스마트팩토리 보안 앤드포인트 식별을 위한 토폴로지 제네레이터 설계 및 구현

[1]김양훈

Design and Implementation of Topology Generator for Sm art Factory Security Endpoint Identification

[1]Yanghoon Kim

요 약

제4차 산업혁명을 기점으로 핵심기술들이 산업에 적용되어 각종 스마트 환경을 구축하기 시작하였다. 제조업의 스마트팩토리는 맞춤형 생산을 위한 광범위한 데이터의 수집과 제어를 실행할 수 있는 IIoT를 핵심기술로 적용하여 고품질 제품을 생산하게 되었다. 그러나, IIoT를 통하여 개방형으로 전환된 스마트팩토리의 네트워크 환경은 다양한 보안 위험에 노출되었다. 보안 침해에 따라 IIoT는 네트워크 망의 교란, 위변조된 IIoT의 사용 및 유지로 인하여 생산 제품, 생산 공정의 품질저하를 나타내었으며, 기업의 비즈니스에 신뢰성에 문제를 발생시킬 수 있다.

이에 따라 본 연구에서는 스마트팩토리 초기 구축 시 IIoT의 안전한 연결 및 활용을 위하여 스마트팩토리에 연결된 IIoT에 대한 실질성 확인과 무해화 환경 구축을 실행할 수 있는 방법으로 IIoT 연결 상황을 확인할 수 있는 연구를 실행하였다.

Abstract

Starting from the 4th industrial revolution, core technologies were applied to industries to build various smart environments. Smart factories in the manufacturing industry produce high-quality products by applying IIoT as a core technology that can collect and control a wide range of data for customized production. However, the network environment of the smart factory converted to open through IIoT was exposed to various security risks. In accordance with security breaches, IIoT has shown degradation in the quality of manufactured products and production processes due to network disturbance, use and maintenance of forged IIoT, and can cause reliability problems in business.

Accordingly, in this study, a method for safe connection and utilization of IIoT was studied during the initial establishment of a smart factory. Specifically, a study was conducted to check the IIoT connection situation so that the practicality of the IIoT connected to the smart factory could be confirmed and the harmless environment established.

Keywords: *Smart Factory, Security, Identification, Endpoint, Internet of Things*

[1] *신한대학교 사이버드론봇군사학과 부교수(kimyh7902@shinhan.ac.kr)*

Received: Jun. 13, 2023, Revised: Jun. 26, 2023, Accepted: Jun. 26, 2023

I. 서론

각종 산업에 최신의 자동화, 고도화된 핵심기술들이 내재화되면서 제 4 차 산업혁명에 따른 기술 활성화가 진화되고 있다. 특히, 핵심기술들의 산업 적용은 스마트 산업을 확산시키고 있다. 이에 따라, 기존의 서버 · 클라이언트 구조로 이루어진 단방향성의 정보화 환경과 차별화되게 사물인터넷을 기반으로 양방향성의 환경을 완성시키고 있다. 지능화된 사물인터넷 환경은 사물 간의 데이터를 주고받는 센싱, 네트워킹을 포함하여 다종, 다량의 광범위한 데이터 수집을 실현시키고 있다. 이러한 광범위한 데이터를 활용한 빅데이터, 인공지능을 통한 서비스 전환은 필수 불가결한 요소가 되어가고 있다. 이러한 추세와 같이 제조업과 같은 전통적인 산업은 현재 활용하고 있는 장비에 IT 기술을 적용하여 관리시스템을 도입함으로써 정보화를 실현하였다. 이어서 제 4 차 산업혁명에 활용되는 기술들의 도입을 검토함으로써 새로운 신 산업 창출에 노력하고 있다. 국내에서 제조업은 스마트 팩토리로의 전환을 위하여 자체적인 시스템의 도입 또는 정부 지원을 통해 체계적인 산업융합환경으로 변화를 추진하고 있다.

제조업의 스마트팩토리는 운영기술(OT, Operation Technology), 산업제어시스템(ICS, Industry Control System) 등을 기반으로 기존의 공장 자동화를 탈피하여 빅데이터, 인공지능, 클라우드 등을 도입하고 업무를 수행한다. 스마트팩토리 솔루션을 기반으로 제품의 수명관리나 모바일 단말관리를 통한 개별 맞춤형 생산을 진행하고 재고의 감소, 인건비 절감의 효과를 보이고 있다[1]. 또한, 스마트팩토리는 제품의 기획단계에서부터 설계와 생산, 그리고 유통 및 판매와 같이 비즈니스 프로세스의 모든 과정에서 제 4 차 산업혁명의 핵심기술인 인공지능, 인공지능, 사물인터넷, 빅데이터, 사이버 물리 시스템 등을 융합시켜 운영하는 것을 목적으로 하고 있다. 특히, 제조공장에서 맞춤형 생산을 위한 광범위한 데이터의 수집과 제어를 위하여 산업용 사물인터넷(이하 IIoT, Industrial Internet of Things)을 핵심기술로 적용 구축하고 있으며 고품질 생산으로 이어지고 있다.

한편, 기존 정보화 수준의 제조공장을 구성하는 다양한 요소 중 네트워크는 산업 네트워크로 구성되어 격리된 사설 네트워크 형태의 닫힌 공간으로 구성한다. 제조 장비 전용의 산업용 프로토콜로 연계되어 생산제조를 수행하였지만, 스마트팩토리 도입을 통하여 산업용 사물인터넷을 적용하게 되었고 장비를 포함한 내 외부 사물들이 서로 연결하게 되면서 다양한 문제점들이 나타나기 시작했다[2]. 네트워크의 연결은 악의적인 외부 공격에 노출되어 악성코드 침입, 장비 감염과 같은 보안 위험이 나타난다. 더불어 편의성 증대로 인하여 내부자의 비정상적인 사용, 오용 등으로 보안침해가 발생하게 될 수 있다.

IIoT 를 통하여 개방형으로 전환된 스마트팩토리의 네트워크 환경은 네트워크를 통한 장비, 장치 SW 업데이트로 악성코드의 침입에 대한 민감성이 증가하고 있으며, 또한 사용자가 직접 설치하는 SW 에서 스마트팩토리를 타겟으로 하는 악성코드로 인한 침해를 현장에서 탐지하기 어려운 상황에 있다. 이러한 상황에서 악성코드에 감염된 IIoT 는 제조공정에 연쇄적인 문제를 갖는 보안 사고를 발생시킨다. IIoT 의 보안 침해는 생산 제품, 생산 공정에 다양한 문제를 발생시키고, 궁극적으로는 기업의 비즈니스에 신뢰성을 낮추게 되는 영향을 발생시킬 수 있다[3].

스마트팩토리는 우선적으로 내부 네트워크 상에서 IIoT 를 통하여 데이터를 교환하기 때문에 방화벽을 통한 보안 모델을 갖추는 것이 일반적이다. 그러나, 실질적인 네트워크의 구현과 장비, 장치의 설치에 있어서 기존의 시스템과의 편리성, 호환성, 유지보수성 등을 고려할 수밖에 없는 상황이다. 또한, 비용적 문제와 기술적 문제도 동반하고 있다. 특히, 정보화 단계에서 순차적인 스마트팩토리 전환 단계에서는 이미 침해당한 IIoT 네트워크 망을 형성하고 있는 경우도 발생한다[4].

보안 침해 등의 사고를 해소하기 위한 침입탐지 기술은 시스템과 네트워크 자원으로부터 비정상적인 사용 등에 대한 정보를 실시간으로 수집, 분석하여 침입 및 침입시도의 징후를 찾아내고 보고하는 형태로 발전하고 있다. 침입탐지 기술은 호스트 기반 탐지 방식과 네트워크 기반 탐지 방식으로 구분되며, 통계, 규칙(Rule), 데이터 학습을 통한 네트워크 패킷에 대한 분석이 핵심기술로 적용된다. 전통적인 방화벽이 탐지할 수 없는 악의적인 네트워크 트래픽 및 컴퓨터 사용을 탐지하기 위해 필요하다. 이와 같은 내용들을 응용하여 스마트팩토리 악성코드 침해 탐지의 시작단계로써 환경을 구성하는 IIoT 등에 대한 현황을 실시간으로 확인하고 보호하기 위한 대상을 식별하는 기술이 필요한 상황이다.

본 연구에서는 스마트팩토리의 보안환경을 구축하기 위한 시작점의 단계로 IIoT 를 식별하여 나타낼 수 있는 자동화 방안에 대하여 제안하고자 한다.

II. 관련연구

2.1 제 4 차 산업혁명과 제조업

증기기관을 이용한 방직 산업의 활성화를 이끈 제 1 차 산업혁명은 제조공정의 혁신으로 생산성을 향상시켰다. 그리고, 전기화학 공업의 발전을 통한 제 2 차 산업혁명을 지나, 정보화를 통한 산업혁명으로 간주되고 있는 제 3 차 산업혁명을 지나왔다. 최근 전 세계적인 성장률 감소와 경제 위기, 수출 증가율 둔화를 포함한 제조업의 한계에 대응하기 위한 새로운 산업혁명을 기대하고 있다[5].

제 4 차 산업혁명은 2016 년 다보스 포럼에서 언급된 이후 고유한 개념을 기반으로 다양한 융합기술과 산업에 연계되고 있다. 특히, 핵심기술로 꼽히는 인공지능, 사물인터넷, 빅데이터, 클라우드 등을 기반으로 초 연결환경과 초 지능화 혁신을 이끌고 있다. 이러한 혁신은 기존 산업, 기업에서 실행되는 기업 내부, 기업 외부, 협력 기업 등의 연계성을 확장 시키고, 생산 자동화를 포함하여 의사결정의 보조와 신사업 창출까지 확산시키고 있다.

특히, 제조산업에도 다양한 변화를 만들고 있다. 제조산업은 전통적인 정보화 기술 도입을 통하여 생산 자동화를 중심으로 ERP 를 구축하여 전사적인 자원관리 체제를 이루고 있다. 여기에 고도화된 기술의 연결을 통하여 스마트팩토리라 불리는 첨단 지능형 공장 체제로 탈바꿈 하고 있다. 스마트팩토리는 제품 기획부터 연계하여 실제 판매까지 비즈니스의 모든 과정을 고도화된 기술로 통합해 최적의 비용을 투자하여 고객 맞춤형의 제품을 제공하는데 목적이 있다.

스마트팩토리에 대한 문헌적 정의는 형태에 따라 조금씩 변화를 갖추고 있으며, 실제 구현의 목적과 대상을 달리 바라보고 있다. 오승철(2019)의 연구에서 스마트팩토리란 생산전략에 기반을 둔 제조 여건 변화에 유연하게 대응하고, 공급망 관리 통합관점의 품질, 비용, 유통 및 제약관리로 생산운영을 신뢰성 있게 수행하는 공정이라 하였다[6]. 또한, 정종필(2020)의 연구에서는 스마트팩토리에 대하여 IT 를 활용하여 생산제품의 기획, 설계, 생산, 유통, 판매 등 비즈니스 프로세스 전체 과정을 통합하여 자동화, 데이터화를 수행하는 지능형 생산공장을 의미하는 것으로 정리하고 있다. 이를 통하여 생산성 향상과 에너지 절감, 작업 환경의 인간중심화, 최적의 비용과 시간으로 맞춤형 제품을 생산하는 방식으로 결론지었다[3].

이러한 개념적 정의를 기반으로 구조를 살펴보면 스마트팩토리제조혁신추진단(2023)에 따르면 스마트팩토리 수준을 미적용 단계에서부터 고도화 단계까지 5 단계로 운영 및 역량을 차별화하여 구분하고 있다. 첫 단계인 ICT 미적용단계에서는 정보화 기술을 거의 도입하지 못한 상태로써 Excel SW 활용 수준에 머물러 있는 상태를 말한다. 두 번째 단계인 기초 수준에서는 생산실적의 정보를 자동 집계하는 수준으로써, 영업관리, 재고관리, 회계관리 등의 일부를 정보시스템으로 전환하여 운영하는 상태로 정의된다. 세 번째, 중간 수준 1 단계에서는 설비의 정보를 자동으로 집계하는 수준이다. 관리 정보시스템 사이에 부분적 연계를 통한 전사적 체계의 기초단계라 할 수 있다. 네 번째, 중간 수준 2 단계에서는 관리 시스템을 통해서 다양한 설비를 자동으로 제어한다. 전 단계에서 일부 관리 정보시스템 간의 부분적 연계에서 향상되어 시스템간 실시간 연동을 구현한 단계이다. 마지막 고도화 단계에서는 관리, 설비, 장비, 자재 관리 시스템들을 유무선 네트워크로 연결하여 스스로 판단하는 지능형 설비체계를 갖춤으로써 시스템을 통한 자율화된 스마트팩토리를 운영하는, 즉 전 제조과정을 포함한 비즈니스 단계의 지능화된 통합운영 단계를 뜻한다.

2.2 스마트팩토리 주요기술과 보안 침해

스마트팩토리에 적용되는 솔루션 단위의 기술은 인공지능, 로봇, 클라우드, 3D 프린팅, 사이버 물리 시스템 등 다양한 기술이 있지만, 스마트팩토리의 생산공정을 포함한 전체 비즈니스 프로세스에 적용되는 요소기술은 분리할 수 있다. 스마트팩토리는 다양한 요소기술 집합체로써, 내외부를 연결하는 응용 시스템 부분, 내부의 제어자동화 부분, 현장 자동화 부분으로 구분하여

제품의 기획, 계발부터 양산까지 제품 생산의 전체 비즈니스 프로세스에 다양한 기술을 적용한다. 이러한 기술의 적용은 보안적 관점에서 IT 와 OT(Operational Technology)의 개념을 구분 시킨다. 보안 관점에서 IT 는 보안 3 요소, 즉 기밀성, 무결성, 가용성을 확보하기 위한 체계를 갖추지만, OT 는 생산공정을 이행하기 위한 가용성을 중요하게 판단한다. 데이터넷(2020)의 기사에 따르면, SANS 社에서 조사한 OT 보안 관련 리포트에 따르면, OT 를 구축한 기업의 34.5%가 인터넷과 같은 공용 네트워크에 연결되어 있으며, 66.4%는 생산공정만이 아닌 기업 비즈니스에 관련된 외부 네트워크에 연결되어 있는 것으로 나타났다. 이에 따라 조사기간 직전 1 년동안 3 회 이상 보안 침해 이력이 있는 시스템의 비율이 2017 년 35.3%에서 2019 년 57.7%로 증가한 것으로 나타났다.

OWASP 가 2019 년 발표한 IIoT 의 취약점에는 안전하지 않은 네트워크 서비스, 안전한 업데이트 메커니즘 부재, 오래된 구성요소 사용, 디바이스 관리 부재 등을 이야기하고 있다. 이처럼 스마트팩토리에서 IIoT 는 필수불가결한 요소이지만, 보안 침해에 따라 IIoT 는 네트워크 망의 교란, 위 변조된 IIoT 의 사용 및 유지로 인하여 생산성 저하를 발생시킬 수 있는 것으로 나타났다.

이러한 IIoT 의 보안 위험을 통해 스마트팩토리 보안 침해가 나타나게 되면, 생산 제품, 생산공정에 다양한 문제를 발생시키고, 궁극적으로는 기업의 비즈니스에 신뢰성을 낮추게 되는 영향을 발생시키게 된다.

III. 스마트팩토리 IIoT 보안연결 토폴로지 제네레이터 설계 및 구현

3.1 IIoT 연결 탐색을 위한 알고리즘 설계

스마트팩토리의 기본 연결구조는 요소기술과 시스템을 중심으로 설계되어 있다. 스마트팩토리제조혁신추진단에서 제시하는 단계별 스마트팩토리 구성에 따르면, 응용시스템의 구성은 설치된 기업의 운영, 공장운영, 공급망 관리 및 최적화, 협력사 등의 연계에 초점이 맞추어져 있다. 제어 자동화의 구성은 공정제어, 인터페이스, 컴퓨터 수치제어, 산업용 센서 구축을 목표로 하고 있으며, 최종적으로 현장 자동화에는 제어자동화의 시스템 연계와 산업용 센서를 통하여 자동화를 실행하게 된다. 이러한 과정에서 발생되는 데이터의 저장과 가공 등에 외부의 클라우드, 가상물리생산 시스템, 지능형 기술 등을 이용하는 것으로 정리된다.

본 연구에서 제안하는 연구 대상은 제어자동화와 현장 자동화의 연계 구조상에 나타나는 IIoT 의 구조에 대한 자동화된 검증, 탐색을 실행하고자 한다. 설계 대상의 스마트팩토리 연결구조는 그림 1 처럼 나타낼 수 있다.

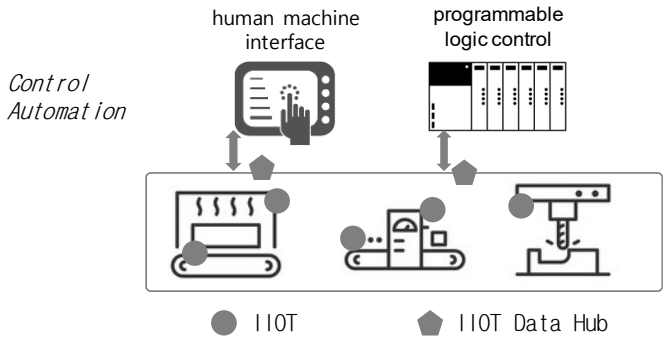

Figure 1. Smart Factory Production Plant Connection Structure
그림 1. 스마트팩토리 생산공장 연결구조

그림 1 의 스마트팩토리 구조를 기반으로 연결성을 확보하기 위하여 그림 2 의 ①처럼 제조공정은 동작하여 데이터를 생산하는 IIoT, 데이터를 집진하는 중간 노드, 최종 데이터를 저장/처리/분석하는 시스템으로 구분할 수 있다. 3 개의 중간 노드를 생산라인 별 장치라면 이에 대해 동작을 유도하는 연결된 개별의 IIoT 가 설치되어 있다. 이러한 상황을 추상화 하면 ②와 같은 형태가

된다. ② 형태에서 토폴로지 구성에 따라 연결하면 ③과 같은 형태가 될 수 있다. ①의 상단 중간 노드에 연결된 IIoT 중 마지막 개체가 위 변조된 것이라면, 실제 토폴로지의 그래프는 ③형태가 된다. 이러한 구성방법을 기반으로 설치된 IIoT 위 변조 등의 탐지를 위하여, 기존의 시스템에 저장된 연결 설정 파일과 로그파일을 기반으로 Iao 에 설계된 프로토콜을 분석하여 허용되는 메시지를 주고 받음으로써, 실제 IIoT 에 대한 확인을 실행한다. 프로토콜은 Modbus, Profinet, Ethernet/IP 에 대한 특성에 따라 국내에 다수 설치되고 있으며 대규모 메시지 전송을 실행할 수 있는 MQTT 프로토콜을 응용한다.

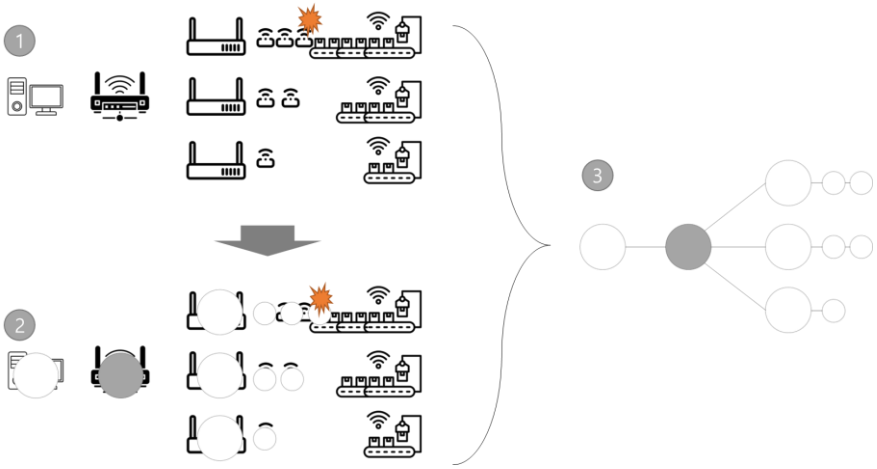

Figure 2. IIoT Topology Generation Procedure and Method based on Industrial Network Protocol
그림 2. 산업 네트워크 프로토콜 기반 IIoT 토폴로지 제네레이션 절차 및 방법

3.2 제네레이터 프로토타입 구현

개념적으로 설계된 산업 네트워크 프토토콜 기반 IIoT 토폴로지 생성을 위하여 기존의 연결 IIoT 의 실체 확인을 위하여 IIoT 에 대한 연결현황 파일(ini)을 기본적으로 저장하고, 비교 인자로 활용한다. main 에서 control 메소드를 이용하여 ini 에 등록되어 있는 IP 체계의 IIoT 를 대상으로 프로토콜 통신을 통하여 Message Call Back 이 일어나는지 정보를 송출한다. 등록되어 있는 IIoT 를 대상으로 연결 현황을 모두 확인하면, 중간 허브를 기반으로 Tree 구조를 그린다. 절차에 대한 토폴로지 생성 시퀀스 다이어그램을 표현하면 그림 3 과 같이 나타난다. 이러한 과정에서 ini 파일을 기반으로 실제 통신이 되는 IIoT 에 대해서는 실체성을 확인할 수 있으며, 연결이 되지 않는 IIoT 에 대해서는 위변조된 상태 또는 고장상태로 파악할 수 있다. 따라서, 현재 IIoT 에 대한 실질적인 현황과 구조를 획득함으로써 스마트팩토리 IIoT 에 대한 무해화 환경을 달성할 수 있게 된다.

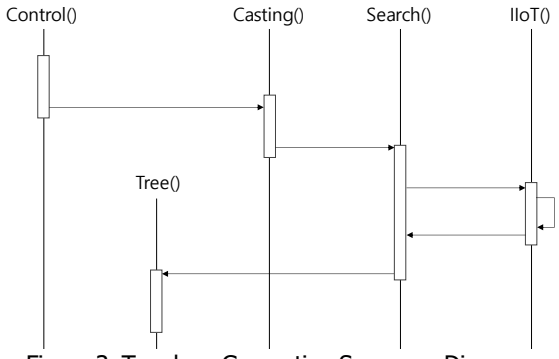

Figure 3. Topology Generation Sequence Diagram
그림 3. 토폴로지 생성 시퀀스 다이어그램

Table 1. Core Source Code for Prototype Implementation
표 1. 프로토타입 구현을 위한 핵심 소스코드

```
void Casting() {
        EthernetClient client_IIoT = server.available() ;
        if(client_IIoT) {
                while (client_IIoT.connected()) {
                        if (client_IIoT.available()) {
                                char c = client_IIoT.read() ;
```

표 1 을 포함하여 IIoT 와의 커넥션을 확보하고, 연결성을 ini 와 비교하여 토폴로지 형태에 대하여 개념적으로 나타내면 그림 4 와 같은 형태로 출력된다.

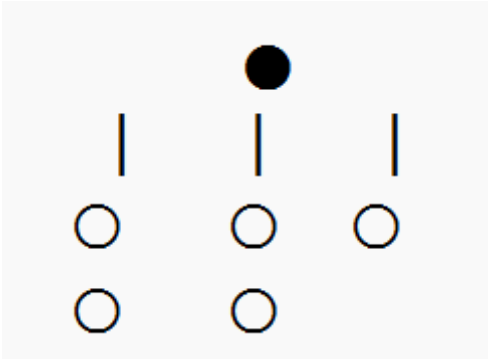

Figure 4. Results of IIoT Topology Generation
그림 4. IIoT 토폴로지 생성 결과

IV. 결론

제조업의 스마트팩토리는 맞춤형 생산을 위한 광범위한 데이터의 수집과 제어를 실행할 수 있는 IIoT 를 핵심기술로 적용 · 구축함으로써 고품질 생산으로 이어지고 있다. 정책적으로 기존의 자동화 공정 중심의 제조업에서 수준별 맞춤형 스마트 팩토리로 전환을 위하여 5 단계로 구분된 특징을 제시하고 있으나, 정부의 지원을 받아 구축하게 된 스마트팩토리의 다수는 고 수준에 이르지 못한 취약점을 내포하고 있다. 이에 따라, 실질적으로 스마트팩토리 구축의 핵심이 되는 IIoT 의 도입은 보안적 위험을 갖게 되었다. IIoT 를 통하여 개방형으로 전환된 스마트팩토리의 네트워크 환경은 네트워크를 통한 장비, 장치 SW 업데이트로 악성코드의 침입에 대한 민감성이 증가하고 있는 상황이다. 이러한 상황에서 악성코드에 감염된 IIoT 는 제조공정에 연쇄적인 문제를 갖는 보안 사고를 발생시키고, 생산 제품, 생산 공정의 보안 침해를 통한 품질저하로 기업의 비즈니스에 신뢰성에 문제를 발생시킨다. 안전하지 않은 네트워크 서비스, 안전한 업데이트 메커니즘 부재, 오래된 구성요소 사용, 디바이스 관리 부재 등의 IIoT 의 취약점으로 인하여 필수불가결한 요소이지만, 보안 침해에 따라 IIoT 는 네트워크 망의 교란, 위 변조된 IIoT 의 사용 및 유지로 인하여 생산성 저하를 발생시킬 수 있다. 이에 따라 본 연구에서는 스마트팩토리 초기 구축 시 IIoT 의 안전한 연결 및 활용을 위하여 스마트팩토리에 연결된 IIoT 에 대한 실질성 확인과 무해화 환경 구축을 실행할 수 있는 방법으로 IIoT 연결 상황을 확인할 수 있는 연구를 실행하였다.

본 연구는 두 가지 기여에 대해 정리할 수 있다. 첫 번째, 제조업의 생산공장에서 정보화 수준 단계에서 스마트팩토리 구축을 위한 초기단계 진입 시 보안적 유의사항을 맞춤형으로 확인할 수 있다. 두 번째, 스마트팩토리 구축 후 보안위험에 따른 침해 발생 이후에도 IIoT 연결성을 검토하여 침해상황을 확인할 수 있는 기술적 토대를 마련하였다.

향후 연구로는 스마트팩토리에 대하여 보안 침해상황을 자동으로 확인할 수 있는 알고리즘에 대하여 연구하고자 한다.

V. 감사의 글

본 논문은 2022 년도 신한대학교 학술연구비 지원으로 연구되었음.

VI. 참고문헌

[1] Korea IR Service, “Smart Factory Solution,” Innovative Growth, 2021-6
[2] Y. H. Woo, H. Y. Kwon, “Study on the Security R&R of OT-IT for Control System Network Boundaries,” Journal of Information Technology Services, Vol. 19, No. 5, pp.33-47. 2020.
[3] J. P. Jung, ″Smart Factory Core Technology and Manufacturing Innovation Advancement Strategy″, Convergence Research Review, Vol. 6, pp. 3-26, 2020.
[4] H. J. Kim, J. Y. Kim and J. R. Paik, ″Analysis of Security Attacks and Design of Defense Strategies Found in Smart Factory″, Proceedings of the Korean Society of Computer Information Conference, Vol 26. No.2, pp. 161-164, 2018.
[5] C. G Yoo, “Low Growth Rate cannot defeat Economic Democracy”, Journal of Korean Social Trend and Perspective, No. 97, pp. 213-253, 2016
[6] S. C. Oh and Y. H. Ahn, “A Study on the Diagnosis Measurement for the Smart Factory Level in the 4th Industrial Revolution,” Korea Logistics Review, Vol. 29, No. 6, pp. 149-162. 2019
[7] H. B. Chang, “A Study on IT Security Strategy for Industrial Technology Security” Korean Journal of Industrial Security, Vol. 2, No. 1, pp. 91-107. 2011.
[8] Y. S. Jung, Y. T. Kim and G. C. Park, “Designing an Automated Production Information Platform for Small and Medium-sized Businesses,” Journal of Convergence for Information Technology, Vol. 9, No. 1, pp. 116-122, 2019.
[9] K. W. Cho, M. H. Jeon and C. H. Oh, “Development of Equipment Control System based on DB Access Method for Industrial IoT,” Journal of the Korea Institute of Information and Communication Engineering, Vol. 20, No. 6, pp. 1142-1147, 2016.
[10] J. S. Han and J. S. Yoo, “Design and Implementation of Modbus Communications for Smart Factory PLC Data Collection,” The Journal of the Korea Contents Association, Vol. 21, No. 4, pp. 77-87, 2021.
[11] Maggi, F., Balduzzi, M., Vosseler, R., Rösler, M., Quadrini, W., Tavola, G., Marcello, P., Davide, Q., & Zanero, S. Smart factory security: A case study on a modular smart manufacturing system. Procedia Computer Science, Vol. 180, pp. 666-675, 2021

저자소개

김양훈 (*Yanghoon Kim*)

2007 년 : 대진대학교 컴퓨터공학과(공학석사)
2011 년 : 대진대학교 컴퓨터공학과 소프트웨어공학 전공(공학박사)
현재: 신한대학교 사이버드론봇군사학과 부교수

관심분야 : 산업보안, 융합보안, 드론, 스마트팩토리