Chapter 02

스마트팩토리 환경의 사이버공격 및 대응체계 현황

장종수_한국전자통신연구원 책임연구원
김영수_한국전자통신연구원 책임연구원
박종근_한국전자통신연구원 책임연구원

I. 서론

강한 전염성과 높은 치사율을 동반한 코로나 팬데믹으로 인한 집합 금지 조치와 수주량 감소 그리고 부품 공급 차질로 인한 완성품 생산 감소에 직면하고 있는 상황에서 가장 큰 타격을 입은 곳 중에 하나는 제조 분야였다. 제어할 수 없는 팬데믹으로 인해 생산성에 차질을 받았고 이로 인해 높은 품질을 유지하며 생산성을 향상하고 에너지를 절감하며 인간 중심의 안전한 작업환경을 제공하기 위한 제조 설비의 디지털화, 자동화, 지능화에 대한 요구가 증가하였다. 독일 IFO 경제연구소가 실시한 “코로나 팬데믹이 제조업에 미친 영향” 설문조사에서 응답 기업의 55% 이상이 제조업의 디지털화를 촉진했다고 대답한 것을 보면 이를 더 잘 알 수 있다[1].

제조업 강국인 독일은 글로벌 금융위기 이후 제조업을 부흥시키기 위해 2011년부터 높은 품질을 유지하며 높은 수익성을 확보하기 위해 제조업 혁신을 이끄는 인더스트리 4.0 정책을 추진해 왔으며, 코로나 팬데믹으로 인해 그 발걸음이 더욱 빨라지고 있다. 이는 이전의 제품별 생산라인, 중앙 제어와 폐쇄적인 연결망, 비효율적인 자산관리 등의 특징을 가지는 소품종 대량생산(Mass Production)에서 모듈 공정, 유연 설비, 분산 제어, 개방형 연결망, 실시간 자산관리 등의 특징을 가지는 다품종 맞춤 생산(Mass Customization)으로 변천을 일으

* 본 내용은 장종수 책임연구원(☎ 042-860-4839, jsjang@etri.re.kr)에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.
***Acknowledgment: This work was supported by Institute of Information Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT)(No.2020-0-00952, Development of 5G Edge Security Technology for Ensuring 5G+ Service Stability and Availability)

킴을 의미하며, 이는 곧 비용을 절감하고 생산 공정을 유연하게 하는 지능형 생산을 가능하게 할 것으로 기대된다.

국내에서도 스마트팩토리 중에서 제조 분야 중소기업의 경쟁력을 강화하기 위해서 2018년 “중소기업 스마트 제조 혁신 전략”을 정부가 발표하였고, 중소기업 제조 강국 실현을 목표로 생산공정의 스마트화를 통한 스마트 제조혁신 기반을 마련하고 있다[2],[3].

이렇게 국가별로 제조 분야의 디지털화, 스마트화를 추진함에 따라 기존의 에어 갭이라고 하는 폐쇄적인 환경이 개방화되고 IT 환경과 융합되고 네트워크로 서로 연결되는 환경으로 변화되어 기존의 IT 환경의 위협 요인을 승계하는 문제를 보이게 된다.

최근 세계 최대 반도체 위탁생산 기업인 TSMC의 공장이 워너크라이 랜섬웨어 공격으로 가동이 중단된 사건이나, 세계 최대 알루미늄 생산업체인 노르스크 하이드로사가 로커고가(LockerGoga) 랜섬웨어 공격으로 가동 중단 및 수동 전환을 하였던 사례를 보면 많은 스마트팩토리가 사이버 공격에 효과적으로 대응하지 못하는 것으로 예측된다.

이에 따라, 본 고에서는 국내외 스마트팩토리 현황을 살펴보고, 스마트팩토리 보안 사고를 통한 보안 이슈를 검토하고 이에 대한 대응체계에 대한 부분을 알아보고자 한다.

II. 대표적 스마트팩토리 구축 현황

1. 해외 스마트팩토리

영국의 “매뉴팩처링 글로벌(Manufacturing Global)” 2020년 5월호에서 “글로벌 10대 디지털팩토리(TOP 10 Digital Factories)”[4]에서 언급한 가장 우수한 스마트팩토리와 대표성을 가지는 글로벌 제조기업 중에서 몇몇 스마트팩토리 구축 현황을 [표 1]로 정리하였다.

[표 1] 국외 스마트팩토리 추진 현황

업체	특징	스마트팩토리 추진 현황
보잉 [5]	2020년 TOP 디지털 공장 선정	유타, 셰필드, 캘리포니아, 사우스캐롤라이나, 워싱턴, 미주리 등의 공장에서 3D 프린팅 기술을 이용하여 부품 수를 최소화하고, 디지털 트윈 기술을 적용하여 공장 생산의 실시간 모니터링 및 공장 자재 흐름의 최적화 방안을 시뮬레이션함으로써 생산성을 최대 50% 향상시킴

업체	특징	스마트팩토리 추진 현황
지멘스 [6],[7]	1997년 “올해의 공장”, 2007년 “유럽 최고의 공장” 선정, 2020년 “글로벌 10대 디지털팩토리” 선정	2020년도 공정의 디지털화와 자동화 수준을 85% 이상 달성하였고, 모든 설비에 1,000여개의 IoT 센서를 연결하고, 디지털 트윈 기술을 적용하여 제품 불량률 0.0012%를 달성하였고, 제품 설계주문의 변경에도 유연하게 대처할 수 있게 됨
GM [8]	2020년 “글로벌 10대 디지털팩토리”	단일 조립 공장에 수천 개의 로봇이 협업하고, 5G 모바일 네트워크, 인공지능, 3D 프린팅, IoT, 클라우드 컴퓨팅, 빅데이터 분석 등의 기술을 적용한 “Factory ZERO(충돌 제로, 배기가스 제로, 정체 제로)”를 통해 효율성과 생산성 향상, 안전문제의 최소화를 실현하여 최고의 품질과 최적화된 비용의 전기차를 생산하고 있음
에릭슨 [4],[9]	2020년 “글로벌 10대 디지털팩토리”	에스토니아 공장에 5G 이동통신, AGV(automated guided vehicles), 증강현실(Augmented Reality) 기술, 환경 센서 등을 적용하여 부품 배송시간 단축과 손상 위험 감소, 부품 품질관리 프로세스의 문제 해결 등의 작업 조건을 개선함
슈나이더 일렉트릭 [10]	에너지관리 및 산업 자동화 전문기업	IoT, 빅데이터 및 예측 분석, 증강현실, 원격 모니터링, 예측 유지관리 기술을 운영 방식에 적용하여 운영 간소화 및 효율성 증대, 에너지 소비 절감 그리고 장비 가동 중지 시간 20% 이상 감소를 이룸
포드 [11]	자동차 회사	스페인 발렌시아 자동차 엔진 공장에 5G 이동통신, IoT 센서, AGV 차량관리, 제스처 인식, 가상현실(Virtual Reality), 에지 컴퓨팅, 로보틱스, 인공지능 기술을 적용하여 보다 효율적이고 환경 친화적이고 저렴한 비용의 운영이 가능한 생산 환경을 구축함
폭스콘 [12]	애플 아이폰 생산 기업	청두 공장과 선전 공장의 완전 자동화/최적화된 제조 프로세스, 스마트 유지관리시스템, 지능형 실시간 모니터링 등을 위해 혼합현실(Mixed Reality), 인공지능, 머신러닝, 사물인터넷, 로봇공학 등을 적용하여 인력 의존도 감소, 생산 효율성 30% 이상 증가, 재고 주기 15% 감소를 이룸
히로텍 (Hirotec) [13]	글로벌 자동차 부품 제조업체	IoT, 클라우드컴퓨팅, 기계학습을 제품 생산 공장에 적용하여 데이터 수집, 저장 및 분석을 통해 시스템 장애를 예측하고 예방하는 작업을 수행하여 시스템 수동검사기간을 획기적으로 단축함

2. 국내 스마트팩토리

국제적으로 인정받는 국내 대기업과 중소벤처기업부의 스마트공장 지원사업 우수기업 두 곳을 통해 국내 스마트팩토리 추진 현황을 정리하면 [표 2]와 같다.

이외에도 많은 국내외 기업들이 역동적인 생산 환경 조성, 안정성/효율성 및 안전성 향상, 운영 및 가동 중지 시간/비용 절감을 통해 경쟁력 확보와 기업 이익 극대화를 위하여 제조 환경을 스마트팩토리로, 인더스트리 4.0 환경으로 지속적으로 변혁시키고 있다.

[표 2] 국내 주요 스마트팩토리 추진 현황

업체	특징	스마트팩토리 추진 현황
삼성 [14],[15]	2020년 TOP 디지털 공장 선정	수원 공장(with KT)과 미국 텍사스 오스틴 공장(with AT&T)에 5G 이동통신, 인공지능, 딥러닝, 혼합 현실, 로보틱스, 사물인터넷(IoT), 클라우드컴퓨팅 등의 기술을 적용하여 제조공정의 70% 이상을 자동화하여 생산라인의 최적화, 효율성 극대화, 환경 안전도 향상을 추진함
포스코 [16][17]	2019년 "등대공장(Lighthouse Factory: 세계 제조업 미래 선도 공장)" 선정 (World Economic Forum)	열연공장에 인공지능 기술을 적용하여 슬래브 절사 시 발행하는 손실을 연간 1만 7,000톤 절감하였으며, 또한 스마트 고로 시스템에 딥러닝 기술을 적용하여 용선 생산량을 연간 약 8만 5,000톤 증산함
LS 일렉트릭 (LS산전) [18]	2021년 WEF '등대공장' 선정	2015년부터 청주 공장을 스마트공장으로 전환을 추진하여, 모든 공정을 로봇이 수행하고, 사물인터넷, 인공지능, 빅데이터 기술 등을 접목함으로써 생산량이 160% 증가하였고, 에너지 사용량은 60% 절감하였으며, 불량률도 100만 개당 7개 수준으로 감소시킴
㈜화요 [19]	주류제조업체	여주공장의 증류 소주 생산 공정에 사물인터넷, 클라우드, 인공지능 등 IT 기술을 적용하여 원료부터 완제품까지 전 공정을 추적하고 관리하는 이력관리 MES(Manufacturing Execution Systems)를 구축함으로써 공정 불량률을 11% 감소하였고, 생산원가를 낮추어 6%의 생산성 향상을 이룸
대양롤랜드(주) [19]	컨베이어시스템 전문기업	로봇시스템과 연계된 생산 정보 수집 체계를 구축하여 제조이력관리, 작업일지 첨단화, 공정 모니터링, 실적 모니터링을 고도화함으로써 고품질의 제품을 균일하게 생산하였고, 시간 당 생산량은 200% 증가, 공정 불량률은 50% 감소, 작업 공수도 55% 감소시킴

III. 스마트팩토리 대상 사이버 공격 사례

이와 같이 국내외에서 생산 공정의 자동화를 넘어서 지능화하는 스마트팩토리 도입이 증가함에 따라 안전한 환경 제공에 대한 관심이 증가하고 있다. 특히, 에어갭 기반의 기존 공장에서 개방형 구조로 전환되고 있고, 아날로그 중심의 제어 체계가 디지털화 및 IP화하여 서로 긴밀하게 상호작용하도록 변화하고 있어서 보안 문제는 심각하게 고려되고 있다. 최근의 솔라윈즈 사태와 TSMC 해킹, 노르스크 하이드로 랜섬웨어 공격 등은 이러한 부분에 대한 시각을 다시 한 번 점검하게 한다.

최초의 산업제어시스템 공격 사례와 최근의 제조 산업 시설에 대한 공격을 검토하면서 스마트팩토리의 사이버위협에 대한 부분을 점검하는 것이 이를 효과적으로 대응하고 예방하기 위한 방안 마련에 도움이 될 것으로 보인다.

1. 이란 원자력 발전소 제어시스템: 스턱스넷(Stuxnet) 공격

폐쇄망으로 운영되는 원자력 발전소의 제어시스템을 대상으로 한 최초의 사이버공격으로 유명하다. 2010년 이란의 부세르 원자력발전소의 감시 제어 및 데이터 수집(Supervisory Control And Data Acquisition: SCADA, SMATC PCS7) 시스템이 윈도 운영체제의 취약점을 이용한 컨피커 웜(Conficker Worm)에 감염되어 수차례 운영 정지되고 최대 1,000개의 원심분리기가 파괴되는 손상을 입었다. 이 컨피커 웜은 감염된 직원의 USB를 통해 폐쇄된 원자력 발전소 제어시스템에 진입하였고, 지멘스 SMATC PCS7 시스템과 통합 관리 도구인 SIMATIC WinCC7와 SIMATIC Step7을 공격하여 농축 시설의 운영 중단과 시설 파괴를 유발하였다[20].

2. 우크라이나 전력시스템: 블랙에너지(BlackEnergy) 멀웨어 공격

산업제어시스템(ICS)에 대한 공격의 또 다른 예로, 2015년 12월 러시아 사이버스파이그룹인 샌드웜(Sandworm)이 우크라이나 전력시스템을 공격하여 6시간 동안 정전을 발생하게 했는데, 이는 이메일 첨부 파일 내에 포함된 악성코드가 실행되도록 유도하는 스피어피싱 공격기법을 사용하여 트로이목마를 설치하고, 이를 통해 우크라이나 전력 네트워크에 진입하여 전력제어시스템을 감염시켜 주요 구성요소를 제거(KillDisk)하여 산업제어시스템을 손상시켰다[21].

3. 반도체 위탁생산 기업의 생산 설비: 랜섬웨어 공격

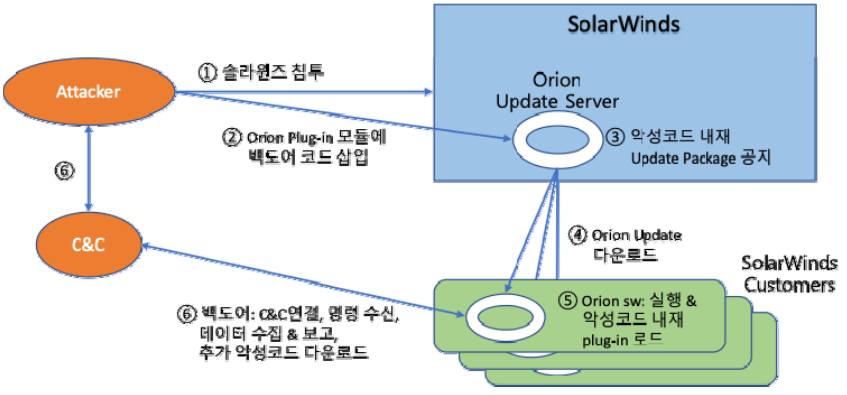
대만의 세계 최대 반도체 위탁생산 기업인 TSMC의 생산 라인이 2018년 워너크라이(WannaCry) 랜섬웨어 공격으로 2일 동안 가동 중단되는 사태가 발생했다. 이는 직원이 워너크라이 변종 악성코드에 감염된 USB를 사용하여 생산 설비의 소프트웨어 업그레이드를 수행함으로 악성코드가 생산 설비에 유입된 것이다. 이로 인해 생산 현장의 PC들이 감염되었고 해당 시스템의 데이터가 암호화되고 무결성이 손상을 입게 되었고, 그 결과로 일부 생산 공장의 기기 1만 대 이상이 손상되어 이틀 간의 가동 중단이 발생하게 되었다. 이로 인한 손실액은 총 약 2억 5,000만 달러(연 매출 3%) 규모인 것으로 알려졌다[22],[23].

4. 세계 최대 알루미늄 제조 시설: 랜섬웨어 공격

2019년 3월에는 세계 곳곳에 지사를 두고 있는 노르웨이 세계 최대 알루미늄 제조업체인 노르스크 하이드로(Norsk Hydro ASA)가 로커고가 랜섬웨어 공격을 받아 노르웨이, 브라질, 카타르 제련소 및 용광로 등의 고도의 자동화 공정 일부가 수동 전환하는 사태가 발생하였고, 금속 압출 공정 장비 등과 같은 광범위한 디지털 모니터링이 필요한 시스템 업무는 중단되었다. 이 악성코드도 직원이 수신한 이메일의 첨부파일에 의해 유입되었고, 이로 인해 5,500만 달러 이상의 업무중단 피해액이 발생했고, 완전 복구에 9개월 이상 소요되었다 [24]-[26].

5. 솔라윈즈: 소프트웨어 공급망 공격

역사상 가장 큰 규모의 공급망 공격인 솔라윈즈 해킹 사건은 2020년 12월 미국의 보안 전문 기업인 파이어아이(FireEye)에 의해 발견되어 모두를 놀라게 했다. 솔라윈즈는 네트워크, 시스템 및 정보 기술 인프라 관리를 지원하는 소프트웨어를 공급하는 미국 기업으로, 저렴하고 강력한 IT 모니터링 및 관리도구 지원으로 유명하여 전세계 많은 기업과 공공기관이 이용하고 있었기에 해당 사건의 여파는 심각했던 것으로 보인다. [그림 1]과 같이 해커들은 솔라윈즈의 모니터링 솔루션 '오리온' 업데이트 파일에 선버스트(SUNBURST) 트로이목마를 심었고, 고객이 해당 애플리케이션을 업데이트할 때 악성코드에 감염되도록 하여 전체



〈자료〉 Radware, "FireEye Hack Turns into a Global Supply Chain Attack," 2020. 12. 17.

[그림 1] 솔라윈즈 공격 개념도

고객사의 3%에 해당하는 18,000여 고객이 감염되는 피해를 입게 되었다. 이는 고객이 신뢰하는 자동 업데이트 플랫폼을 이용하여 악성코드를 합법적으로 배포하는 침입 경로를 보여주었다[27].

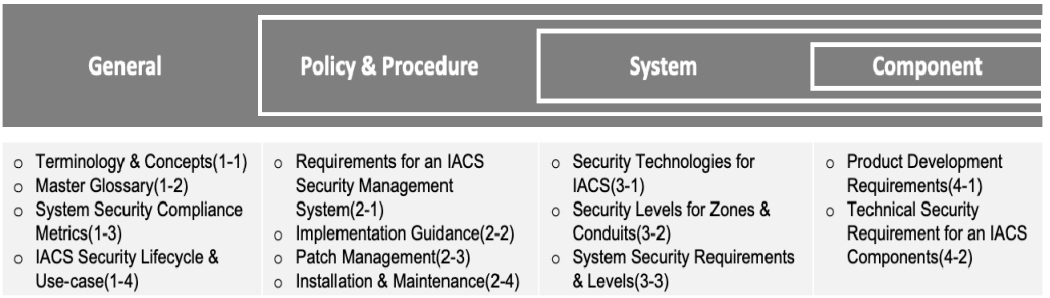
현재 산업제어망에서 가장 많이 일어나는 사이버공격의 경로는 사회공학적인 방법을 이용하여 감염시킨 직원 USB를 이용하거나, 패치 시스템과 같은 신뢰 서비스 채널을 이용한 합법적인 채널을 이용하고 있어 기존의 단품 솔루션에 의한 보안대응으로는 어려움이 있다.

Ⅳ. 스마트팩토리 보안 대응체계

스마트팩토리에 대한 위협의 경로가 다양화되고 증가함에 따라 이에 대한 체계적 관리와 대응체계의 구축은 중요한 숙제 중의 하나이다. 이에 따라 스마트팩토리의 핵심인 산업제어시스템(Industrial Control Systems: ICS) 네트워크 구축과 기업 네트워크와의 연결 시에 고려해야 하는 사이버 보안 고려사항 및 운영기술(Operational Technology: OT) 환경의 보안관리체계로는 ISA/IEC 62443(안전한 산업 자동화 및 제어시스템 구현 절차)와 NIST 800-82(산업제어시스템 보안 가이드라인)을 가장 많이 참고하고 있다. 이와 관련한 국내 가이드라인은 한국인터넷진흥원에서 발표한 “스마트공장 사이버보안 가이드”, “스마트공장 보안 모델” 등을 들 수 있다. 또한, 스마트팩토리 운영의 효율화를 위한 OT-IT 융합과 ICS 네트워크와 기업 네트워크의 연결성 보장으로 인한 복잡성 증가와 사이버 위협의 확산은 총체적인 보안 관리 및 대응체계 수립을 요구하며, 이로 인해 계층적 사이버보안 방어 개념인 NSA(National Security Agency) 심층 방어(Defense-in-Depth) 전략을 적용하는 사례가 늘고 있어, 이에 대한 현황을 알아본다.

1. 산업제어시스템 구축 가이드라인

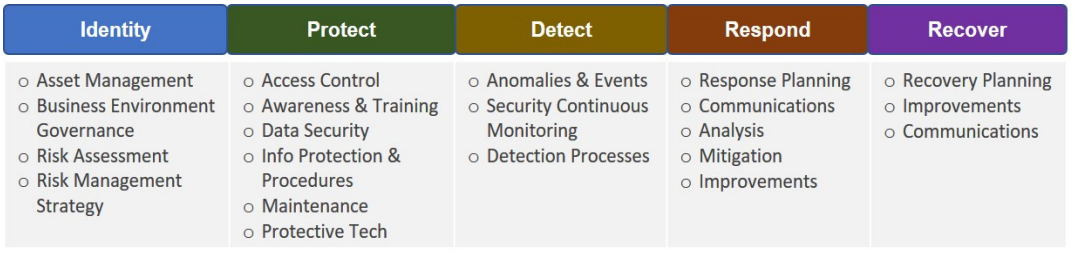
- IEC 62443(산업용 통신 네트워크-네트워크 및 시스템 보안): 산업제어시스템 보안관리 요구사항과 보안기술, 제품의 개발 요구사항 및 산업제어시스템 구성요소에 대한 기술적 보안 요구사항 등이 정의되어 있는 IEC 62443(ISA 99)은 [그림 2]와 같이 산업제어시스템 제품 개발에서부터 운영과 관리에서의 요구사항 표준을 다루고 있다[28].



〈자료〉 International Electrotechnical Commission, "Understanding IEC 62443", 2021. 2. 26.

[그림 2] IEC 62443 표준 구성

- NIST 사이버보안 프레임워크(Framework for Improving Critical Infrastructure Cybersecurity: CSF): 미국 국가안보에 중요한 핵심 인프라 및 기타 분야를 보호하기 위해 미국 오바마 대통령 행정명령-13636호("주요 인프라 사이버보안 개선")에 기반한 NIST CSF도 중요한 문서 중 하나이다. 이 CSF는 비용 효율적이고 유연하며 우선순위에 따라 반복 가능하게 정보보호 및 사이버보안 조치의 구축과 적용을 위한 접근법을 제공하며, 이에 따른 사이버보안 관련 리스크를 관리하기 위한 표준, 지침 및 모범사례를 담고 있다. NIST CSF는 코어, 프로파일, 구현계층으로 구성되며, 그 중에서 프레임워크 코어에 있는 주요 기반시설의 사이버 위협 상황에 대한 인식과 대응 방안을 담고 있어 스마트팩토리의 총체적 보안 대응체계를 수립하는데 중요한 기초가 된다. NIST CSF 코어는 [그림 3]과 같이 식별(Identify) 보호(Protect), 탐지(Detect), 대응(Respond), 복구(Recover)의 연속적인 5가지 기능으로 구성된다[29].
- KISA 스마트공장 사이버보안 가이드: 국내에서도 OT 기술과 IT 기술의 융합을 통해



〈자료〉 NIST, "Framework for Improving Critical Infrastructure Cybersecurity Version 1.1," 2018. 4. 16.

[그림 3] NIST 사이버보안 프레임워크 코어 기능

제조환경의 자동화, 디지털화와 지능화를 본격적으로 추진하고 있고, 4차 산업혁명의 핵심인 인공지능, 빅데이터 분석, 로봇공학, 사물인터넷, 가상현실, 5세대 이동통신기술 등을 반영한 스마트공장 도입을 추진하고 있어서 국가적으로 스마트공장에 대한 보안 요구사항을 제시하고, 스마트공장 보안위협을 식별하여 피해를 최소화하기 위한 “스마트공장 사이버보안 가이드”를 한국인터넷진흥원에서 2019년 12월 발간하였다. 이 가이드북에는 스마트공장에서 발생할 수 있는 보안 위협과 보안 요구사항에 따른 세부 보안 요구사항과 이행방안을 정리하고 있다[30].

- KISA 스마트공장 보안 모델: 과학기술정보통신부와 한국인터넷진흥원이 2020년 12월에 발간한 “스마트공장 보안 모델”은 스마트공장 보안 위협과 대응을 위한 보안요구사항을 정리하고 있는 “스마트공장 사이버보안 가이드”의 후속 문서로 보안요구사항을 실현하기 위한 보안 기술과 보안 솔루션을 제시하고, 활용하기 위한 활용 절차와 사례 기반 활용방안을 제시하고 있다[31].

2. NSA 심층 방어

사이버 보안 심층 방어(Defense-in-Depth: DiD) 모델은 미국 NSA가 제안한 사이버 보안 모델로, 개별 보안 수단의 단일 실패가 전체에 미치는 영향을 최소화하고, 사이버 공격에 대한 방어 효율을 높이고자 계층화된 일련의 사이버 보안 방어 수단을 적용하여 사고의 예방과 완화를 가능하게 하기 위한 접근방법이다.

“NIST SP 800-82: 산업제어시스템 보안”에서는 안전한 산업제어시스템을 구축하기 위한 지침을 제공하는데, ICS 및 일반적인 시스템 토폴로지에 대한 개요와 위협 및 취약성을 식별하고 위험을 완화하기 위한 보안 대책을 권고하고 있다. 특히, 운용 효율화를 위해서 연결성을 제공할 수밖에 없는 산업제어시스템을 위한 효과적인 사이버 보안 구축을 위해 “심층 방어” 전략을 권고하고 있다[32],[33].

OTCSA(Operational Technology Cyber Security Alliance) ICS 보안 모델의 경우도 생각할 수 있는데, IT와 OT의 융합과 산업용 IoT의 확산으로 인해 OT 운영자와 벤더 생태계에 정기적인 기술 요약과 구현 지침을 제공하기 위해 만들어진 OTCS(Operational Technology Cyber Security) 연합이 제시하고 있는 IIoT와 클라우드 서비스가 접목된 스마트팩토리의 퍼듀 모델 기반 OT 보안 가이드라인에서 방화벽과 세그멘테이션, 보안 게이

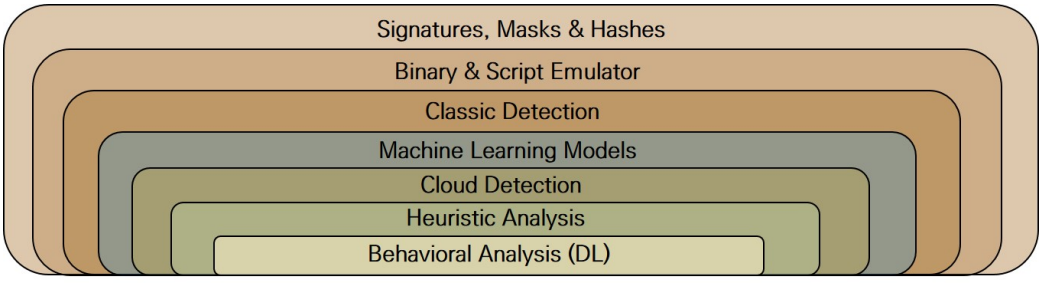
〈자료〉 F5, “F5 Friday: Goodbye Defense in Depth. Hello Defense in Breadth,” 2012. 1. 27.

[그림 4] F5 네트웍스 심층 방어 보안 구조

트웨이를 계층별로 적용한 다중 계층 보안 구성을 정의하고 있다[34].

애플리케이션 서비스 전문기업인 F5 네트웍스는 한 제품이 놓친 것을 다른 제품이 포착할 수 있다는 개념으로 방화벽, IPS 및 안티바이러스 제품을 구축하고 포괄적으로 운영하기 위한 “DEFENSE in BREADTH” 개념([그림 4] 참고)을 적용한 솔루션을 출시하고 산업 현장의 보안성 강화를 위해 적용하고 있다[35].

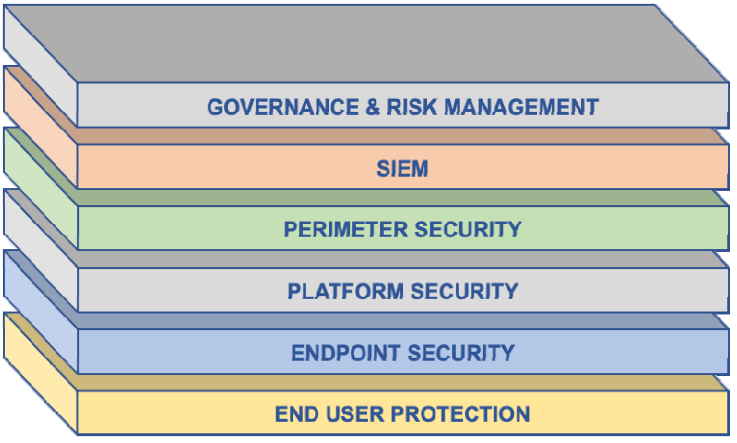
안티바이러스 제품으로 가장 인지도가 높은 보안 회사인 카스퍼스키(Kaspersky)는 보다 새롭고 정교한 악성코드에 효과적으로 대처하기 위해 [그림 5]와 같은 계층화된 방어기법을 AV 제품에 적용하고 있다. 이를 통해 서로 다른 수준의 인프라를 모두 커버하고 다양한 유형의 맬웨어로부터 시스템을 효과적으로 보호하고 방어하고자 한다[36].



〈자료〉 Kaspersky, “The multilayered security model in Kaspersky Lab products,” 2017. 3. 3.

[그림 5] 카스퍼스키의 파일 AV 다중 계층 접근 방식

글로벌 보안 소프트웨어 기업인 트랜드 마이크로(Trend Micro)는 산업제어시스템(ICS)에 대한 ISA/IEC 62443 참조 모델 기반 심층 방어 사이버보안 전략을 구현하는 방법을 제안하고 있다[37]. 트랜드 마이크로의 ICS 심층 방어 전략은 안전한 개발 수명주기/위협



〈자료〉 Abascus Group, "Our Cybersecurity Defense-in-Depth Structure," 2020. 7. 1.

[그림 6] 아바쿠스그룹의 사이버보안 심층 방어 구조

인텔리전스/사고대응/사이버보안 전략을 기반한 총체적인 접근을 기반으로 하고, 방화벽/침입방지시스템/바이러스 백신/무결성 모니터링/데이터 손실 방지 등으로 구성된 SaaS/ 클라우드/가상화/컨테이너 보안이 수행되어지고, IT/OT, 클라우드/가상화, SaaS, SIEM/SOAR (Security Orchestration, Automation and Response) 플랫폼에 대한 통합 보안 가시성/모니터링/관리를 수행할 수 있게 하며, 허용 목록/AV/DLP(Data Loss Prevention)/무결성 검사/가상 패치/취약성 평가 스캐닝을 수행하는 디바이스 및 종단장치 보안 기능이 수행되고, 일시적인 에어 갭 환경에서도 허용 목록, AV, DLP, 무결성 모니터링 등 보안 기능이 수행될 수 있도록 구조화하고 있다.

글로벌 IT 서비스 회사인 아바쿠스(abacus) 그룹은 IT 서비스의 기밀성, 무결성 및 가용성을 보호하고 지속적인 보안 강화와 위험 감소를 위해 [그림 6]과 같이 최종 사용자 보호, 엔드포인트 보안, 플랫폼 보안, 경계 보안, SIEM, 거버넌스/위험 관리 기능으로 계층화된 사이버보안 심층 방어 구조를 적용하고 있다[38].

이러한 심층 방어 전략은 단일 점 실패로 인한 전체 네트워크 및 서비스에 치명적인 결과를 막기 위해 많은 기업에서 사이버보안 솔루션에 적용하고 있다. 효과적인 심층 방어를 위해서는 기존의 사일로기반의 접근 방식이 아니라 포괄적으로 바라보고 유기적으로 연계된 보안 대응을 하는 것이 중요할 것으로 보인다.

V. 결론

현재 국내외 대기업 중심으로 제조 분야 스마트팩토리의 완전자동화와 새로운 기술의 접목을 통한 고도화 및 지능화하려는 시도는 상당 부분 진전을 보이고 있다. 제조 현장의 자율성과 이동성을 극대화하기 위한 5G 이동통신 기술을 제조 현장 통신 인프라에 적용하기 시작했고, 빅데이터 분석을 넘어 머신 러닝과 딥 러닝을 이용한 분석과 예측을 통해 생산 효율화 및 안전한 환경 조성에도 상당한 진척이 있었다.

또한, AR/VR/MR을 이용한 제품 기획, 개발, 테스트 및 교육 환경 고도화와 AGV(Automated Guided Vehicle), 협업 로봇을 통한 생산 효율화, CPS(Cyber Physical System)와 디지털 트윈 기술을 통한 생산 현장 및 전반적인 상황 시각화 등을 수행하고 있고, 이를 통해 최고 수준의 프리미엄 제품 생산을 위한 기반을 다지고 있다.

그러나 아직도 국가스마트제조혁신추진단에서 정의하고 있는 “제품의 기획부터 판매까지 모든 생산과정을 ICT 기술로 통합하여 최소 비용과 시간으로 고객 맞춤형 제품을 생산하는 사람 중심의 첨단 지능형 공장”이라는 전체 생태계를 엮어 가기에는 부족한 부분이 많은 것으로 보인다.

중소기업 일부에서는 인공지능과 VR 기술을 이용하는 업체도 있으나 대부분의 기업은 생산 설비의 자동화를 위한 MES 적용 수준에 머무르고 있는 것이 현실인 것 같다.

대기업 및 중소기업 모두에서 보안에 대한 대응은 아직도 미흡한 것으로 보이며, ISA/IEC 62443과 NIST 800-82, 그리고 KISA의 스마트팩토리 관련 가이드라인에서 정의하고 있는 보안 권고를 적용하는 노력이 필요하다. 적어도 네트워크의 경우는 목적에 따른 네트워크 분리(Segmentation)를 적용하도록 하고, 업무망과 산업제어망 간은 DMZ를 적용하여 안전성을 강화하고, 각 계층 간에는 방화벽을 통한 액세스 제어가 기본적으로 이루어져야 한다. 그리고 기기 인증과 사용자 인증, 권한 관리에서 보다 엄격한 관리가 필요하며, 스마트팩토리 전 생산 공정과 운영상황을 총괄적으로 시각화하고 인공지능 또는 딥러닝이 적용된 분석 엔진과 연계하여 심도 있는 보안 분석, 즉시적인 상황 파악과 즉각적인 대처가 가능하도록 하는 것이 중요하다.

또한, 자동화와 운용 효율화를 추진하고 있는 중소기업의 경우는 방화벽 운용은 반드시 적용해야 하고, 이동식 디바이스(USB, 휴대폰 등)에 대한 관리 및 통제를 위한 노력과 원격

접속에 대한 멀티팩터 인증(Multi-factor Authentication) 및 최소 권한관리를 통한 위협 요인을 최소화하는 것이 우선되어야 한다.

특히, 날로 진화하는 사이버공격에 효과적으로 대응하기 위해서 사이버보안 관점의 심층 방어 모델의 정의 및 총체적인 제어/관리 방안 수립이 필요하며, 중소기업에 특화된 보안모델의 단계적 추진 방안에 대한 제시가 필요하다.

참고문헌

[1] 헬로티, "[코로나19와 제조업Ⅲ] 포스트 코로나 시대를 대비하는 제조업 강국의 현재와 미래", 2021. 3. 2.
[2] 중소벤처기업부, "중기부, 지능형공장보급 2만개 달성", 2021. 1. 4.
[3] 대한민국 정책브리핑, "스마트공장(지능형공장)", 2021. 9. 23.
[4] Manufacturing, "Top 10 digital factories: Boeing," 2020. 6. 1.
[5] Aerospace Manufacturing, "Machining a future," 2020. 1. 22.
[6] 테크월드뉴스, "[스마트팩토리 특집] 제조 기업, 스마트를 입다", 2021. 4. 7.
[7] Manufacturing, "Top 10 digital factories: Siemens," 2020. 6. 1.
[8] Manufacturing, "Top 10 digital factories: General Motors," 2020. 6. 1.
[9] K-smartfactory, "5G & Network-제조분야 5G 선진 사례", 2021. 9. 7.
[10] The American Society of Mechanical Engineers, "9 of the Smartest Factories in the World," 2021. 7. 14.
[11] Enterprise IoT Insights, "Top 10 global manufacturers using 5G," 2021. 10. 27.
[12] CIO Korea, "애플의 아이폰 공장은 '4차 산업혁명'의 우수사례다", 2021. 4. 9.
[13] Internet of business, "Five smart factories – and what you can learn from them,"
[14] Manufacturing, "Top 10 Digital Factories: Samsung," 2020. 6. 1.
[15] 위키리스크한국, "삼성, 글로벌 '스마트팩토리' 기업 톱10 선정… 英 메뉴팩처링 글로벌 '새 혁신 주도'", 2020. 5. 21.
[16] 매일경제, "제조업 패러다임 바꾸는 스마트팩토리", 2020. 7. 10.
[17] 중앙선데이, "포스코, 세계 제조업의 미래 '등대공장'으로 선정", 2019. 7. 26.
[18] 조선일보, "포스코 이어 국내 2번째로 등대공장 선정된 LS 일렉트릭", 2021. 9. 21.
[19] 스마트제조혁신추진단, "스마트공장 지원사업 참여기업 우수사례집(2019~2020 선정)", 2021. 1. 25.
[20] "Stuxnet", https://en.wikipedia.org/wiki/Stuxnet
[21] Kaspersky, "BlackEnergy APT Attacks in Ukraine employ spearphishing with Word Documents," 2016. 1. 28.
[22] 매일경제, "고위험 설비노린 해킹 대비…공장 보안서비스 시장 진출", 2020. 11. 10,
[23] ZDNet, "TSMC says variant of WannaCry virus brought down its plants," 2018. 8. 6.
[24] Micosoft, "Hackers hit Norsk Hydro with ransomware, The company responded with transparency,"

2019. 12. 16.
[25] 전자신문, “공격 횟수 줄어든 랜섬웨어 ‘한 방’ 노린다”, 2019. 9. 19.
[26] LG CNS, “고민되는 팩토리 보안 어떻게 해야 할까?”, 2019. 6. 13.
[27] Radware, “FireEye Hack Turns into a Global Supply Chain Attack,” 2020. 12. 17.
[28] International Electrotechnical Commission, “Understanding IEC 62443,” 2021. 2. 26.
[29] NIST, “Framework for Improving Critical Infrastructure Cybersecurity Version 1.1,” 2018. 4. 16.
[30] KISA, “스마트공장 사이버보안 가이드”, 2019. 12. 1.
[31] KISA, “스마트팩토리 보안 모델”, 2020. 12. 1.
[32] Homeland Security, “Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies,” 2016. 9. 1.
[33] NIST, “NIST SPECIAL PUBLICATION 800-82 REVISION 2- GUIDE TO INDUSTRIAL CONTROL SYSTEMS(ICS) SECURITY,” 2015. 5. 1.
[34] OTCS Alliance, “Introducing the Operational Technology Cyber Security Alliance,” 2019. 10. 22.
[35] F5, “F5 Friday: Goodbye Defense in Depth. Hello Defense in Breadth,” 2012. 1. 27.
[36] Kaspersky, “The Multilayered Security Model in Kaspersky Lab Products,” 2017. 3. 3.
[37] Trend Micro, “A Current View of Gaps in Operational Technology Cybersecurity,” 2020.
[38] Abacus Group, “Our Cybersecurity Defense-in-Depth Structure,” 2020. 7. 1.