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.2019.29.3.629

신뢰성 있는 스마트팩토리를 위한 사이버보안 아키텍처

김 현 진,[1†] 김 성 진,[1] 김 예 솔,[2] 김 신 규,[2] 손 태 식[1,3‡]
[1]아주대학교 컴퓨터공학과, [2]ETRI 부설연구소, [3]아주대학교 사이버보안학과

Cybersecurity Architecture for Reliable Smart Factory

HyunJin Kim,[1†] SungJin Kim,[1] Yesol Kim,[2] Sinkyu Kim,[2] TaeShik Shon[1,3‡]
[1]Department of Computer Engineering, Ajou University
[2]The Attached Institute of ETRI
[3]Department of Cyber Security, Ajou University

요 약

제4차 산업혁명 시대에 들어서며 세계 각국은 제조 산업의 경쟁력 확보를 위해 스마트팩토리를 빠르게 확산시키기 위한 보급 사업을 진행하고 있다. 그러나 스마트팩토리는 네트워크 환경이 폐쇄적이었던 기존 공장과는 달리 내부와 외부의 사물들이 서로 연결되고 다양한 ICT 기술이 활용되기 때문에 보안 취약점이 발생할 수 있다. 그리고 스마트팩토리는 사고 발생 시 경제적인 피해가 매우 크기 때문에 특정 대상에게 금전적 피해를 야기하고자 수행되는 사이버 공격의 대상이 되기 쉽다. 따라서 스마트팩토리에 대한 보안 연구 및 적용이 반드시 필요한 상황이지만 구체적인 스마트팩토리 시스템 아키텍처가 제시되어 있지 않아 스마트팩토리 보안요구사항도 정립되어 있지 않은 상황이다. 이러한 문제점을 해결하기 위해 본 논문에서는 국내외 주요 스마트팩토리 참조모델을 기반으로 스마트팩토리의 주요 특성을 식별하고 이를 반영할 수 있는 스마트팩토리 아키텍처를 도출하였다. 이후 도출된 스마트팩토리 아키텍처를 바탕으로 보안 위협을 식별하였으며 이에 대응할 수 있는 보안요구사항을 제시함으로써 스마트팩토리의 보안성 향상에 기여하고자 한다.

ABSTRACT

In the era of the 4th industrial revolution, countries around the world are conducting projects to rapidly expand smart factory to secure competitiveness in manufacturing industries. However, unlike existing factories where the network environment was closed, smart factories can be vulnerable because internal and external objects are interconnected and various ICT technologies are used. And smart factories are likely to be the subject of cyber-attacks that are designed to cause monetary damage to certain targets because economic damage is so serious when an accident occurs. Therefore, it is necessary to study and apply security for smart factories, but there is no specific smart factory system architecture, so there is no establish for smart factory security requirements. In order to solve these problems, this paper derives the smart factory architecture that can extract and reflect the main characteristics of a smart factory based on the domestic and foreign reference model of smart factories. And this paper identifies the security threats based on the derived smart factory architecture and present the security requirements to cope with them for contributing to the improvement of the security of the smart factory.

Keywords: Smartfactory, Architecture, Security Threats, Security requirement

Received(03. 28. 2019), Accepted(05. 23. 2019)
† 주저자, ny24007@ajou.ac.kr
‡ 교신저자, tsshon@ajou.ac.kr(Corresponding author)

I. 서 론

최근 제4차 산업혁명의 도래에 따라 제조업 분야에서도 스마트팩토리에 관한 관심이 높아지고 있다. 스마트팩토리는 생산 과정에 필요한 전체 사물들을 산업 사물인터넷 기술을 통해 연결하여 통신체계를 구축하고 디지털화하여 CPS(Cyber Physical System), 빅데이터, 클라우드 그리고 인공지능 등 다양한 ICT(Information & Communication Technology) 기술들이 제조업에 활용될 수 있도록 함으로써 생산의 자동화 및 최적화를 추구한다. 이로 인해 기존 노동력 중심의 생산 공정들이 디지털화되고 자동화되어 운영됨으로써 불량률 감소, 생산성 개선 그리고 원가 감축 등의 혁신을 이루고 있으며 다양한 비즈니스 간의 연계를 통해 새로운 부가가치를 창출할 수 있다[1].

이러한 스마트팩토리의 긍정적인 도입 효과로 인해 전통 제조 강국에서는 스마트팩토리를 통해 제조 산업의 경쟁력을 다시 확보하고 경제 침체 현상을 극복하기 위한 노력을 하고 있다. 대표적인 제조 강국인 미국, 독일 그리고 일본에서는 수년 전부터 4차 산업혁명에 대해 대비하고 있었으며, 4차 산업혁명의 성공적인 도입을 위한 정책을 수립하고 실행하고 있다. 미국은 기업들이 4차 산업혁명을 주도적으로 실행하고 있으며 정부는 이에 호응하여 2009년 Remarking America 슬로건을 시작으로 2012년 첨단제조 파트너십 발족과 국가제조혁신 네트워크를 구축하였으며, 독일의 경우 2010년 Industrie 4.0을 통해 제조업 혁신을 위한 정책과 방향을 정하는 사전작업을 수행한 뒤 이를 구체화하고 실행력을 높이기 위한 Platform Industrie 4.0을 2015년 공식 출범하여 4차 산업혁명의 이해당사자인 정부, 기업, 사회단체, 협회 간의 협력 체계를 조성하고 4차 산업혁명에 대응하고 있다[2]. 또한, 일본과 중국에서는 정부 기관이 중심이 되어 국가프로젝트를 통해 스마트팩토리 추진을 진행하고 있으며, 국내의 경우 2014년 제조업 혁신 3.0 추진전략을 시작으로 2015년 5월 스마트공장추진단을 설립하여 스마트팩토리 보급·확산사업을 진행하고 있다[3].

하지만 Stuxnet[4], DUQU 2.0[5], BlackEnergy[6], Industroyer[7] 그리고 TRISIS[8] 등과 같은 실 공격 사례에서 알 수 있듯이 산업제어시스템에 대한 공격이 지능화, 고도화, 타깃화되고 있는 현황에서 스마트팩토리의 보안에 대한 우려 또한 높아지고 있다. 스마트팩토리는 다양한 사물과의 연결성이 증가하여 공격자의 공격 경로가 증가할 수 있으며 다양한 기술들의 접목으로 인해 취약성이 증가할 수 있어 이를 악용한 사이버 공격이 발생할 수 있다. 더욱이 스마트팩토리에 대한 사이버 공격이 성공할 경우 사회·경제적 파급효과가 매우 높기 때문에 사이버 공격의 대상이 될 확률이 높아 스마트팩토리의 보안에 대한 고려는 매우 필수적이다.

그러나 빠른 스마트팩토리 보급 속도에 비해 스마트팩토리에 관한 보안 연구는 더디게 진행되고 있다. 그 이유에 대해 살펴보면 스마트팩토리는 다양한 제조 업종에 적용될 수 있고 사용되는 기술도 한정되지 않아 학술적으로 공통된 스마트팩토리 시스템 아키텍처를 도출하기 어렵기 때문에 보안 연구의 진행이 더디며, 현장에서는 공장들 대부분이 중소기업으로 제조 공정의 데이터화 및 디지털화에 초점을 맞춘 기초 단계의 스마트팩토리화가 우선하여 진행되고 있는 현황에서 보안을 적용할 경우 발생하는 구축 및 운영비용에 대해 부담감을 느끼고 있기 때문이다[4].

위와 같은 사유로 스마트팩토리 보급 사업은 활발히 진행되고 있으나, 아직 스마트팩토리 위협분석 및 보안 요구사항에 관한 연구는 부족한 상황이다. 따라서 본 논문에서는 국내외 주요 스마트팩토리의 참조모델 분석을 통해 스마트팩토리의 주요특징들을 식별하고 이를 반영할 수 있는 스마트팩토리 아키텍처를 도출하였다. 이후 도출된 아키텍처를 바탕으로 스마트팩토리의 주요특징에 초점을 두어 발생할 수 있는 보안 위협과 이에 대응하기 위한 최소 보안 요구사항을 제시하였다.

본 논문의 구성은 2장에서 스마트팩토리 관련 주요 기관들과 해당 기관의 참조모델을 살펴보고 기존 제어공정 시스템 관련 보안 요구사항 표준 및 보안 가이드라인을 살펴본다. 3장에서는 주요 스마트팩토리 참조모델들을 세부 분석하였으며 4장에서는 스마트팩토리 참조모델을 통해 스마트팩토리의 주요특징과 이를 반영하는 스마트팩토리 아키텍처를 도출하였다. 마지막 5장에서는 스마트팩토리의 주요특징에 의해 발생할 수 있는 보안 위협을 식별하고 최소 보안 요구사항을 제시한 뒤 6장에서 결론을 맺는다.

II. 관련 연구

2.1 스마트팩토리 참조모델

주요 국내외 스마트팩토리 참조모델에는 독일 Platform Industrie 4.0 협회의 RAMI 4.0 (Reference Architecture Model Industrie 4.0) 모델, 미국 IIC(Industrial Internet Consortium)의 IIRA(Industrial Internet Reference Architecture)모델 그리고 국내에서는 스마트공장추진단의 스마트팩토리 참조모델이 있다. 위의 기관 간에는 스마트팩토리의 추진 방향성이 다르기 때문에 제시하고 있는 스마트팩토리의 참조모델도 차이점이 존재한다.

2.1.1 RAMI 4.0 참조모델

독일 PI4.0은 생산제조 과정 전체의 표준을 표현할 수 있는 스마트팩토리 참조모델을 만들기 위하여 기존 제조 공정 통합 표준인 ISA(International Society for Automation)- 99/IEC(International Electrotechnics Commission) 62264계층 모델을 기반으로 참조모델을 생성하려 하였다. 하지만 해당 표준은 스마트팩토리를 표현하는데 한계점을 가지고 있었다. 주요한 한계점으로는 스마트팩토리의 경우 생산에 직접 관여하는 최하위 기기부터 생산계획시스템(ERP, Enterprise Resource Planning)까지의 전체 계층들 간의 유연한 정보교환이 필요하나 표준에서는 생산설비시스템에서 제조실행시스템(MES, Manufacturing Execution System)까지의 계층 범위에서 인접한 계층 간 정보교환만 규정하고 있다는 점 그리고 스마트팩토리는 물리적으로 떨어진 공장이나 다양한 비즈니스 도메인 간 정보교환 또한 필요하나 표준에서는 공장 내 도메인으로만 국한되어 있다는 점이 있다[9]. 따라서 Platform Industrie 4.0에서는 스마트그리드 도메인의 주요 참조모델인 SGAM(Smart Grid Architecture Model)을 바탕으로 기존 제조 표준들을 융합할 수 있는 3차원의 스마트팩토리 참조모델인 RAMI 4.0(Reference Architecture Model for Industrie 4.0)을 도출하여 발표하였다.

Fig.1.과 같이 RAMI 4.0은 생명주기와 가치 흐름의 수평적 통합계층, 시스템계층구조의 수직적 통합계층 그리고 이들 간 상호호환을 위한 계층으로 표현되는 참조모델로 구성요소 및 구성은 기존 제조 산업 국제표준을 참조하고 있다. 생명주기와 가치 흐름의 경우 IEC 62890 표준 기반, 시스템계층구조의 경우 IEC 62264/61512 표준을 기반으로 하고 있으며, RAMI 4.0의 산업실적용 및 확장을 위해 기존표준을 수정 및 추가하고 새로운 표준들을 제정하고 있다.

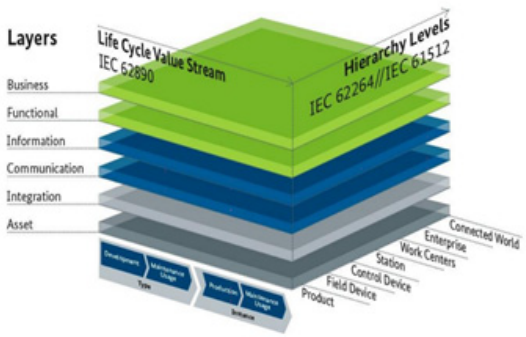

Fig. 1. PI 4.0 Reference Model(RAMI 4.0)

2.1.2 IIRA 참조모델

IIC는 산업인터넷에 필요한 기술을 개발하고 이를 산업 전반에 실적용 하는 것을 가속하기 위한 조직으로 다양한 산업 도메인을 대상으로 하고 있으며 스마트팩토리는 그중 하나의 구성도메인으로 보고 있다. IIC에서는 다양한 산업 영역에 걸쳐 산업 사물인터넷(Industrial IoT) 시스템을 도입하기 위한 참조모델의 필요성을 느끼고 ISO/IEC/IEEE 42010:2011 표준을 바탕으로 IIRA(Industrial Internet Reference Architecture)를 도출하여 발표하였다[10].

IIRA 참조모델은 비즈니스 관점, 사용 관점, 기능적 관점 그리고 구현 관점으로 구분하여 추상적인 아키텍처들을 제공하고 있다. Fig.2.와 같이 참조모델의 각 관점은 계층적으로 구성되며, 상위 계층은 하위 계층이 갖추어야 할 요소를 식별하는 데 도움을 주며, 하위 계층은 상위 계층의 요구사항을 이행할 수 있는 토대를 제공한다. 그러나 참조모델에서는 구성장치, 아키텍처 구조, 통신 규칙 등은 구체적으로 명시하지 않고 있으며 시스템 아키텍처 개발 시 필요에 따라 사용할 수 있도록 가이드라인만 제공하고 있다.

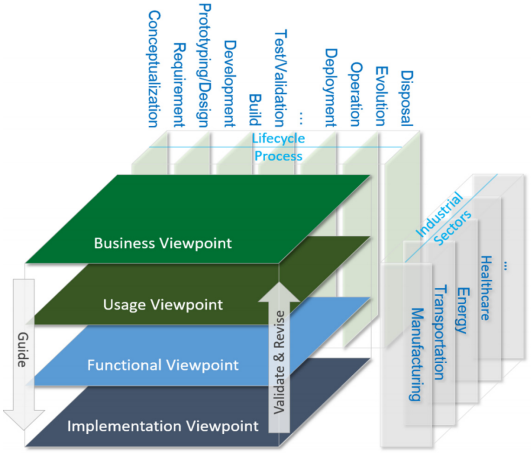

Fig. 2. IIC Reference Model(IIRA)

2.1.3 스마트공장추진단 참조모델

스마트공장추진단은 스마트팩토리 보급 확대 및 고도화에 중점을 맞추어 민관합동으로 설립된 기관으로 스마트팩토리에 대한 이해를 도모하고, 구축에 필요한 정보를 제공하기 위해 스마트팩토리 참조모델을 발표하였다. 11대 주요 업종을 중심으로 스마트팩토리의 주요 설비의 조건, 수준별 요구사항을 정의하고 있다[11]. 스마트공장추진단이 스마트팩토리 보급 사업을 진행할 때 참고하는 자료이기 때문에 구체적인 기술, 운영 등의 관점에서 서술된 것이 아닌 제조 영역별 스마트팩토리의 수준을 정의하는 것에 초점을 맞추고 있다. Fig.3.은 스마트공장추진단에서 식별하고 있는 스마트팩토리의 범위로 제품 주문부터 제작, 출하까지 모든 제조 과정을 포함하고 제어 자동화, 현장 자동화, 응용시스템 영역을 모두 포함하도록 구성되어 있으며 CPPS(cyber physical production system), AI(Artificial Intelligence), Cloud 등 다양한 ICT 기술이 연계되고 있음을 확인할 수 있다.

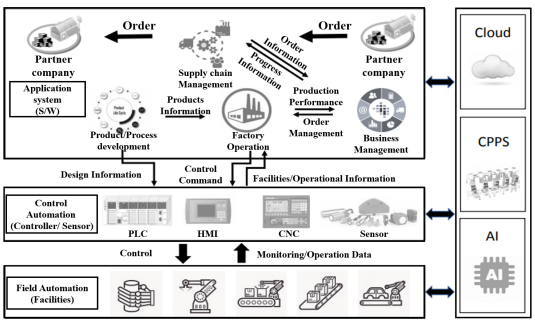

Fig. 3. Korea Smart-Factory Foundation Reference Model

2.2 기존 제조 공정 시스템 관련 보안 요구사항

기존 산업제어시스템의 사이버보안에 있어 주요한 보안표준 및 보안가이드라인으로 학계 및 산업계에서 많이 참고하는 ISA/IEC 62443과 NIST(National Institute of Standards and Technology) 800-82 문서에 대해 살펴본다.

2.2.1 ISA/IEC 62443

ISA/IEC 62443 표준은 산업 자동화 및 제어시스템을 안전하게 구현하기 위한 절차를 정의하는 표준이다[13]. ISA/IEC 62443은 원래 ISA에 의해 ISA99 표준으로 만들어졌으며 ANSI(American National Standards Institute)에 의해 ANSI/ISA-99로 발표되었으나, 2002년에 현재 사용하고 있는 ISA/IEC 62443이라는 표준으로 변경되어 현재 IEC TC 65 WG 10에서 표준화를 진행하고 있다. 대상 산업 도메인을 특정하지 않고 전반적인 산업시스템 모두를 대상으로 하고 있으며, 하드웨어 및 소프트웨어를 포함하는 연속적인 보안 프로세스 구축을 목표로 하고 있다. ISA/IEC 62443 표준 및 기술문서는 네 가지 그룹(일반 정책, 절차, 시스템 그리고 구성요소)으로 나뉘며 각 그룹의 설명은 아래와 같다.

- ◉ 일반: 표준 및 기술문서에서 제시하는 제어시스템의 보안 매트릭스와 개요, 모델, 그리고 용어와 관련된 사항을 다룸
- ◉ 정책 및 절차: 제어시스템에 보안 프로그램을 보다 효율적으로 적용하기 위한 정책 및 절차와 관련된 사항을 다룸
- ◉ 시스템: 제어시스템의 보안을 위한 구조 가이드라인 및 요구사항과 관련된 사항을 다룸
- ◉ 구성요소: 제어시스템을 구성하는 제품의 기술적 요구사항과 관련된 사항을 다룸

2.2.2 NIST SP 800-82

NIST SP 800-82 문서는 산업계 제어시스템 보

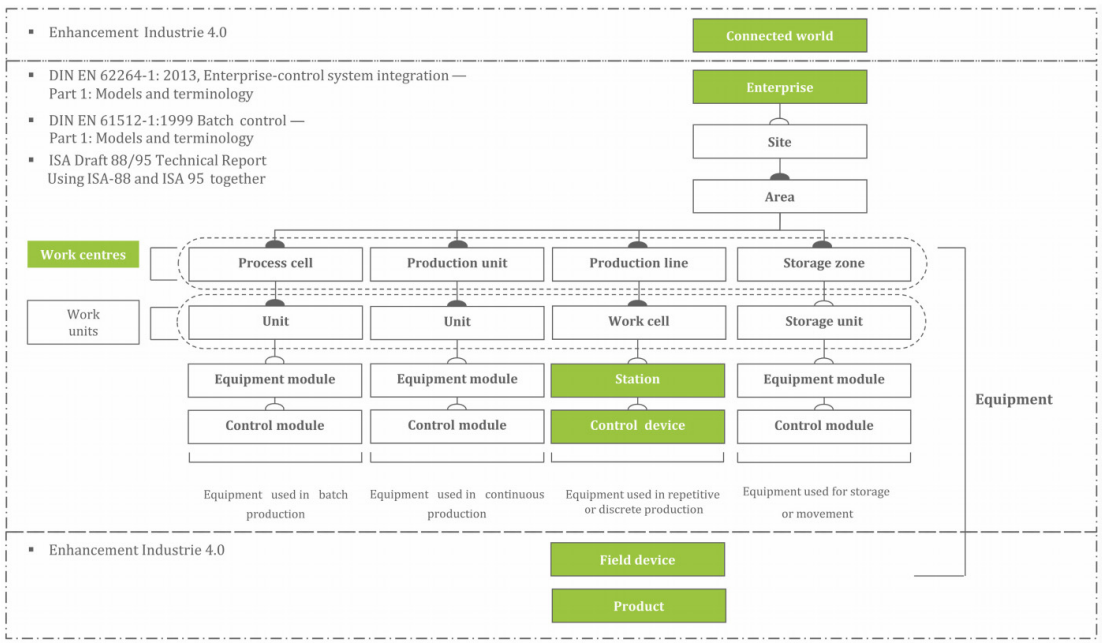

Fig. 4. Hierarchy levels of RAMI 4.0

안 가이드라인을 제시하기 위해 2011년에 처음 개발되었고, 2013년 4월 1차 개정을 거쳐 지난 2014년 5월 2차 개정안의 draft를 공개하였다[12]. 실제 제어시스템의 보안을 모니터링하는 ICS-CERT에서 해당 문서를 주요 참고문서로 선택하였으며, 제어시스템 분야의 보안 관련 연구에서 다수 활용되고 있다. 해당 문서는 SCADA(Supervisory Control And Data Acquisition)/DCS(Distributed Control System)와 같은 산업제어시스템의 구성요소 및 네트워크 구성에 관한 내용을 포함하고 있으며 산업제어시스템에서 보안을 어떻게 적용할지에 대한 가이드라인을 제시하고 있다. 성능과 신뢰도 그리고 안전성에 대한 요구사항을 동시에 만족할 수 있는 가이드라인을 제시하는 것이 목표이다. 해당 문서에는 위험 관리 및 평가, 보안 프로그램 개발 및 배치, 산업제어시스템 보안 구조, 산업 제어시스템에 보안 기술 적용에 관한 내용을 주 내용으로 담고 있다.

앞서 살펴본 보안표준 및 보안 가이드라인은 기존 산업제어시스템을 대상으로 하고 있기 때문에 스마트팩토리에 적용하기 위해서는 스마트팩토리의 주요 특성을 고려한 추가적인 보안연구가 진행되어야 한다.

III. 스마트팩토리 참조모델 분석

RAMI 4.0, IIRA 그리고 스마트공장추진단의 스마트팩토리 참조모델들의 경우 추상적 모델로 구체적인 아키텍처 도출을 위해서는 추가적인 분석이 필요하다. 본 장에서는 RAMI 4.0 참조모델의 구성요소 및 계층구조와 IIRA의 스마트팩토리 관련 기술 그리고 스마트공장추진단의 스마트팩토리 구성 예시에서 네트워크 기술을 분석한다.

3.1 스마트팩토리의 구성요소 및 구조 분석

RAMI 4.0 참조모델의 수직적 통합모델은 생산시스템의 물리적 계층과 기업업무시스템의 기능적 계층의 통합을 위해 IEC 62264 및 IEC 61512 표준을 기반으로 Fig.4.와 같은 계층모델을 제시하고 있다[13]. IEC 62264 표준의 구성요소들을 동일하게 포함하고 있으나, 최하위 계층에 생산하고 있는 제품 자체를 의미하는 제품 계층 그리고 최상위 계층에 스마트팩토리의 공장연합, 외부 엔지니어링 장소, 공급자, 고객 등과 협업을 위한 연결세상 계층을 추가하였으며, 생산 프로세스 방식 및 논리적 구성 집합에 따라 구성요소를 세분화하고 있다. 주요 구성요소의 설명을 정리하면 Table 1.과 같다.

Table 1. Component of RAMI 4.0

Component	Description	Level
Connected World	Collaboration with factory unions, external engineering offices, suppliers, customers, etc.	-
Enterprise	Organization that coordinates the operation of one or more factories.	4
Work Center/ Production Line	Logical group of equipment required for one or more batch production methods Generally, the logical control of one process facility in the workplace	3
Control Device	A group of physical module equipment capable of performing basic control (Examples of control modules are pumps, valves, flow meters, etc.)	2
Filed Device	A group of devices, such as intelligent sensors, actuators, etc.	1
Product	Meaning of the product itself (A set of disparate species assembled together for the production of parts with similar manufacturing requirements.)	-

IIRA는 기능적인 시스템 요구사항을 설명하기 위해 산업사물인터넷 시스템을 제어 도메인, 운영 도메인, 정보 도메인, 응용 프로그램 도메인, 비즈니스 도메인으로 분리하였으며, 도메인별 데이터 및 제어 흐름과 관련하여 각 도메인이 어떻게 관련되어 있는지를 Fig.5.와 같이 보여주고 있다. 각 도메인의 설명을 분석하여 RAMI 4.0의 수직적 통합모델의 계층을 매핑하면 Table 2.와 같다.

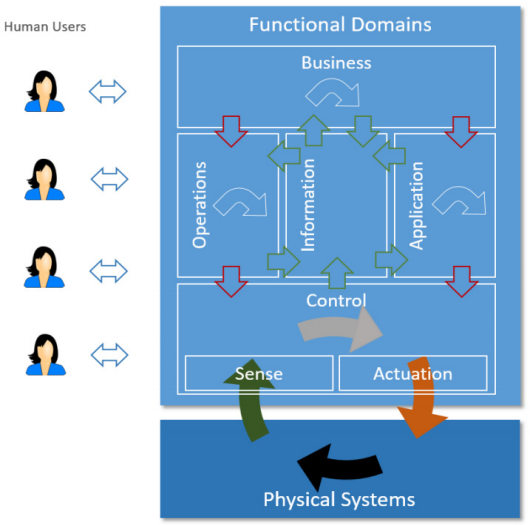

Fig. 5. Functional Domains of IIRA

Table 2. Mapping IIRA Component to RAMI 4.0

Component	Description	Level
Control Domain	Control physical systems using data read from sensors, actuators, etc.	1, 2
Operation Domain	Responsible for provisioning, managing, monitoring, and optimizing systems	2, 3
information Domain	Provide the ability to collect data from multiple domains, transform and analyze these data, and collect high-level information about the entire system.	2, 3
Application Domain	Applications and features that implement specific business functions	1, 2, 3, 4
Business Domain	Provides functions that enable an end-to-end operation of the Internet of things. (ERP, CRM, PLM, MES, HRM. etc.).	3, 4

분석된 바와 같이 RAMI 4.0 참조모델에서는 기존 제조 공정 표준의 계층구조를 따르고 있으며 IIRA 참조모델에서도 기능적 계층구조를 확인할 수 있다. 이는 기존 공장자동화에서는 하나의 장치가 하나의 기능을 수행하는 반면 스마트팩토리에서는 하나의 장치가 다수의 기능을 수행할 수 있어 물리계층 간의 통합은 이루어지나 기능적 관점에서는 계층구조가 유지되는 것을 의미한다. 따라서 기존 공장자동화 수준의 공장도 스마트팩토리는 포함하고 있으며 이는 스마트공장추진단의 스마트팩토리 수준 정의에서도 기존 공장자동화를 기초수준 및 중간수준의 스마트팩토리로 포함하고 있는 것에서도 확인할 수 있다. 따라서 스마트팩토리 아키텍처의 구성요소와 구조는 RAMI4.0의 수직적 통합계층을 기반으로 스마트팩토리의 주요특징을 식별하여 확장하고자 한다.

3.2 스마트팩토리 기술적 분석

스마트팩토리 참조모델에서는 시스템 아키텍처를 제공하고 있지 않고, 사용되는 기술이나 기기 등 실제 구현을 위해 고려해야 할 사항들은 참고사항으로만 언급하고 있다. 따라서 각 참조모델의 문건에서 명확히 언급된 IT 기술들과 함께 기능적 요구사항을 바탕으로 특정 IT 기술의 사용이 명확한 요소들을 선별하여 앞서 분석된 스마트팩토리의 구성요소에 매핑하는 것이 필요하다.

IIRA의 3계층 참조모델에서는 구성요소별 사용되는 IT 기술의 예시를 언급하고 있으며 3계층의 구성 도메인은 앞서 분석된 기능관점의 IIRA 참조모델의 도메인을 기반으로 하고 있으므로 이를 활용하여 매핑할 수 있다. IIRA의 3계층 참조모델의 언급된 IT 기술을 간략 정리하고 RAMI 4.0의 계층구조를 매핑하면 아래 Fig.6.와 같다. IIRA 3계층 참조모델의 사용기술들과 스마트공장추진단의 구성 예시에서 식별된 네트워크 기술을 추가하여 정리하면 아래와 같다.

3.2.1 근접 네트워크(Proximity Network)

필드 디바이스와 제어 디바이스의 근접 네트워크는 센서, 액추에이터와 같은 필드 디바이스와 PLC(Programmable Logic Controller), 컨트롤러 등의 제어 디바이스가 포함된다. 이 네트워크는 유선/무선 통신의 사용이 가능하며, Mesh Network topology, Hub and Spoke Topology 혹은 버스 형태의 토폴로지를 따르도록

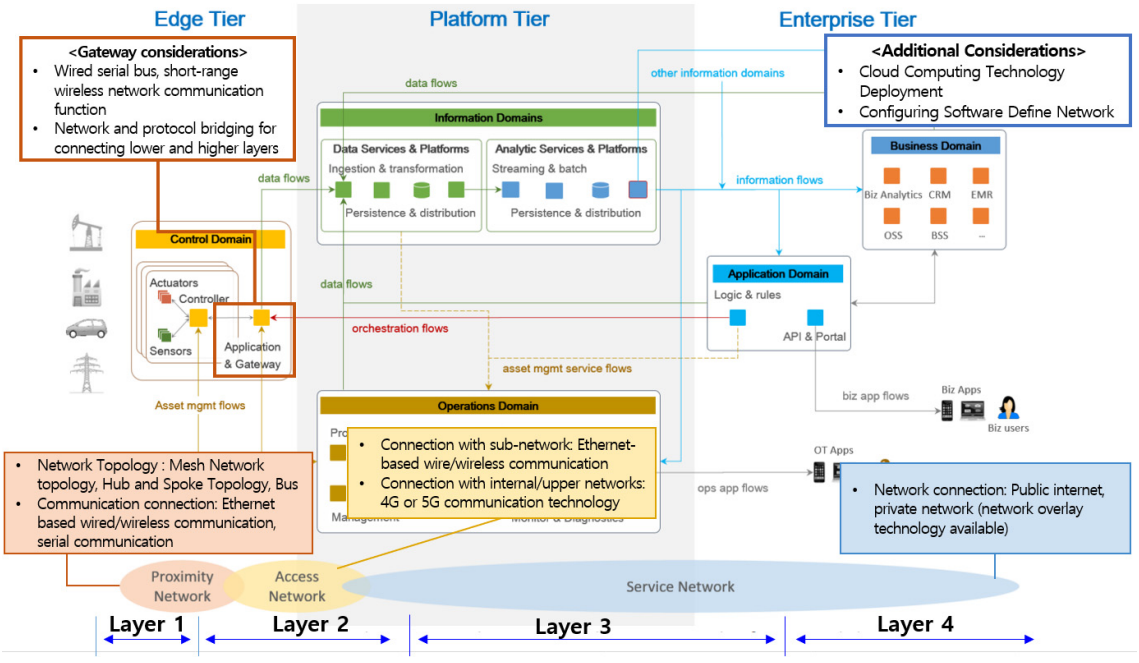

Fig. 6. Mapping a three-tier architecture of IIRA to RAMI 4.0

구성할 수 있다. 일부 센서와 액추에이터는 직접적인 통신 기능이 없을 수 있다. 이 경우에는 PLC 장치나 기타 전용 컨트롤러를 이용하여 상위 계층과 통신하도록 네트워크를 구성할 수 있다. 통신은 RS-232C와 Ethernet 그리고 무선 네트워크의 사용 가능하다고 언급되어 있지만, 이에 국한되지는 않는다. RS-232C 통신의 경우 시리얼 기반의 통신으로 확장성이 매우 떨어지며 RAMI 4.0과 IIRA에서는 통신 가능한 디바이스를 해당 참조모델에서 사용될 수 있는 기기라고 언급하고 있는데, 이를 고려할 때 위와 같은 시리얼 통신은 다수의 디바이스들과 통신이 어렵기 때문에 향후 IP 기반 통신으로 대체될 것으로 사료된다.

3.2.2 접근 네트워크(Access Network)

우선 계층적 구조 관점에서 Station과 Work Centers로 이루어지는 접근 네트워크 계층은 엔터프라이즈 계층에서 가장 하위 단인 필드 디바이스와 제어 디바이스로 접근하기 위해 데이터가 통과하는 영역이다. 이 영역에서는 내부 자산(기기)관리와 간단한 데이터 분석을 통한 제어를 수행한다. IIRA에 따르면 이 계층에서는 공용 네트워크, 회사 네트워크 모두 사용이 가능하며, 4G 혹은 5G 기술이 여기에 적용되어 활용될 수 있다. 참조문서에서는 MES(Manufacturing Execution System)와 HMI(Human Machine Interface)는 하위 계층과의 통신이 가능해야 한다는 요구사항이 존재하여 하위 계층과의 통신에는 앞서 식별한 Ethernet 기반 유선통신 혹은 무선 통신이 사용될 수 있고, 계층 내 통신 혹은 상위 계층과의 통신에는 4G 혹은 5G 등의 기술이 사용될 수 있을 것으로 판단된다.

3.2.3 서비스 네트워크(Service Network)

엔터프라이즈 네트워크로 구성되는 서비스 네트워크는 엔터프라이즈 네트워크와 그 하위 계층의 연결을 담당한다. 이 경우 공용 인터넷이나 공용 인터넷에 네트워크 오버레이 기술을 활용한 사설망(Private Network)이 활용될 수 있다. 이 외의 프로토콜 등의 제약사항은 세 참조모델 모두 존재하지 않았다.

3.2.4 빅데이터 분석 기술

RAMI 4.0, IIRA, 스마트공장추진단 모델에서 공통으로 이야기하고 있는 다양한 센서에서 획득한 데이터를 토대로 분석하여 최적의 운영을 도모하는 기능을 수행하기 위해서는 빅데이터 분석 기능이 필수적이다.

3.2.5 클라우드 컴퓨팅 기술

클라우드 컴퓨팅 기술은 필드 디바이스, 컨트롤 디바이스와 연결할 경우 부족한 IIoT 기기들의 컴퓨팅 파워를 보조해 줄 수 있는 좋은 수단이고, Station 혹은 엔터프라이즈 네트워크와 연결할 경우 다양한 공장의 통합 관리를 도모할 수 있는 뛰어난 기술이다. 실제 스마트팩토리 관련 산업계와 학계의 많은 전문가들은 클라우드를 활용하여 스마트팩토리의 효율성 증가를 기대하고 있고, RAMI 4.0, IIRA, 스마트공장추진단 모델에서도 실제 구현에서 고려될 수 있는 기술로 언급되고 있다.

3.2.6 스마트팩토리 웹 기술

스마트팩토리 웹 기술은 지역적으로 떨어져 있거나 서로 다른 인프라 환경을 가진 공장들을 연결해 공장 간 생산 자원을 효율적으로 운영할 수 있게 해주고 주문 맞춤형으로 유연한 생산을 할 수 있도록 해준다. 이러한 스마트팩토리 웹 중 미국 IIC와 PI4.0의 규격을 동시에 만족하는 KETI(Korea Electronics Technology Institute)의 스마트팩토리 웹 아키텍처에 따르면 스마트팩토리 웹은 서버와 연동되어 데이터를 수집하는 SFW hub와 디바이스 생성, 삭제, 연결, 조회와 같은 디바이스 기본 관리 기능을 제공하는 Factory-Thing Device Management 그리고 데이터를 수집, 저장하고, 애플리케이션에 전달해주는 역할을 담당하는 Factory-Thing Data Management & Analysis 등으로 구성된다[16].

IV. 제안하는 스마트팩토리 아키텍처

스마트팩토리 참조모델들의 구성요소, 구조 그리고 사용기술 분석을 통해 기존 공장자동화 단계에서 스마트팩토리로 발전함에 따라 변경되는 사항들을 중

점으로 빅데이터, 클라우드, 인공지능, 스마트팩토리 웹 서비스 등 스마트팩토리 고려사항으로 언급된 기술을 간략히 접목하여 스마트팩토리 아키텍처를 아래 Fig.7.과 같이 도출하였다. 빅데이터, 클라우드, 인공지능, 스마트팩토리 웹 등의 기술은 아직 각 참조 모델에서 고려할 수 있는 사항으로 언급만 되고 있고, 반드시 설치해야 하는 요소가 아니기 때문에 가장 기본이 되는 구조를 기본 아키텍처에 연동하여 나타내었다.

이를 기반으로 스마트팩토리의 주요특징을 살펴보면 웹/클라우드/AI 기반 서비스 증가, Level 4 및 외부와 Level 1간의 직접 통신 증가, IP 기반 통신 증가, 무선 통신 증가, 외부 공장 연결 증가가 기존 공장과 차별화되는 점이며 각 변경사항에 대한 상세 내용은 아래와 같다.

4.1 웹/클라우드/AI 기반 융합서비스 도입

스마트팩토리의 각 기기들이 IP 통신을 수행하고 외부와의 연결이 증가하면서 더욱 효율적으로 운영하기 위해 각 정보를 스마트팩토리 웹(SFW, Smart Factory Web)을 이용하여 지역적으로 떨어져 있거나 서로 다른 인프라 환경을 가진 공장들을 연결해 공장 간 생산 자원을 효율적으로 운영하도록 스마트팩토리는 변화되고 있다. 이에 따른 웹 서비스가 크게 증가할 것으로 예상하며, 이 외에도 구성하는 스마트 센서 등 IIoT 기기들은 웹 기반의 인터페이스를 제공하기 때문에 스마트팩토리와 관련된 전체 웹 서비스들은 기존보다 증가하게 될 것으로 사료된다.

4.2 스마트팩토리 기기 간 접점 증가

외부와 Level 4의 통신, Level 4와 Level 1의 통신 그리고 스마트팩토리와 클라우드 통신 등 스마트팩토리 기기 간 접점이 많이 증가한다. 예를 들면 빅데이터 분석과 인공지능 기술의 도입으로 인해 더욱 효율적으로 제조 공정을 변경하는 스마트팩토리의 특성상 Level 4 설비와 Level 1 설비가 직접적인 통신이 수행된다. Level 1 설비의 경우 기존 단순 데이터 수집만 수행하던 센서에서 벗어나 일부 제어 기능까지 포함된 스마트 센서로 발전하고, Level 4에서는 각 계층에서 수집된 빅데이터를 분석할 수 있게 되었다. 이에 따라 기존보다 더욱 효율적인 공정 방안을 찾을 수 있게 되고, 생산관리시스템을 통해 공정방안을 실시간으로 하위 Level 1 기기들에게 전달하여 전체 공정의 효율성을 높이게 된다. 따라서 기존에는 IT와 OT 간의 엄격한 망 분리가 이루어졌지만, 스마트팩토리에서는 그 경계가 점차 흐려지고, Level 4와 Level 1간의 통신이 발생할 것으로 사료된다.

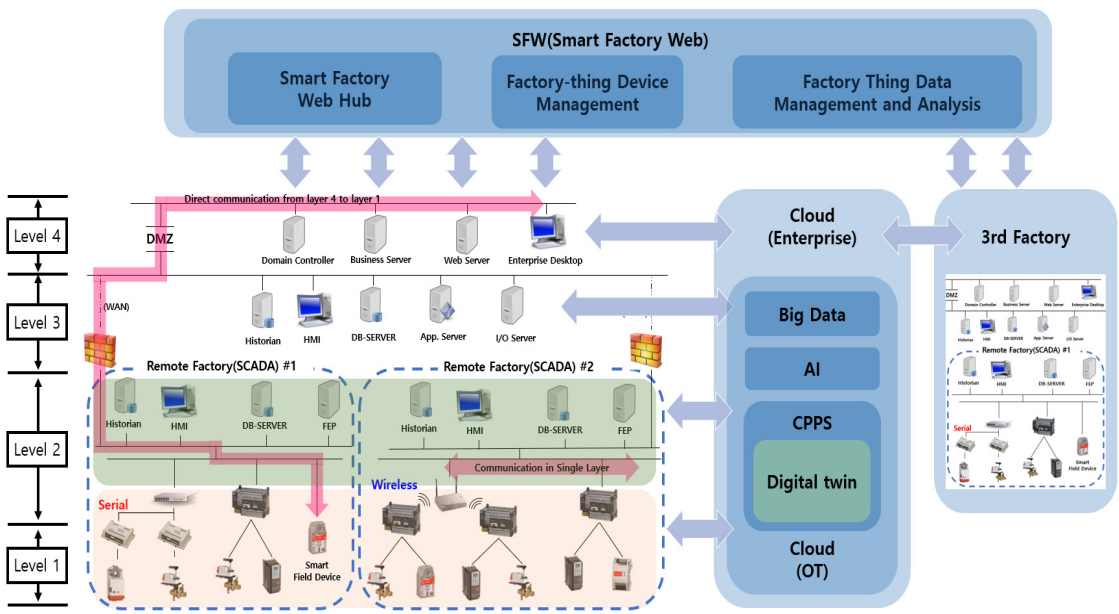

Fig. 7. Smartfactory Architecture based on reference models

4.3 TCP/IP와 같은 표준프로토콜 사용 증가

기존 통신 흐름과 달리 Level 4 기기에서 Level 1 기기로 통신이 직접 전달되는 스마트팩토리의 구조적인 특징상 Level 1 기기들이 기존 시리얼 기반의 통신을 벗어나 IP 기반의 통신으로 발전할 것으로 사료된다. 공장자동화 설비에서는 Level 1 기기들은 특정 Level 2 기기와의 통신만이 중요시되었기 때문에 IP 통신의 도입이 불필요하였으나, 다수의 노드들과 통신을 하게 되는 스마트팩토리에서는 시리얼 통신으로 모두 연결하는 것은 불가능하다. 따라서 스마트센서 등 IIoT 기기들의 보급과 함께 IP 기반의 통신이 증가할 것으로 예상된다.

4.4 Industrial IoT 기기 증가

스마트 센서들의 도입으로 인해 Level 1 기기들의 계층 내 통신이 증가하게 된다. 이에 따라 모든 Level 1 기기들의 통신 형태도 변화한다. 기존 시리얼 기반 통신 구조는 무선 통신을 적극적으로 활용하여 물리적으로 케이블 연결이 어려운 위치에서도 스마트 센서들이 계측 및 제어를 담당하며, 시리얼 통신을 위해 필요한 케이블의 양이 줄어들어 경제적이다. 따라서 스마트팩토리는 무선 통신이 크게 증가할 것으로 사료된다.

4.5 스마트팩토리 간 연계 증가

단일 공장 내부에서 제품 생산의 자동화만을 수행하던 기존 공장과는 달리 스마트팩토리는 제품의 계획부터 고객에게 배송하는 것까지 전체 공정을 자동화한다. 제품 생산에 필요한 재료를 주문하는 등의 임무를 수행하기 위해 공장 간 통신 트래픽이 발생하며, 클라우드 기술이 공장에 도입되고, 스마트팩토리 웹 기술의 도입으로 인해 공장간 통신의 양은 증가할 것으로 예상된다.

V. 스마트팩토리 보안위협 및 보안 요구사항

4장에서 제시한 스마트팩토리 아키텍처는 RAMI 4.0의 구성요소와 구조를 바탕으로 하고 있기 때문에 공장 내부 영역의 경우 기존 공장자동화 시스템과 공통된 부분이 많다. 따라서 스마트팩토리 내부 영역의 보안 위협의 경우 기존 제어시스템에 대한 보안 위협을 계승하고 있으며 해당 보안 위협에 관한 연구는 다수 선행되어 있기 때문에 본 장에서는 앞서 선별된 스마트팩토리의 주요특징에 초점을 맞추어 발생 가능한 보안 위협을 식별하였으며 이를 토대로 필요한 보안 요구사항을 간략히 정리하였다.

5.1 융합서비스 도입으로 인한 보안위협

스마트팩토리의 차별화되는 기술 및 서비스는 앞서 식별한 클라우드, 빅데이터, 인공지능(AI), 스마트팩토리 웹으로 총 4가지이다. 이 중 빅데이터 및 인공지능의 경우 클라우드 플랫폼 위에서 동작할 것으로 예상되기 때문에 보안 위협분석에는 클라우드 보안 위협과 스마트팩토리 웹과 관련된 웹 애플리케이션 보안 위협에 대해 분석하였다. 클라우드 보안 위협분석을 위해 CSA(Cloud Security Alliance) 보안문건[14]을 활용하였으며, 웹 애플리케이션 보안 위협분석에는 OWASP(Open Web Application Security Project) 보안자료[15]를 활용하여 도출된 스마트팩토리 아키텍처에서 발생 가능한 보안 위협만을 식별하였다.

5.2 기기 간 접점 증가로 인한 보안위협

스마트팩토리에서는 제조 및 생산에 직접 관여하는 Level 1 장치와의 통신이 중요하나 이러한 하위 계층 장치의 경우 낮은 하드웨어 성능을 가지고 있어 인증, 암호화, 부인방지 등의 보안 기능이 없는 경우가 많다. 따라서 하위 계층과의 직접 통신이 이루어질 경우 부적절한 사용자와 기기가 권한을 부여받을 수 있으며 데이터의 위변조를 통해 잘못된 정보를 전달하여 잘못된 제품을 생산하고 더 나아가 공장운영을 마비시킬 가능성이 존재한다.

5.3 표준프로토콜 사용 증가로 인한 보안위협

다양한 사물과 연결되어 통신이 필요한 스마트팩토리에서는 기존 시리얼 기반의 통신이 아닌 IP 기반 통신이 요구되어 진다. 이러한 IP 기반 통신은 기존 시리얼 기반의 통신과는 다르게 직접 연결되어 있지 않더라도 접근이 쉽기 때문에 적절한 보안 기능이 없는 경우 공격자가 통신 데이터를 획득하거나 위변조할 가능성이 존재한다.

5.4 IIoT 기기 증가로 인한 보안위협

IIC의 보안 문서[16]에서는 별도의 보안 위협분석을 하고 있지 않으나 OWASP IoT Attack Vector와 STRIDE Threat Mode에 대해서 언급하고 있다. OWASP의 IoT Attack Vector는 IoT 기기의 취약성을 다루고 있으나, 스마트팩토리는 IIoT 기기들로 구성될 것으로 IIC는 예상하고 있기 때문에 스마트팩토리에도 이를 활용하였다. STRIDE는 컴퓨터 보안 위협을 식별하기 위해 Microsoft 사가 개발한 위협 모델로 Risk를 모델링하고, IT 환경의 위협평가를 수행하기 위해 사용된다. 스마트팩토리에 사용되는 IIoT 기기들의 IoT 위협 요소를 확장하며, 총 6개의 위협 분류를 제공한다. 이 위협 분류들은 시스템 혹은 데이터의 기밀성, 무결성, 가용성을 손상시키고, 정상 동작을 방해하는 요소들로 공격자는 이러한 위협을 이용하여 공격을 수행할 수 있다. 이 중 도출된 스마트팩토리 아키텍처에서 발생 가능한 보안 위협만을 식별하였다.

5.5 스마트팩토리 간 연계 증가로 인한 보안 위협

공장간 연계는 직접적으로 금전적 피해와 연결될 수 있다. 기존 공장자동화 단계에서는 제품 생산 과정에서 사용되는 부품의 변경이 필요할 경우 해당 업체 직원과의 토의를 거쳐 변경이 이루어졌지만, 고도화된 스마트팩토리에서는 이 전체 과정이 자동화될 수 있다. 위와 같은 고도화된 스마트팩토리에서 통신 내용을 위/변조할 경우 조립이 불가능한 부품이 생산되어 큰 경제적인 피해를 야기할 수 있다. 그리고 해당 내용을 외부에서 획득 가능할 경우 지적재산권에도 큰 피해를 야기할 수 있다.

스마트팩토리의 5가지의 주요특징에 대해 식별된 보안위협을 최종적으로 Table 3.에 정리하였으며 보안위협에 대응하기 위한 보안 요구사항을 Table 4.에 정리하였다.

VI. 결 론

본 논문에서는 국내외 주요 스마트팩토리 참조모델을 분석을 통해 스마트팩토리의 주요 특성을 반영할 수 있는 시스템 아키텍처를 도출하였다. 이후, 스마트팩토리의 주요기술과 주요 특성을 바탕으로 보안 문건 분석을 통해 스마트팩토리의 보안 위협을 식별하고 해당 보안 위협에 대응하기 위한 보안 요구사항을 정리하여 제시하였다.

하지만 실제 구축하는 기기들에 따라 본 논문에 언급된 위협 및 요구사항이 달라질 수 있기 때문에 향후 실제 고도화된 스마트팩토리 도입 시 본 논문을 기반으로 실제 사용되는 기기들의 특성을 고려한 보안연구가 추가로 필요할 것으로 판단된다.

References

[1] Korea Smart Factory Foundation, “Case Study of Companies Participating in Korea Smart Factory Support Project,” Korea Smart Factory Foundation & Ministry of SMEs and Startups, Sept. 2017, https://www.smart-factory.kr/datum/popup/datumDetail.do?dboardNo=165, Accessed Mar. 19, 2019

[2] Sangdong Lee, “ The global promotion trend and Korea standardization counter strategies of the smart factory,” Korean standards Association, Jul. 2015, http://www.kosmia.or.kr/inc/downboard.php?seq=58, Accessed Mar. 19, 2019

[3] Dongpyeong Shin and Yunna Tang, “An Analysis of Smart Factory Policy and Its Implications for Leading Manufacturing Innovation,” Korea Institute of S&T Evaluation and Planning, Aug. 2018, https://www.kistep.re.kr/c3/sub3.jsp?brdType=R&bbIdx=12207, Accessed Mar. 19, 2019

[4] N. Falliere, L. O. Murchu and E. Chien, “W32.Stuxnet Dossier,” Analysis report, Symantec Corporation, Feb. 2011

[5] K. Lab. “The DUQU 2.0 - technical details,” Analysis report, Kaspersky Lab, Jun. 2015

[6] E-ISAC, “Analysis of the Cyber Attack on the Ukrainian Power Grid,” Analysis report, SANS, Mar. 2016

[7] A. Cherepanov, "Win32/industroyer - a new threat for industrial control systems," Analysis report, ESET, Jun. 2017
[8] Dragos, "TRISIS Malware Analysis of Safety System Targeted Malware," Analysis report, Dragos Corporation, Dec. 2017
[9] Jongwon Kwon, Taeseung Song and Wonseo Cho. "Development Trend of Smart Factory Reference Model for Manufacturing Innovation," The Institute of Electronics and Information Engineers, 43(6), pp. 51-61, Jun. 2016
[10] Shi-Wan Lin, B. Miller, J. Durand, G. Bleakley, A. Chigani, R. Martin, B. Murphy and M. Crawford, "The Industrial Internet of Things Volume G1- Reference Architecture," IIC Consortium, Jan. 2017
[11] Korea Smart Factory Foundation, "Smart Factory Reference Model - focused on Industry(Ver 3.1)," Korea Smart Factory Foundation & Ministry of Trade, Industry and Energy, 2017, https://www.smart-factory.kr/datum/dataWarehouse.do, Accessed Mar. 19, 2019
[12] Stouffer, Keith, Joe Falco, and Karen Scarfone. "Guide to industrial control systems (ICS) security Rev.2," National Institute of Standards and Technology, May. 2015
[13] Reference Architecture Model Industrie 4.0 (RAMI4.0), DIN S P E C 91345:2016-04, Apr. 2016
[14] R. Mogull, J. Arien, F. Gilbert, A. Lane. D. Mortman, G. Peterson and M. Rothman, "Security Guidance For Critical Areas of Focus in Cloud Computing," Cloud Security Alliance, Jul. 2017
[15] OWASP, "The Ten Most Critical Web Application Security Risks," The Open Web Application Security Project Foundation, Nov. 2017
[16] S. Schrecker, H. Soroush, J. Molina, M.Buchheit, JP LeBlanc, R. Marthin, F. Hirsch and A. Ginter, "Industrial Internet of Things Volume G4: Security Framework," Industrial Internet Consortium, Sept. 2016

Table 3. Potential SmartFactory Security Threats

Smartfactory feature	Identifier	Security Threat
Introducing Convergence Services	SF-F1-T1	If authentication and access control is not performed in the Smart Factory Web, Unauthorized users can obtain administrator privileges and cause harm to factories.
	SF-F1-T2	In the absence of non-repudiation, some customers may not be able to order products and pay for them, resulting in economic damage.
	SF-F1-T3	The use of the Smart Factory Web will also affect existing Web application vulnerabilities.
Increased contact between smart factory devices	SF-F2-T1	Low hardware performance of Level 1 device may prevent authentication between devices.
	SF-F2-T2	If there is no authentication function for availability, there is a threat that improper authorization will be granted because access control based on authentication is not performed.
	SF-F2-T3	Level 1 devices can often be controlled and managed through remote access at Level 4. This can lead to increased contact with the outside world and can be exploited as a new attack path.
	SF-F2-T4	If weak encryption methods are used due to low hardware performance problems of level 1 device, there is a threat of communication data interception and manipulation.
	SF-F2-T5	Because of the low hardware performance of the Level 1 device and the high availability of the system, there is a possibility that the non-repudiation function is not performed or the weak repudiation function is performed.
Increased use of open protocols such as TCP/IP	SF-F3-T1	Compared to serial communication, attacker has easy access to device, so there is threat of communication data interception and manipulation
	SF-F3-T2	Because IP-based communications are capable of various DoS attacks, there is a threat of service unavailability
	SF-F3-T3	Unlike serial communications, all internal nodes in the network can communicate, which can lead to communication with inappropriate targets.
Increased use of Industrial IoT	SF-F4-T1	Because wireless communications can communicate with all devices within a given area, it can lead to communication with inappropriate devices.
	SF-F4-T2	Because it is easier for an attacker to approach than wire communication, there is a threat of communication data interception and manipulation.
	SF-F4-T3	Since wireless communications are capable of various DoS attacks, there is a threat of service unavailability.
Increased connectivity between smart factory	SF-F5-T1	Unlike existing plants, there are a variety of user in smart factory. So failure to control access under certification may result in problems with improper administrator privileges.
	SF-F5-T2	If there is no non-repudiation function, it can cause economic damage because the product is ordered from another factory and then not paying for them.
	SF-F5-T3	Because it is easy for an attacker to approach through external communication, there is a threat of communication data interception and manipulation.

Table 4. SmartFactory Security requirement against potential threats

Smartfactory feature	Identifier	Security requirement
Introducing Convergence Services	SF-F1-R1	Smart Factory requires authentication and access control because there are a variety of users and each user must be given different privileges.
	SF-F1-R2	Smart Factory require to provide non-repudiation function because it needs confirmation when ordering products through the Web.
	SF-F1-R3	Smart Factory require to monitor and respond to known vulnerabilities in Web applications because the use of Smart Factory Web also affects existing Web application vulnerabilities.
Increased contact between smart factory devices	SF-F2-R1	Smart Factory require have proper authentication and access control because it is possible to directly access the OT network from the external network.
	SF-F2-R2	Smart Factory require non-repudiation because it is necessary to confirm the responsible person when controlling the internal device from external network.
	SF-F2-R3	Smart Factory require communication confidentiality and integrity because smart factory network can be exposed to the attacker from the outside.
	SF-F2-R4	Smart Factory require traffic monitoring and external access management function because it can be abused to the traffic from external network to internal network of smart factory for the purpose of maintenance.
Increased use of open protocols such as TCP/IP	SF-F3-R1	Smart Factory require a way to guarantee confidentiality and integrity of communication because the attacker can easily acquire and manipulate IP communication than the serial communication.
	SF-F3-R2	Smart Factory require traffic monitoring and ensure communication availability because the DoS attacks can occur against IP communication facilities.
	SF-F3-R3	Smart Factory requires proper authentication and access control because IP based communication can communicate with connected to the network.
Increased use of Industrial IoT	SF-F4-R1	Smart Factory require authentication, access control and wireless access management because wireless communication can communicate with all devices within certain area.
	SF-F4-R2	Smart Factory require confidentiality and integrity of communication because wireless communication is easy for an attacker to acquire and manipulate data.
	SF-F4-R3	Smart Factory require communication availability because there are many attacks that affect the availability of wireless communication such as Jamming, Tempering, Collision, etc.
Increased connectivity between smart factory	SF-F5-R1	Smart Factory require proper authentication and access control because other factory can direct access to the internal area of the factory.
	SF-F5-R2	Smart Factory require non-repudiation functions because it is necessary to confirm the responsible person when ordering products from other factories.
	SF-F5-R3	Smart Factory require communication confidentiality and integrity because the communication between smart factory can be exposed to attackers.

〈저자소개〉

김 현 진 (HyunJin Kim) 학생회원
2014년 8월: 아주대학교 정보통신대학 정보컴퓨터공학사
2016년 8월: 아주대학교 대학원 컴퓨터공학 석사
2018년~현재: 아주대학교 대학원 컴퓨터공학과 박사과정
〈관심분야〉 산업제어시스템 보안, 스마트팩토리 보안, 차량통신 보안, 네트워크 보안

김 성 진 (SungJin Kim) 학생회원
2014년 2월: 아주대학교 정보 및 컴퓨터공학부 공학사
2014년 3월~현재: 아주대학교 컴퓨터공학과 석박사통합과정
〈관심분야〉 스마트그리드 보안, 디지털 포렌식, 네트워크 보안

김 예 솔 (Yesol Kim) 정회원
2014년 2월: 단국대학교 컴퓨터학부 졸업
2015년 8월: 단국대학교 컴퓨터학과 석사
2016년 3월~현재: ETRI 부설연구소 연구원
〈관심분야〉 정보보호, 제어시스템 보안

김 신 규 (Sin-Kyu Kim) 정회원
2000년 2월: 연세대학교 기계전자공학부 졸업
2002년 2월: 연세대학교 컴퓨터과학과 석사
2014년 2월: 연세대학교 컴퓨터과학과 박사
2003년 12월~현재: ETRI 부설연구소 선임연구원/팀장
〈관심분야〉 기반시설보안, 스마트그리드 보안, 취약점 분석, CPS 보안

손 태 식 (Taeshik Shon) 종신회원
2000년: 아주대학교 정보및컴퓨터공학부 졸업(학사)
2002년: 아주대학교 정보통신전문대학원 졸업(석사)
2005년: 고려대학교 정보보호대학원 졸업(박사)
2004년~2005년: University of Minnesota 방문연구원
2005년~2011년: 삼성전자 통신·DMC 연구소 책임연구원
2017년~2018년: Illinois Institute of Technology 방문교수
2011년~현재: 아주대학교 정보통신대학 사이버보안학과 교수
〈관심분야〉 ICS/SCADA, DFIR, Anomaly Detection