국내 산업제어시스템 평가 도구 도입을 위한 CSET 적용 방안 검토

이현영, 신명진*, 박태준**
전남대학교(대학원생), *전남대학교(학부생), **전남대학교(교수)
brasd9806@jnu.ac.kr, *195533@jnu.ac.kr, **taejune.park@jnu.ac.kr

Review of CSET application plan for introduction of domestic industrial control system evaluation tool

Lee Hyun Young, Shin Myung Jine*, Park Tae June**
Chonnam National Univ.

요 약

산업제어시스템은 사이버 공격에 의한 사고시 경제적 손실은 물론 공공의 안전에 미치는 영향이 매우 크다. 최근 미국 원전의 침해 사고뿐만 아니라, 이란의 원자력시설이나 중국의 에너지 관련 주요 기반시설에서 바이러스 침해와 같은 피해가 증가하는 추세로 보안 문제가 대두되고 있다. 이러한 보안 취약점에 대응하기 위해 제어시스템 환경에 대해 보안 취약성을 평가할 수 있는 보안 평가 도구가 필요하다. 따라서, 본 논문에서는 현재 국내 산업제어시스템의 보안 평가 제도 상황을 살펴보고 미국의 사이버 보안 평가 도구인 CSET(Cyber Security Evaluation Tool)를 분석하여 장단점을 살펴보고자 한다.

Ⅰ. 서 론

산업제어시스템은 제어 및 상태 감시 및 관리를 위해 다양한 산업 분야에 폭 넓게 사용되고 있다. 산업제어시스템은 초기에 외부 네트워크와 연결을 물리적으로 차단하여 외부의 공격으로부터 안전하다고 평가받아왔던 것과는 달리, 산업제어시스템의 개방화로 인해 기업의 정보호화 기기 및 시스템에 대한 보안 위협뿐만 아니라, 산업제어시스템을 대상으로 심각한 보안 문제가 발생하고 있다. 대표적인 보안사고 사례를 보면 우크라이나 전력 발전소 제어 시스템 악성코드 감염(2015년 12월)으로 8만여 가구가 정전 피해를 받는 등 대규모 인프라 주요시설의 피해가 발생하였다[1]. 보안에 대한 고려가 부족한 산업제어시스템의 특성을 노리고 공격을 한 것인데, 과거부터 산업제어시스템을 대상으로 한 공격은 계속 발생하고 있으며 최근 들어 그 빈도가 점점 증가하고 있다.

기존의 정보 시스템 분야의 보안 방법은 새롭게 발생하고 있는 보안 위협에 대해 대응하는 것은 한계가 있다. 이에 따라, 선진국들은 ICS 보안 등 다양한 관점에서 보안 평가를 할 수 있는 도구들이 마련되어 있는데 미국에서는 INL이 개발한 주요 기반시설 사이버 보안 평가 도구인 CSET을 제공하고 있고, 영국에서는 CSET보다 간단하게 평가 항목을 제공하고 있다[2]. 하지만, 국내에서는 산업제어시스템을 대상으로 규제 가이드 검토 도구로 활용된 사례가 없다. 새로운 사이버 공격기법을 조기에 발견할 수 있어야 안전하게 제어시스템을 운영할 수 있는데, 이를 위해서는 세계 최고 수준인 미국의 사이버 보안 평가 도구인 CSET을 활용하여 국내도 평가 도구 개발을 연구할 필요가 있다. 본 논문에서는 국내 산업제어시스템 보안성 평가 현황에 대해 살펴보고 CSET 분석 및 도입 시 얻는 이점에 대해 분석한 후, 결론을 짓는다.

Ⅱ. 본론

2.1 국내 산업제어시스템 보안성 평가 현황

국내에는 산업제어시스템에 대한 보안성을 평가하는 제도는 없으나, 현재 원전 계측제어 시스템인 사이버 보안 통합평가도구 CSAMS(Cyber Security Assessment and Management System)을 제시하였다. 하지만, 아직 이 시스템을 도입하여 평가한 사례는 없다.

국내의 규정 현황을 간단히 살펴보면 정보통신기반보호법 및 주요정보통신기반시설 취약점 분석 평가제도에 산업제어시스템 대상 일부 반영되어 있지만, PLC, DCS 컨트롤러, 제어 애플리케이션과 같은 OT 시스템에 대한 평가 기준이 매우 제한적이어서 활용에는 한계가 있다. 보안적합성 검증제도와 정보보호제품 평가 · 인증제도는 IT 정보보호 제품 대상으로 산업제어시스템의 OT 제품에 대한 보안성 평가 제도로 활용하기에 부적절해 보인다[3]. 따라서, 국외 기존 제도 활용 방안을 검토하고, 산업제어시스템 보안성 평가를 위해 별도의 국내 제도 마련이 필요하다.

2.2 CSET 분석

CSET(Cyber Security Evaluation Tool)은 단별 프로세스를 통해 네트워크 방어자를 안내하여 네트워크에서 사이버 보안 관행을 평가하는 데스크톱 소프트웨어 도구이다. CSET은 자산 소유자가 시스템 구성 요소 및 아키텍처, 운영 정책 및 절차에 대한 일련의 자세한 질문을 함으로써 정보 및 운영 시스템 사이버 보안 관행을 평가할 수 있도록 지원한다. 정보 기술(IT) 및 산업제어시스템(ICS) 네트워크 모두에 적용되는 CSET을 통해 사용자는 인정된 많은 정부 및 산업 표준 및 권장 사항을 사용하여 사이버 보안 태세를 종합적으로 평가할 수 있다[4]. Table 1에 나오는 위험 관리 프로세스에 따른 제어 표준 및 질문 세트를 포함하고 있다.

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 800-82 Rev 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 Pipline Security Guidelines April 2011	TSA
Universal Questions Set	Universal

Table 1. Security standard from major infrastructure in the US[2]

먼저 CIA 수준을 선택한 후, 당사 산업체에 적용될 수 있는 보안 표준을 선택한다. 선택된 표준들로 제공되는 질문 세트를 사용하여 사이버 보안 평가 대상 시스템을 출력한다. 설문지가 완료되면 CSET은 사이버 보안 태세를 높이기 위해 권장 사항의 우선순위 목록뿐만 아니라 강점과 약점 영역을 보여주는 차트 대시보드를 제공한다. 그리고 사용자는 네트워크 다이어그램을 이용하여 사이버 보안 영역, 중요 구성 요소 및 네트워크 통신 경로를 손쉽게 정의할 수 있다[5].

2.3 국내 CSET 도구의 도입으로 인한 이점

국내는 산업제어시스템에서 발생하는 위험을 효과적으로 관리하는데 필요한 보안 기술 및 제도를 채택하는 데 뒤처져 있다. 제안된 CSET 도구는 현재 ICS의 사이버 보안 수준을 평가하기 위해 채택할 수 있는 접근 방식을 대표한다. 이 CSET 도구의 방법론은 강점과 약점을 식별하고 보안 허점을 효과적으로 연결하는 방법에 대한 모범 사례 권장 사항도 제공한다.

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, 2013년 원자력 발전소에서 물리적 시스템 자산을 보호하기 위해 활용한 사례가 있다. 또한, 2015년 미국 FFC(Federal Facility Council)에서 CSET을 이용한 사이버 보안 빌딩 제어 시스템 적용을 검토하기도 하였다[2].

이처럼, CSET을 이용하여 얻을 수 있는 이점들은 이와 같다. 기본 사이버 보안 태세 및 제어시스템 네트워크를 평가하는 일관된 수단을 제공하고 사이버 보안 권장 사항 지정하여 표준 기반 정보 분석을 사용한 보고서를 제공한다. 이를 통해 더 자세한 정보를 검토할 수 있고, 경영진 및 다른 직원과 커뮤니케이션할 때 사용할 전문적으로 디자인된 보고서를 제공받을 수 있다. 하지만, CSET이 수행할 수 없는 작업들이 있다. 사용자 입력의 정확성 검증을 할 수 없고, 알려진 모든 사이버 보안 취약점 식별을 하기에는 어려운 점이 있다[6].

현재 국내는 산업제어시스템에 사이버 보안 기술 개발은 아직 확립되어 있지 않은 상태이다. 국내에 CSET을 도입함으로써 얻는 이점들은 다음과 같다. 먼저, 사이버 보안 태세를 확립하고 산업제어시스템 네트워크를 통한 가시성 데이터 확보가 가능해진다. 또한, 산업제어시스템에 보안 기술을 적용하기 위한 체계적이고 일관된 평가자료를 제공하여 사이버 공격으로부터 보호함으로써 안전성, 신뢰성 및 가동율을 증대할 수 있다. 금융 및 IT 산업에서 일어나고 있는 해킹이나 바이러스에 의한 시스템 서비스거부 등과 같은 사고가 산업제어시스템에서 일어날 때 사회적인 파장은 매우 클 것이다. 따라서 본 평가 도구를 활용함으로써 산업제어시스템 사이버보안 사고를 예방하여 ICS에 대한 대국민 수용성을 제고할 수 있을 것이다.

Ⅲ. 결론

ICS 보안은 더 이상 과거와 같이 간과해서는 안되는 주요한 사안이다. 제어시스템의 운영 중단은 타 정보 시스템과는 비교할 수 없을 정도의 큰 피해를 일으킬 수 있기 때문에 이를 안전하게 보호하는 보안 기술 및 이와 관련한 체계적인 규제에 대한 연구가 필요하다.

본 논문에서는 국내 산업제어시스템 보안성 평가의 종류와 그 한계 및 새로운 평가 마련의 필요성에 대해 살펴보고, CSET 평가의 장단점에 대해 알아보았다. 국내 보안성 평가 방식과 비교하여 CSET 도입 사례와 CSET을 도입함으로써 얻는 이점들을 살펴보았을 때, 향후 국내 사이버 보안 평가제도 확립 시 CSET가 기초적인 방향성을 제시할 수 있을 것으로 생각된다. 하지만 CSET 국내 도입 시, CSET 평가의 사용자 입력값에 대한 정확성 검증과 보안 취약점 식별 범위 확장 등의 보완이 필요하다.

ACKNOWLEDGMENT

이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. 2022R1C1C1006967).

참 고 문 헌

[1] 김인순. “우크라이나 정전은 ‘사이버 테러’”, 전자신문, 2016.01, (https://www.etnews.com/20160106000240)

[2] 김현일, 박경연, 서창호 and 문대성. (2019). 보안성 평가 도구 사례 분석 연구. 디지털융복합연구, 17(1), 347-356.

[3] 김우년, 박응기 and 김신규. (2019). 4차 산업혁명 시대의 산업 제어시스템 보안성 평가 방안 연구. 한국통신학회논문지, 44(5), 943-956.

[4] CISA. “CISA’s CSET Tool Sets Sights on Ransomware Threat”, 2021.06, (https://www.cisa.gov/uscert/ncas/current-activity/2021/06/30/cisas-cset-tool-sets-sights-ransomware-threat)

[5] National Cybersecurity and Communications Integration Center(NCCIC), “NCCIC ICS CYBER SECURITY EVALUATION TOOL”

[6] RECIPROCITY, “새로운 사이버 보안 평가 도구 모델에 대해 알아야 할 사항”, 2021.08, (https://reciprocity.com/blog/what-you-should-know-about-the-new-cyber-security-evaluation-tool-model/)

[7] 황재훈, 이서현. “ICS 보안, 더 이상 바치해선 안된다”, AhnLab, 2021.04, (http://www.haesoldata.co.kr/ahnlab20210430/)