Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.5, Oct. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.5.1323

안전한 스마트공장 구축을 위한 위험우선순위(SFRPN) 기반 최소보안요구사항에 관한 연구

이 병 권,[1†] 김 동 원,[2] 노 봉 남[1‡]
[1]전남대학교 대학원, [2]고려대학교 정보보호대학원

Study on Minimum Security Requirement Using Risk Priority Number(SFRPN) for Secure Smart Factory

Byung-gueon Yi,[1†] Dong-won Kim,[2] Bong-nam Noh[1‡]
[1]Chonnam National University, [2]Korea University

요 약

현대의 공장은 스마트기기의 확산과 통신 기술의 발달로 스마트화 됨에 따라 보안 문제가 대두되고 있다. 그 중에서 스마트공장은 기기 간 정보가 상호 교환되기 때문에 스마트공장에서 발생할 수 있는 보안위험을 식별, 평가 및 통제하기 위한 위험관리 방안이 필요하다. 본 논문에서는 국내 스마트공장(기초수준)을 현장에서 확인 한 결과를 토대로 스마트공장 위험우선순위(SFRPN, Smart Factory Risk Priority Number) 모형을 적용하여 국내 스마트공장(기초수준)에서 적용 가능한 최소보안요구사항을 연구 제안한다.

ABSTRACT

According to spreading of smart devices and development of communication technology, the security issues come to the fore in the modern factory. Especially, the smart facpry should be considered the risk management plan how to identify and evaluate, control the risks. In this paper, we suggest the minimum security requirements applying SFRPN(Smart Factory Risk Priority Number) model to domestic smart factory on the basis of the results inspecting factories.

Keywords: smart factory security, smart manufacture security

I. 서 론

1.1 연구배경 및 목적

1960년대 소비재 산업의 생산으로 도약을 시작한 우리나라의 제조업은 1970년대에 추진된 중화학공업 육성 정책에 힘입어 이제는 가전, 반도체, 기계, 조선, 자동차, 철강 등 모든 중요한 산업부문에서 세계 6위권 이내에 진입하여 있다. 이러한 제조업을 기반으로 이제 우리나라는 명실상부한 선진국으로의 도약을 준비하고 있었다. 그러나 1978년 후반 금융위기 이후 일자리 창출에는 역시 제조업이 가장 중요하다는 선지국 간의 공감대가 형성되었고 최근에는 독일에서 시작된 Industrie 4.0 프로그램을 선두로 하여 미국의 첨단제조시스템 프로그램, 일본의 제조업 중흥 프로그램 등 전통 제조 강국들이 제조업을 통한 일자리 창출과 지속적 발전을 위한 프로그램일 시작하였다. 또한 중국 "중국제조 2025" 프로그램을 시작하였다. 최근에는 영국 HVM(High Value Manufacturing)이라는 영국이 강한 첨단산업 위주의 제조업 진흥 프로그램을 시작하고 있다[1]. 전 세계 제조업 분야의 최강자인 독일에서 2011년부터 시작된 "Industrie 4.0" 프로그램은 전 세계에서

Received(09. 12. 2016), Accepted(09. 26. 2016)
† 주저자, ywcaeun@daum.net
‡ 교신저자, bbong@jnu.ac.kr(Corresponding author)

큰 반향을 불러일으켜 왔다. 미래의 인력 부족이나 기술 변화에 대응하여 향후 수십 년간 지속적으로 제조업 경쟁력을 유지하는 것을 목표로 삼고 제조업과 관련된 연구·개발·보급·확산을 목표로하는 "Industry 4.0" 프로그램은 미국, 일본 등 전통 제조 강국들은 물론 대처 수상의 신자유주의 사조에 따라 제조업에서 손을 놓았던 영국이나 기타 유럽의 여러 국가, 그리고 중국까지 영향력을 나타내고 있다. 현재 국내에서는 "Industrie 4.0"에서 제안하는 디지털 생산기술 등 중요 아이디어를 접목시켜 기존의 중소·중견기업 육성 프로그램에 "ICT(Information and Communication Technology)"를 접목시킨 새로운 정부 지원 프로그램인 "스마트공장" 프로그램을 진행하고 있다[1][2]. 국내 제조강국들은 고령화 등 노동기반 약화의 스마트 산업혁명에 대응하기 위하여 제조-ICT 융합(사물인터넷, 센서, 빅데이터 등 ICT 기술 접목을 통한 제조의 스마트화)을 통한 미래 제조업 경쟁력 확보를 위한 노력이 가속화 되고 있다. 이에 정부는 국내 제조업의 글로벌 경쟁력을 강화하기 위해 "제조업혁신 3.0 전략"을 발표하고, 후속으로 "스마트 생산방식 확산" 등 세부실행대책을 수립하여 제조업의 창조경제 구현을 목표로 진행하고 있다. 국내에는 2015년 말 기준으로 1,240개 공장의 스마트화를 완료하였다. 그러나, 현재 구축이 완료된 스마트공장에는 보안이 적용되지 않고 있어 지능화·고도화·타깃화 되고 있는 사이버 공격 및 국가기반산업에 대한 대규모 사이버 테러에 무방비한 실정이다.

본 연구에서는 국내 스마트공장에 적용 가능한 최소한의 정보보호 요구사항을 제시함으로써 효율적인 보안대책마련을 위한 기반이 될 수 있도록 제안 하고자 한다.

1.2 연구 구성

본 논문의 II장에서는 제조분야 와 관련된 보안사고 사례 및 관련 연구에 대해서, III장에서는 스마트공장 보안요구사항에 대해 살펴보고, IV장에서는 연구대상인 국내 스마트공장(기초수준) 중심의 보안요구사항을 위험우선순위를 기반으로 분석 및 연구하였으며, 마지막으로 V장에서는 본 논문의 결론으로 끝을 맺는다.

II. 관련 연구

2.1 국내 스마트공장 의의

국내 스마트공장 사업은 기존의 공장 업무 개선을 위한 제반 단계를 건너 뛰어 ICT 기술을 활용하여 공장 내부의 설비와 자재, 그리고 프로세스를 전부 연결하고 공개시킨다는 특징을 가지고 있다. 기업을 지원하는 단계에서 '수혜 기업'과 '솔루션 공급기업(ICT 기술의 보급 기업)'간의 직접적 거래를 인정하지 않고 사업 초기단계, 중간 단계, 그리고 완료단계에 스마트공장 추진단과 연계된 '코디네이터(Coordinator)' 또는 삼성그룹 지원사업의 경우에는 '멘토(Mentor)'가 관여한다는 점이 기존의 정부지원사업과 다른 점이다[1]. 스마트 공장은 제조가 일어나는 장소라는 의미에 중점을 두고 있다. 스마트공장은 광의의 스마트 공장과 협의의 스마트 공장 의미가 쓰이고 있다. 아직 국내에서 이들에 대한 합의된 의미 정의가 이루어져 있지 않은 상태이지만, 광의의 스마트 공장은 비즈니스 가치 사슬 전반에 최적화를 가능하게 하며, 유연하고 상호운용성을 지원하는 자동화 지능형 설비, 생산, 운영을 통합하고 개방을 통해 고객과 소통하는 공장으로서 설명하고 있고, 협의의 스마트 공장은 제품의 기획·설계, 생산, 품질, 유지보수 등 제조 공장에서의 생산 프로세스에 대한 정보화 및 생산 시스템의 자동화를 실현하는 공장으로 설명하고 있다[2][8]. '스마트공장' 프로그램은 아직 국제경쟁력이 취약 한 중소·중견 기업들의 생산성을 크게 향상시킬 수 있을 것으로 기대된다.

2.2 제조분야 보안 사고 사례

최근 우리는 크고 작은 제조분야의 정보보호 관련 사고를 Table 1.과 같이 경험했다.

실제 2014년 유럽과 미국의 주요 발전업체와 석유공급업체, 에너지 산업 장비 업체들을 대상으르 스피어피싱과 Winodws XP의 취약점을 악용한 드래곤플라이 사이버 스파이 활동이 포착되었다. 드래곤플라이 멀웨어는 미국 및 유럽 전역의 산업용제어시스템 정보 수집을 목적으로 수백 개 업무용 컴퓨터를 감염시켰다[17]. 국내는 한국 수력원자력 발전소의 기밀정보 유출 사건이 지난 2014년 말 총 6회에 걸쳐 제어시스템 설계도가 유출되었으며, 고리와 월성 등 국내 주요 원자력발전소의 원전중단을 협박하는

Table 1. Incidents and case in Industrial security

Year	Description	Ref
2015	3 KEY LEARNINGS : Ransomware Hits A Concrete Manufacturer	[19]
2016	Ransomware on the Rise in Regional Manufacturers	[20]
2016	Toy Manufacturer Website Spreads Crypto-ransomware Through Joomla	[21]
2016	Move over Healthcare, Ransomware Has Manufacturing In Its Sights	[22]
2016	Survey : Rising Concern Over Ransomware", Manufacturing Business Technology	[23]

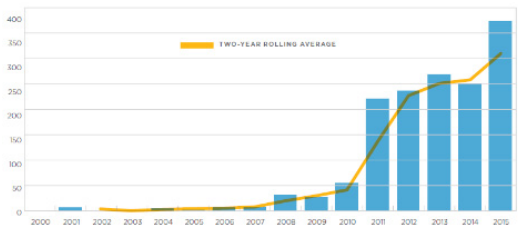

Fig. 1. Annual statistics ICS vulnerabilities [16]

사건이 발생되었다[24]. 또한, Fig. 1.에서 보여주듯이 FireEye에서 최근 발표된 보고서 "2016 Industrial Control Systems Vulnerability Trend Report"에서는 ICS의 보안 취약점의 급속한 증가를 보여주고 있고, 이에 대한 대응책 미비에 대하여 여러 각도로 시사점을 제시하고 있다[16].

첨단 ICT 기술과 제조분야가 결합된 스마트공장(Smart Factory)과 관련된 보안 사고는 단순한 개인의 문제로 국한되는 것이 아니라 전 사회적인 위협이 될 수 있기 때문에 국가적 차원의 위험관리 방안이 모색되어야 할 것이다.

2.3 ISO/IEC 27001 & IEC 62443 & IEC 61508

ISO/IEC 27001:2013 정보보호관리체계는 전체 경영시스템의 일부분을 차지하며, 사업의 위험성 접근에 기초를 두고 정보보안을 수립, 실행, 운영, 감시, 검토, 유지 및 개선하는 정보보호 시스템이다. 이 규격은 정보자산을 적절하게 보호하고 기타 이해관계자에게 신뢰성을 제공하기 위한 적절하고 알맞은 통제를 보장토록 계획한다. 규정된 요구사항은 포괄적이며, 조직의 형태, 규모 및 특성에 관계없이 모든 조직에 적용될 수 있다. ISO/IEC 27001 규격은 PDCA 개념에 따라 ISMS 시스템 구축과 실행, 그리고 지속적 향상 달성을 위한 요구사항으로 구성되어 있는데, PDCA의 각 단계별 활동은 다음과 같다.

- P단계: ISMS 수립 및 관리
- D단계: ISMS 구현 및 운영
- C단계: ISMS 모니터 및 검토
- A단계: ISMS 유지 및 개선

산업제어시스템의 국제표준 제정까지 도달해 있는 조직은 ISA의 ISA-99인데, ISA-99는 ISA62443 시리즈로 표준화안을 작성하고 IEC TC 65 / WG 10에서 각국의 심의를 거쳐 IEC 62443 문서 시리즈로서의 국제 표준이 되어 산업제어시스템의 다양한 보안 표준들 가운데 가장 일반적인 표준으로 주목을 받고 있다[15]. IEC 62443 시리즈는 크게 4개의 시리즈로 분류되며, 총 13권으로 구성되어 있다. 이 중에서 IEC 62443-1-1, IEC 62443-2-1, IEC 62443-3-1, IEC 62443-3-3 은 표준이 개발 제정되어 있는 상태이며, 2015년 12월에 IEC 62443-2-2, IEC 62443-2-3을 제정하여 발표하였다[15].

IEC TC 65에서 보안과 관련된 주요 표준 문서는 IEC 61508 Functional Safety과 IEC 62439 High Availability Automation Network 을 기본으로 살펴볼 수 있다. 이 중에서 IEC 61508 Functional Safety requirement는 전기·전자·프로그램 가능한 전자 안전관리 시스템(E/E/PE)의 기능안전(Functional Safety) 표준이며, 모든 종류의 산업에 적용 가능한 기본적인 기능 안전 표준이 될 의도로 작성되었다. IEC 61508은 시스템, 하드웨어 또는 소프트웨어의 잘못된 명세, 안전 요구사항 명세에서 누락, 하드웨어 우발 고장 메커니즘, 소프트웨어 오류, 공통 원인 고장, 인적 오류, 환경적인 영향, 공급 시스템 전압 불안정 등 위험측 고장에 대한 기능 안전을 확보하기 위한 방법을 제공하고 있다.

본 논문은 정보보호 위험환경을 고려한 통제의 선택, 구현, 관리를 포함한 조직적인 정보보호 표준을 위한 지침과 정보보호 경영 실무에 대한 지침을 제공하기 때문에 ICT 全 분야에서 널리 활용되고 있는 정보보호관리체계(ISMS) ISO/IEC 27002:2013 표준과 산업제어시스템에서 요구하고 있는 안전성 및

산업보안(Safety & Security) 요구사항을 비교 분석하여, 국내 스마트공장의 최소보안요구사항을 연구한다.

III. 국내 스마트공장 보안요구사항 분석

3.1 국내 스마트공장 보안요구사항

국내 스마트공장의 보안요구사항을 도출하기 위하여 스마트공장의 국내외 표준화 및 동향을 조사 분석하고, 현 제조 분야의 정보보호 현황과 기술동향 등을 분석한다. 또한, 정보보호의 국제표준인 정보보호 관리체계 ISO/IEC 27002:2013 "Code of practice for information security controls"[13]을 기반으로 연구한다.

정보보호관리체계(ISMS) ISO/IEC 27001:2013 표준은 정보보호 위험환경을 고려한 통제의 선택, 구현, 관리를 포함한 조직적인 정보보호 표준을 위한 지침과 정보보호 경영 실무에 대한 지침을 제공하기 때문에 ICT 전 분야에서 널리 활용되고 있다. 또한, 정보보호관리체계 국제표준인 ISO/IEC 27002:2013 "Code of practice for information security controls"을 기반으로, 전기·전자·프로그램 가능한 전자 안전관리 시스템(E/E/PE)의 기능안전(Functional Safety) 표준인 IEC 61508[14] 과 산업분야의 보안 표준인 IEC 62443 "Industrial network and system security"[15]를 참조하여 스마트공장의 안전 및 정보보호(Safety & Security) 요구사항을 도출하여, 국내 스마트공장 수준(5수준 - ICT 미적용, 기초수준, 중간수준1, 중간수준2, 고도화) 중 현재 구축되어 있는 "기초수준"에 적합한 통제항목들 도출한다. 도출된 통제항목은 국내 구축된 스마트공장 중 기계, 제조 분야 등에 대한 현장실사를 통해 최소보안요구사항을 도출한다.

3.2 스마트공장 통제항목 분석

스마트공장의 통제항목은 ISO/IEC 27002:2013의 통제분야인 "정보보안 정책(2)", "정보보안 조직(7)", "인적자원 보안(6)", "자산관리(10)". "접근통제(14)", "암호통제(2)", "물리적 및 환경적 보안(15)", "운영보안(14)", "통신보안(7)", "정보시스템 취득 개발 및 유지보수(13)", "공급자 관계(5)", "정보보안 사고관리(7)", "업무연속성 관리(4)", "준수(8)" 114개 통제항목을 기준으로, 전기·전자·프로그램 가능한 전자 안전관리 시스템(E/E/PE)의 기능안전(Functional Safety) 표준인 IEC 61508과 산업분야의 보안 표준인 IEC 62443 (Industrial network and system security)의 안전 및 정보보호(Safety & Security) 요구사항을 비교분석하여 1차 필터링 과정을 통해 스마트공장에 필요한 정보보호 통제항목을 도출한다. Fig. 3.은 스마트공장 정보보호 통제 항목 도출을 나타내고 있다.

1차 필터링을 통해 도출된 보안요구사항과 국내 스마트공장 수준(5수준 - ICT 미적용, 기초수준, 중간수준1, 중간수준2, 고도화) 중 "기초수준" 요구사항인 생산정보 디지털화(바코드·RFID에 기초적 물류정보 수집 수준, 공정물류 중심의 실적관리 수준, Lot-Tracking을 통한 품질 이력관리 수준에 적합한 통제항목을 추가한 2차 필터링을 통해 최종 스마트공장의 보안 통제항목을 도출한다.

분석을 통해 도출된 보안요구사항 및 통제항목은 국내 구축된 스마트공장 중 기계, 제조 분야 등에 대

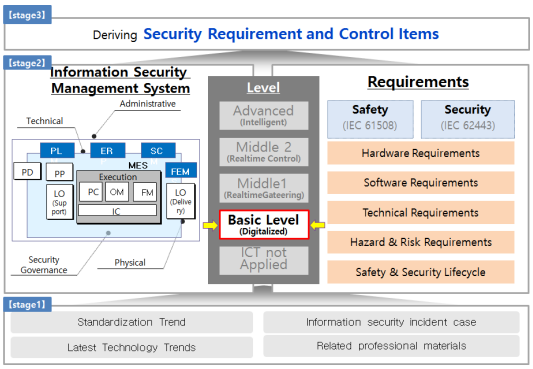

Fig. 2, Research conceptual diagram of the smart factory security requirements

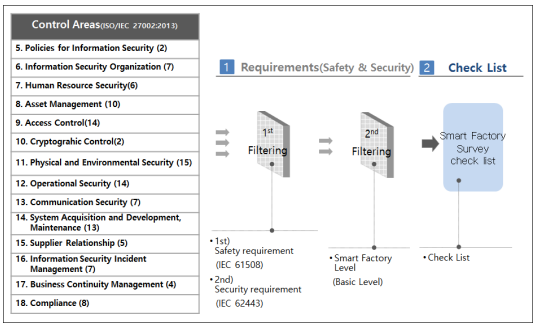

Fig. 3. Smart factory control item derivation process

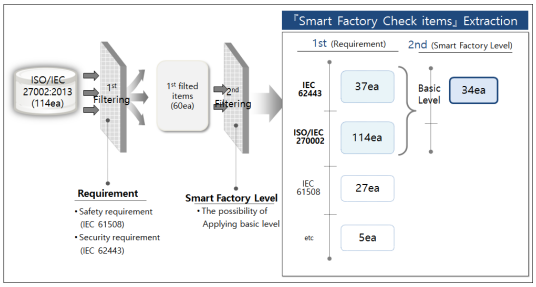

Fig. 4. Smart factory security control item

한 현장실사와 주관적인 평가에 따라 심각도, 영향도를 평가하여 스마트공장 위험우선순위 모형에 적용되며, 통제항목은 Table 4.와 같다.

3.3 국내 스마트공장 실태조사

스마트공장(총 1,240개 중 구축완료 875개, 구축중 365개)중 일부에 대하여 실태조사를 위해 현장을 방문하여 도출된 보안통제항목을 이용하여 설문지를 작성하고, 방문 전 담당자에게 배포하여 인터뷰 및 현장조사 등으로 실시하였다.

실태조사 결과, 스마트공장은 MES(Manufacturing Execution System, 제조실행시스템)를 공통적으로 도입하였다. MES 는 생산현장의 생산활동을 추적 관리하기 위한 시스템이다. 즉 생산현장에서 생성되는 설비현황, 계측, 생산, 품질 데이터들을 취합하여 ERP(Enterprise Resource Planning, 전사적자원관리) 등의 생산계획 시스템에서 생산을 계획하고 작업지시 등을 수립하는 기초데이터를 제공한다.

또한, 국내 스마트공장은 단가 경쟁이 심한 업종으로 보안투자에 대한 보수적으로 접근하고 있다. 또한 보안수준에 대한 편차가 크게 발생하였다. 특이한 점은 스마트공장 특성상 개인정보를 취급하는 경우가 적다. 하지만, 특허, 도면 등 산업보안 측면에서 중요한 정보자산들을 많이 취급하고 있다. 다만, 정보자산에 대한 명확한 식별과 보호를 하기 위한 노력이 매우 부족한 실정이다.

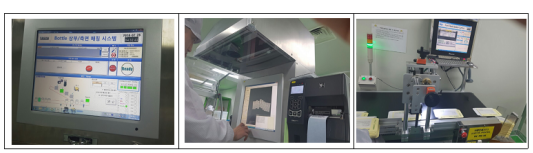

Fig. 5. Smart factories operating system status

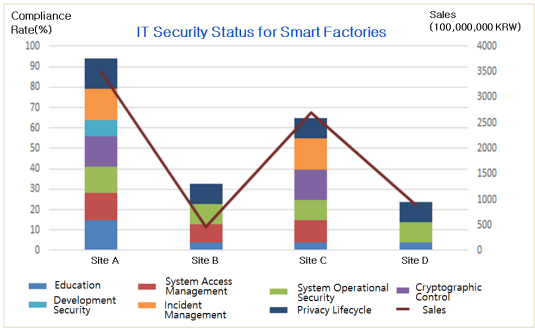

Fig. 6. IT security status for smart factories

IV. 스마트공장 최소보안요구사항

4.1 도입 연구기법

국내 스마트공장의 위험우선순위를 평가하기 위한 방법으로 고장형태영향분석(Failure mode and effects analysis, FMEA, 이하 FMEA) 분석기법을 활용한다. 자동차 산업의 경우, 발생도, 심각도, 감지도를 이용하여 위험우선순위를 계산하고, 항공우주시스템이나 원자력발전소와 같이 임무를 완성하는 것이 중요한 시스템에서는 감지도 점수를 따로 산정하지 않고 심각도를 평가할 때 감지도를 반영하여 평가한다 [12]. FEMA는 1949년 미국 국방성에서 고장이 발생함으로 인해 임무성공과 장비 및 인력의 안전에 미치는 영향에 따라 공장을 분류하기 위해 개발되었다. 그 이후 미국의 항공우주국에서 아폴로 우주산업이나 포드와 같은 자동차 회사에서 성공적으로 적용되면서 널리 알려지기 시작하였다. FMEA 분석에서는 제품의 잠재적인 고장형태(failure mode)를 찾아내고 이들 고장의 영향을 파악한 후 각 고장형태의 위험우선순위(Risk Priority Number, 이하, RPN)를 결정한다 [10][11].

4.2 스마트공장 위험우선순위(SFRPN)

본 논문에서는 고장형태영향분석(Failure mode and effects analysis, FMEA)에서 사용하는 위험우선순위(RPN, risk priority number) 계산식을 인용하여 스마트공장 위험의 우선순위를 평가한다. 스마트공장의 최소보안요구사항을 도출하기 위하여 위험우선순위를 산정하기 위한 요소로, 심각도(S, severity), 영향도(I, impact)로 구성하여 계산한

Table 2. Severity and impact evaluation criteria

Division	Range		Description
Severity	1	Low	When unapplied to the control on smart factory, severity on the inside of the factory
	~	~	
	10	High	
Impact	1	Low	The damaging impact of security requirement (control) throughout the organization
	~	~	
	10	High	

다. 심각도는 보안요구사항(Control)이 미적용 시 스마트공장 내부에 끼 치는 심각한 정도를 나타내며, 영향도는 보안요구사항(Control)이 조직 전체에 끼치는 정도를 나타낸다. 스마트공장의 위험우선순위(SFRPN, Smart Factory Risk Priority Number)을 산정하여, 도출된 스마트공장 최소보안요구사항의 우선순위를 평가한다.

4.3 스마트공장의 위험우선순위 모형

스마트공장의 위험우선순위 모형은 기존의 MIL-STD-883D, MIL-STD-1629A의 모형을 확장한 crisp 위험우선순위 모형[12]을 인용한다. crisp 위험우선순위 모형은 각각의 평가척도를 10점 평가척도로 확장하고, 서열척도에서 무의미 했던 곱의 연산을 '+, -' 연산을 통하여 보정하였으며, 같은 값의 RPN을 제거하고, 동일하게 평가되는 것을 수정하였다[12]. crisp 위험우선순위 모형은 각각의 평가척도를 10점 평가척도로 확장하기 위해서 각각의 평가척도를 0, 1 사이의 값으로 규준화 하였으며 산식은 다음과 같다.

본 논문에서는 crisp 위험우선순위 모형의 척도를 심각도(S)와 영향도(I) 척도를 사용하여 모형화 하였으며, 또한 MIL-STD 882D와 가장 유사한 위험

$$V = \frac{v - \min}{\max - \min}$$

Fig. 7 crisp RPN model evaluation criteria norming formula [12]

$$SFRPN = (Vs \times 0.53 + Vi \times 0.47) - Y \times 0.16$$

V_s: $norming\ severity$, V_i $norming\ impact$
0.53: $severity\ weight\ (crisp\ RPN\ \mathrm{model})$
0.47: $impact\ weight\ (crisp\ RPN\ \mathrm{model})$
0.16: $the\ absolute\ value\ weight\ (crisp\ RPN\ \mathrm{model})$

Fig. 8. The SFRPN is calculated

Smart Factory Risk Priority Number(SFRPN) Model

Impact (I) \ Severity (S)	1	2	3	4	5	6	7	8	9	10
1	100	98	96	93	89	85	79	72	65	58
2	99	94	90	86	81	74	68	61	53	47
3	97	91	82	76	70	63	55	50	43	37
4	95	87	77	64	57	51	45	39	34	29
5	92	83	71	59	46	40	35	30	25	21
6	88	78	66	52	41	31	26	22	18	14
7	94	73	60	48	36	27	19	15	12	9
8	80	67	54	42	32	23	16	10	7	5
9	74	62	49	38	28	20	13	8	4	2
10	69	56	44	33	24	17	11	6	3	1

Fig. 9. Smart factory risk priority number model

우선순위를 찾기 위해 가중치를 추정하였으며, 심각도(S), 영향도(I), 절대값에 대한 각각의 가중치를 추정하였다. 모형화를 위한 산식은 다음과 같다.

이 결과를 통해 10*10 스마트공장 위험우선순위 결과를 얻었으며, 이를 모형화 한다.

도출된 위험우선순위 모형을 스마트공장 보안요구사항에 적용하여 국내 스마트공장의 기초수준에 적합한 최소보안요구사항을 도출한다.

4.4 스마트공장 최소보안요구사항

Ⅲ장에서 도출된 스마트공장 통제항목에 대하여 전문가적 견해를 바탕으로 심각도(S)와 영향도(I)를 평가하고 SFRPN 모형에 적용함으로써, 우선순위를 산정하면 Table 3.과 같다.

Table 3. Smart Factory minimum security requirements

No	Controls	S	I	RPN
1	Information security awareness of company representatives	10	7	**9**
2	Information. Security Officer and department	4	3	**76**
3	Identify assets	5	2	**81**
4	Education	10	6	**14**
5	Human Resource Management	5	5	**46**
6	Information Security Regulations	8	6	**22**
7	Designated protection zones	7	7	**19**
8	Physical protection in outsourcing	4	3	**76**
9	Access control	7	8	**16**
10	Equipment and Media Import, Export	6	10	**17**

11	Access control procedures	9	10	**3**
12	Administrators and special rights management	4	9	**38**
13	External privileges	3	7	**60**
14	Password Management	7	10	**11**
15	Network Access Control	10	10	**1**
16	Manager Application Access Control	4	10	**33**
17	Mobile Device Management Regulations	7	8	**16**
18	Minimize security access system	6	7	**27**
19	Remote Access Control	7	10	**11**
20	Wireless Network Security	7	10	**11**
21	Public Server Security	10	8	**5**
22	Malware Control	7	10	**11**
23	Log Management and Monitoring	1	3	**97**
24	Encryption policy	10	10	**1**
25	personal information encryption	10	10	**1**
26	Apply Information Security for Design Phase	4	5	**59**
27	Important Information Encrytion	7	10	**11**
28	Information transmitted encrypted	8	7	**15**
29	Source program storage	2	3	**91**
30	Information Security Pledge for Development Contract	4	4	**64**
31	Incident Management	5	5	**46**
32	Limit collection of personal information	5	4	**57**
33	Privacy Encryption	7	1	**79**
34	Image information processing devices operating	8	10	**6**

스마트공장의 최소보안요구사항 중 가장 우선순위가 높은 것을 요약하면 다음과 같다.

(1) 네트워크 접근 통제
(2) 암호화 정책
(3) 개인보관 정보 암호화
(4) 공개 서버 보안
(5) 영상정보처리기기 운영
(6) 중요정보 암호화 및 전송 시 암호화
(7) 패스워드 관리
(8) 원격 접근 통제
(9) 무선 네트워크 보안
(10) 회사 대표의 정보보호 인식

V. 결 론

스마트공장은 실태조사 결과 정보보호에 대한 인식이 부족하며, 생산현장에서 취급하는 정보 및 자료들의 보호방안이 절실한 상황이다. 현재 국내에서는 스마트공장 확산을 위해 정부차원에서 노력을 하고 있다. 이에 본 논문에서는 위험우선순위에 기반한 스마트공장의 최소보안요구사항을 제안하였다. 이를 국내 구축된 기초수준의 스마트공장에 대한 최소보안요구사항을 마련하여 최소한의 보안대책을 마련하기 위한 방안으로서 도움이 될 것이라고 기대된다. 현재의 스마트공장 환경은 ICT 외부인력에 의한 위탁관리 환경이 대부분이기 때문에 사이버 공격에 취약할 것으로 판단된다. 특히 스마트공장 보안 전문인력은 전무한 실정이며, 보안 위협 및 취약점 식별이 매우 필요한 실정이다. 본 연구는 스마트공장을 활성화하고 보안성을 확보하기 위한 방안으로서 활용할 수 있다.

앞으로 나아갈 방향으로, 먼저 본 연구에서 제시한 스마트공장의 위험우선순위 평가를 토대로 실 환경에서의 모의검증을 통해 적용 가능성을 검증하고 우선순위를 재 설정하여 효과적으로 보안위협에 대처할 프로세스 및 보안검증 방법에 대한 연구가 필요할 것이다.

Table 4. Domestic smart plant (basic level) control entry vs IEC 62443, ISO/IEC 27002

No	Control	IEC 62443	ISO/IEC 27002
1	Information security awareness of company representatives	-	- A.5.1.1 (Policies for Information Security)
2	Information. Security Officer and department	-	- A.6.1.1 (Responsibility and Role for Information Security)
3	Identify assets	-	- A.8.1.1 (List of Assets)
4	Education	-	- A.7.2.2 (Information security awareness, education, training)
5	Human Resource Management	-	- A.7.1.2 (Conditions of the employment contract) - A.7.2.1 (Management Responsibility) - A.7.3.1 (The responsibility of employment termination and change)
6	Information Security Regulations	-	- A.5.1.1 (Policies for Information Security)
7	Designated protection zones		- A.11.1.1 (Physical security perimeter)
8	Physical protection in outsourcing		- A.11.1.1 (Physical security perimeter)
9	Access control		- A.11.1.2 (Physical access control)
10	Equipment and Media Import, Export		- A.11.1.4 (External and Environmental threats)
11	Access control procedures	- IAC 5.3 (User identification and authentication) - IAC 5.5 (Account Management) - IAC 5.6 (Identity management) - IAC 5.7 (Authentication Management)	- A.9.1.1 (Access Control Policy)
12	Administrators and special rights management	-	- A.9.2.2 (Privileged rights management)
13	External privileges	-	- A.9.2.4 (Review of User Access Rights)
14	Password Management	- IAC 5.9 (The degree of password based authentication)	- A.9.2.3 (Management of user authentication information secret)
15	Network Access Control	- RDF 9.3 (Network separation)	- A.13.1.1 (Network Access control) - A.13.1.3 (Network separation)
16	Manager Application Access Control	- IAC 5.14 (Use notification system) - IAC 5.15 (Connection via an untrusted network)	- A.13.1.2 (Network Services Security)
17	Mobile Device Management Regulations	- UC 6.4 (The wireless using controls)	- A.6.2.1 (Policy for a mobile device)
18	Minimize security access system	- RDF 9.5 (Limited communication between individuals in the general purpose)	- A.9.2.5 (Adjustment and delete of Access Rights)

19	Remote Access Control	- RDF 9.5 (Limited communication between individuals in the general purpose)	- A.6.2.2 (Remote Work)
20	Wireless Network Security	- UC 6.4 (The wireless using controls)	- A.13.1.1 (Network Control)
21	Public Server Security	-	- A.13.1.2 (Network Services Security)
22	Malware Control	- SI 7.4 (Malicious code protection)	- A.12.2.1 (Control of the malicious program)
23	Log Management and Monitoring	- UC 6.10 (Audit work) - UC 6.11 (Auditing storage space) - UC 6.12 (Action on Auditing failed)	- A.12.4.3 (Log of Administrator and Operator)
24	Encryption policy	- DC 8.3 (Information Confidentiality) - DC 8.4 (Persistence of information)	- A.10.1.1 (Policy of Password Control and Using)
25	personal information Encryption	-	- A.10.1.1 (Policy of Password Control and Using책)
26	Apply Information Security for Design Phase	-	- A.14.1.1 (Security requirements analysis and distinguish)
27	Important Information Encrytion	- DC 8.3 (Information confidentiality) - DC 8.4 (Persistence of information)	- A.10.1.1 (Policy of Password Control and Using)
28	Information transmitted encrypted	- DC 8.3 (Information confidentiality) - DC 8.4 (Persistence of information)	- A.13.2.1 (Policies and procedures of Information transfer)
29	Source program storage	-	- A.14.3.1 (Protection of the test data)
30	Information Security Pledge for Development Contract	-	- A.14.2.1 (Security policy of Development)
31	Incident Management	-	- A.16.1.1 (Responsibilities and Procedures)
32	Limit collection of personal information		- A.18.2.4 (Privacy)
33	Privacy Encryption	-	- A.18.2.4 (Privacy)
34	Image information processing devices operating	-	- A.18.2.4 (Privacy)

References

[1] Jin-woo Park, "Government policies and Achievements on Smart Factory," Industrial Engineering Magazine, 23(1), pp. 13-17, Mar. 2016.

[2] Yong-woon Kim besides 3, "International and Domestic standardization for Smart Factory," The Journal of The Korean Institute of Communication Sciences, 33(1), pp. 30-36, Dec. 2015.

[3] Jeong-cheol Lee, "The diagnostic model and Practical using plan for Smart Factory," Korean Institute of Industrial Engineers, pp. 2105-2127, Nov. 2015.

[4] Jeong-cheol Lee, "Industry classification System and Driving direction related to Smart Factory," Korean Institute of Industrial Engineers, pp. 1493-1515, Apr. 2016.

[5] Jong-man Park, "Technology and Issue on Embodiment of Smart Factory in Small-Medium Manufacturing Business," The Journal of The Korean Institute of Communication Sciences, 40(12), pp. 2491-2502, Dec. 2015.

[6] KATS, Standardization Roadmap for Smart Factory, Dec. 2015.

[7] KATS, Smart Manufacturing Standardized Framework, Dec. 2015

[8] Deok-gi Kim, "Smart Factory Part I, Basic concepts and Structures," KS proposed by KATS, Dec. 2015.

[9] ICS-CERT, Industrial Control Systems Cyber Emergency Response Team Report 2015, 2015.

[10] IEC 60812, "Analysis techniques for system reliability-Procedures for failure mode and effect analysis(FMEA)," IEC, Second edition, Jan, 2006.

[11] FMECA, "Failure mode, effects and criticality analysis," FMECA MIL-P-1629, Jan. 2007.

[12] Young-jae Choi, "Risk Evaluation Model for FMEA," Korean Institute of Industrial Engineers, pp. 586-595, Nov. 2012.

[13] ISO/IEC 27002:2013, "Code of practice for information security controls," ISO/IEC, 2013.

[14] ISO/IEC 61508, "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES)," IEC, 1999.

[15] IEC 62443-3-3, "Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels," IEC, Part 3-3, Aug, 2013.

[16] FireEye, 2016 Industrial Control Systems Vulnerability Trend Report, Aug. 2016.

[17] SANS, "The Impact of Dragonfly Malware on Industrial Control Systems," SANS Institute InforSec Reading Room, Jun, 2016.

[18] The Stuxnet Wiki, "https://sites.google.com/site/thestuxnetwiki/"

[19] Teemu M, "3 KEY LEARNINGS : Ransomware Hits A Concrete Manufacturer," F-Secure, Apr, 2015.

[20] Vermont Manufacturing Extension Center, "Ransomware on the Rise in Regional Manufacturers," Vermont Manufacturing Extension Center, Apr, 2016.

[21] Jp Buntinx, "Toy Manufacturer Website Spreads Crypto-ransomware Through Joomla," Bitcoinist.net Cryptocurrency Reviews And Technology, Apr, 2016.

[22] Bill McGee, "Move over Healthcare, Ransomware Has Manufacturing In Its Sights," FORTINET, Jun, 2016.

[23] KnowBe4, "Survey : Rising Concern Over Ransomware," Manufacturing Business Technology, Jul, 2016.

[24] NIS, "2015 National Information Security White Paper," NIS, Apr, 2015.

〈저 자 소 개〉

이 병 권 (Byung-Gueon YI) 정회원
1989년 2월: 전북대학교 컴퓨터공학과 졸업
1992년 2월: 포항공대 대학원 전산과 석사 수료
2005년 2월: 전남대학교 대학원 정보보호협동과정 박사 수료
2001년 1월~2008년 11월:한국정보보호진흥원 팀장
2009년 6월~2012년 5월: (주)안랩 팀장
2012년 6월~현재: 현대오토에버 정보보안실장
〈관심분야〉 정보보호, SCADA보안, 스마트팩토리 보안, IoT보안 등

김 동 원 (Dong-Won Kim) 종신회원
2009년 2월: 서울과학기술대학교 컴퓨터공학과 졸업
2012년 2월: 건국대학교 정보통신대학원 정보보호학과 석사
2014년 2월: 고려대학교 정보보호대학원 정보보호학과 박사 수료
2014년 2월: 현대오토에버 정보보안기술팀 과장
2014년 3월~현재: 서울호서전문학교 사이버해킹보안과 전임교수
〈관심분야〉 시큐어코딩, 정보보호, 모바일 보안, 지능형 차량 보안, SSCA, 정형기법 등

노 봉 남 (Bong-Nam Noh) 종신회원
1978년: 전남대학교 수학교육과 졸업(학사)
1982년: KAIST 대학원 전산학과 졸업(석사)
1994년: 전북대학교 대학원 전산과 졸업(박사)
1983년~현재: 전남대학교 전자컴퓨터공학부 교수
2000년~현재: 전남대학교 시스템보안연구센터 소장
〈관심분야〉 정보보안, 시스템 및 네트워크 보안