Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.6, Dec. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.6.1467

STRIDE 위협 모델링에 기반한 스마트팩토리 보안 요구사항 도출*

박 은 주,† 김 승 주‡
고려대학교 정보보호대학원

Derivation of Security Requirements of Smart Factory Based on STRIDE Threat Modeling*

Eun-ju Park,† Seung-joo Kim‡
Center for Information Security Technologies(CIST), Korea University

요 약

최근 4차 산업혁명에 대한 관심이 증가하고 있다. 그 중 제조업 분야에서는 사이버 물리 시스템(CPS) 기술을 기반으로 제조의 모든 단계를 자동화, 지능화 시킨 스마트팩토리 도입이 확산되고 있는 추세이다. 스마트팩토리는 그 복잡도(Complexity)와 불확실성(Uncertainty)이 크기 때문에 예상치 못한 문제가 발생할 가능성이 높고 이는 제조 공정 중단이나 오작동, 기업의 중요 정보 유출로 이어질 수 있다. 스마트팩토리에 대한 위협을 분석하여 체계적인 관리를 수행할 필요성이 강조되고 있지만 아직 국내에서는 연구가 부족한 상황이다. 따라서 본 논문에서는 스마트팩토리의 전반적인 생산 공정 절차를 대상으로 Data Flow Diagram, STRIDE 위협 모델링 기법을 이용하여 체계적으로 위협을 식별한다. 그리고 Attack Tree를 이용해 위험을 분석하고 최종적으로 체크리스트를 도출한다. 도출된 체크리스트는 향후 스마트팩토리의 안전성 검사 및 보안 가이드라인 제작에 활용 가능한 정량적 데이터를 제시한다.

ABSTRACT

Recently, Interests on The Fourth Industrial Revolution has been increased. In the manufacturing sector, the introduction of Smart Factory, which automates and intelligent all stages of manufacturing based on Cyber Physical System (CPS) technology, is spreading. The complexity and uncertainty of smart factories are likely to cause unexpected problems, which can lead to manufacturing process interruptions, malfunctions, and leakage of important information to the enterprise. It is emphasized that there is a need to perform systematic management by analyzing the threats to the Smart Factory. Therefore, this paper systematically identifies the threats using the STRIDE threat modeling technique using the data flow diagram of the overall production process procedure of Smart Factory. Then, using the Attack Tree, we analyze the risks and ultimately derive a checklist. The checklist provides quantitative data that can be used for future safety verification and security guideline production of Smart Factory.

Keywords: Cyber Physical Systems, Smart Factory, The Fourth Industrial Revolution, Threat Modeling, Security Requirements

Received(11. 13. 2017), Modified(12. 15. 2017), Accepted(12. 15. 2017)

* 본 연구는 미래창조과학부 및 한국인터넷진흥원의 "고용계약형 정보보호 석사과정 지원사업"의 연구결과로 수행되었음 (과제번호 H2101-17-1001)

† 주저자, ejpark93@korea.ac.kr
‡ 교신저자, skim71@korea.ac.kr(Corresponding author)

I. 서 론

최근 세계 경제가 저성장 국면에 진입하면서 사물인터넷(IoT), 인공지능, 사이버 물리 시스템(Cyber Physical System, CPS) 등의 신기술을 기반으로 삼는 4차 산업혁명에 대한 관심이 증가하고 있다. E. A Lee는 사이버 물리 시스템을 연산(Computation)과 물리적 프로세스(Physical processes)을 통합시킨 시스템으로, 임베디드 컴퓨터와 네트워크 모니터링, 물리적 프로세스의 제어로 구성되어 있는 시스템이라고 정의한다. 그리고 물리적 프로세스와 연산은 피드백 루프(Feedback loop)를 통해 상호간에 영향을 미친다고 설명 한다[1]. 사이버 물리 시스템은 센서(Sensor), 작동기(Actuator), 제어기(Control processing unit), 통신 장비와 같은 요소들로 구성되어 있고[2] 현재 스마트 그리드, 의료 및 헬스케어, 교통 시스템, 스마트 홈, 감시제어(Supervisory Control and Data Acquisition, SCADA), 자율주행 자동차 등 다양한 분야에서 관련 연구가 활발히 진행되고 있다. 특히 제조업 분야에서는 시장의 변화를 빠르게 감지해 생산 전략에 반영시키는 능력이 요구되면서 사이버 물리 시스템을 도입한 스마트팩토리가 주목을 받고 있다. 독일의 경우 2012년에 '4차 산업혁명(Industry 4.0)'을 제시하고 자동화 설비 및 솔루션을 중심으로 자국 내 산업 경쟁력을 강화시키려는 노력을 하고 있으며 미국의 경우 2011년 '첨단 제조 파트너십(Advanced Manufacturing Partnership, AMP) 전략'과 2012년 '제조 방식 전략 계획'과 같은 제조업 부흥 정책을 발표해 스마트팩토리 도입을 추진하고 있다. 그 외에 일본에서도 2016년에 '4차 산업 혁명 선도 전략'을 제시하고 중국에서도 2015년에 발표된 '중국제조 2025'를 통해 제조업 경쟁력 강화를 지원하고 있고 국내에서는 2014년도에 '제조업 3.0'을 발표하고 2017년에 '4차 산업 혁명 위원회'를 출범시킴으로써 스마트팩토리 사업을 지원하고 있다[3]. 국내외적으로 스마트팩토리 도입이 증가하고 있을 뿐만 아니라 폐쇄적인 운영 방식을 지닌 기존의 제조 시스템과 차별적으로 다양한 기술과 환경이 통합된 스마트팩토리는 그 복잡도(Complexity)와 불확실성이(Uncertainty)이 크기 때문에 예상치 못한 문제가 발생할 가능성이 높음에도 불구하고 아직 위협 분석과 관련된 연구는 부족한 실정이다. 따라서 본 논문에서는 스마트팩토리의 현장 수준(Field Level)부터 관리자 수준(Management Level)까지 전반적인 생산 공정 절차를 대상으로 STRIDE 위협 분석 모델링을 통해 위협을 식별하고 최종적으로 스마트팩토리에 대한 보안 체크리스트를 도출하는 것을 목표로 한다.

본 논문의 2장에서는 사이버 물리 시스템 및 스마트팩토리와 관련된 연구 동향을 소개하고 스마트팩토리의 취약점에 대한 연구들을 소개한다. 3장에서는 스마트팩토리에 대한 개념과 서비스를 제공하는 업체에 대해 소개한다. 4장에서는 개념도를 토대로 데이터 흐름도를 도출하고 STRIDE 위협 모델링 기법을 적용하여 보안 위협 및 위험 분석을 수행한다. 분석된 위협에 따라 5장에서 보안 요구사항을 도출하고 마지막으로 6장에서 결론 및 향후 연구 방향을 제시한다.

II. 관련 연구

2.1 표준화 작업 현황

2014년에 사이버 물리 시스템 공공 작업 그룹(Cyber-Physical Systems Public Working Group, CPS PWG)이 미국표준기술연구소(National Institute of Standards and Technology, NIST)에 의해 구성 되었고 2016년에 워킹 그룹에서 사이버 물리 시스템 체계(Framework for Cyber Physical Systems)에 대한 문서를 배포하였다[4]. 그리고 이 문서를 토대로 미국표준기술연구소(NIST)에서 사이버 물리 시스템에 대한 표준 문서를 발표하였다. 세 가지 문서는 각각 사이버 물리 시스템의 개요 및 체계에 대한 설명과 작업 그룹에서 작성한 보고서와 타이밍(Timing)에 대한 내용으로 구성되어 있다. 표준에 따르면 사이버 물리 시스템이란 물리적 프로세스와 연산 장치들이 상호작용을 하는 시스템으로 서로 밀접하게 연관되어 의료, 응급 상황, 교통 흐름 통제, 스마트 제조(Smart Manufacturing), 국방 산업, 에너지 공급 등 핵심적인 분야에 새로운 기능들을 제공한다.[5] 사이버 물리 시스템이 주는 이점들을 활용하기 위해서는 각 요소들과 시스템 간의 상호운용성(Interoperability)이 보장되어야 한다. 특히 NIST SP 1500-202에서는 사이버 물리 시스템에서 요구되는 신뢰성, 사이버보안과 프라이버시 위험 및 위험관리 속성(Property)에 대해 작성되어있다

[6]. NIST SP 1500-203에서는 네트워크상에서 존재하는 위협과 대응책을 분석하였다[7].

미국표준연구소(NIST)에서 작성된 문서 중 NIST 800-82에서는 산업 제어 시스템 보안과 관련된 전반적인 내용이 기술되어 있다. 산업 제어 시스템 구성 요소들에 대한 설명과 함께 위협들에 대응하여 심층 방어(Defense in Depth, DiD)를 위한 보안 아키텍처를 소개한다. 보안 아키텍처의 구현을 위해 적용될 수 있는 정책적 가이드라인을 제시한다[8].

2.2 스마트팩토리 위협 관련 연구

제어 시스템은 핵심 사회 기반 시설에 광범위하게 사용되는 만큼 지속적인 연구가 진행되어왔다. Stamatis karnouskos는 핵심 사회 기반 시설을 파괴할 목적으로 만들어진 Stuxnet 웜에 대하여 소개한다[9]. E. Ciancamerla는 감시 제어 시스템에 대한 공격 시나리오를 제시하고 시뮬레이션을 수행한 결과를 보여준다[10]. Brian Meixell은 BlackHat 2013에서 감시 제어 시스템을 대상으로 공격 시나리오를 소개하고 이를 직접 시연하였다[11]. Ralf Spenneberg는 BlackHat 2016에서 PLC상에서 동작하는 바이러스를 구현하여 감염시키고 발견된 취약점에 대하여 발표하였다[12]. Joe Weiss는 2017년에 개최된 DefCon25에서 산업 제어 시스템의 입출력 시스템, 센서 등 현장 수준에서 발생할 수 있는 보안 문제에 대하여 소개하였다[13].

스마트팩토리에서 여러 장비들이 복합적으로 사용되는 만큼 다양한 통신 방식이 사용된다. 현장 수준에서 사용되는 장비들은 WirelessHART, Bluetooth 등의 무선 통신을 사용할 수 있으며 HART, AS-Interface, IO-Link와 같은 유선 통신도 사용 가능하다. 입출력 시스템과 제어 시스템 사이에서는 PROFIBUS, PROFINET과 같은 통신 방식이 사용되고, 관리자 수준에서는 IWLAN(Industrial Wireless LAN), Industrial Ethernet이 사용된다. 그리고 서로 다른 통신 방식들과 기기들을 통합하여 관리하기 위해 OPC UA라는 상호운용성 표준이 사용된다[14]. Slawomir Jasek은 BlackHat 2016에서 Bluetooth통신에서 중간자 공격을 할 수 있는 도구를 소개하였으며 실제로 일부 기기를 이용해 시연하였다[15]. lucas Apa는 BlackHat 2013에서 무선 통신 방식을 이용하는 감시 제어 시스템 장비의 암호 키 생성 및 분배 방식을 역공학을 이용해 분석하고 공격을 수행하여 이를 발표하였다[16]. H. Kim은 IP기반 무선 센서 네트워크를 이용하는 감시 제어 시스템의 취약점에 대해 정리하였다[17].

III. 스마트팩토리 개요

3.1 제조 자동화 모델

제조업 분야에서는 피라미드 형태의 공장 자동화 모델이 제조 프로세스를 설명하기 위해 사용되었다. 공장 자동화 모델은 생산 설비와 센서가 존재하는 Layer0, PLC가 존재하는 Layer1, SCADA가 존재하는 Layer2, MES가 존재하는 Layer3, ERP가 존재하는 Layer4의 총 5개 계층으로 나누어진다[18][19]. Layer0은 Field Level이라 불리기도 하며 제어 장치 및 솔루션이 존재하는 Layer1과 Layer2는 Control Level로 분류된다. 생산 및 자원에 대한 관리가 이루어지는 Layer3와 Layer4는 Management Level로 분류 된다. 생산 설비란 실제로 작업을 수행하는 로봇을 말하고 센서는 제품 및 생산 설비를 식별하거나 공장 내 환경 변화를 감지하여 데이터를 전송한다. PLC는 Layer2에서 승인된 생산 설비 작업 배정에 따라 프로그램을 수정하고 로봇에게 제어 명령어를 전송한다. SCADA는 HMI을 통해 생산 공정 절차를 감시하고 제어한다. MES는 제품을 생산하기 위한 일정을 계획하고 계획에 따라 작업을 배정 한다. ERP는 기업 내 생산, 재무, 회계, 물류, 영업 등 경영 활동과 관련된 모든 절차들을 통합 관리해주는 시스템이다.

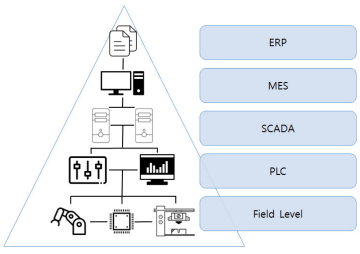

Fig. 1. Pyramid of Automation

3.2 스마트팩토리 유형 구분

국내에서는 스마트팩토리의 IT 기술의 적용과 그

활용 범위에 따라서 4가지 단계로 구분 짓는다[20]. 본 논문에서는 4가지 단계 중 고도화된 스마트팩토리를 분석 대상으로 삼으며, 이는 기초, 중간1, 중간2 단계에서 적용되는 기술들을 모두 포함하고 있다. 고도화된 스마트팩토리는 바코드, RFID 등의 기기를 사용하여 생산 기록을 관리하는 기초(Basic) 단계와 센서를 통해 실시간으로 생산 정보를 받아들여 생산설비를 관리하는 중간1(Middle1) 단계, PLC를 통해 시스템이 상호 연계되어 실시간으로 공장에 대한 자동 제어가 이루어지는 중간2(Middle2) 단계가 모두 구현된 동시에 지능화된 생산 설비들 간에 유선 및 무선 통신을 하며 실시간 주문 정보 및 로봇의 자율적인 판단에 따라 자동적으로 생산 작업이 수행된다.

Table. 1. Smart Factory Implementation Type

Category	Basic	Middle1	Middle2	Advanced
Application of ICT Technology	Few process automation	Production Management based on IT	Real-time integrated system	Customized flexible production based on IoT, CPS
Factory Operation	Production history and defective management	Collection and Management of real-time production Info.	Real-time automatic control of factory	Autonomous production by robots and systems
Automation equipment	Use of Bar code, RFID system	Production equipment management through sensors	Real-time system interlocking through PLC	Wired /Wireless communication between intelligent robots and systems

3.3 스마트팩토리 업체별 서비스 현황

현재 독일, 미국, 일본 등의 기업에서 스마트팩토리 시장을 선도하고 있으며 국내에서도 일부 스마트팩토리 솔루션을 제공하고 있다. Table. 2.는 스마트팩토리 제품 및 솔루션을 제공하는 대표적 해외 기업 A, B, C와 국내 기업 D의 서비스 범위를 3.1절에서 소개한 스마트팩토리 개념도의 각 계층에 따라 정리한 내용이다. 본 논문에서는 생산 설비, 감시제어 시스템, 생산 관리 시스템 등 거의 모든 공정 자동화 솔루션을 보유하고 있고 현재 전 세계 시장

Table. 2. Smart Factory Solution Provider

	A	B	C	D
ERP			ERP	
MES	MES		MES	MES
	Data Analyzing System			Data Analyzing System
SCADA	SCADA	SCADA		
	HMI	HMI		
	PCS			
PLC	Controller	Controller		
		Monitoring		
Field Level	I/O System	Robot		
	Motor	Machines		
	Identification System			
	Frequency Converter			
	Power Supply			

점유율 1위를 차지하고 있는 A사의 제품 설명서를 토대로 위협 분석을 진행한다.

IV. STRIDE 위협 모델링

4.1 가정

본 논문에서는 스마트팩토리 전체 시스템을 대상으로 STRIDE 위협 분석을 실시한다. 단, 각각의 외부 객체들이 상호간에 의사소통을 하는 경우는 분석에 포함시키지 않는다. 예를 들어 고객이 직접 주문을 넣지 못하는 상황일 경우 운영자와의 직접적인 소통을 통해 주문을 넣을 수 있고 운영자는 공장 설비의 오류나 문제가 발생했을 시에 관리자에게 직접 보고를 할 수 있다. 또한 관리자는 운영자에게 직접 설비 제어 또는 수리를 지시할 수 있다고 가정한다. MES 기능 중 품질 관리의 경우에도 사람이 직접 제품에 대한 표본을 추출하여 결과 보고 및 지시가 이루어진다고 가정하여 분석에 포함시키지 않는다.

4.2 데이터 흐름도(Data Flow Diagram)

4.2에서는 스마트팩토리의 데이터 흐름도를 도출한다. 데이터 흐름도는 그래픽을 이용하여 시스템에서 각 프로세스를 따라 흐르면서 변화하는 모습을 나타낸다. Table. 3.은 데이터 흐름도의 구성요소를 나타낸다.

Table. 3. Components of Data Flow Diagram

Element	Description	Shape
External Entity	External Entity generates inputs of data and consume outputs	External Entity
Data Store	Data stores store data temporarily or permanently	Data Store
Process	Process get inputs of data and generates outputs. Forms of data changes with this process	Process
Data Flow	Data Flow indicates movement of data between the external entity, data store and process	
Trust Boundary	Trust boundary indicates changes of privilege levels	Trust Boundary

데이터 흐름도는 일반적으로 Level0(Context Diagram)를 포함하여 보다 구체화 시킨 Level1, Level2까지 도출한다. Fig. 2.는 스마트팩토리를 추상화 시킨 Context Diagram이다.

Fig. 3.은 Context Diagram을 보다 구체화

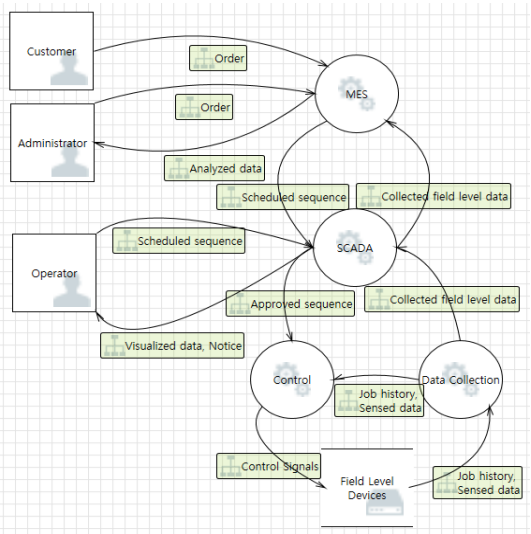

Fig. 2. Level0 DFD for Smart Factory

시킨 데이터 흐름도 Level1을 나타낸다.

Customer와 Administrator는 제품에 대한 주문을 넣을 수 있고 관리자는 MES를 통해 생산 실적 관리, 물류 관리 및 공장 내부 환경 관리 등 생산

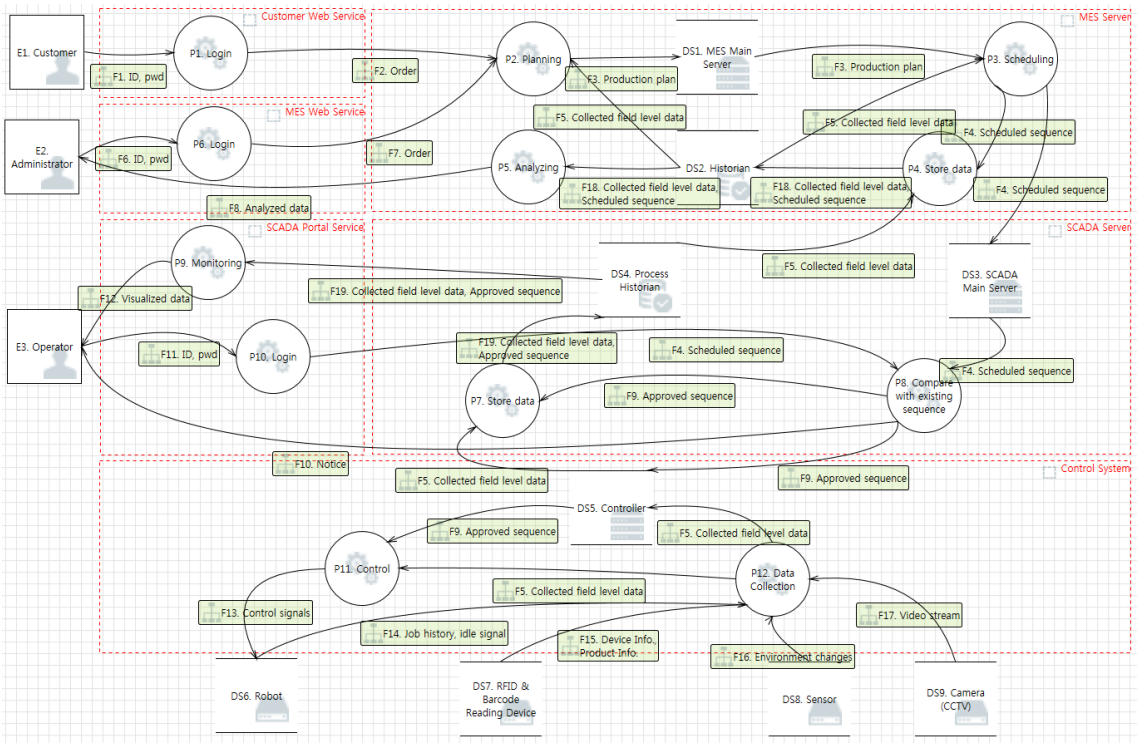

Fig. 3. Level1 DFD for Smart Factory

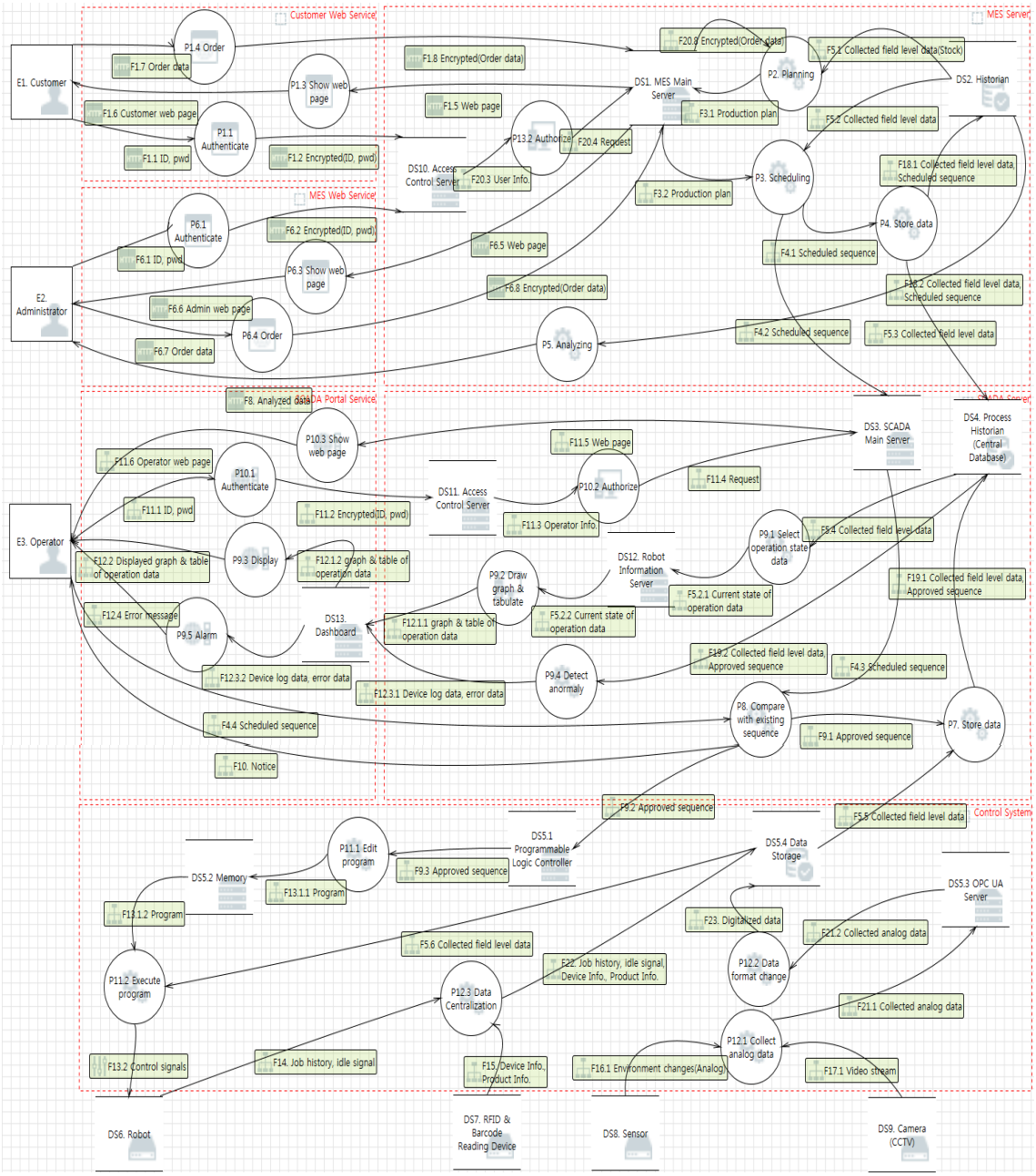

Fig. 4. Level2 DFD for Smart Factory

과 관련된 전반적인 프로세스를 관리한다. Operator는 공장 내 상황을 감시하고 작업을 제어할 수 있다. 현장 수준에서 수집된 데이터는 제어 프로세스로 전달되어 로봇이 자동적으로 작업을 수행할 수 있고 MES에서도 주문 및 수집된 데이터를 토대로 작업 배정이 이루어지는 등 CPS가 도입되어 전반적인 생산 과정에서 자동화가 이루어진 스마트팩토리를 도식화하였다.

Fig. 4.는 Level2를 나타낸다. 데이터 흐름도 Level2의 각 구성 요소들에 대하여 다음의 Table. 4.를 통해 설명한다.

Table. 4. DFD Level2 of the Smart Factory

Group	Component	Explanation
External Entity	Customer	Customers who order products
External Entity	Administrator	Those who manage the overall production process such as production performance management, facility efficiency management, quality management, and logistics management
External Entity	Operator	Operators who monitor plant conditions and control operations
Process	Authenticate	Sends the ID, pwd from the customer, administrator, and operator to the access control server
Process	Authorize	Grant permission using ID, pwd
Process	Show web page	Send a web page in response to a granted permission
Process	Order	The process which the customer orders products directly or the manager places the order
Process	Planning	Planning what, when, how to produce monthly, weekly, daily unit based on orders,
Process	Scheduling	In order to optimize the production process, the work sequence is allocated in real time based on the pre-established plan and the production status
Process	Store data	Save data in Historian
Process	Analyzing	Provides statistically analyzed data to managers for production performance management, facility efficiency management, quality control, and logistics management using data generated at the field level
Process	Select operation state data	Transfer only data related to the operational status of the robot among the data collected at the field level
Process	Draw graph & tabulate	Real-time operational data is graphically charted to help users understand it
Process	Display	Show the user to view schematized real-time operational data
Process	Detect anomaly	Using the data collected at the field level, if the behavior of the robot is different from usual or different from the work sequence
Process	Alarm	Notify user of detected anomalies
Process	Compare with existing sequence	Approve new jobs compared to previously assigned job plans
Process	Edit program	Modify an existing program or create a new program according to the newly approved work sequence
Process	Execute program	Execute program to control the robot
Process	Collect analog data	Collect analog data from various devices in the factory
Process	Data format change	Converts the format of the data so that the collected data can be processed on the PC using the OPC UA protocol
Process	Data centralization	Collect data from all devices in the factory
Data Store	Access Control Server	Server with information of customer, administrator, operator
Data Store	MES Main Server	A server that has order information from customer and manager, and factory schedule and perform a role as a web server
Data Store	Historian	A database that has data from the field level and stores work schedules assigned to devices
Data Store	SCADA Main Server	A Web server that provides portal services and have assigned work sequence
Data Store	Process Historian (Central Database)	A central database that stores all data from the field level and has approved work sequences
Data Store	Robot Information Server	Storing data related to the work status of robots
Data Store	Dashboard	A user interface that allows operators to centrally manage a variety of information
Data Store	Programmable Logic Controller	Save information about approved work sequences
Data Store	Memory	The repository where the program exists that runs the robot
Data Store	OCP UA Server	Has data conversion related information to communicate smoothly between different machines

Group	Component	Explanation
Data Store	Data Storage	Temporarily store data collected from field-level devices
Data Store	Robot	Performs work according to input control signal and transmits work history
Data Store	RFID & Barcode Reading Device	Equipment to collect data from other devices and products for facility management, asset management, semi-finished product input history management, goods receipt and warehouse management, etc.
Data Store	Sensor	Sensors that can detect the environmental changes (temperature, weight, pressure, etc.) inside the factory and the operation of machines
Data Store	Camera(CCTV)	Generate image data that can monitor operation status of facilities
Data Flow	ID, pwd	Customer, administrator, operator input ID, pwd
Data Flow	Encrypted(ID, pwd)	Encrypted ID and password data
Data Flow	User Info.	User information verified by ID and password
Data Flow	Request	Requests that are sent to the web server to populate the web page when granted
Data Flow	Web page	Information about web pages according to incoming requests
Data Flow	Customer, Admin, Operator Web page	Web page information provided to authorized customers, administrators, and operators
Data Flow	Order data	Order data entered from customers and operators and used to establish production plans
Data Flow	Encrypted(Order data)	Order data encrypted on the website and forwarded to the server
Data Flow	Production plan	Production planning data established based on input orders
Data Flow	Scheduled sequence	The work sequence data assigned to each device based on the production plan data
Data Flow	Collected field level data	Data collected at the field level includes the work history of machines, data collected from identification equipment, equipment information, factory environment information collected from sensors, and image data collected from imaging equipment.
Data Flow	Analyzed data	Statistically analyzed data for production performance management, facility efficiency management, quality control, and logistics management
Data Flow	Current state of operation data	Data related to the device's current operational state and workload
Data Flow	Graph & table of operation data	Information on the current operational status and workload of the device
Data Flow	Displayed graph & table of operation data	The current operational status and workload information of the graphical device displayed on the operator's screen
Data Flow	Device log data, error data	The information related to the error and the operation log data of the robot transmitted when the robot is not operated by a predetermined or different operation
Data Flow	Error message	Error messages sent to the operator
Data Flow	Approved sequence	the newly assigned task plan information if there is a change in job scheduling,
Data Flow	Notice	If there is no change in the work order assignment entered by the operator, the notification information sent to the operator
Data Flow	Program	Programs modified or newly created according to the newly assigned work plan
Data Flow	Control signals	According to the created program, the controller converts the converted data into signals that each device can recognize
Data Flow	Job history, idle signal	Work history data and operation status data of machines in factory
Data Flow	Device Info. Product Info.	Data transmitted via RFID and barcode equipment for facility management, logistics management, quality control, etc.
Data Flow	Environment changes	Environmental change data (temperature, humidity, etc.) collected through various sensors for environmental management
Data Flow	Video stream	Video data transmitted through a camera for factory production control
Data Flow	Collected analog data	Data collected from instruments outputting analog signals
Data Flow	Digitized data	The data converted so that PC can receive input through OPC UA protocol

Table. 5. STRIDE Threat Analysis on Smart Factory

Component	No	Name	STRIDE	Description	Threat
Entity	E1	Customer	S	Attacker can spoof Customer account and try to login	T1
			S	Attacker can impersonate and try to get the information sent to Customer	T2
			R	Customer repudiate that he did not receive Customer web page	T3
Entity	E2	Administrator	S	Attacker can spoof Administrator account and try to login	T4
				Attacker can impersonate and try to get the information sent to Administrator	T5
			R	Administrator repudiate that he did not receive Admin web page or Analyzed data	T6
Entity	E3	Operator	S	Attacker can spoof Operator account and try to login	T7
			S	Attacker can impersonate and try to get the information sent to Operator	T8
			R	Operator repudiate that he did not receive the data	T9
Data Store	DS1	MES Main Server	T	Attacker can tamper MES Main Server memory through manipulated data flow(eg. Buffer Over Flow)	T10
			R	MES Main Server repudiate that it did not receive data (Attacker puts data in the logs to confuse or read as code)	T11
			I	Attacker can get Production plan information	T12
			D	Cannot access to MES Main Server	T13
			D	Generate many requests to make slow or consume excessive resource for MES Main Server	T14
중략					
Process	P13.2	Authorize	T	Persistent Cross Site Scripting Vulnerability	T190
			T	Cross Site Scripting Vulnerability	T191
			T	Authorize process can be tampered by spoofed Data Storage	T192
			D	Excessive resource consumption for Authorize process	T193
중략					
Data Flow	F14	Job history, idle signal	D	Interrupt Job history, idle signal flow so that it cannot be sent to the destination	T256
Data Flow	F15	Device Info., Product Info.	D	Interrupt Device Info., Product Info. flow so that it cannot be sent to the destination	T257
Data Flow	F16.1	Environment changes (Analog)	D	Interrupt Environment changes(Analog) flow so that it cannot be sent to the destination	T258
Data Flow	F17.1	Video stream	D	Interrupt Video stream flow so that it cannot be sent to the destination	T259

4.3 Attack Library 수집

Attack Library는 데이터 흐름도를 작성한 이후 시스템에 대한 위협들을 다양한 자료 조사를 통해 수집한 목록이다. Attack Library 작성을 통해 DFD 상에서 각 요소마다 발생 가능한 위협을 찾아낼 수 있다. 본 논문에서는 기술보고서, 논문, 컨퍼런스 및 CVE(Common Vulnerabilities and Exposure)를 활용하여 실제 발생 가능한 공격들을 식별하였다. 다음의 Table. 6.은 스마트팩토리 시스템의 취약점과 관련된 자료들을 조사하여 정리한 Attak Library이다.

4.4 STRIDE 위협 도출

STRIDE는 Microsoft에서 제안한 위협 모델링 기법으로 체계적인 방법을 이용하여 시스템에 대한 위협을 식별한다. STRIDE 위협 모델링 기법은 데이터 흐름도의 각 요소들에 대하여 정보보호를 통해 달성하려는 6가지 목표인 인증(Authentication),

Table. 6. Attack Library for Smart Factory

Source	Category	Title	Author	Ref.
Conference	Web App	Server-Side Template Injection: RCE for the modern webapp	James Kettle	[21]
		HEIST: HTTP Encrypted Information can be Stolen Through TCP-Windows	Mathy Vanhoef	[22]
		HTTP Cookie Hijacking in the Wild: Security and Privacy Implications	Suphannee Sivakorn	[23]
		The Top 10 Web Hacks of 2015	Jonathan Kuskos	[24]
	Network	Compromising Industrial Facilities from 40 Miles Away	Lucas Apa	[16]
		Getattacking Bluetooth Smart Devices - Introducing a New BLE Proxy Tool	Sławomir Jasek	[15]
	Network / System	PLC-Blaster: A Worm Living Solely in the PLC	Ralf Spenneberg	[12]
	System	The Little Pump Gauge That Could: Attacks Against Gas Pump Monitoring Systems	Kyle Wilhoit	[25]
		Remote Physical Damage 101 - Bread And Butter Attacks	Jason Larsen	[26]
		Exploiting Memory Corruption Vulnerabilities on the FreeRTOS Operating System	Joel Sandin	[27]
		Pwning the Industrial IoT: RCEs and backdoors are around!	Sergey Temnikov	[28]
	All	Out of Control: Demonstrating SCADA Device Exploitation	Brian Meixell	[11]
		"Man-in-the-SCADA:" Anatomy of Data Integrity Attacks in Industrial Control Systems	Chris Sistrunk	[29]
Journal	Network	Security and Vulnerability of SCADA Systems over IP-Based Wireless Sensor Networks	H. Kim	[17]
	System	Stuxnet Worm Impact on Industrial Cyber-Physical System Security	Stamatis Karnouskos	[9]
		Modeling cyber attacks on a critical infrastructure scenario	E. Ciancamerla	[10]
Technical Report	Network	Emerson Wireless Security - Automation Solutions	Emerson	[30]
	All	Guide to Increased Security in Industrial Control Systems	MSB	[31]
		Securing Industrial Control Systems-2017	SANS Institute	[32]
		Cyber Security Issues with Level 0 through 1 Devices	Joe Weiss	[13]
		Industrial Control Systems Vulnerabilities Statistics	Kaspersky	[33]
CVE	Web App	CVE-2016-8561	MITRE	[34]
		CVE-2016-9160	MITRE	[34]
		CVE-2017-2683	MITRE	[34]
		CVE-2017-6867	MITRE	[34]
	System	CVE-2016-9159	MITRE	[34]
	Network	CVE-2017-6864	MITRE	[34]
		CVE-2017-6865	MITRE	[34]
		CVE-2017-6871	MITRE	[34]
		CVE-2017-12069	MITRE	[34]

무결성(Integrity), 부인방지(Non-repudiation), 기밀성(Confidentiality), 가용성(Availability), 인가(Authorization)와 대칭되는 위장(Spoofing), 변조(Tampering), 부인(Repudiation), 정보 유출(Information Disclosure), 서비스 거부(Denial of Service), 권한 상승(Elevation of privilege)에 대한 위협들을 식별한다[35]. 본 연구에서 사용한 도구는 Microsoft Threat Modeling Tool 2016으로 사용자가 DFD를 작성하면 해당 도구를 이용하여 자동적으로 위협을 분석할 수 있다[36]. 본 논문에서는 도출된 데이터 흐름도 Level2를 이용하여 스마트팩토리에 대한 위협들을 STRIDE에 따라 분석한 결과 총 259개의 위협이 도출되었다. 다음 Table. 5.는 STRIDE 분석 결과이다.

4.5 Attack Tree

Attack Tree란 자산이나 정해진 목표를 공격하는 시나리오를 제시하는 개념도로써 루트 노드부터 자식 노드로 나누어지는 다중 수준으로 구성되어있다. 4.4에서는 도출된 위협들을 이용해 Attack Tree를 작성하여 스마트팩토리를 공격하는 시나리오를 제시한다. 이러한 과정을 통해 공격자가 스마트팩토리를 공격할 수 있는 방법을 구체화시킨다. 다음의 Table. 7.은 Attack Library 및 STRIDE 분석을 통해 도출된 위협과 작성된 Attack Tree와의 연관성을 보여준다.

Table. 7. Relation between Attack Tree and STRIDE Threats

Attack Tree					Threats
1	Attacker Get Secrets of the Company				
OR	1.1	Get information through the Web Service			
	OR	1.1.1	Get Administrative Privilege		
		OR	1.1.1.1	MITM	T66, T69, T78, T83, T84, T102, T111, T116, T133, T144, T148, T151
		OR	1.1.1.2	XSS	T69, T72, T78, T84, T101, T110, T115, T132, T146, T150, T159, T160, T163, 190, T191
		OR	1.1.1.3	CSRF	T141
	OR	1.1.2	Network Sniffing		
		OR	1.1.2.1	ARP Spoofing	T2, T5, T8, T70, T86, T104, T118, T136, T153, T195, T198, T203, T206, T209, T212, T215, T219, T222, T227, T230, T234, T238, T241, T246, T250, T254
		OR	1.1.2.2	ICMP Redirect	T2, T5, T8, T70, T86, T104, T118, T136, T153, T195, T198, T203, T206, T209, T212, T215, T219, T222, T227, T230, T234, T238, T241, T246, T250, T254
	OR	1.1.3	Get ID, pwd		
		OR	1.1.3.1	Guessing	T1, T4, T7
		OR	1.1.3.2	Social Engineering	T1, T4, T7
		OR	1.1.3.3	Phishing	T1, T4, T7
	OR	1.1.4	Bypass Admission control		
		OR	1.1.4.1	Tailgating	T8
		OR	1.1.4.2	Get access control card	T8
	OR	1.1.5	Bypass Authentication		
		OR	1.1.5.1	Remote File Inclusion	T12, T16, T20, T26, T29, T30, T35, T38, T54, T59, T62, T94, T124, T171, T174, T183
		OR	1.1.5.2	SQL Injection	T15, T23, T37
	OR	1.1.6	Wireless Network Sniffing		
		OR	1.1.6.1	Wardriving	T43, T46, T48, T50
		OR	1.1.6.2	Evil Twin	T43, T46, T48, T50
	OR	1.1.7	IP-based network Sniffing		
		OR	1.1.7.1	ARP Spoofing	T43, T46, T48, T50
		OR	1.1.7.2	ICMP Redirect	T43, T46, T48, T50

Attack Tree					Threats
2	Denial of Service				
OR	2.1	Cannot Access Resources			T13, T22, T28, T31, T40, T45, T47, T49, T51, T56, T61, T67
OR	2.2	Give additional privilege			
	OR	2.2.1	Arbitrary Code Execution		
			2.2.1.1	Buffer Over Flow	T10, T18, T24, T33, T41, T52, T57, T64
	OR	2.2.2	Misuse of Function		T14, T17, T21, T27, T32, T34, T36, T39, T44, T55, T60, T68, T77, T91, T99, T109, T123, T131, T142, T158
OR	2.3	Consume System Resource			
	AND	2.3.1	Sending crafted packet		T63, T74, T88, T93, T96, T98, T106, T120, T128, T138, T155, T162, T170, T173, T177, T182, T187, T193
	OR	2.3.2	Bypass authentication		T66, T69, T72, T78, T83, T84, T101, T102, T110, T111, T115, T116, T132, T133, T144, T146, T148, T150, T151, T159, T160, T163, 190, T191
	OR	2.3.3	Get ID, pwd		T1, T4, T7
OR	2.4	Consume Network Resource			
	OR	2.4.1	Flooding		
		OR	2.4.1.1	SYN Flooding	T196, T199, T200, T201, T204, T207, T210, T213, T216, T217, T220, T223, T224, T225, T228, T231, T232, T235, T236, T239, T242, T243, T244, T247, T248, T251, T252
		OR	2.4.1.2	Get Flooding	T196, T199, T200, T201, T204, T207, T210, T213, T216, T217, T220, T223, T224, T225, T228, T231, T232, T235, T236, T239, T242, T243, T244, T247, T248, T251, T252
	OR	2.4.2	Land Attack		T74, T88, T93, T96, T98, T106, T120, T128, T138, T155, T162, T170, T173, T177, T182, T187, T193
	OR	2.4.3	Ping of Death		T208, T211, T214, T233, T245, T249
OR	2.5	Crash process			
	OR	2.5.1	Teardrop		
	OR	2.5.2	Clicking malicious link		T14, T17, T21, T27, T32, T34, T36, T39, T44, T55, T60, T68
	OR	2.5.3	Arbitrary memory read		T69, T72, T78, T84, T101, T110, T115, T132, T141, T146, T150, T159, T160, T163, 190, T191
OR	2.6	Wireless Network			T73, T80, T87, T105, T112, T119, T127, T154, T166, T178, T186
	OR	2.6.1	Jamming		T45, T47, T49, T51, T255, T256, T257, T258, T259
3	Attacker Control the Factory				
OR	3.1	Privilege Escalation			
	OR	3.1.1	Get ID, pwd		T1, T4, T7
	OR	3.1.2	Bypass Authentication		T66, T69, T72, T78, T83, T84, T101, T102, T110, T111, T115, T116, T132, T133, T144, T146, T148, T150, T151, T159, T160, T163, 190, T191
	OR	3.1.3	Arbitrary Code Execution		
			3.1.3.1	Buffer Over Flow	T10, T18, T24, T33, T41, T52, T57, T64
	OR	3.1.4	Remote Code Execution		

Attack Tree					Threats
			3.1.4.1	Memory corruption	T19,T25,T42,T53,T58,T65,T76,T75,T81,T82,T90,T92,T95,T97,T100,T107, T108, T113, T114, T121, T125, T122, T129, T130, T134, T139, T140, T143, T145, T147, T149, T156, T157, T161, T164, T167, T168, T169, T172, T179, T180, T181, T188, T189, T192, T194, T197, T202, T205, T218, T221, T226, T229, T237, T240
OR	3.2	Access through Wireless Network			
	OR	3.2.1	Data Injection		
		OR	3.2.1.1	Synthesis	T175, T184, T253
		OR	3.2.1.2	Replay	T175, T184, T253

V. 스마트팩토리 보안 요구사항 도출

5장에서는 도출된 위협을 통해 실제로 취약점을 분석하기 위한 체크리스트를 제시한다. 다음 Table. 8.는 스마트팩토리 취약점 분석을 위한 체크리스트이다. 체크리스트는 4.4 Attack Tree를 통해 도출된 실제 공격 기법들에 대한 대응 방안을 토대로 작성되었고 같은 점검 항목이 나온 경우 중복되는 요소를 제거하였다.

VI. 결 론

스마트팩토리는 CPS를 기반으로 기존의 생산 기술에 정보통신기술을 융합하여 제조의 모든 단계가 자동화, 지능화됨으로써 최종적으로 생산성을 극대화 시킨다. 폐쇄적인 운영 방식을 지닌 기존을 제조 시

Table. 8. Checklists for Smart Factory

Category	Related Attack	Checklist	No.
Network	MITM	Check the web site uses SSL	C1
	Spoofing	Fix the MAC Address	C2
		Restrict trusted administer or operator	C3
	Remote File Inclusion	Verify parameter of input data	C4
	SQL Injection	Verify SQL query	C5
	Sending crafted packet	Check the system updates	C6
		Using VPN for protection network communication between cells	C7
		Applying Defense in Depth	C8
	Flooding	Check opened port	C9
		Check unnecessary port for management	C10
	Land Attack	Check IP Address in packet	C11
	Ping of Death	Check IP Address that sending ping consistently	C12
		Check ICMP port is closed	C13
Wireless Network	Wardriving	monitoring system for which wireless LAN station uses network IP resource	C14
		Check for using RADIUS	C15
	Evil Twin	Using pre-operational trigger	C16
	Replay, Synthesis	Use WIDS / WIPS	C17
	Jamming	Check there is anti-jamming techniques	C18
Application	XSS	Check the Domain name	C19
	CSRF	Check that an attacker can get user information	C20
	Phishing	Have plans for educating employee	C21
	Guessing	Restrict the number of times on login trials	C22
		Guideline to make password strong	C23
		Changing password periodically	C24
System	Misuse of Function	Test system functions operate as a specification	C25
	Buffer Over Flow	Check program uses functions that are vulnerable to Buffer Over Flow	C26
	Memory corruption	Applying cell protection concept	C27
	Teardrop	Check there is access control configuration for the system	C28
Physical	Social Engineering	Check employees uses locks for sensitive files	C29
	Tailgating	Check using surveillance devices	C30
	Get access control card	Check using secondary authentication solution for monitoring room or server room	C31

스템과 차별적으로 다양한 기술과 환경을 통합한 스마트팩토리는 그 복잡도(Complexity)와 불확실성(Uncertainty)이 크기 때문에 외부 네트워크 및 무선 통신을 통한 위협, 악성코드에 대한 노출이 증가하는 등 예상치 못한 문제가 발생할 가능성이 높다.

따라서 본 논문에서는 스마트팩토리 전체 시스템에 대한 데이터 흐름도를 작성한 후 이를 토대로 실제 공격 사례 및 공격 기법들을 조사하여 Attack Library를 작성하였다. 그리고 STRIDE 기법을 이용하여 총 259개의 위협을 식별하였다. STRIDE 위협들을 바탕으로 공격자의 목표에 따라 실제 공격 시나리오를 가정한 Attack Tree를 작성하였으며 그 결과에 기초하여 스마트팩토리에 대한 보안 점검을 할 수 있는 체크리스트를 도출하였다.

본 연구를 통하여 도출된 체크리스트는 향후 스마트팩토리 안전성 검사 및 보안 가이드라인 제작에 활용될 것으로 기대된다.

현재 스마트팩토리는 도입이 확산되는 과정 중에 있으며 실제로 고도화된 스마트팩토리에 대한 사례가 극히 적다는 한계점이 존재한다. 따라서 향후 실제 구축된 스마트팩토리 사례를 이용하여 위협 분석을 수행하면 보다 세부적인 항목들을 도출할 수 있을 것으로 기대된다. 더불어 체크리스트 도출 과정에서 국제표준인 공통평가기준을 적용시킨 연구과제가 남아 있다.

References

[1] Edward A. Lee, "Cyber Physical Systems: Design Challenges", 11th IEEE International Symposium on Object Oriented Real-Time Distributed Computing (ISORC), pp. 363-369, May. 2008.

[2] Alvaro A. Cardenas, Saurabh Amin, Shankar Sastry, "Secure Control: Towards Survivable Cyber-Physical Systems", The 28th International Conference on Distributed Computing Systems Workshops, pp. 495-500, Jun. 2008.

[3] Injae Lee, "Domestic and Overseas Introduction Trends of Smart Factory", Institute for Information and Communications Technology Promotion, Sep. 2016.

[4] Cyber Physical Systems Public Working Group, "Framework for Cyber-Physical Systems Release 1.0", May. 2016.

[5] NIST, "Framework for Cyber-Physical Systems: Volume 1, Overview ", Jun. 2017.

[6] NIST, "Framework for Cyber-Physical Systems: Volume 2, Working Group Reports", Jun. 2017.

[7] NIST, "Framework for Cyber-Physical Systems: Volume 3, Timing Annex ", Jun. 2017.

[8] NIST, "Guide to Industrial Control Systems (ICS) Security ", 2015.

[9] Karnouskos, Stamatis. "Stuxnet worm impact on industrial cyber-physical system security." IECON 2011-37th Annual Conference on IEEE Industrial Electronics Society. IEEE, pp. 4490-4494, Jan. 2011.

[10] Ciancamerla, Ester, Michele Minichino, and S. Palmieri. "Modeling cyber attacks on a critical infrastructure scenario." Information, intelligence, systems and applications (IISA), 2013 fourth international conference on. IEEE, pp. 1-6, Jul. 2013.

[11] Brian Meixell, "Out of Control: Demonstrating SCADA Exploitation", Black Hat USA 2013.

[12] Spenneberg, Ralf, Maik Brüggemann, and Hendrik Schwartke. "Plc-blaster: A worm living solely in the plc." Black Hat Asia, Marina Bay Sands, Singapore, 2016.

[13] DEF CON 25 Hacking Conference, https://www.defcon.org/html/defcon-25/dc-25-index.html

[14] Wollschlaeger, Martin, Thilo Sauter, and Juergen Jasperneite. "The future

of industrial communication: Automation networks in the era of the internet of things and industry 4.0." IEEE Industrial Electronics Magazine, vol.11, no.1, pp. 17-27, Mar. 2017.
〔15〕 Black Hat USA 2016, http://www.blackhat.com/us-16/
〔16〕 Lucas Apa, "Compromising Industrial Facilities from 40 Miles Away", Black Hat USA 2013.
〔17〕 Kim, HyungJun. "Security and vulnerability of SCADA systems over IP-based wireless sensor networks." International Journal of Distributed Sensor Networks, vol.8, no.11, Jan. 2012.
〔18〕 Thilo Sauter, "The continuing evolution of integration in manufacturing automation", IEEE Industrial Electronics Magazine, vol.1, no.1, pp.10-19, May. 2007.
〔19〕 D. Bauer, D. Stock, T. Bauernhansl, "Movement Towards Service-orientation and App-orientation in Manufacturing IT", Procedia CIRP, vol.62, pp.199-204, May. 2017.
〔20〕 Korea Embedded Software and System Industry Association, "Smart Factory Status and Implications", KESSIA ISSUE REPORT, Nov. 2015.
〔21〕 James Kettle, "Server-Side Template Injection: RCE for the modern web-app", Black Hat USA 2015.
〔22〕 Vanhoef, Mathy, and Tom Van Goethem. "HEIST: HTTP Encrypted Information can be Stolen through TCP-windows.", Black Hat USA 2016.
〔23〕 Sivakorn, Suphannee, Jason Polakis, and Angelos D. Keromytis. "HTTP Cookie Hijacking in the Wild: Security and Privacy Implications.", Black Hat USA 2016.
〔24〕 OWASP AppSec Europe '16, https://2016.appsec.eu/
〔25〕 Kyle Wilhoit, "The Little Pump Gauge That Could: Attacks Against Gas Pump Monitoring Systems", Black Hat USA 2015.
〔26〕 Jason Larsen, "Remote Physical Damage 101 - Bread And Butter Attacks", Black Hat USA 2015.
〔27〕 ShmooCon Speakers 2016, http://shmoocon.org/2015/12/08/shmoocon-speakers-2016/
〔28〕 Sergey Temnikov, "Pwning the Industrial IoT: RCEs and backdoors are around!", DEF CON 25, 2017
〔29〕 Black Hat Asia 2017, https://www.blackhat.com/asia-17/
〔30〕 Emerson, "Emerson Wireless Security - Automation Solutions", Emerson Process Management, Feb. 2016.
〔31〕 MSB, "Guide to Increased Security in Industrial Control Systems", Swedish Civil Contingencies Agency, Nov. 2014.
〔32〕 SANS Institute, "Securing Industrial Control Systems-2017", Jun. 2017.
〔33〕 Kaspersky, "Industrial Control Systems Vulnerabilities Statistics", 2016.
〔34〕 MITRE, https://cve.mitre.org/
〔35〕 Microsoft, https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx
〔36〕 Microsoft, Microsoft Threat Modeling Tool, https://www.microsoft.com/en-us/download/details.aspx?id=49168

〈저 자 소 개〉

박 은 주 (Eun-ju Park) 학생회원
2016년 2월: 동덕여자대학교 컴퓨터학과 졸업
2016년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 보안공학, 보안 위협 모델링, 금융보안

김 승 주 (Seung-joo Kim) 종신회원
1994년~1999년: 성균관대학교 정보공학과 (학사, 석사, 박사)
1998년 12월~2004년 2월: KISA(舊 한국정보보호진흥원) 팀장
2002년~현재: 한국정보통신기술협회(TTA) IT 국제표준화전문가
2004년 3월~2011년 2월: 성균관대학교 정보통신공학부 조교수, 부교수
2011년 3월~현재: 고려대학교 사이버국방학과/정보보호대학원 정교수
2004년~현재: 한국정보보호학회 이사
2005년~2006년: 교육인적자원부 유해정보 차단 자문위원
2007년 :국가정보원장 국가사이버안전업무 유공자 표창
2007년~2009년: 전자 정부 서비스 보안 위원회 사이버 침해사고대응 실무위원회 위원
2010년 :방송통신위원회 정보통신망 침해사고 민관합동조사단 위원
2012년 3월~2012년 6월: 선관위 디도스 특별검사팀 자문위원
2013년 4월~2013년 12월: IT보안인증사무국 자문위원
2013년 9월~현재: 중앙선거관리위원회 자문위원
2014년 3월~현재: 헌법재판소 자문위원
2014년 12월~현재: 카카오 자문위원
2016년 1월~현재: 한국정보화진흥원 자문위원
〈관심분야〉 보안공학, 암호이론, 정보보증, 정보보호제품 보안성 평가, Usable security