스마트팩토리 도입 기업의 보안강화 사례 연구

Case Study on Security Enhancement of Smart Factory

저자 (Authors)
배춘석, 고승철
Chun-sock Bae, Sung-cheol Goh

출처 (Source)
정보보호학회논문지 29(3), 2019.6, 675-684(10 pages)
Journal of the Korea Institute of Information Security & Cryptology 29(3), 2019.6, 675-684(10 pages)

발행처 (Publisher)
한국정보보호학회
Korea Institute Of Information Security And Cryptology

URL
http://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE08746300

APA Style
배춘석, 고승철 (2019). 스마트팩토리 도입 기업의 보안강화 사례 연구. 정보보호학회논문지, 29(3), 675-684

Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.3, Jun. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.3.675

스마트팩토리 도입 기업의 보안강화 사례 연구

배 춘 석,† 고 승 철‡
수원대학교

Case Study on Security Enhancement of Smart Factory

Chun-sock Bae,† Sung-cheol Goh‡
The University Of Suwon

요 약

제4차 산업혁명의 물결 아래 전 세계 선진 국가들은 스마트팩토리를 핵심기반으로 인식하고 관련 정책 수립 및 산업 육성을 통해 국가의 산업경쟁력을 높이고자 노력하고 있다. 국내 관련 부처들도 제조 혁신 3.0 전략을 수립하여 2025년까지 3만개를 목표로 스마트팩토리 확대를 추진하고 있다. 이에 본 연구에서는 그간의 이론적인 취약점 연구들에서는 부족했던 스마트팩토리 보안 관련 기업 실무 사례를 분석하고 동종업계 적용방안을 제시하여 스마트팩토리의 중요정보 보호 및 안정적인 운영이 되도록 기여하고자 한다.

ABSTRACT

Under the wave of the Fourth Industrial Revolution, developed countries around the world recognize Smart Factory as a core base and strive to enhance the nation's industrial competitiveness through related policies and industry development. Domestic ministries have also set up a strategy for manufacturing innovation 3.0 and are pushing for the expansion of smart factories with 30,000 targets by 2025. In this study, we analyze the practical cases of smart factory security related companies and present the application methods for the same industry. we also intend to contribute to the protectetion of important information in Smart Factory and stable operation.

Keywords: Smart Factory, Smart Factory Security, ICS Security

I. 서 론

1.1 연구의 배경 및 목적

바야흐로 제4차 산업혁명의 시대가 도래 하고 있다. 이에 유럽, 북미, 아시아권의 선진 국가들은 글로벌 시장에서의 산업 주도권과 시장경쟁력을 지속적으로 확보 및 확대하기 위해 스마트팩토리를 핵심기반으로 인식하고 관련 정책 수립 및 표준 정비와 산업 육성에 집중하고 있다.

Received(04. 18. 2019), Modified(05. 27. 2019), Accepted(05. 28. 2019)
† 주저자, csbae01@suwon.ac.kr
‡ 교신저자, goh5703@suwon.ac.kr(Corresponding author)

산업현장에 있는 제조기업들의 입장에서도 새로운 생산성 돌파구의 마련, 고령화로 인한 고숙련 제조인력의 감소, 시장 변화 속도의 증가 대응, 센서, 로봇 등 요소 기술들의 충분한 가격 인하, 정부의 제조업 육성 노력 등에 힘입어 스마트팩토리 도입 및 확산에 긍정적으로 나서고 있다.

국내에서는 2013년도 산업통상자원부의 '산업혁신 3.0 추진 전략' 수립, 2014년도 스마트공장 참조모델 개발 및 배포, 스마트공장 솔루션 기업대상 확산사업 등을 필두로 2015년도 (재)민관합동 스마트공장추진단 발족, 스마트공장 기술개발 로드맵 수립, 스마트공장 진단평가모델 개발, 2017년도에는 2025년까지 스마트공장 3만개를 구축 하겠다는 '스마트제조혁신 비전 2025' 발표, 2018년도 말에 중소벤처

기업부 이하 9개 관계부처 합동으로 2022년까지 스마트공장 3만개를 구축하겠다는 '중소기업 스마트 제조혁신 전략' 발표 등 국가적인 차원에서 총력을 기울이고 있는 상황이다.

이에 본 논문에서는 안전한 스마트팩토리의 도입 및 운영을 위해 실제 스마트팩토리 보안 적용 사례를 제시하고, 국내·외 표준과의 부합성을 비교 분석한다. 이를 통해 그간의 이론적인 취약성 중심의 연구에서 한 단계 더 나아가 스마트팩토리 현장에서의 보안 강화 효과가 기대된다.

1.2 연구의 범위 및 방법, 선행 연구조사

본 연구의 범위는 스마트팩토리를 도입한 특정 기업의 보안강화 방안을 대상으로 한다. 접근방법으로 스마트팩토리 보안 강화 사례분석, 스마트팩토리 보안관련 국내·외 주요 기준과의 커버리지 비교, 그리고 국내 스마트팩토리 도입 기업에 가장 빠르고 효과적인 보안 적용범위 제시 등 단계별 접근을 수행하고자 한다.

스마트 팩토리 보안과 관련된 선행연구는 아직 많지 않은 편이다.

박은주(2017)는 STRIDE 위협 모델링에 기반한 스마트팩토리 보안 요구사항 도출 연구에서 스마트팩토리의 전반적인 생산 공정 절차를 대상으로 데이터 흐름도, MS가 개발한 STRIDE 위협 모델링 기법을 이용하여 체계적으로 위협 식별, 위험 분석, 체크리스트 도출을 논하였다[1].

이송하 등(2018)은 한국형 스마트 팩토리 확산을 위한 사이버보안 위험관리 방안 연구에서 스마트 팩토리 도입 기업의 절대 다수를 차지하는 중소·중견기업이 사이버 위협을 인지조차 못하거나 예산과 인력 부족으로 대책마련 및 실행에 어려운 점을 들어 사이버보험을 하나의 대안으로 제시하고 정부의 지원이 필요함을 논하였다[2].

김일용 외(2018)는 산업제어시스템 환경에서 효과적인 네트워크 보안 관리 모델 연구에서 국내외 산업제어시스템 보안 모델 분석을 통해 제어시스템 참조 모델을 제안하고 산업제어망 보안관리 모델을 논하였다[3].

이용주 외(2018)는 스마트 팩토리 엔터티를 위한 블록체인 기반의 효율적인 역할기반 접근제어 연구에서 스마트 팩토리 엔터티에 최적화되어 효율성과 보안성을 유지할 수 있는 접근제어 방법을 블록체인 기반으로 구현하는 방법을 논하였다[4].

허진(2018)은 AHP 기법을 적용한 스마트공장 보안요인 우선순위에 관한 연구에서 네트워크 보안, 플랫폼·서비스 보안, 디바이스 보안 요인 간 우선순위를 논하였다[5].

한석호(2019)는 스마트 팩토리 보안관리 항목 연구 에서 기존 정보보호관리체계와 스마트 팩토리 보안 관련 연구들을 분석하여 스마트 팩토리 환경에 필요한 보안관리 항목들의 도출을 논하였다[6].

선행 연구들은 주로 이론적인 접근으로 스마트팩토리 도입에 따른 위협요인과 보안관리 항목들을 체계적으로 나열하는 데 집중했다면, 스마트팩토리 보안을 도입한 사례가 아직은 많지 않은 현실에 비추어 볼 때 이론적인 접근을 실체화 할 수 있는 계기를 제시 한다는 측면에서 실제 사례에 대한 연구는 매우 중요하고도 시급하다.

II. 국내 'A'사의 스마트팩토리 보안 강화 사례 분석

2.1 'A'사의 스마트팩토리 도입 이전 보안 체계

'A'사는 제조 분야 전자부품을 주로 생산하는 대기업으로서 수만명의 종업원과 국내 및 해외에 다수의 공장 및 설비를 보유하고 있다.

스마트팩토리 도입 이전에는 공장 내 장비들이 연결되어 운영되는 통신망을 폐쇄망으로 구성하였다. 폐쇄망이기 때문에 네트워크를 통한 망 외부에서의 악성코드 유입, 외부로의 데이터 전송 등이 불가하므로 해킹사고, 데이터 유출에 대한 위험이 낮다고 판단하였으며, 장비 PC에 대한 백신설치, 보안패치, 주기적인 점검 등도 적용하지 않고 있었다.

공장 입구에서 출입자들에 대한 저장매체 휴대여부 검사, 카메라 봉인 등 보안통제를 수행하고 있었기 때문에 장비PC, 작업용 PC에 대한 USB 등 사용 통제도 적용하지 않았다.

반면 업무망에서는 서버, 스토리지 등 전산실 네트워크 영역과 일반 직원용 PC에 대해 물리적, 기술적, 관리적 보안 통제가 충분하게 적용되어 잘 운영되고 있었다. 인터넷은 사용자의 로컬PC에서만 접속이 가능 하며 업무망 내의 가상데스크톱인프라를 통해서만 업무시스템에 접속이 가능하도록 망분리를 적용하였다.

Table 1. Security System Before Introduction Of Smart Factory In Company 'A'

Sector	Control Objects	Description
Operation Network	Network Type	Closed network operation
	Equipment PC management etc.	Do not install vaccine
		Do not patch the operating system (OS) etc.
		Do not limit USB media
	Access control	Storage media import / export control
		Check camera seal and damage
Biz. & OA Network	OA area	Perform administrative and technical controls such as Internet access blocking, PC media control, PC security, periodic security check.
	computer room	Perform technical controls as like a restricted area setting and management, Network configuration other than OA area separately, Server security, etc.
Internet	Malicious code blocking	Allow users to local PC only, Application and operation of security solution such as blocking malicious code infiltration

2.2 'A'사의 스마트팩토리 도입으로 인한 보안 취약성 증가 요인 분석

'A'사는 스마트팩토리 도입을 통해 생산성과 품질을 한 층 더 향상하고자 하였다.

업무망에 위치한 전사적 자원관리 관련 시스템(ERP, SCM, CRM 등)과 제조실행관리 관련 시스템(MES, PLM)이 연동되고, 제조실행관리시스템은 공장의 생산라인에 위치한 주요 장비PC와 제어용 설비(SCADA, DCS, HMI, PLC 등)와 연결된다. 이를 통해서 고객의 제품 수요관리에서 생산계획, 제조 및 검사 관리, 장비관리 등 연속적인 데이터 흐름이 가능하고 작업자의 개입이 최소화된 자동화 생산이 이루어진다. 또한 각종 제조 장비에서 수집된 생산 공정 정보, 장비 상태 정보, 결함 관련 정보 등 대량의 건수와 크기를 가진 실시간성을 포함한 데이터가 수집되고 빅데이터 분석과 기계학습 등 인공지능 기술을 활용한 생산 공정 개선, 제품 결함 판정 자동화, 최적의 수율확보를 위한 온도 및 습도 자동 조절 등 제조 환경 최적화가 가능해진다.

이와 같이 스마트팩토리 구현과정에서 기존의 폐쇄망으로 운영되던 공장의 제조 설비는 업무망과 연결이 된다. 따라서 외부로부터의 악성코드 유입, 불법적인 데이터 유출 시도 등 보안 위협에 노출되고 취약성으로 인한 정보유출, 장비 가동 중단 등 사고 위험은 현격하게 높아질 것으로 예상되었다.

Table 2. Expected Threat Source, Related Assets And Vulnerability In Implementing Smart Factory of Company 'A'

Threat Source	
First, it connects with business network. Secondarily, it infects malicious code through internet linked to business network. It infects information through unauthorized medium such as virus, Ransomware infection, etc., and transmits data related to production by workers. Attempts and delays in production due to abnormal traffic growth, etc.	
Related Assets and Vulnerability	
Operation Network	Inadequate monitoring and blocking of malicious code, virus, etc.
Production Equipment PC	Missing vaccine and security patches
SCADA, DCS, HMI, PLC,	Insufficient control of access by unauthorized person
MES	Insufficient interception againet access by unauthorized persons, attempts to leak production-related information, etc.
Product design, production related information	Insufficient interruption of transmission through network or unauthorized medium such as USB, Insufficient response to data loss by Ransomware etc.

2.3 'A'사의 스마트팩토리 보안 강화 방안 및 시사점

스마트팩토리 구현에 따른 보안 위협을 대응하기 위해 'A'사는 보안 강화 방안을 수립하였다. 최근 급증하고 있는 랜섬웨어 감염으로 인한 데이터 유실 사례와 바이러스 공격 등에 의한 공장 가동 중단 위험성은 스마트팩토리 보안 강화 요구의 가장 큰 동인이 되었다.

보안강화 방안은 외곽 관련 4개, 연구소 관련 5개, 인터넷망 관련 1개, 업무망 관련 1개, 생산망 관련 9개, 정책 및 교육훈련 관련 3개로 총 23개가 도출 및 적용 되었다.

Table 3. 'A' Company Security Controls For Smart Factory

Control Objects	Security Controls	Details
Outer boundary	Worker / visitor access control	Introduced intelligent unmanned badge (visitor card) issuer
	Media import and export control	Intelligent storage media search
	Seal Damage Automatic Detection	Whether the seal of the mobile phone is damaged or not, the intelligent automatic reading system
	Screening search	Introduction of high-risk index (suspicious behavior, special business, scheduled retirement, security breach history, etc.)
laboratory	Network separation	Separate workspace / dedicated virtual desktop PC
	Block mail	Block mail functions
	Install MDM	Mandatory installation of Mobile Device Management (MDM) program
	Output security	Printing QR code to document together, manage shredding date, manage shredding history
	Back up data such as designs	Product design, customer related information Periodic backup
Internet	VPN connection PC control	PC virus pre-check when connecting to external VPN such as home, PC room, dormitory
Business network	Server / DB access control	Unauthorized access control system, blocking bypass path, monitoring
Operation network	Introduced internal DMZ	Introduction of DMZ network between business network and production network, location of MES, buffer zone construction
	Production PC Asset Management	Production equipment PC asset management, OS / vaccine version management performed
	Production PC vaccine distribution management	Introduction of distribution management system for Vaccine not installed, latest version Upgrade required PC
	Unnecessary program control	Non-authorized SW installation source blocking, Malicious code inflow, production PC performance issue management
	Unauthorized device control	Blocks unauthorized devices (USB, wireless Wi-Fi router, phone, etc.), collects usage log and performs monitoring
	Process information	Control access to screen information

Control Objects	Security Controls	Details
	access control	of Main facility / server with Iris authentication, identification with ID card
	Use Secure USB	USB Port unlock only by Authorized user, authorized security USB
	Network traffic pattern management	Automatically detects and responds to abnormal patterns by learning network traffic patterns between the production network and Internet, Intranet
	Back up equipment information etc.	Periodic backup including equipment information, production related information
Policy / Training	Smart Factory Security Framework	Establishment and improvement plan of smart factory security framework
	Smart Factory Security Guide	Establish smart factory security vulnerability and response guide
	Periodic training	Conduct security training regularly (once a month) at new occasions for new operators, production and research staff

'A'사는 기존의 OA망에서의 시스템 운영 및 보안 관리 서비스를 수행하고 있는 IT아웃소싱업체인 'B'사의 전문성을 활용하여 스마트공장의 보안강화를 위한 컨설팅을 사전 수행하였고, 위협요인과 취약성, 위험평가 등을 통해 'A'사 환경에 가장 적합한 보안강화 과제들을 도출할 수 있었다. 스마트팩토리 보안 정책 및 가이드, 보안 프레임워크를 먼저 수립하고 이를 기반으로 필요한 보안강화 과제들을 우선순위 기반으로 단계적으로 수행하였다. 스마트팩토리 보안 취약점에 대한 보안통제를 매우 체계적이고 효과적으로 수행한 모범사례로 볼 수 있다.

III. 주요 스마트팩토리 보안 표준과 'A'사의 강화된 보안체계 비교, 동종 업계 적용방안

3.1 NIST800-82 해외 표준과 비교 및 시사점 도출

3.1.1 NIST800-82 해외 표준과의 비교 결과

미국표준연구소(NIST)에서 발표한 산업제어시스템(ICS)보안가이드 NIST SP800-82는 스마트팩토리 보안에 필요한 전반적인 내용을 포함하고 있다[7]. 연방 정보 시스템과 조직에 대한 보안 및 프라이버시 통제 가이드(NIST800-53)에서 제시하는 보안통제 기준선 17개 범주의 세부 요건 총 175개를 준용하고, 이 중 산업제어시스템의 특성을 감안하여 보완된 보안통제 86개로 구성된다. 'A'사의 스마트팩토리 보안 방안의 적정성 여부를 판단하기 위해 NIST의 86개의 보안 통제와 비교해 본 결과 85개(98.8%) 항목에서 부합한 것으로 나타났다.

Table 4. NIST SP800-82 Security Control Vs. 'A' Company Conformed Number Status

Controls	base line	supplemented for ICS	conformed (Not Covered)
1.Access Control	18	16	16
2. Awareness and Training	4	3	3
3. Audit and Accountability	12	8	8
4. Security Assessment and Authorization	8	6	5(-1)
5. Configuration Management	11	5	5
6. Contingency Planning	10	5	5
7. Identification and Authentication	8	6	6
8. Incident Response	8	2	2
9. Maintenance	6	1	1
10. Media Protection	7	1	1
11. Physical and Environmental Protection	17	4	4
12. Planning	5	2	2

Controls	base line	supplemented for ICS	conformed (Not Covered)
13. Personnel Security	8	1	1
14. Risk Assessment	4	2	2
15. System and Services Acquisition	13	2	2
16. System and Communications Protection	22	12	12
17. System and Information Integrity	14	10	10
Total	**175**	**86**	**85**

3.1.2 NIST800-82 표준과의 비교 결과 시사점

NIST 800-82 표준의 스마트팩토리 보안을 고려한86개 항목에 대해 85개의 높은 부합성을 나타낸 'A' 사의 보안 수준을 볼 때 'A'사의 스마트팩토리 보안 환경은 매우 안전하다고 할 수 있다.

부합하지 않은 항목은 1개이다. 범주 4. 보안 평가 및 인증(security assessment and authorization) 부문 8번 요건(CA-8) 침투테스트이다. 해당 요건의 목적은 테스트 과정에서 산업제어시스템이 부정적인 영향을 받지 않도록 산업제어시스템망을 보장하는 것이다.

NIST 표준은 관련하여 보완된 고려사항을 제시하고 있다. 일반적으로 산업제어망은 시간 제약에 고도로 민감하고 매우 제한된 자원을 가지고 있다. 따라서 침투테스트를 수행하기 위해서는 실 환경에 대해 복제, 가상화, 시뮬레이션 된 시스템을 사용해야 한다. 실 환경은 테스트 수행을 위해서는 미리 중지되어야 한다. 테스트는 해당 중지된 동안에만 일어나도록 계획되어야 한다. 만약 침투테스트가 산업제어시스템 바깥 영역에서 수행된다면, 산업제어시스템망으로 영향이 전파되지 않도록 상당한 주의를 기울여야 한다.

이와 같은 NIST 표준의 침투테스트 요건을 만족하기 위해서는 별도의 테스트용 산업제어시스템망과 유사 생산설비에 대한 투자가 필요하다.

만약 실 생산 환경에서 침투테스트를 수행하게 된다면, 예상치 못한 부정적 영향으로 생산에 차질을 줄 위험이 있다. 통상 제품 납기를 맞추기 위해, 또는 제품 단위당 생산원가를 낮추거나 보다 높은 생산결과를 달성하기 위해 년 중 내내 가동중단 없이 24시간 운영되는 생산시스템의 특성을 볼 때, 침투 테스트를 위해 실 생산 환경의 가동을 중단하는 것은 받아들여지기 힘든 사항이다.

따라서 스마트팩토리망의 안전성 보장을 위한 침투테스트는 현실적으로 별도 테스트 환경에 대한 투자 의사결정의 어려움과 실 환경에서의 중단 및 부정적 영향 발생 위험으로 NIST 표준에서 제시하는 요건을 부합하기에는 상당한 어려움이 있다.

3.2 국내 KISA 표준과 비교 및 시사점 도출

3.2.1 KISA 표준 가이드와의 비교 결과

한국인터넷진흥원(KISA)의 스마트공장 중요정보 유출방지 가이드[8]에서 제시하는 10개 범주의 25개 세부 항목에 대해 'A'사의 보안 강화 방안을 비교한 결과는 23개(92.0%)항목에서 부합한 것으로 나타났다.

Table 5. KISA Security Guide For Smart Factory Data Protection Vs. 'A' Company Case

Security Controls	Conformity
1. Establish a dedicated information security organization and grant responsibility and authority	
1.1 Operating an organization to protect critical information	O
1.2 Establishing and Scoping Critical Information Protection Policies	O
2. Strengthen human security management measures to prevent leakage of important information	
2.1 Personnel management of external cooperative staff and overseas branches	O
2.2 Information security awareness training for important information	O
2.3. Virtual training for infiltration outflow scenarios	X
2.4 Establishing measures to enhance the accountability of personnel who can access sensitive information (confidentiality pledge)	O
3. Identify, classify, manage and control critical information	
3.1 Identification and management of	O

Security Controls	Conformity
important information	
3.2 Assigning the security level of important information	O
3.3 Control of critical information by security level	O
4. Controlling leakage prevention from the stage of generating important information	
4.1 Control over important information producers	O
4.2 Control of critical information generation environment	O
4.3 Access control to important information generating place	O
5. Apply authority-based systematic control when accessing important information	
5.1 Prepare a technical device to check and control access rights of important information accessors	O
5.2 History management and monitoring methods for accessing and utilizing important information	O
6. Prepare countermeasures against malicious code infringement and propagation when using important information and conduct security control	
66.1 Proper network separation of smart factories	O
6.2 Preventing malicious code infiltration using anti-virus software	O
6.3 Secure Information System Patch Plan	O
6.4 Path analysis and countermeasures against malicious code	O
7. Establish and control critical information retention policies	
7.1 Keep sensitive information encrypted	O
7.2 Record and control access personnel when printing important information	O
8. Prepare and control spill prevention measures when providing external information	
8.1 Corporate Business Network and ICS Network Structure	O
9. Establish and control procedures and methods of destroying important information	
9.1 Important Information Destruction Procedures	O
9.2 Important Information Safe Destruction Methods	O
10. Check vulnerability of information system and regular security audit to prevent leakage of important information	
10.1 Periodic Vulnerability Check and Mock Hacking	X
10.2 Perform regular security audits on the information system	O
Conformed Item Count	**23**
Not Conformed Item Count	**2**

3.2.2 KISA 표준 가이드와 비교 결과에 따른 시사점

KISA 표준 가이드와 부합 하지 않는 2개 항목은 침해사고 유출 시나리오에 맞는 가상훈련, 정기적인 취약점 점검 및 모의해킹 수행이다.

표준 가이드에서는 가상훈련과 모의해킹은 훈련 대상자의 정보 유출 인지 유무에 따라 블랙박스 훈련, 화이트박스 훈련으로 나누어 시행하도록 권고한다. 수행을 위해서는 이를 위한 별도의 테스트 환경 구비가 필요하다. 스마트팩토리의 복잡하고 고도화된 구성 특성 상 별도 테스트 환경을 구축하기 위해서는 상당한 비용투자가 수반되어야 한다. 실제 환경을 이용해서 가상훈련, 모의해킹을 수행하려면 생산 중단이라는 중대한 의사결정이 필요하고, 생산 중단 없이 수행하게 된다면 어떠한 부정적 영향이 발생할지 예상할 수 없다.

이러한 비용투자와 생산 중단 어려움이라는 제약사항은 KISA에서 가이드 하는 가상훈련, 모의해킹이 현실적으로 적용되기 어려운 중대한 이유이다.

3.3 보안 대응 조치 적정 범위, 동종 업계 적용방안

3.3.1 스마트팩토리 수준별 보안 대응조치 필요 범위

(재)민관합동 스마트공장추진단에서 정의한 스마트팩토리 수준은 기초단계, 중간1, 중간2, 고도화의 4단계로 구성된다. 각 수준은 식별·측정·제어 자동화 및 통신 능력, 실시간 운영 능력, 실시간 최적 의사결정 능력 등 스마트공장의 성숙도 지표에 의해 결정되며, 국내 전체 기업의 95%이상을 차지하는

중소, 중견기업은 자체적으로 스마트공장을 구축하지 못하는 기초수준이하로 파악되고 있다[9].

각 수준 별·기업규모 별로 보안 대응 조치의 필요 범위에 대해서는 대상이 되는 통신망과 주요자동화 및 정보시스템을 아래 Table 6.과 같이 정리하였다. 중간수준-2 이상에서는 망 구성이 4계층 이상으로 복잡하고 자동화 및 정보시스템의 수도 매우 많아서 상당한 수준의 보안 대응 조치가 필요하다. 반면에 중간수준-1 이하에서는 기초적인 보안 통제 조치만으로도 어느 정도 안전성을 확보할 수 있을 것으로 판단된다.

Table 6. Scope Of Security Countermeasures By Smart Factory Level And Company Size

Level / company Size		
Level Description	Network configuration	Automation system
Advanced / Global-level large enterprise		
The ultimate level of realization of business activities in cyberspace through the creation of cyber physical systems (CPS) based on IoT Internet	Production network - Internal DMZ network - OA network - External DMZ network - Internet network connection	Intermediate level 2 + IoT based CPS, Big data based diagnosis, Operating system, CPPS, Etc.
Intermediate-2 / major company		
Sharing parent company and supply chain related information and engineering information, and real time company operation based on demand and supply planning optimization and control automation	Production network - OA network - External DMZ network - Internet network connection	Medium level 1 + MES, SCM, CRM, PLM, 3D printing, DW, MDM, Etc.
Intermediate-1 / A midsize company		
Automatically obtains facility information as much as possible and automates corporate operations.	Production network - OA network Partially linked	Basic level + ERP, PDM, CAE, CAM, CAS, CAPP, DCS, SCADA, HMI, BOM Etc.
Basic / Small Business		
By utilizing basic ICT, it collects and utilizes information in some fields of production and builds its information system with minimum cost through utilization of infrastructure of parent company.	Production network - OA network separation	CAD, POP, Etc.

3.3.2 동종업계 적용 방안

'A'사의 스마트팩토리 보안 방안을 기초로 기업 규모에 따라 동종업계 적용방안을 정리하였다. 망구성에 따라 적용해야 할 솔루션이 달라지는 점과 기업규모에 따른 보안 투자 여력, 자동화 수준과 정보시스템 수 및 작업자 등 인원수를 감안하여 적용이 필요한 보안 솔루션을 도출하였다.

'A'사와 같은 대기업 이상은, 전체 솔루션 23개뿐만 아니라 고도화 수준에 따라 추가적으로 필요한 보안 방안을 적용하여야 한다.

중견 기업의 경우 연구소, 업무망, 생산망 영역의 솔루션을 중심으로 적용을 검토하고, 솔루션 자동화 수준이 높게 적용된 경우에는 오프라인 수작업 대장 형태로 가능한 수준에서 축소하여 방안을 적용할 필요가 있다.

중소기업의 경우에는 폐쇄망 내의 공장 운영이 중심이 되므로 연구소, 생산망 내의 수작업 대장 형태의 최소화된 보안 관리를 수행하도록 한다. 외곽 부문에서의 인원출입통제, 매체 반·출입 통제, 카메라 등 봉인, 주기적인 보안 교육훈련은 기업규모에 상관없이 공통적으로 수행하여야 할 부분이다.

다만, 중견 및 중소기업의 경우 스마트팩토리 확

산이 본격 궤도에 오르고 관련 보안방안 적용사례가 어느 정도 늘어나는 시점에 본 적용방안에 대한 실증적인 연구가 추가로 진행될 필요가 있다.

Table 7. Mapping Result Between Company 'A' Security Controls and Each Business Size

Sector	Security Controls	Company scale		
		Small	Midsize	Major
Outer boundary	Worker / visitor access control	O	O	O
	Media import and export control	O	O	O
	Seal Damage Automatic Detection	△	△	O
	Automatic Screening search	△	△	O
laboratory	Network separation	N/A	O	O
	Block mail	N/A	O	O
	Install MDM	X	X	O
	Output security	X	O	O
	Back up data such as designs	O	O	O
Internet	VPN connection PC control	N/A	X	O
Business network	Server / DB access control	N/A	O	O
Operation network	Introduced internal DMZ	N/A	X	O
	Production PC Asset Management	△	△	O
	Production PC vaccine distribution management	△	△	O
	Unnecessary program control	△	△	O
	Unauthorized device control	△	△	O
	Process information	X	X	O
	access control			
	Use Secure USB	X	X	O
	Network traffic pattern management	N/A	N/A	O
	Back up equipment information etc.	O	O	O
Policy / Training	Smart Factory Security Framework	X	X	O
	Smart Factory Security Guide	X	X	O
	Periodic training	O	O	O
Mandatory(O)Count		**5**	**9**	**23**
Mandatory(Manual)(△)Count		**6**	**6**	**0**
Optional(X) Count		**6**	**7**	**0**
Not Applicable(N/A) Count		**6**	**1**	**0**

IV. 결 론

본 연구 결과를 통해 스마트팩토리를 도입하고자 하는 기업 및 관련 정부 부처에서 추진하는 정책 관련 보안 수준 강화에 아래와 같이 기여할 수 있다.

- 스마트팩토리 보호 대상 자산의 식별: 기업의 규모에 따른 스마트팩토리 수준과 연동하여 통신망, 주요 자동화 및 정보시스템을 확인
- 취약성의 확인: 스마트팩토리 도입 이전의 'A'사의 사례 참조를 통해 쉽게 보안 취약성에 대한 이해 및 확인
- 보안 통제 방안의 식별: 기업 규모 및 스마트팩토리 수준에 따라 도입을 검토해야하는 보안 통제 방안의 이해, 도입 의사 결정
- 중소기업의 안전한 스마트팩토리 확산 지원: 정부 관련 부처에서 안전한 스마트팩토리 도입 및 운영을 위한 중소기업 지원방안 수립 등에 참조

References

[1] Eun-ju Park and Seung-joo Kim, "Derivation of security requirements

of smart factory based on STRIDE Threat Modeling", Journal of the korea institute of information security & cryptology, 27(6), pp. 1467-1482, Dec. 2017

〔2〕 Song-ha Lee, Hyo-jung Jun and Tae-sung Kim, "A study on cyber security risk management for diffusion of korean smart factories", The journal of korean institute of communications and information sciences, 43(10), pp. 1741-1750, Dec. 2018

〔3〕 Il-yong Kim, Hee-teag Lim, Dae-bum Ji and Jae-pyo Park, "A efficient network security management model in industrial control system Environments", Journal of the korea academia-industrial cooperation society, 19(4), pp. 664-673, Apr. 2018

〔4〕 Yong-joo Lee and Sang-ho Lee, "Efficient RBAC based on block chain for entities in smart factory", Journal of the korea convergence society, 9(7), pp. 69-75, Jul. 2018

〔5〕 Jin Hoh, "A study on priority of smart factory security factors using AHP approach", Ph.D Thesis, Sangmyung university graduate school of business administration, Feb. 2018

〔6〕 Seok-ho Han, "A study on security management items for smart factory", M.E Thesis, The Graduate School of Chung-Ang University, Feb. 2019

〔7〕 Keith Stouffer, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams and Adam Hahn, "Guide to industrial control systems (ICS) security", NIST SP800-82 R2, May 2015

〔8〕 KISA, Smart factory important information leakage prevention guide, Mar. 2017

〔9〕 Korea smart factory foundation, Smart factory reference model - focused on industry, 3rd Edition, Jul. 2017

〈저자소개〉

배 춘 석 (Chun-sock Bae) 정회원
1993년 2월: 전남대학교 경영학과 학사
2017년 2월: 건국대학교 정보보안학과 석사
2018년 3월~현재: 수원대학교 컴퓨터학과 박사과정
1993년 4월~현재: ㈜LG CNS 클라우드아키텍처팀 재직, 정보관리기술사(2008)
〈관심분야〉 정보보호, 데이터센터 구축 및 운영, 클라우드컴퓨팅

고 승 철 (Sung-cheol Goh) 종신회원
1981년 2월: 연세대학교 수학과 학사
1983년 2월: 연세대학교 수학과 석사
1992년 8월: 포항공과대학교 수학과 박사
2011년 9월 ~현재: 수원대학교 정보보호학과 교수
〈관심분야〉 정보보호, 국방사이버보안, 암호학, 클라우드컴퓨팅