산업제어시스템의 보안 기술 연구 동향 및 고찰

이영헌, 류정현, 박종혁*
*서울과학기술대학교 컴퓨터공학과
e-mail : {movestos, jh.ryu, jhpark1}@seoultech.ac.kr

Research Trends and Considerations of Security Technology of Industrial Control System

Young Hun Lee, Jung Hyun Ryu, Jong Hyuk Park*
Department of Computer Science and Engineering, Seoul National University of Science and Technology (SeoulTech), Seoul, 01811, REPUBLIC OF KOREA
e-mail : {movestos, nykim, jhpark1}@seoultech.ac.kr

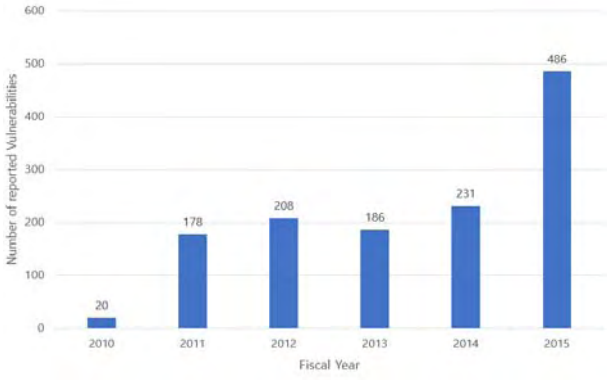
요 약

최근 국가기반시설을 제어하고 관리하는 산업제어시스템에 대한 사이버보안 위협이 증가함에 따라 보안의 중요성이 증가하고 있다. 산업제어시스템에서의 보안 기술은 일반적인 IT 시스템의 보안 기술과는 많은 차이가 있다. 산업제어시스템과 IT 시스템은 인간이 컴퓨터 시스템을 통해 정보를 처리하는 것은 같지만 IT 시스템은 정보 처리의 효율성을 위해 시스템을 사용하는 반면, 산업제어 시스템은 시스템의 효율성을 위해 정보를 처리하는 부분으로 이에 알맞은 새로운 보안 체계 구성이 필요하다. 초기에는 폐쇄망 위주로 구성되었던 산업제어시스템에서 ICT(Information & Communication Technology) 발전으로 외부로부터의 사이버 위협이 가중되었다. 편리성과 효율성이 증대된 만큼 ICT의 취약점 또한 산업제어시스템에서 문제가 발생하고 있지만, 현재 산업제어시스템의 보안 기술에 대해서는 국내에 널리 알려지지 않고 있다. 본 논문에서는 산업제어시스템 및 보안정책에 대해 논의한다. 관련 보안사고의 사례 및 보안 기술을 살펴봄으로써 미래 산업제어시스템의 발전과 보안 공격에 대한 충분한 보안 체계를 구축하여 종합적이고, 적합한 보안 대책을 마련하는 것에 도움이 될 것이다.

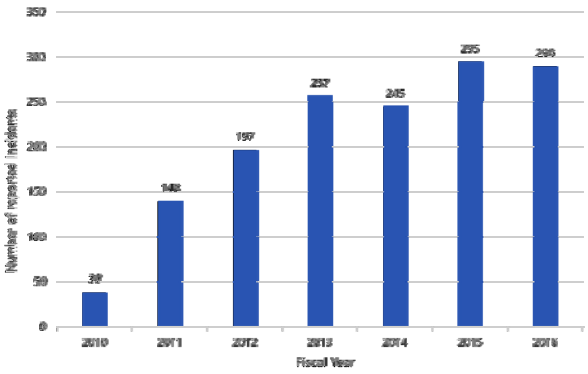
1. 서론

현재 산업제어시스템은 산업현장에서 감시와 관리, 제어를 위해 쓰이고 있는 다양한 형태의 제어시스템이라고 한다. 초기 산업제어시스템은 독립적인 네트워크를 구성하였고 외부 네트워크와 연결을 물리적으로 차단하여 외부의 공격으로부터 안전하다고 평가받고 있었다. 하지만 최근 정보통신 기술의 발전으로 국가기반시설을 효율적으로 제어 및 관리하기 위해 폐쇄적인 환경에서 표준화되고 공개된 기술로 전환되었다. 이로 인해 외부의 사이버 공격에 노출될 가능성이 커지고 공격 방법이 다양화되고 있다. 이러한 추세는 미국 국토안보부 산하의 CS-CERT에서 발표한 산업제어시스템 보안취약점과 보안사고 통계자료로 (그림 1), (그림 2)에서 보여준다 [1][2]. 특히 2010년 20건에 불가하던 취약점의 개수는 2015년 486건으로 크게 증가했고, 보안사고 또한 2010년 39건에서 2016년 290건까지 증가하여 앞으로 더 많은 보안취약점과 보안사고가 발생할 것으로 예측된다.

국내 산업제어시스템의 보안 관리체계 동향으로는 산업제어시스템에 대한 관계 법령(2001년 정보통신기반보호법)의 제정으로 시작된다. 법의 내용을 보면 국가 금융, 운송, 에너지, 국방 등의 전자 제어관리 시스템 및 정보통신망을 정보통신기반시설로 지정하도록 하였으며, 2001년부터 2013년까지 정보통신기반시설에 대한 취약점 분석, 평가 기준을 1차에서 3차에 걸쳐 수립 및 배포하였다 [3]. 이는 새로운 유형에 대한 취약점 공격 방법을 예방하기 위함이다.



(그림 1) 산업제어시스템 보안취약점 발견 건수



(그림 2) 산업제어시스템 보안사고 건수

산업제어시스템의 보안에 관한 관리실태에 대해서는 정보보안 관리실태 평가로 이루어진다. 5가지 항목에 대해서 평가되는 이 평가는 정보보안 정책, 정보자산 보안관리, 인적 보안, 사이버 위기관리, 전자정보보안, 정보시스템 보안으로 나누어지며 각 항목에 대해서 점수를 합산하여 5단계로 평가결과를 산출한다. 관리실태 평가는 2004년에 도입하였으며 2013년까지 국가기관, 연구기관, 공기업, 준정부기관으로 대상을 확대하여 평가를 수행하고 있다 [4].

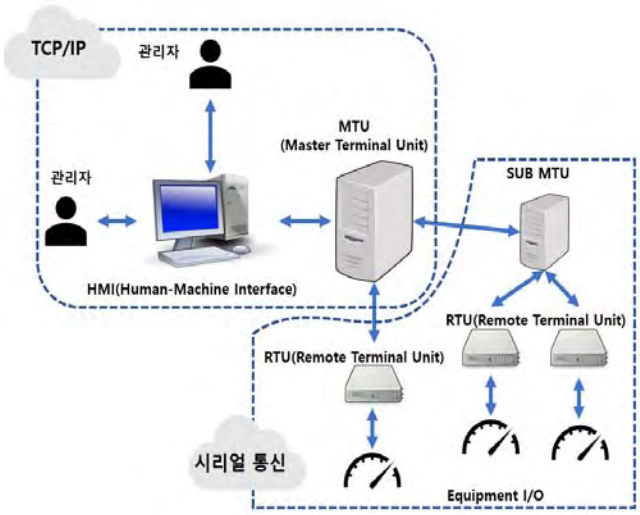
이에 따라 본 논문에서는 산업제어시스템 관련 보안 동향 및 보안 기술에 대해 논한다.

2. 산업제어시스템의 개념 및 발전과정

산업 제어시스템은 산업 생산 영역에서 사용되고 있는 여러 형태의 제어시스템을 나타내는 것으로, 국가기반시설인 전력, 수자원, 석유, 교통망, 금융망 등과 같은 운용에 핵심적인 역할을 담당한다. 보통 SCADA(Supervisory Control And Data Acquisition), DCS(Distributed Control Systems), 그리고 PLC(Programmable Logic Controllers) 제어시스템이 사용되고 있다.

그중 산업제어시스템에 많이 사용되고 있는 SCADA 시스템은 실시간으로 넓은 장소에 위치한 자원들의 정보를 수집하고 이를 중앙 컴퓨터에 전송하여 관리자가 원격으로 모니터링 또는 제어할 수 있도록 한다. SCADA 시스템은 하드웨어적으로 데이터 수집과 제어를 담당하는 MTU(Mater Terminal Unit), 데이터 전송과 센서의 모니터링을 담당하는 RTU(Remote Terminal Unit), 소프트웨어적으로는 수집된 데이터를 통해 입출력 장치로 사용되는 HMI(Human-Machine Interface)와 네트워크로 구성되어있다. (그림 3)은 SCADA의 시스템 구조를 간략히 보여준다.

초기 SCADA 산업제어시스템은 하드웨어적 위주의 형태로 구현한 1세대 모놀리식, 2세대 분산처리, 3세대 네트워크 위주로 발전해왔으며 점차 대형화, 자동화가 진행되었다 [5]. 현재는 ICT 발전으로 무선 및 클라우드 형태의 SCADA시스템이 4세대 시스템으로 진행되고 있다 [6-7].



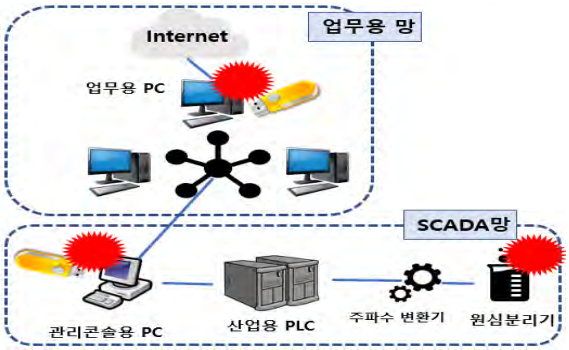
(그림 3) SCADA 시스템 구조

3. 산업제어시스템 관련 보안사고 사례

산업제어시스템은 다양한 분야에서 사용되므로 이와 관련된 보안사고에 관한 내용은 다양하다. 산업제어시스템과 관련하여 발생하였던 국내외 보안사고 사례는 <표 1>과 같다.

특히, 최초의 제어시스템 악성코드인 Stuxnet의 공격 형태를 보면 인터넷과 연결된 업무용 망을 통해 윈도우 취약점이나 제로데이 취약점을 이용한 공격을 하였다. 이후 감염 USB를 통해 SCADA망 내부까지 침투하여 SCADA의 산업용 PLC 제어시스템의 정보 탈취 또는 관리자 제어 명령 처리 함수를 변조하여 주파수 조절을 통해 원심분리기의 파괴를 유발하였다 [8].

산업제어시스템의 공격 사례와 같이 국가기반시설의 공격 사례가 계속해서 지속되고 있다. 이는 통신, 금융, 교통, 에너지체계 마비로 인해 국가 혼란 사태를 유발할 수 있으며 물리적 파괴를 통해 단순히 국민들의 불편만을 일으킬 뿐 아니라 심각한 경제적 피해, 심각한 사회 혼란을 일으켜 국가의 재앙 수준의 피해가 발생할 가능성이 있다.



(그림 4) Stuxnet 공격 시나리오

<표 1> 국내외 산업제어시스템 보안사고 사례

연도	발생국	내용	비고
2008	터키	1,760km 길이의 석유 송유관 카메라 통신 소프트웨어 취약점을 이용해 네트워크 통제 및 악성코드 삽입, 알람 무력화, 네트워크 무력화, 네트워크 장애 발생 및 석유압력 변조로 폭발사고 유도	해킹
2010	이란	우라늄 농축시설 시스템의 유지보수용 데스크톱이 직원의 실수로 스턱스넷에 감염, 원심분리기 1,000개 고장 및 교체	악성 코드
2011	한국	특정 은행 전산망 해킹으로 시스템 손상 및 금융 서비스 마비	악성 코드
2011	미국	일리노이주 상수도 시스템에 원격 침투 후 펌프 시스템 파괴	해킹
2012	사우디	정유회사 Aramco가 악성코드 Shamoon에 감염되어 네트워크 마비	해킹
2013	이스라엘	터널 보안소 요금 시스템 통한 악성코드 감염으로 고통 혼잡 발생	악성 코드
2013	한국	방송 및 금융 등 6개사 기업 전산 시스템이 악성코드로 인한 접속 장애, 시스템 파괴 등 발생	악성 코드
2014	독일철강	독일 철강회사의 용광로 제어시스템에 장애 발생	해킹
2015	우크라이나	전력 발전소 제어시스템 서비스 중단하여 정전 유발, 8만가구 정전 발생	악성 코드
2016	방글라데시	방글라데시 중앙은행 계좌 해킹되어 1000억 피해	해킹

4. 산업제어시스템의 보안기술

● White List 기반 탐지 기술

제어시스템의 설치 및 운영단계에 필요한 모든 파일과 프로세스에 대한 정보를 저장하여 등록되지 않은 정보들은 모두 차단하는 방법이다. 프로그램 또한 White Listing 관리 서버를 통해 업데이트하도록 하여 추후에 악성코드가 유입되는 것을 방지한다. 필수 정보를 저장하기 위해서는 제어시스템 제조사와 실제적 운영자 간의 협조가 필요하다.

제어시스템이 구형이거나, 기존 제어시스템의 제조사 또는 운영자의 변경이 있었다면 현실적으로 모든 내용에 대해 목록화하여 저장하는 과정에 한계점이 존재한다.

기존 범용성 환경을 위해 Black List 기반 탐지방법도 있었으나 점차 지능적으로 변화하는 공격 방법에 대응하기 위해 White List 기반 탐지방법으로 변화하였다. <표 2>는 White List 기반 탐지방법과 Black List 기반 탐지방법을 비교하였다 [9].

<표 2> White List, Black List 기반 탐지 방법 비교

	White Listing 기반 탐지 방법	Black Listing 기반 탐지 방법
처리방식	사전 예방	사후 처리
프로그램 제어	허용된 프로그램만 사용	모든 프로그램 사용 가능
자원 사용률	낮음	높음
보안 수준	높음	낮음
업데이트 주기	주기적	실시간
가용성	제한적 환경	범용적 환경

● 시그니처 탐지 기술

기존 공격에 대한 패턴에 대한 공격을 탐지하는 방식으로 기존 공격에 있어 분석이 완료된 공격은 탐지하고 차단할 수 있다. 다만, 제어시스템이 사용하는 소프트웨어에 대한 취약점 패치가 나오지 않은 시점의 공격 방법인 제로 데이(Zero Day) 공격이나 변형, 새로운 악성코드에 대한 공격에 대해서는 탐지하기 어려운 부분이 있다. 따라서 제어시스템의 보안을 담당하는 백신 및 보안제품 제조사에서 최신 탐지 패턴을 업데이트하고 실시간으로 적용해야 한다.

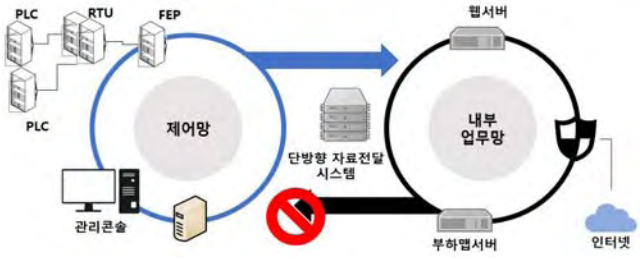
● 이상 행위 탐지 기술

평소 네트워크상 트래픽의 상태가 정상범위를 벗어나거나 시스템의 자원 사용률이 갑자기 증가하는 등 비정상적일 때 이를 탐지하여 이상 행위로 간주, 분석하는 방법이다. 이러한 방법은 기존 시그니처 탐지방법에서 탐지하지 못했던 새로운 공격기법을 탐지할 수 있다는 장점이 있다. 다만 제어시스템의 정상적인 작동 수준 내에서 공격이 이뤄지면 탐지가 어려운 단점이 있다.

● 물리적 단방향 자료전달 기술

물리적 단방향 자료전달 장치는 네트워크 간 데이터 전송 기술 중 하나로써 내부 제어시스템에서는 데이터를 보낼 수 있는 있지만, 업무망에서 제어망으로 (그림 5)와 같이 데이터를 보낼 수 있는 회선 자체를 제거한 기술이다 [10].

또한, 우리나라의 주요 정보통신 기반 시설 취약점 분석·평가 기준과 국가정보원에서는 전자제어시스템 보안가이드라인에 따르면 제어시스템은 외부 인터넷망과 내부 업무망에 대해 망분리 의무화 조치를 해야 한다고 명시되어 있다 [11].



(그림 5) 물리적 단방향 자료전달 시스템 [12]

업무망과 제어망이 물리적으로 분리되어 있으므로, 내부 업무망에서 기존 구성된 제어망 내부 장치와 설정은 변경할 수 없다는 단점이 존재한다.

5. 결론

본 논문에서는 산업제어시스템의 구성과 발전현황을 파악하고 산업제어시스템의 국내외 사고 사례를 통해 외부의 침입과 내부의 실수 등 다양한 상황에 따른 대응기술에 대해 서술하였다.

주요 국가기반 구조와 다양한 산업현장에서 운용중인 산업제어시스템은 다양한 제어 기능을 수행하고 있다. ICT를 이용한 자동화로 효율성과 편의성이 증대면서 산업제어시스템에 대한 의존도가 높아지고 있지만 이에 대한 취약점 또한 드러나고 있다.

취약점을 이용한 사이버 공격의 피해는 가상의 자산을 다루는 IT시스템과는 다르다. 실제 물리적 자산을 다루고 있는 산업제어시스템에 대한 공격은 물리적 장비파괴, 복구시간의 장기화에 따른 불편함 초래, 더 나아가 시설 이용자의 안전과 생명을 위협한다.

그러므로, 빠르게 변화하고 있는 ICT 환경에 대한 산업제어시스템의 보안 표준 개정 및 보안 체계에 관한 연구, 전문 인력 양성, 보안 산업의 활성화가 시급하다.

Acknowledgement

이 논문은 2018년도 정보(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. 2016R1A2B4011069).

참고문헌

[1] K. Stouffer, J. 외 2명, "Guide to industrial control systems(ICS) security", NIST Special Publication, vol.800, no.82, 2011.

[2] ICS-CERT, "ICS-CERT Year in Review", 2009-2016.

[3] Shahzad, A 외 3명, "the SCADA review: system components, architecture, protocols and future security trends." American Journal of Applied Sciences, vol.11, no.8, pp.1418-1425, 2014.

[4] 국가사이버안전센터, "정보보안 관리실태 평가 소개", 정보보호학회지, vol.23, no.5, pp.9-11, 2013.

[5] USACE, "Supervisory Control and Data Acquisition (SCADA) Systems for Command, Control, Communications, Computer Intelligence, Surveillance, and Reconnaissanmce (C4ISR) Facilities", TM 5-601, 2006.

[6] Ashish N Koushik1 외 1명 "4th Generation SCADA Implementation for Automation", IJARCCE vol.5, pp.629-631, 2016.

[7] 정성모, "스마트 그리드 보호를 위한 SCADA 보안 솔루션 설계", 한남대학교 일반대학원, 2010.

[8] 서정택 "국내 원자력 시설 사이버보안 기술개발 및 적용현황", 원자력안전규제 정보회의, 2017.

[9] 안철수연구소. "월간安 11월 : 최악의 악성코드 심층분석 및 대응 방안", pp.17-20, 2010.

[10] 김경호 외 4명, "제어망 특성을 반영한 물리적 일방향 자료전달 시스템 설계". 정보과학회논문지 : 정보통신, vol.40, no.5, pp.126-130. 2013.

[11] 미래창조과학부. "정보통신기반보호법 제9조". 제2013-37호

[12] 한전KDN. 물리적 일방향 자료 전달 시스템 솔루션 (1Gbps) 구성도