Journal of Digital Convergence
Vol. 17. No. 1, pp. 347-356, 2019

ISSN 1738-1916
https://doi.org/10.14400/JDC.2019.17.1.347

보안성 평가 도구 사례 분석 연구

김현일[1], 박경연[1], 서창호[2*], 문대성[3]
[1]공주대학교 융합과학과 박사과정, [2]공주대학교 융합과학과 교수, [3]한국전자통신연구원(ETRI) 책임연구원

A Study and Analysis on Case Study of Security Evaluation Tool

Hyun-il Kim[1], Kyungyun Park[1],Changho Seo[2*], Daesung Moon[3]
[1]Ph.D Student, Department of Convergence Science, Kongju National University
[2]Professor, Department of Convergence Science, Kongju National University
[3]Principal Researcher, Electronics and Telecommunications Research Institute(ETRI)

요 약 최근, 산업제어 시스템의 개방화로 인해 민간, 공공 분야 정보시스템에서 구조적 패러다임의 큰 변화가 제안되고 있다. 이에 따라, 기존 정보시스템의 보안 기술 수준으로 대응할 수 없는 미래 주요 기반 시설 제어시스템의 잠재적 사이버 보안 문제가 최근 대두되고 있으며, 이러한 보안 취약점에 대응하기 위해 다양한 기반 시설 제어 시스템 환경에 대해 입체적으로 보안 취약성을 평가할 수 있는 보안 평가 도구가 필요하다. 하지만 현재 국내 사이버 보안 평가 환경은 점검 항목의 대부분이 기술적인 영역에 한정되어 있어 한계점이 존재한다. 이를 극복하기 위해, 미국의 사이버 보안 평가 도구인 CSET(Cyber Security Evaluation Tool)을 국내 다양한 기반 시설의 제어 시스템 환경에 맞게 적용하기 위한 많은 연구가 필요하다. 따라서, 본 논문에서는 기존의 보안 평가 도구를 적용하는 다양한 연구 사례 분석을 통해 국내 원전, 전력 등의 기반 시설에 적용할 방안에 대해 분석하고 앞으로의 연구 방향을 제안한다.

주제어 : 미국 사이버 보안 평가 도구, 분산제어시스템, 스카다, 개방형 시스템, 보안성 평가

Abstract Recently, the liberalization of industrial control systems has been accompanied by a major change in the structural paradigm of information systems in the public and public sectors, and potential cyber security problems in the future major infrastructure control systems that cannot respond to the level of security of existing information systems. To cope with this, a cyber security evaluation tool that can evaluate security vulnerability in three dimensions against various infrastructure control system environment is needed. However, a cyber security evaluation in the domestic environments does not have the concept of the current security status and satisfy settings of the infrastructure. Also, the most of items in that environments have had short-term inspection themselves which makes a limitation by a technical area. In order to overcome this problems, many researches are needed to apply CSET (Cyber Security Evaluation Tool) which is the US cyber security evaluation tool to the control environment of various domestic infrastructure. In this paper, first, we analyze methods to apply to the major domain through the analysis of various case studies on existing security assessement tools. Finally, we discuss future directions.

Key Words : CSET, DCS, SCADA, Open systems, Security evaluation

*This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea goverment(MSIT) (No.2017-0-00213, Development of Cyber Self Mutation Technologies for Proactive Cyber Defense and No.2018-0-01369, Developing Blockchain Identity Management System with Implicit Augmented Authentication and Privacy Protection for O2O Services
*Corresponding Author : Changho Seo(chseo@kongju.ac.kr)
Received November 12, 2018 Revised December 28, 2018
Accepted January 20, 2019 Published January 28, 2019

1. 서론

최근, 산업제어시스템의 개방화로 인해 주요 기반시설을 제어할 수 있는 하드웨어 및 소프트웨어 기술의 보편화가 이루어 지고 있다. 이에 따라, 민간·공공 분야 정보시스템의 구조적 패러다임의 큰 변화가 주목받고 있다. 하지만, 산업 제어 시스템의 개방화로 인하여 개인 혹은 기업의 정보화 기기 및 시스템에 대한 보안 위협뿐만 아니라, 국가적인 손상을 줄 수 있는 주요기반 시설의 제어 시스템에 대한 심각한 보안문제가 발생하였다[1].

기존의 정보 시스템 분야의 주요 활용 보안 방법은 새롭게 발생된 보안문제를 해결함에 있어 한계가 있다. 이에 따라, 사이버보안 분야의 선진국들은 이미 보안 취약점에 대하여 다양한 관점에서의 약점을 체계적으로 도출할 수 있는 보안 평가 도구에 대한 방법을 제안하였고, 현재 사용하고 있다[2-4]. 미국의 NIST(National Institute of Standards and Technology)에서는 제어 시스템 네트워크 대상의 사이버 보안 평가 도구인 CSET(Cyber Security Evaluation Tool)을 제공하고 있다[5]. 또한, 영국의 CPNIC(Center for Protection of National Infrastructure)는 CSET보다 간단하게 평가 항목을 제공하는 SSAT(SCADA Self Assessment Tool)를 개발 및 제공하고 있다[1]. 하지만 국내에서는 기반시설의 현재 보안 상태 및 목표 설정에 대한 개념이 도입되어 있지 않고, 점검 항목의 대부분이 기술적인 영역에 한정되어 있어 자체적·단발적인 점검이 불가하다. 따라서, 사이버 보안에 대해 세계 최고 수준인 미국의 사이버 보안 평가 도구인 CSET을 국내의 환경에 맞게 적용하기 위한 연구가 필요하다.

본 논문의 2장에서는 미국의 사이버 보안 평가 도구인 CSET에 대해 분석하고, 3장에서는 이를 적용하기 위해 국내 원전, 전력 등의 주요 기반 시설의 제어시스템 환경을 분석한다. 4장에서는 국내의 환경에 맞게 ICS보안 평가 도구를 적용할 방안에 대해 분석하고 앞으로의 연구 방향을 제시하고 5장에서 결론을 짓는다.

2. CSET 분석

CSET은 NIST, 북미 전력 신뢰도 공만(NERC), 교통안전청(TSA), 미 국방부(DoD) 및 기타 기관의 다양한 표준을 통합하며, 민간·공공 기간과의 협력체계를 통해서 수집한 다양한 신규 보안사고 사례 및 대안이 지속적으로 업데이트 된다. CSET을 이용하여 주요 기반시설의 사이버 보안 위험 분석 프로세스에 적용한 연구 사례를 살펴보면, 2011년 스마트 그리드(Smart Grid) 기반 시설의 전력 시스템 통신 파트에 적용한 사례가 있고[2], 2013년 원자력 발전소에서 물리적 시스템 자산을 보호하기 위해 활용한 사례가 있다. 또한, 2015년 중국의 SCADA 사이버 보안을 고려한 파워 시스템 신뢰성 측정 연구[3]를 진행하였고, 2015년 미국 FFC(Federal Facility Council)에서 CSET을 이용한 사이버 보안 빌딩 제어 시스템 적용을 검토하였다[4].

CSET 도구는 아래와 같이 조직 직급 체계 및 직무에 따른 주요 기반 시설 보안 업무 관리자, 관리범위를 규정하고 있다.

- IT 정책 및 절차 (예 : 최고 정보 보안 책임자)
- IT 보안 계획 및 관리 (예 : 정보 기술 이사)
- IT 인프라 구조 (예 : 네트워크 및 시스템 관리자)
- IT 운영 (예 : 구성 및 변경 관리자)
- 비즈니스 운영 (예 : 운영 관리자)
- 위험 관리 (예 : 기업 / 운영 리스크 관리자)

또한, Table 1에 나오는 위험 관리 프로세스에 따른 제어 표준 및 질문 세트를 포함하고 있다.

Table 1. Security standard from major infrastructure in the US[5]

Standards/Question Sets in CSET	Short Name
NIST Special Publication 800-53 Rev 3	800-53 R3
NIST Special Publication 800-53 Rev 3 App I	800-53 R3 App I
NIST Special Publication 800-53 Rev 4	800-53 R4
NIST Special Publication 800-53 Rev 4 App J	800-53 R4 App J
NIST Special Publication 800-82	SP800-82
NIST Special Publication 800-82 Rev 1	SP800-82 V1
NIST Special Publication 800-82 Rev 2 (Draft)	SP800-82 V2
Consensus Audit Guidelines (CAG)	CAG
Components Questions Set	Components
CFATS Risk-Based Performance Standards Guide 8-Cyber	CFATS
CNSSI No. 1253 Baseline	CNSSI 1253
CNSSI No. 1253 Industrial Control System (ICS) Overlay V1	CNSSI ICS
Catalog of Recommendations Rev 7	COR 7
DOD Instruction 8500.2	DOD 8500.2
INGAA Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry	INGAA
Key Questions Set	Key
NIST Framework for Improving Critical Infrastructure Cybersecurity V1	NCSF V1
NEI 0809 Cyber Security Plan for Nuclear Power Reactors	NEI 0809
NERC CIP-002 through CIP-009 Rev 3	NERC Rev 3
NERC CIP-002 through CIP-009 Rev 4	NERC Rev 4
NISTIR 7628 Guidelines for Smart Grid Cyber Security: Vol. 1	NISTIR 7628
NRC Regulatory Guide 5.71	NRC 5.71
TSA Pipeline Security Guidelines April 2011	TSA
Universal Questions Set	Universal

현재 CSET은 6.2 버전으로 PC 데스크탑 환경에서 구동된다. CSET에서 보안 표준을 선택한 후, 제공하는 질문 세트를 사용해 사이버 보안 평가 대상 시스템을 출력한다. 그리고 해당 제어 시스템의 자체 평가를 통해 사이버 보안 평가 보고서를 제공한다[6].

3. 국내 제어시스템 환경 분석

산업 제어 시스템(ICS, Industrial Control Systems)은 주요 기반 시설 감시 제어 및 데이터 취득을 목적으로 군·내외에서 널리 활용되고 있으며, 전통적인 범용 네트워크 및 OS 기반 IT 보안 기술로 대응할 수 없는 요소들을 포함한다.

산업 제어 시스템은 산업 공정 제어에 사용되는 여러 유형의 제어 시스템 및 관련 계측 전용 시스템으로 SCADA(스카다, Supervisory Control and Data Acquisition), DCS(분산제어시스템, Distributed Control System)으로 분류할 수 있다. 이들 시스템은 프로그램이 가능한 PLC(로직 컨트롤러, Programmable Logic Controller), RTU(원격 단말기, Remote Terminal Unit), HMI(인간-기계 인터페이스, Human-Machine Interface)로 구성되며, 전용 통신 설비로 이들 단위 모듈과 상호 연동된다.

3.1 SCADA 시스템

SCADA는 산업현장 전체, 또는 지리적으로 넓게 퍼져 있는 산업 단지를 전반적으로 감시하고 제어하는 집중화된 시스템을 주로 말한다. 대부분의 제어 동작은 RTU와 PLC에 의해 자동으로 이루어지며, 운영자가 내릴 수 있는 제어 명령은 보통 기본적인 작업 변경이나 관리 수준의 작업 조정에 한한다.

예를 들어, 어떤 PLC가 특정 작업 공정에 사용되는 냉각수의 흐름을 조절한다면, SCADA 시스템은 그 흐름의 세부 설정을 바꾼다거나, 냉각수 손실이나 온도 등에 대한 경보를 표시하고 기록하도록 설정하는 정도의 작업을 허용하게 된다. 그리고 피드백(Feedback) 신호는 RTU와 PLC에 전달되지만, SCADA 시스템은 그 피드백 신호의 전체적인 성능을 관장하게 된다[7].

SCADA 시스템은 유선과 무선 통신을 모두 이용해왔고, SONET/SDH(동기식 광통신망, Synchronous Optical Networking)도 철도나 발전소와 같은 대규모의 시스템에 많이 사용되었다.

SCADA 시스템의 프로토콜(Protocol)은 가볍게 동작할 수 있는 형태로 설계된다. 예를 들어, 마스터 스테이션이 RTU의 데이터를 주기적으로 검사하려고 할 때에만 정보를 전송하는 경우가 많다.

현재 널리 사용되는 산업계 구형 프로토콜은 Modbus, RTU, RP-570, Profibus Conite 1 등이 있다. 이 통신 프로토콜은 모두 SCADA 공급사에 의존적인 형태이다[8]. 또한 최근 상하수도 설비, 전력 계통 등과 같이 여러 현장 및 국가 현장 전역 관리를 목적으로 셀 무선 통신망 및 WAN(Wide Area Network)을 이용하여 데이터를 교환하는 SCADA 시스템이 일반화되고 있으며, 보안의 중요성이 증가함에 따라 위성 통신을 사용하는 경우도 증가하고 있다.

과거의 RTU 및 기타 자동 제어 장치들은 수많은 회사들에 의해제어 전용 프로토콜을 만들어 운용하였지만, 최근에는 공정 제어 상호연동을 위한 산업계 표준 OLE (OLE for Process Control, OPC) 프로토콜이 각종 하드웨어, 소프트웨어간의 통신을 위해 널리 사용되고 있다.

3.2 DCS 시스템

DCS는 주요 기반 시설의 감시 제어 및 데이터 취득을 위한 목적으로 널리 사용되는 ICS 시스템의 한 종류이다. DCS는 자동화 컨트롤러(예: PAC)가 시스템 전체에 걸쳐 분산되어 분산 시스템에 설치된 자동화 프로그램 기반으로 동작될 수 있으며, 동시에 중앙 운영 시스템의 제어가 가능하 시스템이다. DCS의 목적은 중앙 집중식 제어가 아닌 플랜트 근처에서 제어기능을 구현하여 신뢰성을 높이고 설치 및 유지보수 비용을 줄이는 것이다. 현재 SCADA와 DCS 시스템의 기능은 매우 유사하지만, DCS

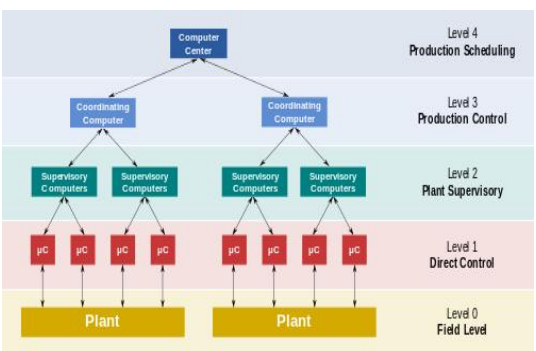

Fig. 1. Structure diagram of DCS system

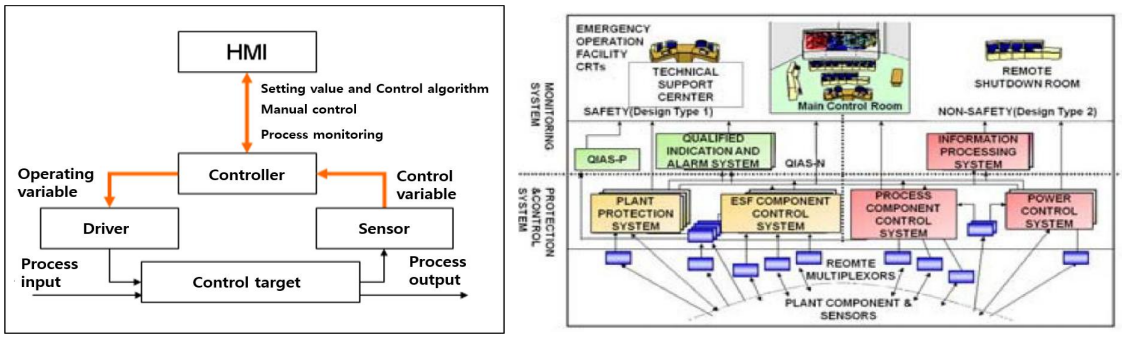

Fig. 2. Overview of the nuclear control system[9]

는 높은 신뢰성과 보안이 중요하고 제어실이 지리적으로 멀리 떨어져 있는 대규모 연속 공저 공장에 주로 사용된다.

DCS의 핵심 속성은 시스템의 노드(Node) 주변에 제어 처리를 분산시켜 안전성을 확보하는 것으로 이는 단일 프로세서 오류를 완화시키는 효과가 있다. 예를 들어, 특정 프로세서에 장애가 발생하면 전체 프로세스에 영향을 주는 중앙 컴퓨터의 계단식 오류 전파 특성과 다르게, DCS는 시스템 프로세스의 한 섹션에만 영향을 미친다.

Fig. 1는 분산된 자동화 제어기(PAC)를 사용한 일반적인 제조 산업제어 환경의 계층적 DCS 모델을 보여준다. 레벨 0은 필드 장치(Field devices) 및 제어 밸브(Control valve)와 같은 최종 제어 요소가 포함된다. 레벨 1에는 산업화된 I/O 모듈과 관련 분산 전자 프로세서(Distribued electronic processor)가 포함된다. 그리고 레벨 2에는 시스템의 프로세서 노드에서 정보를 수집하고, 운영자 제어 화면을 제공하는 감독(모니터링, 제어)컴퓨터가 포함된다. 레벨 3은 프로세스를 직접 제어하지는 않지만 생산 모니터링 및 모니터링 대상과 관련된 생산 관리 레벨이고, 마지막으로 레벨 4는 생산 스케쥴링(Scheduling) 레벨이다.

DCS는 연속 일괄 처리 기반 제조 프로세스에 사용되는 전용 시스템으로 DCS 프로세스는 석유 화학 및 정유 공장, 보일러 제어 및 발전소 시스템, 원자력 발전소, 식품 및 식품 가공, 자동차 제조, 제약 제조, 그리고 농업 응용 분야 등이 있다.

3.3 원전, 국방 적용 환경

본 절에서는 앞 절에서 설명한 산업 제어 시스템(SCADA, DCS)의 원전, 국방 등의 주요 도메인 적용 환경에 대해 설명한다.

3.3.1 원전 산업제어시스템

원자력 발전소는 원전계측설비(MMIS, Man-Machine Interface System)에 산업제어시스템이 적용되며, 원전 계측 시스템의 개략도는 Fig. 2와 같다. 원적 계측 시스템은 원자로의 운전 보호와 감시 및 시스템 제어 기능을 수행하며, PCL 및 DCS 기반으로 설계 제작된다. Fig. 2에서 살펴보면, 보호 및 제어 시스템에서는 장치 컨트롤러(PAC 혹은 PLC)와 장치가 탑재되어 세트포인트 설정 기반으로 원하는 프로세스대로 센서 및 액츄에이터가 자동화 제어된다. 모니터링 시스템(Monitoring system)에서 RTU는 장치 컨트롤러로부터 수집된 센서 신호를 디지털 데이터로 변화하여 관리 시스템으로 전송하는 역할을 하며, HMI를 통해서 감독관은 원전 시스템을 제어 및 모니터링 한다.

3.3.2 국내 전력 산업제어시스템

국내 전력 산업에서는 송전 계통, 급전(DAS, 전기 배급) 계통, 에너지 관리 시스템(EMS, Energy Management System)에서 SCADA 시스템이 활용되며, 전력 분야의

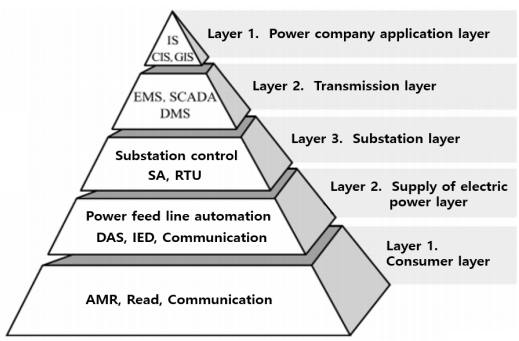

Fig. 3. Overview of industrial control system in electric power field

산업 제어 시스템의 개략도는 Fig. 3와 같다. 송전 및 급전을 위한 제어소의 RTU에서는 상위 제어설비에서 송출된 명령을 수신하여, 현장 전력 설비를 제어한다. 또한, 변전소 현장에서 취득한 상태정보와 계측정보를 상위 제어설비로 송출한다. 예를 들어, 현장 차단기가 닫힘 상태임을 감지하면 그 결과를 전송하는 방식으로 원격감시 기능을 수행한다.

4. 국내 산업제어 시스템 보안성 평가 방안

이러한 폐쇠적인 SCADA 시스템의 보안 위협은 폐쇄적인 SCADA 기술에서 표준화되고 공개된 기술로의 이전, 그리고 SCADA-인터넷-사내 네트워크간 연결이 증가하는 현재 SCADA 시스템들이 외부 공격에 대해 취약함을 의미한다. 또한, 일부 SCADA 시스템이 잠재적으로 사이버 공격에 취약한 것으로 여겨짐에 따라 보안 취약성 문제가 대두되었다.

다음은 국내 주요 도메인 산업 제어 시스템의 침해 사례를 소개한다. 또한 Table 2에서는 이러한 침해 사례의 위협원인 및 대안을 정리하였다.

1. 2000년 호주 퀸즈랜드, 하수처리 시스템 제어권 탈취사고
2. 2003년 플로리다 잭슨빌, CSX 기차신호시스템 사고
3. 2003년, Davis-Besse 원자력발전소 사고
4. 2006년 미국 Alabama 주, Browns Ferry 원자력 발전소 정지 사고
5. 2010년 6월, Stuxnet의 출현

이러한 SCADA 시스템의 변화와 보안 침해 사례를 통해서, 주요 기반 시설의 위험을 Table 3와 같이 정리할 수 있다. Table 3에서 보이는 것처럼 주요 기반 시설은 운영 간소화, 성능향상, 비용 절감을 위해 외부의 IT 서비스 및 시스템에 연결됨에 따라 연결성(통합성), 개방성(공개성)을 가지게 되었으며, 서비스 영역 및 영역의 확대로 업무 중단 시 커다란 사회 혼란과 범국가 차원의 피해가 발생할 가능성이 증가되었다. 따라서, 주요 기반시설의 분류 및 특성별로 전문화된 보안 위험 관리 프로세스가 필요하다.

기존에 제공되는 보안성 평가 도구(CSET, CRT 등)들은 국가별로 조직 체계, 법률 등의 속성 차이가 있기 때문에 국내에 바로 적용하는 것이 어렵다. 먼저, 국내 환경에 적합한 주요 기반시설 사이버 보안 위험 관리를 위해서는 국가적 차원의 협력 체계 및 법률 정립, 주요 기반시설별 산업제어 시스템 보안 관리를 위한 조직 체계 적립 등이 필요하며, 구체적인 위험 관리 전략은 Table 4과 같이 정리 될 수 있다.

다음으로, 사이버 보안 위험 관리 프로세스에 대한 최초 전략 수집, 보안 관리 개선 등 지속적·영구적인 운영을 위해서 주요 기반 시설 보안 전략 및 실행에 따른 효과를 평가할 수 있는 효과적인 도구가 필요하다.

Table 2. Examples of industrial control system infringement and corresponding threat agents and alternatives

Exmaples	Threat(Threat agent)	Preparations
Davis-Besse Nuclear slammer worm infection	Infringement of control system via Internet(Malware)	Strengthen logical and pysical control R & D about strengthening technology
Brown Ferry Nuclear power plant shut down	Loss of functionality due to large network traffic(PLC)	Strengthen logical and pysical control Strengthen of security system and deucation R & D about strengthening technology
Hatch Nuclear power plant shut down	Update unproven software (Update file)	Strengthen logical and pysical control Strengthen of security system and deucation R & D about strengthening technology
Stuxnet	Infringement of control sytem via Internet, Ingringement of control system via USB (Hostile country - Malware)	Strengthen logical and pysical control Strengthen of security system and deucation
Duqu	Information leakage(Malware)	Strengthen logical and pysical control Strengthen of security system and deucation
Attempt to hack nuclear power field	Infringement of control system via Internet(Hostile country)	Analyze cyber infringement accident and develop technology

Table 3. The properties and risks of major infrastructure

character	Main content	Threats
Connecti vity (Integrity)	Connect and integrate with external IT services in a Closed system	▪ Lack of security in access links provided to vendors for maintenance of control systems in major infrastructure. ▪ Lack of strong authentication scheme and encryption method.
Opennes s	Open major infrastructure publicly by using public / standard protocols	▪ Universal / standard technology is vulnerable to attack by being easily exposed to external attacks. ▪ Many attackers are more likely to obtain basic knowledge. through open source and technical information of major infrastructure
Complete ness (Intention al)	As the role and purpose of major infrastructures become more diverse intentional attacks are elaborated and expanded	▪ The emergence of a new type of cyber attack that is difficult to cope with existing known security technologies. ▪ The types of attacks vary from internal threats to organized crime and terrorism.

Table 4. Risk management for major infrastructure

Character	Main Content
Risk identification	▪ Identify risks and threats by considering the dependencies and interdependencies of major infrastructure
Setting goals of security infrastructure	▪ Establish national goals and prioritization strategies to improve security and elasticity ▪ Establish and set goals competencies to address activities and resources as well as identified risks and threats
Implementing activities for risk management	▪ Prioritize and enforce major infrastructure risk management activities by analyzing and adjusting the importance of infrastructure, cost and risk reduction potential through the collaboration of professional and operating organizations at the national level
Measurement	▪ Analyze and evaluate the threats of major infrastructures (quantitative / qualitative). ▪ Audit and supervise the risk management process. ▪ Develop direct / indirect indicators of risk management activities, and evaluate the effectiveness of risk management efforts at each stage.
Improving security management	▪ Report on implementation of change through security management, e-evaluation, strategy and goal achievement and integrate improvements and effects into future plans.

현재, 국내에서는 주요 기반 시설에 대한 보안 위험을 정량적으로 평가할 수 있는 표준이 존재하지 않으며, 이를 위한 다양한 연구가 현재 진행 중에 있다[10-13]. [12]에서는 국내 전력 SCADA 시스템의 사이버 보안 위험 평가를 위한 정량적 방법론에 대한 연구를 진행했으며, 위험(T, Threat), 취약성(V, Vulnerability), 자산(A, Asset)이 조합되어 실질적으로 발생 가능한 위험(R, Risk)을 정의하였으며, 수식 (1)과 같이 해당 인자간의 관계를 공식화하였다.

$$R = T \times V \times A \tag{1}$$

또한 기존 IT 시스템에서의 보안위협을 분석하고, 전력시스템에 대한 적용 개연성을 분석하였다. 산업제어시스템에서의 위협은 물리적으로 구분되는 컴포넌트(Component) 기반 공격와 네트워크 대상으로 한 프로토콜로 분류하였고, 일반적인 SCADA 시스템의 컴포넌트 및 네트워크 구성에서 현재까지 알려지 침해 사례를 기반으로 위협의 가중치(Weight)를 정의하였다.

Table 5는 기존 IT 시스템 환경에서 알려진 시스템 위협과 SCADA 시스템을 구성하는 컴포넌트 및 네트워크 회선과의 상관성을 표현하는 행렬(Marix)로써 $V_{i,j}$로 표기한다. 이는 정보 자산의 가치를 분석하기 위해 종래 연구된 IT 설비가 공격당했을 때의 기대정전비용(expected interruption cost)을 기준으로 산정하였다. Fig. 5는 지역 RTU와 전력계통 모선(연관성)을 도식화 한 것으로, 이를 통하여 수식 (2)와 같이 자산 가치를 계산식으로 도출하였다.

$$A_n = \sum_{k=1}^{p} (LV_{nk} \times OC_{nk}) \tag{2}$$

수식 (2)에서 $LV_{nk}(C)$는 해당 설비의 소실 가치(Lost value)이고, $OC_{nk}(P)$는 해당 설비가 위협에 노출되었을 때 발생할 수 있는 기대 정전비용(Outage cost)으로 표현하며 C는 통신설비(Communication infrastructure), P는 전력계통(Power system)을 의미한다. 여기서 k는 n번째 자산의 하위 구성성분으로써 n번째 자산이 여러 하위요소로 구성되어 있을 때를 일반화하였다. Fig. 4의 예를 든다면, 말단 RTU 단이 3개의 RTU로 구성되어 있을 때 $k=3$이라고 할 수 있다.

Table 6는 위협 수준의 정량적 데이터로 Matias Negrete-Pincetic, Burris 등의 기존 전력 시장에서 통계 기반으로 사이버 위협 및 영향을 정량화한 연구[14]를 근거로 공격 발생빈도, 공격 형태별 피해 규모 등을 산정하여 사이버 위협에 대한 가중치를 정규화하였다.

Table 5. Matrix of risks for major infrastructure[12]

Component / Risk factor	SCADA server	TCP/IP	Serial	RTU, TCP/IP Terminal
Eavesdropping	V_{0101}	V_{0102}	V_{0303}	V_{0404}
Traffic Analysis	V_{0201}	V_{0202}	V_{0303}	V_{0404}
EM/RF Interception	V_{0301}	V_{0202}	V_{0303}	V_{0404}
Indiscretions by Personnel	V_{0401}	V_{0202}	V_{0303}	V_{0404}
Media Scavenging	V_{0501}	V_{0202}	V_{0303}	V_{0404}
Trojan Horse	V_{0601}	V_{0202}	V_{0303}	V_{0404}
Trapdoor (Backdoor)	V_{0701}	V_{0202}	V_{0303}	V_{0404}
Service Spoofing	V_{0801}	V_{0202}	V_{0303}	V_{0404}
Masquerade	V_{0901}	V_{0202}	V_{0303}	V_{0404}
Bypassing Controls	V_{1001}	V_{0202}	V_{0303}	V_{0404}
Authorization Violations	V_{1101}	V_{0202}	V_{0303}	V_{0404}
Physical Intrusion	V_{1201}	V_{0202}	V_{0303}	V_{0404}
Replay	V_{1301}	V_{0202}	V_{0303}	V_{0404}
Theft & Illegitimate Use	V_{1401}	V_{0202}	V_{0303}	V_{0404}
Denial of Service	V_{1501}	V_{0202}	V_{0303}	V_{0404}

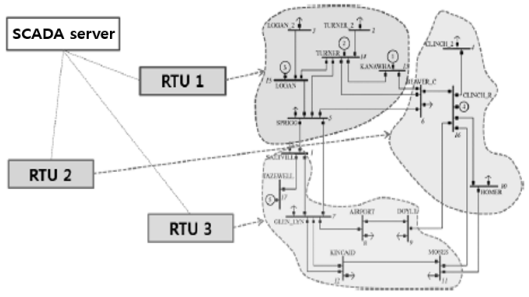

Fig. 4. Correlation of RTU and power system

또한 Table 7은 취약성의 경우 해당 위협이 실현되는 여부와 상관관계가 있음으로 정의하고(위협=외생변수, 취약성=내생변수), 취약성(V)을 위협이 발생한 경우에 완전치를 통과시킬 경우를 1, 그리고 점차 낮아져서 하나도 통과시키지 않을 경우를 0으로 정의($0 \leqq V \leqq 1$)하였다. 또한, 과거의 연구에서 취약성 데이터가 없는 경우 0.5(50%), 전력 계통 구성 성분별(서버, 통신선로, RTU) 보안 강도 우선 순위를 매기고 여기에 50%의 취약성을 적용하였다. 예를 들어, 보안의 강도는 서버가 가장 강하고 하위로 내려갈수록 작다고 판단할 수 있으므로 SCADA 서버, TCP/IP 구간, 시리얼 구간, RTU의 우선순위로 가중치를 부여하였다.

또한, 정전비용은 2008년도 한국전기연구원에서 수행한 연구보고서를 근거로 Table 8을 도출하였다. Table 6, 7에서 산출된 위협, 취약성 가중치를 기반으로, 1시간 정

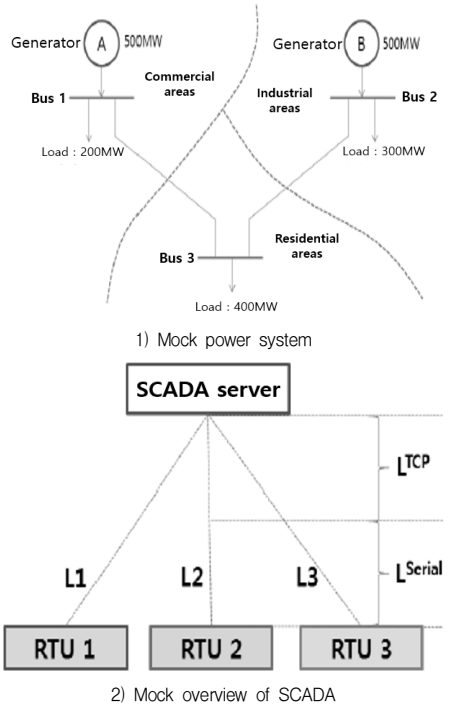

Fig. 5. Mock correlation of RTU and power system

전을 기준 주거용 2,800(원/kW), 산업용 127,420(원/kW), 상용용 37,365(원/kW) 기준[17]으로 기대정전비용을 계산하여, Fig. 5의 모의 전력 계통으로 시물레이션 결과 Table 9과 같다.

[12]의 연구에서는 국내 전력계통 산업제어 시스템의 보호 자산 위협과 취약성을 고려한 위험 비용 모델링 과정이 비교적 체계적으로 이루어졌다. 다만, 취약성 가중치를 판단함에 있어 서버, 통신선로, RTU 등의 취약성 우선순위 결정에서 서버가 가장 취약성이 낮고, RTU가 가장 취약하다는 것과 산업제어 시스템 구성 개체간 상대적인 취약성을 50%로 가정하는 것은 논리적 근거가 부족하다. 오히려, 소프트웨어적으로 본연의 기능을 조작할 수 없는 RTU가 취약성이 가장 낮다고 판단할 수 있다. 또한, 상기 연구에서는 평가 대상 시스템의 논리적, 물리적 제어 수단의 구성에 따른 취약성 및 위협 영향이 보안 위험 비용 계상에 고려되어 있지 않으며, 제어 계층(PLC, PAC 등)에 대한 취약점 및 위험 요소는 고려되지 않았다(최근, 제어 계층 통신에도 아날로그 기반에서 디지털 기반으로 프로토콜이 변화하고 있으며, 하드웨어 변조 가능성도 있음).

Table 6. Quantificational results for risks of major infrastructure[12]

	SCADA server	L_1^{TCP}	L_2^{TCP}	L_3^{TCP}	L_1^{Serial}	L_2^{Serial}	L_3^{Serial}	RTU1	RTU2	RTU3	Total
Eavesdropping	0.0072	0.0182	0.0182	0.0182	0.018	0.018	0.018	0.0016	0.0016	0.0016	0.1206
Traffic Analysis	0	0	0	0	0	0	0	0	0	0	0
EM/RF Interception	0	0	0	0	0	0	0	0.0132	0.0132	0.0132	0.0396
Indiscretions by Personnel	0.04	0	0	0	0	0	0	0	0	0	0.04
Media Scavenging	0.04	0	0	0	0	0	0	0	0	0	0.04
Trojan Horse	0.032	0	0	0	0	0	0	0.0160	0.0160	0.0160	0.08
Trapdoor (Backdoor)	0.032	0	0	0	0	0	0	0.0160	0.0160	0.0160	0.08
Service Spoofing	0.032	0	0	0	0	0	0	0.0160	0.0160	0.0160	0.08
Masquerade	0	0	0	0	0	0	0	0.0363	0.0363	0.0363	0.1089
Bypassing Controls	0	0	0	0	0	0	0	0.0363	0.0363	0.0363	0.1089
Authorization Violations	0.048	0	0	0	0	0	0	0.0220	0.0220	0.0220	0.114
Physical Intrusion	0.0216	0.035	0.035	0.035	0.036	0.036	0.036	0.0044	0.0044	0.0044	0.2478
Replay	0	0	0	0	0	0	0	0.0363	0.0363	0.0363	0.1089
Theft & Illegitimate Use	0	0	0	0	0	0	0	0.0363	0.0363	0.0363	0.1089
Denial of Service	0.064	0.074	0.074	0.074	0	0	0	0	0	0	0.286
Total	0.3168	0.1272	0.1272	0.1272	0.054	0.054	0.054	0.2344	0.2344	0.2344	

Table 7. Quantificational results for weakness of major infrastructure[12]

	SCADA server	L_1^{TCP}	L_2^{TCP}	L_3^{TCP}	L_1^{Serial}	L_2^{Serial}	L_3^{Serial}	RTU1	RTU2	RTU3
Vulnerability level	0.0179	0.0357	0.0357	0.0357	0.0536	0.0536	0.0536	0.0714	0.0714	0.0714

Table 8. Calculation for interruption cost of power system[15]

	SCADA server	L_1^{TCP}	L_2^{TCP}	L_3^{TCP}	L_1^{Serial}	L_2^{Serial}	L_3^{Serial}	RTU1	RTU2	RTU3
	All areas	Commercial areas	Industrial areas	Residential areas	Commercial areas	Industrial areas	Residential areas	Commercial areas	Residential areas	Industrial areas
Power outage cost $OC_n^k(P)$ [Million won]	46,819	7,473	38,226	1,120	7,473	38,226	1,120	7,473	38,226	1,120

Table 9. Results of risk estimation considering risk and weakness[12]

	SCADA server	L_1^{TCP}	L_2^{TCP}	L_3^{TCP}	L_1^{Serial}	L_2^{Serial}	L_3^{Serial}	RTU1	RTU2	RTU3
Threat(T)	0.3168	0.1272	0.1272	0.1272	0.054	0.054	0.054	0.2344	0.2344	0.2344
Vulnerability(V)	0.0179	0.0357	0.0357	0.0357	0.0536	0.0536	0.0536	0.0714	0.0714	0.0714
Assets(A) [Million won]	46,819	7,473	38,226	1,120	7,473	38,226	1,120	7,473	38,226	1,120
Risk(R) [Million won]	265.50	33.94	173.59	5.09	21.63	110.64	3.24	125.07	639.76	18.74
Ratio of risk(%) [threat 1 case]	0.57%	0.45%	0.45%	0.45%	0.29%	0.29%	0.29%	1.67%	1.67%	1.67%

[12]의 연구 사례 분석을 통해, 국내 주요 도메인의 기반 시설에 적합한 사이버 보안 평가 도구 개발을 위해 필요한 연구방향을 다음과 같이 제안한다.

1. 국내 주요 도메인의 정보자산 비용 산출 방안 연구
 - 예 : 전력 계통의 경우 기대정전비용 산출

2. 산업제어 시스템 특성별 구성 요소에 대한 취약성 정량화 연구
 - 컴포넌트 : SCADA 서버, RTU, PLC, PAC
 - 네트워크
· Modbus, RTU, RP-570, Profibus, Conite 1 등 구형 프로토콜
· IEC 60870-5-101 또는 IEC 60870-5-104, IEC 61850, DNP3, OLE 등 상호연동형 프로토콜

3. 논리적 · 물리적 제어에 따른 취약성 상관관계 연구
 - 애플리케이션 firewall, 백신 등
 - SCADA 서버 및 네트워크 인프라에 설치되는 라우터, 방화벽 등
 - 네트워크 물리적 망분리

4. 보안 정책, 보안 조직, 인적 자원 보안, 제어 정책, 운영 관리에 따른 가중치 정량화 연구
 - 보안 위험 정량 평가를 위한 질의어 세트 개발
 - 질의어 기반 정량적 보안 평가 및 권고

5. 결론

본 논문에서는 미국의 국가 주요 기반시설 사이버보안 평가도구인 CSET을 이용하여, 국내에 바로 도입이 가능한지의 여부를 우선적으로 검토하였다. 하지만 이는 국가별 속성의 차이로 인해 국내 국가 주요 도메인 시설에 바로 적용하는 것은 어려운 것으로 판단된다. 현재 국내에서는 보안 위협을 정량적으로 평가할 수 있는 표준이 존재하지 않은 상태에서 이를 위한 연구가 진행중인 것으로 조사되었다. 이에, CSET의 보안 평가 방법과 접근방식이 유사한 국내 전력 계통의 사이버 보안 평가 방법에 대한 연구를 소개하였고 분석하였으며, 그 결과로써 기존 연구의 문제점과 국내 사이버 보안 평가 도구 도입을 위해서 선결해야할 문제점을 제시하였다. 따라서 향후 국내에 적합한 보안 평가 도구 적용을 위한 문제 해결 및 본 논문에서 제시한 방향으로의 많은 연구가 필요하다.

REFERENCES

[1] HelloT. (2010). *Control system publication and security issues.* HelloT(Online). http://magazine.hellot.net/magz/article/articleDetail.do?flag=all&showType=showType1&articleId=ARTI_000000000035281&articleAllListSortType=sort_1&page=1&selectYearMonth=201009&subCtgId

[2] G. N. Ericsson. (2010). Cyber security and power system communication—essential parts of a smart grid infrastructure. *IEEE Transactions on Power Delivery, 25(3),* 1501-1507.

[3] T. H. Woo. (2013). Systems thinking safety analysis: nuclear security assessment of physical protection system in nuclear power plants. *Science and Technology of Nuclear Installations,* 2013.

[4] Y. Zhang, L. Wang, Y. Xiang & C. W. Ten. (2015). Power system reliability evaluation with SCADA cybersecurity considerations. *IEEE Transactions on Smart Grid, 6(4),* 1707-1721.

[5] ICS-CERT. *Assessments.* CEST Cyber Security Evalutaion Tool. https://ics-certus-cert.gov/Assessments

[6] ICS-CERT. *Downloading and Installing CSET.* CEST Cyber Security Evalutaion Tool. https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET.

[7] WIKIPEDIA. *SCADA.* https://en.wikipedia.org/wiki/SCADA

[8] NCS. (2004). *Supervisory Control and Data Acquisition (SCADA) Systems.*

[9] C. K. Lee. (2004). *Design of an Integrated I&C System* Daejeon : KAERI.

[10] Y. R. Choi. (2009). *Development of IT-based Cyber Security Technology for Nuclear Power Plant.* Daejeon: KAERI.

[11] Y. J. Kim, J. H. Lee & J. I. Lim. (2009). A Study on the Secure Plan of Security in SCADA Systems. *Journal of the Korea Institute of Information Security & Cryptology, 19(6),* 145-152.

[12] D. J. Kang, J. J. Lee, Y. Lee, I. S. Lee & H. K. Kim. (2013). Quantitative Methodology to Assess Cyber Security Risks of SCADA system in Electric Power

Industry. *Journal of the Korea Institute of Information Security & Cryptology, 23(3),* 445-457.

[13] H. Kim. (2009). *Analysis of Overseas System based Evaluation Cases and Technology.* Naju: KISA.

[14] M. Negrete-Pincetic, F. Yoshida & G. Gross. (2009, July). Towards quantifying the impacts of cyber attacks in the competitive electricity market environment. *In IEEE Power Tech Conference* (pp. 1332-1336).

[15] Korea Electrotechnology Research Institute. (2008). *A Study to investigate Industrial Customer Interruption Cost for Power System Planning.* Seoul : Korea Electrotechnology Research Institute.

김 현 일(Kim, Hyun Il) [정회원]

- 2014년 2월 : 공주대학교 응용수학과 학사(이학사)
- 2014년 3월 ~ 2016년 2월 : 공주대학교 융합과학과 석사(공학석사)
- 2016년 2월 ~ 현재 : 공주대학교 융합과학과 박사과정
- 관심분야 : 데이터 보안, 시스템 보안, 정보보호
- E-Mail : hyunil89@kongju.ac.kr

박 경 연(Park, Kyung Yun) [정회원]

- 2002년 2월 : 연세대학교 경영학사(경영학사)
- 2010년 2월 : 충남대학교 경영석사(경영학석사)
- 2017년 3월 ~ 현재 : 공주대학교 융합과학과 박사과정
- 2000년 10월 ~ 2004년 9월 : 삼일회계법인
- 2004년 11월 ~ 2007년 3월 : 한영회계법인
- 2007년 4월 ~ 2011년 10월 : 한국연구재단 기금사업팀
- 2011년 11월 ~ 현재 : 신우회계법인 이사
- 관심분야 : 정보보호 기술, 정책 및 경영
- E-Mail : cpakypark@hanmail.net

서 창 호(Seo, Chang Ho) [정회원]

- 1990년 2월 : 고려대학교 수학과 학사(이학사)
- 1992년 2월 : 고려대학교 수학과 석사(이학석사)
- 1996년 8월 : 고려대학교 수학과 박사(이학박사)
- 1996년 8월 ~ 1996년 12월 : 국방과학연구소 선임연구원
- 1996년 12월 ~ 2000년 2월 : 한국전자통신연구원 선임연구원, 팀장
- 2000년 2월 ~ 현재 : 공주대학교 응용수학과, 융합과학과 교수
- 관심분야 : 암호알고리즘, PKI, 무선인터넷 보안, 시스템 보안, 정보보호 등
- E-Mail : chseo@kongju.ac.kr

문 대 성(Moon, Dae Sung) [정회원]

- 2007년 2월 : 고려대학교 전산학과 박사(공학박사)
- 2009년 3월 ~ 현재 : 과학기술대학원대학교 정보보호공학 전공책임교수
- 2000년 12월 ~ 현재 : 한국전자통신연구원 정보보호연구본부 책임연구원
- 관심분야 : 정보보호, 네트워크보안, 영상처리, 바이오인식
- E-Mail : daesung@etri.re.kr