정 보 보 호 학 회 지
제27권 제2호, 2017. 4

스마트공장 보안성 강화를 위한 제어 시스템 보안 기술

허 신 욱*, 이 가 람*, 김 동 주*, 김 호 원**

요 약

최근 현장에서는 4차 산업혁명 이슈 확산과 함께 스마트공장에 대한 관심이 고조되고 있다. 불과 몇 년 전만 해도 정부와 연구소, 대학의 주요 관심 대상이었던 스마트공장은 현업에서 활동하는 경영진에게 스마트공장이 현재의 제조업 위기 탈출과 미래 경쟁력 확보를 위한 유일한 탈출구로 인식되어 적극적인 관심 표명으로 이어진 것으로 보인다. 현장의 경영자들은 스마트공장 실현 기술 개발과 현장 적용의 필요성을 인지하고 있지만, 적용에 대해 우려하는 부분도 아직 많이 존재한다. 예를 들어, 스마트공장 도입에 많은 금액이 필요하다는 점, 그리고 보안 취약성 문제, 기업 데이터 유출 문제가 그 대표적 우려 사항이라고 볼 수 있다. 이에 본 고에서는 투자 금액 이슈는 고려하지 않고 스마트공장을 실현하기 위한 필수 요소인 보안 취약성 문제와 이를 해결하기 위한 보안 기술에 대해 살펴보고자 한다. 즉, 스마트공장의 주요 네트워크와 플랫폼에 대한 보안 이슈 및 기술, 그리고 산업 현장의 보안 기술의 특성 등에 대해 논의하고자 한다.

Ⅰ. 서 론

스마트공장은 갈수록 떨어지는 국내 제조업의 경쟁력을 높이는 유일한 기술로 널리 인식되고 있다. 또한, 많은 사람이 스마트공장을 미래 4차 산업 혁명 변화의 가장 중심에 있다고 보고 있다. 이러한 중요성 때문에 그동안 정부와 대학, 연구소, 기업에서는 스마트공장 실현을 위해 많은 노력을 하고 있다. 특히, 산업부의 스마트공장 추진단 활동과 미래부, 산업부의 스마트공장 관련 다양한 연구/개발 지원책이 그 대표적인 사례라고 할 수 있다. 하지만, 그동안 스마트공장이 실제 제조 현장에서 그다지 활발하게 수용되지는 못했다. 그 주된 이유로는 주로 제조현장에서 스마트공장 자체에 대한 장점을 인지하지 못하는 점, 투자 금액에 대한 부담, 그리고 스마트공장화로 인한 보안 취약성 야기 및 기업 기밀 정보 유출문제와 같은 부정적인 이슈 때문이었다. 이에, 본 고에서는 이 중에서 스마트공장 활성화를 위해 중요한 요소인 보안 취약성 문제 해결 방안을 중심으로 살펴보고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 스마트공장 주요 구성 환경과 스마트공장 환경에 특화된 보안 취약성 이슈, 보안 이슈를 살펴본다. 3장에서는 스마트공장 보안 기술의 특성과 현황에 대해 살펴본다. 마지막으로 4장에서는 본 논문의 결론을 내린다.

Ⅱ. 스마트공장 환경과 보안 취약성 이슈

2.1. 스마트공장 환경

스마트 공장에 대한 다양한 정의가 존재하지만, 쉽게 공장 자동화(FA, Factory Automation)가 발전된 형태로서, IoT, 빅데이터, 클라우드, CPS(Cyber Physical System), 스마트 센서, 3D 프린팅 등 다양한 ICT 기술과 제품의 기획・설계, 생산, 유통・판매 등 제조 전 과정이 지능적으로 융합된 산업이라고 볼 수 있다. 또한, 개별 공장의 설비(장비)・공정이 생산네트워크로 연결되고 모든 생산 데이터・정보가 자동화 및 정보화되어 가치사슬 전체가 실시간 연동, 통합된 시스템이 구축됨으로써 최소비용・시간, 생산성 향상, 에너지 절감, 생산 환경 안전성 및 개인 맞춤형 제품 등 최적화된 생산 운영이 가능한 미래 공장을 실현할 수 있는 패러다임이라고 볼 수 있다. 이러한 특성을 가지는 스마트 공장은 업종별/공장 수준별 특성에 따라 다양한 형태로 나타날 수 있는데 다양한 공장 간 협업 운영이 지속됨으로써 유연한 생산체계가 구축될 수 있다.

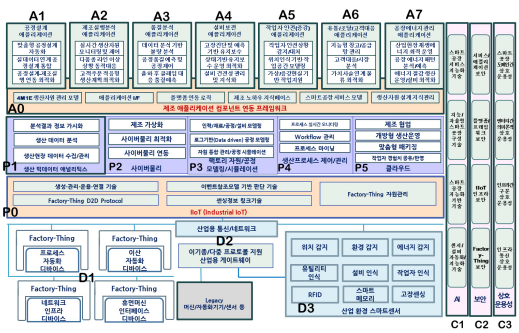
* 부산대학교 컴퓨터공학과
** 부산대학교 산업대학원 부원장

2.2. 스마트공장 주요 기술 구성 요소

아래 그림처럼 스마트공장 요소기술 영역은 크게 스마트공장 애플리케이션(A), 플랫폼(P), 센서 및 디바이스(D), 인공지능/보안/상호운용성 등 공통 요소 기술(C)로 구분할 수 있다[1,2].

스마트공장 애플리케이션(A)은 지능화 및 네트워크화된 제조현장의 각종 장비, 작업자, 시스템이 공장 내부 상황, 물류 상황, 시장, 고객 반응 등과 통합/최적 운영되는 응용 서비스를 의미한다. 플랫폼(P)은 공장 설비, 자원, 데이터를 상호 연동/운영/제어, 서비스 연동하는 수단이 되며, 센서 및 디바이스(D)는 다기능 센서, 제어기, 유무선 통신 장비, 능동적 제조관리를 위한 스마트 메모리 등, 스마트공장에서 필요로 하는 장비를 의미한다.

스마트공장에서는 인공지능과 보안, 상호 운용성을 스마트공장 주요 구성 요소에서 공통으로 필요로 하는 요소로 보고 있다. 즉, 스마트공장 주요 구성 요소 간 연동 시 데이터/서비스 간의 상호 운용성 보장을 위한 통신/인터페이스/데이터/정보 연동, 데이터/정보에 대한 지능화 처리를 통한 고부가가치 창출, 그리고 구성 요소 자체 혹은 연동시의 보안성 및 프라이버시 보호를 위한 보안 기술의 필요성이 중요하게 간주되고 있다[1].



〔그림 1〕 스마트공장 주요 기술 구성도〔2〕

2.3 스마트공장 보안 특성

2.3.1. 스마트공장 구성 제어 시스템 특성

스마트공장은 기존의 IT 시스템과 비교해 볼 때, 그 구성 요소의 특성에 있어서 많은 차이점이 있다. IT 시스템의 경우, 사용자의 개인정보와 기업 내부 데이터 보호를 위한 기밀성이 중요하게 간주된다. 하지만 스마트공장인 경우에는 생산 설비 데이터나 실시간 공정데이터 등에 대한 기밀성보다 오히려 정확한 설비 상태와 상황 인지 및 제어, 생산품질 및 수율을 위한 데이터 무결성 및 가용성이 더 중요한 요소라고 알려져 있다. 만약, 무결성과 가용성이 침해받을 경우, 생산 지연, 장비 오작동 이 발생할 수 있으며 이로 인해 사업 손실, 장비 파괴, 환경 파괴, 개인 안전 등에 악영향을 줄 수 있다.

또한 IT 시스템의 경우에는 소프트웨어에 대한 업데이트 및 패치가 용이하고 시스템 생명 주기(Life Cycle)가 3~5년으로 짧은 반면, 산업 제어 시스템에서는 소프트웨어 업데이트 및 패치가 거의 일어나지 않으며 시스템 생명 주기가 15년 이상으로 길다. 따라서 스마트공장 산업 제어 시스템에 보안 취약점이 발생할 경우 IT 시스템에 비해 대응이 더욱 어려운 상황이다.

또한, 산업 제어 시스템에서 사용되는 DNP, Modbus, Fieldbus 등과 같은 통신 프로토콜의 경우 대부분 폐쇄망에서 운영되어 식별, 인증과 같은 보안 기술을 고려하지 않았다. 이 프로토콜들은 대부분 컴퓨팅 연산 능력이 제한적인 환경에 적합하도록 설계되었고 무결성과 신뢰성을 중점적으로 고려하였다. 반면에 IT 시스템의 경우 대부분 컴퓨팅 연산 능력이 제한적이지 않고 TCP/UDP 기반의 응용프로토콜인 HTTP, CoAP, MQTT 등에 TLS/DTLS와 표준화된 보안 기술을 적용하여 사용하고 있다. TLS/DTLS의 경우 식별 및 인증, 데이터의 기밀성 및 무결성 등 통신 보안에 필요한 보안 요구사항들을 대부분 충족시킨다.

IT 시스템의 경우 오랜 시간 다양한 영역에서 보안 취약점이 노출되고 이를 해결하는 과정에서 비약적인 보안 기술의 발전이 이뤄졌다. 하지만 산업 제어 시스템의 경우 최근까지 폐쇄적으로 운영되었기 때문에 보안에 대한 관심이 거의 없었다. 최근 스마트공장이 이슈화됨에 따라 보안 기술에 대한 관심이 고조되고 있으며 이에, 스마트공장의 보안 요구사항을 충족시킬 수 있는 보안 기술 개발이 시급한 상황이다.

2.3.2. 스마트공장 보안 요구사항 및 보안 취약성

기존의 산업제어 시스템 통신/네트워크는 IP 기반의 인터넷이 연결됨에 따라 보안 취약성이 매우 높아지게

되었다. 최근 많은 관심을 받고 있는 스마트공장 역시 이러한 산업 제어 시스템을 기반으로 하고 있기 때문에, 기존 산업 제어 시스템이 가지는 보안 요구사항과 보안 취약성을 모두 가지게 된다. 따라서 이러한 보안 요구사항을 고려하고 취약성을 해결해야 할 필요가 있다.

산업 제어 시스템의 보안 요구사항은 IT 시스템과 달리 높은 신뢰성을 보장해야하기 때문에, 가용성 및 무결성이 기밀성에 비해 높은 우선순위를 가진다. 하지만 보안 취약성을 해결하기 위한 암호화 및 인증/인가 기법, 로그 저장, 모니터링 시스템, 추가적인 프로토콜 등으로 인해 가용성이 낮아질 수 있기 때문에 이러한 점을 고려하여 보안성을 강화하는 기법을 연구 및 개발할 필요가 있다.

아래 표 2에서 확인할 수 있듯이 산업 제어 시스템 관련하여 수많은 보안 취약점 및 공격 기법들이 발견되었다. 먼저 OS와 응용 소프트웨어에서 발생하는 보안 취약성을 보면, OS의 경우, embedded OS, 구버전 Windows 사용과 같은 보안 취약성을 가지고 있는 경우가 많으며, DOS 공격 가능성, 원격 제어 가능성 등이 존재한다. 또한, 응용 소프트웨어의 경우 보안 취약성을 고려하지 않고 성능 및 기능 위주로 개발되는 경우가 많아 fail 출력이나 Buffer overflow 등을 통해 공격이 가능한 취약점을 가진다. 그리고 제어 시스템이 일반적으로 OTA(Over the Air) 업데이트가 용이한 특성을 가짐에 따라 펌웨어에 바이러스 또는 웜을 심는 공격이 용이한 취약점을 가진다.

네트워크와 관련된 취약점으로는 다음과 같다. 일반적으로 산업 제어 시스템에서는 telnet, ftp, DNP3, Modbus와 같은 보안 취약성이 높은 프로토콜을 사용하고 있기 때문에 잠재적인 취약점이 존재한다고 볼 수 있다. 또한, 제어 시스템은 사용자의 편리한 운용 및 관리를 위해 웹 인터페이스 또는 서버를 구현하는 경우가 많은데 이로 인해 웹 보안 취약성을 가지게 된다. 이 외에도 proprietary 프로토콜이 비정상 트래픽 감지를 하지 못해 오작동을 일으키는 불완전한 IDS 시스템을 포함하여 방화벽 등 통신 프로토콜을 위한 네트워크보안 기술이 부족한 상황도 다양한 취약성을 가지는 원인이 된다. 하드웨어와 같은 물리 상에서도 제어 시스템은 구조/동작 특성에 크게 의존하거나 물리적 보안 특성으로 인한 여러 가지 취약성을 가지게 된다.

〔표 1〕 스마트공장용 제어시스템 보안 취약성/공격 유형

보안 취약성 유형			
1	Worm, Virus	16	Legacy OSes and application
2	DOS, DDOS	17	Inability to limit access
3	Unauthorized access	18	Inability to revoke access
4	Unknown access	19	Unexamined system log
5	Unpatched system	20	Accidental misconfiguration
6	Little or no use of anti-virus S/W	21	Improperly secured device
7	Limited use of host-based firewall	22	Improperly secured wireless
8	Improper use of ICS workstation	23	Unencrypted link to remote site
9	Unauthorized application	24	Password sent in clear text
10	Unnecessary application	25	Default password
11	Open FTP, Telnet, SNMP, HTML port	26	Password management problem
12	Fragile control device	27	Default OS security configuration
13	Network scan by IT staff	28	Unpatched router / switche
14	Cloning attack	29	Unprotected firmware
15	Unprivileged access to the I/O interface	30	Gateway to attack application/monitoring service

Ⅲ. 스마트공장 보안 기술

스마트공장 인프라 및 서비스는 대부분 기존 산업 제어 시스템/네트워크에 기반을 두면서 인터넷과 연동된다. 이 때문에, 스마트공장의 다양한 구성 요소(센서/디바이스, 네트워크, 플랫폼, 애플리케이션) 보안 취약성과 레거시 산업 네트워크와 연동시의 보안 취약성, 플랫폼 연동시의 보안 취약성, 서비스 애플리케이션 보안 취약성이 중요 이슈가 된다. 각 요소별 보안 취약성 해결을 위한 보안 기술을 살펴보면 다음과 같다.

3.1. 센서/디바이스 보안 기술

스마트공장용 센서와 디바이스는 다양한 기능을 가지며, 아두이노 등 소형 오픈 소스 하드웨어 형태의 디바이스에서 대형 공장 장비까지 매우 다양한 크기와 특성을 가진다. 하지만, 기본적으로 이러한 스마트공장에서 사용되는 디바이스는 기능과 통신/네트워크, 하드웨어와 소프트웨어 관점에서의 특성은 유사하기 때문에 기존의 인터넷상의 디바이스가 갖는 보안 취약성과 동일한 형태의 보안 취약성을 갖는다. 즉, 각 센서와 디바이스에 대한 펌웨어/OS 보안 취약성 대응, 코드 인증/무결성 보장, 디바이스 주요 정보(비밀키 정보 등) 보안, 프로토콜 보안, 설비 접근 제어/보안 관리 기술 등이 필요하다. 기존 인터넷상의 디바이스와 필요로 하는 보안 기술은 유사하지만 이를 적용/운용하는 환경은 매우 다르다. 대부분의 공장용 디바이스는 초기 개발 시 접근제어와 기밀성, 무결성 제공 수단을 고려하지 않고 개발되기 때문에 보안 요구 사항을 만족시키기 위한 추가 개발이 필요하다.

3.2. 스마트공장용 네트워크 보안

스마트공장용 네트워크는 제어 시스템에 특화된 통신/네트워크 프로토콜을 가지는 경우가 많다. 예를 들어, DNP3나 Field Bus, 시리얼 통신 등, 보안 적용이 어렵거나 심지어 표준에서조차 보안이 정의되지 않은 프로토콜을 사용하는 경우가 많다. 이럴 경우에는 BITW(Bump in the wire) 개념으로 보안을 제공할 수 있다. 또한, 공장용 네트워크에서는 IDS/IPS가 없는 경우가 많은데 이는 기존의 IDS/IPS가 TCP/IP 프로토콜에 기반하여 개발되어 있기 때문에, 공장용 네트워크 프로토콜에 적합한 IDS/IPS는 존재하지 않는 경우가 많다. 또한, 기존의 인터넷상에서의 Anomaly 감지 기술도 공장용 네트워크 프로토콜의 특성과 기능/동작 특성을 고려하여 개발되지 않았기 때문에 실제 적용하기 위해선 공장 상황에 맞게 재개발할 필요가 있다.

3.3. 플랫폼 보안

스마트공장은 다양한 센서와 디바이스(Factory Thing)가 연동되고 각종 장비/센서에서 수신되는 정보를 저장/가공/분석/연동하기 위한 소프트웨어 플랫폼을 필요로 한다. 이러한 플랫폼에는 각종 디바이스/네트워크에서 제공하는 보안 기술과 연동할 수 있는 보안 에이전트와 플랫폼 자체에서 인증/인가/접근 제어 기능을 갖는 보안 기술, 기업 프라이버시 보호 기술, 서비스 연동시의 보안연관/인증/인가/접근제어, 데이터 연동시의 보안 기술(예: OPC-UA 보안 등)이 필요하다.

3.4. 애플리케이션 보안

스마트공장 서비스/애플리케이션은 제조 설비와 각종 산업용 통신/네트워크, 제조 서비스용 프레임워크, 각종 제조 애플리케이션이 융복합 통합 센싱/운영/제어되는 서비스 환경이다. 이 때문에 다양한 보안 기술이 필요하다. 센싱 정보/공정 정보에 대한 기밀성, 무결성 제공뿐만 아니라, 접근제어, 보안 관리/보안정책, 취약성 대응/침해 대응, 보안 관제/물리보안, 위험 관리, 신뢰성 보장, ID 식별/관리, SCADA 보안, 영상 보안, 기업 프라이버시 보호, 비정상행위(Anomaly) 탐지, 바이러스 탐지, 서비스 API 보안 등 다양한 보안 기술 필요하다. 특히, 스마트공장 애플리케이션에서는 정보 분석이 매우 중요한데, 정보 저장/가공/분석/활용시의 기업 프라이버시 보호 기술, 산업 기밀 유출, 공정 기밀(공정 노하우) 유출 방지, 분석 정보에 대한 소유권 이슈가 존재한다.

Ⅳ. 결 론

본 논문에서는 4차 산업혁명의 가장 중심에 위치한 스마트공장 구성 요소에 대한 주요 보안 취약성과 보안 요구 사항, 그리고 필요한 보안 기술에 대해 살펴보았다. 그리고 스마트공장에서 사용되는 센서/디바이스, 통신/네트워크, 플랫폼, 애플리케이션에 대한 보안 기술을 살펴봤다. 스마트공장은 최근에는 TCP/IP 프로토콜을 사용하는 장비가 개발되어 적용되고 있지만, 대부분은 초기 개발 시 보안이 정의되지 않거나 보안 기술을 적용하기 어려운 레거시 공장 네트워크를 사용하는 경우가 많다. 또한, 스마트공장 환경에서는 기밀성, 무결성 제공보다 주로 가용성과 신뢰성, 접근 제어에 더 비중을 두는 경우가 많다. 이에, 보안을 적용해야 하는 스마트공장의 보안 요구 상황과 장비 및 사용하는 네트워크

종류 등, 현황을 고려하여 공장 현지에서 필요로 하는 가용성과 신뢰성 손실이 발생하지 않는 범위에서 보안 기술을 개발해야 한다.

참 고 문 헌

[1] 2017년 스마트공장 기술개발 로드맵, 산업통산자원부, 2017.1

[2] 스마트공장 핵심기술 개발 사업 연구기획보고서, 산업통산자원부, 2017.4

[3] Andrew Wright, Cyber Security for the Power Grid: Cyber Security Issues & Securing Control Systems, ACM CCS, Nov. 2009

[4] Joseph Weiss, Protecting Industrial Control System, 2010

〈저 자 소 개〉

허 신 욱 (Shinwook Heo)
학생회원

2015년 2월 : 부산대학교 정보컴 퓨터공학부 학사 졸업
2015년 3월 ~ 현재 : 부산대학교 컴퓨터공학과 석, 박사 통합 과정
관심분야 : IoT 보안, 인공지능/딥러닝

이 가 람(Garam Lee)
학생회원

2016년 2월 : 부산대학교 정보컴퓨터공학부 학사 졸업
2016년 3월 ~ 현재 : 부산대학교 전기전자컴퓨터공학과 석사 과정
관심분야 : SW 암호 최적화 구현, IoT 보안, 역공학, 임베디드 보안, 머신러닝

김 동 주 (Dongju Kim)
학생회원

2016년 2월 : 동서대학교 컴퓨터공학부 학사 졸업
2016년 3월 ~ 현재 : 부산대학교 컴퓨터공학과 석사 과정
관심분야 : 인공지능/딥러닝 응용 보안

김 호 원 (Howon Kim)
종신회원

1993년 2월 : 경북대학교 전자공학과 학사 졸업
1995년 2월 : 포항공과대학교 전자전기공학과 석사 졸업
1999년 2월 : 포항공과대학교 전자전기공학과 박사 졸업
1998년 12월~2008년2월 : 한국전자통신연구원 정보보호연구단 선임연구원/팀장
2003년 7월~2004년 6월 : 독일 보훔대학교 PostDoc.
2008년 3월~현재 : 부산대학교 정보컴퓨터공학부 교수
2013년 8월~현재 : 부산대학교 사물인터넷연구센터장
2016년 3월~현재 : 부산대 산업대학원 부원장
관심분야 : 인공지능/딥러닝, IoT 보안, 스마트공장 플랫폼, 클라우드 플랫폼, 암호 칩 설계