이 일 구 교수 지도

석사학위 청구논문

고신뢰 OT 시스템을 위한 데이터 중심의 네트워크 기반 보안 메커니즘

2024

성신여자대학교 일반대학원

미래융합기술공학과

문 정 현

고신뢰 OT 시스템을 위한 데이터 중심의 네트워크 기반 보안 메커니즘

이 일 구 교수 지도

이 논문을 석사학위논문으로 제출함

2023년 11월

성신여자대학교 일반대학원
미래융합기술공학과
문 정 현

인 준 서

문정현의 석사학위 논문으로 인준함

2023년 11월

심사위원장 김 성 민 (서명 또는 인)

심 사 위 원 이 일 구 (서명 또는 인)

심 사 위 원 임 연 섭 (서명 또는 인)

성신여자대학교 일반대학원

논문개요

기술 발전과 함께 데이터의 가치가 높아지며 다양한 산업의 중요 자산으로 부상함에 따라, 데이터 관리 및 처리의 중요성이 커지고 있다. 데이터 분석을 통해 정보를 생산하는 등 활용이 확대되고, 사이버 공격 역시 지능화되어 데이터를 대상으로 한 보안과 프라이버시에 대한 강화의 필요성이 증가하고 있다. 이에 따라, 산업 기밀을 보호하고 데이터를 효과적으로 관리하는 것이 중요하며, 신뢰할 수 있는 시스템을 위한 데이터 보안 메커니즘에 연구의 필요성이 요구되고 있다. 특히 운영 기술(Operational Technology, OT) 시스템은 정보 기술(Information Technology, IT)과 융합되면서 새로운 보안 이슈가 발생하고 있으며 이에 대응하기 위한 현대적인 보안 체계가 필요하다.

본 논문은 OT 시스템의 산업적 특성과 이로 인한 보안의 취약성을 분석한다. OT 산업 보안 현황과 OT 산업의 디지털화로 인한 피해 사례들을 분석하여 산업보안 강화의 중요성을 강조한다. OT 시스템이 공격받더라도 데이터 무결성을 보장하여 높은 신뢰도 바탕으로 OT 보안이 가능한 데이터 중심의 두 가지 보안 메커니즘을 제안한다. 에어갭(Air gap) 기반의 보안 내재화 방안을 적용한 이상 징후 탐지 시스템은 공격 행위에 따른 센서 데이터 변화를 통해 악성 행위 탐지가 가능함을 확인했다. 또한, In-network computing 기법을 OT 시스템에 적용한 INCOS(In-Network Computing base Operational technology System)는 데이터 프라이버시를 제공함에도 OT 문제 상황을 효과적으로 대응할 수 있다. 실험을 통해 테스트 정확도는 98.33%, 검증 정확도는 98.89%의 결과로 모델의 일반화가 이루어짐을 확인하고, 분류 보고서를 통해 일반 상황에서는 96%, 위험 상황에서는 98% 이상의 정밀도를 보여 모델이 OT 환경에서 발생할 수 있는 danger, fire, gas, non, tsunami 5가지 위험 상황에 대해 정확하고 일정한 성능을 보이고 있음을 입증하였다.

목 차

표 차 례

그림 차례

Ⅰ. 서 론

디지털 전환의 가속화와 기술의 발달로 인해 데이터가 폭발적으로 증가하고 있다. 4차 산업혁명의 핵심인 인공지능, 빅데이터, 사물인터넷(Internet of Things, IoT), 클라우드 등의 기술이 전통적인 산업과 융합되어 데이터 활용이 향상되고 있다. 장치의 긴 수명주기와 높은 가용성을 특징으로 하는 운영 기술(Operational Technology, OT)은 정보 기술(Information Technology, IT)과의 결합으로 인해 확대된 보안 및 프라이버시 문제를 해결해야 한다. OT 시스템은 제조, 교통, 에너지 분야 등에서 중요한 기능을 수행하고 있지만, 보안 솔루션을 적용하는 과정에서 변화에 저항성이 강해 기술 도입에 제약이 있다. 특히, 보안 패치의 어려움과 장치 간 상호 운용성 문제로 인해 기술적 취약점이 존재하며, 이를 노린 사이버 공격이 증가하고 있다. 이는 단순한 기술적 문제를 넘어 산업의 안정성과 국가 안보에까지 중요한 영향을 미치고 있다. 본 논문은 OT 시스템의 보안 취약점을 파악하고, 현대 산업 환경 데이터를 활용하여 환경에 적합한 보안 체계를 제안하여, OT 시스템의 보안 위협을 해결하고 데이터의 무결성을 유지하는 두 가지 새로운 방법론을 제안한다.

첫째, 노후화되고 다양한 프로토콜을 사용하는 OT 시스템의 보안 문제를 해결하기 위해 보안 내재화 중심의 강화 방안을 도입하고자 기술적, 법적, 관리적 방안을 제시한다. 특히, 에어갭(Air gap) 기반의 이상 징후 탐지 시스템은 데이터의 변화를 통해 이상 징후를 식별하여 보안 위협에 신속하게 대응할 수 있도록 설계하였다. 이를 통해 기존 시스템의 한계를 극복하고, 보안 기능을 시스템 설계에 내재화함으로써 OT 시스템의 취약점을 감소시킨다. 이로 인해 OT 시스템이 IT와의 융합 과정에서 발생할 수 있는 다양한 보안 위협에 효과적으로 대응할 수 있다.

둘째, OT 시스템의 보안 강화를 위한 INCOS(In-Network Computing based Operational technology System)를 제안한다. 높은 공격 표면을 가진 OT 시스템의 피해를 줄이기 위해, In-network computing 기술을 활용함으로써 중앙 서버로의 데이터 전송을 최소화한다. 이를 통해 데이터 처리의 효율성을 높이고, 보안성은 강화한다. 변화의 저항성이 높은 산업 환경의 특성을 고려하여 기존 시스템의 한계를 극복하는 방안을 제시함으로써 고신뢰 OT 시스템 구축에 기여한다.

본 논문은 2개의 PART로 구성된다. Ⅱ절 PART 1에서는 OT 보안 취약점과 산업보안 관련 정책을 분석하고, 보안 내재화 중심의 기술적, 법적, 관리적 OT 산업보안 강화 방안을 제안한다. Ⅲ절 PART 2에서는 기존 레거시 OT 산업의 문제점을 분석하고, In-network computing 기반 OT System 메커니즘에 대해 설명한다. 마지막으로 Ⅳ절에서는 두 연구를 요약하고 논문을 마무리한다.

Ⅱ. PART 1: 보안 내재화 중심의 OT 산업보안 강화 방안

1. 서론

4차 산업 혁명 시대가 도래함에 따라 인공지능, 빅데이터, IoT, 로봇 등의 최첨단 IT 기술이 OT 산업과 융합하면서 종래의 산업과 사회의 핵심 가치가 '노동, 자본' 중심에서 '데이터, 기술' 중심으로 변화되고 있다. OT는 산업 장비, 자산, 프로세스 및 이벤트를 직접 모니터링하거나 제어하는 하드웨어와 소프트웨어를 통칭한다[1]. OT는 미국 중심의 스마트 제조와 독일 중심의 스마트팩토리 개념에서 발전했으며, COVID 19 팬데믹 이후 가속화된 디지털 전환으로 인해 OT와 IT 네트워크 간의 융합이 촉진됨에 따라 산업 시장이 확대되었다. OT 산업을 포함한 글로벌 산업형 사이버 보안 시장 규모가 2020년 33억 달러에서 2025년 102억 달러, 연평균 성장률이 약 25.3%인 것이 이를 증명한다[2].

이러한 산업과 경제의 성장과 함께 산업보안의 개념이 OT 보안으로 발전하여 새로운 보안 시스템 구축에 대한 요구로 이어지고 있다. 산업보안은 산업 활동에 유용한 정보, 인원, 문서, 시설, 자재를 산업 스파이나 경쟁 관계에 있는 대상에게 침해당하지 않도록 보호하고 관리하는 활동을 의미한다. 전통적인 산업보안이 기술 및 정보 유출 방지에 초점을 맞췄다면, OT 보안은 테러, 해킹, 안전사고, 재해로 인한 산업적 손실이 발생하는 것을 최소화하는 비즈니스와 산업 운영의 연속성에 초점 맞춘다. 즉, 산업보안은 정보 유출 방지와 정보의 기밀성을 가장 중시하고, OT 보안은 연속적인 운영과 정보의 가용성을 가장 중시하는 차이점이 있다[3].

과거에는 여러 위치에 분산되어 완전히 격리된 상태로 작동하던 OT 시스템이 점차 IT 망과 연결되어 운용되면서 보안 취약성이 커지고 있다[1]. 그

림 1은 이러한 OT 네트워크와 외부 네트워크 간 연결되어 운용되는 OT 시스템 연결 유형의 변화를 보여준다[4]. 이와 같은 산업시설의 스마트화는 원격 유지보수 및 데이터 분석을 통한 운영 환경 개선을 가능하게 하지만, 동시에 OT 인프라에 대한 운영 리스크를 증가시킨다. IT 망의 취약성에서 비롯된 대표적인 OT 피해 사례는 2019년 대만의 반도체 기업인 TSMC의 랜섬웨어 감염 사고다. 이 사고로 인해 약 48시간 동안 공장 가동이 중단되었고, 이로 인해 약 3천억 원의 손해를 입었다. 또한, 지난 2021년 5월 미국의 송유관 운영업체 콜로니얼 파이프라인이 랜섬웨어 공격을 당해 미국 동부지역의 석유 공급이 중단되는 사고가 발생했다. 해당 업체는 랜섬웨어로 암호화된 정보 복구를 위해 사이버 범죄 조직에 5백만 달러를 지불했다. 과거에는 OT 보안사고의 결과로 사이버 공간에서의 정보 유출에 그쳤지만, 현재는 물리적 공간의 기반 시설·산업현장·공공인프라 중단과 대규모 피해로 이어져 재산과 안전을 위협함에 따라 OT 산업보안 강화의 필요성이 강조되고 있다.

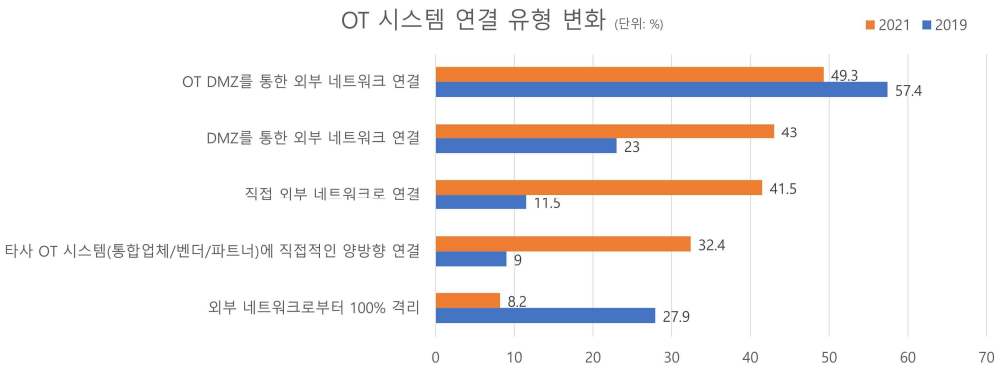

FIGURE 1. OT System 연결 유형 변화

2021년 상반기 보안 트렌드 보고서에 따르면, 공공·정부, 의료, 교육, 금융 등을 포함하는 산업군 중 제조업에서 침해사고 발생비율이 29.5%로 가장 높았다[5]. 한국은 국내총생산(Gross Domestic Product, GDP) 대비 제조업 비중이 30% 수준으로 주요국 중 가장 높다[6]. 이러한 OT 보안사고

의 특성과 국내 산업에서 차지하는 OT 중요성을 고려하면, 국가 경쟁력 제고를 위한 효과적인 OT 보안 체계 구축이 시급하다.

본 연구에서는 앞서 살펴본 OT 산업의 특성을 기반으로 효과적인 OT 보안 체계 구축을 위해 OT 산업이 지니는 주요 보안 취약점과 OT 산업보안 관련 정책을 분석한다. 그리고 보안 내재화를 중심으로 데이터 기반의 OT 산업기술 보호 방안을 제안하고 OT 산업보안 강화를 위한 제도를 제안한다. 본 논문의 2장에서는 OT 보안 취약점을 분석한 내용을 바탕으로 OT 산업의 기술적 보안 이슈를 도출하고, 3장에서는 OT 산업보안 관련 정책을 분석함으로써 현 법제의 한계점과 이에 대한 대응 방안을 제시한다. 4장에서는 OT 산업의 기술 보호를 위한 방안을 기술적, 법적, 관리적 관점에서 검토하고, 마지막으로 5장에서는 결론을 맺으며 향후 연구 방향에 대해 논한다.

2. OT/ICS 보안 강화 방안 선행 연구

본 장에서는 OT/ICS(Industrial Control System) 보안 강화를 위한 선행 연구를 분석한다. OT와 IT의 결합으로 인해 OT/ICS Security는 새로운 보안 위협을 고려해야 하며, 표 1은 선행 연구의 제안 방법과 한계점을 요약한 표이다.

Zahra Jadidi 외 1인[7]은 산업 제어 시스템을 위한 위협 사냥 프레임워크인 ICS-THF(Industrial Control System Threat Hunting Framework)를 제안했다. ICS-THF는 위협 사냥 트리거(Threat hunting triggers), 위협 사냥(Threat hunting), 사이버 위협 인텔리전스(Cyber threat intelligence)의 세 단계로 구성된다. 이를 통해 식별, 행동 예측 및 검증, 향후 활용할 지표를 생성함으로써 산업 제어 시스템의 엔드포인트에서 선제적으로 사이버 위협을 탐지하고 대응할 수 있다. 그러나 ICS-THF는 가설 검증과 위협에 대한 정보 수집 과정이 수동적으로 이루어지기 때문에, 시스템의 확장 가능성과 운영 효율성에 제약이 있다. Akashdeep Bhardwaj 외 4인[8]은 시그니처 기반 보안 도구와 같은 전통적인 위협 탐지 방법들이 알려지지 않은 사이버 공격에 대응할 수 있도록 하고, 산업 제어 시스템에서의 행동 기반 공격을 실시간으로 탐지하고자 CTI(Capturing-the-Invisible) 알고리즘을 제안하였다. CTI는 장치 로그를 이벤트 로그로 변환하여 산업 제어 시스템의 로그 데이터를 분석한다. 이때, 이벤트의 고유한 쌍을 찾아 추적하며 정상적인 활동과 구별되는 숨겨진 프로세스를 식별한다. 실험을 통해 종래 사용되는 프로세스 검색 알고리즘 대비 시간, 적합성 검사 등에서 더 나은 결과를 입증하였다. 그러나, 제안 방법은 데이터 무결성에 문제가 생길 경우 공격 탐지의 정확도가 저하될 수 있다. Kelei Miao 외 2인[9]은 산업 제어 시스템에서의 방어 전략 설계 용이성을 위해 두 가지 공격 신호 추정기를 제안하였다. 허위 데이터 주입 공격을 실시간으로 추정하기 위해 LASE(Linear Attack Signal

TABLE I

OT/ICS 보안 강화 방안 선행 연구

Category	Refs	Method	Limitation
OT/ICS Security	[7]	- MITRE ATT&CK 매트릭스와 다이아몬드 모델을 통합한 ICS-THF로 초기 탐지 효과를 입증함	- 수동 작업이 포함되어 있어 확장성과 운용성에 제약이 있음
	[8]	- 산업용 제어 장치 로그를 바탕으로 경고 ID 없이 공격을 탐지하는 알고리즘을 제안함 - 숨겨진 작업과 행동 기반 사이버 공격을 효율적으로 탐지함	- 데이터 무결성이 깨질 경우 탐지의 정확도에 영향을 미칠 수 있음
	[9]	- 방어 전략 설계 용이성을 위해 허위 데이터 주입 공격 신호의 파형을 선형 및 비선형으로 추정하는 LASE와 NASE를 제안함	- 대규모 OT 시스템 적용 시 확장성 및 연산 효율성의 문제, 고도화된 공격에 대응 어려움
	[10]	- 개발한 키트를 통해 생성된 데이터로 도메인 이상 탐지를 평가함 - 다양한 시나리오 모사가 가능하여 제한적이었던 OT/ICS 연구가 가능함	- 광범위한 산업 특성으로 인해 범용적인 실험 환경 구축은 어려움

Estimator)는 선형, NASE(Nonlinear Attack Signal Estimator)는 복잡한 공격 패턴과 광범위한 산업 제어 시스템에서의 공격을 추정하기 위해 비선형 접근을 사용하는 방법을 사용하였다. 실험을 통해 추정기가 효율적이며, 추정

기의 성능에 공격 신호의 빈도가 영향을 주는 것을 확인하였다. 그러나, 제안 방법은 확장성과 연산 효율성의 한계로 인해 실제 대규모 OT 시스템에 적용이 어렵다. 또한, 사이버 위협이 고도화되고 있어, 새롭고 복잡한 공격 유형에 대응하기 어려울 수 있다. S Mubarak 외 6인[10]은 산업 제어 시스템의 공격 탐지 향상을 위해 기존 연구 환경의 한계를 인지하고, 이를 해결하기 위한 새로운 테스트 키트를 제시한다. 키트를 활용하여 생성된 데이터를 바탕으로 기계 학습 기법을 사용하여 도메인 이상 탐지를 평가하였으며, 이외에도 일반적인 OT 트래픽과 다양한 공격 시나리오를 모사하는 데이터를 생성할 수 있다. 이를 통해 기존에 제한적이었던 OT/ICS 연구의 활성화에 기여하였다. 그러나 OT 산업의 광범위한 특성으로 인해 범용적인 실험 환경을 구축하는 것은 어려운 한계점이 있다.

3. OT 보안 취약점 분석

OT 보안은 전반적인 산업 운영 기술 환경을 보호하는 행위 및 체계를 포함한다. 본 장에서는 OT 장비의 구조 및 프로토콜을 분석한 후, 이를 기반으로 보안 취약점을 분석한다. 또한, 주요 OT 기술 표준 및 OT 보안사고 사례와 그에 따른 대응 현황을 검토하여 OT 장비의 기술적 보안 이슈를 도출하였다.

1) OT 장비 구조

① OT 계층 구조

OT 보안 전략을 수립하기 위해서는 OT 환경 구조에 대한 이해가 수반되어야 한다. 한국인터넷진흥원의 '스마트공장 계층 구조 아키텍처'에 따르면, 스마트팩토리는 0계층부터 5계층까지 6개 계층으로 나뉘며 0~3.5 계층까지 OT 망에 해당한다. 표 2는 계층별 주요 OT 장비의 주요 구성요소의 종류와 기능을 보여준다[11].

② OT 장비 프로토콜

그림 2와 같이 OT 산업용 네트워크 프로토콜은 단일 표준이 아니라 다양한 OT와 ICS 프로토콜이 활용되고 있다[12]. 문제는 프로토콜별로 요구하는 보안 패치 요구사항이 다르므로 신속한 보안 대응이 어렵다는 점이다. 또한, 기타로 분류된 항목들이 포함하는 종래의 OT와 ICS 네트워크 프로토콜은 암호화를 하지 않거나 인증을 생략하는 경우가 많다. 그리고 윈도우XP 또는 윈도우7과 같이 제조사의 지원이 종료된 운용 체계가 사용되고 있다. 이러한 레거시 시스템은 업데이트 및 패치를 지원하지 않기 때문에 새롭게 발견된 취약점에 대응할 수 없다[13]. 2020년 플로리다 수질 처리 시스템 보안사고는 구버전의 운영체제를 SCADA 시스템에 사용해서 발생한 대표적인 피해 사

TABLE II

OT 환경 계층별 주요 OT 장비

계층	구분	주요 구성요소		설명
0	제어망 (OT)	센서	계측 센서	현장에서 작업을 수행하는 설비
			안전 센서	
			스마트 센서	
		액츄에이터	제어 장치	
			개폐 장치	
			변환 장치	
		로봇		
		생산장비		
1		PLC(Programmable Logic C Controller)		현장 설비에 명령을 내리고 통제
		RTU(Remote Terminal Unit)		
		DCS(Distributed Control System)		
		DAQ(Data Acquisition)		
		IED(Intelligent Electronic Device)		
		Micro Controller		
2		SCADA(Supervisory Control and Data Acquisition)		현장 설비를 원격 관리하고 운영하는 시스템
		HMI(Human Machine Interface)		
		Mobile		
3	운영망 (OT)	MES(Manufacturing Execution System)		전체적인 생산 체계 관리 및 운영
		PLM(Product Lifecycle Management)		
		RTD(Real Time Dispatcher)		
		Historian		
		FEMS(Factory Energy Management System)		
4~5	IT망	ERP(Enterprise Resource Planning)		공정과 관련된 전사적 비즈니스 관리
		SCM(Supply Chain Management)		
		CRM(Customer Relationship Management)		
		그룹웨어		

레이다. 이 SCADA 시스템은 지난 2020년 1월 14일 이후부터 업데이트를 중단한 윈도우7 운영체제의 32비트 버전을 사용했으며, 원격 접속을 위해 동일

한 암호를 공유하고 방화벽 보호 기능이 설치되지 않은 상태였던 것으로 보고되었다. 이렇듯 제조설비 업체가 OT 보안 업체의 권고에도 불구하고 노후화된 장비들을 지속해서 사용하는 이유는 공장의 가동이 제조설비 업체의 수익과 직결되는 가용성 때문이다. OT 산업의 가용성으로 인한 신속한 보안 취약점 패치의 어려움은 OT 산업보안을 약화시키는 원인이다. 그러므로 버전과 종류에 상관없이 가용성을 해치지 않으면서 OT 보안을 강화할 수 있는 솔루션이 요구된다.

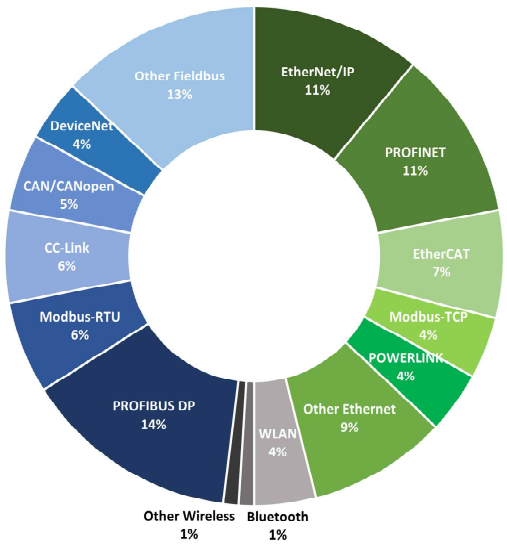

FIGURE 2. 산업용 네트워크 프로토콜 시장 점유율

2) OT 보안 이슈 분석

① OT 보안 위협 분석 및 보안 요구사항

본 장에서는 ICS를 위한 MITRE ATT&CK 프레임워크를 기반으로 OT 보안 장비의 취약점을 분석한다. 이 프레임워크는 산업제어 시스템의 특성상 발생할 수 있는 재산적 피해와 인적 피해를 고려하여 시스템의 가용성 측면을 중심으로 설계되었다[14]. 해당 프레임워크의 ATT&CK for ICS는 12개의 공격 전략(Tactic)과 88개의 공격 기술(Technique)로 구성되어있다.

이때 공격 전략은 공격자의 공격 목표에 따른 행동을 의미하며, 공격 기술은 공격자가 목표에 대한 공격 전략을 달성하는 방법을 나타낸다. 공격 기술은 공격자의 공격을 통해 발생하는 피해를 명시하고 있으며, 앞서 분류된 공격 전략에 따라 다수의 공격 기술이 존재할 수 있다. 이를 통해 보안 공격에 활용되는 공격 기술을 가시화할 수 있으며, 침해사고 대응체계 구축을 돕는다. 그림 3은 이란 원자력발전소 해킹 사건의 원인이었던 스턱스넷 악성코드 공격 구조도이다. 웜 바이러스인 스턱스넷은 USB를 통한 개인 PC 감염을 통해 시작되었다. 이후 공유 폴더와 취약점으로 인해 내부 네트워크로 바이러스가 전파되었으며, 관리자 PC가 감염됨에 따라 대규모 산업 장비 피해가 발생했다. 해당 그림을 통해 OT 보안 사고는 타겟 산업 장비를 대상으로 한 감염이 단계적으로 이루어짐을 확인할 수 있다. 이처럼 대규모의 OT 보안 사고는 여러 단계를 걸쳐 수행되기 때문에 표 3의 MITRE ATT&CK for ICS 전략들을 각 단계에 대응시킴으로써 공격 현황을 구체화하고 신속하게 대응할 수 있다.

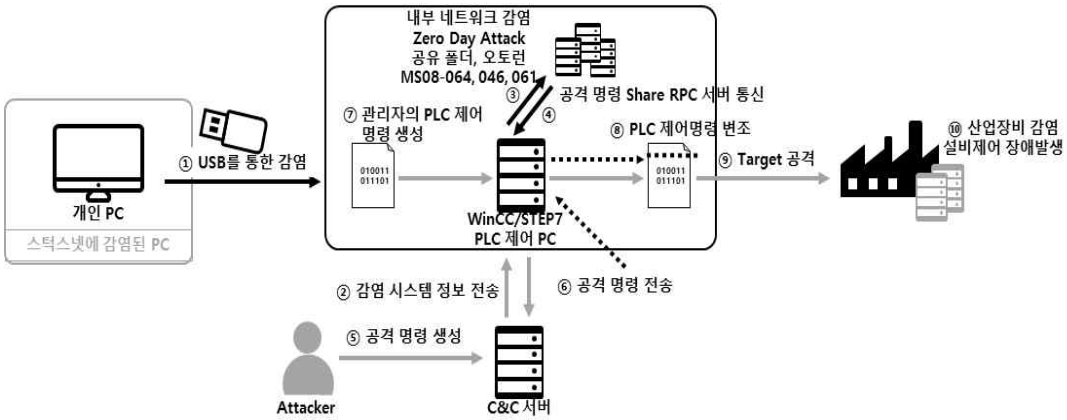

FIGURE 3. 스턱스넷 악성코드 공격 구조도

상술한 MITRE ATT&CK 프레임워크 이외에 NIST 800-82, IEC 62443-4-2 외 주요정보통신기반시설 기술적 취약점 분석·평가, TTA 표준

TABLE III
MITRE ATT&CK for ICS tactics

공격 전략 (Tactic)	특징	공격 기술 (Technique) 특징
최초 침투 (Initial Access)	- 여러 시스템, 장치 및 계정에 대하여 경유 시스템을 이용하여 목적 시스템을 공격하는 기법인 피봇팅(Pivoting)을 수행 - 운영 기술 자산, OT 네트워크의 IT 리소스, 외부 원격 서비스 및 웹사이트 등을 진입 벡터로 활용	- 표적 공격(전략적 웹 침해, 워터링 홀 공격) 수행 - 소프트웨어 취약점으로 인한 IT 네트워크에서 산업 네트워크로의 확산 ex) SMBv1을 대상으로 한 MS17-010
악성코드 실행 (Execution)	- 공격자가 원격 시스템 또는 로컬을 통해 악성코드나 프로그램을 임의로 실행하기 위한 전술 - 권한상승, 발견 등의 공격 전략과 결합되어 활용	- 지정된 동작에 따라 작동하는 실행 파일 및 악성 파일로 원격 대상을 감염 - 악성코드 실행을 통한 제어 장치 동작을 제어

지속성 유지 (Persistence)	- 공격자가 ICS 네트워크 환경에 침입한 후 지속적으로 접속 유지를 위한 전술 - OT 장비를 대상으로 한 사이버공격은 APT (Advanced Persistent Threat) 공격의 형태로 이루어지는 경우가 많기에 지속성 유지가 중요	- 제어 장치에 대한 관리자 접근 권한 확보 - 제어 시스템 장치 내 모듈식 하드웨어 장치를 대상으로 감염 및 악성파일 업로드
권한 상승 (Privilege Escalation)	- 공격자가 ICS 네트워크에 침입하여 시스템의 높은 권한을 얻는 전술 - 시스템 약점, 잘못된 설정 및 취약점을 이용함으로써 이루어짐	- 소프트웨어 취약점 악용 및 IAT(Import Address Table) 후킹을 통한 함수 호출 리디렉션 - 상위 엔드포인트 시스템 손상으로 이어질 수 있음
회피 (Evasion)	- 공격자가 침입한 시간 동안 탐지되는 것을 피하고자 사용되는 전술 - 공격자는 신뢰할 수 있는 장치와 프로세스를 활용 및 악용함으로써 활동을 숨길 수 있음	- 탐지 회피를 통해 추가 접근 권한 획득 및 메시지 스푸핑, 프로세스 제어 손상

발견 (Discovery)	- 공격자가 ICS의 원격 시스템에 접근한 후 목표물을 평가하고 식별하기 위한 정보를 찾기 위해 사용되는 전술	- 공격자가 ICS의 원격 시스템에 접근한 후 목표물을 평가하고 식별하기 위한 정보를 찾기 위해 사용되는 전술
시스템 내부 이동 (Lateral Movement)	- 공격자가 ICS의 원격 시스템에 접근한 후 제어하는 전술 - 여러 시스템, 장치 및 계정에 대하여 경유 시스템을 이용하여 목적 시스템을 공격하는 기법인 피봇팅을 수행	- IT 및 OT 네트워크로의 확산을 통한 피해 규모 확대
시스템 내부 이동 (Lateral Movement)	- 공격자가 목표 대상의 시스템 정보와 데이터를 수집하는 전술	- 제어 장치에 대한 OPC 프로토콜 정보, 컨트롤러의 작동정보, 물리적 프로세스에 대한 정보 수집 - 제어 장치를 대상으로 한 표적 공격으로 이어짐
명령 및 제어 (Command and Control)	- 공격자가 ICS 네트워크와 시스템에 침입하여 컨트롤러 및 플랫폼을 제어하려는 전술	- 공격자가 ICS 네트워크와 시스템에 침입하여 컨트롤러 및 플랫폼을 제어하려는 전술

안전 장치 억제 (Inhibit Response Function)	- 사용자가 안전과 관련된 기능에 대해 대응하지 못하도록 하는 전술 - 장비 파괴, 작업자 개입 기능 제한, 인적 피해 등을 포함(능동적 억제)	- 제어시스템 공격에 대한 경보 기능을 무력화 및 악용함으로써 사용자의 공격 대응 저해
공정 제어 손상 (Impair Process Control)	- 공격자가 제어 절차를 물리적으로 손상하거나 비활성화하는 전술 - 물리적 환경을 조작하는 활성 절차 또는 매개변수, 제어 논리 조작, 프로세스 결과 난독화 등을 포함	- 물리적 제어를 통한 제어 장비 운영자와 하위 사용자의 안전 위협
시스템 충격 (Impact)	- 공격자가 ICS의 데이터 조작하거나 시스템을 중단 및 파괴하려는 전술 - 즉각적인 중단뿐만 아니라 장기적인 손상 및 손실도 포함	- 생산성 및 수익 손실, 운영 정보 유출 및 재산 피해 - 제어 장비에 대한 운영자의 가용성, 가시성 저해

산업제어시스템 보안요구사항 등 다양한 산업제어시스템 보안 표준이 존재한다. NIST 800-82는 산업제어시스템의 안전, 신뢰성, 성능 요구사항과 보안 가이드를 제공한다. 해당 표준은 외부 원격접속 보안, 사용자 정책 기반 차세대 방화벽(NGFW), 미러링 모드 네트워크 침입탐지시스템(IDS), 통합 로깅 및 로그 수집의 네 가지를 기본 보안요건으로 제시한다. 또한, IT 시스템과 비교하여 산업 제어시스템이 가지고 있는 취약성과 위험 요소를 도출하여 산업제어시스템을 보호하기 위한 기술과 대응책을 제공한다[15]. IEC 62443-4-2는 제어시스템을 구성하는 네 종류의 구성요소(호스트 디바이스,

소프트웨어 애플리케이션, 임베디드 디바이스, 네트워크 디바이스)의 보안 기능 수준을 정의한 문서이다. IEC 62443 전반에 걸쳐 적용되는 기초 보안 요구사항(Foundational Requirement, FR)은 식별 및 인증 제어, 사용 제어, 시스템 무결성, 데이터 기밀성, 제한된 데이터 흐름, 이벤트에 대한 적시 대응, 자원 가용성 요구사항을 규정한다[16].

정부 차원에서도 산업제어시스템 및 산업기반시설에 대한 보안 표준이 제정되고 있다. 해외에서는 ICS 보안에 대한 제도를 정비하고 전담 기관을 중심으로 국가 차원의 산업제어시스템 보안을 강화하고 있다. 미국은「산업제어시스템 기능 향상 법」을 개정하여 산업제어시스템에 대한 연방 차원의 규제를 강화했다. 이를 통해 주요 산업시설에 대해 보안 점검 및 대응 권고에 대한 법적 권한을 확보했다. 일본은 제어시스템 보안검토 위원회를 설립하고, 사회기반시설의 보안 강화를 목적으로 ICS 보안 인증 제도를 추진했다[17]. 중국은 국가산업시설 및 민간 산업시설 전반의 보안 강화를 위해 ICS 보안 전담 정보안전사업연맹을 설립했다.

국내의 경우 행정안전부와 KISA에서 주요정보통신기반시설 대상 취약점 분석 및 평가 가이드를 제시했다. 정보통신기반보호법(제9조) 및 시행령(제17조)에 따라 매년 주요 정보통신기반시설 대상 총 453개 항목의 취약점 분석 및 평가를 시행했다. 특히 ICS 관련 항목은 22개에서 20년 53개로 약 2.5배 증가하였다. 또한, 국가정보원과 국가보안기술연구소의 주도로 산업제어시스템보안에 대한 KS 국가표준을 제정했다. KS X IEC 62443-4-2는 종래의 IEC 62443-4-2를 기반으로 작성되었으며, 국내 제조 환경을 반영하여 산업제어시스템에 요구되는 기술적 보안 요구사항을 정의했다. 이를 통해 공공분야 기반 시설과 민간분야 제조시설에 대한 사이버 공격을 방어하는 데 중요한 기틀을 마련했다.

② OT 보안사고 피해 및 대응

OT 사이버 보안 사고는 2000년대 초 처음 등장했으며, 공격 표적이 개인이나 중소기업 대상 정보 공격에서 주요 기업의 산업제어 시스템 및 국가 기반 시설로 확대되고 있다. 최근 준정부 테러 조직 및 국가 단위의 공격으로 발전함에 따라 사이버 안보 관점에서의 체계적인 대응의 필요성이 증대되고 있다[18]. 또한, OT 사이버 보안 위협이 지능화된 랜섬웨어나 APT 공격을 활용한 공급망 공격과 같은 새로운 지능형 공격에 따른 피해가 증가하고 있다[19]. 이처럼 공격이 지능화되고 고도화되면 산업 피해 규모가 더 커질 것으로 예상된다.

OT 사이버 보안 사고에 따른 피해 비용은 시스템 복구 비용 및 매출이익 손실과 같은 직접적 피해액뿐만 아니라 생산효율 저하, 보안 사고 예방을 위한 비용 투자와 같은 간접적 피해액을 포함한다. 또한, 기업 이미지 손상, 법적 보상비 등으로 인한 잠재적 피해액 역시도 피해 비용 산정에 고려해야 한다. 이러한 OT 보안 위협의 사회·경제적 파급력과 OT 장비의 특징을 고려하여 종래의 정책과 상생할 수 있는 OT 산업보안 강화 방안이 요구되고 있다.

TABLE IV

주요 OT 사이버 보안 사고 분석

구분	원자력 발전소 감염사고(2010)	TSMC 랜섬웨어 감염사고(2018)	Norsk Hydro 랜섬웨어 감염사고(2019)	이란 철도 시스템 해킹(2021)
위험	물리적 시설 파괴	기업활동 중단, 데이터 및 시스템 파괴	기업활동 중단, 데이터 및 시스템 파괴	기반 시설 중단
공격 대상	원자력 발전소	반도체 생산 설비 및 자사 컴퓨터 시스템	서버, PC 등 정보시스템	IT 시스템 및 철도 시스템
침해 내용	웜 바이러스(스턱스넷)가 침투하여 1000여 대 원심분리기 파괴 및 발전소 가동 중지	USB를 이용한 악성코드(워너크라이 변조) 유입	랜섬웨어(록커고가) 변종을 이용한 파일 암호화	해킹집단이 멀웨어 유포하여 시스템 침투
손실 비용	규명되지 않음	약 3000억 원(연 매출 3%)	약 4100만 달러(약 588억) 손실, 주가 3.4% 하락	규명되지 않음
영향	원자력발전소와 우라늄 농축시설의 가동이 중단됨	48시간 동안 공장 가동 중단으로 납품 지연 및 기업 신뢰도 하락	전 세계 알루미늄 생산량 감소에 따른 알루미늄 가격 1.3% 상승	철도 시스템 하루 동안 마비

4. OT 산업보안 관련 정책 분석

본 장에서는 국내 OT 산업보안 관련 정책을 분석함으로써 정책 측면에서의 한계점과 고려사항을 분석하고 제안한다.

1) 중대재해처벌법에 기반한 OT 보안 사고 분석

2022년 1월부터 시행된 '중대재해처벌등에관한법률'[20]은 경영책임자 처벌 강화를 통한 억제이론에 바탕을 두고 기업의 안전·보건 조치 의무를 강화하여 중대산업재해를 예방하고 종사자와 시민의 생명과 신체를 보호하는 것에 목적을 두고 있다. 이 법은 중대 재해 발생시 안전 및 보건 의무를 다하지 않은 사업주 또는 경영책임자에 대한 강화된 처벌을 규정하고 있다.

표 5는 중대재해처벌법과 유사한 해외의 산업재해 예방 관련 법제를 비교한 표이다. 중대재해로 인한 피해는 일반적으로 부상자와 사망자가 다수 발생하므로 사전 예방이 중요하다[21]. 영국은 기업의 형사책임에 대한 높은 사회적 관심도와 노동 현장에서의 산업재해의 심각한 실태에 대응하고자 2007년 기업과실치사 및 기업살인법을 제정했다. 호주는 8개 주 중 4개 주의 형법 및 산업안전법을 개정해 중대재해 관련 기업주와 법인을 처벌한다[21]. 영국과 호주의 법제는 사망사고 또는 중과실을 범죄 성립 조건으로 규정하고 있지만, 한국의 중대재해처벌법은 범죄 성립 조건을 중대재해 또는 과실로 규정해 해외 법제보다 범죄 성립될 가능성이 크다. 또한, 개인 처벌의 하한형과 손해배상의 경우에도 영국과 호주는 별도 규정이 없는 반면에 국내 중대재해처벌법은 개인 처벌의 하한형을 1년 이상, 손해배상액을 손해액의 5배 이내로 규정했다. 이는 해외 법제보다 중대재해처벌법의 처벌 수위가 높다는 것을 의미한다. 중대재해처벌법이 시행된 이후 7개월 동안 고용노동부에 의해 공식 수사 중인 중대재해 사건은 총 100건을 넘어

섰으며, 사업 발주자와 도급인뿐만 아니라 산업현장과 공중이용시설까지도 광범위하게 적용 대상으로 포함하고 있다.

TABLE V
중대재해처벌법 관련 해외 법제 비교

구분	영국	한국	호주
법제	2007 기업과실치사 및 기업살인법 (Corporate Manslaughter and Corporate Homicide Act 2007)	중대재해 처벌 등에 관한 법률	8개 주 중 4개 주의 형법 및 산업안전법에 규정(연방법 아님)
범죄성립 조건	사망사고 또는 중과실	중대재해(사망+일정 규모 이상 재해) 또는 과실	사망사고 또는 중과실
처벌 대상	법인	개인, 법인	개인, 법인
개인처벌의 하한형	없음 (사업주 개인에 대한 처벌 없음)	1년 이상	없음 (상한형만 명시)
손해배상	없음	손해액의 5배 이내	없음

앞으로는 중대재해처벌법에 의해 APT 공격, 랜섬웨어 등의 사이버 해킹으로 인해 OT 보안 사고가 발생해도 처벌받을 수 있다. 2021년도의 이란 철도 시스템 해킹 사건은 해킹집단이 지능형 멀웨어를 유포하여 철도 시스템에 침투함에 따라 데이터 삭제 및 프로세스 파괴로 교통부 사이트가 다운된 사건이다. 만약 이 사건이 현재 한국에서 발생해 교통이 마비되어 1

명 이상의 사망자 또는 동일한 사고로 2개월 이상 치료가 필요한 부상자가 10명 이상 발생하면 표 6의 중대시민재해에 해당하여 중대재해처벌법 적용이 가능하다.

TABLE VI

중대재해처벌법상 중대재해

용어	구분	개념	항목
중대재해	중대산업재해	「산업안전보건법」 제2조 제1호에 따른 산업재해 중 다음 각 목의 어느 하나에 해당하는 결과를 야기한 재해	가. 사망자가 1명 이상 발생
			나. 동일한 사고로 6개월 이상 치료가 필요한 부상자가 2명 이상 발생
			다. 동일한 유해요인으로 급성중독 등 대통령령으로 정하는 직업성 질병자가 1년 이내에 3명 이상 발생
	중대시민재해	특정 원료 또는 제조물, 공중이용시설 또는 공중교통수단의 설계, 제조, 설치, 관리상의 결함을 원인으로 하여 발생한 재해로써 다음 각 목의 어느 하나에 해당하는 결과를 야기한 재해	가. 사망자가 1명 이상 발생
			나. 동일한 사고로 2개월 이상 치료가 필요한 부상자가 10명 이상 발생
			다. 동일한 원인으로 3개월 이상 치료가 필요한 질병자가 10명 이상 발생

또한, 사고가 발생한 교통 시스템이 표 7에 나타난 것과 같이「중대재해처벌 등에 관한 법률」제2조 제5호에 따른 공중교통수단 중 하나에 해당할 경우 중대시민재해에 기반한 중대재해처벌법 적용이 가능하다.

동법의 제정 전에는 사건 발생의 책임이 불분명했으나, 동법에서는 책임 소재를 명확하게 규정하여 중대재해가 발생하지 않도록 산업안전보건에 대한 직접적인 관리 책임을 부과하고 있다. 이에 따라 국내 주요 기업들은

TABLE VII

중대재해처벌법 제2조 제5호

정의	불특정다수인이 이용하는 다음 각 목의 어느 하나에 해당하는 시설
항목	가. 「도시철도법」 제2조 제2호에 따른 도시철도의 운행에 사용되는 도시철도차량
	나. 「철도산업발전기본법」 제3조 제4호에 따른 철도차량 중 동력차·객차(「철도사업법」 제2조 제5호에 따른 전용철도에 사용되는 경우는 제외한다)
	다. 「여객자동차 운수사업법 시행령」 제3조 제1호 라목에 따른 노선 여객자동차운송사업에 사용되는 승합자동차
	라. 「해운법」 제2조 제1호의2의 여객선
	마. 「항공사업법」 제2조 제7호에 따른 항공운송사업에 사용되는 항공기

사업주와 경영책임자의 책임을 면피하기 위해 최고 안전 책임자(Chief Security Officer, CSO)를 선임하는 등의 조치가 이뤄지고 있다. CSO는 물리보안, 기술보안 등을 책임져 사고 예방 전권을 가지는 기업 안전 총책임자지만, 국내에서는 주로 CISO(Chief Information Security Officer)의 역할인 정보 보안에 초점이 맞춰진 업무를 수행하는 한계점이 존재했다. OT 보안 사고에 대한 명확한 책임 소재를 규명하기 위해서는 종래의 산업안전 보건에 대한 관리 책임 체계를 기저에 두되, IT와 OT가 융합되는 OT 보안의 특성에 대한 이해가 필요하다. 더불어, 관리적·물리적 보안에 대한 총체적인 역량을 갖추고 있어야 한다.

2) 산업기술보호법에 기반한 OT 보안 사고 분석

전 세계적으로 공급망의 불안전성이 증가하여 경제안보의 중요성이 대두되고 있다[22]. 최근 국내 기업을 대상으로 한 사이버 해킹을 통한 기술 유

출 시도가 계속되며 심각한 위협이 되고 있다[23]. 이는 연구개발 지원을 통한 기술 확보도 중요하지만, 기술 유출을 방지하고 비밀 유지 의무를 부여하는 것 또한 매우 중요함을 시사한다. 따라서 국내에서는 산업기술의 유출방지 및 보호에 관한 법률(약칭:산업기술보호법)을 통해 산업 기술을 보호하고 있다[24]. 해당 법률은 불법 해외 유출을 방지하고 국가 산업 경쟁력을 강화해 국가의 안전과 국민 경제의 안정을 보장하기 위해 지난 2006년 제정되었다. 표 8은 산업기술보호법의 제14조와 제36조(벌칙)를 정리한 표로, 산업기술보호법의 구성요건적 행위에 따라 산업 기술 유출에 의한 OT 보안사고도 처벌 가능함을 확인할 수 있다. 종래 OT 보안사고 분석은 주로 랜섬웨어 감염 및 외부자의 개입과 같은 외부 원인에 초점을 맞췄지만, 최근 장비의 운영 기술에 대한 원리를 부정 취득해서 공개하는 내부자의 행위도 OT 보안사고의 원인으로 확장되고 있다. 이러한 보안 위협을 포괄하기 위해 운영 기술을 제 3자에게 공개하거나 사용하도록 하는 행위는 산업기술보호법 제14조와 제 36조에 입각하여 처벌받을 수 있으며, 해당 법률은 제2항부터 제4항까지의 규정을 통해 징역형과 벌금형의 병과가 이루어질 수 있음을 규정하고 있다.

TABLE VIII
산업기술보호법

제14조	구성요건적 행위	국내 사용 목적 벌칙	해외 사용 목적 벌칙
제1호	부정(방법)취득, 사용, 공개	산업기술: 15년 이하의 징역 또는 15억원 이하 벌금	국가핵심기술: 3년 이상의 징역 및 15억 이하 벌금 병과
제2호	비밀유지위반행위(유출 등)		산업기술: 15년 이하의 징역 또는 15억원 이하 벌금
제3호	사후 부정취득, 사용, 공개		

제4호	중과실 취득, 사용, 공개	3년 이하의 징역 또는 3억원 이하의 벌금 병과 가능	해당사항 없음
제5호	미승인 또는 부정승인 수출 추진	10년 이하의 징역 또는 10억원 이하 벌금	산업기술: 15년 이하의 징역 또는 15억원 이하 벌금
제6호	해외사용 목적 미승인 또는 부정승인 해외 인수, 합병 등	해당사항 없음	
제6의2	해외사용 목적 미신고 또는 부정신고 해외 인수, 합병 등		
제6의3	비밀유지위반행위 (부정목적 거부, 기피, 사본보유)	10년 이하의 징역 또는 10억원 이하 벌금	
제7호	명령 미이행	10년 이하의 징역 또는 10억원 이하 벌금	
제8호	목적 외 사용, 공개	3년 이하의 징역 또는 3억원 이하 벌금	

산업기술보호법뿐만 아니라 영업비밀보호법, 국가첨단전략산업법 등 산업기술 보호를 위한 법률이 강화되고 있지만, 유출 사고 및 피해는 매년 지속적으로 발생하고 있으며 피해 규모가 증가하는 추세다[25]. 표 9는 경찰청에서 공개한 최근 5년간 산업기술유출사범 연도별 검거현황으로, 매년 100건 이상 발생하는 산업기밀 유출 사고를 방지하기 위해 제도적 장치만으로 대응하기 어려운 현실을 보여준다. 국가 안전보장을 위한 산업기술보

호법과 건전한 거래 질서 유지를 위한 영업비밀보호법의 입법 취지는 다르지만, 두 법률의 형사벌칙 규정에 별다른 차이점이 존재하지 않는다. 이는 두 법률의 경합 적용에 따른 법리 해석의 어려움으로 이어질 수 있으므로 산업기밀 유출행위와 영업비밀 침해행위를 구분한 법리 적용이 요구된다[26]. 또한, 산업기밀 유출범죄 방지를 위한 인프라 투자와 산업보안 전문 인력양성을 하고 있지만, 일부 대기업을 제외한 중소·벤처 기업들의 산업기밀 유출에 대한 대응 체계가 부족하다. 따라서 중소·벤처 기업들의 효과적인 OT 보안 사고 예방 및 대응을 위한 예산, 조직, 인력을 마련할 수 있도록 정부의 정책 지원 마련 및 기술 안보 체계 구축, 전문인력양성 등의 중장기적인 대책 수립이 필요하다.

TABLE IX
산업기술유출사범 연도별 검거현황

구분	검거건수 (단위: 건)			검거인원 (단위: 명)		
	국외	국내	계	국외	국내	계
2016	13	101	114	59	267	326
2017	13	127	140	36	300	336
2018	20	97	117	69	283	352
2019	12	100	112	40	341	381
2020	17	118	135	53	292	345

5. OT 산업기술 보호 방안

OT 산업기술의 보호를 위해서는 OT 산업의 고유 특성을 고려한 보안 내재화 중심의 기술적 대책과 정책 지원이 요구된다. 본 장에서는 2, 3장에서 분석한 종래 OT 보안 위협 및 관련 정책을 분석한 결과에 기반하여 OT 산업기술 보호를 위한 OT 산업의 기술적·정책적 관점의 개선방안을 제안한다.

1) OT 산업기술 보호를 위한 기술적 방안

중소벤처기업부는 데이터 기반의 인공지능 솔루션을 적용한 스마트 공장 사업을 추진했다. 그러나, 표 10에서와 같이 대부분의 제조 회사들이 생산 관리 시스템(MES)과 전사적 자원 관리(ERP) 도입 등 정보화 사업 중심으로 생산 관리를 수행하고 있으며, 데이터 중심의 제조 프로세스 혁신 수준이 매우 미흡한 것을 알 수 있다.

TABLE X
스마트 공장 데이터 기반 인공지능 솔루션 보급현황

장비	장비 수	비율(단위: %)
MES(Manufacturing Execution System)	8,355	66.0
ERP(Enterprise Resource Planning)	2,188	17.3
기타	1,048	8.3
PLM(Product Lifecycle Management)	574	4.5
FEMS(Factory Energy Management System)	254	2.0
SCM(Supply Chain Management)	122	1.0
자동화/디지털화	119	0.9
소계	12,660	100

위와 같은 문제점을 해결하기 위해서 본 장에서는 센서를 활용한 데이터 중심의 이상 징후 탐지 시스템을 제안한다. 종래 OT 망에서 사이버 공격이 발생한 근본적인 원인은 디지털 혁신으로 OT 인프라가 IT 망 시스템

과 급속하게 연결되면서 기존 IT 시스템이 노출되었던 위협에 그대로 노출되었기 때문이었다. 이에 따라, IT 망과 OT 망이 연결되는 3계층과 4계층 사이에 센서를 물리적으로 부착시킴으로써 비용 효율적인 보안 대응을 수행한다. 즉, OT 장비 및 프로토콜의 종류와 관계없이 부착한 센서를 통해 데이터를 수집함으로써 이상 징후를 발견하고, 제로 트러스트 보안 체계를 구축할 수 있다.

본 논문에서 제안한 아이디어는 그림 4와 같이 센서부와 데이터 수집부, 데이터 분석부 및 보안 대응부로 구성된다. 센서부는 OT 시스템의 결함을 파악하기에 적합한 센서를 사용할 수 있으며, 온습도 센서, 압력 측정 센서, 전압 측정 센서, 진동 측정 센서 등 다양한 센서를 포함한다. 이때, 해당 센서는 OT 시스템과의 망 분리인 에어갭(Air gap)을 확보함으로써 해커가 시스템을 해킹하더라도 데이터에 대한 유효성은 확보할 수 있다. 데이터 수집부와 데이터 분석부 및 보안 대응부는 OT 시스템에 대하여 수집한 데이터를 분석하고, 필요한 보안 대응책을 자동으로 제공한다. 종래의 데이터 기반의 접근법은 모든 OT 장비에 센서를 부착함에 따라 분석해야 할 데이터가 기하급수적으로 많고, 수동 대응에 따른 어려움도 존재했다. 본 아이디어는 IT 망과 OT 망이 연결되는 3계층과 4계층 사이에 선별적으로 센서를 배치함으로써 효율적인 이상 징후 탐지를 도모한다. 또한, 그림 5와 같이 의심 데이터 및 이상 데이터에 대한 단계적인 분석을 수행한다. 수집 및 분석된 데이터를 기반으로 일차적으로 의심 데이터가 존재하는지를 판단한다. 이때, 의심 데이터는 이상 행위로 의심이 되는 모든 데이터를 말한다. 의심 데이터에 따른 의심 데이터 분석을 수행한 후, 이차적으로 이상 데이터가 존재하는지 판단한다. 이때, 이상 데이터는 특정 네트워크 흐름이 임계치를 넘은 것과 같이 특정 임계치를 넘어선 이상 값을 보이는 데이터를 말한다. 이상 데이터가 존재할 경우, 보안 패치 및 점검과 사

후 모니터링이 수행된다. 이러한 일련의 흐름을 통해 육안으로 확인하기 어려웠던 종래의 한계점들을 극복하고 OT 시스템의 이상 징후에 대한 가시화 및 능동적인 대응을 수행한다.

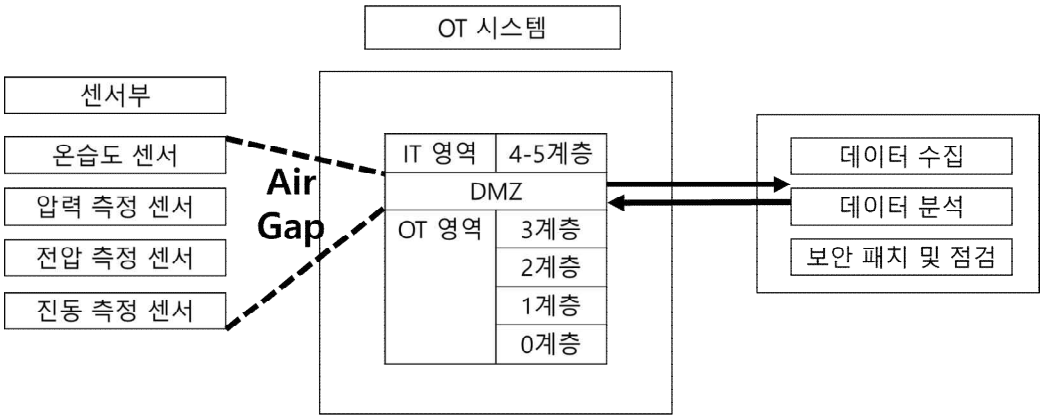

FIGURE 4. 제안 아이디어 구성도

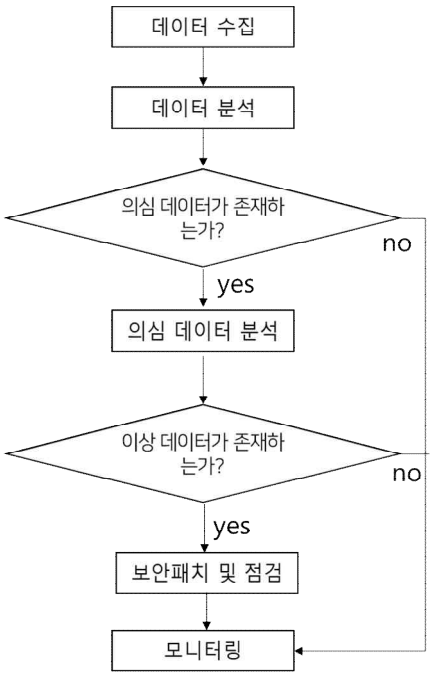

FIGURE 5. 제안 아이디어 흐름도

본 연구에서는 PC를 OT 장비로 가정하고, 과부하 프로그램을 공격자의 공격 행위로 가정했다. 이후, 온도 센서를 통해 공격 행위에 대한 이상 징후 탐지가 가능함을 입증했다. 제안 아이디어는 IT 망과 OT 망이 연결되는 3계층과 4계층 사이에 선별적으로 센서를 부착시킴으로써, 악성 정보가 유입될 수 있는 경로를 파훼하는 것을 목표로 한다. 표 11은 시간 경과에 따라 공격 행위를 수행했을 때의 온도 변화 추이를 보여주며, 실험 결과는 소수점 세 번째 자리에서 반올림한 결과를 작성하였다. 우측의 값들은 해당 시간에 측정을 시작했을 때의 온도, 마지막으로 측정했을 때의 온도, 그리고 해당 시간 내 온도 값들의 평균값을 보여준다. 공격 행위를 시작한 1, 3, 5, 7, 9 시점에서는 측정을 시작했을 때 온도에서 마지막으로 측정했을 때 온도까지 약 1~4도의 상승세를 보인다. 이와 달리, 공격 행위를 중지한 2, 4, 6, 8, 10 시점에서는 측정을 시작했을 때 온도에서 마지막으로 측정했을 때 온도까지 약 0.5 ~ 3도의 하락세를 보인다. 이를 통해, 공격자의 공격 행위에 따른 변화 추이를 센서 데이터 값을 통해 확인할 수 있다. 즉, 공격자의 공격 행위와 센서 데이터 값 간의 선형적인 관계를 보임으로써

TABLE XI
실험 결과

시간 (경과)	과부하	온도 변화 추이 (단위: °C)		
		시작	끝	평균값
1	작동	48.76	52.92	52.10
2	중지	52.89	49.50	50.31
3	작동	49.52	54.47	53.78
4	중지	54.47	53.30	53.26
5	작동	53.30	54.88	54.16
6	중지	53.85	53.30	53.62
7	작동	53.32	55.56	55.11
8	중지	55.53	53.85	54.24
9	작동	53.88	55.30	55.39

온도 센서를 통해 공격 행위에 대한 이상 징후 탐지가 가능함을 보여준다.

2) OT 산업기술 보호를 위한 법적 방안

최근 경제 안보 시대에 첨단핵심 기술을 보호하고 국가 경쟁력을 확보하기 위한 산업보안 인적 역량 강화 및 기술개발에 대한 논의가 적극적으로 이루어지고 있다[27]. 전문인력 확보는 첨단핵심 기술 주도권 확보를 위해 필수적이다. 이에 더하여, 산업 시장의 성장을 위해서는 각 산업 시장이 내포한 보안 인식과 역량을 강화해야 한다. 표 12에 따르면, 시장 초기 단계에 정보보호체계 구축 비용과 보안 위협에 의한 손해가 보안의 중요한 판단 요소이지만, 산업 시장 성장에 따라 보안의 비즈니스 기회 창출을 위한 전략적 가치가 중요해진다[28, 29]. 글로벌 기업 및 주요 국가는 중장기적인 보안 인식에 기반해 기술적 보안, 물리적 보안, 관리적 보안의 3요소를 고려한 융합보안 관점의 정책을 제안하고, 산업 성장을 도모하고 있다.

TABLE XII
기술 보안의 역할 및 인식 변화 과정

시기	보안 인식
초기 단계	- ‘비용’ 관점에서의 보안 인식
중기 단계	- ‘전략적 가치’ 관점에서의 보안 인식
최종 단계	- ‘새로운 비즈니스 기회 창출’ 영역으로 보안을 인식 - 보안에 대한 양적 투자 확대

미국은 2021년「혁신경쟁법」제정을 통해 첨단기술 산업에서의 리더십을 확보하고 국가 전략산업 경쟁력 강화를 목적으로 기술개발 투자를 확대했다. 미국의 산업 활성화 정책의 효과를 분석한 연구에 따르면 미국이 지난 1970년부터 산업 정책 활성화를 위해 무역 조치, 기업 보조금, 연구 개발을 정책 수단으로 활용해왔으며, ①산업의 경쟁력 강화 정도 ②고용 창출 정도 ③산업의 진보 정도를 정책 효과의 판단 기준으로 여러 산업군을 대상

으로 평가를 수행했을 때 연구 개발 지원, DARPA(Defense Advanced Research Projects Agency) 지원 프로그램이 가장 가시적인 성과를 실현했다고 보고했다. 일본은 지난 2022년 2월「경제안전보장추진법」을 발의하여 경제 안보 측면에서 위협이 되는 행위를 사전에 방지하고자 했다. 공급망 강화를 위한 우선순위 지정을 통해 특정 중요물자 안전 공급 확보, 특정 중요기술개발을 우선으로 시행했다. 이와 달리, 광범위하게 도입되어 민간 부문에 충격이 큰 기간 인프라 투자는 민간이 대응할 수 있는 기간을 부여하여 민간의 입법 수용성을 제고했다[30]. 이러한 입법 방법은 충분한 숙의를 통한 입법화 과정, 입법 수용성 제고를 위한 단계별 접근, 경제안보 관점에서 효과적이었다. 국내의 경우, 국가사이버안보 기본계획(2019)과 제1차 부정경쟁방지 및 영업비밀 보호 기본계획(안)(2022~2026)을 통해 산업혁신 생태계를 조성할 계획이다. 이러한 흐름을 기저에 두고, OT 산업기술 보호를 위해서는 앞서 검토한 중대재해처벌법, 산업기술보호법에 대한 검토뿐만 아니라 OT 산업기술 보호와 관계되는 여러 합동 기관 및 부처 간의 충분한 숙의와 가시적인 정책 효과 판단 기준이 필요하다.

3) OT 산업기술 보호를 위한 관리적 방안

기술주도권 확보를 위해 필수전략기술로 지정된 ICT 기술에 대한 R&D 투자를 확대하는 노력이 전 세계적으로 이루어지고 있다. 그 예로, 국내에서는 표 13과 같이 주요 행정기관을 중심으로 보안 인재양성과 산업기술 보호를 추진함으로써 첨단 산업 기술 보호 역량을 강화하기 위해 노력하고 있다. 또한, 코로나19 이후 디지털 기술이 경제사회 변화의 중심으로 역할이 확대됨에 따라 전 산업에서 디지털 융복합 혁신을 창출하기 위한 초연결 신산업 핵심기술 개발이 가속화되고 있다. 정부는 인공지능, 블록체인, 확장 현실(eXtended Reality, XR), 메타버스, 반도체, 양자, 사이버 보안 등

핵심 유망분야에 2025년까지 약 2.6조원 규모의 예산 투자 계획을 발표했다. 특히 과학기술정보통신부는 '대한민국 디지털 전략'에서 사이버 보안 10만 인재 양성, 4대 방어 기술(억제·보호·탐지·대응) 개발, 사이버 보안 및 개인정보보호 대학원 확대 등의 사이버 보안 디지털 인재 양성에 대한 세부 전략을 발표했다. 그러나 현재 보안 인력양성과 관련된 정책들은 계속해서 제안되고 있으나 이미 정립된 유망분야와 독립적으로 보안 인력양성 계획을 단행하는 것은 보안의 특수성인 '보안 내재화(Security by Design)'를 고려하지 못한 정책 기조라 볼 수 있다.

TABLE XIII
보안 인재양성 관련 기술 보호 동향

주요 행정기관	기술 보호 동향
과학기술정보통신부	국가연구개발 사업의 기술 보호 강화를 위한 보안대책 수립 시행, 보안관리 조치 및 사고 대책, 보안과제 분류 등을 위한 국가연구개발혁신법 개정('20.6)
산업통상자원부	국가핵심기술을 73개 기술, 12개 분야로 확대 지정('21.7)하고 보호조치 사항의 세부 지침을 마련
중소벤처기업부	기술보호 전문가의 종합진단을 통한 중소기업 기술보호 사업 추진 및 중소기업 기술보호 역량 인증체계 마련
특허청	부정경쟁방지법(제2조의2)에 따른 부정경쟁방지 영업비밀보호를 위한 범정부 차원의 기본계획을 수립하고 관련 조직 확대('21.7)

보안 내재화란 요구사항 분석 및 설계 단계에서부터 제품의 보안성(Security), 신뢰성(Reliability), 안전성(Safety) 등의 요소를 종합적으로 고려해 복잡도(Complexity)를 감소시키고, 궁극적으로 제품의 신뢰성(Trustworthy)을 달성하는 것을 말한다[31]. 보안의 내재화 역량을 보유한 보안 전문인력 양성은 지능화된 보안 위협에 대한 대응을 위한 필수 요건이다. 이는 비단 OT 산업보안뿐만 아니라, 인공지능 보안, 블록체인 보안,

메타버스 보안 등 모든 핵심 유망분야에 적용된다. 가속화된 디지털 전환의 결과로 각 산업군의 데이터들이 IT 시스템을 기반으로 연결됨에 따라 표 14와 같이 보안 공격 표면이 확장되고, 이에 따른 보안 대응이 필요하기 때문이다[32]. 보안 내재화를 중심으로 한 대응은 사이버 보안 사고 피해 규모 완화를 도울 뿐만 아니라, 작업장 안전 환경 개선에 기여한다. 그리고, 디지털 기술에 대한 신뢰성 제고 및 산업 발전에 기여, 더 나아가 국내외 안보 위협 완화를 돕는다[33]. 반면, 보안 내재화를 고려하지 못한 정책은 빠르게 지능화되는 사이버 위협의 속도를 따라가지 못할 뿐만 아니라 투자 예산 대비 큰 피해액으로 인해 실효성 제고에 대한 논의가 계속해서 이어질 것이다. 따라서 산업 발전을 위해서는 개별 산업군에 대한 보안 내재화 검토가 이루어져야 하며, 이를 관리할 수 있는 융합보안 인재양성 방안이 필요하다. 즉 현재의 사이버 보안 인력 양성 기조를 기반으로 하되, 기술과 산업의 특수성을 고려한 정책을 수립함으로써 융합을 위한 혁신을 도모해야 한다.

TABLE XIV

유망기술 대상 공격 표면(Attack surface)

산업명	공격 표면
인공지능 (AI)	- 머신러닝 학습에 쓰이는 데이터셋 조작을 이용해 공격 특성 분류의 정확성을 저하시키는 데이터 공격(Data poisoning) - 진위 여부를 가리기 어려운 가짜 데이터를 생성하는 딥페이크 공격
블록체인	- 보안이 취약한 개인·기업을 표적으로 한 중간자 공격(Man in the middle attack) - 블록체인 배포와 함께 제공되는 암호화 키 관리에 대한 보안 위협 발생
확장현실 (XR)	- 현실 세계와 연동된 데이터의 처리· 분석 과정에서의 보안 위협 발생 - IoT 센서와 지능형 CCTV를 통한 정보 수집 과정에서의 개인 정보 유출 위협
메타버스	- 디지털화된 민감정보(생체 신호, 행동 및 감정 정보 데이터, 소비 성향, 접속 시간 및 위치 등) 유출 및 데이터 위·변조 위협
반도체	- 통신용 반도체 제품(산업용 이더넷)을 대상으로 한 데이터 통신 보안 위협 등장 - 반도체 FPGA를 대상으로 하드웨어 디바이스의 논리적 결함을 기반으로 권한 상승, 원격제어 공격 - 스파이칩 탑재를 통한 하드웨어 기반 공급망 공격 유발
양자	- 종래 암호체계를 무력화시키는 양자 연산 방식 등장
5G/6G	- 5G/6G 네트워크에 연결된 IoT 장비(헬스케어용 스마트 기기, 커넥티드 카, 스마트 시티)를 대상으로 데이터 침해, 탈취, 조작 - 5G/6G 네트워크 취약점

6. 요약 및 소결론

OT 산업은 제조업을 중심으로 전력, 가스, 철도, 상하수도, 스마트공장, 석유화학, 선박 제조사, 자동차 부품 등 전통 산업과 결합하며 확대되고 있다. 최근 4차 산업의 발전과 함께 OT 망과 IT 망이 연결되면서 IT 망의 OT 보안사고가 급증했고, 그 수단과 방법이 지능적이고 정교해지고 있다. 특히, OT는 IT와 다른 특성에서 기인한 보안 위협이 존재하고 이에 따른 파급력이 매우 크기 때문에 OT 보안 법체계를 강화하고 있지만, OT 산업의 고유한 특성을 고려한 기술적 솔루션과 효과적인 제도에 관한 연구와 투자가 부족한 상황이다.

이에 따라 본 논문에서는 OT 산업 기술 보호를 위해 센서 기반의 기술적 방안과 법적, 관리적 방안을 제시했다. 센서 기반의 이상 징후 탐지 방식은 에어갭을 기반으로 종래 방식 대비 데이터 유출의 위험도를 낮추면서, 저렴한 센서로 경제적 파급력이 큰 OT 보안사고를 예방한다는 점에서 비용 효율적인 방식이다. 또한, 종래 OT 장비 프로토콜의 한계점을 해결하며 OT 장비의 가용성을 확보하며 OT 보안을 강화할 수 있는 방식이다. 법적 방안으로는 중대재해처벌법을 통해 불명확한 OT 보안사고에 대한 책임소재 규명 필요성, 산업기술보호법을 기반으로 OT 산업 기술 보호를 위한 중장기적인 대책 수립 필요성을 지적했다. 마지막으로, 관리적 방안으로 보안 내재화 중심의 OT 산업보안 강화를 위한 보안 전문인력 양성 및 융합보안 인재양성 방안 정책 수립의 필요성을 제기했다.

본 연구는 보안 내재화를 중심으로 OT 산업기술 보호를 위한 기술적, 법적, 관리적 방안을 제안하는 것에 의의를 둔다. 이러한 보안 내재화 기반의 접근 방식은 비단 OT 산업뿐만 아니라, 최근 활발하게 연구되고 있는 여러 유망 기술의 성장 동력으로 작용할 것으로 예측된다. 본 연구팀은 향후 실제 OT 시스템 공정 데이터에 본 논문에서 제안한 기술적 방안을 적

용함으로써 본 방안의 정확성, 비용 효율성, 보안성을 실험할 예정이며, OT 산업 기술 보호 방안 마련을 위한 지속적인 연구를 진행할 것이다.

Ⅲ. PART 2: In-Network Computing 기반 OT System

1. 서론

OT 시스템은 연속성과 가용성이 중요해 기존의 방식을 고수하며 변화의 저항성이 강한 레거시 산업(Legacy industry)이다. 이로 인해 기존의 기술, 방법론, 운영 모델에 크게 의존하며, 변화를 느리게 받아들여 현재 20~30년 전 장비를 사용하는 경우가 많고 고도화된 공격 기법에 대응하기 어려워 취약한 부분이 많다. 이로 인해 높은 공격 표면(Attack surface)을 가진 OT 보안은 다수의 공격포인트를 제공하고, 공격으로 인한 피해의 규모가 커 공격자들에게 매력적인 목표가 되어 그 피해가 점점 증가하고 있다. 이러한 피해를 방지하기 위해 임계치 기반 및 중앙 집중형 알람 시스템이 활용되고 있으나, 현재 OT 알람 시스템은 시스템 특성을 충분히 고려하지 못하고 있어 보안 위협에 취약한 상태이다. 기술 발전에 따라 현재 다른 산업에서는 인공지능이 널리 활용되고 있으나, OT 산업은 향후에도 인공지능이 적용되기 어려울 것으로 예상된다. 따라서 이러한 산업의 특성을 고려하여 산업 시스템의 보안성과 효율성을 동시에 향상시킬 수 있는 새로운 접근 방식이 필요하다.

중앙 집중형 시스템은 널리 사용되며 산업 성장에 이바지했으나, 효율성, 안보 등의 복합적인 이슈로 인해, 한계에 다다랐다는 평가를 받고 있다[34]. 중앙 집중형 OT 시스템은 여러 센서와 장비에서 수집된 데이터가 중앙 서버로 전송되어 처리된다. 이를 바탕으로 모니터링, 제어, 의사결정이 가능하며, 해당 방식은 데이터 관리와 처리에 있어서는 효율적이지만 구조적 취약성으로 인한 계산 오버헤드 문제가 있다. 산업 분야의 데이터는 다양한 형태의 구조화되지 않은 대규모의 비정형 데이터가 서버로 전송되다 보니, 전송 과정에 있어 보안과 데이터 프라이버시 문제가 존재한다. 이러한 문제는 시스

템의 단일 장애 취약점이 될 수 있으며, 이는 데이터 유출이나 시스템 장애로 이어질 수 있다. 본 연구에서는 인 네트워크 컴퓨팅(In-network computing) 기반의 OT System을 제안하여 중앙 서버에 대한 의존성 문제를 해결한다. OT 네트워크는 네트워크 및 OT 장치가 서로 연결되어 네트워크를 형성하고 있는데, 제안 시스템은 데이터 처리를 네트워크 장치가 수행하여 보안 문제를 해결한다. 해당 방법은 기존 시스템 대비 보안을 강화하면서도 정확도는 유지할 수 있어, OT를 포함한 다양한 환경에서도 적용 가능할 것으로 기대된다.

본 연구의 기여점은 다음과 같다. In-network computing 기반 OT 시스템의 도입을 통해, 네트워크 장치들이 현장에서 데이터를 처리함으로써 중앙 서버로의 데이터 전송 시 발생할 수 있는 보안 취약점을 줄인다. 이는 데이터 처리 효율과 사용성을 높이고, 중앙 서버에 대한 의존도를 낮춰 전체적인 시스템의 보안 구조를 강화하고 신뢰성을 높이는 데 기여한다.

PART 2는 다음과 같이 구성된다. 2장에서는 종래 OT 산업에서 사용되던 임계치 기반 모델과 중앙 집중형 시스템을 개선하기 위한 선행 연구를 검토한다. 3장에서는 OT 시스템 강화에 방해되는 원인을 분석하고, 이를 바탕으로 4장에서 보안 강화 방안을 제안한다. 5장에서 성능을 검증하고자 수행한 실험 환경과 결과를 분석하고, 6장에서 결론으로 마무리한다.

2. OT 알람 시스템 선행 연구

현재 임계치 기반 모델과 중앙 집중형 모델은 OT 알람 시스템으로써 널리 활용되고 있다. 해당 모델을 활용하여 OT 문제 상황 해결을 시도한 선행 연구를 살펴보고, 이를 통해 OT 보안 강화의 필요성을 확인한다. 표 15는 각 시스템의 선행 연구를 요약한 것이다.

임계치 기반 시스템은 임곗값을 설정하여 기준치를 초과하는 이상 상황이 감지될 경우 경고가 발생하는 시스템이다. OT 시스템에서 가장 널리 사용되는 알람 시스템으로, Yang Xu 외 10인[35]은 파이프라인 누출을 감지하기 위해 동적 임곗값 식별 방법(Dynamic Threshold Identification Method, DTIM)을 제안했다. DTIM은 라만 분산 광섬유 센서(Raman distributed fiber sensor, RDFS)를 사용하여 온도를 측정하고, 정상 임계치를 벗어난 온도 데이터를 찾아 누출을 감지한다. 임계치를 초과할 경우 알람이 발생하며, 누출률과 1미터 오차 이내의 정확한 위치를 추정할 수 있어 빠른 조치가 가능하다. 그러나 DTIM은 다양한 환경에 널리 적용되어 활용되기 어려운 방법으로 유연성이 낮고, 중앙 집중식 데이터 처리로 인해 네트워크 규모가 커질 경우 성능이 저하될 수 있다. Minu Treesa Abraham 외 5인[36]은 강우 임곗값과 MEMS(Micro Electro Mechanical Systems) 기울기 센서 데이터를 결합한 임계치 기반 산사태 조기 경보 시스템을 제안하였다. 산사태 예측 정확도가 현장 데이터와 결합하였을 때 84%에서 92%로 향상되어, 제안 방법이 산사태 잠재 위험을 낮출 수 있음을 입증하였다. 지면 움직임 및 강우량 조합이 효과적이기는 하나, 제안 방식을 활용하기 위해 대량의 센서를 설치할 경우 성능 저하를 피하기 위해서는 대규모 데이터 처리에 대한 고려와 확장성 측면에서의 분석이 필요하다.

중앙 집중형 모델은 중앙 서버를 통해 작업이 통합적으로 처리되며, 시

스템의 모든 자원에 접근하고 모니터링할 수 있다. 이로 인해 데이터 처리 및 관리에 있어 효율적이지만, 모든 권한이 중앙에 있어 해커의 공격이 성공할 경우 시스템 전체의 취약점이 될 수 있다. Rana Aamir Raza Ashfaq 외 4인[37]은 침입 탐지 시스템(Intrusion Detection Systems, IDS)의 성능 향상을 위해 퍼지 기반 준지도 학습 접근 방식을 제안하였다. 이 방식은 레이블 여부의 구분 없이 통합된 데이터를 퍼지를 통해 분류함으로써 IDS 효율성을 높였다. 실험에는 KDDTest+와 KDDTest-21 두 가지 데이터 세트를 활용하고, 제안 알고리즘이 82.41%와 84.12%로 다른 분류기 모델 대비 좋은 성능을 보임을 입증하였다. 그러나 준지도 학습은 데이터가 복잡할 경우 실시간 데이터 처리가 어려울 수 있어 실제 시스템 적용 시 이에 대한 고려가 필요하다. Wu Wang 외 4인[38]은 산업 시스템에서 공격 탐지 정확도를 높이기 위해 의사결정 나무, XGBoost 등의 기계학습, 딥러닝 기법을 소개하고 평가하였다. 실험 결과, XGBoost가 과적합을 방지하는 페널티 항을 갖고 있다 보니, 과적합과 이상치에 강인하여 0.989의 정확도로 가장 좋은 성능을 보였다. 이를 통해 사이버 위협 탐지 시스템에 XGBoost를 적용할 경우, 공격 탐지 및 대응에 대한 성능을 개선할 수 있을 것으로 기대된다. 그러나, 해당 실험에서는 특정 데이터셋만을 대상으로 실험이 진행되어, OT 시스템을 고려한 보다 복잡한 환경이나 데이터셋을 통해 성능이 검증되어야 한다. 본 장에서 분석한 임계치 기반 및 중앙 집중형 시스템 선행 연구를 통해, OT 시스템 보안 강화를 위한 새로운 접근 방식이 필요함을 확인하였다. 다음 장에서는 OT 보안 요구사항 분석을 위해 OT 시스템 특징에 대해 분석하고 고려 사항에 대해 확인한다.

TABLE XV
OT 알람 시스템 선행 연구

Category	Refs	Method	Limitation
Threshold based System	[35]	- 파이프라인 누출 감지를 위해 동적 임곗값 식별 방법을 제안함	- 중앙 데이터 처리 방식으로 인해 규모가 커질 경우 성능이 저하될 수 있음
	[36]	- 산사태 예측을 위해 강우 임곗값과 기울기 센서를 결합한 경보 시스템을 제안함 - 정확도가 84%에서 92%로 증가하며, 위험 예측의 가능성을 입증함	- 확장성 측면에서의 성능 저하 가능성이 있음
Centralized System	[37]	- 퍼지 기반 준지도 학습 접근 방식을 제안함 - 퍼지를 통해 샘플을 분류하여, 다른 분류기 모델 대비 좋은 성능을 보임	- 데이터 품질에 따라 정확도가 낮아질 수 있음
	[38]	- 산업 시스템에서 공격 탐지 정확도를 높이기 위해 기계학습 기법을 소개하고 평가함 - XGBoost가 0.989의 정확도로 가장 좋은 성능을 보임	- 특정 데이터셋 한정으로 실험이 진행되어 다양한 환경에서의 성능 검증이 필요함

3. OT 시스템 특징 분석 및 보안 강화 고려사항 분석

OT 시스템은 IT와 분리되어 단말기에 원격으로 접근하는 것이 불가능했던 과거와 달리, 온라인 연결은 되었지만 전문 OT 프로토콜에 의존하는 등 기술 발전은 더뎌 다른 분야보다 제한된 연구 조건을 가지고 있다. 특히, 기술 발전을 고려하지 않고 운영되고 있는 레거시 산업 시스템(Legacy industrial system)은 첨단 보안 솔루션에 대한 지원뿐만 아니라, 기본적인 보안 조치마저 미흡하다[39]. 이로 인해 교통, 공장 등을 포함한 주요 인프라에 대한 보안 사고 발생 시 치명적인 결과를 초래할 수 있어 OT 보안 강화가 필요하다. 본 장에서는 OT 시스템의 특징을 확인하고, 보안 강화를 위한 고려 사항을 분석한다.

1) 레거시 산업 시스템

레거시는 유산이라는 뜻으로, 오래전에 개발된 기술이나 방법론이 사라지지 않고 현대에도 영향을 미치거나 쓰이는 기술을 레거시 시스템이라고 한다. 레거시 산업은 설계대로 작동하며 안정성을 제공하지만, 현대의 기술 발전 속도 대비 기술 혁신이 느리게 적용된다. OT 장비는 20~30년 이상 사용할 목적으로 다양한 프로토콜과 OS를 사용해 특수 제작되어 복잡성은 높지만 호환성은 낮다[40]. 이로 인해 시스템 통합이 어려우며, 오래된 OS를 사용하는 등 기본적인 보안 조치가 부족하다. 또한, 초기 OT 시스템은 온라인과 격리된 환경에서 작동하도록 설계되어, 암호화, 인증과 같은 보안 기능에 대한 필요성이 낮았다[41]. 그러나, OT와 IT가 통합되며 구조적으로 연결됨에 따라, 공격 표면이 넓어져 트로이목마(Trojan), 스턱스넷(Stuxnet)과 같은 사이버 위협이 산업 제어 시스템에 영향을 미치고 있다. 이로 인해, 산업 자동화를 위해 개발된 Modbus, PROFIBUS(Process Field Bus), DNP3(Distributed Network Protocol version 3) 등의 프로토콜은 폐

쇄적 환경에서는 안정적인 통신을 제공했지만, 명령어 패킷에 대한 무결성 확인 누락 등 다양한 취약점과 버전 차이로 인한 호환성 등 해결해야 하는 과제가 많다[42]. 이처럼 OT/ICS 보안에 대한 요구가 커짐에 따라, 미국 국립표준기술연구소(National Institute of Standards and Technology, NIST)는 Special Publication(SP) 800-82r3, Guide to Operational Technology Security를 발표하며 OT 보안 가이드라인을 제공하고, 기업 및 학계에서는 이러한 요구 사항을 준수하기 위한 기술을 개발 및 적용하고 있다. OT 보안 강화를 위해서는 기술적 이해를 바탕으로 최신 기술을 결합한 포괄적인 접근 방식이 필요하며, 이를 통해 오래된 시스템을 유지하면서도 산업 인프라를 효율적으로 보호할 수 있다.

2) 넓은 공격 표적 대비 제한된 실험 환경

최근, 산업 시설의 스마트화와 함께 OT 망을 대상으로 한 해킹, 악성코드 감염 등 다양한 사이버 공격과 피해가 증가하고 있다. OT 시스템은 중단될 경우 심각한 손실이나 재해로 이어질 수 있기 때문에 가용성 및 무결성이 중요하다[43]. 이로 인해, OT 보안 강화를 위한 연구의 필요성이 증대되고 있음에도 불구하고, 실제 환경에서의 테스트 진행이 어려운 상황이다. 실제 OT 환경에서의 실험은 시스템 다운이나 생산 중단과 같은 예상치 못한 문제가 발생할 수 있고, 이에 따른 피해가 막대하기 때문이다. 이를 방지하고자 대부분의 OT 보안 연구는 실제 환경이 아닌, 공개 데이터세트를 기반으로 진행된다. 표 16은 OT 보안 연구에 사용되는 주요 데이터 세트를 정리한 것으로, 공격은 허위 데이터 주입 공격(False data injection), 정찰(Reconnaissance), 서비스 거부 공격(Denial of Service, DoS), 스푸핑(Spoofing) 네 가지로 분류되며, 공개된 데이터세트를 활용한 연구도 제한적임을 알 수 있다[44]. 다양한 산업에서 활용되는 OT 시스템

은 구성 요소와 프로토콜이 복잡하며, 제한된 실험 환경에서는 이러한 시스템의 다양성을 충분히 반영하기 어렵다. 이로 인해 실제 환경에서 발생 가능한 취약점과 공격 유형을 포괄적으로 다루기 어려워, 현실적인 보안 솔루션을 개발하고 검증하는 데 한계가 있다. 따라서, 넓은 공격 표면을 커버하기 위해서는 다양한 방식을 결합하거나, OT의 특성을 고려한 새로운 보안 기법이 개발되어야 한다.

TABLE XVI
주요 OT 데이터 세트

데이터세트명	공격 대상	공격 유형	Type
BATADAL (BATtle of the Attack Detection Algorithms)	C-Town 물 분배 시스템	허위 데이터 주입 공격	센서, 액추에이터
GP (Gas Pipeline)	가스 파이프라인 시스템	허위 데이터 주입 공격, 정찰, 서비스 거부 공격	네트워크
HAI (HIL-based Augmented ICS Security)	터빈, 보일러, 수처리 시스템	허위 데이터 주입 공격	센서
SWaT (Secure Water Treatment)	수처리 시스템	허위 데이터 주입 공격	센서, 액추에이터
WADI (Water Distribution Testbed)	수처리 시스템	허위 데이터 주입 공격, 스푸핑	센서, 액추에이터

4. In-Network Computing 기반 OT System

산업 환경에 대한 이해를 바탕으로 한 OT 시스템 강화의 필요성이 커짐에 따라, 본 장에서는 기존 알람 시스템의 한계점을 분석한다. 이후, 이를 해결하기 위해 In-network computing 기반의 OT 시스템인 INCOS를 제안하여 데이터 기반의 보안 강화를 제공하고, 시스템의 효율성과 신뢰성을 높인다.

1) 종래 OT 알람 시스템

OT 알람 시스템은 실시간 모니터링과 제어를 목적으로, 다양한 산업 공정에서 발생할 수 있는 잠재적 위험을 감지하고 경고하는 데 사용된다. 이러한 시스템은 산업 공정의 안전성과 효율성을 유지하는데 필수적인 역할을 수행함에 따라, 산업 환경에서 중요한 역할을 한다.

현재 대부분의 OT 알람 시스템은 임계치를 기반으로 운영된다. 이는 수많은 센서 및 장치에서 발생하는 데이터, 파라미터가 설정된 임계치를 초과하거나 미달할 때 알람이 발생하는 시스템을 의미한다. 이런 임계치는 온도, 압력, 소리 등이 될 수 있으며 다양한 산업 환경에 맞게 임계치, 알람 유형, 반응 프로토콜 등을 설정할 수 있다. 또한, 산업 환경에서 발생할 수 있는 문제에 빠르게 대응하기 위해 실시간 모니터링을 제공하여 문제를 식별하고 작업자들이 위험 상황에 적절히 대응할 수 있도록 한다. 이러한 임계치 기반 알람 시스템은 센서의 잦은 고장, 복잡한 산업 환경에서의 다양한 변수 등으로 인해 신뢰성이 떨어진다[45]. 이는 오탐(False alarm)과 위험 상황의 미탐(Miss detection) 문제를 야기하고, 효과적인 위험 대응을 방해하여 작업자의 피로도를 증가시킨다. 또한, 이상 탐지에 있어 복합적인 판단이 아닌 하나의 데이터만을 활용하므로, 임곗값을 무단으로 변경하는 것만으로도 장비를 손상, 정지시켜 막대한 피해를 초래할 수 있다.

임계치 기반 모델의 한계를 개선하기 위해 다른 분야에서는 중앙 집중형 모델이 널리 사용된다. 기술의 발전을 통한 성능 향상을 최우선하는 다른 산업과 달리, OT는 안정성과 예측 가능성이 중요하여 신기술이나 프로세스를 도입에 있어 보수적이다. 이로 인해 보안 업그레이드 등의 조치가 제한되며, 중앙 집중형 모델을 포함한 신기술 역시 도입하기 어렵다. 그러나, 본 논문에서는 이러한 모델이 OT 시스템에 접목되어 널리 사용되고 있음을 가정한다. 중앙 집중형 모델은 각각의 장치 데이터를 중앙에서 학습하는 방법으로, 대량의 데이터를 활용하는 만큼 하나의 센서 값으로만 상황을 판단하는 임계치 기반 모델 대비 정확도가 높다. 따라서, 오탐, 미탐 등의 성능 개선과 효율성 향상을 기대할 수 있지만, 안전에 관한 중요 데이터가 한 곳에 모여 활용될 경우 산업기밀 및 정보 유출, 프라이버시 문제가 생길 수 있다. 따라서 OT 환경은 안정성과 가용성이 중요하지만 사이버 공격으로 인한 피해가 큰 만큼, 단순히 다른 분야에서 활용되는 기술을 그대로 도입하는 것이 아닌 산업의 특성을 고려한 효율적이고 안전한 보안 솔루션이 요구된다.

2) INCOS

In-network computing은 스위치, 라우터 등의 네트워크 장비가 논리, 산술 작업을 수행함으로써, 네트워크 전체에 작업이 분산되는 컴퓨팅 기술이다. 해당 기술을 통해 정보의 중앙 집중 이슈를 해결하고, 전통적인 중앙 집중식 시스템 대비 부하를 낮춰 성능 향상을 기대할 수 있다[46]. 또한, 해당 기술은 범용 기술로써, 모니터링, 데이터 집계, 혼잡 제어 등 다양하게 활용할 수 있다[47]. 이상 탐지에 적용할 경우, 실시간으로 네트워크 트래픽의 비정상 패턴을 탐지하여 초기 공격 차단 등의 신속한 대응을 할 수 있다[48]. 또한, 패킷 전달 등의 목적으로 네트워크 내에서 역할을 수행하던 장비가 데이터

처리하기 때문에 데이터의 유출 위험이 낮다. 데이터 처리 시 외부 메모리에 액세스 하지 않아 대기 시간이 적으며, 실시간 데이터 처리와 높은 처리량을 제공한다[49]. 이러한 특징을 바탕으로 제안하는 INCOS는 네트워크 및 OT 장치들이 네트워크를 형성하여 서로 연결되는 구조를 가진다. 각각의 구성요소들은 다음의 역할을 수행한다. 네트워크 내 OT 센서는 데이터를 수집하고, 네트워크 장비는 데이터를 처리한 뒤 본래 역할인 중앙 서버로 전달을 수행한다. 이 과정에서 비정상적인 패턴이나 보안 위협을 실시간으로 탐지할 수 있어 공격에 대한 신속한 대응이 가능하고, 시스템에 신뢰성을 제공한다. 또한, INCOS는 데이터 처리 결과를 전파하므로, 원시 데이터 전송을 최소화하여 정보의 중앙 집중 문제를 해결한다. 이를 통해 중앙 집중형 시스템에 존재하는 문제를 개선하고, OT 데이터와 시스템의 보안성을 강화할 수 있다.

5. 성능 평가

1) 실험 환경, 모델

본 연구에서는 OT 시스템에 In-network computing을 적용했을 때 성능을 평가하기 위해 Python 3.7.12 환경에서 모델을 구축하여 학습하였다. 표 17은 실험 환경을 요약한 표로, 31Gi RAM과 Ubuntu 운영 체제가 탑재된 CPU 4xAMD EPYC 7B12를 활용했다.

TABLE XVII
실험 환경

구분		사양
Python Version		3.7.12
CPU	Core	4
	model name	AMD EPYC 7B12
Memory (RAM)		31Gi
OS	name	Ubuntu
	Version	20.04.3 LTS

INCON 분류 모형은 LSTM 모델로 구성하고, 상황별 결과를 확인하였다. 그림 6은 실험에서 활용한 LSTM 모델의 구조도로, 이 모델은 시계열 데이터로 분류되는 소리 데이터를 처리하기 위해 선택하였다. 모델은 LSTM 레이어와 3개의 밀집(dense) 레이어로 구성된다.

2) 데이터셋

OT는 제조, 에너지 관리, 수처리 시설 등과 같이 광범위한 환경을 포함하므로, OT 시스템에서 발생할 수 있는 5가지 위험 상황의 wav 파일로 구성된 데이터셋을 선정하였다. OT 환경에서의 위험 상황은 다양하지만, OT 산업에서의 위험을 일반화하여, 경보, 화재, 사회 제반 시설의 문제, 자연재해로 인한 문제, 일반 상황으로 구분하였다. 이에 따라, danger, fire,

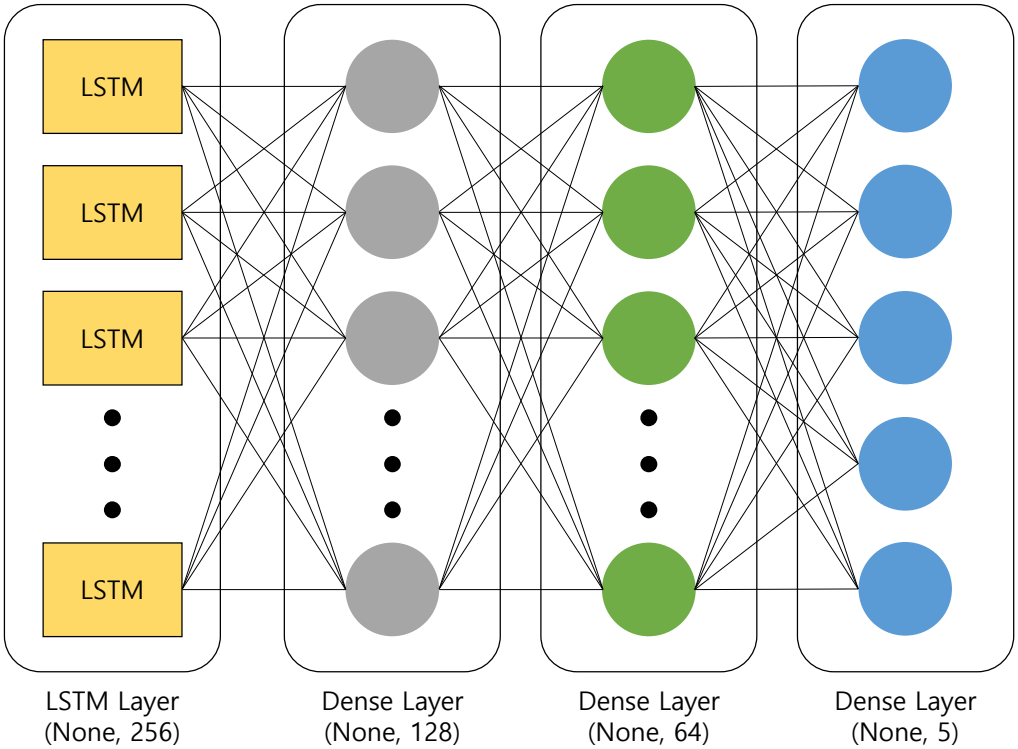

FIGURE 6. 네트워크 레이어 구조도

gas, non, tsunami 상황의 소리 데이터가 각각 600개씩, 총 3000개로 구성된다[50]. 확장자는 wav로, MFCC(Mel-Frequency Cepstral Coefficients) 오디오 데이터 전처리를 수행하였다. MFCC는 스펙트럼 분석을 통해 소음과 같은 불필요한 정보는 줄이고 특징을 추출하여 음성 및 오디오 처리 분야에서 널리 사용되는 알고리즘이다. 이를 통해 정확도와 데이터 처리 효율성을 향상할 수 있어, 본 논문에서도 전처리 후 최종 과정에서 np.array로 모델이 학습할 수 있도록 변환하였다. 각 상황별 주파수 및 음조 예시는 그림 7, 8과 같다.

3) 실험 결과 및 분석

본 장에서는 INCOS의 성능을 검증하기 위해 각 소리별 분류 실험 결과

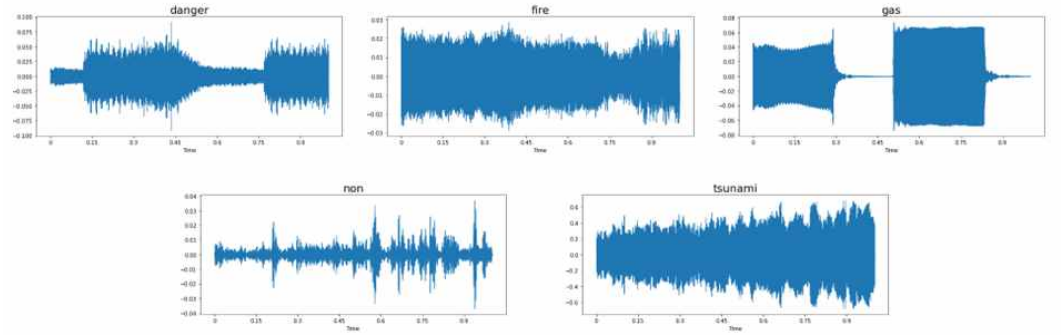

FIGURE 7. 데이터셋 파형 그래프 예시

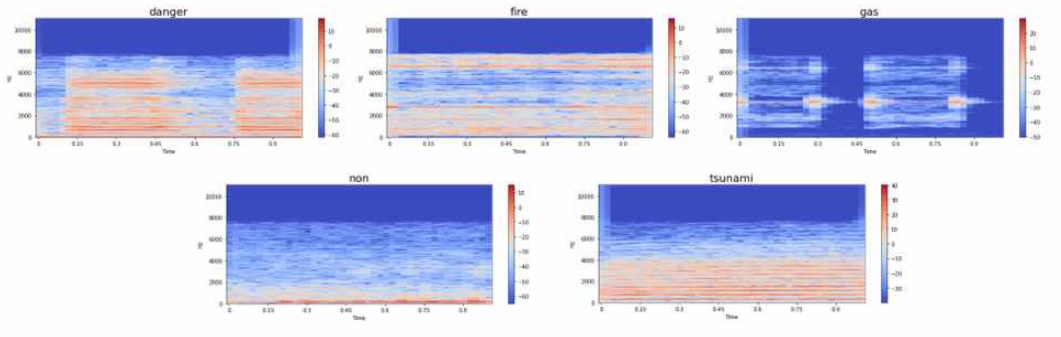

FIGURE 8. 데이터셋 주파수 스펙트럼 그래프 예시

를 분석한다. 논문에서 소개한 모델은 임계치 기반 모델, 중앙 집중형 모델, INCOS로 3가지이지만, 향후 기술이 발전하여 적용될 경우만을 가정하였다. 오픈소스로 공개된 실험을 통해 본 논문에서 제안한 INCOS의 성능을 확인하였으며, 성능 지표로 정확도(Accuracy), 손실(Loss), 정밀도(Precision), 재현율(Recall), F1-score을 사용한다[51].

표 18은 실험 Accuracy와 Loss을 정리한 것으로, 실험 결과는 소수점 세 번째 자리에서 반올림한 결과를 작성하였다. 테스트 accuracy는 98.33%, loss는 10.18%로 모델이 테스트 데이터에 대해 높은 정확도를 보이지만, 특정 케이스에 대해서는 불확실성을 갖고 있다. 검증 과정에서의 accuracy는 98.89%, loss는 5.51%로, 모델이 검증 데이터셋에서 더 높은 성능을 보인

다. 이는 해당 데이터셋에 대해 더 잘 일반화되어, 모델이 과적합 없이 일관된 성능을 유지하고 있음을 나타낸다. 또한, 훈련 데이터에 대해 accuracy 100%와 0.0041%의 아주 낮은 loss를 보여, 모델이 훈련 데이터를 완벽하게 학습했음을 알 수 있다.

TABLE XVIII
위험 상황 분류 정확도, 손실

구분		결과 (단위: %)
Test	Accuracy	98.33
	Loss	10.18
val	Accuracy	98.89
	Loss	5.51
train	Accuracy	0.00
	Loss	100

그림 9는 에폭 수에 따른 모델의 훈련 및 검증 accuracy를 알 수 있는 그래프로, 모델이 훈련 데이터를 빠르게 학습하고 있음을 확인할 수 있다. 약 10 에폭 이후부터 모델이 수렴하여, 일반화 과정이 잘 진행됨이 확인된다. 훈련과 검증 accuracy 사이에 차이가 적어 과적합이 발생하지 않았으며, 모델이 안정적으로 학습되어 훈련 데이터와 검증 데이터에서 모두 높은 정확도를 달성했다.

그림 10은 에폭별 훈련과 검증 과정에서의 loss을 평가한 그래프이다. loss는 모델 예측 값과 실제 값의 차이를 나타내는 지표로, 값이 낮을수록 모델 성능이 좋다는 것을 의미한다. 그래프는 모델이 초기에 빠르게 학습하고, 훈련 데이터에 대한 예측 성능이 향상되고 있음을 보여준다. 약 10 에폭 이후부터는 훈련과 검증 loss 모두 안정화되어, 모델이 높은 성능을 유지하고 있다. 또한, 훈련과 검증 과정에서의 차이가 적어, 모델이 학습 과정에서 안정적으로 loss를 줄이고, 과적합 없이 일반화되고 있음을 확인할 수 있다.

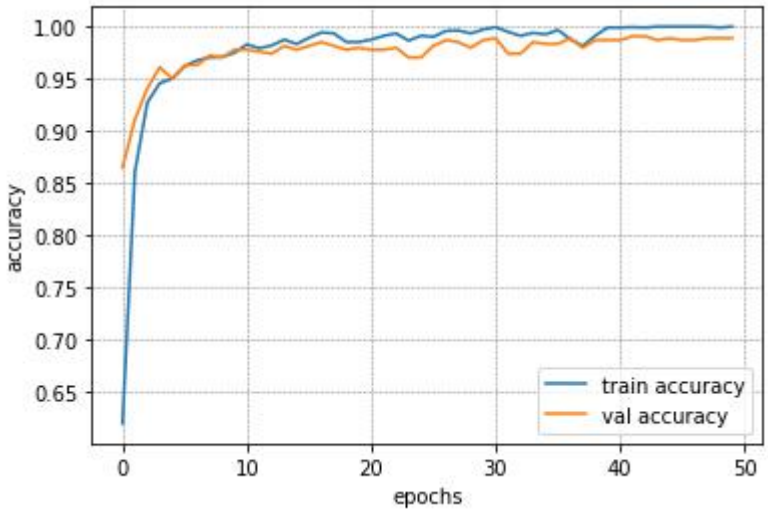

FIGURE 9. 학습 결과에 따른 정확도

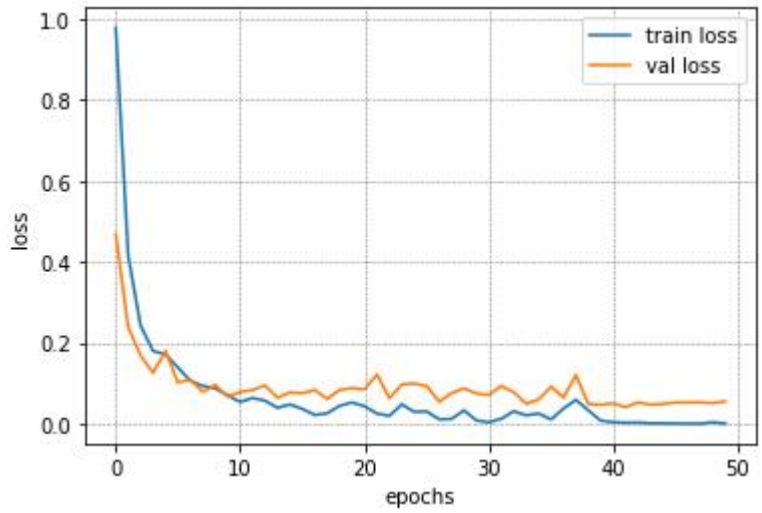

FIGURE 10. 학습 결과에 따른 손실

그림 11은 검증 데이터에 대한 혼동 행렬로, 상황별 예측 정확도가 높아, 모델이 상황을 효과적으로 구별할 수 있음을 보인다. 또한, 잘못 분류된 사례가 상대적으로 적어, 모델의 분류 성능이 우수한 것을 알 수 있다.

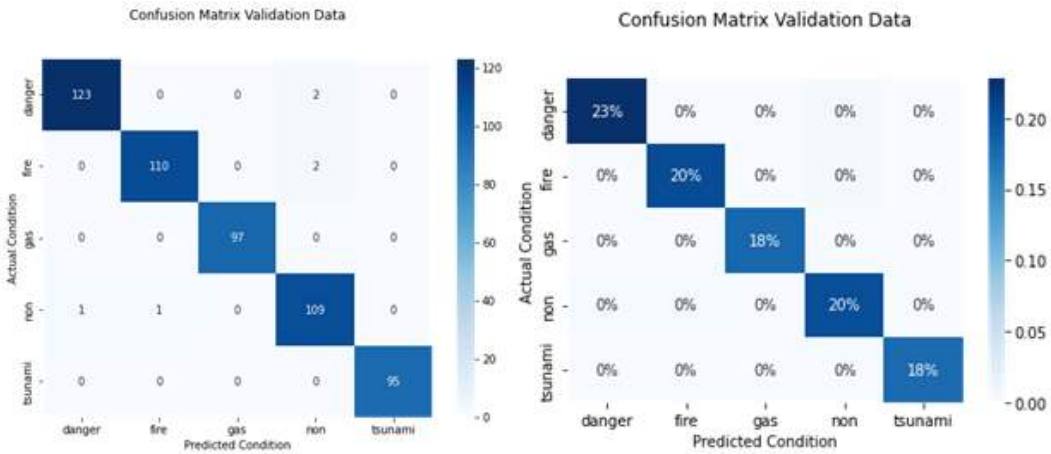

FIGURE 11. 검증 데이터의 혼동 행렬 예측

표 19는 모델의 상황별 Precision, Recall, F1-score를 보여주는 분류 보고서다. Precision은 모델 결과의 신뢰성을 의미한다. recall은 hit rate이라고도 하며, 실제 true인 것을 얼마나 맞췄는지에 대한 것으로 결과 재현성을 알 수 있다. F1-score는 precision과 recall의 평균으로, 해당 값이 높을수록 성능이 좋다. 따라서 본 실험의 분류 보고서에 대한 분석은 다음과 같다. gas와 tsunami 클래스에 대한 100%의 precision과 recall은 모델이 해당 위험 상황을 완벽하게 분류했음을 의미한다. 반면에, non 클래스의 recall은 상대적으로 낮아 잘못된 양성 예측을 할 가능성이 있다. INCOS 방식을 활용하여 네트워크 내에서의 분산된 데이터 처리를 통해 보안 문제가 감소되었음에도 분류 정확도 등에서 좋은 결과를 보임을 확인하였다. 이처럼 일반 상황보다 위험 상황에 대해 효과적으로 탐지되는 결과를 통해 INCOS가 복잡한 상황에서도 뛰어난 성능을 발휘할 것으로 기대된다.

TABLE XIX

위험 상황별 분류 보고서 (단위: %)

	precision	recall	f1-score	support
danger	0.99	0.98	0.99	125
fire	0.99	0.98	0.99	112
gas	1.00	1.00	1.00	97
non	0.96	0.98	0.97	111
tsunami	1.00	1.00	1.00	95
accuracy			0.99	540
macro avg	0.99	0.99	0.99	540
weighted avg	0.99	0.99	0.99	540

6. 요약 및 소결론

전 세계적으로 사이버 위협이 증가하며 OT 시스템이 공격자들의 주요 타깃으로 떠오른 만큼 OT 보안의 중요성이 부각되고 있다. 특히 피해가 발생할 경우 사회 전반에서 영향을 미치는 OT 시스템을 보호하기 위해 안전한 알람 시스템을 운영하기 위한 기술이 연구되고 있다. 하지만, 레거시 산업 프로토콜과 제한된 실험 환경 등의 시스템 특징으로 인해 OT 보안 강화의 한계가 있다. 종래의 실시간 알람 시스템은 센서의 잦은 고장 등의 문제로 false alarm 및 miss detection 등의 문제가 다양하게 존재한다. 시스템 도입의 유동성이 높은 다른 분야에서는 중앙 집중 시스템을 통해 여러 개의 데이터를 활용하여 정확도는 높였으나, 모든 데이터가 중앙 서버로 전송되다 보니 속도와 프라이버시 침해 문제가 존재한다. 본 연구에서는 처리 속도와 보안 강화, 효율성을 동시에 개선하기 위해 INCOS을 제안하였다. INCOS는 In-network computing 기술을 기반으로 네트워크 장치에서 데이터를 처리하여 결과만을 중앙 서버에 전달하는 메커니즘을 통해 보안 문제를 효율적으로 해결했다. 또한, 위험 상황에 대한 효과적인 탐지 능력과 높은 정확도를 통해 INCOS가 OT 시스템은 물론, 데이터 보안이 중요한 다양한 분야에도 적용될 수 있는 가능성을 확인하였다. 향후 연구에서는 사이버 위협에 대한 분석을 수행하고, INCOS를 활용하여 위협에 대응하는 구제적인 전략을 개발하고자 한다.

Ⅳ. 결론

기술 발전과 함께 사이버 공격은 유형과 피해 규모가 점차 확대되고 있어 높은 공격 표현을 가진 OT 기기 보안의 중요성이 증가하고 있다. 그러나 OT 장비와 같은 노후화되고 유연성이 낮은 장치들은 처리 능력과 가용성의 제한 때문에 기존의 보안 기법을 적용하기 어렵다. 따라서 기존의 시스템을 지속적으로 운영되며, 기본적인 동작을 해치지 않으면서 적용할 수 있는 보안 기술에 대한 연구개발의 필요성이 강조되고 있다. 본 연구에서는 고신뢰 OT 시스템을 위한 데이터 중심의 네트워크 기반 두 가지 보안 메커니즘을 제안하였다.

OT 장비들은 수십 년 동안 설계되어 기술적으로 구식인 경우가 많아 수명 주기가 긴데 반해 기존 시스템의 교체 및 통합, 업그레이드, 보안 패치 등이 어렵다. OT 산업 기술 보호를 위해 융합 보안을 고려한 보안 내재화 중심의 기술적, 법적, 관리적 방안을 제안하였다. 제안하는 기술적 에어갭 방안은 저비용 센서를 통해 악성 공격으로 인한 영향을 받지 않으면서도 안전하고 효율적으로 공격을 탐지할 수 있음을 입증하였다.

또한, 중앙 집중형 OT 알람 시스템의 보안 문제를 해결하는 INCOS을 제안했다. INCOS는 네트워크에 존재하는 장치들이 직접 데이터를 처리하여 원시 데이터가 아닌 결정된 값을 중앙 서버에 공유한다. 실험을 통해 위험 상황 분류는 높은 성능을 달성하면서도, 보안 문제를 개선하여 OT 시스템에서의 네트워크 안정성과 효율성이 보장됨을 확인하였다.

향후 연구로는 복잡한 OT 알람 시스템에서 발생하는 false alarm과 miss detection 문제를 해결하고, fault tolerant를 개발하여 사전에 OT 장애를 방지하고는 데이터를 보호할 수 있는 보안 메커니즘을 제안할 계획이다.

참고문헌

[1] Han Eun Hye, How to improve security vulnerabilities due to increased IT and OT linkage.REVIEW OF KIISC, vol. 30, no. 5, pp.55-60, 2020.

[2] Frost & Sullivan, Increasing Sophistication of Attacks and Evolving Threat Landscape Powering Global Industrial Cybersecurity, 2022.

[3] DongJun Choi, JaeWoo Lee, A security study for Control Network: Security Threat Using Control Protocol, The Journal of Society for e-Business Studies, vol. 25, no. 2, pp.99-108, 2020.

[4] Sans, A SANS 2021 Survey: OT/ICS Cybersecurity, 2021.

[5] ADTcaps, Security Trends Report for the First Half of 2021, 2021.

[6] Jeong Se-yoon, Manufacturing and Manufacturing in the Era of the Fourth Industrial Revolution IDX, The Journal of The Korean Institute of Communication Sciences, vol. 35, no. 1, 12-20, 2017.

[7] Z. Jadidi and Y. Lu, A Threat Hunting Framework for Industrial Control Systems, in IEEE Access, vol. 9, pp. 164118-164130, 2021.

[8] A. Bhardwaj, F. Al-Turjman, M. Kumar, T. Stephan and L. Mostarda, Capturing-the-Invisible(CTI): Behavior-Based Attacks Recognition in IoT-Oriented Industrial Control Systems, in IEEE Access, vol. 8, pp. 104956-104966, 2020.

[9] Miao, Kelei, Xiufang Shi, and Wen-An Zhang, Attack signal estimation for intrusion detection in industrial control system, Computers & Security, vol. 96, pp. 101926, 2020.

[10] Mubarak, Sinil, et al, Industrial datasets with ICS testbed and attack detection using machine learning techniques, Intell, Autom. Soft Comp, vol. 31, pp. 1345-1360, 2022.

[11] KISA, Smart Factory Security Model, 2021.

[12] HMS Industrial Networks, Industrial network market shares 2020

according to HMS Networks, https://www.hms-networks.com/news-and-insights/news-from-hms/2020/05/29/industrial-network-market-shares-2020-according-to-hms-networks, 2020

[13] Jae-Yoon Shim, June-Kyoung Lee, Convergence Security Technology of OPC-UA Protocol Gateway based on DPI & Self-Similarity for Smart Factory Network, Journal of the Korea Institute of Information Security & Cryptology, vol. 26, no. 5, 1305-1311, 2016.

[14] Choi, S., Yun, J. H., & Min, B. G, Probabilistic attack sequence generation and execution based on MITRE ATT&CK for ICS datasets, 2021 Cyber Security Experimentation and Test Workshop (CSET), pp. 41-48, 2021.

[15] NIST, SP 800-82 Rev. 3 (Draft), Guide to Operational Technology (OT) Security, 2022.

[16] IEC 62443-4-2:2019, Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components, Feb. 27, 2019.

[17] Woonyon Kim, Eung-Ki Park, Sin-Kyu Kim, Yoon-Seok Jee, Trends in the Security Assessment System for Industrial Control Systems, REVIEW OF KIISC, vol. 29, no. 2, pp. 5-15, 2019.

[18] Oh-min Kwon, A study on improving convergence security regulations in a digital transformation society, Legal theory practical research, 7(4), 75-103, 2019

[19] Lee Eung Kyu and KimJungDuk. A Case Study on ICT Supply Chain Attacks, Research on Information Technology Architecture, vol. 16, no. 4, pp. 383-396, 2019.

[20] Ministry of Trade, Industry and Energy, punishment of serious accidents, no. 17907, 2022.

[21] Kang, Young Ki, Lee, Chang Dai, and Lee, Sung Nam, Review of Corporate Responses to the Enforcement of the Serious Accident Punishment Act, Sogang Journal of Law and Business, vol. 11, no. 2, pp. 211-245, 2021.

[22] Ban Kiljoo, The Rise of Economic Security in the New Cold War Era and

South Korea's Strategic Option.The Journal of Strategic Studies, vol. 29, no. 2, pp. 297-330, 2022.

[23] Seul-gi Kim, Dea-woo Park, The Research for Cyber Security Experts, Journal of the Korea Institute of Information and Communication Engineering, vol. 21, no. 6, pp. 1137-1142, 2017.

[24] Ministry of Trade, Industry and Energy, Act on the Prevention and Protection of Industrial Technology, no. 17163, 2020.

[25] Yu Ha-rang, Research on deriving key factors for estimating the extent of damage from technology leaks, Master's thesis at Chung-Ang University Graduate School, 2020.

[26] Cho Yong Sun, Review of the Revised 2019 Trade Secret Protection Act and Industrial Technology Protection Act: Focusing on Civil and Criminal Remedies, Journal of the Korean Society of Security and Security, no. 61, pp. 333-352, 2019.

[27] Lee Joon-Ho and Seung-Soo Shin, A Study on the Necessity of Expanding National Core Technologies according to the Establishment of the Concept of National Industrial Security, Korea Industrial Security Research, vol. 11, no. 1, pp. 327-349, 2021.

[28] ASIS/IOFM, United States Security Industry Survey; ASIS/IOFM, The United States Security Industry : Size and Scope, Insights Trends, and Data, 2017

[29] Chansoo Park, Minji Kang, and Iejung Choi, Strategy on Building Korea's Industrial Security Ecosystem in the Global Technology Competition Era, policy research, pp. 1-237, 2019.

[30] Jeon Hyun-hee, Main Contents of Japan's Economic Security Promotion Act and Our Response Tasks, Institute for Industrial Economics, 2022.

[31] Ilgu Lee, Sowon Jeong, and Yurim Choi, Cyber KillChain Based Security Policy Utilizing Hash for Internet of Things, Digital Convergence Research, vol.

16, no. 9, pp. 179-185, 2018.

[32] Soo-young Kang, Seung-joo Kim, .Analysis of Security Requirements for Secure Update of IVI(In-Vehicle-Infotainment) Using Threat Modeling and Common Criteria.Journal of the Korea Institute of Information Security & Cryptology, vol. 29, no. 3, pp. 613-628, 2019.

[33] KIM IL HWAN, A Study on the Improvement of Personal Information Protection Legislation in the Hyper-Connected Society, Sungkyunkwan law, vol. 29, no. 3, pp. 35-74, 2017.

[34] Qin L, Peña-García A, Leon AS, Yu J-C, Comparative Study of Energy Savings for Various Control Strategies in the Tunnel Lighting System, Applied Sciences, vol. 11, no. 14, 2021.

[35] Y. Xu et al., Pipeline Leak Detection Using Raman Distributed Fiber Sensor With Dynamic Threshold Identification Method, in IEEE Sensors Journal, vol. 20, no. 14, pp. 7870-7877, 15 July15, 2020.

[36] Abraham, M.T, Satyam, N, Bulzinetti, M.A, Pradhan, B, Pham, B.T, Segoni, S, Using Field-Based Monitoring to Enhance the Performance of Rainfall Thresholds for Landslide Warning. Water, vol. 12, 2020.

[37] Ashfaq, Rana Aamir Raza, et al, Fuzziness based semi-supervised learning approach for intrusion detection system. Information sciences, vol. 378, pp/ 484-497, 2017.

[38] Wang, Wu, et al, Cyber-attacks detection in industrial systems using artificial intelligence-driven methods, International Journal of Critical Infrastructure Protection, vol. 38, 2022.

[39] R. Khan, K. McLaughlin, B. Kang, D. Laverty and S. Sezer, A Seamless Cloud Migration Approach to Secure Distributed Legacy Industrial SCADA Systems, 2020 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, pp. 1-5, 2020.

[40] Serror, Martin, et al, Challenges and opportunities in securing the

industrial internet of things, IEEE Transactions on Industrial Informatics, vol. 17, no. 5 pp. 2985-2996. 2020.

[41] Køien, G.M, Zero-Trust Principles for Legacy Components, Wireless Pers Commun, vol. 121, pp. 1169 - 1186, 2021.

[42] O. Givehchi, K. Landsdorf, P. Simoens and A. W. Colombo, Interoperability for Industrial Cyber-Physical Systems: An Approach for Legacy Systems, in IEEE Transactions on Industrial Informatics, vol. 13, no. 6, pp. 3370-3378, 2017.

[43] Dhirani LL, Armstrong E, Newe T, Industrial IoT, Cyber Threats, and Standards Landscape: Evaluation and Roadmap, Sensors, vol. 21, no. 11, 2021.

[44] Koay, A.M.Y., Ko, R.K.L. Hettema, H. et al., Machine learning in industrial control system (ICS) security: current landscape, opportunities and challenges, J Intell Inf Syst, vol. 60, pp. 377 - 405, 2023.

[45] C. Hwang and T. Lee, E-SFD: Explainable Sensor Fault Detection in the ICS Anomaly Detection System, in IEEE Access, vol. 9, pp. 140470-140486, 2021.

[46] S. Kianpisheh and T. Taleb, A Survey on In-Network Computing: Programmable Data Plane and Technology Specific Applications, in IEEE Communications Surveys & Tutorials, vol. 25, no. 1, pp. 701-761, 2023.

[47] M. Blöcher, L. Wang, P. Eugster and M. Schmidt, Holistic Resource Scheduling for Data Center In-Network Computing, in IEEE/ACM Transactions on Networking, vol. 30, no. 6, pp. 2448-2463, 2022.

[48] H. Wu, Y. Shen, X. Xiao, G. T. Nguyen, A. Hecker and F. H. P. Fitzek, Accelerating Industrial IoT Acoustic Data Separation With In-Network Computing, in IEEE Internet of Things Journal, vol. 10, no. 5, pp. 3901-3916, 1 March, 2023.

[49] S. Kianpisheh and T. Taleb, A Survey on In-Network Computing: Programmable Data Plane and Technology Specific Applications, in IEEE Communications Surveys & Tutorials, vol. 25, no. 1, pp. 701-761, 2023.

[50] Kaggle, Alarm dataset,

https://www.kaggle.com/datasets/devisdesnug/alarm-dataset, 2022

[51] Kaggle, https://www.kaggle.com/code/devisdesnug/rnn-mfcc/notebook, 2022

[52] Ryu, Jung-hwa, Ilgu Lee, Moon, Jung-hyun. OT Industrial Security Enhancement Focused on Security-by-Design. Korea Industrial Security Research, vol. 13, pp.91-118, 2023.

ABSTRACT

Data-centric network-based security mechanism for highly reliable OT systems

Jung-Hyun Moon
Department of Future Convergence
Technology Engineering
Graduate School of Sungshin University

As the value of data increases with technological advances and emerges as an important asset in various industries, the importance of data management and processing is increasing. The use of data analysis is expanding, such as producing information, and cyberattacks are also intelligent, and the need to strengthen security and privacy targeting data is increasing. Accordingly, it is important to protect industrial confidentiality and effectively manage data, and research is required for a data security mechanism for a reliable system. In particular, as operational technology (OT) systems converge with information technology (IT), new security issues arise, and a modern security system is needed to cope with them.

This paper analyzes the industrial characteristics of the OT system and its security vulnerability. It emphasizes the importance of strengthening industrial security by analyzing the current status of OT industry security and cases of damage caused by the digitization of the OT industry. We propose two data-oriented security mechanisms that ensure data integrity even if the OT system is attacked and enable OT security based on high reliability. It was confirmed that the anomaly detection system applied with the air gap-based security internalization method was capable of detecting malicious behavior through changes in sensor data according to the attack behavior. In addition, INCOS (In-Network Computing Base Operational Technology System) applying the In-Network computing technique to the OT system can effectively respond to OT problem situations even though it

provides data privacy. Experiments confirmed that the model was generalized with 98.33% test accuracy and 98.89% verification accuracy, and classification reports showed more than 96% accuracy in general situations and 98% in dangerous situations, proving that the model showed accurate and constant performance for five risk situations that could occur in the OT environment.

ACKNOWLEDGEMENTS

본 논문의 PART Ⅰ은 2023년 2월, 산업보안연구학회(KCI 저널)의 제13권 pp.91-118에 게재된 '보안 내재화 중심의 OT 산업보안 강화 방안' 연구 결과를 바탕으로 작성하였습니다[52]. 해당 연구의 후속 연구 결과를 토대로 확장하여 연구한 결과를 바탕으로 작성한 논문입니다. 해당 연구에 기여해 준 류정화 학생과 지도해 주신 이일구 교수님께 감사드립니다.