

국외 산업제어시스템 보안기술 연구개발 동향

김우연*, 이수연**

요약

산업제어시스템에 대한 사이버보안 위협에 대응하기 위한 세계 각국의 산업제어시스템 보안기술 연구개발이 진행되고 있다. 미국은 에너지 분야를 중심으로 산업제어시스템 보안을 위한 응용기술 개발, 현장실증, 제품화 과정이 진행될 수 있는 연구개발 프로그램인 CEDS와 학계 중심의 TCIPG 프로그램을 진행하고 있으며, EU는 FP7 프로그램에서 연구소, 학계, 산업제어시스템 운영기관, 산업제어시스템 제조사 등이 참여하여 연구개발을 수행중이다. 일본도 산업제어시스템 제조사가 참여하는 제어시스템 사이버보안 센터를 중심으로 사이버보안 기술 개발을 진행 중이다.

본 논문은 미국, EU, 일본 중심으로 국외의 산업제어시스템 보안기술 연구개발 현황에 대해서 설명하고, 이러한 현황분석을 통해 산업제어시스템 사이버보안 기술 연구개발의 특징을 살펴봄으로써, 국내 산업제어시스템 사이버보안 기술 연구개발에 참고가 되고자 한다.

I. 서론

산업제어시스템은 계측 및 제어, 상태 감시 및 관리를 위해 다양한 산업분야에 걸쳐 폭 넓게 사용되고 있다. 이러한 산업제어시스템은 일반 IT환경의 시스템과는 달리 인터넷망과 분리되어 운영되고 제어시스템 네트워크 통신을 위한 전용 프로토콜이 사용되고 있다. 따라서 산업제어시스템을 대상으로 한 사이버 위협의 가능성이 없다고 인식되어 왔다. 하지만, 이러한 인식은 2010년 스텍스넷(Stuxnet) 악성코드가 발견됨에 따라 급격한 전환을 맞게 되었다. 이후 산업제어시스템에 대한 사이버사고는 매년 지속적으로 증가하고 있으며, 사이버사고에 활용될 수 있는 제어시스템 보안취약점 발견 건수도 매년 지속적으로 증가하는 추세에 있다. 이러한 추세는 미국 국토안보부 산하의 ICS-CERT (Industrial Control System - Cyber Emergency Response Team)에서 발표하고 있는 통계에 잘 나타나 있다[1]. 2010년 39건이던 사고 발생건수는 2014년 245건으로 증가했고, 보안취약점 발견 건수 역시 2010년 18건에서 2014년 159건으로 증가했으며, 사이버사고 발생 분야는 산업제어시스템 전분야에 걸쳐 발생하고 있다.

또한 2014년 독일의 연방정보보안국에서 발간한 보고서에 따르면 독일 철강회사를 대상으로 한 APT 공격으로 인해 제철소 시스템에 실제 피해가 발생하였음을 보고하였다[2]. 공격자는 스피어피싱 이메일 공격과 정교한 사회공학적인 기법을 통해 제철소의 업무용 네트워크에 침투한 후 제철소 생산 제어시스템 네트워크로 침투하였으며, 사이버 공격의 결과로 제어 컴포넌트에 문제가 발생하여 용광로가 제어되지 않은 채 중단됨으로써 심각한 손실이 발생하였다[2]. 이 사건은 2010년 발생한 스텍스넷 이후 두 번째로 사이버공격에 의해 물리적 피해가 발생한 사건으로 기록 되었다.

본 논문에서는 증가하는 산업제어시스템의 보안위협에 대응하기 위하여 세계 주요국에서 진행되고 있는 산업제어시스템 보안기술 연구개발 현황을 살펴보고자 한다.

본 논문은 총 5장으로 구성되어 있다. II장에서는 미국의 산업제어시스템 보안기술 연구개발 현황에 대해서 살펴보고, III장에서는 EU의 산업제어시스템 보안기술 연구개발 현황에 대해서 설명한다. IV장에서는 일본의 산업제어시스템 보안기술 연구개발 현황에 대해서 살펴보고, 마지막으로 V장에서는 국외의 산업제어시스템 보안기술 연구개발의 특징을 요약한다.

* 국가보안기술연구소 (wnkim@nsr.re.kr)

** 고려대학교 정보보호대학원 박사과정 (llyeon33@gmail.com)

[표 1] 산업제어시스템 사이버사고 발생 현황 및 보안취약점 발견 현황(회계년 기준)

구분	2010년	2011년	2012년	2013년	2014년
산업제어시스템 사이버사고 건수	39	140	197	257	245
산업제어시스템 보안취약점 발견 건수	18	139	137	187	159

II. 미국의 산업제어시스템 보안기술 R&D 현황

미국은 산업제어시스템 보호를 위하여 에너지 분야 [3,4], 댐 분야, 화학 분야, 교통 분야 등의 여러 분야에서 사이버보안 로드맵을 개발하였다. 이러한 분야별 로드맵은 2006년에 미국 에너지부에서 개발한 에너지분야 사이버보안 로드맵[4]을 근간으로 하고 있다.

미국의 산업제어시스템 보안기술 연구개발은 산업분야별 제어시스템 사이버보안 로드맵의 비전과 전략 목표를 달성하는데 필요한 보안기술 중심으로 연구개발을

추진하고 있다. 2006년 처음 개발 후 2011년에 개정된 에너지분야 사이버보안 로드맵의 비전은 “2020년까지 사이버공격에도 필수 기능을 유지할 수 있는 복원력 있는 에너지 전달 시스템을 설계, 설치, 운영, 유지하도록 한다.”이며, 이를 위해 5가지 전략 목표를 수립하였다 [3]. 미국 에너지부는 이러한 5가지 전략별로 [표 2]와 같이 주요활동 아이템을 추진하고 있으며, 이러한 전략 중 “신규 보안대책 개발 및 구현” 전략이 산업제어시스템 보안기술 연구개발과 관련성이 가장 높고 다른 전략들도 일부 보안기술 연구개발과 관련되어 있다[5]. 본 논문에서는 미국 에너지부 중심으로 진행되고 있는 연구개발 프로그램인 CEDS(Cybersecurity for Energy Delivery Systems)와 TCIPG(Trustworthy Cyber Infrastructure for the Power Grid)를 설명하고자 한다.

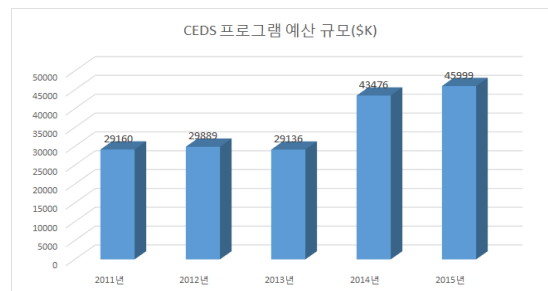
[표 2] 사이버보안 로드맵 전략과 에너지부의 주요활동(5)

Strategies	DOE Activities
Build a culture of Security	- Training - Education - Improved Communication within Industry
Assess and monitor risk	- Electricity Subsector Cybersecurity Capability Maturity Model - Situational Awareness Tools - Common Vulnerability Analysis - Threat Assessments - Consequence Assessments
Develop and implement new proactive measures	- Support Cybersecurity Standards Development - Near-term Industry-led R&D Projects - Mid-term Laboratory Academia R&D Projects - Long-term Laboratory Academia R&D Projects
Manage incidents	- NSTB(National SCADA Test Bed) - Outreach - Cyber Exercises
Sustain security improvements	- Product upgrades to address evolving threats - Collaboration among all stakeholders to identify needs and implement solutions

2.1. CEDS 프로그램

미국 에너지부는 전력, 석유, 가스 등 같은 에너지 분야 산업제어시스템을 보호하기 위한 연구개발 프로그램인 CEDS를 2011년부터 진행하였으며, 이를 위해 [그림 1]과 같이 매년 대규모의 연구개발 예산(안)을 투입하고 있다.

이러한 예산 투입을 통해 고위험 장기 프로젝트는 국립연구소 및 학계 중심, 중간위험도의 중기 프로젝트는



[그림 1] CEDS 프로그램 예산 규모

1) 미국 에너지부에서 의회에 제안한 회계연도별 예산(안) 중 CEDS 프로그램 관련 예산

국립연구소 중심, 저위험 단기 프로젝트는 산업계 중심으로 프로젝트를 수행한다. 프로젝트 수행단계는 학계와 국립연구소가 중심이 되어 제어시스템 운영 현장에서 활용 가능한 응용기술을 연구하는 단계, 산업계가 참여하여 프로토타입을 개발하는 단계, 개발된 프로토타입을 제어시스템 현장에서 실증하는 단계를 거쳐 최종 상용 제품을 만드는 과정으로 진행된다. CEDS 프로젝트에 참여하는 주요 기관은 [표 3]과 같다.

[표 3] CEDS 프로젝트 참여 주요 기관(5)




구분	주요 기관
학계	Cornell University, Iowa State Georgia Institute of Technology Illinois Institute of Technology UC-Davis, UC Berkeley University of Illinois University of Tennessee-Knoxville 등
국립연구소	Argonne National Laboratory Idaho National Laboratory Oak Ridge National Laboratory Los Alamos National Laboratory Lawrence Berkeley National Laboratory Lawrence Livermore National Laboratory Pacific Northwest National Laboratory Sandia National Laboratory
산업계 (Solution Provider)	ABB, Alstom Grid, ACS, Cigital, Inc. EPRI, Foxguard Solutions, GE Grid Protection Alliance, Grimm Honeywell, ID Quantique, NexDersense OSIsoft, Opal-RT, RTDS Technologies Schneider Electric, SEL Siemens, Telvent, Utility Advisors Utility Integration Solutions, ViaSat 등
제어시스템 운영기관	Alstom, AMeren, Burbank Water and Power CenterPoint Energy, Chevron, Dominion Duke Energy, Entergy, Idaho Falls Power Electric Reliability Council of Texas National Rural Electric Cooperative Association Pacific Gas & Electric, Peak RC TVA, Southern Company Washington Gas Energy Systems 등

이러한 과정을 통해 제품화된 예는 SEL의 이더넷 보안 게이트웨이인 SEL-3620이다. 해당 기술은 서로 다른 제조사 보안장비간에 상호운용성을 지원하기 위한 기술로써, SNL 연구소에서 2006년 연구를 시작하여 Lemnos Interoperable Security 라는 이름의 기술을 개발하고, 2008년에는 SNL 연구소와 EnerNex, SEL, 7개 네트워크 보안 업체 등의 산업계 및 제어시스템 운영기관인 TVA가 공동으로 프로토타입을 개발하였다.

[표 4] Ethernet Security Gateway 개발 과정(5)

R&D 단계	수행 년도	참여기관	연구결과
응용기술 연구	2006	SNL	Lemnos Interoperable Security 기술
프로토타입 개발	2008	EnerNex, TVA SNL, SEL Network Security Vendor(7개사)	프로토타입
현장 실증	2009	TVA	TVA사에서 실증 완료
상용 제품화	2009.12.	SEL	SEL-3620 출시 (보안게이트웨이)

[표 5] CEDS의 주요 현장 활용 기술(5)

기술명	연구 기관	기술 설명
Sophia	INL, BEA 등	IP 기반 제어시스템 네트워크 트래픽의 실시간 시각화를 통해 보안현황을 평가하는 도구 
Padlock	SEL SNL TVA	방화벽, 이벤트 로깅, 원격 접근제어 기능을 제공하는 펠드장치 설치용 장비 
Exe-Guard	SEL SNL Dominion	실행 가능 파일에 대한 Whitelist를 생성하여 장치 무결성 검사 
SIEGate	GPA	제어시스템 운영센터간 안전한 정보 교환을 위한 게이트웨이 기술 개발



(그림 2) SEL의 Ethernet Security Gateway 제품

개발된 프로토타입은 연구에 참여했던 TVA사에서 2009년 실증을 통해 기술의 실효성을 확인하고 2009년 12월 SEL에서 상용제품으로 출시하였다.

CEDS 프로그램에서 개발되어 현장실증이 진행된 기술은 [표 5]와 같다.

2.2. TCIPG 프로그램

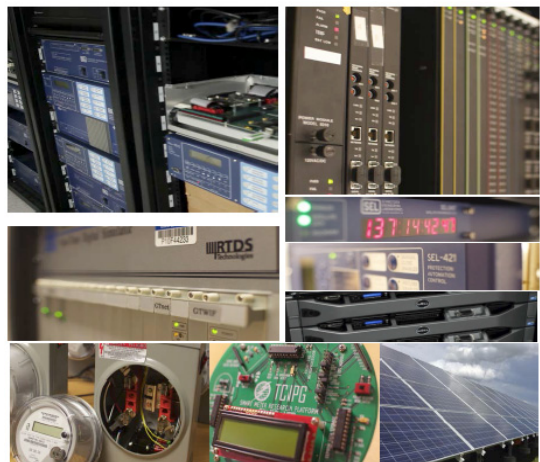
TCIPG 프로그램은 일리노이 대학교(UIUC) ITI(Information Trust Institute) 주관으로 워싱턴 주립 대학, UC Davis 대학, 다트머스 대학, 코넬 대학의 5개 대학이 중심이 되어 추진하는 대표적인 학계 연구개발 프로젝트이다[6]. TCIPG 프로그램은 2005년부터 2008년까지 수행된 TCIP(Trustworthy Cyber Infrastructure for the Power)의 연계 프로그램으로써 2009년 9월 30일에서 2015년 8월 30일까지 약 5년간 연구가 수행되었으며, 미국 에너지부 중심의 CEDS 프로그램내 학계 프로그램으로 지원되었다[6]. TCIPG 프로그램은 4개 기술 분야에 총 28개 세부과제가 수행되는 프로그램으로써 세부사항은 [표 6]과 같다.

(표 6) TCIPG의 연구개발 분야(6)

기술 분야	세부 분야	주요 연구개발 내용 (일부)
Trustworthy Technologies for Wide Area Monitoring and Control	Communication and Data Delivery (5개)	- Functional security enhancements for existing SCADA systems
	Applications (2개)	- GridStat middleware communication framework
	Component Technologies (2개)	- Cryptographic scalability in the smart grid - PMU-enhanced power system operations
Trustworthy	Active Demand	- Development of the Information

Technologies for Local Area Management, Monitoring, and Control	Management (3개)	layer for the V2G framework implementation - Password changing protocol
	Distribution Networks (1개)	- Trustworthy framework for mobile smart meters
Responding To and Managing Cyber Events	Design of Semi-automated Intrusion Detection and Response Techniques (6개)	- A game-theoretic response and recovery engine - Assessment and forensics for large-scale smart grid networks - Specification-based IDS for smart meters
Trust Assessment	Model-based Assessment (3개)	- 802.15.4/ZigBee Security Tools - Security and Robustness
	Experiment-based Assessment (5개)	Evaluation and Enhancement of Power System Applications - Synchrophasor Data Quality

TCIPG 프로젝트들의 수행을 위한 기반으로써 송전, 배전, 미터링, 분산전원, 홈 오토메이션이 가능한 중단 간 제어 기능을 지원하는 테스트베드를 구축하여 운영하고 있다. 테스트베드는 프로젝트 수행에 필요한 실험을 수행하고 전력 시스템의 신뢰성을 분석하는 등의 용



(그림 3) TCIPG의 테스트베드

도로 활용되며, [그림 3]과 같이 구축되어 있다.

III. EU의 산업제어시스템 보안기술 R&D 현황

EU에서는 2007년부터 2013년까지 진행된 FP7 프로그램내에서 산업제어시스템 관련 보안기술 연구개발이 진행되고 있다. FP7 후속 프로그램인 Horizon 2020에서도 기반시설 보호를 위한 ICT의 역할이라는 주제로 기반시설의 SCADA 시스템 보호를 위한 연구개발을 지원하고 있다. 본 장에서는 FP7 프로그램에서 수행되었거나 수행되고 있는 산업제어시스템 관련 보안기술에 대해서 소개하고자 한다.

ESCoRTS 프로젝트는 유럽의 표준화 기구인 CEN, EU의 제어시스템 제조사(ABB, Areva, Siemens), 제어시스템 운영기관(발전, 송변전, 수처리) 등이 참여한 컨소시엄에서, 제어시스템 보안 표준의 현주소를 검토하고 향후 추진방향을 수립하기 위한 목적으로 수행되었다[7]. 제어시스템 보안과 관련된 국제표준 및 가이드라인 13건, 미국주도의 표준 및 가이드라인 14건, 유럽주도의 표준 및 가이드라인 10건 등 전 세계의 37개 제어시스템 보안관련 표준, 가이드라인, 규제지침을 분석하

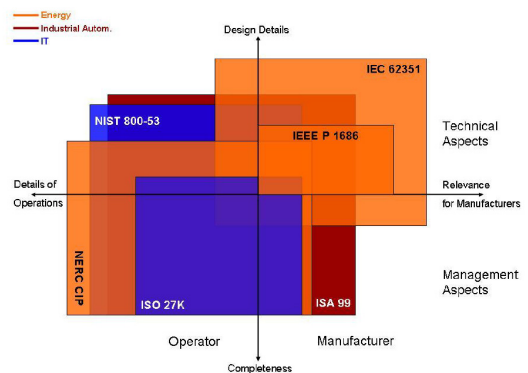
였다. 분야별로는 제어시스템 산업 공통 분야 5건, 에너지 분야 12건, 산업자동화 분야 13건, 석유 및 가스 분야 4건, 화학분야 2건이 포함되어 있다[7]. 이 중에서 NERC CIP, ISO 27000, ISA 99/IEC 62443, CPNI/NISCC, NIST 800-53, IEC 62351, IEEE 1686 등의 7건에 대해서는 심층 분석을 통해 [그림 4]와 같이 기술적 측면과 관리적 측면의 특징을 분석하였다.

VIKING 프로젝트는 전력 송·변전 및 배전 네트워크의 감시·제어를 수행하는 제어시스템을 대상으로 안전하고 복원력 있는 산업제어시스템의 설계, 운영, 분석을 위한 방법론을 개발하고 시험하여 평가하기 위한 프로젝트이다[8]. SCADA 시스템의 취약성 분석은 전체 SCADA 네트워크상의 잠재적 위협 목표물을 선정하고, 모델 기반으로 SCADA 시스템의 취약성을 분석하는 단계로 진행된다. 잠재적 위협 목표물에는 제어망, 제어망과 업무망간 연계 접점, 변전소망, 변전소망과 제어망간 통신 채널, IED, 제어망과 인터넷 연계구간 등이 대상이며, 분석 모델은 공격자가 SCADA 시스템을 공격하여 전력 네트워크에 영향이 발생하면, 전력망과 연계된 사회기반시설에 유발되는 피해비용을 분석하는 접근법을 채택하였다[8]. 이러한 분석 과정을 통해서 ① 보안위험과 피해 결과를 추정, ② IT시스템과 제어시스템 솔루션 구현에 있어서의 차이점 분석, ③ 조작된 데이터 탐지를 위한 어플리케이션 수준 IDS의 활용 방안 마련, ④ 안전한 전력시스템 통신을 위한 솔루션 활용 방안 마련, ⑤ 취약 지점 식별 및 대책 마련 등을 연구하였다.

CockpitCI 프로젝트는 기반시설에 대한 사이버위험을 자동으로 탐지 및 분석하여, 기반시설 운영측면의 위험을 준 실시간으로 예측하고, 기반시설 운영기관간에

[표 7] EU의 산업제어시스템 보안기술

프로젝트명	주요 내용
ESCoRTS	- European network for the Security of Control and Real-Time Systems - 2008.6.16. - 2010.12.15. (2년 6개월)
VIKING	- Vital Infrastructure, networkS, INformation and control systems manAgement - 2008.11.1. - 2011.11.30. (3년 1개월)
CockpitCI	- Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures - 2012.1.1. - 2014.12.31. (2년)
PRECYSE	- Prevention, protection and REaction to CYber attackS to critical infrastrucreEs - 2012.3.1. - 2015.2.28. (3년)
SPARKS	- Smart grid Protection Against cybeR attackS - 2014.4.1. - 2017.3.31. (3년)



[그림 4] 심층 분석한 7건의 표준 문서의 특징 비교

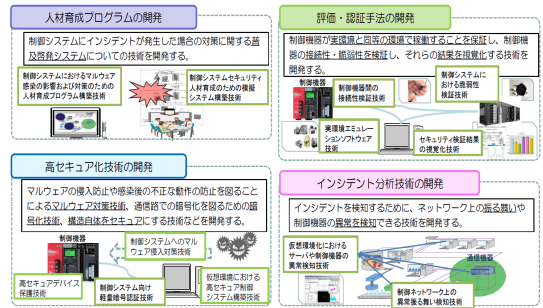
준 실시간으로 관련 정보를 공유하여 기반시설 서비스 품질을 유지할 수 있는 시스템과 전략을 개발하기 위한 연구이다[9].

PRECYSE 프로젝트는 자산과 관련된 위협과 취약점을 식별하는 방법론을 연구하여, 복원력을 향상시킬 수 있는 보안 아키텍처를 설계하고, 기반시설 대상의 사이버 공격을 예방 및 대응할 수 있는 도구를 개발하여 에너지와 교통 분야에서 도구의 적절성을 실증하는 프로젝트이다. 이 프로젝트는 SCADA 시스템을 공통의 보안 정책이 적용되는 시스템의 그룹을 의미하는 보안 엔클레이브로 구분하고, 네트워크 경계 보호 및 내부 이상행위 탐지, 이벤트 상관관계 분석, 보안대책 관리 시스템을 표준을 기반으로 오픈소스 형태로 개발하였다[10]. 이상행위 탐지 관련해서는 유럽에서 수자원, 가스, 전력 시스템에 주로 사용되는 IEC 60870-5-104 SCADA 프로토콜에 대한 DPI를 통해 SCADA IDS를 개발하였고, ICT 시스템과 산업제어시스템의 보안 이벤트를 수집하여 상관관계 분석을 수행하는 AECID(Automatic Event Correlation for Incident Detection) 시스템을 적용하였다[10].

SPARKS 프로젝트는 스마트그리드를 대상으로 사이버 위협 평가 방법 및 도구를 개발하는 연구로써, 오스트리아의 AIT가 중심이 되어, 독일의 프라운호퍼연구소와 SWW Wunsiedel GmbH, 영국의 퀸즈대학, 오스트리아 케플러 대학의 에너지연구소, 아일랜드 EMC의 RSA와 United Technologies Research Centre, 스웨덴의 KTH, 스위스의 Landis+Gyr AG 등 9개 연구기관이 공동연구를 수행하고 있다. 연구결과물은 AIT의 SmartEST 실험실, Nimbus의 마이크로그리드, SWW Wunsiedel의 스마트그리드 환경에서 실증을 수행한다[11].

IV. 일본의 산업제어시스템 보안기술 R&D 현황

일본은 2012년 기술연구조합인 제어시스템 보안센터(Control System Security Center, 이하 CSSC)를 설치한 후 본격적인 제어시스템 보안기술 R&D를 추진하기 시작했다. 일본은 제어시스템 보안성 강화 기술, 제어시스템 보안 검증 기술, 제어시스템 사이버 사고 분석 기술, 인재육성 프로그램 개발의 4대 중점 추진분야를 선정하여 이에 대한 기술개발을 진행하고 있다[12].



(그림 5) 일본의 제어시스템 보안기술 연구개발 현황

제어시스템 보안성 강화 기술 분야는 악성코드의 침입방지 기술, 감염이후의 오동작 예방 기술, 통신 과정에서 암호화를 수행하는 암호화 기술, 제어시스템 구조 자체를 안전하게 하는 기술 등을 개발한다. 제어시스템 보안 검증 기술 분야는 제어기기가 실제 환경과 동일한 환경에서 동작하는 것을 확인하고, 제어기기의 접속성, 취약성을 확인해서 그 결과를 시각화하는 기술을 개발하고 있다. 제어시스템 사이버 사고분석 기술 개발 분야는 네트워크 기반 사이버사고의 감지 기술 및 제어기기의 이상을 감지할 수 있는 기술을 개발하고 있으며, 그 예로는 제어망에서의 이상행위 감시기술, 가상 환경 하에서 서버나 제어기기의 이상 감시 기술이 있다. 인재육성 프로그램 개발에서는 제어시스템 사이버 사고 대응 능력 향상을 위한 인재 육성 기술을 개발하는 것으로써, 제어시스템의 악성코드 감염 영향 및 대응을 위한 프로그램 구축 기술, 제어시스템 보안 인재 육성을 위한 모의 시스템 구축 기술을 개발하고 있다. 이러한 개발



(그림 6) CSSC의 테스트베드

기술은 [그림 6]과 같은 CSSC의 테스트베드인 CSS-Base6를 활용하여 현장과 유사한 환경에서 연구 개발이 진행되고 있다.

V. 요약

본 논문에서는 증가하는 산업제어시스템 보안위협에 대응하기 위해 미국, EU, 일본 등에서 수행하고 있는 산업제어시스템 사이버보안 기술 동향에 대해서 살펴본다. 국외의 사례를 분석한 결과 산업제어시스템 사이버보안 기술 연구개발의 특징은 ① 응용기술 개발, 프로토타입 개발, 현장실증, 제품화 과정의 장기간 단계적인 연구개발이 필요하며, ② 산업제어시스템 운영기관 및 제조사가 참여하여 현장실증을 수행함으로써 활용이 가능하도록 연구개발이 수행되며, ③ 기존에 개발된 사이버보안 기술이라도 산업제어시스템의 특징에 맞게 커스터마이징 할 수 있는 기술의 연구개발도 필요하다. 국내에서도 산업제어시스템 운영사, 연구소, 산업제어시스템 제조사, 보안업체 등이 참여하여 스마트그리드를 포함한 산업제어시스템을 보호하기 위한 사이버보안 기술 개발이 진행되고 있다. 이렇게 개발된 기술이 산업제어시스템 운영사들이 참여하는 실증사업을 거쳐 현장에 적용될 수 있는 연구개발 체계가 잘 구축된다면, 우리나라의 산업제어시스템이 사이버보안 위협으로부터 좀 더 안전해 질 수 있을 것으로 기대된다.

참고 문헌

- [1] ICS-CERT, "ICS-CERT Year in Review," 2014.
- [2] Federal Office for Information Security, "The State of IT Security in Germany 2014," 2014.
- [3] Energy Sector Control Systems Working Group, "Roadmap to Achieve Energy Delivery Systems Cybersecurity," Sep. 2011.
- [4] Energetics Incorporated, "Roadmap to Secure Control Systems in the Energy Sector," Jan. 2006.
- [5] Carol Hawk, "Cybersecurity for Energy Delivery Systems(CEDS)," Aug. 2014.
- [6] Bill Sanders, "Trustworthy Cyber Infrastructure for the Power Grid(TCIPG)," Aug. 2014.
- [7] Luc Van den Berghe, "ESCoRTS A European network for the Security of Control & Real Time Systems," Luxembourg workshop, May 2010.
- [8] Gunnar Björkman, "The VIKING Project - Towards more Secure SCADA Systems," First Workshop on Secure Control Systems, Apr. 2010.
- [9] Tiago Cruz, Jorge Proenca, Paulo Simoes, Matthieu Aubigny, and Moussa Ouedraogo, "Improving Cyber-Security Awareness on Industrial Control Systems: The CockpitCI Approach", Proceedings of the 13th European Conference on Cyber Warfare and Security, Jul. 2014.
- [10] Kieran McLaughlin, Sakir Sezer, Paul Smith, Zhendong Ma, and Florian Skopik, "PRECYSE: Cyber-attack Detection and Response for Industrial Control Systems", ICS-CSR, Sep. 2014.
- [11] <https://project-sparks.eu/>
- [12] 小林 偉昭, "CSSCの進めるテストベッドCSS-Base6と EDSA認証について", 制御システムセキュリティティカンファレンス 2014, Feb., 2014.

<저자 소개>



김우년 (Woo-Nyon Kim)

정회원

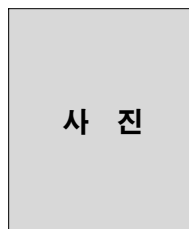
1996년 2월 : 안동대학교 컴퓨터공학과 졸업

1998년 2월 : 경북대학교 컴퓨터공학과 이학석사

2000년 2월 : 경북대학교 컴퓨터공학과 박사수료

2000년 3월~2003년 12월 : ㈜니츠 선임연구원

2003년 12월~현재 : 국가보안기술연구소 책임연구원/실장
관심분야 : 기반시설보안, SCADA 보안, 제어시스템 보안, 취약점 분석, 네트워크 보안



이수연 (Su-Yeon Lee)

학생회원

2007년 3월~현재 : 고려대학교 정보보호전문대학교 박사(과정)

관심분야 : 정보보호정책, 기반시설 보안, SCADA 보안, 취약점 분석, 네트워크 보안