체별로 보안요구사항을

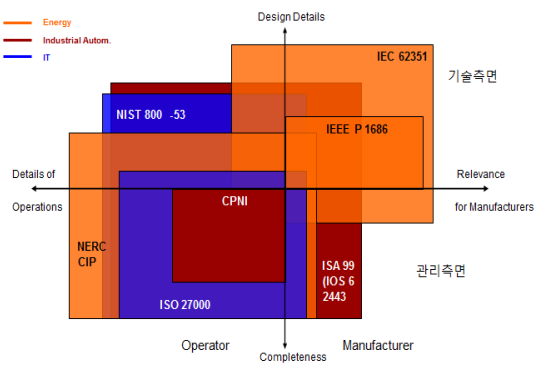


〔그림 2〕 미국 ICS 응용분야별 보안표준 추진기관

개발하고 있다.

ICS 표준의 범위와 관련해서 EU의 ESCoRTS(A European network for the Security of Control & Real Time Systems) 프로젝트[18]에서 다양한 ICS 보안기준 레벨과 각 해당 주체(이용자) 위치를 개념적으로 IT 정보보호 관련 표준 범위와 ICS 표준 범위를 기술, 관리, 운용, 제조 측면에서 분석한 것이다. [그림 3]에서 보면, ICS 정보보호 관련 표준화는 일반 IT 시스템의 정보보호 관리체계를 구축하여 이를 심사하는 ISMS (ISO27000) 체계와 유사한 방향으로 나아가고 있다. 하지만 ICS는 IT와 다르게 정보보호 기본요소 중에서 가용성을 제일 중요하게 여기고 있으며 실시간성과 업무 연속성 보장이 그 무엇보다도 중요시된다. 이러한 ICS 특성을 반영하여 IT 정보보호 기술 및 보안요구사항을 ICS에 적합하도록 수정·보완하여 표준안을 마련하고 있다. 특히, IEC 62443은 IT 시스템 운영조직에 대한 정보보호 관리체계를 정의하고 있는 ISO 27000을 포괄하고 있으며, 정보보호 관리체계 구축에 필요한 정보보호 대책을 정의하는 NIST 800-53을 어느 정도 포괄하고 있음을 보여준다.

그리고, IEC 62443은 범위, 이용, 분야측면에서 포괄적인 보안표준을 담고 있음을 보여준다.[19-21]



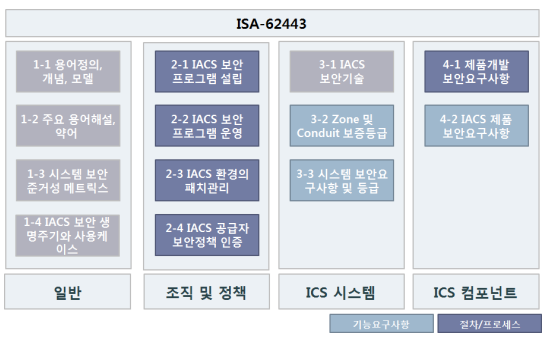
〔그림 3〕 ICS 보안표준 범위(출처:ESCoRTS)

2.2. ISA-62443(IEC62443)

앞서 언급한바와 같이 기존 IT시스템과 달리 ICS의 보안목표는 감시제어 시스템의 가용성, 현장설비 및 장치 보호, 현장 작업운영 지속, 실시간 대응 등이다. IT는 물리적 자산 보다는 정보자산 보호에 중점을 두고 있으나 ICS는 현장 설비 등 물리적 자산 보호에 정보보호 중점을 두고 있다. 이러한 보안목표의 차이점은 보안목적으로 이어져 이를 만족시키기 위한 정보보호 대책 및 보안요구사항 정의를 ICS 환경에 맞게 변경할 필요성이 생겼다. 이에 ISA는 IT 정보보호 관련 표준을 토대로 ICS 정보보호를 위한 ISA 62443 표준을 개발하였다. ISA-62443은 4개 Part로 구성되어 있으며, 각 Part는 다시 세부 주제로 나누어서 사이버보안 준거성 점검을 위한 매트릭스를 정의한 기술규격을 정의하고 있다.

좀더 상세히 살펴보면, ISA 62443-1-1,2은 전체 ISA 62443의 요약본으로 전체 문서시리즈에서 사용되고 있는 용어에 대해 정의하고 있다. 기본 개념으로 Security Aspect, 보안프로그램의 성숙도, 모델, 시스템 정의, 기본요구사항, 시스템 세분화, 보안등급, 보안 생명주기 등을 다루고 있다. 각 이슈별로 다루고 있는 세부 주제는 다음과 같다.

· Security Aspect : 인력, 프로세스, 기술

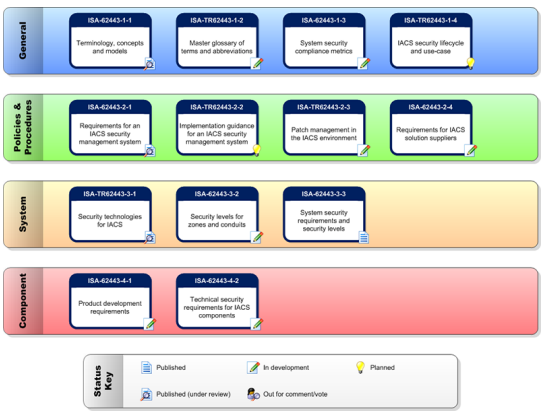


〔그림 4〕 ISA-62443 구성

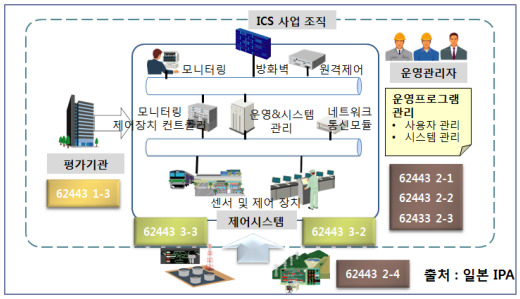
- 보안프로그램 성숙도 : 개념, 기능분석, 구현, 운영, 재활용 및 폐기
- 모델 : 참조모델, 물리적 구조
- 시스템 정의 : 기능관점, 시스템 및 인터페이스 관점, 제조 활동 관점, 자산 관점
- 기본요구사항 : 식별 및 인증, 접근통제, 무결성, 암호, 데이터 흐름통제, 실시간 대응, 가용성
- 시스템 세분화 : zone, conduit, channel
- 보안등급 : 3등급 보안체계
- 보안 생명주기 : 자산분석 단계, 개발 및 구현 단계, 유지관리 단계 등

ISA 62443-1-3은 표준 정합성 점검, ICS 제품 및 서비스에 대한 안전한 개발 요구사항 준수, 서비스 생명주기 동안에 걸친 품질에 대한 모니터링 및 관리 점검, ICS 서브시스템 또는 컴포넌트가 제거되었을 때 시스템 폐기 요구사항 준수 점검, 평가인증 기관에서 활용할 수 있는 ICS 보안성 측정 등의 목적으로 활용하도록 하였다. ISA 62443-2는 ICS를 운영하는 사업자가 갖추어야 하는 보안정책, 보안조직, 자산관리, 인력관리, 물리적 보안, 통신·운영관리, 접근통제, 정보시스템 생명주기, 보안사고 대응, 사업연속성, 준거성 등 보안관리체계(CSMS, ICS System Management System)에 대해 62443-2-1, 62443-2-2, 62443-2-3에서 요구사항을 정의하고 있으며, ICS 운영 사업자에게 ICS 구성요소 또는 시스템 제공자들이 제품 또는 시스템 개발생명주기에서 준수해야 할 사항은 62443-2-4에서 정의하고 있다.

ISA 62443-3은 ICS 시스템에 대한 인증, 접근통제 암호, 로그감사, ICS SW 보안, 물리적 보안에 보안기술



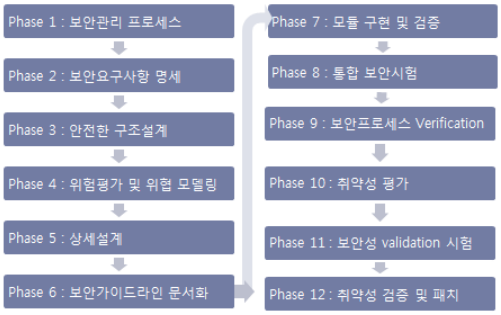
〔그림 5〕 ISA/IEC 62443 표준(출처:http://isa99.isa.org)



〔그림 6〕 ICS 구성도에서 ISA 62443 Positioning

및 보안요구사항을 설명하고 있으며, 이들 요구사항의 각 등급에 대해 기술하고 있다.

ISA 62443-4-1는 제품 개발 단계(12단계)에서의 보안요구사항을 기술하고 있으며, ISA 62443-4-2는 7개의 보안카테고리(식별 및 인증, 이용통제, 시스템 무결성, 데이터 비밀성, 제한된 데이터 흐름, 이벤트 응답시간, 자원 가용성)와 52개의 상세 요구사항을 담고 있고, 응용, 임베디드 디바이스, 호스트 디바이스, 네트워크 컴포넌트 등에 악성코드 보호를 위한 추가요구사항을 기술하고 있다.



〔그림 7〕 ISA-62443-4 단계별 보안요구사항 주요내용

Ⅲ. ICS 정보보호 평가·인증 동향

본 장에서는 ICS을 구성하는 제품 또는 시스템이 보안요구사항이나 관련 표준을 만족하고 있으며 정확하게 구현되어 있음을 시험·평가하고 이를 인증하는 평가인증 체계에 대해 살펴본다. ICS 정보보호 평가인증 제도는 미국 ISA의 ISASecure 프로그램, 네덜란드의 WIB, 캐나다 Archilles 등이 있다. 또한, 미국 NIST에서는 CC(ISO/IEC 15408) 기준에 따른 보호프로파일(PP;Protection Profile) 개발 동향에 대해 살펴본다.

〔표 1〕 ICS관련 보안성 평가인증 제도 비교

평가·인증제도	ISASecure Program	WIB	Achiles
인증 대상	ICS System : SAA ICS Device : EDSA	ICS System	ICS Device
기준 성격	단체표준 (IEC 국제표준에 반영)	단체표준 (IEC 62443-2-4에 반영)	단체표준
주관 기관	미국 ISCI	네덜란드 석유 관련 기업단체	캐나다 Wurldtech사
인증 효력 지역	미국	유럽	전세계

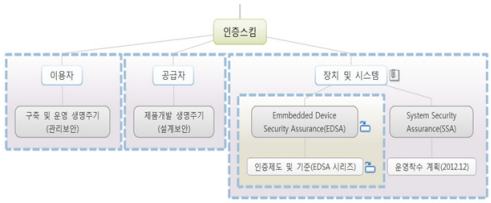
3.1. 미국 ISASecure 프로그램

미국 ISA의 ASCI(Automation Standards Compliance Institute)는 ICS 평가인증 스킴 문서 개발, 평가인증 제도 설립, 평가기관 인정 제도 마련 등 ICS 평가인증에 필요한 작업을 진행하고 있다.

ISASecure 프로그램은 ICS 운영에 참여하는 개체를 이용자, 공급자, 장치 및 시스템 등으로 구분하고 개체의 특성을 고려한 평가인증 제도를 개별적으로 개발하려는 계획을 가졌다. 이중에서 장치 및 시스템 평가인증 제도 개발에 먼저 착수하였고, ICS 장치에 대한 평가인증 제도 “EDSA(Embedded Device Security Assurance)”와 ICS에 대한 시스템레벨에서의 평가인증제 “SSA(System Security Assurance)”으로 평가인증 체계를 이원화하였다.

ISCI는 2008년 부터 EDSA 평가인증 스킴 개발에 착수하여 2009년에 EDSA 프레임워크를 개발하였으며, EDSA 프레임워크에는 ISA Secure 시험규격 범위 뿐만 아니라, 장치를 시험하기 위한 시험 전략과 시험 성공/실패를 결정할 수 있는 기준도 포함되어 있다. 이를 토대로 2010년 4월에 “EDSA 2010.1” 평가기준을 발표하였고, 2010년 11월에 ISCI는 ‘Exida’와 시범 평가를 수행해서 인정기관인 ANSI(American National Standas Institute)로 부터 Exida는 평가인증 기관으로 인정을 받았다.

2011년 부터 EDSA 인증을 시작하였으며, SSA 인증은 2012년 12월 착수를 목표로 작업을 진행하였으나, 현재까지 실질적인 인증은 시작하고 있지 않다.[22]



〔그림 8〕 ISASecurity Program 개요

3.2. 네덜란드 WIB

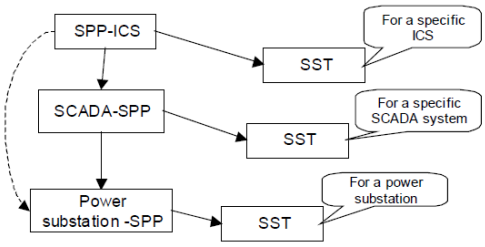
네덜란드 WIB는 1962년에 유럽 석유·화학 플랜트 관련 민간단체가 주도해 구성한 단체로 현재, 전세계 75개 이상의 회원사가 포함되어 있다. WIB는 2010년 11월에 ICS의 시스템에 대한 보안요구사항을 정의한 WIB V2.0을 개발해 발표하였다. 50개의 업체가 참여한 Plant Security WG에서 개발하였으며 현재 유럽 단체표준으로 활용되고 있다. 보안요구사항은 총 272개로 구성되어 있고, 3등급 체계로 구성되어 있다. Bronze는 148개 요구사항, Silver는 218개 요구사항, Gold는 272개 요구사항을 만족해야 인증을 받을 수 있다. 이중에서 조직에 관한 보안요구사항은 ISO/IEC 62443-2-4에 반영되었다. 보안요구사항에 대한 상세 내용은 2010년 10월에 발표된 “WIBReport:M2784-X-1050.1 – ver2.0”을 통해 공개하였다. 이 기준은 총 35개의 절차영역(PA; Process Areas)이 있으며, 조직, 시스템 능력, 시스템수용 시험과 허용, 관리와 지원 PA로 나눠져 있다.

3.3. 캐나다 Achilles

캐나다의 Wurldtech사는 WIB가 2010년에 발표한 ICS 시스템 평가기준을 확장하여 ICS 장치에 대한 평가기준을 개발하였다. 이러한 기준을 기반으로 ICS 장치를 인증하는 Achilles Practices Certification을 운영하고 있다. Achilles Practices Certification은 제조업체의 사이버 보안 절차, 실무지침, 개발, 시험, 유지관리 등 시스템 생명주기 전반에 걸친 모범사례로 구성되어 있다. 인증 등급은 Gold, Silver, Bronze로 나눠 인증마크를 부여하고 있다. 현재 5개 제품이 인증을 받았다.[23]

3.4. 미국 NIST ICS-PP

앞서 말한 ISASecurity 프로그램은 업계가 중심이 되



〔그림 9〕 SPP-ICS와 관련 PP/ST개발 관계

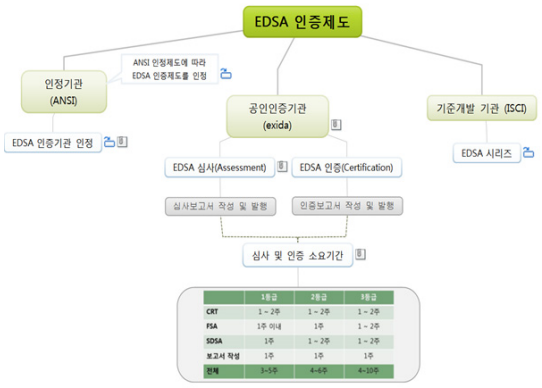
어 개발된 평가·인증 프로그램으로 미국정부에서는 ICS에 대한 보안성 평가를 위해 다양한 시도가 이뤄졌었다. 특히, NIST(National Institute of Standards and Technology)의 후원으로 NIST-PCSRF(Process Control Security Requirements Forum)에서 “System Protection Profile -Industrial Control Systems Version 1.0”을 개발하였다. SPP는 ICS의 보안 요구사항을 기술하기 위해 CC(ISO/IEC 15408)에 기반으로 작성하였다.

SPP는 일반적인 산업 통제 시스템에 적용될 최소한의 보안 요구사항들을 문서화하였다. 특정 ICS가 요구되는 일련의 보안 요구사항을 준수해야 할 경우 SPP를 기본으로 하고, SST를 만들어 구체적인 산업 요구 사항을 기술해야 한다. 또한, SCADA, DCS에 관련된 시스템 PP를 만들었으며, 세부 디바이스에 대한 컴포넌트 PP 개발을 추진하였다. 그러나 현재, 세부 PP개발은 중단된 상태이다.[24]

Ⅳ. ISASecure®EDSA 인증

ISA의 ISCI는 직접 평가를 하는 대신 제3의 평가기관을 인정하는 스킴을 개발해서 일정 수준의 능력을 가진 기관이 평가를 할 수 있도록 평가기관 인정 및 평가도구를 개발할 수 있도록 필요한 최소 요구사항을 정립하였다. 또한 ISA99 기준에 따른 인증 프로그램을 EDSA(Embedded Device Security Assurance)로 명명하고, 이를 위해 ISCI는 2010년 9월에 평가기관 인정 및 운영에 관한 “EDSA-200, Chartered Laboratory Operation and Accreditation specification”와 통신 안전성 시험 도구 공식 승인에 관한 “EDSA-201, Recognition Process for Communication Robustness Testing(CRT) Tools specification”을 발표하였다.

EDSA-200은 EDSA 평가인증 제도의 평가인증 기관으로 인정받으려는 시험 기관에게 상세정보를 제공하



〔그림 10〕 EDSA 인증제도

며, EDSA-201은 EDSA 평가에 사용될 시험도구로 공식 승인받고자 하는 개발 업체에게 상세 정보를 제공한다. 또한, ISCI는 같은 시기에 EDSA 평가인증 제도의 최상위 문서로서, ISASecure EDSA 평가인증 제도 운영의 전반적인 사항을 규정한 “EDSA-100, Certification Scheme document”를 공개하였다. EDSA 100에는 EDSA 평가인증 제도에 관한 개요, 평가인증 기관 인정에 관한 사항, 시험도구 공식 승인에 관한 사항을 요약하여 명시하고 있다. ICS 구성요소로 ICS 시스템에 내장되는 장치에 대한 평가기준은 “EDSA 300 ISASecure Certification Requirements”에 정의되어 있다. EDSA 평가·인증 조직구성 및 역할은 아래와 같다.

- 최종 이용자 : Embedded deivice에 대한 조달기준 정의, EDSA 인증 요구, 특정 등급 요구
- 장치 개발업체 : ICS 장치 개발업체 또는 공급업체로서 EDSA 평가 신청기관
- 평가인증 기관(Chartered Laboratories) : 장치 개발업체의 평가·인증신청을 접수받아, 장치를 평가하고 인증하는 기관
- CRT 시험기관 : CRT 요구사항에 대한 장치의 통신프로토콜 취약성 시험을 수행하여 평가제출물의 일환으로 평가인증기관으로 시험 결과서를 제출
- CRT 시험도구 제공업체 : 평가·인증기관 또는 CRT 시험기관이 CRT 시험을 수행할 수 있도록 시험도구를 제공하는 기관으로서 장치 개발업체들은 평가인증을 신청하기 전에 미지 CRT 시험도구를 이용하여 시험을 수행할 수 있음
- ISCI : ISASecure EDSA 인증스킴 개발 및 유지관리,

CRT 도구 상호인정 승인, EDSA 규격 해석, 인증제품 목록 공개용 웹사이트 운영

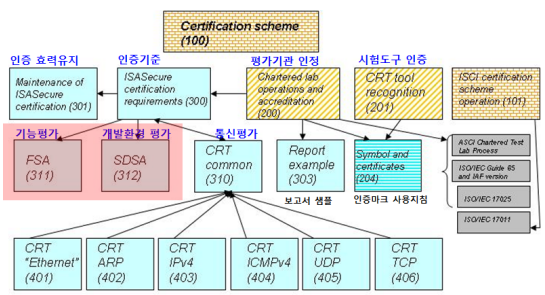
- EDSA 인정기관 : ANSI 인정기준에 따라 EDSA 평가 인증 기관으로 신청한 기관에 대해 자격을 평가하고 인정 여부를 결정

4.1. EDSA 인증매뉴얼 및 평가기준

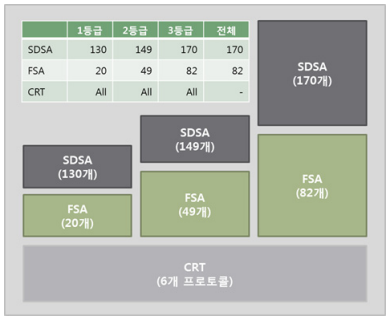
ISASecure®EDSA 인증은 ICS 임베디드 장치에 대해 안전한 물리레벨(Safety Integrity Level) 인증인 ISO/IEC 61508과 유사한 형태를 지니고 있다. EDSA 인증은 세부 3가지 인증으로 구성되어 있으며, ICS 구성장치에 대한 기능성에 대한 보안평가인 (FSA; Functional Security Assessment)와, ICS 장치 개발생명주기 동안 따라야할 소프트웨어 개발 보안 평가 (SDSA;Software Development Security Assessment). 그리고, 기기의 통신 강인도 테스트 (CRT; Communication robustness testing)를 만족하는지를 평가한다.

상세 기준과 관련해 EDSA-100,101은 EDSA 평가인증 제도 운영에 관한 전반적인 사항을 정의한 최상위 정책서이고, EDSA-200 시리즈는 평가인증 체계를 구성하는 기관으로 EDSA 평가인증 기관, CRT 시험기관 등을 승인하고 이들을 운영·관리하는 사항과 이들 기관이 사용하는 인증마크에 대한 사용지침을 정의한 제도 운영에 관한 문서이다.

EDSA-300 시리즈는 EDSA 평가대상 제품을 평가하는데 기준으로 사용하는 평가등급 및 세부 보안기능요구사항을 정의한 평가기술에 관한 문서이다. 마지막으로 EDSA-400 시리즈는 EDSA 평가대상 제품의 통신 프로토콜 취약성을 시험하기 위해 OSI 참조모델의 네트워크 계층에 해당하는 통신프로토콜 6종(Ethernet, ARP, IPv4, ICMP, UDP, TCP)에 대한 시험 규격을 정



〔그림 11〕 ISASecure EDSA 인증스킴 문서체계



〔그림 12〕 EDSA 평가등급 체계

의한 문서이다. 향후 다른 통신프로토콜에 대한 EDSA CRT 시험규격은 추가로 제정할 예정이다.

EDSA는 3등급 체계를 가지고 있으며 1등급에서 3등급으로 보안등급이 올라갈수록 SDSA 요구사항 및 FSA 요구사항 개수가 증가한다. 하지만 CRT는 모든 등급에 대해 동일한 수준으로 평가된다. 1등급 평가기간은 3-5주, 2등급 평가기간은 4~6주, 3등급 평가기간은 4~10주 정도 소요된다. 다음은 평가등급 체계를 도식화한 것이다.

또한, EDSA 평가 대상은 다음과 같다.

- Programmable Logic Controller(PLC)
- Distributed Control System(DCS) Controller
- Safety Logic Solver
- Programmable Automation Controller
- Intelligent Electronic Device(IED)
- SCADA Controller
- Remote Terminal Unit(RTU) 등

평가 신청기관은 신청 등급에 따라 EDSA-301, EDSA-310, EDSA-400 시리즈, EDSA-311, EDSA-312에 명세된 요구사항을 만족시킴을 입증할 수 있는 기술문서와 인증자가 추가로 요청한 기술문서를 제출해야 한다.

4.2. FSA : EDSA-311

FSA(Functional Security Assessment)는 ICS 장치의 구현 오류를 검사하기 위해 보안기능 요구사항이 목표로 하는 보안수준으로 구현되었는지 평가(특정보안기능요구사항을 충족하지 평가)하는 보안기능 평가로,

7개의 카테고리와 83개의 세부 요구사항을 담고 있다. 또한, SDSA와 같이 보안수준에 따라 충족해야할 요구사항이 다르다. 특히 할 점은 요구사항 충족여부에 대해 '할당가능(Allocatable)' 개념을 둬, 요구사항 중 일부가 평가대상 장치 주변 장치 에서 실현 될 수 있음[EDSA-200 3.1.4]을 허용하고 있다. 세부 보안기능요구사항은 NIST 800-53의 정보보호 통제항목과 IEC 62443-1에 정의된 기능요구사항을 토대로 정의되었다.

4.3. SDSA : EDSA-312

소프트웨어 개발 보안평가인 SDSA(Software Development Security Assessment)는 제어시스템 개발업체가 S/W 개발 및 유지보수 단계에서의 체계적인 설계 오류를 탐지하고 방지하기 위한 보안 요구사항을 만족하는지를 평가한다.

SDSA는 제품개발 프로세스가 안전하게 이뤄지고 있는지를 검사하는 것으로 12개의 활동 단계와 각 단계에 대한 169개의 세부 요구사항으로 이뤄져 있으며, 보안수준에 따라 충족해야할 요구사항이 다르다. 소프트웨어 개발 프로세서는 V-Model을 적용하고 있다. 또한, ISO/IEC 15408(CC:Common Criteria)과 IEC 61508 요구사항을 기본으로 다음과 같은 생명주기 단계별로 요구사항을 정의하고 있다. ISO/IEC 15408은 정보보호 기능을 갖는 IT시스템의 안전성과 신뢰성을 보증하기 위한 보안기능요구사항과 보증요구사항을 정의하는 평가기준이다. IEC 61508은 전기/전자 안전 시스템 및 프로그래밍이 가능한 안전시스템에 대한 기능의 안전성을 16단계로 세분화된 생명주기에 따라 정의한 국제표준이다.

ISO/IEC 15408 중에서 생명주기 정의를 다루는 ALC_LCD, 개발도구 관리에 관한 사항을 다루는 ALC_TAT, 개발환경의 보안관리 대책을 다루는 ALC_DVS, 형상관리체계를 다루는 ALC_CMC, 형상관리 범위를 다루는 ALC_CMS 등 보증클래스와 평가대상제품의 소개를 다루는 ASE_INT, 위협 모델링을 다루는 ASE_SPD, 보안요구사항을 정의하는 ASE_REQ 등 보안목표명세서에 관한 보증클래스를 참조하고 있다. 이외에도 기본설계 및 상세설계를 다루는 ADV_TDS, 인터페이스 명세를 다루는 ADV_FSP와 시험 범위를 분석하는 ATE_COV 등을 참조하고 있다.

4.4. CRT : EDSA-313

'CRT(Communication robustness testing)'는 기기의 강인도(Robustness) 시험을 통해 잘못된 형태의 메시지를 보내는 등의 취약점을 찾기 위한 시험으로 IP 기반 프로토콜을 구현하고 있는 ICS 장치에 대한 보안성을 시험하기 위한 요구사항을 정의하고 있다.

EDSA-400에 기반한 보안성 시험의 목적은 구현 정확성 및 표준 적합성을 시험하기 위한 것이 아니라, 네트워크 프로토콜에 대한 잘 알려진 서비스 거부공격 등에 내성을 가지고 있는지 확인하고 프로그래밍 오류를 포함하고 있지 않는지 확인하기 위함이다. 악성코드 유입 위험성에 대한 사항은 SDSA 평가에서 확인된다. EDSA-400에는 시험 도구 및 시험 절차에 관한 요구사항도 포함하고 있다.

현재 시험대상 통신 프로토콜은 그룹1의 6개(Ethernet, ARP, IPv4, ICMP, UDP, TCP)로 향후 계속 추가될 예정이다. 향후, 그룹2(BOOTP, DHCP, DNS, NTP, SNTP, FTP, HTTP, SNMP, Telnet), 그룹3(HTTPS, TLS, Modbus), 그룹4(OPC, IPv6 등), 그룹5(MMS, SSH 등)도 제공될 예정이다.

외부 인터페이스 시험은 다음과 같은 2가지 목적을 위해 수행하는 것이다.

- 평가대상 제품에서 활성화 되어 있는 포트 및 서비스 식별. 핵심 프로토콜 시험에 기초자료로 활용
- 포트 스캔 동안 평가대상 제품에 있어 기본 서비스인지를 시험

또한, CRT를 위한 시험도구 인증에 대해서는 EDSA-201(Recognition process for communication robustness testing tools)에서 정의하고 있으며, 현재 아래와 같은 3개사의 제품이 인증을 받았다. ICS 디바이스 개발업체는 EDSA인증을 평가위해서는 아래 도구를 활용해 시험결과 값을 평가기관에 제출해야 한다.[25-27]

- Wurldtech사의 Achilles Test Platform
- Codenomicon사의 DEFENSICS
- FFRI사의 Raven for ICS/FFR Raven ES

또한, ISASecure는 ICS의 특별한 그룹을 평가하기 위한 SSA(System Security Assurance) 인증과 안전한 개발 생명주기 보증을 위한 SDLA (Security Development Lifecycle Assurance)을 추진 중에 있다.

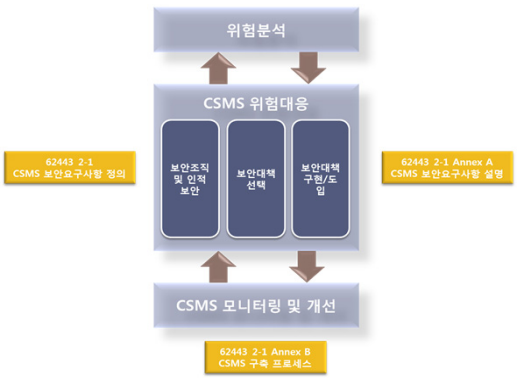
4.5. CSMS : ISASecure SSA

제품에 대한 인증제도인 EDSA와 더불어, ICS를 운영하는 사업자가 갖추어야 하는 보안요구사항에 대해 ICS 시스템 보안관리체계(CSMS, ICS System Management System) 인증체계를 수립 중에 있다. 아직 구체적인 인증 스킴은 발표되어 있지 않았으나, 관련 기준(IEC62443-2-1) 개발을 추진 중에 있다.

IEC 62443-2-1은 ICS 운영조직이 ISMS와 같은 CSMS를 구축하는데 참조할 수 있는 보안요구사항과 구축 프로세스를 명세하고 있다. 부록 A 및 부록 B에서 ICS 환경에서의 위협을 도출하여 위험을 분석하고 이에 따른 CSMS 보안요구사항을 정의하여 적절한 보안대책을 선택 및 도입하는 CSMS 구축 프로세스를 구체적으로 설명하고 있다. 다음 그림은 IEC 62443-2-1의 주요 골자이다.

IEC 62443-2-1는 ISMS(ISO/IEC 27001)와 같은 CSMS를 구축하는데 참조할 수 있는 보안요구사항과 구축 프로세스를 명세하고 있다.

IEC 62443-2-1과 ISO/IEC 27001의 통제항목을 명세하는 수준이 상이하여 일부 항목에 대해서는 한 개의 통제항목이 여러 통제항목으로 중복되는 경우가 있어 정확한 수치는 아니지만, IEC 62443-2-1는 총 126개의 통제항목이 있으며, 26개가 ISO/IEC 27001 통제



〔그림 13〕 IEC 62443-2-1 주요내용

〔표 2〕 IEC 62443-2-1과 ISO 27001 통제항목 개수 비교

	IEC 62443-2-1	ISO/IEC 27001
통제항목	126개	100개
고유 통제항목	26개	27개
공통 통제항목	100개	73개

항목과 상이하다.

〔표 3〕 IEC 62443-2-1 고유 통제항목

분류	통제항목	내용
위험분석, 분류 위험평가	ICS 네트워크 기본 구성도	위험평가 대상 자산을 식별하기 위해 조직은 ICS를 구성하는 시스템, 장치, 네트워크 및 보안장비 등의 기본 구성도를 작성해야 한다.
	물리적 자산에 대한 위험평가 결과, 사람의 생명안전에 대한 위험평가, 사이버보안에 대한 위험평가 결과 통합	자산에 대한 전체적인 위험을 파악하기 위해서는 물리적 자산, 사람의 생명안전, 논리적 자산의 위험평가 결과를 통합해야 한다.
	ICS 생명주기 전반에 걸친 위험평가 수행	개발, 구축, 변경 및 폐기 등 전체 생명주기의 모든 단계에 대해 위험평가를 수행해야 한다.
정보보호 대책	물리적 보안 및 사이버 보안 대책 수립	자산을 보호하기 위한 물리적 보호과 사이버 보안 대책을 수립하여 정보보호 정책 및 절차에 반영하여야 한다.
	중요자산의 우선순위 설정	예를 들어 화재, 침수, 사이버 보안사고, 서비스 중단, 천재지변 등으로 인해 ICS 운용이 중단된 경우 우선적으로 보호해야 하는 ICS 구성요소의 순위를 정해야 한다.
	계정 정지 또는 삭제	직무변경으로 인해 불필요한 계정은 즉시 정지 또는 삭제하여야 한다.
	시스템 관리자 등 중요 이용자에 대한 강화된 인증방법 적용	모든 시스템 관리자 및 응용프로그램 환경설정 관리자을 인증하는 경우 강한 패스워드와 같은 강화된 방법을 적용해야 한다.
	ICS 장치에 대한 물리적 또는 논리적 접근 허용 규칙 설정	ICS 장치에 대한 접근 허가는 논리적 접근통제(역할 기반 접근통제) 및/또는 물리적 접근통제(CCTV 등)를 해야 한다.

분류	통제항목	내용
정보보호 대책 구축	시스템 개발, 변경 및 유지보수에 대한 정보보호 정책 적용	ICS 기존 환경에 신규 시스템을 도입하는 경우 신규 시스템의 보안기능요구사항은 기존의 정보보호 정책 및 지침에 부합해야 한다. 또한 유지 보수를 위한 업그레이드, 변경을 하는 경우에도 마찬가이지다.
	정보보호 정책 및 절차 검토 및 유지관리	시스템 변경에 따른 보안영향 분석을 통해 사업 연속성을 보장할 수 있도록 정보보호 정책 및 절차를 검토하여 최신 상태로 유지해야 한다.
	사이버 보안사고 대응 계획 전파	사이버 보안사고 대응계획은 관련 부서 모두에게 전달되어야 한다.
	보안사고 대응 및 해결	발견된 보안사고 처리 및 대응방안 마련을 위한 조직이 있어야 한다.

현재, CSMS(62443-2-1) 인증체계 구축과 관련해서 ISA와 협력으로 일본 IPA에서 자국내 CSMS 인증제도 마련 및 구축을 위해 국제표준화 준비 등 다양한 사업을 추진중에 있다.[28,29]

Ⅴ. 결 론

본 논문에서는 ICS(산업제어시스템)에 대한 각국의 보안성 평가·인증 동향을 분석을 하였으며, 특히, 미국을 중심으로 진행 중인 ICS 보안 평가·인증 제도에 대해 알아보았다. 이런 세계적인 추세와 더불어 향후 국내에서 이에 대응하기 위한 다양한 노력이 필요할 것으로 예상된다. 이를 위해 향후 아래와 같은 연구가 필요할 것으로 예상된다.

(1) ICS 보안관리 인증체계(CSMS) 구축검토
- ISMS 인증제도와 유사한 형태의 CSMS 인증체계 구축 검토
- ISMS와 CSMS 인증 병행운영 방안 검토
- CSMS 인증 획득에 대한 인센티브(정부조달 조건, 시범사업 지원 등) 마련

(2) ICS장비 인증(EDSA) 대응방안 수립
- EDSA 보안기준 분석을 통해 국내 ICS디바이스 개발 업체에 인증 취득을 위한 기술지원
- 국내 인증체계(평가·인증기관 및 스킴) 구축 및 ISA(ISCI)와 상호인증 추진

(3) 주요정보통신기반시설 내 제어시스템의 취약점점검 및 모의해킹 항목 추가
- 프로토콜 시험인 CRT 및 EDSA 장치의 보안기능 시험항목 추가
- ICS 시스템의 구성요소 평가 및 인증(시스템 평가)을 위한 방안 마련

(4) 실증시설(테스트베드) 확대 구축 및 인력양성
- KISA에서 운영중인 제어시스템 테스트베드 확대 구축·운영
- ICS 보안사고 매뉴얼개발 및 정보공유 체계마련
- ICS 보안사고 대응훈련 방안 마련
- ICS 정보보호대책의 효과 검증
- ICS 융합 보안 전문인력 양성

(5) 시험 도구 및 평가기술 개발
- ICS 보안성 평가기술 개발 : 보안성 검증 패턴정보, 시험도구, 프로토콜별 시험 시나리오, 운영환경별 시험 시나리오 등
- ICS 시험도구 개발 : 통신프로토콜 취약성 시험, 보안기능 시험
- EDSA의 CRT 시험도구 인증 추진

(6) 국제 표준개발 참여 및 가이드라인 개발
- ICS 사이버보안을 위한 신규 표준 아이템 도출 및 제안
- ICS 보안관련 국제표준에 기초한 ICS 보안 가이드라인 개발 및 배포 : 공통 가이드라인, ICS 응용 분야별 세부 가이드라인 개발

참 고 문 헌

[1] NIST SP800-82, “Guide to Industrial Control System Security,” National Institute of Standards and Technology, 2011.

[2] Y.-T. Cha, B.-H. Cho, and J.-C. Na, “Security Technology Trends and Prospective of Industrial Control System,”. KEIT PD Issue Report, vol. 13-6, pp. 79-100, 2013.

[3] Falliere, Nicolas, Liam O. Murchu, and Eric Chien. “W32. stuxnet dossier.” White paper, Symantec Corp., Security Response (2011).
[4] A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke, “SCADA Security in the light of Cyber- Warfare,” Computer & Security, pp.418-436, 2012.
[5] ANSI/ISA-99.02.01-2009 standard, Security for Industrial Automation and Control Systems Part 2: Establishing an Industrial Automation and Control Systems Security Program (2009), https://www.isa.org/isa99/
[6] http://isa99.isa.org/ISA99%20Wiki/Home.aspx
[7] A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke, “SCADA Security in the light of Cyber- Warfare,” Computer & Security, pp. 418-436, 2012.
[8] Y.-H. Chen, “Introduction of Information Security for Industrial Control System,” Korea Institute of Information Security and Cryptology, vol. 19, no. 5, pp. 52-59, 2009.
[9] W.-S. Seo and M.-S. Jun, “A Direction of Convergence and Security of Smart Grid and Information Communication Network,” J. of the Korea Institute of Electronic Communication Sciences, vol. 5, no. 5, pp. 477-486, 2010.
[10] I.-S. Koo, K.-W. Kim, S.-B. Hong, G.-O. Park, and J.-Y. Park, “Digital Asset Analysis Methodology against Cyber Threat to I&C System in NPP,” J. of the Korea Institute of Electronic Communication Sciences, vol. 6, no. 6, pp. 839-847, 2011.
[11] [WIB] http://www.wib.nl/
[12] http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
[13] www.nist.gov/smartgrid/upload/nistir-7628_total.pdf
[14] http://webstore.iec.ch
[15] http://www.iso.org/
[16] http://www.iec.ch/smartgrid/standards/
[17] http://standards.ieee.org/
[18] http://cordis.europa.eu/project/rcn/87538_en.html
[19] ISO / IEC), International ISO / IEC Standard 27002:2005 (E), Information Technology－Security Techniques－ode of Practice for Information Security Management, first edition 2005-06-15.
[20] E. Humphreys, “Implementing the ISO / IEC 27001 information security management system standard,” Artech House, 2006.
[21] NIST SP800-53, “Recommended Security Controls for Federal Information System,” National Institute of Standards and Technology, 2012.
[22] http://www.isasecure.org/ISASecure-Program.aspx
[23] http://www.wurldtech.com
[24] “System Protection Profile-Industrial Control Systems”, NIST, Version 1, 2004.04
[25] Wurldtech사의 Achilles Test Platform, http://www.wurldtech.com/product_services/discover_analyze/achilles_test_plaform/
[26] Codenomicon사의 DEFENSICS, http://www.codenomicon.com/defensics/
[27] FFRI사의 Raven for ICS/FFR Raven ES, http://www.ffri.jp/
[28] 일본 정보처리추진기구(IPA), http://www.ipa.go.jp/about/press/20130415.html
[29] 일본, 제어 시스템 보안 센터 (CSSC) http://www.css-center.or.jp

〈저자소개〉

손 경 호 (Son Kyung Ho)
정회원
2001년 2월 : 성균관대학교 전기전자컴퓨터공학과 졸업
2004년～현재 : 성균관대학교 컴퓨터공학과 석·박사과정 수료
2013년～현재 : 강남대학교 컴퓨터미디어 공학부 겸임교수
2001년 1월～현재 : 한국인터넷진흥원 정보보호산업기획팀
관심분야 : 침해사고대응기술, 융합/CPS보안, 보안평가