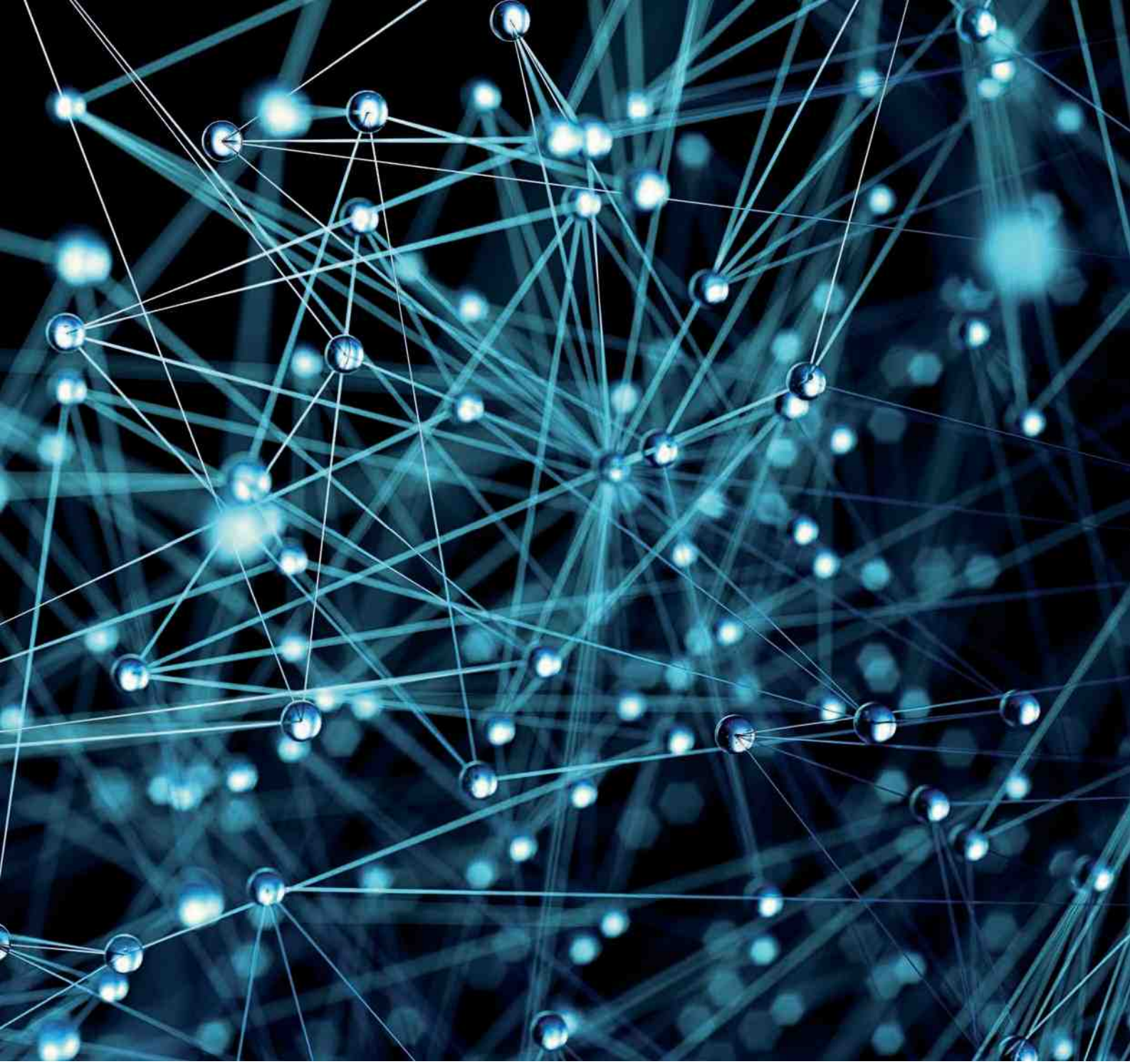


백서

IoT 2020: 스마트 및 보안 IoT 플랫폼

[일러두기]

- 본 서는 IEC에서 발행한 White Paper를 국문으로 번역 발간한 것입니다.
- 본 한국어 번역본의 저작권은 IEC 귀속됩니다. IEC는 한국어 번역에 대한 오역, 오류 등으로 인한 어떠한 책임도 지지 않으며, 번역의 책임은 한국전력공사 기술기획처에 있습니다.
- 본 백서의 영문 원본은 IEC 홈페이지를 통해 온라인으로 확인할 수 있습니다. http://www.iec.ch/whitepaper

[발간사]

한국전력은 1898년 한성전기 설립을 시작으로 올해 창립 120주년을 맞았습니다. 그 동안 한전은 수많은 위기와 어려움을 극복해 왔으며, Forbes紙 선정 '글로벌기업 2000'의 전력 유틸리티 부문에서 3년 연속 최상위권을 기록하는 등 그 성과와 가능성을 국내외에서 인정받고 있습니다. 이러한 성과는 한전이 대한민국 국민여러분과 한전 임직원의 피와 땀으로 이뤄낸 결과이며, 글로벌 선도 전력회사로 대외에서 당당히 인정받은 결과입니다.

한전이 대한민국 대표 에너지 기업으로서 세계적인 위상을 인정받은 것은 매우 영광스러운 일이지만, 한편으로는 '에너지전환'과 '디지털변환'이라는 거대한 변화의 시대에 한전이 미래 에너지 시대를 선도해 나가야 한다는 막중한 책임감을 느꼈습니다. 본 IEC 백서의 국문본 번역 작업은 이러한 전력산업의 선도자라는 사명감으로 시작하였습니다. 세계적으로 저명한 학계 및 산업계의 석학과 경영진이 참여하여 편찬한 IEC 백서를 국내 전력산업의 미래를 위해 불철주야 헌신하고 계시는 많은 전력인들과 공유하고자 합니다.

IEC(International Electrotechnical Commission, 국제 전기전자 표준위원회)는 전기전자기술 분야의 국제표준화 기관이며, IEC 산하 MSB(Market Strategy Board, 시장전략이사회)는 주요 기술동향을 파악하고, 향후 예상되는 시장활동 및 요구기술을 분석하기 위해 매년 IEC 백서(White paper)를 개발하고 있습니다.

4차 산업혁명의 시대를 맞이하여 산업간 경계가 빠른 속도로 허물어지고 있고, 수많은 경쟁자들이 새로운 시장에 진입하며, 지금은 상상도 못한 새로운 세상이 열리게 될 것입니다. 많은 사람들이 4차 산업혁명이 일어나면 대규모 실업이 발생할거라고 말하고 있고, 수많은 직업군이 사라질 것이며, 인간의 삶은 지금과는 상당히 달라질 것이라고 합니다. 우리는 무엇을 어떻게 준비해야 할까요? 저는 지난 2017년부터 MSB 위원으로 활동하면서, 다가오는 대변혁의 미래에너지 시대를 대비하여 가능한 많은 사람들이 IEC 백서를 통해 작지만 분명한 도움이 된다고 생각합니다.

아무쪼록 한국어 번역본 발간을 흔쾌히 승낙해 준 IEC 중앙사무국과 순조로운 진행에 도움을 주신 한국표준협회에 감사드립니다. 또한, 본 백서 번역에 동참해 준 기술기획처 및 전력연구원 관계자 여러분께도 깊은 감사를 드립니다.

2018년 9월

한국전력공사 부사장 김종성

요약

사물인터넷(IoT) 시장 전망에 따르면, IoT는 이미 글로벌 경제에 영향을 미치고 있다. 앞으로 다가올 5~10년 동안 얼마만큼의 경제적 영향을 끼칠지에 대한 평가는 각 컨설팅 기관별로 다소 상이하지만, (IDC는 2020년까지 USD 1.7조 예측[1], Gartner는 2020년까지 USD 2조 예측[2], McKinsey는 2025년까지 USD 4조 ~ 11조 성장 예측[3]), IoT 기술의 경제에 미치는 영향력이 상당하며 앞으로 계속 증가할 것이라는 예측에는 이견이 없어보인다.

비록 이미 그 영향력이 상당하다고는 하지만, Gartner는 IoT와 IoT 관련 비즈니스 모델이 현재 아직 성숙한 단계에 이르지 못했기 때문에[2] IoT가 경제(아마도 사회 전반)에 미칠 변혁은 아직 시작되지도 않았다는 점을 지적한다.

본 IEC 백서는 IoT의 차기 핵심 단계(즉, 스마트 및 보안 IoT 플랫폼 개발)에 무엇이 수반될 수 있을 지에 대한 전망을 제공한다. 이런 플랫폼은 보안부문의 기능을 상당수 개선하며, 일반적으로 IoT용으로는 설계되지 않던 "레거시" 시스템으로 구성된 여타 기존 IoT 플랫폼과의 간격을 좁혀준다. Gartner 예측에 따르자면 2020년까지 모든 IoT 프로젝트의 80%는 부적합한 데이터 수집 방법으로 인해 이행 단계에서 실패할 것으로 보인다[4]. 그러므로 스마트 및 보안 IoT 플랫폼의 주된 목적 중 하나는 "플랫폼을 위한 플랫폼(Platform of Platforms)" 역할을 하는 것이다.

본 백서에서는 IoT 시스템 설계와 더불어 아키텍처 패턴에 특별히 중점을 두어 현재 IoT가 처한 상황에 대한 개요를 밝힌 후 현재 IoT 프레임워크가 지닌 제약과 결점에 대해 기술한다. 그런 제약과 결점은

보안성, 상호 운용성, 확장성과 연관된다. 차세대 스마트 및 보안 IoT 플랫폼의 기능과 요구사항을 도출하기 위해 산업, 공공 및 소비자 도메인의 몇 가지 사용 사례를 살펴본다. 그리고 이런 사례와 서로 다른 중점 부분을 토대로 스마트 및 보안 IoT 플랫폼의 기능과 요구사항을 유추한다. 그런 다음 연결성, 처리 및 보안 부문의 플랫폼 수준 기술을 강조하여 스마트 및 보안 IoT 플랫폼에 대한 차세대 지원 기술을 살펴본다.

사물인터넷에 결부되어있는 야심찬 비전이 결실을 맺으려면 상호운용성 활성화계획 개발과 같은 상당한 수준의 표준화 노력이 필요할 것이므로 본 백서에서는 이러한 상황에 대응하기 위한 바람직한 미래 IoT 생태계 환경을 제시한다.

본 백서는 일반적 특성만 다루는 데서 그치지 않고 특별히 IEC 및 IEC 위원회에 대한 공식적인 권고로 끝맺음한다. IEC에 대한 주요 권고는 다음과 같다.

- IEC가 핵심 역할을 수행하여 IoT 표준화 생태계 환경을 주도적으로 구축한다.
- ISO/IEC JTC 1 리더에게 핵심적인 IoT 표준화 활동에 대한 임무를 할당한다.
- 정부 기구와 보다 긴밀한 협조를 하며 적극적인 참여를 이끌어내고 IEC 결과물을 통해 대응해야 할 관련 요구사항 및 관심사항을 파악한다.

감사의 말

본 백서는 프로젝트 리더, SAP 및 프로젝트 파트너, Fraunhofer AISEC의 적극적인 도움을 받아 IEC 시장 전략 이사회(MSB)의 IoT 2020 프로젝트 팀이 작성하였다. 이 프로젝트 팀은 다음과 같이 4차례 모임을 가졌다.

2015년 11월(Walldorf, DE)
2016년 1월(Munich, DE)
2016년 3월(일본, 도쿄)
2016년 5월(Walldorf, DE)

그 밖에 다수의 온라인 회의를 개최하였다. 본 프로젝트 팀의 구성원은 다음과 같다.

Mr. Bernd Leukert, SAP, MSB Member, Project Director

Dr. Dr. Timo Kubach, SAP, Project Manager

Dr. Claudia Eckert, Fraunhofer AISEC, Project Partner

Dr. Kazuhiko Tsutsumi, Mitsubishi Electric, MSB Member

Mr. Mark Crawford, SAP
Ms. Nina Vayssiere, SAP
Mr. Ebin Thomas Kandathil, SAP
Dr. Uwe Kubach, SAP
Mr. Anirban Majumdar, SAP
Mr. Alan Southall, SAP
Mr. Fabian Biegel, SAP

Ms. Krista Grothoff, Fraunhofer AISEC

Mr. Mario Hoffmann, Fraunhofer AISEC

Mr. Philipp Stephanow, Fraunhofer AISEC

Dr. Seisuke Kano, AIST
Dr. Hiroyuki Sawada, AIST
Dr. Kai Cui, Haier
Dr. Daisuke Matsubara, Hitachi
Dr. Motonobu Saito, Hitachi
Mr. Tadashi Kaji, Hitachi

Dr. Yun Chao Hu, Huawei Technologies

Mr. Xiangqun Liu, Huawei Technologies

Dr. Jijun Luo, Huawei Technologies

Mr. Ulrich Graf, Huawei Technologies

Dr. Sadayuki Watanabe, METI

Dr. Tetsushi Matsuda, Mitsubishi Electric

Mr. Noritaka Okuda, Mitsubishi Electric

Dr. Yasunori Mochizuki, NEC Corporation

Dr. Ernoe Kovacs, NEC Corporation

Dr. Gürkan Solmaz, NEC Corporation

Mr. Hiroshi Takechi, NEC Corporation

Dr. Akihisa Ushirokawa, NEC Corporation

Dr. Fang-Jing Wu, NEC Corporation

Mr. Peter Lanctot, IEC, MSB Secretary

목 차

약어 목록

기술 및 과학 용어

약어	영문	한글
5G	5th generation cellular access	5G, 제 5세대 셀룰러 액세스
ACE	authentication and authorization for constrained environments	제한된 환경에 대한 인증 및 권한 부여
ADECP	autonomaous data exchange control profile	자율 데이터 교환 제어 프로파일
API	application programming interface	애플리케이션 프로그래밍 인터페이스
ARM	architectural reference model	아키텍처 참조 모델
ASE	asymmetric searchable encryption	비대칭 검색 가능 암호화
BCM	business continuity management	비즈니스 연속성 관리
CACC	cooperative adaptive cruise control	협업 순응 주행 제어
CAGR	compound annual growth rate	연평균 성장률
CAM	cooperative awareness message	협업 인지 메시지
CMMI	capability maturity model integration	기능 성숙 모델 통합
CoAP	constrained application protocol	제한된 애플리케이션 프로토콜
COP	common operational picture	공통 작전 상황도
CPS	cyber physical system	가상 물리 시스템
CRISP-DM	cross industry standard process for data mining	데이터 마이닝에 대한 산업 간 표준 프로세스
CRM	customer relationship management	고객관계 관리
CT	communication technology	통신 기술
DENM	decentralized environmental notification message	분산 환경 통보 메시지
DevOps	development and operations	개발 및 운영
DPM	digital product memory	디지털 제품 메모리
eMTC	enhancements for machine type communications	기계 유형 통신에 대한 향상

약어	영문	한글
ERP	enterprise resource planning	전사적 자원 계획
FCW	forward collision warning	전방 추돌 경고
GPS	global positioning system	위치 결정 시스템
GSM	global system for mobile communications	모바일 통신에 대한 글로벌 시스템
HSM	hardware security module	하드웨어 보안 모델
HSPA	high speed packet access	고속 패킷 액세스
HTTP	hypertext transfer protocol	하이퍼텍스트 전송 프로토콜
HV	host vehicle	호스트 차량
HW	hardware	하드웨어
I/O	input/output	입출력
IaaS	infrastructure as a service	서비스로서 인프라
IAM	identity and access management	ID 및 액세스 관리
ICT	information and communications technology	정보 통신 기술
IIRA	industrial internet reference architecture	산업 인터넷 참조 아키텍처
IM	identity management	ID 관리
IMT Advanced	international mobile telecommunications-advanced	국제 모바일 전기통신-어드밴스
IoT	Internet of Things	사물인터넷
IoT-A	Internet of Things architecture	사물인터넷 아키텍처
IoT RA	Internet of Things reference architecture	사물인터넷 참조 아키텍처
IP	internet protocol	인터넷 프로토콜
IRI	internationalized resource identifier	국제 자원 ID
IT	information technology	정보 기술
LAN	local area network	로컬 영역 네트워크
LPWAN	low power wireless access network	저전력 무선 액세스 네트워크
LTE	long term evolution	LTE
M2M	machine to machine	기계대기계
MBB	mobile broadband	모바일 브로드밴드
MES	manufacturing execution system	제조 실행 시스템
MoU	memorandum of understanding	양해각서
MQTT	message queuing telemetry transport	메시지 대기열 텔레미터법 전송

약어	영문	한글
NB-IoT	narrowband Internet of Things	협대역 사물인터넷
NFC	near field communication	근거리 자기장 통신
NGSI	next generation service interface	차세대 서비스 인터페이스
OEM	original equipment manufacturer	OEM, 원 장비 제조업체
OIDC	OpenID Connect	OpenID Connect
OODA	observe-orient-decide-act	관찰-방향설정-결정-실행
OPC	object linking and embedding for process control	프로세스 제어를 위한 개체 연결 및 임베드
OpenIOC	open indicators of compromise	OpenIOC
OSS	open source software	오픈 소스 소프트웨어
OT	operational technology	운영 기술
OWL	web ontology language	웹 온톨로지 언어
PaaS	platform as a service	서비스로서 플랫폼
PDCA	plan-do-check-act	계획-실천-확인-조치
PIR	private information retrieval	개인 정보 검색
PKI	public key infrastructure	공개 키 인프라
PLC	programmable logic controller	프로그램 가능 로직 컨트롤러
PLM	product lifecycle management	제품 수명주기 관리
POS	point of sale	판매 시점
ProSe	proximity service	근접 서비스
PUF	physical unclonable function	물리적 복제 불가 기능
QC	quality control	품질 관리
QoS	quality of service	서비스 품질
RAMI 4.0	reference architectural model industrie 4.0	reference architectural model industrie 4.0
RAT	radio access technology	무선 액세스 기술
RDF	resource description framework	자원 기술 프레임워크
REST	representational state transfer	표현 가능 상태 전송
REST API	RESTful application programming interface	REST 방식 애플리케이션 프로그래밍 인터페이스
RFID	radio frequency identification	무선 주파수 ID
ROI	return on investment	투자수익률
RSU	roadside unit	도로변 장치
RV	remote vehicle	원격 차량
SAML	security assertion markup language	보안 증명 마크업 언어
SC	subcommittee	소위원회
SCIM	system for cross-domain identity management	도메인 간 ID 관리 시스템
SCM	supply chain management	공급망관리

약어	영문	한글
SDN	software defined networking	소프트웨어 정의 네트워킹
SDO	standards developing organization	표준 개발 기구
SDP	software defined perimeter	소프트웨어 정의 경계
SLA	service level agreement	서비스 수준 협약서
SMG	semantic mediation gateway	의미론적 중재 게이트웨이
SSE	symmetric searchable encryption	대칭적 검색 가능 암호화
SSO	single sign-on	단일 사인온
STIX	structured threat information expression	구조화 위협 정보 표현
SW	software	소프트웨어
TAXII	trusted automated exchange of indicator information	지표 정보의 신뢰 자동화 교환
TCP	transmission control protocol	전송 제어 프로토콜
TLS	transport layer security	전송 계층 보안
TPM	trusted platform module	트러스트 플랫폼 모듈
TSP	trust, security and privacy	신뢰, 보안 및 개인정보보호
UML	unified modeling language	통합 모델링 언어
UWB	ultra wideband	초광대역
VPN	virtual private network	가상 사설망
WAN	wide area network	광대역 네트워크
WG	working group	실무 그룹
WoT	web of trust	web of trust

조직, 기관 및 회사

약어	영문	한글
3GPP	3rd Generation Partnership Project	3세대 파트너십 프로젝트
AIOTI	Alliance for Internet of Things Innovation	사물인터넷 혁신 협회
AISEC	Fraunhofer Institute for Applied and Integrated Security	독일 프라운호퍼 AISEC
AIST	Advanced Industrial Science and Technology	일본 산업기술 종합 연구소
BITKOM	German Federal Association for Information Technology, Telecommunications and New Media	정보 기술, 전기통신 및 뉴미디어에 대한 독일 연방 협회
BMWi	German Federal Ministry for Economic Affairs and Energy	독일 연방 경제에너지부
CSA	Cloud Security Alliance	클라우드 보안 연합
IDC	International Data Corporation	IDC
IEC	International Electrotechnical Commission	국제 전자기술 위원회
IEEE	Institute of Electrical and Electronics Engineers	전기 전자 기술자 협회
IETF	Internet Engineering Task Force	인터넷 기술 표준 기구
IIC	Industrial Internet Consortium	산업 인터넷 컨소시엄
ISO	International Organization for Standardization	국제 표준화 기구

약어	영문	한글
ISO/IEC JTC 1	Joint Technical Committee 1 of ISO and IEC	ISO/IEC 공동기술위원회
ITU	International Telecommunication Union	국제 전기통신 연합
ITU-R ITU	Radiocommunication Sector	무선 통신 부문
ITU-T ITU	Telecommunication Standardization Sector	전기 통신 표준화 부문
METI	Japanese Ministry of Economy, Trade and Industry	일본 경제 산업성
MIT	Massachusetts Institute of Technology	메사추세츠 공대
MSB	Market Strategy Board (of the IEC)	시장 전략 이사회
NGMN	Next Generation Mobile Networks Alliance	차세대 모바일 네트워크 연합
NIST	National Institute of Standards and Technology	국립 표준 기술 연구소
OMA	Open Mobile Alliance	오픈 모바일 연합
SMB	Standardization Management Board (of the IEC)	표준화 관리 이사회
VDMA	German Mechanical Engineering Industry Association	독일 기계 공학 산업 연합
W3C	World Wide Web Consortium	월드 와이드 웹 컨소시엄
WRC	ITU-R World Radiocommunication Conferences	ITU-R 세계 무선 통신 회의
ZVEI	German Electrical and Electronic Manufacturers' Association	독일 전기 및 전자 제조업체 연합

용어

브라운필드 접근방법

이미 확립된 기존(레거시) 소프트웨어 애플리케이션/시스템의 특정 문제 영역과 관련하여 새로운 소프트웨어 시스템을 개발하여 배포하는 비즈니스 솔루션 접근방법

Cloud Foundry® 접근방법

서비스로서 오픈 소스 클라우드 컴퓨팅 플랫폼(PaaS)

가상 물리 시스템(CPS)

1. 성능 향상을 위한 적응 및 예측 시스템의 구축을 위해 공동 설계된 하이브리드 네트워크 연결 사이버/엔지니어링 물리 요소[출처: 미국 국립표준기술연구소(NIST)]
2. 컴퓨팅 및 물리적 구성요소의 시너지를 기반으로 구축되는 엔지니어링 시스템[출처: 미국 국립과학재단]

엣지

전체적인 IoT 시스템의 운영 도메인을 구성하는 측면

참고: 엣지는 일반적으로 센서, 컨트롤러, 작동기, 태그 및 태그 판독기, 통신 구성요소, 게이트웨이 및 물리적 장치 자체로 구성된다.

게이트웨이 중재 엣지

모든 최종 노드에서 데이터 흐름과 연결을 집계하는 장치

Hadoop®

상용 하드웨어로부터 구축된 컴퓨터 클러스터에서 대규모 데이터 세트를 분산 저장 및 처리하기 위한 오픈 소스 소프트웨어 프레임워크

람다 아키텍처

배치 및 스트림 처리 방법을 활용하여 대용량 데이터를 처리하도록 설계된 데이터 처리 아키텍처

의미론적 상호 운용성

명확한 공유 수단을 통해 데이터를 교환할 수 있는 컴퓨터 시스템 기능

5G
제 5세대 모바일 네트워크

현재 4G/IMT 고급 표준을 뛰어넘는 모바일 전기통신의 차세대 핵심 단계

제1절
소개

기계와 운영 기술(OT) 간의 상호 소통 방식, 또한 이것들과 오늘날의 IT 환경을 대표하는 기반 정보 기술(IT) 플랫폼이 소통하는 방식, 그리고 이러한 기계를 사용하고 통제하는 인간(소비자, 운영자 및 의사결정권자)이 기계 및 운영 기술과 소통하는 방식이 사회 전반에 미치는 영향이 부정적인 것으로 감지되고 있어 이러한 현상에 대해 많은 사람들이 기고하고 있다.

사물인터넷(IoT) 하면 공통적으로 언급되는 이 혁신성을 최초로 언급한 사람은 Kevin Ashton(MIT Auto-ID 센터의 공동 설립자)으로 RFID 및 기타 센서에 대한 글로벌 표준을 개발했다.[5]. 현재 ISO/IEC 정의에 따른 사물인터넷(IoT)이란 “상호 연결된 개체, 인간, 시스템 및 정보 자원이 지능형 서비스와 결합되어 현실 세계와 가상 세계의 정보를 처리하고 대응할 수 있도록 돕는 인프라이다[6].”

"사물인터넷”이라고 하는 신기술은 가상 물리 장치(사물)의 운영 기술을 센서, 컨트롤러, 게이트웨이 및 서비스와 연결하는 데 필요한 폐쇄형 루프 네트워크를 생성하기 위해 오늘날의 인터넷 백본을 공동으로 사용하는 일련의 소비자와 산업 및 공공 부문 그리고 하이브리드 네트워크를 지칭한다. 이렇게 생성된 네트워크는 클라우드 기반이거나 기존의 온프레미스 기반일 수 있으며, 다양한 기법 및 접근법을 사용하는 장치 기능의 최적화에 맞춰 설계된 서비스를 제공하기 위해 의례 특화된 IoT 플랫폼을 사용한다. 대부분의 혁신적인 기술이 그렇듯 이러한 플랫폼은 광범위한 솔루션 제공자들이 자신들의 경험을 토대로 새로운 요구사항을 충족시키기 위해 기존 솔루션 패키지를 재개발하는 방식으로 개발이 이루어진다.

그러나 이런 신종 기술의 잠재성을 실현하려면 기능 최적화 이상의 새로운 접근법이 필요하다.

본 백서는 이런 새로운 접근법과 관련 요구사항을 간결하고 구체적으로 기술한다. 본 백서의 목적은 의사결정권자, 설계자, 개발자 및 구현자가 단순한 변화에 그치지 않고 장치 식별, 모니터링 및 제어 방식에 있어 극적인 변화를 가져오고자하는 차원에서 IoT 계획 특성을 변경할 수 있도록 돕는 것이다. 또한 장치와 네트워크의 안전성을 보장하고 상호 의존적인 다중 시스템이 상호 공조하는 환경 조성 방법에 대해 기술한다.

1.1 배경

오늘날의 IoT는 장치에 부착된 센서로부터 기능 및 환경 데이터를 수집해서 해당 장치 주변의 근접 네트워크에서 기초 분석을 수행하거나 특정 형태의 네트워크를 통해 해당 데이터를 온프레미스 엔터프라이즈 또는 클라우드 플랫폼으로 전달하는 것에 주로 집중하고 있다. 원격 장치 제어 기능이 제한적이고, 데이터 검색, 저장 또는 정적/배치 프로세스로 제한된 데이터 용도에 주로 사용되는 여러 IoT 애플리케이션의 경우, 대체로 이런 모델로도 충분하다.

그러나 그런 제한적인 접근법은 새롭게 개발된 혁신적인 기술의 실질적인 장점을 수용하지 못하고 투자수익률(ROI)이 미미하여 자원 배분에 대한 결정을 내려야 하는 임원들에게는 신뢰를 제대로 심어주지 못한다. 이런 상황에서 예지 정비, 시각화, 물류 추적 시스템, 가정 자동화, 공공 감시, 텔레매틱스, 원격 장치 구성/관리와 같은 첨단 서비스를 제공하는 새로운 IoT 플랫폼이 등장하고 있다.

이런 서비스가 일괄적으로 기업의 핵심 운영과 관련된 모든 측면에 대해 새로운 인사이트를 제공하고 기업의 총 운영비 절감을 비롯해 신규 혹은 개선된 산업/소비자/공공 부문의 서비스를 제공은 물론, 새로운 시장 개척 기회를 부여함으로 투자 의사결정이 당면 과제인 당사자들에게 훨씬 더 큰 가치를 제공한다. 그럼에도 불구하고 의사결정권자들 사이에서는 이런 신성장 동력에 의한 ROI 및 IoT의 변화 가능성에 대한 강한 의구심이 일고 있다.

또한 이런 새로운 접근법은 당면한 과제만큼이나 많은 문제를 야기한다. 이전에는 격리되어있어 매우 안전했던 장치들이 지금은 상당한 위험에 노출될 수 있는 가능성이 생기면서 보안이 더욱 중요해지고 있다. 장치와 장치 연결 네트워크가 다양해지면서 더욱 더 많은 개인 정보가 캡처되고 공유됨에 따라 특히 소비자 IoT 공간에서의 개인정보보호에 대한 관심이 크게 증대되었다. 오늘날 제조, 물류, 보건은 물론 기타 모든 부문에 속하는 산업 및 공공 부문 환경에서 다수의 장비가 낙후되어 디지털화가 불가능하거나 IoT 네트워크에 연결할 수 없으므로 신규 장비에 대한 투자는 몇 년마다 장치를 교체해야 하는 일반적인 소비자 공간과 비교하더라도 훨씬 더 어렵다.

1.2 새로운 전진

오늘날의 솔루션 제공업체들은 특별히 IoT용으로 설계된 첨단 서비스 및 플랫폼을 개발하는데 상당한 진척을 보이고 있다. 이런 새로운 플랫폼과 서비스는 물론 IoT의 혁신적인 잠재력을 확대하고 있지만 아직 한참 부족한 것도 사실이다. IoT가 제공하는 혁신적인 기회를 완전히 실현하려면 오늘날의 IoT 플랫폼 및 장치, 센서, 작동기 및 이들이 지원하는 네트워크의 발전이 필수적이다. 딥 러닝(deep learning) 및 인공지능을 활용한 보다 복잡한 데이터 분석 기법을 위해서는 새로운 접근법이 적용된 획기적인 발전이 필요할 것이다.

자율주행차와 완전 재조합 플랜트 설비 등의 자동화 장치로 인해 실시간 동작을 지원하기 위한 시스템 응답성이 절대적으로 필요해지고 있다. 또한 이를 위해서는 실시간으로 스트리밍되어 메모리에 저장되는 대용량 데이터에서 빠른 검색을 통해 지연시간을 0 수준으로 낮출 수 있는 기능이 필요하다. 실시간 IoT 애플리케이션에서는 근접 네트워크 내에서 또한 전체 네트워크 범위에서 복잡한 처리를 할 수 있는 실시간 플랫폼 지원이 필요하다. 산업 적용 도메인 간 데이터 활용(예: 스마트 홈 산업 적용 부문 생성 데이터를 자동화 부문에 이용)은 새로운 비즈니스 모델 개발의 원동력이 될 수 있다. 통신 운영자와 같은 수평적 산업과 자동차 제조업체와 같은 수직적 산업이 파트너십을 이뤄 신종 사업 모델을 통해 수익을 창출할 수 있다.

IoT 네트워크가 그 어느때보다 중요한 업무 요소로 자리잡음에 따라 장치의 복원성, 안전성, 보안성, 동적 구성, 반자동 혹은 전자동의 재조합 또는 재구성이 핵심 이슈로 떠올랐다. 발빠른 대응은 새로운 IoT 플랫폼 아키텍처의 개발을 촉진할 뿐 아니라 상상을 뛰어넘는 새로운 기회를 불러오고 여러 요구사항을 생겨나게 할 것이다.

이러한 요구사항과 요구사항의 충족을 위한 첨단 플랫폼, 장치, 네트워크 및 아키텍처를 구현하려면 데이터 의미론, 상황화, 변환 및 전송에 대한 표준, 분석 엔진 정보 공유에 대한 표준, 보안성, 연결성, 상호 운용성 및 신흥 IoT 스마트 생태계의 구성 요소 관련 기타 측면에 대한 표준을 생성하고 향상시켜야 한다. 이 신흥 생태계의 첨단 플랫폼(이후 스마트 및 보안 IoT 플랫폼으로 지칭)에서는 스마트 IoT 장치 및 이들을 연결하는 스마트 네트워크의 기능을 개선하고 확장시킬 수 있는 능력이 더욱 요구되고 있다.

1.3 범위

본 백서에서는 다음과 같은 주요 질문을 다룬다.

- 기존 IoT 아키텍처에서 제공하는 주요 기능은 무엇이고 제한사항이나 결점은 무엇인가?
- 기존 기능이 스마트 시티와 같은 미래의 신종 애플리케이션을 실현하기에 충분한가? 충분하지 않을 경우 어떤 기능을 추가하거나 혹은 향상시켜야 하는가? 스마트 및 보안 IoT 플랫폼은 어떤 모습이어야 하는가?
- 기존 기술이 충분한가? 충분하지 않을 경우 현재 애플리케이션의 요구사항을 충족시키기 위해 기존 기술을 개선 및 조정하는 것만으로 문제 해결이 가능한가? 아니면 신기술이 필요한가?
- 어떤 국제 표준이 수립되어 있는가 혹은 현재 조사 중인 표준이 있는가? 수립되어 있는 경우 IoT 애플리케이션 지원을 위해 추가적인 표준화 노력이 필요한가?
- 새로운 표준을 정의하거나 발행 또는 유지관리하기 위한 요구사항을 누가 파악해야 하는가?
- IEC의 역할은 무엇이어야 하는가?

1.4 이 백서의 구조

본 백서는 다음과 같이 구성된다.

- 제2절에서는 IoT 현황 개요를 제공하고 데이터 상관관계와 정보 검색, 연결성과 통신, 통합과 상호운용, 보안성, 개인정보보호와 신뢰를 비롯하여 기존 IoT 플랫폼의 기본적인 기능을 기술한다. 또한 오늘날의 IoT 플랫폼 구축에 사용되는 가장 공통적인 아키텍처 패턴을 기술하고 기존의 표준 아키텍처에 대한 간략한 개요를 제공한다. 기존 IoT 시스템의 주요 결점 및 제한사항을 파악할 수 있도록 이에 대한 세부 내용을 제공하면서 이 장을 끝맺는다.
- 제3절에서는 보안성, 통합성 및 결합성과 더불어 첨단 분석 및 시각화와 같은 주요 논제와 관련하여 겪게 되는 결점에 대해 체계적으로 파악하여 기술한다.
- 제4절에서는 3가지 서로 다른 적용 부문(즉, 산업, 소비자 및 공공 부문)에 대한 차세대 IoT 사용 사례를 중점적으로 살펴본다.
- 제5절에서는 스마트 및 보안 IoT 플랫폼과 스마트 장치 및 스마트 네트워크에 대한 개요를 제공한다. 또한 스마트 및 보안 IoT 플랫폼 구축 시 나타날 것으로 예상되는 기술적 과제를 설명한다.
- 제6절에서는 스마트 및 보안 IoT 플랫폼을 실현하는 데 필요한 몇 가지 주요 차세대 지원 기술(enabling technologies)을 중점적으로 살펴본다.
- 제7절에서는 현재 표준 현황과 스마트 및 보안 IoT 플랫폼에 대한 표준화 요구사항을 기술한다.
- 제8절에서는 IEC 및 기타 표준 관련 조직(예: 정부)에 대한 구체적인 표준 개발 권고사항을 제시하면서 본 백서를 마무리한다.

제2절
오늘날의 IoT

IoT, IoT 플랫폼, IoT 아키텍처 및 IoT "사물" 자체에 대한 "표준" 정의는 다양하다. 차세대 IoT와 스마트 및 보안 IoT 플랫폼에 대한 공유 비전의 토대를 올바르게 정립하기 위해 IoT의 현황, IoT 시스템을 구성하는 다양한 컴포넌트, 주요 IoT 아키텍처 정의에 대한 IEC의 입장을 정확히 정의할 필요가 있다.

2.1 IoT 컴포넌트

기존 및 신흥 IoT 아키텍처 패턴(2.3절 참조)이 여러 가지 있지만 이 모두가 물리 장치, 엣지 및 플랫폼 개념이라는 단일 컴포넌트 세트를 공통적으로 공유한다. 이어지는 절에서 이런 개념을 구체적으로 기술하고 본 백서에 사용되는 공통적인 용어 정의를 제공한다.

2.1.1 물리 장치

오늘날의 IoT 시스템 아키텍처에서, 사물인터넷의 "사물"은 가상 물리 장치, 장치, 엔드포인트, 엔티티, 인격 엔티티 등 다수의 명칭으로 불린다. 그림 2-1을 보면 이런 사물의 상주 도메인(즉, 개별 식별정보)에 관계없이 물리적인 장치로서 공통 속성을 공유한다. 이런 물리 장치는 장치에 내장되거나 작동기 또는 컨트롤러 형태로 장치에 직접 부착되는 등으로 일정 수준의 컴퓨팅 기능을 포함할 수 있다. 또한 물리 장치는 다른 물리 장치, 엣지 플랫폼, 게이트웨이 및 하나 이상의 IoT 시스템에 직접 연결할 수도 있다.

2.1.2 엣지

오늘날의 IoT 시스템 아키텍처에서 "엣지"의 개념은 전체 IoT 시스템의 운영 도메인을 구성하는 측면과 연관된다. 엣지는 일반적으로 센서, 컨트롤러, 작동기, 태그 및 태그 판독기, 통신 컴포넌트, 게이트웨이 및 물리 장치 자체로 구성된다. 엣지는 운영 컴포넌트가 상호 간, 플랫폼 간, 그리고 경우에 따라서는 다른 엣지의 컴포넌트 간에 직접 연결하여 통신 및 상호작용을 하는 공간이다. 엣지는 플랫폼에 직접 연결되는 단일 물리 장치처럼 작을 수도 있고 종합적 통신 기능 컴포넌트 및 엣지 컴퓨팅 플랫폼과 모든 제조 설비를 갖춘 제조 플랜트만큼 클 수도 있고 혹은 그 중간 규모일 수도 있다. 엣지 내에는 처리를 지원하는 플랫폼이 존재하거나 존재하지 않을 수도 있다. 엣지 통신 컴포넌트는 컨포넌트들이 연결하는 독립적인 단일 LAN(로컬 영역 네트워크) 또는 복수 LAN으로 구성될 수 있으며, 컴포넌트는 이 LAN에 연결하기 위해 하나 이상의 프로토콜 및 0개(0개의 경우 직접 게이트웨이에 연결) 이상의 라우터를 사용해서 엣지 게이트웨이/허브/버스에 연결하고 더 나아가 더 큰 네트워크 또는 클라우드 기반 솔루션(플랫폼 포함)에 연결한다. 로컬 네트워크는 내부 연결 또는 게이트웨이/허브 연결을 위해 허브 앤 스포크(Hub and Spoke), 메시(mesh), WiFi, 셀룰러 또는 기타 토폴로지를 사용할 수 있다.

엣지 처리는 엣지 컴포넌트나 시스템 기능의 요구사항 또는 제한사항을 다룬다. 산업 현장에 사용되는 장치의 경우 이런 요구사항 및 제한사항으로 장치 연결에서 로컬 연결 기능만 사용할 수 있다는 점을 들 수 있다.

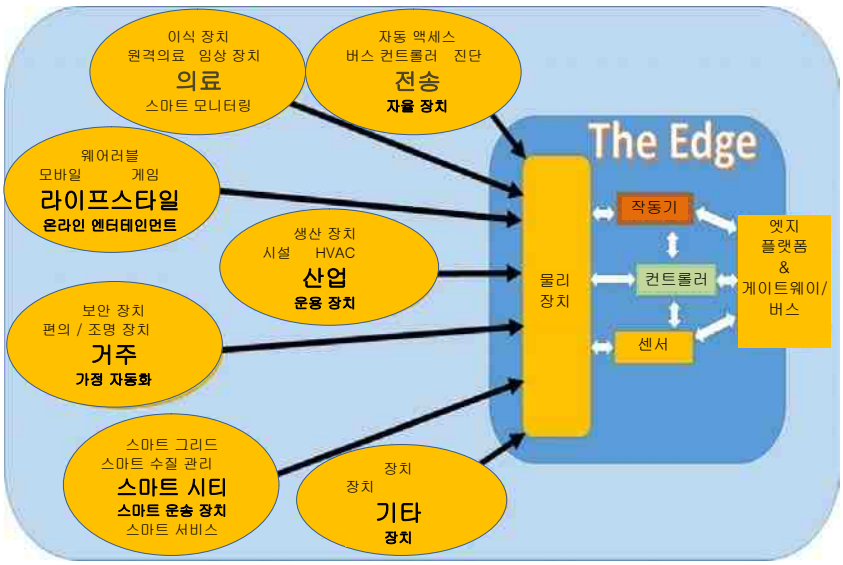


그림 2-1 | 일반적인 엣지 환경

기타 요구사항으로 장치가 오프라인에서 작동하도록 적절하게 구성하는 것이 있다. 즉, 특정 장치는 쉼없이 24시간 온라인에 연결할 수 없기 때문에 오프라인일 때 데이터를 수집하여 온라인에 연결되었을 때 데이터를 업로드하기 때문이다. 또한 IoT 플랫폼의 확장으로서 또는 IoT 플랫폼과 독립적으로 엣지 분석, 엣지 트랜잭션 처리 또는 또 다른 엣지 기능에 대한 필요나 요구가 있을 수 있다. 이 플랫폼에 모든 데이터를 전송하여 저장할 필요는 없기 때문에 엣지가 로컬 스토리지 기능을 제공한다. 플랫폼에 전송되는 데이터 용량을 줄이기 위해 장치 데이터의 동적 필터링, 샘플링 또는 집계가 가능한 엣지 처리가 종종 필요하다.

2.1.2 플랫폼

오늘날의 IoT 시스템 아키텍처에서, 일반적으로 IoT 플랫폼이란 하나 이상의 통합 엣지 환경을 아우르는 아키텍처의 기능적 측면을 물리적으로 일괄 실현하는 도메인들의 중앙 허브를 나타낸다. IoT 플랫폼은 상호운용 가능 IoT 서비스 및 해당 서비스의 관리를 제공하기 위해 다양한 애플리케이션과 컴포넌트가 들어가는 통합된 물리/가상 엔티티 시스템이다. 여기에는 네트워크, IoT 환경, IoT 장치(센서, 컨트롤러, 작동기, 태그 및 태그 판독기, 게이트웨이), 부착된 물리 장치, IoT 운용 및 관리, IoT 시스템의 공급자/시장/일시적 이해관계자에 대한 외부 연결 등이 포함된다[7]. 일반적인 IoT 플랫폼은 다음과 같은 도메인을 포함하거나 이러한 도메인과 상호작용한다[8].

- **컨트롤** – IoT 장치에 센서, 작동기, 통신, 자산 관리 및 실행을 포함할 수 있도록 제어 메커니즘에 의해 실행되는 기능으로 구성된다. 산업 환경에서, 일반적으로 컨트롤 시스템은 물리 장치에 연결되는 IoT 장치에 근접하여 위치한다. 소비자 환경에서 컨트롤 시스템은 근접 또는 원격 장소에 위치할 수 있다. 공공 환경에서 컨트롤 시스템은 일반적으로 근접 또는 원격 조합을 포함한다.

- **운용** – 일반적으로 IoT 플랫폼 및 복수 컨트롤 도메인 간 운용 최적화와 관련하여 예측, 최적화, 모니터링/진단, 프로비저닝/배포 및 관리를 포함한다.
- **정보** – 일반적으로 IoT 플랫폼 및 엣지의 일부 기능과 관련하여 핵심 IoT 분석 및 데이터로 구성되고, 최적화된 의사결정, 시스템의 전반적 운용 및 시스템 모델의 개선을 지원하기 위해 데이터를 수집, 변환, 유지 및 모델링하는 일을 담당한다.
- **애플리케이션** – 일반적으로 IoT 플랫폼에 대한 애플리케이션이지만 비즈니스 도메인의 일부인 컴포넌트를 포함할 수도 있다. 일반적으로 애플리케이션 프로그램 인터페이스, 사용자 인터페이스, 로직 및 규칙으로 구성되며 IoT 시스템 자체에 대한 기능 실현 로직의 구현을 담당한다.
- **비즈니스 도메인** – 일반적으로 운용, 정보, 애플리케이션 도메인에 정의되고 컨트롤 도메인에 일부 정의된 핵심 IoT 기능을 갖춘 플랫폼과 분리된 플랫폼에 대한 도메인이며, IoT 기능에 CRM, ERP, 대금청구, 결제 등의 백엔드 애플리케이션을 통합한다.

IoT 플랫폼 자체는 클라우드에 위치하거나, 온프레미스에 위치하거나, 클라우드 및 온프레미스에 모두 위치할 수 있다. 이 플랫폼은 단일 서버, 복수 서버 또는 물리 및 가상 서버의 조합으로 구성될 수 있다. 소속된 물리적 위치나 아키텍처에 관계없이, IoT 플랫폼을 구성하는 도메인(운용, 정보, 애플리케이션뿐 아니라 비즈니스/컨트롤 측면도 포함)에서는 도메인 간, 비즈니스 도메인의 백엔드 애플리케이션 간, 엣지에 상주하는 물리적 시스템/컨트롤 도메인 간에 여러 데이터/컨트롤 흐름이 이루어진다. IoT 플랫폼의 추가 서비스에는 IoT 시스템 외부 자원, 네트워크 서비스, 클라우드 통합 서비스 및 개별 플랫폼 제공자가 정의한 다른 여러 서비스에 액세스하기 위한 자원 교환이 포함된다.

2.2 IoT 시스템 설계

2.1절에서 기술한 IoT 시스템 컴포넌트의 사용 시 IoT 시스템 설계자를 지원하는 여러 도구가 있다. 그 가운데 핵심은 ISO/IEC/IEEE 아키텍처 기술 표준이다[9]. 또한 다양한 표준화 기구와 IoT 중심 컨소시엄이 제공하는 다수의 IoT 아키텍처/참조 아키텍처도 이용 가능하다. 하위 절에서는 IoT 2020 스마트 및 보안 IoT 플랫폼에 대한 다양한 옵션과 잠재적 기회에 대한 이해 증진을 위해 가장 눈에 띄는 접근법의 개요를 제공한다.

2.2.1 ISO/IE 30141, 사물인터넷 참조 아키텍처(IoT RA)

국제표준화기구(ISO) 및 IEC의 공동기술위원회 1(ISO/IEC JTC 1)은 작업 그룹(WG) 10에 권고사항 검사 및 제공과 사물인터넷에 대한 국제 표준 개발을 인가하였다. 이 그룹의 첫 번째 주요 결과물은 국제 표준 ISO/IEC 30141의 규격 초안(working draft)이다. 이 규격 초안은 IoT 구현자들이 직면한 문제와 IoT 아키텍처 설계 및 구현의 구체적 측면에 대한 주요 세부 내용을 제공하는데 이는 원활한 상호 운용성과 플러그 앤 플레이 IoT 시스템의 설계에 있어 이후 IoT 설계자들의 방향성을 설정하는 데 도움이 된다. 이 초안에서는 IoT 세상의 다양한 컴포넌트와 더불어 개념 모델, 참조 모델, 뷰 구성의 참조 아키텍처를 정의한다. WG 10은 2.2절에서 언급한 다른 아키텍처를 정의하는 수많은 그룹과 협력 계약을 체결하고 있으며, 현재 규격 초안에서 그룹이 제공하는 내용을 쉽게 확인할 수 있다.

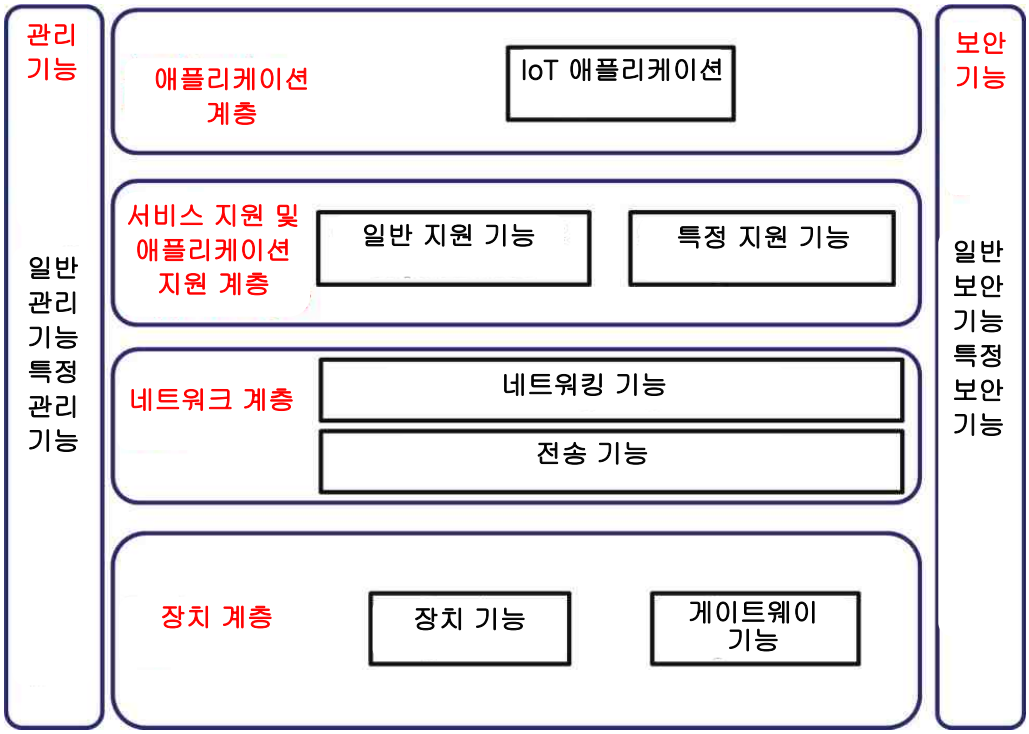


그림 2-2 | ITU-T Y.2060 개요

2.2.2 ITU-T Y.2060

국제전기통신연합 전기통신 표준화부문(ITU-T) 연구 그룹 13에서 ITU-T Y.2060을 작성하였다. 이 표준은 IoT의 기능적 특징과 높은 수준의 요구사항 및 IoT 참조 모델을 정의하고 있다[10]. 정의된 기능적 특징에는 상호 연결성, 사물 관련 서비스, 이질성, 동적 변경, 거대한 규모 등이 있다. IoT에 대한 높은 수준의 요구사항 목록에는 ID 기반 연결성, 상호 운용성, 자동 네트워킹, 위치 기반 기능, 보안성, 개인정보보호, 고품질과 높은 안전성의 인체 관련 서비스, 플러그 앤 플레이 및 관리의 용이성 등이 포함되어 있다.

이 모델은 공식적으로 주요 용어인 “장치”, “사물” 및 “사물인터넷”을 핵심 개념(여러 모델과 마찬가지로, IoT의 특별한 기능인 장치 연결성에 중점을 둠)으로 정의한다. 그림 2-2와 같이 이 모델은 애플리케이션, 서비스 지원 및 애플리케이션 지원, 네트워크 및 장치 등 4개의 계층으로 구분된다. 이 모델은 각 계층에 필요한 관리 기능 및 보안 기능을 다룬다.

보안성은 일반 및 특정 보안 기능으로 구분된다. 특정 기능은 애플리케이션 요구사항에 영향을 받는다. 일반 기능은 애플리케이션 독립적이며 각 계층에 대해 정의된다. 권한 부여 및 인증이 애플리케이션, 네트워크 및 장치 계층에서 정의된 기능이다. 애플리케이션 계층에는 애플리케이션 데이터 기밀성 및 무결성 보호, 개인 정보 보호, 보안성 감사 및 바이러스 백신 기능이 추가된다. 네트워크 계층에는 데이터 이용과 더불어 신호 데이터 기밀성 및 신호 무결성 보호가 추가된다. 장치 계층에는 장치 무결성 검증, 액세스 제어, 데이터 기밀성 및 무결성 보호 기능이 추가된다.

2.2.3 IIC IIRA

산업 인터넷 컨소시엄(IIC)은 IoT의 산업 애플리케이션에 중점을 둔다. IIC 산업 인터넷 참조 아키텍처(IIRA)는 그림 2-3과 같은 4가지 관점(비즈니스, 활용, 기능 및 구현)을 정의한다. 비즈니스 및 활용 관점은 산업 시스템 구현 시 비즈니스 문제 및 비즈니스 사례에 부여되는 중요도를 결정하고, 설계에서 시스템이 사용되는 도메인 및 컨텍스트의 의미를 결정한다. 특별히 기술적으로 강조되는 관점은 기능과 구현 관점이다. 기능 관점은 아키텍처 뷰를 컨트롤, 운용, 정보, 애플리케이션 및 비즈니스의 기능 도메인으로 구분한다. 구현 관점은 일반적인 아키텍처(구조, 컴포넌트 배포, 연결 토폴로지)에 중점을 두어 시스템 컴포넌트(인터페이스, 프로토콜, 동작 등)의 기술적 설명, 기능 컴포넌트 및 기능-구현 컴포넌트에 대한 활용 관점 활동의 구현 매핑, 주요 시스템 특성의 구현 맵을 제공한다. 이런 관점은 아키텍처 설계자들이 고유한 아키텍처 뷰를 작성할 수 있도록 돕는다.

보안성(및 보안/안전 관련 문제)은 각 관점과 관련하여 명확하게 식별하고 논의한다. 이와 같이 보안 문제를 특정 관점과 함께 논의하면 모든 이해관계자가 보안 중심 설계의 중요성을 이해하게 된다. 안전성, 개인정보보호 및 신뢰, 복원성, 통합성, 상호 운용성 및 결합성, 연결성, 데이터 관리, 분석, 지능적 및 탄력적 제어, 동적 결합성, 자동 통합 등 주요 시스템 문제는 개별적으로 다룰 것이다.

그림 2-3 | IIC 산업 인터넷 참조 아키텍처

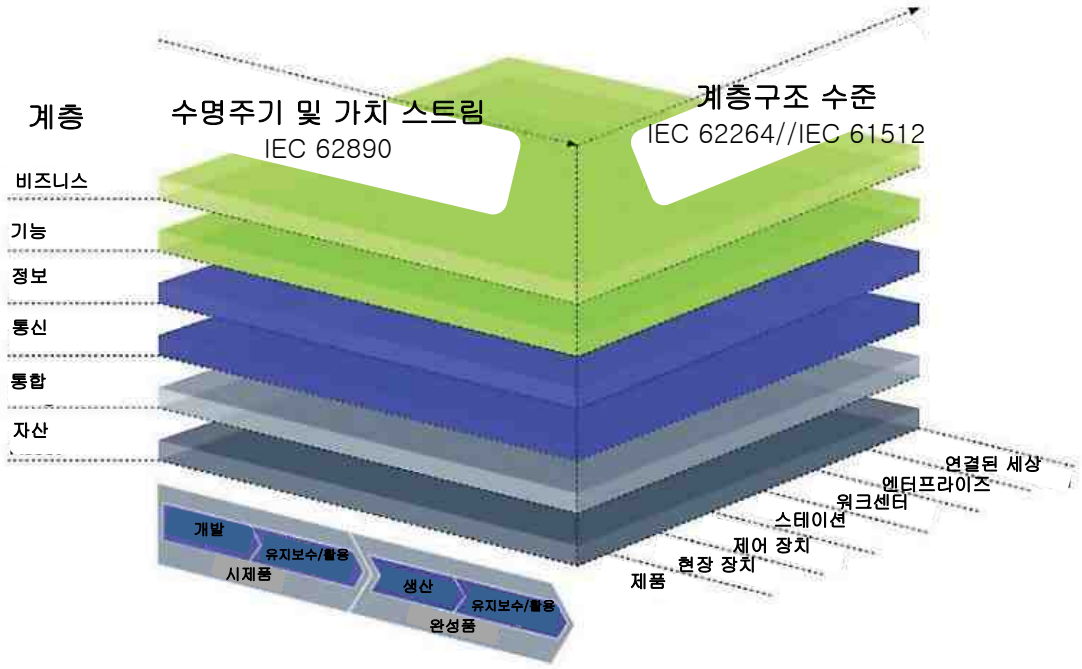


그림 2-4 | 산업 참조 아키텍처 모델 4.0

2.2.4 RAMI 4.0

현재 개발이 한창인 산업 참조 아키텍처 모델 4.0(RAMI 4.0)은 BITKOM(독일 연방 정보 기술 협회), ZVEI(독일 전기 및 전자 제조업체 협회) 및 VDMA(독일 엔지니어링 협회)가 차세대 산업 제조 시스템의 참조 아키텍처를 구축하기 위해 공동으로 추진하고 있다[11].

그림 2-4와 같이 RAMI 4.0의 핵심은 Industrie 4.0 기술 분류에 사용되는 3차원 계층화 모델이다. 이 모델은 국제 표준 IEC 62264 및 IEC 62890을 통합하여 확립된 모델을 통해 차세대 시스템의 서로 다른 측면을 기술한다.

이 모델은 공장 또는 시설의 다양한 기능을 표현하는 엔터프라이즈 IT 및 제어 시스템용 IEC 62264 표준 시리즈에 따라 "계층구조 수준"을 정의하고, Industrie 4.0의 용도로 확장되어 IoT 및 서비스 인터넷("연결된 세상"이라고 함)과 작업물("제품"이라고 함)에 대한 연결성을 포함한다. 또한 이 모델은 설계, 생산, 배달, 활용, 유지보수 등의 전체 "수명주기 및 가치 스트림"을 다루며, 제품 및 시설 수명주기를 표현하는 IEC 62890을 토대로 하여 설계 및 시제품 단계와 생산 단계를 구분하는 수단으로 "시제품(type)"과 "완성품(instance)" 개념을 추가한다. 마지막으로 "계층" 축은 기계를 컴포넌트 속성으로 분류하려는 목적으로 공간을 6개의 계층으로 구분한다.

기본 RAMI 모델에는 보안 기능이 추가되어, 모델의 각 계층 및 각 차원 내에 보안성이 구축된다.

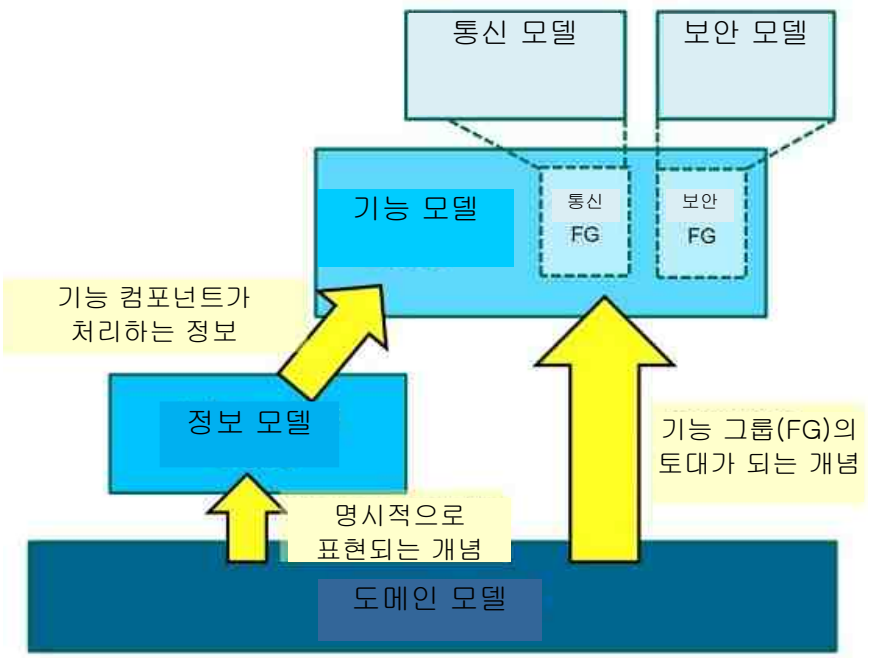


그림 2-5 | IoT-A ARM

2.2.5 IoT-A ARM

제 7차 프레임워크 프로그램의 유럽 등대 통합 프로젝트(European Lighthouse Integrated Project)인 IoT-A는 IoT-A 아키텍처 참조 모델(ARM)을 IoT 기술의 성장과 개발 촉진 용도로 쓰일 기초적인 참조 아키텍처 문서로서 개발했다. [12] IoT-A ARM은 ARM의 가장 추상적인 컴포넌트를 구성하는 참조 모델과 함께 3가지 컴포넌트로 이루어진다. 그림 2-5와 같이 이 참조 모델은 도메인, 정보, 기능, 통신 및 보안 모델로 구성된다. 도메인 모델은 “장치”, “IoT 서비스” 및 “가상 엔티티”(물리적 엔티티를 모델링)와 같은 IoT의 핵심 개념을 기술한다. 정보 모델은 IoT 시스템에 있어 정보의 일반적인 구조적 속성을 정의한다. 기능 모델은 도메인 모델에 정의된 관계를 바탕으로 기능 그룹을 구분한다.

통신 모델은 IoT 환경에서 통신의 복잡성을 다룬다. 신뢰, 보안성 및 개인정보보호(TSP) 모델은 IoT 사용 사례 시나리오에 대한 중요도에 따라 구체적으로 식별하여 각각을 개별적으로 다룬다.

IoT 참조 모델과 더불어 ARM은 “호환 IoT 아키텍처 구축의 표준”인 IoT 참조 아키텍처를 정의하며, 실제 아키텍처를 생성하는 데 있어 IoT 시스템 설계자를 안내하는 지침을 포함하고 있다.

2.2.6 AIOTI 참조 아키텍처

사물인터넷 혁신 연합(AIOTI)은 IoT 시장에서 유럽 기업 간의 대화와 교류를 진전시키고 지원하기 위해 2015년에 사물인터넷 혁신연합이다. AIOTI는 두 가지 IoT 모델(도메인 모델과 기능 모델)을 개발했다.

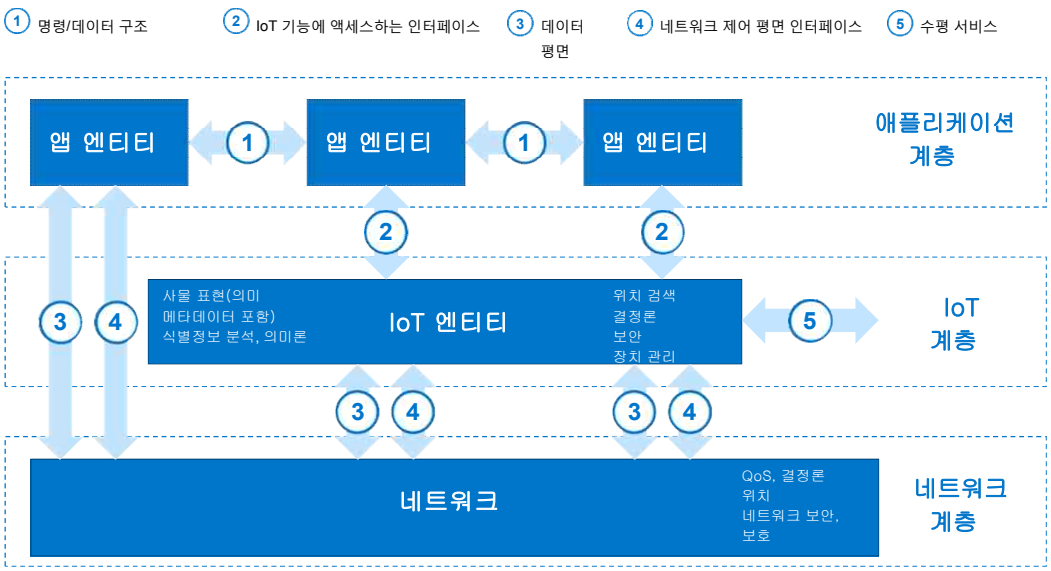


그림 2-6 | AIOTI 참조 아키텍처

IoT-A 도메인 모델(2.2.5절 참조)에서 파생된 AIOTI 도메인 모델은 최상위 수준에서 도메인의 주요 개념 및 관계를 캡처해서 도메인에 대한 공통 어휘 목록을 제공하며 다른 모든 모델 및 분류 체계의 토대가 된다. 이 모델에서 사용자(인간 또는 기타 사물)는 물리적 엔티티와 상호작용한다. 이 상호작용은 가상 엔티티(물리적 엔티티의 디지털 표현)와 연관된 IoT 서비스가 중재한다. 그런 다음 IoT 서비스는 실제 물리적 엔티티의 기능을 수행하는 IoT 장치를 통해 사물과 상호작용한다.

AIOTI 기능 모델은 도메인 내의 기능 및 인터페이스(상호작용)를 기술하되, 도메인 외부의 상호작용도 제외하지 않는다. 그림 2-6과 같이 이 기능 모델은 애플리케이션, IoT 및 네트워크 등 3개의 계층으로 구성된다.

이 기능 모델은 IoT 시스템의 기능과 기능 간 인터페이스를 기술한다. 기능에 특정한 구현이나 배포가 필요한 것은 아니므로 운영상의 배포에서 기능이 물리적 엔티티에 반드시 상응해야 한다는 가정을 두어선 안된다. 하나의 물리적 장비에서 여러 기능의 그룹화는 기능 모델의 인스턴스화를 통해 여전히 가능하다.

2.3 아키텍처 패턴

2.2절에 제시된 다양한 참조 아키텍처의 활용 시 다양한 아키텍처 패턴이 등장하여 광범위한 채택과 구현이 이뤄지고있다. 다음 절에서는 스마트 및 보안 IoT 플랫폼의 요구사항 및 기회에 대한 이해 증진을 위해 이들 중 가장 인기 있는 패턴을 소개한다.

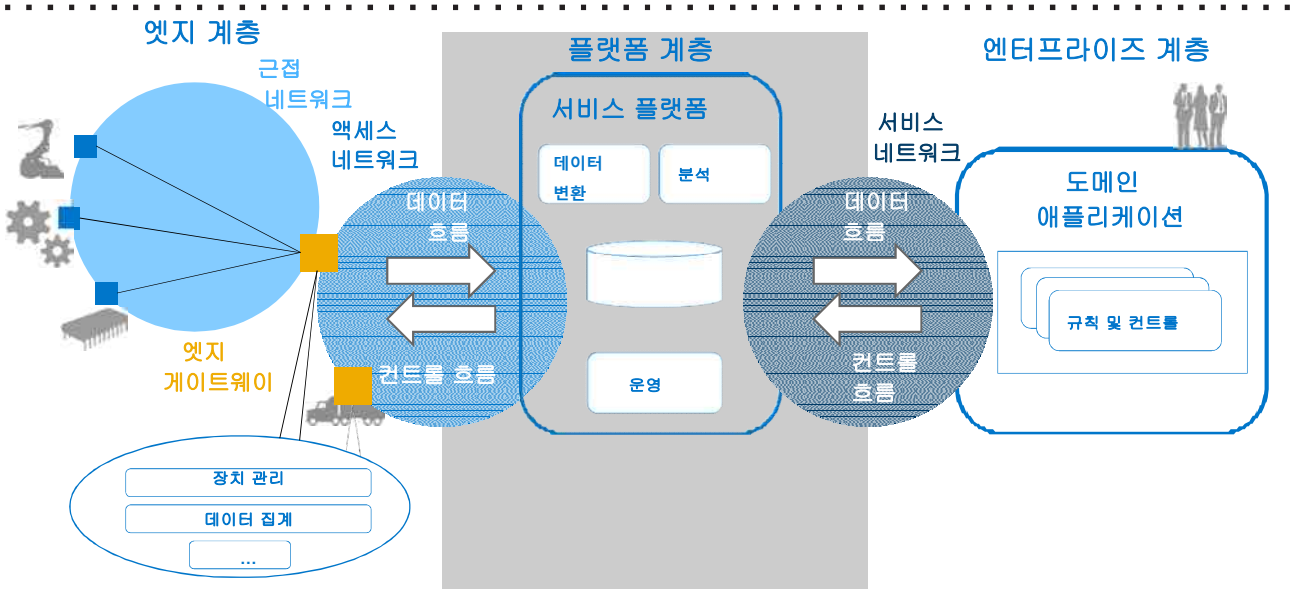


그림 2-7 | 3계층 아키텍처 패턴

2.3.1 3계층 아키텍처

이 3계층 아키텍처는 근접, 액세스 및 서비스 네트워크로 연결되는 엣지, 플랫폼 및 엔터프라이즈 계층으로 구성된다. 이 아키텍처뿐만 아니라 이어지는 다른 아키텍처의 네트워크에서는 모두 일반적으로 RFID, Bluetooth, Cellular, ZigBee, Z-Wave, Thread 및 Ethernet과 같은 유무선 지원 기술 조합을 사용한다. 그림 2-7과 같이 엣지 계층은 근접 네트워크를 사용하여 엣지 노드(장치 또는 “사물” 수준)에서 데이터를 수집한다.

본 데이터는 액세스 네트워크를 거쳐 플랫폼 계층으로 전달되며 이 계층에서 엣지 계층의 데이터를 처리하여 엔터프라이즈 계층으로 전달하고 아울러 엔터프라이즈 계층의 제어 명령을 처리하여 다시 액세스 네트워크를 거쳐 엣지 계층으로 되돌려 중계한다. 플랫폼 계층은 서비스 네트워크를 사용하여 최종 사용자 인터페이스, 제어 명령 및 도메인별 애플리케이션을 제공하는 엔터프라이즈 계층과 통신한다[13].

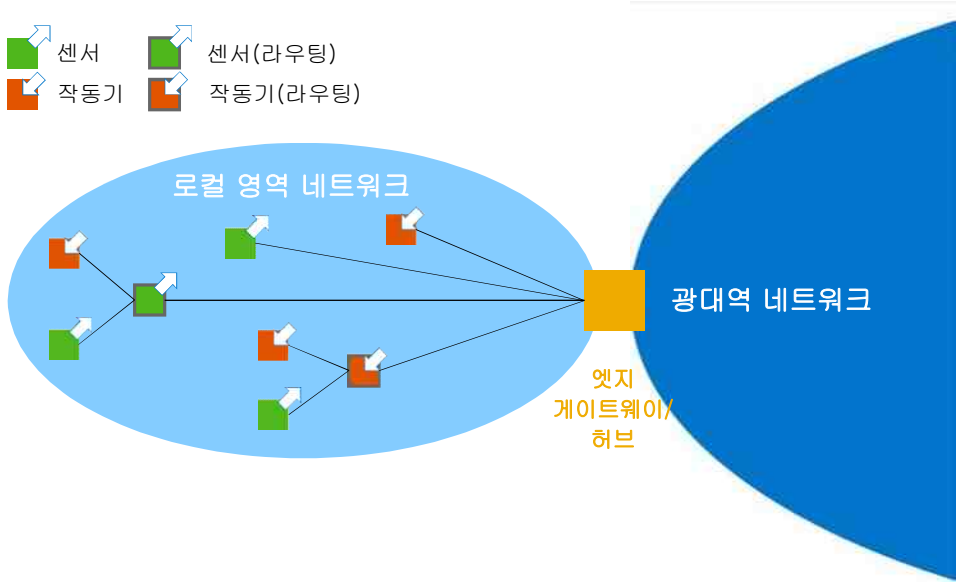


그림 2-8 | 게이트웨이 중재 엣지 아키텍처 패턴

2.3.2 게이트웨이 중재 엣지 연결 및 관리

게이트웨이 중재 엣지 연결 및 관리는 게이트웨이가 한쪽 편의 엣지 노드에 대한 로컬 영역 네트워크(LAN)와 그 반대편의 광대역 네트워크(WAN) 사이의 중재자 역할을 하는 아키텍처 패턴이다. 이는 WAN 네트워크의 엔드포인트 역할을 하며, 잠재적으로는 LAN 상의 엣지 장치에 대한 관리 엔티티로서 엣지 장치를 WAN과 격리하는 역할을 한다. 그림 2-8과 같이 센서와 작동기는 엣지 게이트웨이에 직접 연결하거나 하나 이상의 라우터를 통해 연결한다. LAN 자체의 토폴로지는 허브 앤 스포크(Hub and Spoke)(LAN 내의 모든 통신이 엣지 게이트웨이 경유) 또는 메시(피어 투 피어)(일부 엣지 노드가 라우팅 기능 보유)일 수 있다. 엣지 게이트웨이 자체를 경유하지 않는 다른 노드 간 연결 경로가 있을 수도 있다.

2.3.3 엣지 투 클라우드

엣지 투 클라우드(edge-to-cloud) 아키텍처 패턴은 모든 엣지 자산을 엣지 게이트웨이 뒤에 격리하는 대신 직접적으로 광대역에 연결하며 처리 기능을 포함한다는 점에서 게이트웨이 중재 엣지 패턴과 다르다[13].

2.3.4 다계층 데이터 스토리지

다계층 데이터 스토리지는 기능 및 스토리지 제약을 최적화하기 위해 기능과 목적별로 스토리지 계층을 분리하려는 데이터 아키텍처이다. 예를 들어 스토리지 계층은 기능, 용량 및 아카이브 목적에 따라 별도 계층으로 구분될 수 있다.

2.3.5 분산 분석

분산 분석 아키텍처는 엣지에 근접한 근접 분석을 중앙집중화된 아키텍처 부분의 집중 분석과 결합한다. 예를 들어 이 아키텍처 패턴은 지연시간이나 다른 네트워크 제약으로 인해 완전한 중앙 처리가 차선의 솔루션이 될 경우 적절하다.

2.3.6 람다(Lambda) 아키텍처

람다 아키텍처는 IoT용으로 설계되지 않았고 분석을 위한 데이터 흐름 이외에 구현 뷰의 어떤 측면도 다루지 않는다는 점에서 본 절에서 제시하는 다른 참조 아키텍처와 다르다. 람다 아키텍처를 여기에 포함하는 이유는 센서에 의해 생성되는 방대한 양의 데이터를 처리할 수 있는 IoT 시스템 설계에 널리 사용되고 있고 중요하기 때문이다.

람다 아키텍처는 그와 같은 처리를 배치 뷰와 스트림 뷰의 두 가지 뷰로 구분하여 IoT 빅 데이터와 연관된 대량 데이터 흐름의 실시간 처리에 대한 요구사항을 다룬다. 이 아키텍처 자체는 3개의 계층[즉, 마스터 데이터 세트(변경불가, 추가 전용)를 담당하는 배치 계층, 효율적인 검색을 위해 배치 계층의 데이터 뷰를 색인화하는 서비스 계층, 저지연 기능 및 스트림 뷰의 최신 데이터 액세스를 제공하기 위한 실시간 데이터의 고속 계층]으로 구분된다. 수신 데이터는 보다 높은 지연시간 및 전체적인 처리를 위한 배치 계층과 데이터나 분석을 신속히 제공하기 위한 즉각적인 처리용 고속 계층 모두에 전송된다. 아직까지 배치 계층은 보다 정확하고 완벽한 방식으로 통합되지 않았다.

이는 실시간 애플리케이션이 수백 또는 수천 엣지 장치로부터 수신되는 데이터를 처리해야 한다거나 관련된 데이터가 방대함에도 불구하고 일부 상황에 예비적 혹은 즉각적으로 대응할 수 있어야 한다는 점에서 IoT 아키텍처와 특별한 관련성을 갖는다. 동시에 이런 동일 애플리케이션에 지속 응답, 초기 결과 보정, 이력 또는 아카이브 용도, 확장 분석 등을 위해 본 데이터와 연관된 보다 정확한 분석이 필요할 수 있다.

2.4 IoT 특징

2020 스마트 및 보안 IoT 플랫폼을 올바르게 정의하려면 IoT 아키텍처 개념 및 패턴에 대한 이해와 더불어 오늘날 IoT의 일반적인 특징을 완전히 파악하는 것도 중요하다. 이어지는 하위 절에서는 오늘날의 IoT에 대한 중요 고려사항을 나타내는 IoT 시스템의 핵심 특징을 살펴본다.

2.4.1 데이터 상관 관계 및 정보 검색

스마트 데이터 처리야 말로 IoT 기능의 핵심이다. 오늘날의 IoT에서 센서를 널리 분배하고 데이터를 신속하고 효율적으로 수집할 수 있는 기능은 새로운 형태의 협업을 촉진한다. IoT 시스템의 컴포넌트는 스트림, 배치 및 비동기 데이터 등의 서로 다른 특정 유형의 데이터를 생산한다. 소규모 학습과 관련한 데이터 처리는 엣지용으로 추진될 수 있는 경우가 많은 반면 대규모 처리는 중앙집중화를 요구하는 경향이 있다. 그와 같은 데이터는 프로세스 개선, 오류 탐지 및 실제 상황의 비즈니스 워크플로우 통합을 지원하여 시스템 피드백 용도로 처리 및 사용될 수 있다. 오늘날의 IoT는 또한 데이터 사용을 더 실용적이면서 직관적으로 만들어 해석을 용이하게 하기 위해 IoT가 생성하는 데이터의 의미론적 모델을 사용한다. (스마트 시티 등의) 의미론이 지원되는 공동세계 모델과 엔티티에 대한 모든 특성 정보를 구성하는 데이터 추상화로 가상화된 엔티티를 활용함으로써 데이터를 제공하는 센서보다 차원높은 현실세계 엔티티를 모델링할 수 있다. 제공하는 정보의 의미론에 모든 정보 출처가 합의될 수 있으므로 적정 수준의 추상화는 실시간 상황 처리에 유용하다.

2.4.2 통신

오늘날 IoT의 통신 아키텍처는 특정 상황에서 어떤 네트워크와 엣지 아키텍처의 조합이 유용한가에 따라 가변적이다. 현재 통신은 대부분 VPN을 통해 또는 전용 공공 네트워크를 사용하여 이루어진다. 기존 애플리케이션은 엣지와 중앙집중화 서버 및 집계 지점 사이에서 발생하는 통신에 의존한다. 오늘날의 IoT 통신 기능은 이미 엔터프라이즈들의 일반적인 독립부문에서 사용되고 있다. 공장 통합 솔루션은 특정 제조 영역 내의 응용 및 개선만 허용하지만 IoT 플랫폼은 여러 이종 엔티티에서 정보를 수집할 수 있고 일반적인 엔터프라이즈 독립부문을 넘어선 협업을 지원한다.

2.4.3 통합 및 상호운용

오늘날의 IoT 솔루션은 통합 및 상호운용의 수준을 달리하여 특성화된다. 통합 노력을 통해 시스템이 원래 상호운용 목적으로 설계되지 않았던 요소와 협업하도록 변경되는 경우가 많다. 그러나 아직은 완전히 가용한 단계가 아니며, 기업체 내에서 제품들 간에는 일정 수준의 통합 및 상호 운용성이 갖춰져 있으나, 상위 수준의 기술에 있어서는 그 기술보다 수준이 낮은 기술과 통합되어 있는 경우도 있다.

대개의 경우 통합은 통신을 위한 공통 분모로 HTTP 및 REST API를 사용하고 IP가 중간에 존재하는 일반적인 모래시계 모델을 기반으로 한다. IoT 서비스의 인에이블러(enabler)는 온프레미스인지 클라우드인지와는 관계없이 서로 다른 제공자가 제공하기 때문에 이는 특히 유용하다. 그러나 이는 지원 솔루션의 일부인 사물지능통신 네트워크를 제외하지 않는다. 추가로 스마트 제품/스마트 서비스 스택(예: Cloud Foundry, OpenStack)에 있어 오픈 소스 컴포넌트 개발 및 활용 모두를 위한 개방형 프로토콜(예: MQTT, OPC 및 웹 소켓)에 대한 지원이 확대되는 추세이다.

산업 도메인 간의 의미론적 상호 운용성은 다수의 표준 개발 기구(SDO), 단체 및 오픈 소스 소프트웨어(OSS) 이니셔티브에서 날이 갈수록 관심을 끌고 있는 새로운 IoT 특성이다. 이러한 상호 운용성 이니셔티브와 새로 등장하는 그 밖의 다른 이니셔티브는 산업 도메인 간에 데이터의 활용을 가능하게 하고 새로운 비즈니스 모델의 개발 수단을 제공한다.

2.4.4 보안, 개인정보보호, 신뢰

위에서 말했듯이 IoT는 다수의 서로 다른 장치, 센서 및 작동기로 구성되며 심지어 클라우드 인프라로만 구성될 수도 있다. 분명한 사실은 이런 범용 솔루션은 보안성 측면에서 적합하지 않다는 점이다. 보안에 대한 오늘날의 IoT 기능은 대략적으로 센서 보안, 장치 보안, 엣지 보안 및 클라우드 인프라와 네트워크 보안으로 구분될 수 있다. 지금까지 자원과 기능이 제한적인 센서는 암호화 알고리즘과 주요 관리 필요성의 간접비용으로 인해 보안 메커니즘이 제외되는 경우가 많았다. 적용 부문에 따라 여러 장치에서 이와 같은 사실을 확인할 수 있다(예: 노후된 장비가 주를 이루는 산업 설비, 가정 자동화 환경 등에 사용되는 일반 소비자 기기). 오늘날의 IoT에서 장치 보안은 주로(경우에 따라 배타적으로) 네트워크 및/또는 엣지 보안과 결부된다(표준 보안 프로토콜(예: TLS) 또는 표준 필터링 기술(예: 방화벽, 보안 게이트웨이, 엣지 노드)을 채택하여 암호화 통신 채널을 구축). 장치 보안은 주로 소비자 요구 및 기능에 따라 건별로 구현된다. 엣지 및 네트워크 게이트웨이에 보안 기능을 삽입하는 것이 게이트웨이 너머의 엔드포인트 및 장치를 일괄적으로 보호하는 가장 쉬운 방법이다. 이렇게 하면 접근 통제, 인증, 침입 탐지 등의 메커니즘을 지원하기 위해 각 장치를 교체하거나 손을 댈 필요가 없다. 그러나 대개 IoT 장치는 물리적으로

접근이 가능하다. 다시 말해서 IoT 장치에 대한 네트워크 보안은 첫 번째 보호 수준일 뿐이다. 장치 및 센서 자체에서의 두 번째 보호 수준과, 엣지 및 플랫폼 기능과 조합하여 장치에 대한 보안 모니터링 및 위협 분석을 제공하는 두 번째 보호 수준 역시 필요하다. 관련성 높은 여러 솔루션이 이미 존재하는 사용 사례들을 찾아볼 수 있는데, 예를 들어 감시 및 비디오 카메라는 데이터 및 장치 수준에서 무결점 보호를 구현하여 법정에서 사용 가능하다. 또한 보안이 필요한 대상은 적용 부문에 따라 달라진다는 점을 주목해야 한다. 일부 부문의 경우, 기업체는 제품에 대한 피드백 메커니즘 및 통제와 관련된 보안 문제를 생성되는 데이터의 보안 문제보다 훨씬 중요하게 평가하며 그에 따라 솔루션이 설계된다. 클라우드 보안과 관련하여 ID 및 액세스 관리, 격리 및 가상화, 침입 탐지와 같은 여러 보호 메커니즘이 이미 사용 중에 있다.

오늘날의 IoT에서는 생성되는 데이터의 사용 권한을 부여하는 서비스 수준 협약서(SLA)를 이용자와 체결함으로써 개인정보보호 고려사항을 주로 비기술적 수준에서 관리한다. 기술적 수준에서는 매우 단순한 메커니즘만 개인정보보호에 채택된다. 공통적인 기능으로는 민감한 정보를 숨기기 위한 암호화, 개인 식별정보 항목 대신 별칭 사용, 집단 내에서 개인 정보 데이터를 숨기기 위한 집단화(aggregation) 등이 있다. 클라우드 인프라 내의 개인정보보호에서는 데이터를 암호화하여 저장 및 통신하거나 무단 정보 유출을 방지하기 위한 액세스 통제 방식을 채택하는 등의 충분히 확립된 수단을 사용한다. 데이터 분석의 경우 개인정보보호 강화 기술이 부족한 경우가 많으므로 법적 규정을 준수하는 데이터 처리를 위해 SLA 및 기타 이용자 약정 등의 비기술적 수단으로 대체되고 있다. 요약하면, 오늘날의 IoT에서 개인정보보호 기능은 데이터 출처에서 개인정보를 보호하는 '개인정보보호 중심 설계' 접근법에 중점을 둔다.

개인정보보호를 유지하는 동시에 IoT의 거대한 잠재력을 제대로 활용하려면 애플리케이션 의존 방식으로 데이터 활용 및 데이터 처리를 제어하기 위해 보다 융통성 있는 기능이 요구된다[14].

IoT의 엔티티 사이에 신뢰를 구축하려면 고유한 장치, 서비스 및/또는 트랜잭션 ID와 함께 강력한 인증이 요구된다. 오늘날 IoT의 신뢰 구축은 공통적으로 사용자, 서버 및 네트워크 장비(예: 게이트웨이)의 인증서 내에 등록되는 ID를 기반으로 한다. 인증서는 잘 알려진 공개 키 인프라(PKI)를 사용하여 생성 및 제어된다. 장치 식별은 ID 프록시 역할을 수행하는 게이트웨이에 위임되는 경우가 많다. 보안이 핵심적인 일부 환경에서는 트러스트 플랫폼 모듈(TPM)과 같은 하드웨어 기반 트러스트 앵커가 사용되며 이 앵커는 제공된 ID 속성이 특정 장치에 속한다는 하드웨어 기반 트러스트 근거와 높은 수준의 신뢰성을 제공한다. 일부 장치와 게이트웨이는 이미 신뢰실행환경(TEE)을 활용하여 애플리케이션을 격리하거나 서로 다른 컨테이너 구현(예: 리눅스 시스템)을 사용하여 애플리케이션에 대한 격리된 실행 환경을 제공한다.

IoT는 동적 시스템 복합 체계(system of systems)이기 때문에 수명기간 전체에 걸쳐 IoT 컴포넌트의 신뢰 가치를 입증하는 수단이 요구된다. 그러나 일반적으로 이런 종류의 무결성 입증은 오늘날의 IoT에 아직 존재하지 않는다.

제3절

오늘날 IoT의 한계 및 결함

오늘날의 IoT 플랫폼은 소비자와 산업 양단 둘 다를 아우르는 IoT 가상 물리 시스템의 배치 및 개발이 직면한 현재 식별된 이슈들을 다루기 위해 특별히 고안된 플랫폼이 지니는 기존의 해결책이 아닌 다른 목적에 맞게 만들어진 여러 구성요소들이 혼합 절충된 형태를 띈다. 현재의 많은 IoT 솔루션에서는 이질적인 스토브 파이프 애플리케이션 및 시스템이 협업을 하도록 하는 노력이 필요하다. 이런 시스템은 IoT용으로 설계되지 않은 기존 프로토콜, 표준 및 개념을 사용한다. 그들 중 다수는 IoT의 실제 잠재 역량에 대한 인사이트가 없이 구축되었다. 대신 그런 시스템은 단지 물리 장치의 OT를 기존 IT, 백엔드 플랫폼 및 애플리케이션과 한데 묶으려는 시도를 한 것뿐이다. 모든 시스템은 장치 등록, 대용량 장치 온보딩 및 대용량 잠재 데이터 문제를 다룬다.

이런 다수의 다양한 IoT 구축 접근법을 조사하면 보안성, 안전성, 통합성, 상호 운용성, 결합성, 데이터 관리, 분석, 복원성, 결합성, 가상화 및 규정과 같은 부문에 있어 경계를 허무는 기초적인 논의가 절실함을 알 수 있다. 이런 논제는 모두 비용 상승 요인이며 이는 오늘날의 IoT가 기초 기술 단계에서 제기능을 하는 데에도 큰 장애물로 작용한다.

이어지는 절에서는 현재 IoT 계획이 직면한 논제 각각이 지니는 핵심적인 문제들을 살펴본다.

3.1 보안, 신뢰, 개인정보보호 및 ID 관리

시스템의 보안 속성은 보안 모델에 의해 기술된다. 이런 모델은 일반적으로 특정 보안 정책 및 그 정책을 구성하는 규정이 적용 및 관리되는 엔티티를 기술한다. IoT 시스템의 동적 변경에 대응할 수 있는 전체 보안 모델을 개발 및 유지하는 것은 갈수록 어려워지고 있다. 서로 다른 OEM, 서로 다른 센서, 서로 다른 물리적 시설 보안 접근법에 관련된 장치의 지속적인 추가로 인해 보안 복잡성이 기하급수적으로 증가하고 있다. 소비자/파트너/시스템 제공자의 책임과 같은 문제와 관련된 솔루션은 보안 커뮤니티에서 여전히 공감을 얻고 있다. 현재 차세대 IoT를 위해 오늘날의 IoT가 갖춰야할 급속한 진전과 혁신성을 가능케 하는 동시에 중요 업무 시스템을 지원할 수 있는 전반적으로 유연하면서도 다이나믹한 IoT 보안 모델이 존재하지 않는다. 오늘날의 IoT 시스템은 항상 기존 센서, 장치 및 인프라 컴포넌트와 더불어 서비스를 연결하는 재개발식 접근법으로 구축되고 있다. IoT는 이런 요소 각각에 대해 새로운 수준의 노출을 유발하고 있다. 현재 IoT 플랫폼에는 각각 개별적인 수준의 보안성을 갖춘 이종 컴포넌트를 제공하는 광범위한 다양한 벤더의 기술 솔루션이 포함되어 있다. IoT 컴포넌트 내에 보안 대책이 있다고 해도 IoT의 연결성 기능 또는 데이터 상관관계 및 정보 검색 기능으로 인한 의존성을 고려하여 설계된 것은 아니다.

예를 들어 산업 장치는 물리적으로 보호받는 격리된 환경에서 사용할 목적으로 설계되었기 때문에 적정 인증 메커니즘이 결여된 경우가 많다. 오늘날 IoT의 일부로서 이들은 다수의 다른 장치, 특히 오늘날의 비즈니스 IT에서 고유한 잘 알려진 보안 결함의 영향을 받는 백엔드 시스템과 상호 연결된다. 예를 들어 브라우저 취약성을 악용하여 비즈니스 IT 플랫폼에 대한 접근권을 얻은 공격자는 보호가 취약한 IoT 산업 장치에 대한 접근권도 확보할 가능성이 있다. 그럴 경우 안전 사고를 포함하여 심각한 손상으로 이어질 수 있다. 소비자나 산업 환경으로부터 대량의 엔드포인트 유입은 취약한 링크 악용의 온상이 될 수 있다. 지금까지 완전히 폐쇄적인 동종 시스템 세트로 구성되었던 환경에서 이러한 엔드포인트의 강화, 장치 간의 통신 보안, 장치 및 정보의 신뢰성 확보가 새로운 과제로 대두되고 있다. 종합적인 위험 및 위협 분석 방법과 함께 IoT 플랫폼에 대한 관리 도구가 요구된다.

3.1.1 신뢰

오늘날의 IoT에 있어 보안 수단은 네트워크 및 엣지 보안에 중점을 둔다. 하드웨어 기반 트러스트 앵커 또는 모니터링과 엣지 뒤에서 운영되는 IoT 장치에 적절히 통합된 위협 분석 서비스와 같은 심층 보호를 제공하는 적정 보안 개념이 결여되어 있다. 복잡한 IoT 환경 내에서 적절한 식별 및 인증 기능과 이들의 조화 또한 없다. 이로 인해 보안이 중요한 IoT 애플리케이션 및 스마트 시티 시나리오와 같이 IoT 컴포넌트 간 즉시 연결성을 요구하는 미래 애플리케이션에 대한 선결요건인 신뢰 구축이 어렵다. 데이터 유효성은 또 다른 문제이다. 데이터 분석 엔진에 유효한 데이터가 공급되도록 보장하기 위해 IoT의 신뢰 관리가 필요하다.

3.1.2 개인정보보호

오늘날의 IoT에 있어 개인정보보호 유지는 여전히 해결되지 않은 과제이다. Gartner와 같은 선구자들은 특히 언론 및 대중 토론에 오르내리는 불미스러운 일들을 고려할 때 디지털 윤리의 개발 및 유지에 대한 필요성이 절실하다고 내다보고 있다[15]. IoT를 통한 개인 정보 데이터 분석의 잠재성이 무궁무진하기에 융통성이 부족한 설계 원칙으로 만들어진 개인정보보호를 뛰어넘는 보호 기술이 요구된다. 예를 들어 사용 제어, 준동형 암호화 또는 검색 가능 암호화는 기존 결점을 극복하는 잠재적인 대안이다. 이런 기술적 과제 이외에도 법적 규제 요구사항도 풀기 어려운 과제이다. 벤더들은 지역별로 상당한 차이를 보이는 개인정보보호 규정에 대응해야 한다.

3.1.3 ID 관리

현재 엔터프라이즈의 ID 및 액세스 관리(IAM) 솔루션은 애플리케이션, 자원 및 데이터에 대한 사용자 액세스 승인 시 최소 액세스 정책에 중점을 둔다. 그러나 IoT 측면에서 현재 IAM 시스템은 ID 및 엔티티를 대규모로 저장하도록 조정하는 기능이 제한적이다. 이 제한으로 인해 IoT 기반 애플리케이션에 대한 애플리케이션 통합 계층이 결여되는 결과가 나타났다. 현 단계에서 서로 다른 솔루션에 걸쳐 IoT 엔티티 및 그 ID를 탐지하고 관리하는 방법에 대한 전체적인 프레임워크가 존재하지 않는다. 더욱 향상되고 폭이 넓어진 엔티티 관계를 모두 취급하려면 현재 IAM 시스템의 개선이 필요할 것이다. 향상된 IAM의 역할은 인증(및 권한 부여) 수단과 액세스 승인 방식을 변경하는 것이다. 현 추세는 최소 권한 액세스가 아니라 예상 역할을 토대로 제한적인 액세스를 제공하는 것이다. 그와 같이, 사용자가 장치에 대해 인증한 방식에 따라 동일 장치의 인증이 서로 다른 액세스 기능으로 귀결될 수 있다. 또한 IoT의 경우 일반적인 IAM 시스템에서 사물지능통신(M2M; machine-to-machine) 엔티티를 포함해야 한다.

이런 통신 중 일부는 가상 클라우드 엔티티와 같이 수명이 짧은 엔티티를 기반으로 하기 때문에 이런 작업은 복잡할 것이다. 이런 엔티티의 일부는 독점적 통신 및 ID 체계를 사용한다. IoT 기반 시스템에서 ID를 취급하려면 일반적으로 IAM 플랫폼을 수정할 필요가 있을 것이다.

3.2 안전성

시스템 안전성과 신뢰성은 다수의 OT 플랫폼에 있어 최우선 순위이다. 다시 말해서 이는 시스템 및 해당 구성요소가 용인할 수 없는 상해 위험 또는 물리적 손상의 위험을 초래하지 않도록 하고, 위해로부터 환경을 보호하고 필수 안전 프로세스의 중단을 방지하는 것을 의미한다. 예전에는 대부분의 OT 시스템이 네트워크에 연결되지 않았기 때문에 보안 및 개인정보보호가 우려되지 않았다. IoT는 기본적으로 이런 관점을 바꿔놓고 있다. 오늘날의 IoT에 결여되있는 부분은 의도적인 공격에 의해 발생된 결함으로 인한 종속성을 고려한 전체론적인 위험 및 위협 분석이다. IoT를 통해 OT와 IT가 연결됨으로써, 원격 공격자가 산업/소비자/공공 부문 IoT 시스템의 취약성을 악용하여 OT 시스템에 침입해서 시스템의 안전성과 신뢰성을 무너뜨릴 수 있다.

또한 장치의 재구성 및 업데이트와 실시간 모니터링 및 운영 재프로그래밍을 포함하는 원격 관리의 채택으로 인해 심각한 차세대 보안 및 안전 우려가 발생하고 있다. 포트가 개방되어 있고 악성 코드의 침입 가능성이 있는 IoT 시스템이 운송, 도시 공공 안전, 수도 등 안전이 필수적인 장치 및 시스템에 도입됨에 따라 현재 적절하게 취급되고 있지 않은 새로운 보안 및 안전 요구사항이 나타나고 있다.

3.3 통합성, 상호 운용성 및 결합성

오늘날의 IoT 시스템에서는 다양한 컴포넌트를 하나의 집합체로 통합하는 방식을 다룬다. 이 통합성을 통해, 호환 가능한 신호 수단 및 프로토콜을 토대로 각 시스템 컴포넌트가 다른 시스템 컴포넌트와 통신할 수 있다. 그림 3-1과 같이 통합성은 통합 스택의 최하위층을 구성한다. 상호 운용성은 통합성 위에 구축되며 컴포넌트가 공통적인 개념 모델 및 상황에 따른 정보 해석을 토대로 상호 정보를 교환하는 기능이다. 가장 높은 층에는 결합성이 존재하며, 이는 상호작용 당사자들의 행동 예상에 따른 요구사항을 충족하기 위해 재조합 방식으로 컴포넌트가 다른 컴포넌트와 상호작용하는 기능이다.

3.3.1 통합성

통합성 기능은 IoT 시스템의 인에이블러(enabler)이다. IoT가 지닌 복잡한 특징들으로 인해 이전과 다른 복잡한 연결성 문제가 발생하면서 새로운 해법이 요구된다. IoT 시스템에 기능과 성능에 대한 새로운 요구에 부합하여 지속적으로 늘어나고 있는 엔드포인트, 지리적 분산 정보 출처 및 새로운 시스템 간 요구사항이 추가되고 있다. IoT 시스템은 세션유지 및 연결끊김에 대한 연결 문제 해결도 필요하다. 특히 말그대로 이벤트 즉각적 대응 시간을 요구하는 필수 안전 컴포넌트의 경우 네트워크 속도 요구가 지속적으로 가중되는 가운데 네트워크 부하 증가가 발생하고 있다. 다중 네트워크 자원을 통한 데이터 취득과, (예를 들어 방화벽으로 중무장된 내부 네트워크를 통한) 엣지 방향의 로직 푸시백으로 인해 상당한 문제가 발생하고 있다. 백엔드에서 엣지까지의 규칙 페더레이션(rule federation)은 새로 개선된 프로토콜을 요구한다.

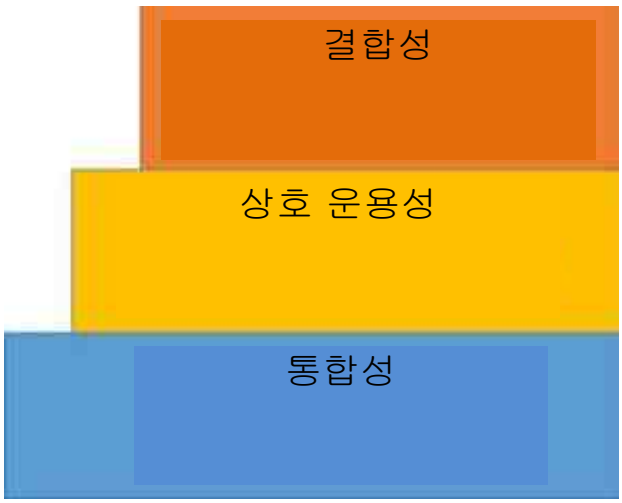


그림 3-1 | 통합 스택

3.3.2 상호 운용성

IoT 시스템은 4가지 컴포넌트(즉, 구문 변환, 도메인 변환, 의미 변환 및 맥락화)에 의존하여 컴포넌트 간의 진정한 상호 운용성을 목표로 한다[13].

연결성 프레임워크 계층(ISO/IEC 7498 OSI 모델의 계층 5부터 7까지)은 시스템 사이의 다양한 컴포넌트 간 데이터 구조 및 변환 규칙에 대한 지식을 이용하여 구문적 상호 운용성 메커니즘을 제공한다. 존재 검색을 채택하는 IoT 시스템은 부분적으로 이 요구사항을 다룬다. 또한 IoT 시스템은 도메인 변환을 사용하여 한 데이터 도메인에서 다른 데이터 도메인으로 변환(예: OT 시스템의 정보를 IT 시스템 정보로 변환)한다. IoT 시스템 구문 변환을 위해서는 송수신하는 컴포넌트/시스템 간의 구문 이해가 필요하다. 지금 현재 실현 가능한 맥락화 메커니즘은 존재하지 않는다. 비록 일부 구문 및 도메인 변환 수준에서 일부 진전이 있기는 했지만 오늘날의 IoT 시스템은 지속적으로 4가지 상호 운용성 컴포넌트를 상대로 악전고투하고 있다. 이런 문제의 취급을 위한 필수 표준을 개발하기 위해서는 상당한 노력이 필요하다.

또한 IoT 시스템은 API 의존성 관리 결여도 취급해야 한다. API 하나만 변경해도 전체 시스템이 혼란에 빠질 수 있다. 마이크로서비스와 서비스 조율은 여전히 어렵다. 서로 다른 IoT 독립부문들이 상호 운용이 불가능한 서로 다른 클라우드 백엔드 또는 온프레미스 솔루션을 사용하기 때문에 백엔드 프로세스와의 상호 운용성(즉, 엔드 투 엔드 프로세스 통합)은 여전히 해결되지 않은 문제이다.

3.3.2.1 의미론적 상호 운용성

오늘날의 날로 복잡해지는 이종 IoT 시스템에는 현실세계 엔티티 추상화와 시계열 기반 및 위치 기반의 수 많은 모델들이 포함되어 있다. 비즈니스 사용자, 데이터 모델러, 시스템 설계자 등이 단순 스프레드시트 분석에서 보다 복잡한 UML 설계에 이르기까지 다양한 기법을 통해 오랫동안 이런 데이터 모델을 구축해 왔다.

그러나 오늘날의 IoT 시스템은 데이터를 모호하지 않은 공유된 의미로 교환하는 데에 애를 먹고 있다. 데이터 모델에서 시간이 많이 걸리는 수동 매핑을 하지 않는 한 구문적 상호 운용성이 거의 없으며 이는 오늘날의 IoT에 적합하지 않은 취약한 구현을 생성한다. 기계적 계산이 가능한 로직, 추론, 지식 검색, 데이터 페더레이션 등은 복잡한 수준의 구문적 상호 운용성을 요구한다. 온톨로지는 일반적으로 단일 시스템 또는 사용 사례로 제한되며 일관된 명명 규칙 및 정의 규칙을 갖고 있지 않다. ISO/IEC 11179 및 ISO 15000-5와 같은 국제 표준을 따를 경우 일관되게 명명, 정의 및 구문적으로 이해되는 메타데이터를 사용할 수 있지만, 이 경우 광범위한 IoT에서 그와 같은 데이터의 규모를 조절하고 데이터를 사용 가능하게 조정하는 추가적인 노력이 요구된다.

3.3.2.2 맥락화

맥락화는 엔드포인트, 센서, 인간, 환경 등 캡처 당시의 환경 전체를 이해해서 해당 정보를 완전히 이해 가능한 메타데이터 형태로 기록하는 것이다. 오늘날의 IoT 시스템은 특히 엣지 정보의 맥락화가 제대로 되어 있지 않아 곤란을 겪는다. 이러한 IoT 정보의 맥락화는 진정한 의미의 상호 운용성을 달성하기 위해 거쳐야 하는 단계이며 양질의 분석과 안전한 실행을 보장하는 데 있어 핵심적이다. 컨텍스트 데이터를 모호하지 않게 식별 및 공유하기 위한 합의된 표준 또는 방법론은 현재 없는 실정이다. 또한 컨텍스트 데이터에는 기밀 데이터가 포함될 수 있다. 엣지 컴퓨팅은 컨텍스트 데이터를 엣지에 격리하여 유지하는 데 유용하다. 그러나 엣지 컴퓨팅을 위협으로부터 보호할 필요가 있다.

3.3.3 결합성

결합성은 상호작용 당사자들의 행동 예상에 따른 요구사항을 충족하기 위해 재조합 방식으로 컴포넌트가 다른 컴포넌트와 상호작용하는 기능이다[16]. IoT에서 이는 IoT 시스템의 자체 구성 능력과, 환경 변화에 따라 조정 및 재구성할 수 있는 역량으로 해석된다. IoT 시스템은 현재 동적 환경에서의 응답성 문제를 취급하고 있다. IoT 시스템은 일반적인 점대점(point-to-point) 클라이언트-서버 모델을 넘어 그물형 다대다(many-to-many) 모델로 전환 중이며, 이를 위해 다양한 수준의 동시 응답 관련 자율성을 보장하고 융통성 있는 구성에 대한 필요를 해결하기 위한 새로운 접근법이 필요하다. 자율 시스템은 동적 상태를 처리하고 안전성과 복원성을 보장하는 데 있어서 어려움이 가중되고 있다. 오늘날의 IoT 시스템에는 운영 환경, 상호작용 엔티티, 사용자 정신 상태, 예기치 않은 문제 등의 관련사항을 포함시켜 컨텍스트에 대해 예상되는 모순된 추정을 해결하는 메커니즘이 부족하다. 또한 IoT 시스템은 자체적으로 형성되는 구성에서 실시간 활동 및 상태 변화를 처리하는 동적 관계의 지원 기능이 부족하다.

3.4 복원성

오늘날의 IoT 시스템은 기능을 여전히 유지하면서 시스템 혹은 컴포넌트 장애를 처리하면서 기능성을 유지하는 역량에 관한 고질적 과제에 봉착해있다. 군사 및 민간 핵심 시스템(예: 군 전투기, 민간 운송, 전투 작전 지원, 비상 대응) 설계자들은 그와 같은 동시 발생성을 충분히 이해하고 계획을 수립한다. 이런 계획 수립의 목적은 시스템 복원성을 제공하는 것이다. 복원성은 “할당된 임무를 완수하는 중에 부정적인 상황을 방지, 흡수 및 관리하고 사고 발생 후 운영 기능을 복원할 수 있는 시스템 상태”이다[13]. 안전이 필수적인 이런 컴포넌트 및 시스템은 복원성이 필수 기능이다. 그러나 복원성은 이런 사용 사례에 국한되지 않으며, 여타 다수의 IoT 애플리케이션에서도 마찬가지로 필요로 하는 기능이다.

IoT 시스템 및 시스템들의 복잡한 관계로 인해, 정적 솔루션의 개발 없이 복원성에 영향을 주지 않으면서 상호 운용성 및 결합성을 구현하기 위한 하위 시스템 네트워크가 필요하다. 스마트 플랫폼은 해당 시스템이 지원하는 컴포넌트의 복원성 관리를 위한 보다 진전된 접근법을 개발해야 한다.

3.5 데이터 수집, 관리 및 소유권

오늘날의 IoT는 데이터의 분량, 유형, 위치 그리고 그 민감도에 있어 전대미문의 수준이다. IoT 시스템과 이 시스템을 지원하는 플랫폼은 엣지 환경에서 이들을 연결하는 다수의 엔드포인트와 센서의 폭발적인 성장을 경험하고 있다. 다중 아키텍처 패턴은 데이터가 제공 혹은 분석되는 장소, 시기, 이유 및 방법의 프로세스를 더욱 복잡하게 한다. 장치 및 엔티티 지향 데이터는 보다 높은 추상화 계층을 요구하고 있다. IoT 시스템 자산 이질성은 다중 출처에 대한 데이터 액세스를 얻는 데에 문제를 일으키고 있다.

이런 대용량 데이터 생성으로 데이터 수집, 저장, 검색 및 쿼리에 관련된 심각한 문제가 대두되고 있다. IoT 시스템은 정확히 어떤 데이터를 얼마나 많이 수집하고 저장할지를 늘 고심한다. 일부 시스템은 오늘날의 플랫폼 애플리케이션이 사용하지 않는 다량의 원시 데이터를 엣지에서 저장하려고 시도한다. 소비자들은 더욱 더 많은 데이터 캡처(기본적으로 모든 출처로부터의 모든 데이터를 항상 캡처하는 것)를 원하지만 엣지에서의 데이터 집계는 꺼리는 것으로 나타났다. 그 결과 일부 IoT 시스템은 연결 파이프를 데이터만으로 가득 채우려고 한다.

데이터 소유권, 특히 IoT 데이터 소유권의 일반적인 논제에 대한 논란이 분분하다. 누가 어떤 데이터를 소유할 것이며 데이터가 어디로 가는지를 누가 통제할 것인가에 대한 화두는 규제, 윤리 및 재무적 관점에서 주된 쟁점이 된다 소비자들은 자신들이 모든 데이터를 소유한다고 믿는다. OEM(original equipment manufacturer)은 엔드포인트에서 취급하는 데이터를 소유하거나 적어도 데이터 액세스 권한을 소유한다고 생각한다. PaaS(Platforms-as-a-Service) 제공자들도 대개 애플리케이션 제공자들처럼 데이터를 소유한다고 생각한다. 여러 이종 집단에서 더 많은 플레이어를 지닌 이종 IoT 시스템이 더 많이 배포되면서 데이터 소유권 문제는 날이 갈수록 복잡해진다. 이 문제를 더욱 복잡하게 만드는 것은 개인적 및 사업적 데이터 수집기와 분석 서비스에 데이터를 제공함으로써 최종 사용자 사용권 계약을 직접적으로 또는 우회하여 위반하는 IoT 시스템 제공자이다. 기업체들은 영업 데이터 및 거래 기밀의 보호뿐 아니라 (예를 들어 저장, 처리 또는 소비하는 제3자 입력 데이터의 개인정보보호 위반과 관련한) 책임의 제한에 지대한 관심을 갖고 있다. 특히 최종 사용자는 시스템에서 특정 용도로 자신의 데이터를 사용할 수 있도록 동의하는 경우에도 사생활 데이터 등의 개인 데이터가 적절하게 보호되기를 원한다. 오늘날의 IoT 플랫폼은 모든 당사자가 자신의 데이터에 대해 적정 수준의 통제권을 행사하고 언제 어디서 누가 어떻게 어떤 용도로 그런 데이터를 사용하는지를 조회할 수 있는 강력한 데이터 권한 관리 시스템이 부족하다.

3.6 고급 분석 및 고급 데이터 처리

오늘날의 IoT에서 센서와 시스템은 극히 다량의 데이터를 생성한다. 따라서 일반 처리 기법만으로는 부족하다. IoT 데이터 처리 및 분석은 이런 대용량의 시스템 및 센서 데이터를 변환하고 기술적, 예측적 및 규범적으로 분석하여 처리한다. 이런 데이터의 전송은 방대한 대역폭을 필요로 하며 다량의 원시 데이터는 불필요하거나 쓸모가 없다. 그에 따라 (특히 안전 관련 시스템의 경우) 엣지와 물리 장치 자체에서의 분석에 더 관심을 두지만 이로 인해 데이터 관리, 고급 분석 및 운영 제어 등의 영역에서 추가적인 복잡성이 양산된다.

물리 장치 또는 엣지에서 실행되는 분석이 지니는 중요한 한 가지 문제는 다중 엣지 및 시스템 간에 데이터를 크라우드소싱할 때에만 드러나는 다수의 인사이트 결과를 유실한다는 점이다. 오늘날의 환경에는 엣지 분석 및 클라우드 분석을 조율하는 기술이 없다. 그와 같은 조율은 미래형 스마트 및 보안 IoT 플랫폼 구축 시 필수적이다.

추가적인 문제는 센서 간 시간 동기화의 결여이다. 시스템에서는 메시지가 순서 없이 전달되므로 보편적으로 적용되는 시간 동기화 기법이 필요하다. 고급 분석 시스템에 사용 가능한 데이터가 유용하지 않을 경우가 많다(예를 들어 데이터 손실, 데이터 손상, 잘못된 데이터). 이런 데이터는 오늘날의 IoT에서 이미 배포되고 있는 예측 분석 및 기타 분석 형태에 대한 새로운 접근법을 염두하지 않고 설계되었기 때문이다. IoT 시스템은 순수 데이터를 수신 및 처리하는 데 있어 매우 고전하고 있다. 엔드포인트 종료와 같은 의도치 않은 인간 개입은 데이터의 전체성을 감소시켜 데이터의 컨텍스트에 영향을 준다. 비록 기계 생성 데이터는 일반적으로 품질이 높지만 오늘날의 IoT 내에서 엣지 데이터는 구문 및 컨텍스트의 잘못된 이해와 데이터 손상을 지속적으로 겪기 때문에 엣지 컴퓨팅으로 생성된 데이터는 적정 품질에 미치지 못한다. 또한 IoT 시스템은 애초에 이 시스템용으로 설계되지 않은 데이터를 사용하려고 시도하고 있다. 이로 인해 구문 및 의미론적 문제가 생기며 IoT 시스템 간에 유용한 데이터 교집합이 매우 적다. 또한 IoT 분석 시스템은 소셜 및 크라우드 소싱 데이터 사용과 같은 차세대 개념을 이제 막 처리하기 시작했다.

3.7 가상화

오늘날의 IoT 플랫폼은 대부분 가상화 기능이 결여된 레거시 장치 및 레거시 IT 시스템에 의존한다. 이런 장치에는 일반적으로 독자적인 "스마트" 기능들이 이미 갖춰져 있다. 최종 사용 지침은 소프트웨어 다운로드를 통해서만 제공된다. 오늘날의 IoT 장치에는 대개 가상화 기능(일반 관리 계층을 장치에 제공하는 추상화 수준의 추가 가능) 및 가상 머신(기능을 동적으로 추가 가능)이 내장되어 있지 않다.

3.8 확장성

IoT의 분산 특성은 데이터 센터 외부 데이터를 생성 및 처리할 뿐 아니라 핵심 데이터 센터 또는 클라우드에서 대량 후처리 분석 시스템 구축할 수 있도록 한다. 현재 대부분의 데이터 센터는 이런 새로운 요구사항에 부적합한 일반적인 아키텍처에 의존한다. 그러므로 2020년까지 모든 IoT 프로젝트의 80%는 부적합한 데이터 수집 방법으로 인해 구현 단계에서 실패할 것이다[4]. 예상되는 엄청난 성장에 속도를 맞추는 것은 물론 그러한 요구사항을 충족시키기 위해(예: Gartner 예측에 따르면 데이터 집중 산업은 2020년까지 스토리지 내에서 500%까지 증가할 것으로 보인다.) IoT 요구사항을 효율적으로 지원할 수 있는 역량을 갖춘 웹 스케일 IT가 요구된다. Gartner의 정의에 따르면 웹 스케일 IT는 신속하고 가벼우며 지속가능한 원칙을 활용하는 웹 기반 IT 서비스의 빠르며 확장 가능한 개발 및 제공을 가능하게 하는 시스템 지향적 아키텍처 패턴이다. 오늘날의 IoT에는 웹 스케일 IT 기능이 결여되어 있다.

3.9 규정

IoT는 사회를 보다 효율적이고 안전하고 보다 친환경적으로 만드는 데 도움을 줄 수 있으므로 정부 기관들은 유용한 혁신 지원과 소비자 보호 사이의 적절한 균형을 갖춘 규제를 마련하려고 노력한다. 비록 그 목표는 같지만, 서로 다른 지정학적 주체들 간의 접근법은 크게 다르다. 이로 인해 시장에서 상당한 혼란이 야기되며, 지정학적 경계 내외부에서 동종 및 이종 시스템의 설계, 구축, 배포 및 운영의 복잡성이 가중된다.

제4절

차세대 스마트 및 보안 IoT 플랫폼의 사용 사례

그림 4-1 | 스마트 및 보안 IoT 플랫폼 핵심 기능

제2절과 3절의 자료로 미뤄볼 때 현재 최신 IoT는 기능이 제한적이고 결점이 많아 곤욕을 치루고 있음이 분명하다. 이들이 혼재되어 가용 IoT 솔루션을 제한하고 스마트 및 보안 IoT 플랫폼의 개발을 가로막고 있다. 뿐만 아니라 이런 결점의 극복은 IoT의 잠재력을 십분 활용하기에는 턱없이 부족하다. 차라리 필요한 기능을 제대로 정의하기 위해 미래에 대비한 사용 사례를 새로 조사하는 편이 더 바람직한 실정이다. 이 절에서는 산업계, 공공 부문 및 소비자 측면에서 그런 사용 사례 3건의 개요를 제공하고 미래 IoT 시스템과 스마트 및 보안 IoT 플랫폼이 갖춰야 할 그림 4-1과 같은 핵심 기능을 선정하여 제시한다. 스마트 및 보안 IoT 플랫폼은 분명 기능 및 요구사항 추가를 필요로 하지만 본 백서의 나머지 부분은 여기에서 정의하는 것들로 제한한다. 표 4-1에 나열된 이 3가지 사용 사례와 더불어 기타 미래 대비 사용 사례에 대한 추가 세부사항은 부록에서 확인할 수 있다.

표 4-1 | 미래 대비 사용 사례

사용 사례 도메인	사용 사례의 명칭	기술어
산업	비즈니스 연속성 관리	BCM
	고급 유지보수 서비스용 이상 탐지 시스템	Anom Detect
	협업 공급망관리(SCM)	CSCM
	예측 유지보수 및 서비스	Pred Maint
공공	스마트 및 보안 IoT 플랫폼을 이용한 스마트 시티	Smrt Cty
	소셜 센서	Soc Sens
소비자	특수 요구가 있는 사람을 포함하여 승객을 위한 대중교통의 탑승 경험의 개선	Journ Exp
	커넥티드 카	Conn Car
	WISE 스키잉	Ski
	가정용 장치 스마트 팩토리	Smrt Fact

4.1 산업 도메인: 생산 라인의 비즈니스 연속성 관리

비즈니스 연속성 관리(BCM)는 해당 조직의 IT 및 OT 시스템에서 수집된 데이터를 활용하여 조직의 비즈니스 프로세스 연속성을 보장한다. 그림 4-2와 같이 BCM의 목적은 수집된 IT 및 OT 데이터를 토대로 처리된 고급 위험 평가를 제공하고 조직의 비즈니스 프로세스에 대한 영향을 완화하는 데 필요한 조치를 구현하는 것이다.

BCM IoT 플랫폼은 센서 융합 기술을 활용하여 다양한 보안 시스템(IT 시스템)에서 사건 정보를 수집할 뿐만 아니라 생산 제어 시스템(OT 시스템)에서 계획 및 실제 생산 데이터를 수집한다. BCM IoT 플랫폼은 다른 조직들로부터 위협 탐지 정보를 가져와 다른 상호 의존적 시스템의 상황에 대한 인사이트 및 현재와 미래 공격에 대한 응집 지식을 얻는다. 이 플랫폼은 사건 정보를 분석하고 사건에 대한 위험 분석을 수행한다. 또한 생산 활동에 대한 영향을 최소화하는 위험도 완화 계획과 같은 보안 대책을 마련한다. BCM IoT 플랫폼은 영향을 받는 하위 시스템의 격리 또는 제품 라인의 중단과 같은 보안 대책을 구현한다. IoT 플랫폼은 생산 데이터를 분석하여 각 생산 현장의 관련 기능에 맞는 최적의 생산 계획을 작성한다.

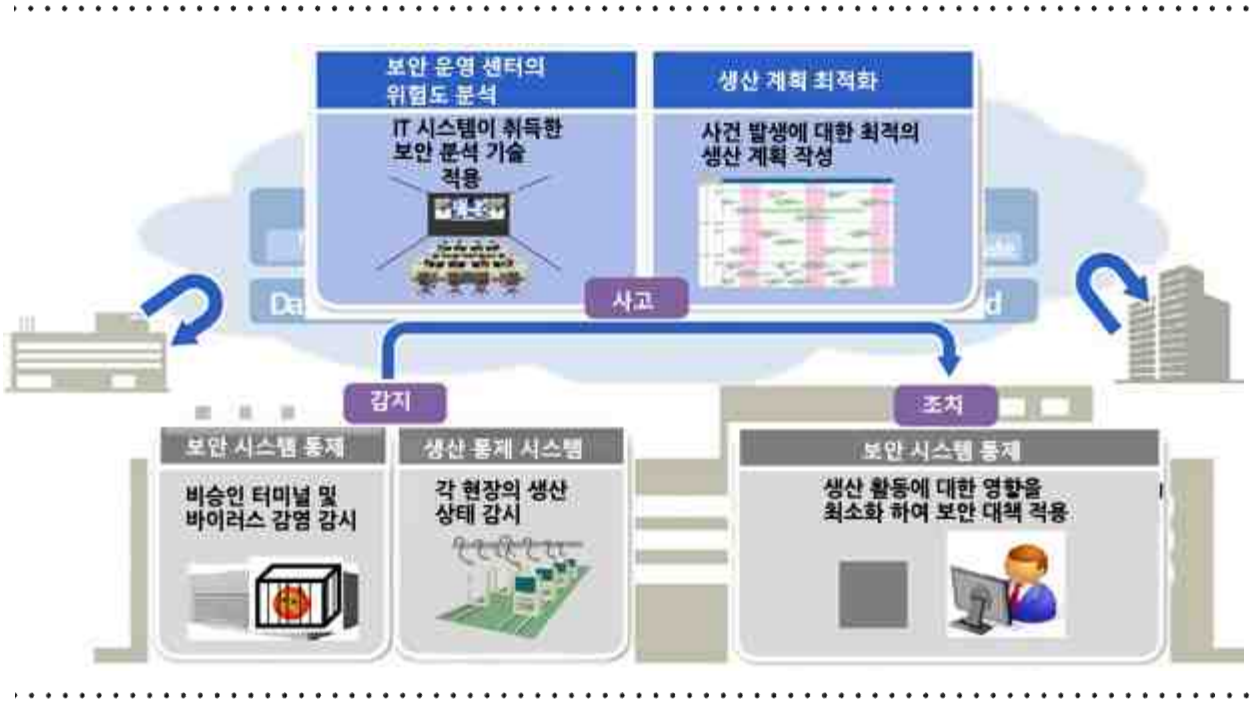


그림 4-2 | 산업 도메인 사용 사례

기존 기술은 본 사용 사례를 실현하기에 역부족이며
다음과 같은 개선이 필요하다.

연결성	▪ 결점 – 네트워크 지연시간 문제, 멀티 플랫폼 액세스 및 인증 ▪ 필요한 향상 – 멀티 플랫폼 액세스 및 인증 구현에 요구되는 지연시간 및 프로토콜을 지원하는 강력한 네트워크킹
처리	*데이터 수집 및 관리* ▪ 결점 – 장치 및 센서 수와 그에 따른 데이터 흐름에서 예상되는 폭발적 증가를 지원하는 기능 부족. 맥락화된 상태 정보 부족. 센서 데이터 정리 ▪ 필요한 향상 – 고급 데이터 저장 기법, 고급 데이터 공학 기능, 인메모리 데이터베이스, 표준화 상태 정보에 대한 메타데이터 맥락화 표준 *분석* ▪ 결점 – 산업 수준의 분석을 지원하는 메모리 및 알고리즘 측면에서 기능 부족. 분산 분석 루틴 부족 ▪ 필요한 향상 – 인메모리 데이터베이스, 자가 학습 및 최적화를 통한 향상 알고리즘, 인공지능, 구문적 상호 운용성, 데이터 맥락화, 분산 플랫폼 솔루션
메모리	–

감지	▪ 결점 – 센서 증가 용량, 데이터 교환 중재 솔루션, 센서 인증, 무결성 증거. IT/OT 협업, 작동, 센서 인터페이스, 센서 재조합 기능 ▪ 필요한 향상 – 보안 및 관련 요구사항에 일치하는 분산 플랫폼 및 필요 데이터를 지원하기 위한 고급 센서 기능. 향상된 센서 재구성 기능, 군용 수준 복원성 및 동적 결합성을 갖춘 고급 감지 기능
조치	*제어 인터페이스 장치* ▪ 결점 – IT/OT 통합에 대한 프로토콜이 제한적 ▪ 필요한 향상 – IoT 개념 및 기회를 100% 활용하도록 표준 개선 *작동* ▪ 결점 – 범위 및 조건에 대한 평가 역량. 멀티 플랫폼 연결성에 대한 우선순위 지정 루틴 ▪ 필요한 향상 – 분해, 평가, 조건 작동을 지원하는 온보드 처리 기능을 갖춘 고급 작동기 장치
보안	*보안 모델* ▪ 결점 – IoT 시스템의 동적 변경과, 시스템 공격 수준에서 예상되는 급속 진행에 대응할 수 있도록 전체적인 보안 운영을 조성 및 유지하기 위한 보안 모델 ▪ 상호 의존적인 IoT 시스템에 최적화된 고급 보안 기능(상호 의존적인 시스템에서 시스템 위협에 대한 보호 대책을 구현하기 위해 현재 기능의 최적화와 시스템 간의 협업 보안을 포함시켜 전체적인 상황 뷰 실현). 이런 기능은 계획–실행–점검–조치(PDCA) 및 관찰–위치 파악–결정–실행(OODA) 등의 기존 보안 기능을 IT 및 OT 시스템의 요구사항에 맞게 최적화하고 새로운 보안 기능(예: 상호 의존적인 시스템 간의 협업 보안)을 포함시켜 전체적인 상황 뷰를 얻을 수 있도록 한다. *보안 ID 및 IM* ▪ 결점 – 시스템에서 IoT 엔티티 및 그 ID를 검색하고 관리하기 위한 전체 프레임워크(다양한 유형의 장치와 상호 의존적인 시스템으로 구성되는 IoT 시스템에 필수적). ▪ 필요한 향상 – 보안 강화 기능을 위한 고급 작동 기능

그림 4-3 | 스마트 시티 최적화

4.2 공공 부문: 스마트 시티

스마트 시티 솔루션은 광범위하고 다양한 센서와 데이터 소스를 집합적으로 포함한 다수의 이종 IoT 플랫폼을 통합한다. 여기에는 온도, 습도, 소음, 가스 및 동작 센서, 카메라, 모바일 장치, 네트워크 스니퍼, 스마트 계량기, 수도 계량기 및 대민 서비스를 개선하는 동시에 도시 기능을 집합적으로 모니터링하고 도시 운영을 최적화하는 수많은 다른 장치가 포함되어 있다. 스마트 시티 IoT 플랫폼은 구문적 상호 운용성을 이용하여 이런 다양한 IoT 플랫폼의 다중 감지 정보를 도메인 간 및 실시간 정보 매시업으로 변환한다. 고급 데이터 마이닝 및 기계 학습 기법을 통해 다양한 각 플랫폼 및 운영 환경에 쉽게 액세스하여 주민 및 여러 기관에 맞는 애플리케이션을 제공함으로써 적절한 조치가 이루어지게 할 수 있다. 스마트 시티 플랫폼에는 공공 안전 향상, 도시 이동 수단 개선, 공공 시설 사용 최적화 및 물리적 개체와 연관되는 수많은 대민 서비스 향상을 위한 실시간 애플리케이션이 포함될 것이다. 스마트 시티 플랫폼과 Platform of Platforms(플랫폼을 위한 플랫폼)은 서비스 최적화를 위해 스마트 및 보안 감지에 크게 의존한다. 이들은 공공, 민간 및 개인 부문(필요에 따라 익명화)의 데이터 조합을 사용하여 스마트 시티 환경의 보다 전체적인 뷰를 원활하게 확보한다. 또한 도메인 간 통신 기법을 사용하여 지정학적 엔티티에서 개별 기관이 배포한 이질적인 IoT 시스템들을 통합함으로써 도메인 간 협업 및 최적화를 달성한다(그림 4-3 참조).

스마트 시티 플랫폼과 Platform of Platforms(플랫폼을 위한 플랫폼)은 시민 서비스 최적화에 중점을 두고 개발 중인 고급 데이터 처리 및 차세대 분석을 지원하기 위해 정보의 구문적 명확화와 맥락화에 크게 의존한다. 이런 플랫폼은 5G 및 인메모리

데이터베이스와 같은 고급 연결성을 활용하여 해당 지정학적 경계 내에서 수많은 장치에 의해 생성되는 방대한 양의 데이터를 이동 및 처리할 것이다. 이 플랫폼은 병렬 네트워크 연결 시스템에서 처리 토폴로지를 취급하기 위한 엣지 인지 스트림 처리를 지원할 것이다.

Platform of Platforms(플랫폼을 위한 플랫폼) 및 개별 플랫폼은 텍스트 생성 기술을 사용하여 시민들의 삶의 질이 보장되는 더 스마트하고 안전한 환경을 조성한다.

기존 기술은 본 사용 사례 실현에 부족하며 다음과 같은 향상이 요구된다.

연결성	▪ 결점 – 충분한 네트워크 대역폭, 네트워크 세션, 일시적 연결성 지원 ▪ 필요한 향상 – 5G와 같은 차세대 통신 아키텍처 및 프로토콜
처리	*데이터 수집 및 관리* ▪ 결점 – 경직되고 융통성이 없는 상호운용 정보 구조 및 어휘. 환경 메타데이터 메커니즘. 장치에서 플랫폼으로 단방향 흐름만 가진 장치. 데이터 소유, 데이터 보호 및 데이터 공헌에 대한 투명성과 통일성 결여. 다양한 데이터 출처의 비구조화되고 불필요 데이터가 많으며 간헐적인 데이터를 의미있는 맥락화된 정보로 해석하여 실시간 시스템을 지원할 역량이 없음 ▪ 필요한 향상 – 도메인 내 및 도메인 간의 정보 투명성을 위한 구문적 상호 운용성 표준과, 원본 형식에 관계없는 상위 IoT 온톨로지. 환경 컨텍스트 데이터에 대한 컨텍스트 메타데이터 표준. 장치, 센서, 작동기 및 플랫폼 간에 주문형, 맥락화, 다중 방향 데이터 흐름 지원 *분석* ▪ 결점 – 분석이 너무 경직되어 서비스 품질(QoS) 요구사항(예: 비상 대응) 및 시스템 재구성을 충족하지 못함. 날씨, 사회적 유행 및 최신 상황과 같은 변화에 대처하는 역량이 제한적 ▪ 필요한 향상 – 계획된 QoS 요구사항 및 고유 QoS 요구사항에 맞게 장치, 엣지 및 플랫폼 간에 작업을 동적으로 분할할 수 있는 알고리즘 및 도구를 사용하는 분산 분석. 계획된 변경 및 시스템 복원성을 위해 시스템 랜드스케이프 변경을 지원하는 동적 재구성 기능. 애플리케이션 실행을 촉진 및 관리하기 위해 병렬 네트워크 연결 시스템에서 처리 토폴로지를 취급하는 엣지 인지 스트림 처리 *시스템 상호 운용성* ▪ 결점 – 동적 작업 할당 및 서비스 마이그레이션이 전혀 지원되지 않는 경직된 아키텍처. 운영상의 조정 및 협업이 충분히 성숙되지 않음. 이종 플랫폼 환경에서 상호운용성을 보장하기 위한 표준의 일관성 부족 ▪ 필요한 향상 – 이종 시스템 간의 조정 및 협업을 위한 이종 엔티티 솔루션(장치, 하위시스템, 네트워크 및 서비스). 동적 온보딩 및 시스템 재구성 기능
메모리	–
감지	–

조치	*제어 인터페이스 장치* ▪ 결점 – 안전하고 보안이 확보된 데이터 보급, 원격 관리, 작동 권한 및 도메인 간 제어 *작동* ▪ 결점 – 융통성이 없는 경직된 프로그래밍 ▪ 필요한 향상 – 장치, 엣지, 플랫폼 및 시스템 환경의 실시간 상황에 기반하여 조정 가능한 유연한 루틴
보안	▪ 결점 – 운영 기술 보안성 및 안전성 관리. 안전한 운영의 연속성을 보장하기 위한 예방–탐지–위협 완화의 강력한 수명주기 관리 ▪ 필요한 향상 – 작동 권한 제어, 엔티티 간 데이터 교환의 인증, 자동화된 보호, 이상 완화 전략

4.3 소비자 도메인: 특수한 도움이 필요한 승객의 대중 교통 탑승 경험 개선

이 탑승 경험 IoT 시스템은 특수한 도움이 필요한 사람을 포함하여 승객 개인의 필요 및 선호를 토대로 목적지까지의 경로를 최적화해준다. 기본 플랫폼은 승객 이동을 모니터링하면서 경로 이탈을 식별하고 동적인 대안을 제공하며 승객 안전과 보안을 감독한다. 먼저 승객이 시스템에 교통 이동 정보를 입력하면 승객이 제공한 정보와 승객의 요구 및 선호에 따라 경로를 찾는다. 탑승 경험 IoT 시스템은 승객의 교통 이동을 모니터링할 최적화된 체크포인트를 선택한다. IoT 시스템은 실제 사용자 데이터와 버스 및 철도 운영자, 경찰 또는 도시 기관과 같은 이해관계자 관련 교통 서비스 데이터를 크라우드소싱 및 분석하여 예상 교통 이동 시간을 동적으로 판별한다. 스마트 및 보안 IoT 플랫폼은 모든 필수 개인정보보호, 데이터 소유권, 데이터 사용 규제 제한 및 지침을 제공한다.

탑승 경험 IoT 시스템의 스마트 및 보안 IoT 플랫폼은 스마트 시티 IoT 시스템에 대한 플랫폼 및 버스와 기차 등의 대중교통 운영을 조정하는 솔루션과 인터페이싱하며 다른 모든 승객의 불편을 최소화하는 동시에 개별 승객의 특별한 요구를 보다 원활히 지원한다. 예를 들어 버스 IoT 시스템은 탑승 경험 시스템과 협업하여 주어진 시간에 주어진 경로의 버스에 휠체어 또는 특수한 요청에 적합한 장비가 완전히 갖춰지도록 한다.

탑승 경험 IoT 시스템은 자체 운영 경험과, 다른 시스템으로부터 공유한 경험을 기반으로 한 자가 학습 기법을 활용한다. 또한 상황별 지식 취득 및 분석을 채택하여 그 시스템 자체와 기타 관련된 시스템을 동적으로 재구성하며, 이종 시스템 간에 공유되는 고급 정보를 이용하여 스마트 시티 시스템에 개별적으로 공급한다. 맞춤형 선택 접근법을 사용하면 현실세계의 역동성으로 인해 유발되는 불확실성 및 변동성을 관리할 수 있다. 관리상의 결정 및 상황별 적용은 기본 IoT 시스템을 구성하는 사물의 보안, 신뢰, 관리, 위치, 관계, 정보 및 컨텍스트 속성을 토대로 한다.

기존 기술은 본 사용 사례를 지원하기에는 부족하며 다음과 같은 향상이 요구된다.

연결성	▪ 결점 – 연결성 프로토콜의 표준화 ▪ 필요한 향상 – 연결 신뢰성 및 속도의 필요한 개선 지원을 위해 5G 표준 채택
처리	*데이터 맥락화 및 데이터 관리* ▪ 결점 – 강력한 데이터 맥락화 ▪ 필요한 향상 – 사용자, 시스템, 인터페이스 시스템 및 기타 연결되는 모든 것에 대한 표준화된 맥락화 메커니즘 *분석* ▪ 결점 – 개별 사용 사례에 중점을 둔 분석 알고리즘. 일시적 플랫폼 연결성을 지원하는 분산 분석. 애플리케이션에 맞는 컨텍스트 기능. ▪ 필요한 향상 – 분산 플랫폼을 지원하는 분산 분석. 부가가치 분석이 가능하도록 데이터의 동적 맥락화를 지원하는 표준화된 맥락화 메커니즘 *동적 구성* ▪ 결점 – 지속적인 개선을 지원하는 시스템 적용성 ▪ 필요한 향상 – 지속적인 동적 구성과 서비스 개선을 지원하는 기계 학습 알고리즘
메모리	–
감지	–
조치	–
보안	▪ 결점 – 물리적 센서 보호. 정보 조작. 개인정보보호 데이터 신뢰. 데이터 익명화. 개별 추적 및 위치. ▪ 필요한 향상 – 정보 출처 위험 노출 및 조작을 극복하는 데이터 신뢰 가치 메커니즘. 이종의 상호 연결된 IoT 시스템 및 플랫폼에서 적용 가능한 안전한 장치 식별 및 무결성 솔루션

제5절

스마트 및 보안 IoT 플랫폼의 기능 및 요구사항

5.1 미래 IoT 시스템의 일반 품질

미래 IoT 시스템과, 스마트 및 보안 IoT 플랫폼에 의한 지원을 통해 장치, 엣지 및 플랫폼에 대한 새로운 기능을 실현하고 그런 기능의 영향을 처리하기 위해 새로운 기술적 요구사항이 많이 생겨날 것이다. 예를 들어 새로운 정보 보안 기능은 엣지 컴퓨팅 및 센서에서 추가적인 기능을 요구한다. 센서 그룹과 IoT 게이트웨이의 상호작용을 관리하기 위한 새로운 API는 다양한 아키텍처 패턴과 운영 환경(예: 클라우드)을 캡슐화하고 상위 계층(예: IoT 애플리케이션, 서비스 인터페이스, 구성 제어 등)에 대한 단일 뷰를 제공하기 위해 장치 지원과 플랫폼 지원이 모두 필요하다.

단일 플랫폼이 IoT 아키텍처 패턴의 중앙에 상주하는 일반적인 개념은 대체될 것이다. 스마트 및 보안 IoT 플랫폼은 상호 의존적인 시스템 다수가 일반적인 독립부문의 속박을 벗어나 상호 보완적인 관계 속에서 협업하여 서로 다른 IT 및 OT 시스템에서 부가가치 서비스와 비즈니스 프로세스의 최적화를 가능하게 하는 “공생 생태계”를 실현할 것이다[17]. 서로 다른 상호 의존적인 시스템에서 정보의 통합과 보안 대책의 구현은 스마트 및 보안 IoT 플랫폼이 대응하는 가장 중요한 두 가지 과제이다. 이런 플랫폼에서는 시스템 통합성과 복원성 요구사항을 지원하기 위해 엣지에서 장치의 자율 배포와 더불어 동적 재구성까지 가능할 것이다.

스마트 및 보안 IoT 플랫폼은 새로운 운영 체제(예: 개발, 배포, 유지보수 및 향상에 대해 Cloud Foundry® 접근법을 따르는 오픈 소스 기반 시스템)를 사용한다. 이 플랫폼은 컴퓨팅 기능을 극대화하고 향상된 데이터 공학 기법을 지원하기 위해 Hadoop®, Lambda 아키텍처 및 신생 접근법을 강화하는 인메모리 데이터베이스 기술을 사용한다.

스마트 및 보안 IoT 플랫폼은 다음과 같다.

- 확장 감지 기능, 다중 연결된 IoT 시스템 간의 센서 융합 지원, IoT 제품성에 대한 기존 개념 및 신개념을 위해 개발된 알고리즘을 크게 강화하고 확장하는 미래형 분석 지원을 제공한다.
- 정보에 대한 이해를 높이고 분석 기술을 근본적으로 향상시키기 위한 새로운 표준을 토대로 하는 새로운 데이터 컨텍스트 메커니즘 및 데이터 의미론을 활용한다.
- 장치 보호 극대화, 다양한 지정학적 엔티티의 개인정보보호 요구사항 등의 복잡한 문제에 대처하는 보안 향상을 제공한다.
- 다양하고 지속적으로 변하는 유형의 사이버 및 물리적 위협에 대응하기 위해 계획-실천-확인-조치(PDCA), 관찰-방향설정-결정-실행(OODA) 및 상호 의존적인 시스템 간 협업 보안 운영과 같은 IT 및 OT 시스템의 핵심 보안 기능과 정책을 지원한다.

스마트 및 보안 IoT 플랫폼은 네트워크를 통해 장치, 제품 및 엣지 간의 전방위 데이터 흐름을 허용함으로써 "사물" 관련 정보의 수집, 저장 및 분석과 엔터프라이즈 및 IoT 특정 애플리케이션의 통합을 지원한다. 이 플랫폼은 서로 다른 데이터 유형 및 서로 다른 처리 기술을 초월하는 통합적 방식으로 대용량 엔드포인트 데이터를 처리하고 수명주기를 관리하는 수단을 제공한다.

핵심 플랫폼 서비스/기능을 결합하여 새로운 혁신적인 애플리케이션을 개발하도록 활성화하며 스마트 및 보안 제품과 서비스(구성 변경, 소프트웨어 업데이트, 원격 제어) 및 연결의 원격 관리를 지원한다. 더욱이 IoT 시스템 작동 방식의 중대한 진전으로서 스마트 및 보안 IoT 플랫폼이 게이트웨이, 제품 또는 장치(엣지 및 포그 컴퓨팅)에서 분산 데이터 (전)처리를 지원한다.

미래 IoT 시스템은 IoT 기능에서 파생된 특유의 "스마트" 기능을 통합할 것이다. 스마트 및 보안 IoT 플랫폼과 이 플랫폼에 포함되는 제품 및 서비스는 일상생활에서 쉽게 찾아볼 수 있게 될 것이다. 이런 기능에는 연결성 향상(인터넷, 클라우드 및 상호 간), 다양한 수준의 자율권, 몇 가지 IoT 엔티티와 시스템에 걸친 프로세스의 최적화를 위한 데이터 수집 및 처리 기능, 컨텍스트 인지, 자체 최적화 동작 등이 있다. 이런 기능은 소유자, 제조업체 및 서비스 제공자가 시스템 및 컴포넌트를 보다 원활하게 모니터링 또는 제어할 수 있게 하는 예측 유지보수와 규범적인 서비스를 촉진할 것이다. 이들은 표준 작업(예: 장치 온보딩)에 대한 최대 수준의 자동화를 지원할 것이며 엔티티 간 협업(집단 지능)을 촉진할 것이다. 검색 기능(예: 엔티티에 대한 지역 정보)은 시스템 컴포넌트 및 하위 시스템에 대한 컨텍스트를 제공하고, 엔티티의 이동, 상태 변경 또는 컨텍스트 변경에 따라 생성된 데이터를 파악하는 데 필요한 엔티티, 속성 및 메타데이터를 기술한다.

하위 수준에서 이런 "스마트 기능"은 시스템 컴포넌트의 설계, 제조, 사용 또는 유지보수에 대한 정보를 저장하는 "메모리"를 제공할 것이다. 높은 수준에서 그런 기능은 시스템 특정 질문(예: 현재 날씨, 대중에 대한 관련 세부사항 등)을 할 수 있는 기능을 제공할 것이다. 개발 프로세스에 있어 통합성과 상호 운용성 기능이 복잡한 IoT 시스템 개발 시 여러 벤더의 제품 통합을 지원할 것이다.

미래 IoT 시스템은 설계, 개발, 운영 및 유지보수를 포함하여 IoT 시스템과 컴포넌트의 전체 수명주기에 걸쳐 "전체적인 보안 기능"을 제공할 것이다. 이런 새로운 기능은 예를 들어 비즈니스 IT와 OT 간의 상호 의존성을 고려할 것이다. 그러므로 스마트 및 보안 IoT 플랫폼은 새로운 위협 분석 및 위험도 관리와 더불어 잠재적인 공격을 발견하여 퇴치하는 자체 회복 기능을 제공할 것이다. 시스템 복원성을 개선하기 위해 장치, 플랫폼 및 서로 다른 엔터프라이즈에 걸쳐 진정한 보안 협업 관리 시스템이 구축될 것이다. 이런 보안 협업 시스템은 새로운 종류의 위협 정보 메커니즘을 실행하여 조직 간에 신뢰할 수 있는 방식으로 보안 관련 정보를 교환할 수 있다. 또한 스마트 및 보안 IoT 플랫폼의 구현 대상 스마트 기능은 센서, 장치, 서비스 등의 관련 "사물"을 식별하고 데이터 무결성, 데이터 소유권 및 개인정보보호를 보장하기 위해 보다 진전된 기능을 요구할 것이다. 서로 다른 센서, 장치 및 시스템의 이종 데이터를 수집, 통합 및 처리하기 위해 새로운 연합 ID 및 액세스 관리가 요구된다. 미래 IoT 시스템에서는 엔터프라이즈 경계 간에 통제 가능한 데이터 소유권을 보장하기 위한 새로운 기능을 제공하여 구현 대상 미래 IoT 사용 사례를 지원해야 한다.

소비자 및 엔터프라이즈의 개인정보보호를 유지하는 동시에 대용량 데이터를 유용하게 활용하려면 검색 가능 또는 준동형 암호화 같은 암호화 방법이 요구된다.

표준 준수는 이미 복잡한 문제이며, 보다 동적이고 변경이 가능한 복잡한 IoT 시스템이 서로 다른 지역 및 규제 영역의 규정 준수 기능을 구축해야할 필요성을 제시할 것이다. 스마트 및 보안 IoT 플랫폼에는 IoT 시스템이 이런 복잡한 규제 현황을 탐색하고 이를 준수하도록 지원하는 기능이 내장될 것이다.

5.2 핵심 기능 및 요구사항

다음 절에서는 각 기능이 식별된 미래 IoT 사용 사례(부록 참조)와 연계되는 미래 스마트 및 보안 IoT 플랫폼의 핵심 기능을 기술한다. 또한 기술, 인프라, 조직 및 프로세스에 관한 추가 요구사항을 담은 전망이 제공된다.

5.2.1 연결성

엣지 및 플랫폼 수준에서 제공될 주요 연결성 기반 기능 중 하나는 실시간 상황 처리 및 감지수행이다. 이를 위해 데이터 소스와 시스템의 수신 부분에 대한 실시간 연결성 유지 기능이 중요하며 장치/제품과의 낮은 통신 지연시간, 로컬 컨텍스트 데이터에 대한 액세스 용이 및 중앙집중화 서버로 전송되는 데이터 용량의 감소로 인해 경우에 따라 엣지 수준의 실시간 상황 처리 및 감지수행이 필요하다.

장치 및 엣지 수준의 특별한 영향을 고려하여 원격 액세스 기능과 보안 연결성을 엔드 투 엔드로 구현할 필요가 있다. 따라서 신뢰할 만하고 보안이 확보된 연결성은 인증과 액세스 제어와 마찬가지로 장치로부터 플랫폼에 이르기까지 필수적인 요소이다. 장치의 보안 원격 액세스 기능이 플랫폼에 의해 유지되어야 할 뿐 아니라 IoT 시스템 자체에 대한 보안 원격 액세스도 플랫폼에 의해 지원되어야 한다. 이는 엣지 수준에서도 동일하게 적용되며, 인증 및 액세스 제어 기능뿐 아니라 장치 수준에서와 연결에서 데이터 무결성과 데이터 신뢰성을 보장하는 기능이 필수적이다.

제품 수준에서는 미래 IoT 장치에 대한 연결성 기능 및 요구되는 부분들이 여러 방식에서 현재 IoT 엔티티에 요구되는 분들과는 다를 가능성이 있다. 장치와 제품은 독립부문 내의 단일 시스템이 아니라 잠재적으로 여러 가지 시스템에 연결하는 기능이 필요하며, 그런 기능은 장치나 제품 내에만 포함되지 않고 제품 외의 다른 장소에 귀속되어 있을수 있다. 특히 장치의 이동성을 고려하여 서로 다른 대역폭과 프로토콜에 맞게 적용하는 것(서로 다른 시점에서 서로 다른 자원을 사용할 수 있음)도 미래에 필요한 기능이며, 이는 하드웨어 기반에서 소프트웨어 정의 네트워킹 솔루션으로의 전환을 촉발한다. 마찬가지로 소프트웨어를 사용하여 새로운 표준에 맞춰 장치 연결성 기능을 업그레이드할 수 있는 역량은 추후 유연하고 쉽게 구성할 수 있는 IoT 시스템을 유지하는 데 있어 중요한 요소가 될 것이다.

	산업				공공		소비자			
	BCM	Anom Detect	CSCM	Pred Maint	Smrt Cty	Soc Sens	Journ Exp	Conn Car	Ski	Smrt Fact
실시간 상황 처리	•	•	•	•	•		•	•	•	•
다중 시스템 연결성	•	•	•	•	•	•		•	•	•
원격 기능	•	•	•	•	•			•	•	•
모든 대역폭/프로토콜에 대한 적용성				•	•			•	•	•
새로운 연결성 표준으로 업그레이드 가능성	•			•				•	•	•
합법적 감청 기능					•					
원격 액세스	•	•	•	•	•	•	•	•	•	•
인증 및 액세스 제어	•	•	•	•	•	•	•	•	•	•
신뢰성 및 무결성	•	•	•	•	•	•	•	•	•	•

5.2.1.1 연결성 – 추가 요구사항

위에서 기술한 새로운 연결성 기능을 실현하기 위해서는 여러 가지 기술적 요구사항이 필요하며 그 가운데 가장 중요한 것 하나는 전체 시스템에서 지연시간을 대폭 감소하는 것이다. 특히 실시간 시스템이나, 구성이 동적으로 변경될 수 있는 시스템(구성 엔티티 세트가 크게 변동됨)의 경우 네트워크와 장치 수준 모두에서 낮은 지연시간이 요구될 것이다. 동시에 기존 프로토콜은 지연시간 감소 대책에도 불구하고 지연시간이 높은 시스템을 취급하는 데 충분하지 않을 수 있다. 예를 들어 TCP는 신호 전송 시간이 높게 설계되지 않았기 때문에 위성 연결 지연시간이 높다는 특별한 문제가 있다. 그러므로 미래 IoT 플랫폼이 지원하는 새로운 연결성 기능은 TCP/IP를 뛰어넘는 새로운 네트워크 프로토콜이 필요할 수 있다.

그러나 지연시간 감소 및 허용한도가 유일한 연결성 관련 요구사항은 아니다. 여러 자율 시스템 간 데이터 교환을 위해 새로운 통신 인터페이스도 필요하다.

5.2.2 처리

장치에서 대량의 다양한 데이터가 수집됨에 따라, 갈수록 더 복잡해지고 동적으로 변하는 애플리케이션뿐 아니라 더 대단해지는 기기 및 엣지 처리 기능을 다루기 위해 IoT 시스템의 모든 단계에서 처리 기능이 확장되어야한다. 장치 및 엣지 수준의 전처리 향상을 통해 중앙 서버로 전송되는 데이터의 응답 시간 단축 및 용량 감소가 가능하며 온보드 분석 기능 또한 갈수록 더 강력해질 것이다. 또한 기계 학습은 장치, 엣지 및 플랫폼의 필수 부분이 될 것이다.

고급 데이터 처리 지원을 위해 미래 IoT 시스템은 통제 하에 있는 장치/제품 및 외부 시스템에 의해 제공되는 데이터를 토대로 맥락화 정보를 제공할 필요가 있다. 이는 또한 다중 센서가 가상 장치에 대해 동적으로 구성되는 가상 센서 데이터의 처리에도 영향을 준다.

따라서 엣지에 있는 장치의 동적 구성 및 자가 구성이 특별한 기능으로 간주되며, 자가 치유 및 복원성을 위한 처리 기능이 특별히 유용해진다.

동적으로 변하는 이종의 미래 IoT 시스템 환경에서 데이터 소유권 문제를 해결할 수 있도록 데이터 소유권을 추적하고 데이터 액세스 규칙을 시행하기 위한 새로운 기능이 미래 플랫폼 기능에 있어 필수적인 부분이 될 것이다.

동시에 더 많은 데이터 익명화 기능이 엣지에 존재할 것이다. 하위 수준의 익명화는 모든 IoT 시스템을 위한 옵션이 될 수 없으며 서로 다른 익명화 알고리즘이 서로 다른 수준의 데이터에 적용된다. 그러므로 데이터 수집 시 일부 개인정보보호가 추가될 것으로 예상할 수 있지만 정보 보유와 익명성 사이에는 상쇄성이 있는 경우가 많으며 다수의 애플리케이션에 있어 보다 높고 중앙집중화된 수준에서 처리될 때까지 데이터 처리 목적으로 정보를 보유해야할 수 있다.

	산업				공공		소비자			
	BCM	Anom Detect	CSCM	Pred Maint	Smrt Cty	Soc Sens	Journ Exp	Conn Car	Ski	Smrt Fact
온보드 분석	•	•	•	•	•	•	•	•	•	•
오프보드 분석	•	•	•	•	•	•	•	•	•	•
기계 학습	•	•	•	•	•	•	•		•	
맥락화	•	•	•	•	•	•	•	•	•	•
익명화					•	•	•	•	•	•
정보 매시업	•	•	•	•	•	•	•	•	•	•
구문적 상호 운용성	•	•	•	•	•	•	•	•	•	•
장치의 동적 구성	•	•	•	•	•			•	•	•
동적 구성가능성					•			•	•	•
데이터 소유권 추적		•	•	•	•	•	•	•	•	•
집단 인지		•	•		•					

5.2.2.1 처리 – 추가 요구사항

5.2.2.1.1 확장성 및 운영

플랫폼 수준과 장치 수준에서 더욱 더 새로워진 기능에 의해 요구사항들이 추가되는 것을 감안하면 미래 IoT 플랫폼을 지원하고 미래 IoT 데이터 처리의 복잡성을 처리하기 위해 새로운 운영 체제 기능으로 구성된 새로운 시스템 아키텍처가 필요할 것이다. 3.8절에서 이미 언급했듯이 미래 IoT 플랫폼의 웹스케일 IT를 채택하려면

클라우드 아키텍처 향상과 높은 수준의 프로세스가 요구된다. 즉, 엔터프라이즈 IT 부서들이 공공 클라우드 제공업체와 유사하게 규모의 경제와 속도 및 관리 편의성뿐만 아니라 인프라, 시설 및 프로세스의 자동화를 위해 설계된 클라우드 기반 기술을 제공해야 한다. IoT 이니셔티브들은 본질적으로 “빠른 실패(fail-fast)” 성격을 띠며 동시에 여러 이해관계자에게 적용되어 신속하고 지속적인 제공이 요구되므로

서비스 제공의 개발/운영(DevOps) 모델이 구현되어야 한다.

5.2.2.1.2 가격 책정

또한 복잡한 데이터 처리에 대한 현재의 컴퓨팅 성능 가격대로는 대개의 IoT 시스템 적용 및 구현 비용이 매우 높을 수 있다. 예를 들어 IoT 시스템에 대한 새로운 비즈니스 및 사용 사례를 활성화하려면 플랫폼 수준에서 저비용의 컴퓨팅 성능 기술이 요구된다. 엣지에 있어 컴퓨팅 기능 및 암호화 기능을 가속화하는 기술이 필요하다. 차세대 IoT 시스템을 촉진하려면 가격과 기능 간의 보다 적절한 균형이 실현되어야 한다.

5.2.2.1.3 신뢰성 없는 도메인의 데이터 처리

미래 IoT 시스템의 성능 요구사항으로 인해 장치에서 수집된 데이터에 대한 컴퓨팅이 최대한 장치에 근접하여 수행되어야 하는 시나리오가 발생할 것이다. 종종 그런 도메인은 데이터 소유자의 보안 요구사항을 충족할 수 없으므로 처리를 하는 IoT 시스템의 컴포넌트에 데이터가 공개되지 말아야 한다. 그러므로 컴퓨팅 수행을 허용하고 데이터 소유자에게 유의미한 결과를 도출하는 동시에 데이터의 기밀성 및 무결성도 보호할 수 있는 메커니즘이 요구된다.

5.2.2.1.4 데이터 공학

데이터 공학자들은 특정한 비즈니스 의문을 풀어줄 모델을 생성할 수 있을 것이다. 이런 모델은 어떤 소규모 집단의 사람들에 의해 소비될 것이다. 그런 모델이 IoT 플랫폼의 일부가 되지 않고 비즈니스 프로세스를 지원하는 플랫폼 상에서 애플리케이션에 의해 사용되지 않으면 CRISP-DM(Cross Industry Standard Process for Data Mining)의 규모가 조절되지 않을 것이다. IoT 플랫폼이 모델 생성 프로세스와 실행 가능한 인사이트 구현에 있어 중요한 역할을 수행한다.

CRISP-DM 프로세스에 있어 비즈니스 질문의 정의는 비즈니스 전문가가 수행한다. IoT 플랫폼은 플랫폼 도구를 이용한 데이터 이해, 데이터 준비, 모델링, 평가 및 배포 프로세스를 관장한다. CRISP-DM 프로세스의 각 단계를 취급하기 위한 특별한 도구가 설계되어 이용 가능하다.

가치 있는 인사이트를 추출하고 조치를 취하기 위해서는 데이터 공학 알고리즘과 사람이 필요하다. 데이터 공학 모델이 추출한 실행 가능한 인사이트는 사람이 바로 사용할 수는 없다. 이 기능은 IoT 플랫폼에 임베드되어, 플랫폼 및 기타 연결된 플랫폼 상에서 실행되는 애플리케이션이 이 데이터를 사용하여 도메인 전문가가 비즈니스를 최적화하도록 지원한다.

데이터 공학의 미래는 과거보다 더 분명하다. IoT의 급속한 성장과 함께 2018년까지 IoT 장치에 의해 생성될 데이터는 1년에 403조 기가바이트에 달할 것이다[18]. 텍스트, 이미지 및 동영상에 대한 데이터 마이닝과 같은 “비데이터” 마이닝 부문의 성장도 예상된다. 이는 데이터 공학 기술 분야의 커다란 발전을 가져올 것이다. 데이터 이해, 데이터 준비, 기능 선택 및 평가와 같은 데이터 공학 작업의 자동화가 훨씬 더 일반적이게 될 것이다.

데이터 공학 예측이 보다 일반화되고 제로 풋프린트(최종 사용자가 소프트웨어를 전혀 설치하지 않고 사용하는 애플리케이션)로 진행될 것이다. 덕분에 기업들은 막대한 데이터 공학 인프라 예산을 절감하게 될 것이다. 뿐만 아니라 다수의 오픈 소스 솔루션이 시장에 선보일 전망이다.

데이터 공학 프로젝트의 성패는 기대 관리, 비즈니스 이득, 데이터 품질, 팀워크 및 분석을 실행에 옮기는 역량에 달려 있다.

5.2.2.1.5 상호 운용성

이종 센서, 장치 및 플랫폼 간의 상호 운용성이 높으면 컴포넌트가 상호 통신을 주고받고 원활한 정보 공유가 가능하게 될 것이다. IoT 피라미드 구조에서 서로 다른 수준의 다양한 부분(예를 들어 이해관계자가 다수인 제조 라인이나 공급망 네트워크) 간 상호작용은 다양한 파트너 간 협업을 촉진한다. 따라서 플랫폼에서 필요할 특별히 중요한 특별 기능 중 하나는 구문적 상호 운용성에 대한 실질적인 지원이다. 다시 말해서 시스템의 서로 다른 부분이 동일 통신 표준(공통어 접근법)을 공유하거나, IoT 플랫폼에서 다중 표준을 통합하고 다양한 언어 간 변환(통합 접근법)이 가능해야 한다.

상호 운용성 요구사항은 플랫폼 수준에서도 통합에 영향을 준다. 비즈니스, 안전성 및 복지를 포함한 사회의 다양한 측면에 IoT를 활용하려면 단일 플랫폼뿐만 아니라 Platform of Platforms(플랫폼을 위한 플랫폼), 즉 플랫폼들이 상호 협업하는 플랫폼 시스템을 고려할 필요가 있다. 일반적으로 플랫폼은 다양한 계층으로 구성되며, 각 계층에는 몇 가지 IT 시스템이 포함된다. 서로 다른 규칙(독립부문 시스템)을 토대로 하는 IT 시스템은 상호 간 또는 긴밀한 통신이 불가능하다. 이로 인해 서로 다른 격리된 IT 시스템뿐만 아니라 이런 플랫폼 간 통신을 처리 및 관리하는 특정 메커니즘이 요구된다.

그런 메커니즘을 구축할 수 있는 한 가지 해법은 각 IT 시스템 및 플랫폼에 데이터와 정보를 교환할 수 있는 출입구를 제공하는 것이다. 그와 같은 출입구를 가리켜 “프로파일”이라고 한다. 이 프로파일은 각 IT 시스템 또는 플랫폼이 필요로 하거나 제공하는 정보와 속성이 포함된 콘텐츠의 색인이다. 프로파일은 다른 IT 시스템 및 플랫폼의 요청에 응답하여 액세스 제어 및 데이터 제공 기능을 수행한다. 프로파일은 이중 변환 및 협업 프로파일로 구분되며 전자는 개별 플랫폼에서 데이터 교환을 처리하고 후자는 서로 다른 플랫폼 간에 협업을 관리한다.

5.2.3 메모리

제품 수명주기, 성능 데이터, 출처 및 기타 현실세계 요소에 대한 정보를 제공하는 디지털 제품 메모리(DPM) 기능을 엣지에서 사용하려면 분석 및 애플리케이션 컴포넌트에 통합하기 위해 플랫폼 수준의 지원도 필요할 것이다. DPM은 소형화된 임베드 시스템을 일상적인 개체 및 제품에 통합함으로써 실현 가능할 것이다[19].

메모리 향상과 더불어 소형화되어 통합된 임베드 시스템도 성능 데이터의 저장 기능 및 패턴 인지 기능을 향상시킬 것이다. 자원의 위치와 애플리케이션의 적용 위치에 따라 엣지와 보다 추상적인 수준 모두에서 이러한 기능을 기계 학습 및 분석에 사용할 수 있다.

	산업				공공		소비자			
	BCM	Anom Detect	CSCM	Pred Maint	Smrt Cty	Soc Sens	Journ Exp	Conn Car	Ski	Smrt Fact
디지털 제품 메모리		•	•	•					•	
패턴 인지	•	•	•	•	•				•	•
기능 데이터	•	•	•	•	•			•	•	•

5.2.3.1 메모리 – 추가 요구사항

스마트 및 보안 IoT 플랫폼에서 미래 IoT 기술을 개발하려면 플랫폼 자체가 비관계형 데이터베이스 스토리지 기술(예: Hadoop®, Spark 등)을 지원해야 할 것이다. 미래 IoT 시스템의 빅 데이터 분석을 지원하려면 인메모리 기술 등에 기반한 새로운 데이터 스토리지 및 처리 기술이 요구된다. 엣지 스토리지 및 처리에서 클라우드를 지원하는 기술도 개발되어야 한다.

5.2.4 감지

차세대 IoT 시스템은 감지된 데이터의 고급 감지 기능 및 보호를 모두 요구할 것이며, 특히 갈수록 복잡한 감지 기능과 센서 데이터를 처리하여 엣지의 다른 장치뿐만 아니라 그것들이 포함된 IoT 시스템의 다른 부분 모두와 교환이 필요하다 장치가 보다 많은 정보를 수집할 수 있게 됨에 따라 IoT 시스템 또한 이렇게 갈수록 증가하는 복잡하고 방대한 센서 데이터 및 장치의 새로운 감지 데이터에 대응, 통신 및 처리하는 기능이 필요할 것이다. 장치들 사이에서 데이터를 직접 교환할 수 있을 뿐만 아니라 플랫폼 중재 감지 데이터 교환 기능에 대한 요구도 발생한다. 플랫폼과 더불어 엣지 기능도 정확성, 신뢰성 및 개인정보보호 목적 등 모두를 위해 원시 센서 데이터 정리를 지원해야 할 것이다. 플랫폼뿐만 아니라 엣지와 장치도 장치에서 취득되는 센서 데이터의 신뢰성을 평가하고 IoT 시스템 내의 다양한 엔티티와 통신을 주고받는 데이터의 신뢰성을 보장하는 기능이 필요할 것이다. 데이터의 신뢰성을 보장하기 위한 통합은 플랫폼 컴포넌트에 의해 사용 및 전송되는 데이터의 무결성과 개인정보보호를 평가하고 보장하는 기능이다.

현 세대 센서는 대부분 인증을 요구하거나 지원하지 않지만 대개의 차세대 센서와 장치는 복잡성 및 고급 처리 기능으로 인한 인증 기능, 다양하고 동적으로 변하는 엔티티(일반 제조업체의 독립부문에 속한 엔티티와 반대)에 속하는 다른 IoT 시스템 컴포넌트와의 상호작용, 구성 가능성, 기능 향상으로 인해 사용 가능한 새로운 종류의 애플리케이션 등을 필요로 할 것이다.

또한 센서 수준에서 초정밀 위치 기반 기능을 지원하고 센서와 연관된 데이터 종류에 새로운 차원을 제공하는 고급 위치 감지 기술이 센서에 적용될 것이다. 또한 특히 초정밀 위치 기능에 의해 제공되는 보다 높은 정밀도의 데이터 처리를 위해, 그리고 소스 개인정보보호 보장과 애플리케이션 및 IoT 시스템에 의한 분석 지원을 위해 플랫폼의 지원이 필요할 것이다. 매우 구체적인 센서 데이터를 수집할 수 있는 엣지의 장치는 필터링 및 일반화 기능과 더불어 민감한 데이터 노출이 최소로 유지되도록 보장하기 위해 암호화 저장 및 통신 기능도 필요할 수 있다.

엣지 수준에서 차세대 IoT 시스템은 센서 융합 기술을 사용하여 통제 하에 있는 다중 센서의 정보를 외부 시스템의 정보와 통합함으로써 가상 센서를 구성하는 기능을 제공할 수 있다. 센서를 해당 기능의 양쪽 부분으로 재구성하는 기능은 복잡성으로 인해 현재는 그런 기능을 갖추고 있지 못한 감지 장치로 더욱 더 확산될 것이다.

	산업				공공		소비자			
	BCM	Anom Detect	CSCM	Pred Maint	Smrt Cty	Soc Sens	Journ Exp	Conn Car	Ski	Smrt Fact
감지 기능 포함 장치 수의 증가에 대응	•	•	•	•	•	•	•	•	•	•
감지 데이터의 중재 교환	•	•	•	•	•	•	•	•	•	•
데이터의 신뢰성	•	•	•	•	•	•	•	•	•	•
원시 데이터의 정리	•	•	•	•	•	•	•	•	•	•
초정밀 위치 기반 기능		•	•		•		•	•	•	•
개인정보보호					•	•	•		•	
데이터 무결성	•	•	•	•	•	•	•	•	•	•
인증을 요하는 복잡한 센서	•	•	•		•			•	•	•
센서 재구성 기능				•	•			•	•	•

5.2.4.1 감지 – 추가 요구사항

특징적인 감지 기능을 제공하기 위한 한 가지 요구사항은 초정밀 위치 기술의 개발이다. 이는 비콘, 초광대역(UWB), 영상 기반 위치 결정 등을 통해 촉진될 수 있다. 또한 이 요구사항은 장치 수준과 플랫폼 자체 모두에 영향을 준다.

5.2.5 조치

5.2.5.1 제어 인터페이스 장치

스마트 및 보안 IoT 플랫폼 및 엣지 기능은 장치 그룹의 교정 및 제어 기능(런타임 및 구성)을 제공한다. 또한 플랫폼의 기능은 장치의 동적 온보딩을 포함하여 장치의 동적 구성과 그런 장치 그룹의 관리를 지원한다.

플랫폼은 환경 및 컨텍스트에 따라 장치가 제어되는 방식을 맞춤화하는 기능을 갖출 수 있다. 플랫폼의 기능은 인증 지원에 더해 예측 유지보수, 액세스 제어 및 권한 부여의 경우와 같이 안전 요구사항을 보장하도록 확장된다. 더구나 미래 스마트 및 보안 IoT 플랫폼은 플로어 제어(floor control)를 활성화하고 계층적/협업적 제어 전략을 취급하여 IoT 장치의 자체 제어 집단(swarm)의 관리를 지원한다. 마지막으로 플랫폼의 기능은 보안의 집단 제어뿐만 아니라 컨텍스트 인지 제어로 확장될 수 있다.

그 밖에도 제어 운용을 통해 IoT 장치 자체의 기술적 운영을 제어한다. 구동 운용은 IoT 장치가 연결되는 가상의 물리적 시스템을 제어한다. 미래 IoT 시스템의 기능은 연결된 장치의 세부관리를 넘어서서 장치의 운영에는 어느 정도의 자유를 부여하고 장치가 준수해야 하는 일반 운영 정책을 제어하기에까지 이른다.

이러한 기능의 예: IoT 장치의 자체 제어 집단을 관리하는 제어 정책(계층적/협업적 제어 전략), 장치의 컨텍스트 인지 제어 및 환경/컨텍스트에 따라 해당 동작 적용

	산업				공공		소비자			
	BCM	Anom Detect	CSCM	Pred Maint	Smrt Cty	Soc Sens	Journ Exp	Conn Car	Ski	Smrt Fact
교정		•	•	•	•	•	•		•	
장치 그룹의 제어		•	•	•	•			•	•	•
장치의 동적 구성		•	•	•	•	•	•	•	•	•
컨텍스트에 따라 장치가 제어되는 방식 적용		•	•	•	•		•	•	•	•
안전성 요구사항	•			•	•		•		•	
인증 및 액세스 제어와 권한 부여	•	•	•	•	•	•	•	•	•	•
플로어 제어	•	•	•		•	•			•	
집단/자체 최적화 제어 지능		•	•		•				•	
보안의 집단 제어		•	•		•					
컨텍스트 인지 제어		•	•		•		•		•	

5.2.5.2 구 동

작동은 IoT 장치가 연결되는 가상 물리 시스템을 포함하여 현실세계를 조작하기 위해 미래 IoT 시스템이 제공하는 실행 기능이다. 추상화 및 복잡성 측면에서 서로 다른 광범위한 구동 작업이 존재한다. 직접적인 구동 운용은 단순한 전원 스위치 또는 전구 켬/끔과 같은 장치의 실행을 취급하며, 범위가 한정된 구동 운용은 주어진 범위, 즉 지형적 범위 내의 일정한 특성 또는 주어진 실행 조건을 지닌 모든 장치를 조작한다. 범위 한정 작동은 엣지나 플랫폼 컴포넌트에 의해 장치의 직접적인 작동으로 전환될 수도 있고, 장치로 전달되어 자체 범위를 점검할 수도 있다.

조건적인 구동 운용은 특정 조건이 충족될 때 시작된다.

플랫폼에서의 구동은 IoT 시스템으로부터 구동 작업을 요청하는 여러 가지 어플리케이션의 대량 요청을 취급해야 한다. 이는 조율, 충돌 해결 및 복구 절차를 요한다. 기능적 요구사항 외에는 보안 및 안전 작동 보장, 애플리케이션 및 장치의 양에 따라 규모 조절, 충돌되는 요청 처리, 오류 처리 및 진단 메커니즘 제공 등의 필요성이 있다.

한편 엣지 장치는 구동 작업 송수신, 구동 작업의 진행(작동의 품질 포함) 제어, 구동 자체 상태 및 IoT 시스템에 대한 컨텍스트 통보, 주어진 작동 수단의 신뢰할 수 있는 수행을 위한 기능이 필요하다. 또한 엣지 장치는 장치와 플랫폼에 대한 통신 중단 문제도 처리한다.

오늘날 엣지 장치는 단일 플랫폼에만 연결한다. 미래에는 다중 플랫폼 또는 애플리케이션(멀티 테넌트 엣지)에 연결하는 엣지 장치를 고려할 수 있다. 이 경우 동기화, 플로어 제어, 충돌 해결 및 오류 복구에 대한 기능이 필요하다.

작동의 특수한 측면은 직접적으로 연결되지 않으나 광학, 음향, 무선 또는 기타 물리적 신호 등을 통해 간접적으로 영향을 받는 시스템에 영향을 준다는 점이다. 이런 경우의 예로는 무선 비콘 범위 내에 있을 때만 실행이 허용되는 장치를 들 수 있다. 키(key)가 없는 자동차 시스템 또한 이런 경우의 예이다. 직접적으로(예: 텍스트나 디스플레이를 통해) 또는 간접적으로(예: 조명 상태를 조작하여) 인간의 동작에 영향을 주는 모든 종류의 시스템도 여기에 포함된다.

5.2.5.3 사용자 I/O

고급 사용자 I/O 기능은 미래 IoT 혁신에 당연히 포함될 부분이며 시스템의 모든 수준에서 지원할 필요가 있다. 촉각 인터페이스, 증강 현실 도구(예: 안경) 및 다중 장치 사용자 인터페이스는 모두 차세대 IoT 시스템의 사용성 향상과 사용자 체험의 일부가 될 것이다.

이런 고급 사용자 I/O 기능은 플랫폼에서 고급 처리 및 분석, 가상 모델 및 시뮬레이션 기능(예: 작업장 레이아웃)에 의해 지원되며 사용자의 직접적인 주변을 훨씬 넘어 사용자의 작업 및 이해를 확장할 것이다. 그러나 단일 플랫폼에서만 전체 IoT 시스템을 세부적으로 모델링 및 시뮬레이션하는 것은 수집되는 데이터 분량으로 인해 부적절할 수 있다. 그런 경우 모델링 및 시뮬레이션을 엣지로 이동하고 플랫폼에서 기본 컴포넌트를 통합 및 조율하는 기능을 넘겨받는다.

촉각 인터페이스를 통한 제어는 단기간의 사건에 대한 응답을 필요하게 만들 때가 있다. 원격 위치에서 촉각 인터페이스를 통해 제어할 때 물리적 거리로 인한 통신 지연시간이 문제가 될 수 있다. 그런 경우 엣지 기능에 원격 사용자가 사건에 신속히 대응하도록 지원하는 프록시 역할을 하는 기능이 있다면 효율적일 수 있다.

접근성 역시 차세대 IoT 기능으로, 모두에 대해 보다 단순하고 개선된 사용자 인터페이스를 지원하며 특수한 도움이 필요한 사용자도 수용한다(예: 웨어러블 장치의 신호에 보다 자연스럽게 응답하는 고급 인공 기관).

	산업				공공		소비자			
	BCM	Anom Detect	CSCM	Pred Maint	Smrt Cty	Soc Sens	Journ Exp	Conn Car	Ski	Smrt Fact
촉각 인터페이스		•	•					•	•	•
다중 장치 사용자 인터페이스		•	•	•	•		•	•	•	•
가상 모델링		•	•	•	•				•	
시뮬레이션	•	•	•	•	•		•		•	
접근성		•	•		•		•			
증강 현실				•	•				•	
사용성 및 사용자 경험	•	•	•	•	•				•	

5.2.5.4 조치 – 추가 요구사항

미래 IoT 플랫폼은 구동 작업의 서로 다른 범주(직접, 범위 한정, 조건, 구성)를 지정 및 수행하고 장기 구동 작업(예: 제어 루프)을 지원하는 시스템 메커니즘을 요구한다. 또한 구동 작업의 진행과 상태를 모니터링하는 메커니즘도 필요하다. 장치, 엣지 및 클라우드 간 구동 작업의 자동 및 컨텍스트 인지 분배를 위한 기술이 요구된다. 아울러, 적정 인증 및 권한 부여를 포함하여 구동의 보안화 수행을 지원하는 기술도 필요하다. 믿을 수 있고 신뢰성이 있는 구동은 신뢰성 있는 작업 수행을 보장하고 네트워크 또는 장치와 같은 시스템의 장애 복구가 가능하려면 새로운 기술 및 확장 시스템 아키텍처가 필요하다. 수행과 관련된 기타 요구사항으로는 낮은 지연시간 실행을 지원하는 기술 및 프로토콜과 더불어 중단 허용(disruption-tolerant) 실행의 제공이 있다.

5.2.6 보안

미래 IoT 시스템에 대한 Platform of Platforms(플랫폼을 위한 플랫폼) 개념 적용은 IoT 시스템에서 모든 컴포넌트 엔티티와 하위 시스템 정책을 통합하는 엔드 투 엔드 보안 정책과 위험도 관리 기능을 개발하는 기회를 제공한다. 플랫폼은 유사한 기능을 가진 엣지에서 장치에 의해 촉발될 수 있는 보안 문제 및 사건을 관리하기 위해 비관리 영역에서 엣지 장치의 자원을 관리 및 대리하는 기능도 제공해야 한다. 원칙적으로 이 플랫폼은 ISO 27001의 계획-실천-확인-조치(PDCA)에 상응하여 가용 물리적 자원과 보안 강건성 측면에서 최적화된 프레임워크를 제공해야 한다.

또한 이 플랫폼은 IoT 시스템에서 장치를 모니터링하고 이상을 탐지하는 기능도 제공할 것이다. 이런 기능에 있어 중요한 것은 사건을 판별하기 위해 데이터를 조율 및 분석하기 위한 추가 기능이다.

이는 시스템 위협 탐지 및 대응을 위한 관찰-방향설정-결정-실행(OODA) 주기의 절반이다. 이 주기의 나머지 절반은 복원성과 장애 허용 능력(가상 물리 공격 포함)이다.

IoT 시스템에 대한 관리 정책에 더해 플랫폼은 시스템 간 ID 상관관계, 연합 ID 관리, 장치 ID 보안화 및 진본성 관리, 특히 데이터에 대한 책임 및 부인 방지의 관리 기능도 제공해야 한다.

적용성과 대응성이 있으며 협조적인 보안이 플랫폼 수준에서 지원되어야 하는 중요한 추가 기능이며, 장치와 엣지에서 지원할 필요가 있는 기능도 있을 수 있다. 간단히 말해 시스템은 적용성 있게 새로운 위협 정보를 통합 및 학습하고, 추가 위협에 대한 계획을 세우고, 이런 계획을 실시할 수 있어야 한다. 또한 신속하고 적합하게 위협 및 공격에 대응하고 최대한 손상을 완화해야 한다. 마지막으로 서로 다른 엔티티가 소유할 수 있는 시스템 내 서로 다른 하위 시스템 사이에 협조적으로 문제를 진단하고 완화 및 예방 보안 계획을 구현할 수 있어야 한다. 이런 기능은 오늘날의 IoT와 차별화되는 미래 IoT 시스템의 특징이다[20].

엣지 수준에서 미래 IoT 시스템은 장치/제품을 인증 및 권한 부여하고 ID를 판별하며 ID를 토대로 장치/제품 액세스 제어 기능을 제공해야 한다.

엣지 장치는 IoT 시스템 내에서 더 큰 책임을 질 수 있으므로 해당 자원과 기능을 사용하여 플랫폼에 의해 정의된 보안 플랫폼 내에서 동적 요구를 충족하고 비관리 영역에서 보안 문제와 사건을 관리할 수 있다. 장치는 물리적 자원 및 보안 강화 측면에서 플랫폼이 배포한 최적 보안 프레임워크에 맞추면서 시스템 위협에 대한 탐지 및 대응 기능도 제공할 것이다.

전체적인 보안 정책 관리는 플랫폼 수준의 문제이지만 보다 역량 있는 장치라면 해당 위치에서 필요할 수 있는 로컬 정책 취급과, 보다 종합적인 보안 정책 전략의 일환으로 플랫폼에 의해 관리될 정책 취급을 위한 자체 정책 관리 기능이 필요할 것이다. 더 나아가 장치는 연합 ID 관리, 시스템 간 ID 상관관계 등을 용이하게 하기 위한 ID 관리 기능 향상을 필요로 하며 장치는 ID를 보호하는 기능을 갖추도록 설계되어야 한다. 장치 자체가 이런 기능을 제공할 수 없으면 엣지 기능이 이들을 IoT 시스템에 연결하는 프록시 역할을 할 필요가 있다.

이에 따라 엣지는 적절한 장치 및 제품 ID, 이들로부터 취득된 데이터의 신뢰성 확인 기능, 시스템 간 ID 상관관계 및 연합 ID 관리 기능을 제공해야 한다.

장치는 복원성 향상과 장애 허용 기능을 갖출 필요가 있을 것이다. 현재 IoT 장치는 상위 수준 서비스 및 애플리케이션이 이상 탐지 수행을 위해 사용하는 데이터를 제공할 수 있는 반면, 미래 IoT 장치에서는 엣지에서 이상을 탐지하는 기능을 추가함으로써 공격을 완화하고 (단지 원격 처리를 위한 정보 집계에 그치는 대신) 장애의 발생 장소와 시기를 탐지할 수 있게 될 것이다.

	산업				공공		소비자			
	BCM	Anom Detect	CSCM	Pred Maint	Smrt Cty	Soc Sens	Journ Exp	Conn Car	Ski	Smrt Fact
엔드 투 엔드 정책 관리	•	•	•	•	•	•	•	•	•	•
가용 물리적 자원 및 보안 측면에서 최적화된 프레임워크	•	•	•	•	•			•	•	
복원성	•	•	•	•	•			•	•	•
장애 허용 능력	•	•	•	•	•		•	•	•	•
시스템 위협 탐지 및 대응	•	•	•	•	•	•	•		•	
장치의 모니터링	•	•	•	•	•	•	•	•	•	•
협조 및 위협 분석	•	•	•	•	•		•	•	•	•
ID 관리	•	•	•	•	•	•	•	•	•	•
장치의 ID 보안	•			•	•	•	•	•	•	•
인증 관리	•	•	•	•	•	•	•	•	•	•
이상 탐지	•	•	•	•	•				•	

5.2.6.1 보안 – 추가 요구사항

5.2.6.1.1 ID 보안 및 ID 관리

미래 IoT 시스템은 수없이 많은 행위자와 컴포넌트로 이루어지며 서로 다른 수준에서 상호 신뢰를 해야 하는 이종 시스템 환경에 포함될 것이다. 이런 요소는 복제 장치를 포함한 신종 공격의 대상이 될 것이다. 정확하고 완전하며 적시성이 있는 데이터는 모든 IoT 시스템의 핵심이다. 데이터 무결성 및 진본성을 보장하고 간섭 및 조작이 없는 데이터 제공과 처리를 보장하는 기술이 요구된다. 이에 따라 미래 IoT 시스템에서 장치와 스마트 개체를 식별하기 위해 공개키 기반구조(PKI)보다 뛰어난 확장 가능하고 효율적인 기술이 필요하다. 복제가 불가능한 방식으로 고유 ID와 사물을 결합하기 위해 자료 기반의 확장 가능하고 효율적인 새로운 기술이 요구된다. 또한 서로 다른 시스템에서 이종 데이터를 수집, 통합 및 처리하기 위해 연합 ID 관리 시스템이 요구된다.

5.2.6.1.2 다면적이고 동적인 컨텍스트에서 개인정보보호 유지[21] [22]

IoT 시스템의 개인정보보호 문제는 시스템이 개별 요소들의 조합 이상의 의미를 가진다는 사실 때문에 복잡하다. 애플리케이션 또는 데이터 분석 수준에서 나타나는 우려사항과는 확실히 다른 하위 수준의 장치에 대한 개인정보보호 고려사항이 있으며, 시스템의 어느 수준에서라도 개인정보보호 위반이 발견될 경우 전체 시스템에 악영향을 준다.

예를 들어 하위 수준의 RFID 태그는 가시거리 없이 고속으로 판독 가능하다[23]. 다시 말해서 개체의 위치(따라서 특정인의 위치)를 노출하는 데이터를 원격으로 취득할 수 있다. 수동적 공격일지라도 효과적으로 행인을 도청하면 판독기 근처에서 무선으로 태그를 판독하여 사용자 위치 및 개인정보를 알아낼 수 있으며 일정 기간에 걸쳐 특정인에 대해 함께 전달된 RFID 태그 조합은 고유 ID로 효과적으로 사용되어 그들의 위치와 활동을 소리없이 추적하여 다른 정보 조각과의 상관관계를 분석할 수 있다.

(무선 센서 네트워크 등의 경우) 하위 수준일지라도 일단 통신에 연결되면 개인정보보호 위반에 대한 발생 가능성이 증가한다. 센서는 대개 컴퓨팅 및 저장 기능이 극도로 제한되어 있으므로 데이터 스트림 내용의 보안을 확보하는 새로운 방법(예: 임베드 및 경량 암호화)이 필요하다. 센서는 종종 엔드 투 엔드 암호화를 지원하지 않는 홉 투 홉(hop-to-hop) 통신 스키마를 사용한다. 따라서 새로운 키 교환 체계와 라우팅 프로토콜을 개발하여 포함시켜야 한다.

의도되지 않은 센서 데이터의 원격 액세스는 개인정보보호 위험 수준의 한 예이지만 그런 데이터에 의도적으로 액세스하는 서비스조차도 사용자 개인정보보호에 대한 과제를 제시한다. 데이터에 접근하는 의도적인 서비스는 공익기업, 장치 제조업체, 애플리케이션 제공자 등의 출처와 상관없이 사용자 데이터의 기밀성을 침해할 추가적인 공격 여지를 제공하므로 사용자 데이터는 액세스 권한을 보유한 엔티티의 보안에서 허용하는 만큼만 기밀성이 유지된다. 더 나아가 데이터 소유자 관점에서 보면 사용자 데이터에 대해 일반적으로 적합한 액세스 권한을 갖는 서비스도 모두 잠재적인 적이다. 공유 인프라를 통해 저장, 전송 및 처리되는 데이터가 등장하면서 미래 IoT 플랫폼은 적절한 액세스 제어를 시행하고 위반 시 저장된 데이터를 보호하는 새로운 서비스 및 신기술이 필요할 것이다.

또한 자신의 데이터가 일단 타인의 손에 들어가게 되면 무슨 일이 일어날지를 통제할 수 있는 능력을 부여하는 사용 제어와 같은 신기술이 필요하게 된다. 이는 소비자 만족을 위해서만 바람직한 속성이 아니고 기업체의 법적 과제이며 다수의 관할 지역(예: 유럽 연합)에서 최종 사용자의 권리이다. 미래 IoT 시스템은 엔드 투 엔드 개인정보보호 보장을 유지하는 동시에

로컬에서 데이터 노출을 통제하고 다양한 다른 시스템과 인터페이싱하는 방법을 모색해야 한다.

5.2.6.1.3 신뢰 구축

오늘날 대부분의 기술적 신뢰 구축 인프라는 사용자 또는 조직의 형태로 암호화 키와 키 소유자 간의 연관성을 보장하는 것을 목적으로 한다. WoT(Web of Trust)와 같은 분산 접근법이 존재하는 반면, 가장 실용적으로 사용되는 인프라(예: CA 기반 PKI)는 공통적으로 인정하는 신뢰 엔티티 세트를 중심으로 구성되어 상호 인증을 통해 임시적 신뢰 관계를 구축할 수 있다. 그런 인프라는 IoT에 국한되어있지 않는 몇 가지 잘 알려진 결함을 갖고 있다. 예를 들어 가까운 과거의 사례에서 암호화 인증서가 비승인 사용자에게 발급되었기 때문에 엔티티(특히 인증 기관)에 등록된 신뢰가 모든 경우에 정당화되는 것은 아님이 드러났다. 또한, 등록, 인증서 발급 및 취소, 그리고 상호 인증은 상당한 수동 작업을 요하며 장치 간 통신의 경우 사전에 설정을 해야 하는 대단히 무거운 프로세스이다. 따라서 사용자 상호 작용 없이 사전에 등록되지 않은 알 수 없는 상대에 대해 신뢰를 임시로 구축해야 하는 대부분의 IoT 시나리오에서는 중앙 신뢰 구축 인프라가 불가능하다. 그러므로 새로운 경량 신뢰 구축 알고리즘이 요구된다.

5.2.6.1.4 위협 분석 및 위험도 관리

보안 요구사항 및 기능을 고려할 때, 보안 구현을 지원하는 보다 고급화된 기술일지라도 성능과 보안의 균형은 여전히 매우 중요하다. IoT 애플리케이션 및 플랫폼의 각 속성에 따라 다양한 보안 요구사항에 상응하여 보안 기능을 제공하는 아키텍처를 지원할 필요가 있다. 특히 3가지 핵심 요구사항은 적용성, 대응성 및 협조성이다[24].

미래 IoT 시스템은 새로운 위협이 발견될 때마다 시스템에 선제 대책을 추가하는 기능인 적용성을 통합할 필요가 있다. 이 경우 보안 관리에서 널리 사용되는 기법인 PDCA 주기를 사용한다. PDCA는 새로운 위협을 식별하여 대응 방식을 결정하고 대응책 구현 방법을 계획한 후 이를 구현 및 평가하는 지속적인 프로세스를 통해 새로운 위협 발견을 처리하는 방법이다.

그러나 선제적인 보안만으로는 충분하지 않은 경우가 많다. 미래 IoT 시스템은 손상 완화를 위해서도 적절히 대응해야 할 필요가 있을 것이다. 사건 대응 수단의 중요성이 계속 커진다는 것은 공격이나 재난 발생 후 손상을 가능한 한 최소화하고 신속하게 복구하기 위해 대응성 개념이 필수적임을 의미한다. 이는 실시간 또는 실시간에 가까운 방식으로 상황을 모니터링하고 평가하여 무엇을 수행할지를 결정한 후 그 결정에 대한 조치를 취하는 OODA 루프로 달성할 수 있다.

마지막으로 협조성은 미래 IoT 시스템의 핵심 요구사항이다. IoT 시스템의 상호 의존성 증가는 고급 서비스를 제공하지만 공격이나 재난에 의해 특정 하위 시스템이 손상될 경우 다른 상호 의존적인 하위 시스템에 영향을 주어 전체 IoT 시스템에서 보다 광범위한 손상으로 이어질 수 있다. 이를 처리하기 위해 필요한 사항은 서로 다른 하위 시스템들이 서로의 상황에 대한 정확한 평가를 수립하도록 하는 협조성 개념을 적용하는 것이다.

그러므로 미래 IoT 플랫폼의 보안을 위해서는 시스템의 다양한 계층, 전체적 시스템 및 시스템의 전체 수명주기를 모두 고려하는 동적 보안 및 공격 모델을 개발하는 것이 필요하다.

미래 IoT 플랫폼은 시스템 요소의 손상이 전체 시스템에 미치는 영향을 감안해야 한다. 넓은 의미로 볼 때, 공격이나 재해로 인해 날로 다양해지는 위협에 대한 대책을 지속적으로 수립하는 과제를 해결 하는 데에 두 가지 방식이 있으며 이는 적응형 보안 및 전체 시스템 보호 기능과 관련된다.

고급 보안 기능을 갖추더라도 치명적인 사건(예: 자연재해)이 발생할 위험은 여전히 남아 있다. 연결된 시스템으로 인한 위협과 더불어 물리적 보안에 대한 명백한 위협(예: 인간의 운영 실수, 시스템 장애 및 자연 재해)으로 인해 중대한 손상이나 법적 책임이 발생할 수 있으므로 미래 IoT 시스템 아키텍처의 보안 설계 및 구현의 일환으로 향상된 보안 대책이 필요할 것이다. 보안 수준과 비용의 절충은 개별 상황(즉, 사용 사례와 비즈니스 환경)에 크게 의존한다. 예를 들어 의료 장비의 생산 및 배포를 위한 보안 수준과 비용을 소비재의 경우와 비교해 볼 수 있다. IoT 시스템 컴포넌트의 설계 및 구현 중에 개별 위험도를 평가하고 보안과 비용의 절충에 대한 결정을 하기 위해 적절한 방법 및 모델이 필요하다. 미래 IoT 시스템, 단말 장치, 엣지 장치 및 플랫폼 자체에 의해 발생하는 복잡성의 증가로 인해 특히 가상 물리 공격과 관련하여 보다 발전된 위험도 분석 및 관리를 위한 일반 정보와 지원이 필요하다.

복잡한 시스템의 전체 수명주기에 걸친 위험도 평가 및 위험도 관리 방법('지속적인 보안 관리' 주제 참조 – 위험도 관리 내용에 대한 보충 설명)은 보안 관련 데이터를 수집하고 처리하며 해당 데이터를 토대로 동적 및 온라인 위협 분석을 수행하기 위해 새로운 기술이 필요하다.

이종 및 분산 소스에서 발생하는 신뢰성 있고 편향된 데이터를 처리할 수 있는 실시간 위협 분석을 수행하기 위해 기계 학습 알고리즘을 토대로 하는 새로운 접근법이 요구된다. 요구되는 새로운 위협 분석 알고리즘은 높은 정확도의 경고와 최소량의 긍정 오류(false positive)를 생성해야 한다. 또한 이런 알고리즘은 학습 데이터를 고의로 공격 및 변조하여 기본적인 기계 학습 알고리즘의 동작을 제어하려는 적대적인 공격에 탄력 있게 대응해야 한다. 미래 IoT 시스템에서 조기 경고 대응 기능을 활성화하기 위해 새롭고 협조적인 위험도 관리 시스템과 보안 프로토콜이 요구된다.

5.2.6.1.5 지속적인 보안 관리

IoT 시스템의 취약한 컴포넌트는 관련 당사자(예: 플랫폼 제공자 또는 IoT 서비스 소비자)의 보안 요구사항을 위반할 수 있다. 그런 취약성의 악용은 모든 참여자의 비즈니스 모델을 위협한다. 이런 위험도를 완화하기 위해 IoT 컴포넌트의 보안 감사에서는 해당 컴포넌트가 보안 요구사항 세트를 충족하는지 여부를 조사해서 보안 수준을 제시한다.

일반적으로 보안 감사는 특정 기간(예: 1년) 동안 유효하다고 추정되는 결과를 작성하는 별개의 작업이다. IoT의 경우, 안정성에 대한 이 전제는 유지되지 않는다. IoT 컴포넌트는 시간의 흐름에 따라 변하며 때에 따라 이런 변경사항은 플랫폼 제공자나 서비스 소비자가 탐지하거나 예측하기 어렵다. 더군다나 IoT 컴포넌트의 보안 수준만 별개로 고려하는 것은 IoT 서비스가 서로 상호작용하는 수많은 이종 기술(예: 플랫폼 및 장치)의 결과라는 점을 간과한 것이다.

그러므로 IoT 시스템에 대한 보안 감사는 IoT 서비스의 지속적인 변경사항을 탐지하고 보안 수준에 대한 영향을 실시간으로 평가할 수 있는 서로 다른 접근법을 요구한다. 또한 그런 방법은 공격자로부터 IoT 서비스를 보호하는 데 요구되는 완화 및 예방 보안 대책의 토대를 구축한다.

제6절

스마트 및 보안 IoT 플랫폼에 대한 차세대 지원 기술

이 절에서는 스마트 및 보안 IoT 플랫폼을 실현하는 데 필요한 몇 가지 핵심 차세대 지원 기술을 중점적으로 살펴본다. 제4절에서 기술한 사용 사례에 대해 필요한 향상을 살펴보고 이들을 제5절에서 제시한 기능과 결합하여 마지막으로 지원 기술을 도출한다.

생산 라인, 스마트 시티 및 대중교통의 탑승 경험 개선에 대한 비즈니스 연속성 관리와 관련된 본 백서의 3가지 주요 사용 사례 분석은 결점과 필요한 부분의 개선이 중첩됨을 설명한다. 보안, 실시간 데이터 관리 및 상호 운용성은 IoT 측면에서 새로운 것이 아니지만 핵심 요소로 남아 있으므로 차세대 기술의 전체 영역이 원활하게 구현되어 일상적인 현실세계 시나리오에 적용되어야 한다.

보다 구체적인 수준에서, 사용 사례로부터 도출된 기술 향상은 다음과 같은 영역에 자리하며 이에 대해서는 제4절 및 제5절에서 간단히 살펴보았다.

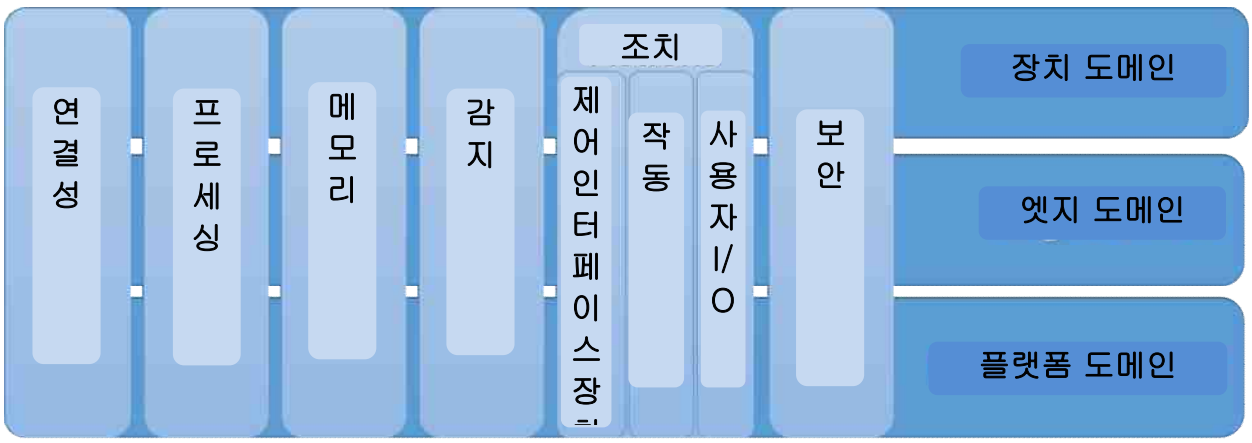


그림 6-1 | 주요 개선 영역

6.1 연결성

6.1.1 차세대 위성 연결용 전송 계층 프로토콜(보다 높은 대역폭, 높은 지연시간)

현재 IP 네트워크에서 전송 프로토콜로 널리 사용되고 있는 TCP(전송 제어 프로토콜)는 혼잡 제어 기능을 갖추고 있다. 이 기능은 전송 장치가 한 번에 전송 가능한 데이터 용량을 추산하는 메커니즘을 통해 실현된다. 작은 수치에서부터 용량을 점증적으로 증가시키다가 패킷 손실 탐지 등의 사건을 통해 간접적으로 혼잡이 탐지되는 시점에 용량을 줄이는 방식으로 이 데이터를 추산한다. 위성 연결은 주로 높은 대역폭과 지연시간(예: 수 천 밀리세컨드)을 가지며, 한 번에 전송되는 데이터 용량을 양호하게 추산할 수 없으면 TCP가 가용 대역폭을 완전히 활용할 수 없다. TCP가 동시 전송 데이터 용량에 대한 추산 값을 얻을 때까지 일정 시간이 소요되므로 TCP가 위성 연결의 전체 대역폭을 활용할 수 있게 되기 전에 위성 연결을 통한 엔드 투 엔드 통신이 종료된다는 점에서 문제가 발생한다. 전송 장치가 대역폭 정보를 추산하지 않고 통신 장비가 대역폭 정보를 제공하도록 하여 대역폭과 지연시간이 높은 위성 연결의 대역폭을 완전히 활용할 수 있도록 하는 등의 새로운 프로토콜 기술을 개발하여 도입하는 것이 효율적일 수 있다.

6.1.2 차세대 통신 시스템

6.1.2.1 5세대 셀룰러 액세스(5G)

5G 무선 네트워크 용량 면에서 1000배 늘어나고, 1000억 개 이상의 장치에 대한 연결을 지원하며, 지연시간 및 응답시간이 극도로 낮으면서 전송속도 10Gb/s의 개별 사용자 경험을 지원할 것이다. 이런 네트워크의 배포는 2020년부터 2030년 사이에 실현될 전망이다. 5G 무선 액세스는 새로운 무선 액세스 기술(RAT)과 개선된 기존 무선 기술(LTE, HSPA, GSM 및 WiFi)을 토대로 구축된다. 무선 네트워크 혁신을 통한 돌파구는 완전히 새로운 방식으로 경제 및 사회적 성장을 촉진할 것이다. 5G는 인간과 연결된 기계 사이에 영거리(zero-distance) 연결성을 제공할 수 있는 네트워크를 실현할 것이다.

5G 기술의 개발은 ICT 네트워크 인프라 혁신의 돌파구를 실현하는 초석이다. 어디에 있는지에 관계없이 인간과 연결된 기계 사이에 거의 즉각적으로 영거리 연결성을 달성하는 초광대역 및 지능형 파이프 네트워크 기능이 바로 그 첫 단계이다.

차세대 IoT 시스템가 관련하여 대규모 용량 및 연결뿐 아니라 갈수록 다양해지는 서비스, 애플리케이션 및 사용자 세트(직업 및 생활과 관련된 매우 다양한 요구사항)를 지원하기 위해 5G 무선 네트워크가 필요할 것이다. 매우 다른 네트워크 배포 시나리오들에 대해 사용 가능한 모든 독립적인 대책들을 유연하고 효율적으로 사용하는 것도 필요하다. 모바일 네트워크는 점차 인간과 인간 및 인간과 기계 연결을 위한 기본 네트워크 액세스 수단이 될 것이다.

이런 네트워크는 제공되는 서비스 품질, 신뢰성 및 보안 면에서 고정 네트워킹의 발전에 부응할 필요가 있을 것이다. 이를 위해 5G 기술은 초고해상도 영상 통신과 몰입형 멀티미디어 상호작용을 가능하게 하는 광케이블급 10Gb/s 속도를 지원할 수 있어야 할 것이다. 이런 기술은 지연시간이 밀리초 미만인 초광대역폭에 의존할 것이다.

갈수록 다양해지는 광범위한 모바일 서비스의 각 성능 요구사항은 1 밀리초~몇 초까지의 지연시간, 수백~수백만까지의 셀당 상시 접속 사용자 수, 몇 밀리초에서 꼬박 며칠에 이르기까지 등 작동 주기는 다양할 것이다.

동시에 5G는 1% 미만~약 100%까지의 신호 부하를 제공할 것으로 예상된다.

아래의 5G 하이퍼서비스 큐브는 5G 네트워크에서 실행해야 하는 다양한 유형의 서비스에 필요한 처리량, 지연시간 및 연결 수 측면의 다차원 개요를 제공한다.

그림 6-2 | 5G 하이퍼서비스 큐브

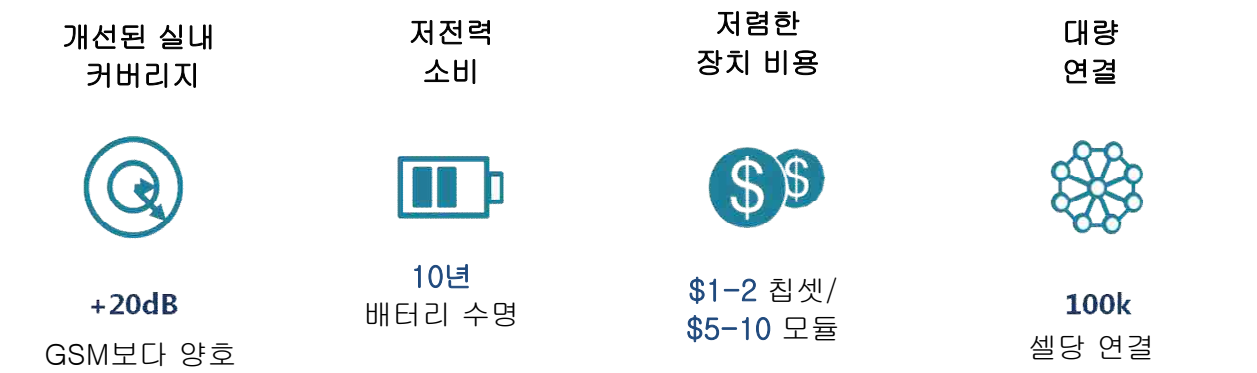
6.1.3 저전력 무선 액세스 네트워크(LPWAN)

LPWAN 시장의 역사는 약 10년 정도 되었다. 현재 이 시장을 지원하는 기술(솔루션)은 분할되어 있고 비표준화되어 있으므로 신뢰성이 부족하고 보안성이 열악하며 운영 및 유지보수 비용이 비싸다는 단점이 있다. 더욱이 새로운 오버레이 네트워크 배포는 복잡하다.

최근 들어 광역 유비쿼터스 커버리지, 기존 네트워크의 고속 업그레이드, 낮은 전력 소비의 10년 배터리 수명 보장, 높은 결합도, 저비용 단말기, 플러그 앤 플레이, 높은 신뢰성 및 높은 반송파 등급 네트워크 보안, 통합 비즈니스 플랫폼 관리 등의 다양한 장점을 제공하여 위의 단점을 보완하는 3GPP Rel.13 LTE Cat-M1(eMTC) 및 Cat-NB1(협대역-IoT) 등의 새로운 표준이 정의되었다. 중복 비용이 매우 적기는 하지만 초기 네트워크 투자 비용은 꽤나 상당할 수 있다. 위에 언급한 구축된 기술 중 하나인 협대역 IoT(NB-IoT)는 LPWAN 시장 요구사항을 완전히 충족하여 운영자들이 이 새로운 분야에 진입할 수 있도록 지원하므로 여기에서는 LPWAN 기술의 예를 구체적으로 살펴본다.

NB-IoT는 초저가(USD 5) 모듈과 탁월한 연결성(100K/cell) 덕분에 운영자들이 스마트 계량 및 추적과 같은 일반적인 비즈니스를 운영할 수 있도록 지원하고 스마트 시티나 e보건과 같은 추가적인 산업 도메인 진출 기회도 제공한다.

NB-IoT는 보다 많은 사물이 연결될 수 있도록 하지만 이에 따른 빅 데이터의 상업적 가치 관리는 주요한 과제이다. 운영자는 관련 산업과 협력관계를 수립할 수 있다. 즉, 연결 서비스뿐 아니라 데이터도 판매할 수 있다.



우선 LPWAN 애플리케이션은 지하나 실내 어디에나 배포될 수 있기 때문에 이 애플리케이션의 경우 커버리지가 기본 요구사항이다. 현재 2G/3G/4G 기술은 인간 사용자 연결용으로 설계되었으므로 M2M 연결에 적용할 때 커버리지가 부족하다. 중국의 어느 도시 데이터는 2G 기술을 갖추고 있는 스마트 계량기 중 약 2% 정도는 약한 커버리지 때문에 데이터를 보고할 수 없는 것으로 나타났다. 그러므로 해당 전력 회사는 그런 2% 사용자의 데이터를 수동으로 확보해야 한다.

또한 저전력 소비는 스마트 계량기, 스마트 주차, 웨어러블 장치 등의 애플리케이션에서 스마트 그리드에 이르기까지 모든 LPWAN 사용 사례 중 약 80%에서 필수조건이다. 그런 애플리케이션에 대한 기본 요구사항은 일단 장치가 설치되고 나면 몇 년 동안은 유지보수 서비스를 필요로 하지 않아야 한다는 점이다. 그렇지 않을 경우 유지보수 비용이 상승할 것이다. 대규모 연결 애플리케이션에서 며칠 간격으로 배터리를 교체해야 한다면 재앙에 가까울 것이다.

대부분의 LPWAN 장치는 연기 탐지 센서, 토양 감지 센서 또는 보안 센서와 같은 센서이다. 그런 장치의 경우 단가가 매우 저렴하며 대부분 USD 10 정도에 판매된다. 이런 센서들을 연결하려면 통신 모듈 역시 매우 저렴해야 하며 통신 모듈이 총 가격의 50%를 넘지 않아야 한다. 그렇지 않으면 운영자가 센서 관련 애플리케이션을 설치하는 데 큰 걸림돌이 될 것이다.

POS(Point Of Sales) 기계 및 스마트 계량기 등의 스마트 장치 애플리케이션의 경우 이미 몇 가지 후보 IoT 기술이 사용 중이다. NB-IoT는 커버리지와 전력 소비 측면에서 이런 기술을 압도하지만 그런 스마트 장치를 선정할 때 가격도 사용자 입장에서 중요한 요소이다. 2G 모듈의 현재 가격은 USD 8에서 USD 13 사이이고 가장 저렴한 SigFox 모듈은 이미 USD 9로 하락했다. 업계의 공통적인 견해는 NB-IoT 모듈의 이상적인 가격은 USD 5 미만이어야 한다는 것이다.

모바일 광대역(MBB) 연결 수의 증가는 사용자 인구에 따라 제한되지만 IoT 연결은 자동차, 계량기, 동물, 식물 등 수없이 많은 사물에 연결되므로 IoT 연결 수의 증가 추세는 다가오는 수년 내에 MBB 연결 수 증가보다 훨씬 빠를 것이다. Machina의 예측에 따르면 총 IoT 연결 수는 270억 개로 증가하고[25] 그 가운데 CAGR이 18%를 차지할 전망이다. IoT의 일부인 NB-IoT의 연결수도 상당히 증가할 전망이다. 일상 사물들을 연결할 수 있도록 NB-IoT 셀의 용량은 MBB 셀보다 훨씬 커야 한다. 모든 가구에 평균 40개의 장치가 있고 평방 킬로미터당 가구 밀도가 1500이라고 가정하면 각 셀에서 100,000개의 동시 연결 용량이 필요하다.

6.1.4 사용 사례에 대한 매핑

	산업				공공		소비자			
	BCM	Anom Detect	CSCM	Pred Maint	Smrt Cty	Soc Sens	Journ Exp	Conn Car	Ski	Smrt Fact
차세대 위성 연결에 대한 전송 계층 프로토콜					•			•	•	
제 5세대 셀룰러 액세스(5G)				•	•			•	•	•
저전력 무선 액세스 (LPWAN)					•	•		•	•	•

6.2 처리

6.2.1 시스템 구성 및 동적 구성

새로운 센서 융합 기술은 “물리적 센서”뿐 아니라 소셜 미디어, 사람의 입력(이른바 인간 센서), 크라우드소싱 데이터 등의 “가상 센서”로부터 얻은 데이터를 고려할 것이다. 이런 감지 데이터를 신기술의 설계에 통합하면 (미래형 스마트 시티 등을 위한) 센서 융합 및 처리의 고급 기능들이 개발될 것이다. 미래 IoT 플랫폼에서는 압축된 방식의 데이터 수집이 예상되기 때문에 이런 신기술은 데이터 수집 시 데이터 활용을 극대화하고 개인 정보 기밀 누출을 최소화하는 방법을 취급한다. 실시간 DevOps 기술은 업데이트된 소프트웨어를 개발 및 배포하기 위한 애자일(agile) 프로세스이다. 프로그래밍 및 재구성 가능한 소프트웨어 컴포넌트(예: 데이터 분석의 알고리즘 또는 데이터 가상화 도구)를 신속하게 분리 또는 재결합하여 미래 IoT 플랫폼의 동적 업데이트 및 요구사항에 맞게 적용할 수 있다.

6.2.2 데이터 맥락화

컨텍스트를 제공하는 다량의 메타데이터를 다양한 IoT 컴포넌트 자체가 개별적 및 집단적으로 캡처한다. 또한 데이터 자체는 수집된 데이터 이면의 투명한 정보 또는 숨겨진 정보를 추출하기 위한 맥락화 변환 프로세스의 대상이 될 수 있다. 전체적으로 이 컨텍스트는 컨텍스트별 마이닝 및 분석 알고리즘을 통한 특정 지식 도메인에서 의미 있는 형태의 데이터를 나타낸다. 데이터 맥락화의 새로운 기법은 이력적 데이터 분석, 실시간 상황 인지 및 상황 예측을 상당히 향상시킬 것이다. 이력적인 데이터 분석은 컨텍스트별 정보 및 기능을 점증적으로 갱신한다. 실시간 상황 인지는 특정 사건을 탐지하며 이를 토대로 알 수 없는 사건의 컨텍스트별 특징을 발견한다. 상황 예측은 미래에 일어날 일을 예측한다. 데이터 맥락화 프로세스는 분산 플랫폼의 모든 구성요소에서 발생할 수 있다.

데이터 맥락화 기법의 예는 다양한 스마트 시티 애플리케이션에서 볼 수 있다. 모바일 장치(예: 랩탑, 스마트폰 및 태블릿)의 인기가 높아짐에 따라 특정 지역의 혼잡도는 그런 모바일 장치로부터 방출되는 신호 및 위치 포함 감지 데이터를 토대로 추정할 수 있다. 인간의 이동에 대한 컨텍스트별 정보는 주변 네트워크 신호 뒤에 숨겨진다. 이력적 데이터 분석은 이동 패턴(예:

열차 정류장의 주간 패턴)의 규칙성을
찾는다.

실시간 상황 인지는 혼잡도를 탐지한다. 추가 환경 컨텍스트 데이터는 다른 센서에서 이용 가능하다. 다양한 서비스를 지원하는 플랫폼 간의 상호 참조는 추가로 컨텍스트를 제공한다. 상황 예측은 이력적 데이터 및 실시간 데이터를 토대로 혼잡 집단의 시간 및 위치를 예측할 수 있다. 엣지 계층에서 IoT 게이트웨이는 데이터가 플랫폼으로 전송되기 전에 가벼운 데이터 필터링 및 개인 기밀 정보 해싱을 수행한다. 주요 데이터 맥락화 작업은 플랫폼에서 수행된다. 그러나 미래에는 IoT 게이트웨이의 기능이 향상될 것이기 때문에 실시간 상황 인지는 엣지 측으로 마이그레이션될 수 있다. 반면 높은 수준의 컨텍스트별 정보는 클라우드에 보고되어 이력적 데이터 분석 수행에 사용되며 데이터가 축적되면서 추가로 상황 예측을 수행한다.

미래 스마트 및 보안 IoT 플랫폼은 수많은 데이터 소스 및 사용자와 애플리케이션들을 수용할 것이므로 미래 데이터 맥락화 기술이 특정 서비스 품질 요구사항을 위한 융통성 있는 처리 토폴로지를 관리할 것으로 예상된다. 이 목표를 달성하기 위해 처리 작업을 엣지의 서로 다른 엔티티 및 다운스트림 감지 엔티티로 적절하게 오프로드할 수 있다. 그러므로 데이터 교환 모델 및 인터페이스의 표준화는 병렬 데이터 분석의 촉진에 대한 탐색이 필요하다. 정보 메시업을 촉진하기 위해 최종 장치, 기계, 엣지 및 플랫폼으로부터 데이터 수집, 상황 주석 달기 및 메시업 추가를 수행하기 위한 표준화된 추가 인터페이스도 예상된다. 예를 들어 의미적 장소로서 초정밀 정보의 추상화에 주석을 다는 것은 앞에서 언급한 이동성 분석에서 모바일 장치, 플랫폼 등의 데이터 수집 시 수행할 수 있다.

마지막으로 미래의 맥락화 정보 모델은 정보를 전체 시스템에 사용 가능한 상황별 지식의 메타데이터로 변환한다.

6.2.2.1 자원 관리의 최적화

미래 플랫폼에서는 데이터 및 처리 작업부하가 엄청나게 증가한다. 더군다나 미래 플랫폼은 다양한 애플리케이션에 대한 멀티 테넌시(multi-tenancy) 지원을 제공할 필요가 있다. 대규모 및 실시간 IoT 애플리케이션의 배포 및 유지보수 비용은 비싸기 때문에 미래 플랫폼에서는 다중 애플리케이션과 사용자 간의 자원 공유, 엣지와 플랫폼의 자원 관리, 프론트엔드와 백엔드 간의 처리 작업부하 분배 등을 최적화하여 데이터 맥락화 프로세스의 규모를 확대할 필요가 있다.

6.2.2.2 실시간 개발 및 운영(DevOps)

실시간 데이터 스트리밍, 데이터 처리 및 작동은 미래 IoT 애플리케이션을 촉진하기 때문에 다양한 IoT 애플리케이션들이 개발될 수 있도록 주문형 방식을 통한 IoT 서비스의 빠른 개발 및 운영이 요구된다. 이 목표를 달성하기 위해 실시간 DevOps는 새로운 IoT 애플리케이션의 발매 수명주기를 단축시킬 수 있으며 개발자는 재프로그래밍 및 재구성 가능 데이터 맥락화 컴포넌트를 함께 연결하여 즉각적으로 새로운 서비스를 작동할 수 있다.

6.2.3 자율적인 데이터 교환

장치, 장비, IT 시스템, 플랫폼 등의 엔티티 간에 수행되는 자율 데이터 교환을 위해, 데이터 통신을 관리하는 프로파일이 중요한 역할을 한다. 자율 데이터 교환을 활성화하려면 데이터 교환 규칙을 구축할 필요가 있다. 데이터 교환 규칙을 토대로 프로파일을 설계해야 하며 필요충분한 통신 관리 기능을 제공해야 한다. 또한 데이터 사용 목적과 데이터 보안 수준 등의 상황에 따라 권한을 제어하는 융통성 있는 데이터 액세스 제어 기능을 제공해야 한다.

미래 IoT 시스템은 IoT 장치가 장치들 간에 직접(장치 대 장치) 또는 엣지/클라우드 플랫폼의 중재를 통해 데이터를 자율적으로 교환할 수 있도록 한다. 더욱이 데이터를 저장하는 IoT 시스템은 이 데이터를 다른 IoT 시스템과 교환한다(초연결 IoT). 이 자율 데이터 교환을 제어하려면 IoT 사용자와 더불어 IoT 네트워크 제공자가 자율 데이터 교환을 제어할 수 있도록 하는 시스템 메커니즘이 필요하다. 시스템 메커니즘은 서비스 개발자, IoT 사용자 및 IoT 네트워크 제공자를 대신하여 자율적으로 작업을 수행할 필요가 있다. 따라서 각 프로파일에서 그런 필요를 캡처해서 시스템 메커니즘이 이 프로파일을 자율적으로 해석해야 한다. 그런 프로파일을 가리켜 "자율 데이터 교환 제어 프로파일(ADECP)"이라고 한다. 이런 ADECP에는 교환할 수 있는 데이터와 해당 조건을 정의하는 데이터 교환 규칙이 포함되어야 한다. 또한 이 프로파일에는 프로파일 유효 기간과, 온라인 리포지토리에 대한 프로파일 유효성 검사의 필요 시기가 기술된 메타데이터도 포함되어야 한다. 이 프로파일은 필요충분한 통신 관리 기능을 제공해야 한다. 또한 식별된 상황과 컨텍스트에 따라 권한을 제어하는 융통성있는 데이터 액세스 제어 기능을 제공해야 한다. 예를 들어 대상 시스템의 데이터 사용 목적과 데이터 보안 수준을 고려할 수 있다. 마지막으로 이 프로파일은 자율 데이터 교환 중에 사용될 네트워킹 메커니즘(예: 암호화 데이터, 암호화 전송 계층, 가상 네트워크 슬라이싱 등)을 지정해야 한다.

IoT 플랫폼에서 ADECP 프로파일의 각 기능에 대해 시스템 메커니즘이 필요하다. 다음과 같은 시스템 메커니즘은 이미 정의되어 있을 수 있다.

- ADECP 프로파일의 관리(생성, 변경, 수명주기, 삭제)
- ADECP 프로파일의 감사(ADECP 프로파일의 효과를 모니터링해서 이 정보를 프로파일 작성자에게 제공하여 효과 파악)
- 장치, 엣지 컴퓨터 및 클라우드 서비스에 자율 정보 교환을 지시하는 제어 기능
- 자율 데이터 교환의 보안 설정을 시행하는 제어 기능
- 현재 상황 및 컨텍스트를 파악하고 변화하는 상황에 맞게 자율 데이터 교환 기능을 적용하는 정보 기능
- 네트워크 제어 기능

6.2.4 센서 융합 기술

센서 융합 기술은 서로 다른 다중 센서에서 취득된 데이터를 결합, 통합 및 연결하여 스마트 감지를 활성화함으로써 관찰된 사물, 상황 및 컨텍스트에 대한 보다 포괄적인 정보를 얻는다. 센서에는 이미지 또는 영상 센서, 음파 센서, 악취 센서, 촉각 센서 등이 있지만 데이터 소스는 물리적 센서로 제한되지 않는다. 스마트폰 및 모바일 장치에서 수집된 소셜 미디어 데이터와 통계적인 데이터는 "소셜" 센서의 데이터로 간주될 수 있다. 또한 네트워크 비콘도 도시에서 인간의 이동 및 네트워크 사용 정보를 기술하는 감지 정보를 제공할 수 있다. 센서 융합에서는 여러 센서 및 센서 유형을 사용하여 수집된 정보를 통해 보다 포괄적인 정보를 취득할 수 있다. 그러므로 미래 센서 융합에서는 센서 자원이 공유되어 여러 당사자에게 여러 목적으로 널리 사용될 것이다. 그러나, 미래 센서 융합을 사용하는 애플리케이션(예: 스마트 시티 애플리케이션 또는 공공 기관에서 사용하는 애플리케이션)의 핵심 기능은 무결성 및 권한 부여 기능이다.

정보 거버넌스(information governance)의 한 가지 예는 장치 무결성 및 권한 부여 기능을 모두 제공하는 것이다. 장치 무결성 기능은 다양한 기관에 의해 설치될 기기의 무결성을 보장하여 해당 기기에서 취득된 정보가 신뢰성이 갖도록 한다.

사용자는 알아야할 필요가 있는 경우에만 정보를 수신한다. 또한 권한 부여 기능은 다양한 기관이 필요한 정보에 액세스할 수 있도록 하면서 다차원 액세스 권한을 사용하여 정보를 보호한다. 다시 말해 특정 상황에서 협업하는 다양한 기관들에서 적정 사용자가, 적정 장소에서, 적정 시점에 "알아야할 필요"를 토대로 데이터 세트에 액세스할 수 있도록 각 보안 정책을 시행할 수 있다. 또한 기관 간 협업이 가능하도록 하는 것 외에, 스마트 시티의 비전을 실현하기 위한 군집 밀도 추산을 실시하기 위해 센서 융합 기법이 활용되어 왔으며 스마트 시티의 비전에서는 CO_2, 소음, 온도 및 습도 센서와 같은 물리적 센서를 사용하여 인간의 이동 및 환경 조건 간의 상관관계를 추출한다.

6.2.5 기계 학습

IoT는 전례없는 분량의 데이터를 생성하고 있다. 이 데이터는 수 없이 많은 시나리오와 사용 사례(예를 들어 보안이 필수적인 플랜트에서 위협 탐지 및 제4절에서 기술한 스마트 시티의 최적화된 자원 활용)에 필요한 정보를 제공한다. 과거에 그런 시나리오는 전문가의 경험이나 추정을 토대로 프로그래밍 규칙 기반 시스템을 통해 실현되었다. 본질적으로 수동 생성 인사이트에 의존한 반면, 시스템 관찰 및 액션 트리거는 자동화되었다. 그러나 미래 IoT 시스템의 역동성과, 서로 다른 기술 스택 수준에서 생성되는 데이터의 양은 인간이 필요한 옵저버 및 예측기 그리고 작동기를 명확히 프로그램 하는 데에 필요한 인사이트를 도출하지 못할 정도로 많다.

기계 학습은 컴퓨터가 명시적으로 프로그래밍하지 않고도 대량의 데이터로부터 학습할 수 있도록 지원한다. 생생되는 IoT 데이터 스트림을 지속적으로 모니터링하는 지능형 알고리즘은 시스템 상태 및 동작 패턴을 관찰하여 가장 확률이 높은 미래 시스템 상태를 예측하고 이런 인사이트를 잠재적으로 활용하여 원하는 미래 상태로 이끌기 위한 제안 또는 조치를 도출할 수 있다. 그러므로 기계 학습을 사용하면 이전에는 수동으로 생성되었던 인사이트를 자동으로 생성할 수 있으며 이는 복잡하고 데이터 집약적인 미래 IoT 사용 사례를 실현하는 데 필요하다.

궁극적으로 기계 학습은 현재의 자동화된 프로세스 및 서비스에 대한 논리적 확장인 자율 비즈니스로 이어져 단순히 인력을 대체하는 수준 이상의 효율성 및 생산성 향상을 가져올 수 있다[26]. 기계 학습에 의해 "사물"이 보다 지능화되므로 그런 사물에는 디지털 비즈니스 및 IoT 세상에서 구매 및 판매 기능도 추가될 것이다. 이는 수익, 효율성 및 고객관계 관리에 대한 새로운 기회를 제공하는 동시에 현명하고 윤리적으로 관리해야 하는 위험도 수반된다[27].

6.2.6 가상화

새로운 가상화 기술을 포함한 미래 IoT 플랫폼을 지원하기 위해 가상 머신에 운영 체제 및 비즈니스 로직으로 구성된 로직이 제공될 수 있다. 공장에서 생산되는 장치에는 하드웨어, 가상화 계층 및 관리 계층만 포함되어 있고 장치는 클라우드에 연결하여 특정 기능을 수행할 수 있는 비즈니스 로직을 다운로드할 수 있다. 판매된 장치에는 클라우드에 연결하는 로직만 포함되어 있기 때문에 장치 제조업체는 해당 장치의 최종 기능에 대한 정보가 없는 일반 장치를 제작할 수 있다. 이 장치가 기계에 연결되어 표준 인터페이스를 통해 기계 ID를 취득한다. 장치는 준비가 완료되어 연결 보고를 기다리고 있는 클라우드에 그 ID를 보고한다. 그러면 클라우드가 그 장치에 요구되는 소프트웨어 콘텐츠를 제공하며 장치는 해당 콘텐츠를 다운로드하고 가상 머신을 인스턴스화하여 작동 준비를 한다.

또한 이 관리 계층은 클라우드와의 안전한 비즈니스 콘텐츠 통신을 보장한다.

6.2.7 사용 사례에 대한 매핑

	산업				공공		소비자			
	BCM	Anom Detect	CSCM	Pred Maint	Smrt Cty	Soc Sens	Journ Exp	Conn Car	Ski	Smrt Fact
시스템 구성 및 동적 구성	•	•	•	•	•				•	•
데이터 맥락화	•	•	•	•	•	•	•		•	•
자율 데이터 교환	•	•	•	•	•	•	•		•	
센서 융합 기술	•	•	•	•	•	•			•	•
기계 학습	•	•	•	•	•	•	•	•	•	•
가상화				•	•			•	•	

6.3 메모리

최신 스트리밍, 인메모리 및 기타 스토리지 기술은 IoT에 대한 실시간 상호작용 및 낮거나 제로 수준의 지연시간 액세스를 지원하며 정보 저장 방식도 변화를 겪고 있다. 사물과 장치를 가상 표현하고 제품 자체에 데이터를 분산 저장하는 개념은 보다 큰 확장성을 지원하며 중앙에서 조율되지 않는 IoT 비즈니스 네트워크 또는 공급망의 설정이 용이하게 이루어지도록 한다.

6.3.1 디지털 제품 메모리

디지털 제품 메모리(DPM)는 개체가 자체 정보를 가지고 이 정보를 개체 간 및 개체 주변의 사물에 전달하는 IoT 비전을 다룬다. 이전에는 RFID 태그 또는 데이터 매트릭스 코드를 통해 상당한 용량의 데이터를 미리 저장하여 쉽게 액세스할 수 있었다. 미래 IoT 시스템에서는 의미론적 제품 메모리 기능이 구축되어 이 기술을 개선할 것이다.

이 개념은 의미론 기술, M2M 통신, 지능형 센서 네트워크, RFID 기술 및 다중 상호작용을 토대로 한다. 제품 메모리는 단거리 무선(예: Bluetooth, ZigBee, NFC)을 사용하여 제품 메모리 간 및 주변 환경 간에 통신을 주고 받을 수 있다. 의미론 기술은 지능형 환경에서 다양한 제품 메모리 간의 데이터 교환 및 제품 메모리와의 사용자 친화적 대화가 가능하도록 지원한다[28].

DPM의 의미론은 도메인 및 산업에 따라 달라지며 다양한 연구 프로젝트의 대상이다. 제조업의 경우 German Plattform Industrie 4.0의 Reference Architecture Model Industrie 4.0(RAMI 4.0)이 관리 셸 개념을 제공하며 이는 제품 마스터 데이터, 제품 출처, 수명주기, 적용 가능한 처리 방법 및 수행해야 할 작업의 의미론적 개념을 정의한다. 관리 셸은 RDF, RDF 스키마, OWL 등의 서로 다른 방식으로 구현할 수 있다 [29].

6.3.2 사용 사례

	산업				공공		소비자			
	BCM	Anom Detect	CSCM	Pred Maint	Smrt Cty	Soc Sens	Journ Exp	Conn Car	Ski	Smrt Fact
디지털 제품 메모리				•	•				•	

6.4 감지

지난 10년 동안 스마트폰이 방대한 범위의 센서를 통합하는 일종의 블랙홀이었으나 이제는 모바일이 이 환경에서 빠져나가고 있다. 센서는 스마트폰을 넘어 인체, 자동차, TV, 세탁기 및 기계는 물론 건물로까지 그 영역을 확장하고 있다[30].

6.4.1 초정밀 위치 기술

GPS는 4대 이상의 GPS 위성이 교신에 방해를 받지 않는 한 지구 위 어디에서든지 날씨와 관계없이 위치 및 시간 정보를 제공해주는 우주 기반 항법 시스템이다[31]. 이는 모바일 전화기에서 이미 표준화된 센서 기술의 한 가지 예이지만 웨어러블과 같은 새로운 부문의 시작이기도 하다.

GPS의 작동 기능은 1995년 7월 17일에 완전히 본궤도에 진입하여[32] 원래 설계 목표를 완수했다.

6.4.2 사용 사례

그러나 기술의 추가적인 발전과 기존 시스템에 대한 새로운 요구로 GPS 시스템을 개선하려는 노력이 펼쳐지고 있다. 2015년 초 현재 고품질 GPS 수신기는 3.5미터 이상의 수평 정밀도를 제공한다. GPS와 함께 증폭 장치를 사용하면 보다 높은 정밀도를 달성할 수 있다. 이 덕분에 몇 cm 내에서 실시간 위치 제어가 가능하며 mm 수준에서 임무 종료 후 측정이 가능하다[33].

GPS의 차세대 주요 개선 단계인 GPS IIIA는 2017년에 시작될 것이며 이 프로젝트를 통해 민간 및 군용 사용자 모두를 위한 추가 항법 신호와 함께 새로운 지상 기지국 및 위성이 추가된다. GPS IIIA는 레거시 컴퓨터와 통신 시스템을 네트워크 중심 아키텍처로 교체하여 보다 빈번하고 정밀한 위성 명령을 지원함으로써 모든 사용자를 위한 정밀도와 가용성 개선을 목적으로 한다[34].

	산업				공공		소비자			
	BCM	Anom Detect	CSCM	Pred Maint	Smrt Cty	Soc Sens	Journ Exp	Conn Car	Ski	Smrt Fact
초정밀 위치 기술					•		•	•	•	•

6.5 조치

IoT는 몇 가지 영역에서 사용자의 동작을 덜 요구하지만 중요한 결정 및 생성 프로세스는 항상 사람이 정해야 하기 때문에 대부분의 영역에서는 여전히 사용자의 상호작용이 핵심적일 것이다. 사용자가 최선의 결정을 내릴 수 있도록 하려면 IoT 시나리오에 있어 방대한 가용 데이터로부터 실질적이고 신뢰할 수 있는 정보를 추출하는 것에 그치지 않고 그 데이터를 쉽게 사용하도록 만들어 적정 세부 수준으로 집계하는 것이 중요하다.

디스플레이에서 일반적인 2-3차원 데이터 표현 이외에 증강 현실과 가상 현실이 더욱 중요해질 것이며 사용자가 신속하고 편리하게 처리할 수 있도록 데이터와 정보를 시각화하는 방법에 있어 새로운 접근 방법이 필요할 것이다.

6.5.1 증강 현실

증강 현실은 컴퓨터가 생성한 감각 입력(예: 영상, 그래픽 또는 GPS 데이터)에 의해 요소가 증강(또는 보강)되는 물리적 현실세계 환경의 실시간 직/간접 뷰이다. 증강 현실은 현실 뷰가 장치에 의해 수정(증강되기보다는 감소)되는 보다 일반적인 개념(매개 현실(mediated reality))과 연관이 있다. 따라서 이 기술은 인간의 현재 현실 인식을 향상시키는 방식으로 기능한다[35].

6.5.2 가상 현실

가상 현실은 현실(또는 상상) 세계에 자리잡고 있는 물리적 존재를 시뮬레이션하는 환경을 복제하여 사용자가 그런 세상과 상호작용하도록 지원한다. 가상 현실은 인공적으로 감각 경험을 생성하며 주로 시각에 중점을 두지만 청각과 촉각을 포함할 수 있다. 최신 가상 현실은 특수한 입체 디스플레이로 표시되며 일부 시뮬레이션은 추가적인 감각 정보를 포함하고

가상 현실 사용자를 대상으로 스피커나 헤드폰을 통한 실제 소리에 중점을 둔다. 이제 고급 촉각 시스템에는 일반적으로 의료, 게임 및 군용 애플리케이션에서 포스 피드백(force feedback)으로 알려진 촉각 정보가 포함된다. IoT 애플리케이션에 있어 몰입형 환경은 실물과 똑같은 경험을 생성하기 위해 현실세계와 유사해야 하며 이는 몰입형 컴퓨팅 역량과 구현 노력을 요구한다.

6.5.3 촉각 인터넷

다수의 미래 IoT 애플리케이션과 기능은 실현을 위해 극도로 낮은 지연시간을 요구할 것이다. 사용자 I/O 영역에서 가장 기대되는 발전 중 하나는 이른바 촉각 인터넷의 출현이다[36]. 촉각 인터넷이란 사용자 응답 시간의 실제 지연시간을 중심으로 극히 낮은 지연시간 I/O 대역폭을 통해 구현되는 인터페이스 및 실시간 상호작용을 지칭한다. 국제전기통신연합의 통신 표준화 부문(ITU-T)의 예측에 따르면 이런 실시간 인간 컨텍스트에서 작업을 수행하려면 “촉각 인터넷 애플리케이션에서 1밀리초의 엔드 투 엔드 지연시간이 필요하다”[37]. 이는 간단한 장치 및 IoT 시스템의 모든 부품에 적용되며 틀림없이 장치 및 플랫폼 수준에서의 지원이 필요할 것이다.

6.5.4 사용 사례에 대한 매핑

	산업				공공		소비자			
	BCM	Anom Detect	CSCM	Pred Maint	Smrt Cty	Soc Sens	Journ Exp	Conn Car	Ski	Smrt Fact
증강 현실				•	•		•		•	
가상 현실					•				•	
촉각 인터넷					•			•		•

6.6 보안

차세대 지원 기술은 전체 조직 간의 위협 분석 정보를 교환하기 위해 보안 및 신뢰성이 확보된 시스템 협업 기술을 제공한다. 동시에 센서 수준에서 융합 기술도 다중 데이터 소스의 IT 및 OT 데이터 통합을 지원한다. 위험도 평가 정보 처리를 위해 데이터 공학 기술이 포함된다.

장치 간 통신, 장치와 엣지 간 통신 또는 장치와 플랫폼 간 통신에서 보안 장치 식별 기술 및 차세대 암호화 기술(예: 임베드된 암호화)이 IoT 사용 사례에 대한 주요 지원 기술이다. 개인정보보호 향상 기술 및 차세대 암호화 기술(예: 검색 가능한 암호화)이 개인정보보호에 필요하다.

6.6.1 요소별 보안 기술

6.6.1.1 사물의 ID

폐쇄형 시스템에 있었던 장치가 IoT 시스템에 연결되면 IT 시스템에서 흔히 경험하는 사이버 공격의 목표물이 될 수 있다. 각 장치를 식별 가능하게 하는 장치 ID의 보안화는 해당 장치에 의해 생성된 데이터의 진본성 및 IoT 시스템에서 해당 데이터를 분석하여 취득한 결과의 신뢰성을 보장하는 데 있어 중요하다. 그러므로 사물 식별은 보안 IoT 실현의 주요 선결요건이 될 것이다. 인간의 생체 정보 인증이 갈수록 인간 사용자 인증 표준으로 자리잡는 것과 마찬가지로 미래에는 사물도 그럴 것이다. 물리적 복제 불가 기능(PUF)은 사물에 대한 생체 정보를 인증하는 수단이다. 암호화 키 및 ID는 복제가 불가능한 물질의 속성을 지니므로 비밀 키를 기반으로 하는 일반 암호화로 PUF를 사용할 수 있다. 키가 부품에 내장되어 있어 분리할 수 없다는 것이 차이점이다. 추가로 새로운 암호화 프로토콜은 양자 컴퓨터 시대의 보안 대안이 될 수 있는 PUF를 통해 구현될 수 있다.

IoT 시스템에 연결된 장치는 물리적 보안을 제공할 수 없는 환경에 위치할 수 있으므로 분해 또는 물리적 복제에 의한 공격을 받을 수 있다. 따라서 장치가 물리적으로 복제되더라도 장치 ID의 위조를 방지하는 기술(예: PUF 및 TPM(트러스트 플랫폼 모듈))과 함께 해당 기술의 운영 및 관리 기술이 중요하다. PUF는 결합된 부품(예: 카드 본체와 내장 칩으로 구성된 스마트 카드)을 식별할 수 있는 서로 다른 물질 조합을 통해 구성할 수도 있다.

부품들이 분리되면 부품의 ID 및 연관된 비밀 키와 함께 PUF가 파괴된다. 그런 기술을 토대로 다수의 컴포넌트로 이루어지는 복잡한 제품의 무결성을 검사할 수 있다.

PUF 정보가 센서 데이터(예: 워터마크)와 분리 불가능하게 결합되어 있으면 측정 소스부터 클라우드에 이르기까지 센서 데이터의 무결성을 보장할 수 있으므로 보안이 중요한 결정을 내릴 때 이런 데이터를 사용할 수 있다.

6.6.1.2 준동형 암호화

준동형 암호화 체계는 암호문에 대한 수학적 연산을 가능하게 한다. 이런 계산 결과는 복호화될 수 있으며 상응하는 일반 텍스트에 대해 실행되는 동일 연산의 결과와 일치할 것이다.

이는 가변성(malleability)이라고 하는 암호화 속성에 기인한다. 일반적으로 암호화 체계의 목적상 가변성은 바람직하지 않은 속성이다. 알고리즘이 이 속성을 가지면 공격자는 암호문을 관련된 일반 텍스트로 복호화되는 다른 암호문으로 변환할 수 있다. 준동형 암호화 체계일 경우 가변성은 수학적 계산의 결과가 다시 해독되도록 할 수 있다. 준동형 암호화는 Graig Gentry가 완전 준동형 체계를 처음으로 소개한 2009년에 널리 알려졌다. 그 전에도 준동형 속성의 암호화 체계가 이미 알려져 있었다. 그럼에도 불구하고 준동형 속성이 있다는 것은 특정 연산 하에서만 암호문이 가변적임을 의미한다. 예를 들어 ElGamal은 곱셈에서 준동형이 되는 암호화 체계이다. Gentry의 체계는 덧셈과 곱셈 모두에서 준동형이었던 최초의 체계였으며 그런 이유로 종종 완전 준동형 체계라고 불린다. 이 체계는 암호화 데이터에 대한 데이터 분석이나 검색 패턴 비표시 암호화 데이터 검색과 같은 광범위한 애플리케이션을 지원한다. 그러나 해당 애플리케이션에서 이 암호화 체계의 성능이 너무 낮았다. Gentry는 비트 연산당 30분 정도의 시간이 걸리는 것으로 보고했다.

완전 준동형 암호화에 대한 몇 가지 새로운 접근법이 아직 개발 중이며 보다 효율적인 체계는 아직 등장하지 않았다. 예를 들어 이른바 "약식 준동형 암호화"라고 하는 체계는 아직도 개발 중이다. 이런 체계에서는 암호문에 대해 어떤 종류의 연산은 무한히 허용하는 반면 다른 종류의 연산은 적은 수만 허용한다. 예를 들어 암호문에 대한 덧셈을 무한히 허용하는 반면 곱셈은 2회만 허용하는 체계가 있을 수 있다.

6.6.1.3 검색 가능 암호화

현재 개발 중인 암호화 도메인의 또 다른 새로운 접근법은 "검색 가능 암호화"이다. 이는 스토리지 제공자가 암호화된 데이터에서 키워드 또는 패턴을 검색할 수 있도록 지원하는 암호화 체계를 말한다. 제공자는 저장된 데이터를 복호화할 수 없으므로 키워드 검색을 수행할 수 있지만 기반이 되는 일반 텍스트의 어떤 정보도 얻지 못한다. 검색 가능 암호화와 관련하여 다음 3가지 개념이 주요 관심사항이다.

- **대칭적 검색 가능 암호화(SSE)**는 대칭적 암호를 바탕으로 한다. 데이터 소유자가 암호화 전에 데이터를 구성할 수 있도록 자신의 데이터를 암호화한다. 데이터 소유자는 관련 데이터에 효과적으로 액세스할 수 있는(예를 들어 키워드 검색이 가능한) 추가 데이터 구조을 포함시킬 수 있다. 이런 데이터를 준비하고 나면 데이터 소유자가 이를 비신뢰 서버에 업로드한다. 당연히 데이터 암호화에 사용된 비밀 키에 대한 액세스 권한이 있어야만 서버에 저장된 암호화 데이터를 검색할 수 있다. 이 접근법의 한 가지 단점은 서버에 쿼리를 제출하면 검색 패턴이 서버에 노출된다는 점이다.

- **비대칭적 검색 가능 암호화(ASE)** 또는 공개 키 검색 가능 암호화는 암호화된 데이터를 생성한 당사자가 아니어도 검색할 수 있다는 점에서 SSE와 차이가 있다. 그러므로 비수정 ASE인 SSE도 (암호화된 데이터가 저장된) 비신뢰 서버에 사용자의 쿼리가 노출되므로 SSE와 비교할 때 ASE는 더 많은 잠재적 시나리오를 지원한다.
- **단일 데이터베이스 개인 정보 검색(PIR)**은 사용자가 조회하는 사항(즉, 검색 쿼리)이 노출되지 않는 상태에서 서버에서 데이터를 검색하는 데 중점을 둔다. SSE 및 ASE와는 대조적으로 쿼리 대상 비신뢰 서버의 데이터가 암호화되지 않는다. 사용자의 쿼리를 숨기기 위해서는 해당 서버의 모든 데이터 항목을 취급해야 한다. 그러므로 PIR 체계는 데이터베이스 규모에 있어 선형인 작업을 요구하며 이는 본 접근법의 단점이다. 그러나 다중 쿼리 및 다중 사용자에 대한 비용을 분할 지불하는 장점이 있다.

미래 IoT 플랫폼에서 효율적으로 사용 가능한 준동형 또는 검색 가능 암호화 스키마를 제공하려면 추가 연구 및 개발 작업이 필요하다.

6.6.1.4 신뢰 구축

위에서 언급했듯이 현재의 신뢰 구축 아키텍처는 주로 공개 키로 신뢰를 구축하여 사용자에게 할당하는 데 중점을 둔다. 미래 IoT 시나리오는 추가로 트랜잭션 및 계약의 신뢰와 더불어 장치 및 플랫폼 무결성에서의 신뢰도 요구할 것이다.

6.6.1.4.1 플랫폼의 신뢰

IoT에서는 이전에 알려지지 않은 장치가 이전에 알려지지 않은 피어(peer)와 자연스럽게 상호 연결되며, 애플리케이션에 포함되기 위해 해당 피어와 신뢰를 구축해야 한다. 기술적으로 이는 플랫폼이 특정 보안을 갖추고 있는 신뢰 피어로 요약되므로, 피어들은 장치가 애플리케이션에 포함될 수 있는 범위, 해당 피어에 의해 제공되는 데이터의 신뢰성 및 해당 피어에 할당될 수 있는 컴퓨팅 작업을 자동으로 결정할 수 있다. 특정 유형의 공격에 대한 보호를 제공하는 보다 높은 신뢰 수준은 사용 기간 만료 후 중요 데이터 원격 삭제와 같은 미래 사용 제어 기술의 시행을 촉진하거나 신뢰 장치 제공 센서 데이터의 순위를 피어 데이터보다 높게 지정할 것이다. 일반적으로 원격 플랫폼에서 신뢰를 자동으로 구축하는 두 가지 접근법(즉, 하드웨어와 소프트웨어 원격 증명)이 존재한다. 하지만 두 가지 모두 현재 불완전하다. 하드웨어 원격 증명은 개념적으로 바람직하지만 저가 센서 하드웨어도 천문학적 비용이 들 수 있는 하드웨어 보안성 모듈(HSM) 또는 트러스트 플랫폼 모듈과 같은 특정 하드웨어 모듈로 인해 높은 비용이 발생한다. 또한 그런 하드웨어에 의한 추가 자원 소모는 대다수의 배터리 전원 공급 장치에 있어 부적합하다. 소프트웨어 원격 증명의 경우에는 개념적으로 전체적인 플랫폼에서 신뢰를 보증할 수 없지만 대부분의 애플리케이션에 대해 적정 보호 수준을 달성하는 실용적인 접근법이 존재할 수는 있다. 미래에는 코드 난독화, 화이트박스 암호, 제어 흐름 무결성, 기본 실행 환경에 애플리케이션을 복잡하게 뒤섞기 등의 기존 기술이 더욱 개발되고 통합되어 전체적인 소프트웨어 전용 원격 증명을 제공할 것이다.

6.6.1.4.2 트랜잭션 및 계약의 신뢰

특정 ID 및 플랫폼 구성을 통해 신뢰를 구축하는 것 이외에 미래 IoT 애플리케이션은 피어 간 트랜잭션 및 계약의 신뢰를 구축할 필요가 있으며 이를 제3자에게 입증할 수 있어야 할 것이다. 이 문제에 대응하는 기술로서 현재 부상하고 있는 한 가지는 블록체인 기반 프로토콜이다. 이 경우 트랜잭션은 중앙 신뢰 엔티티에 저장되지 않고, 공통 신뢰 원장에 대한 합의에 이른 여러 개의 동등한 피어에 고르게 분산된다(개별 공격자가 대다수의 정직한 클라이언트에 대해 악의적인 활동을 하기 어려움). 일반적인 블록체인의 변형들은 이보다 더 나아가서 과거 트랜잭션을 신뢰성 있는 방식으로 문서화하는 동시에 신뢰성 있는 컴퓨팅 작업 실행을 통합함으로써 스마트 계약(즉, 서비스 수준 협약, 액세스 제어, 보험에 대한 피어 간 자체 실행 계약)이 생성될 수 있도록 한다. 블록체인을 기반으로 하는 스마트 계약은 인간의 직접적인 개입이 배제된 장치 간 비즈니스 핵심 상호작용을 위한 선결요건이기 때문에 미래 IoT 신뢰 인프라의 주요 구성 블록 중 하나가 될 것이다.

그러나 비트코인, 네임코인, 이더리움 등의 현재 블록체인 기반 솔루션은 보안이 중요한 IoT 애플리케이션에 적합하려면 아직도 추가 연구 및 개발이 요구된다. 제한 없는 스토리지 요구사항, 네트워크에 연결하는 피어에 대한 대용량 데이터 전송, 신뢰성 있는 피어 투 피어 인프라가 네트워크를 좌우하는 몇 가지 중앙 엔티티로 변질, 검증되지 않은 보안 프로토콜 등은 모두 블록체인 기반 접근법의 현재 모멘텀을 뒤집을 잠재성을 갖고 있다. 한 가지 해법은 스토리지 및 대역폭이 제한된 IoT 애플리케이션에 대해 최적화된 블록체인 프로토콜들을 적절히 적용함으로써 특정 트랜잭션에 대해 검증된 보안성을 제공하는 것이다.

6.6.1.5 시스템 협업 기술

상호 의존적인 시스템 간의 공조 보안 대책을 활성화하는 사이버 위협 분석 기술은 보안 IoT 플랫폼을 실현하는 데 있어 필수적이다. 이 기술의 목적은 IoT 플랫폼에 포함된 상호 의존적인 각 시스템의 상황을 캡처하는 공통 작전 상황도(COP)를 제공하는 것이다. 이 기술은 각 조직의 상황을 나타내는 데 사용되는 표준화된 용어, 기계 판독 가능 정보 교환을 위한 메커니즘 및 서로 다른 조직의 정보에 대한 중앙집중화 프레젠테이션 및 관리를 제공한다. 이 기술은 각 시스템의 운영자가 시스템 장애, 사이버/테러리스트 공격 및 자연 재해와 같은 사건을 실시간에 가까운 방식으로 정확히 평가할 수 있도록 지원하여 해당 사건이 시스템이 미칠 영향을 평가하는 데 도움을 줄 것이다. 또한 이 기술은 서로 다른 시스템이 각 시스템에서 취득 및 관리하는 위협 분석 정보를 공유하여 현재와 미래 공격에 대한 보다 응집력 있는 지식 기반을 실현하도록 지원한다. 현재 관련 기술로는 OpenIOC(Open Indicators of Compromise), STIX(Structured Threat Information eXpression) 및 TAXII(Trusted Automated eXchange of Indicator Information)가 있다[38].

CMMI(기능 성숙 모델 통합) 및 IEC 62443에 의해 제공되는 것과 같은 성숙 모델은 공조 및 보안 IoT 플랫폼 실현에 있어 핵심적인 컴포넌트다. CMMI는 해당 플랫폼에 적용되는 보안 요구사항의 충족에 대해 시스템 및 운영자의 성과를 정의하는 성숙 수준을 제공한다. 이는 상호 의존적인 시스템의 보안 기능을 평가하는 표준화된 기준을 제공하여 이들 간의 보안 수준을 보장하기 때문에 상호 의존적인 시스템의 운영자에게 매우 중요하다.

6.6.2 서비스로서의 보안

미래 IoT 시스템의 보안 아키텍처 및 서비스에 대한 새로운 요구사항이 넘쳐나는 것을 걸림돌로 보는 것 아니라 오히려 미래 비즈니스 모델의 핵심으로 자리할 만한 촉망되는 기술적 지원 서비스의 개발 원동력으로 여겨야 한다. 두 가지 주요 연구 흐름(보안 모니터링 자동화와, 데이터 수집 방지에서 데이터 사용 제어로의 패러다임 전환)이 새로운 유형의 서비스들을 제공하는 기반이 될 것이다.

6.6.2.1 사용 제어를 통한 개인정보보호

미래 지원 기술로 볼 수 있는 한 가지 완화 방법은 데이터 사용 제어이다. 이 방법은 데이터 사용이 지속적인 프로세스이고 목적을 가지며 바이너리가 아니라는 점에서 일반적인 액세스 제어 개념의 확장이지만 데이터 관점과 연산 측면에서는 구분되어야 한다. 단일 시점에 주체의 데이터 자원 액세스를 단순히 규제만 하는 일반적인 액세스 제어에서는 이런 측면들을 다루지 않는다. 데이터가 다양한 시스템에 의해 처리되기 때문에 미래 데이터 사용 제어 기술은 데이터를 추적하고 레이블링하며, 대량 데이터 세트에 대한 개인정보보호 속성을 적용하기 위해 세부적인 사용 제한들을 정의하는 한편 이에 대한 학습 알고리즘 및 분석 실행을 지원한다. 한 가지 예는 개별 사용자의 익명성을 제거할 수 없는 특정 집계 수준에서 데이터 관점을 적용하는 것이다. 또 다른 예는 원시 데이터에 대한 액세스는 허용하지만 특정 데이터 세트의 조합을 불허하여 사용자의 개인 정보를 보호하거나 분석 결과에 영향을 주지 않고 개인 데이터에 작은 변화를 주는 것이다.

6.6.2.2 지속적인 보안 감사

IoT 시스템의 보안 수준에 대한 지속적인 추론을 위해서는 증거(즉, IoT 시스템의 관찰 가능한 정보)의 자동 수집 및 평가가 필요하다. 증거 수집 방식에 따라 테스트 기반 및 모니터링 기반 방법으로 구분할 수 있다. 테스트 기반 감사는 IoT 시스템에 대한 일부 입력을 제어하고 출력을 평가하여 증거를 수집한다. 예를 들어 컴포넌트 인터페이스를 호출하여 응답을 검사한다. 모니터링 기반 감사는 IoT 시스템의 운영 전개에 따라 생성된 로그 파일, 성능 지표 등의 증거를 분석한다.

IoT 시스템의 지속적 보안 감사를 위해 해결해야 할 몇 가지 과제가 있다. 첫째, 특정 시점에 특정 IoT 시스템을 구성하는 컴포넌트를 정하기 위해서 IoT 시스템 컴포넌트를 일관성 있게 정의하고 기술하는 방법이 필요하다. 더욱이 이런 서비스 내역은 이종 IoT 시스템 간에 교환되어 IoT 컴포넌트의 분산 검색을 지원해야 한다. 둘째, IoT 서비스 내역이 있으면 IoT 시스템의 실시간 보안 수준을 동적으로 평가할 수 있는 테스트 기반 및 모니터링 기반 방법을 개발해야 한다. 이런 감사 방법은 소형 장치에 대해 요구되는 가벼운 접근법인 최소 평가부터 플랫폼 및 엣지 컴포넌트의 포괄적 보안 평가에 이르기까지 여러 이종 IoT 컴포넌트를 평가할 수 있어야 한다.

6.6.3 ID 관리

최신 ID 및 액세스 관리(IAM) 시스템은 서로 다른 장치 및 시스템의 데이터를 보안 및 통합 관리할 수 있도록 지원한다. 미래 IoT 시스템에서는 서로 다른 엔티티 간의 자율 데이터 교환이 사용 제어나 신뢰 장치 ID와 같은 고급 보안 및 신뢰 관리 기술을 토대로 제어되어야 한다. 동시에 서로 다른 도메인의 애플리케이션은 격리가 필요하고 보안 경계 기술은 사건에 영향을 받는 하위 시스템의 격리를 보장할 필요가 있다.

6.6.3.1 IoT에 대한 IAM 기술

웹에서 최신 IAM 기술 스택은 SAML[39], OpenID-Connect OIDC) [40], OAuth 2.0[41] 및 SCIM[42]으로 구성된다. SAML이 다국적 기업 및 대학과 같은 대규모 조직에서 널리 알려져 있는 반면 OpenID-Connect는 나온 지 얼마 안 되었으나 이미 Google 및 Facebook과 같은 대규모 ID 제공업체의 웹 애플리케이션 및 서비스에서 인증을 위한 기술로 자리잡고 있다. SAML은 ID 연합 및 SSO 기능을 포함하여 다양한 IAM 요구를 다룬다. 그러나 이 프로토콜의 복잡성과 대부분의 소프트웨어 구현이 차지하는 면적이 IoT에 대한 유용성을 제한한다. OAuth 2.0과, 특히 제약이 있는 환경에 대응하여 현재 새롭게 등장한 ACE[43]와 같은 확장은 IoT 생태계에 잘 들어맞는다. 더욱이 OAuth 2.0 프로토콜은 CoAP[44] 및 MQTT[45]와 같은 제한적인 장치 프로토콜과 호환된다. 결과적으로 OAuth 2.0은 OT 부문[46]으로도 진출하고 있다. OAuth 2.0은 또한 확장성이 높아 사용 사례 중심 구성 및 사용이 가능하다. 개인 키 소유 증명 체계[47]와 같이 OAuth 2.0에 처음에 없었던 기능이 점차 추가되고 있다. 전통적이고 확립된 프로토콜 및 개념을 넘어 대체 접근법이 등장하고 있다. 예를 들어 IoT에 대한 블록체인 기반 접근법은 정책 강화, 장치 등록 및 책임 기능을 내장하였다. 그러나 그런 개념의 성공 가능성은 아직 의문의 여지가 남아 있다.

6.6.3.2 애플리케이션 격리 및 보안 경계 기술

소프트웨어 정의 경계(SDP)는 위험한 애플리케이션 인프라를 격리하고 네트워크 기반 공격으로부터 다른 애플리케이션 인프라를 보호하기 위해 동적으로 보안 경계를 구축하는 데 사용되는 기술이다. CSA(클라우드 보안 연합)는 SDP 연구를 위한 특별 실무 그룹을 설립했으며 이미 표준[48]을 발행했다. 이 실무 그룹은 더 나아가 IaaS용 SDP 연구에 착수하였다. 소프트웨어 정의 네트워크킹(SDN)을 사용하여 SDP 기능을 활성화함으로써 비승인 액세스 및 멀웨어에 대한 네트워크 수준 보안[49]을 달성할 수 있다. 이 시스템은 방화벽과 공조해서 이상 행동을 탐지하여 대상 하드웨어를 격리 및 차단하고 다른 하드웨어로 정상 실행을 계속하도록 통신 경로를 동적으로 재라우팅하는 적절한 네트워킹을 결정한다.

6.6.4 사용 사례에 대한 매핑

	산업				공공		소비자			
	BCM	Anom Detect	CSCM	Pred Maint	Smrt Cty	Soc Sens	Journ Exp	Conn Car	Ski	Smrt Fact
사물의 ID				•	•	•	•	•	•	•
준동형 암호화				•	•	•	•		•	
검색 가능 암호화					•	•	•		•	
신뢰 구축				•	•	•	•		•	
보안화 시스템 협업 기술	•	•	•	•	•	•	•	•	•	•
사용 제어를 통한 개인정보보호					•	•	•		•	
지속적인 보안 감사					•		•			
IoT용 IAM 기술	•	•	•	•	•	•	•	•	•	
애플리케이션 격리 및 보안 경계 기술	•	•	•	•	•			•	•	

제7절
표준

IoT 표준화 환경을 살펴보면 분명 사분오열된 시도와 중복된 계획들 밖에 없을 것이다. 그도 그럴 것이 웹 서비스, 클라우드 컴퓨팅 및 그 이전에 진행된 다수의 계획들이 그랬듯이 이 기술에 대한 과열 양상으로 볼 때 스마트 및 보안 IoT 플랫폼 달성에 있어 이런 분열은 방해가 된다.

7.1 환경

IoT를 둘러싼 표준화 현황에 대한 이해를 돕기 위해 현재 환경과 더불어 바람직한 환경 모두를 살펴볼 필요가 있다.

7.1.1 현재 IoT 표준화 환경

현재 환경에 대한 분석은 다음과 같은 주요 시사점을 제공한다.

7.1.1.1 주요 부정적 상황

- **이니셔티브** – IoT 스택의 모든 계층에서 수평 및 수직 공간 모두에 다수의 경쟁 표준 및 컨소시엄 이니셔티브가 존재한다. 이 문제에 대해 공식 확인된 수치는 없으나 한 IEC 회원에 따르면 50개 이상의 주요 표준화 이니셔티브가 해당 제품 유형에 직접적으로 영향을 주는 것으로 밝혀졌다고 한다.
- **요구사항** – 표준 개발 조직과 컨소시엄은 광범위하고 다양하며 일관성 없는 경쟁적인 요구사항이 난립하고 있는 상황에 직면해 있다. 이는 산업계의 치열한 경쟁으로 인해 빚어진 결과라는 점에서 이해할만 하다. 하지만 기술에 대한 투명성 결여가 상황을 더욱 복잡하게 만들고 있다. 표준화해야 할 것과 계속 경쟁이 필요한 것에 대한 명확한 합의가 부족한 실정이다. 설상가상으로 다양한 SDO 및 컨소시엄 자체 간의 경쟁이 문제를 더욱 가중시키고 있다.
- **데이터 소유권 및 개인정보보호** – 데이터 소유권과 개인정보보호를 둘러싼 문제도 상당하다. 모든 당사자(최종 사용자, 장치 또는 센서 소유자/제조업체, IoT 시스템 제공자 또는 이 시스템의 계약자, 플랫폼 제공자 등) 간에 의견충돌이 심하다.
- **정부** – 지역의 모든 관련 담당 기관에서 IoT 규제 책임 및 기회를 조사하고 있다. 대개의 경우 IoT 혁신에 부정적인 영향을 주거나 민간 부문 및 개인을 희생양 삼아 정부의 요구사항에만 지나치게 편협하게 중점을 두는, 비현실적이거나 제약이 심한 경계를 설정할 것이기 때문에 IoT에 불리할 것으로 예상된다.

7.1.1.2 주요 긍정적 상황

- **새로운 융합** – 요구사항과 결과물 조정을 둘러싸고 융합 움직임이 나타나고 있다. 산업 인터넷 컨소시엄(IIC), Industrie 4.0 이니셔티브, China 2025 및 OpenFog가 표준 대신 요구사항을 정의하고 있는 IoT 기관의 예이다. 이들은 모두 기존 표준의 수정 또는 새 표준의 개발을 위해 해당 SDO에 그런 요구사항을 제공하는 데 적극적이다.

이들은 공동 협력도 시작하고 있다. 이에 대한 모범 사례로는 각 참조 아키텍처를 협업적으로 결정하고 관계를 증대 및 확대할 다른 기회를 모색하고 있는 IIC 그룹과 I4.0 그룹 간의 새로운 관계, 일본 로봇 혁명 이니셔티브와 Industrie 4.0 간의 협업 계약 향상, 일본 경제 산업성(METI)과 독일 연방 경제 에너지부(BMWi) 간에 최근 서명한 협력 발전 협약 등이 있다.

- **새로운 분석** – 다수의 선두 SDO 및 컨소시엄은 IoT를 둘러싼 연구 및 분석에 적극적으로 참여하고 있으며 양질의 결과들이 나타나고 있다. 일부 모범적인 예로는 스마트 및 보안 IoT 플랫폼에 대한 본 IEC 백서, IIC IIRA & IIC 보안 프레임워크 문서, Industrie 4.0 RAMI, IoT에 대한 ISO/IEC JTC 1 WG 5 보고서, ISO/IEC JTC 1 WG 9 빅 데이터 및 WG 10 IoT의 작업 등이 있다.
- **당연한 선택** – 과열 양상이 진정됨에 따라 표준/컨소시엄 공간의 일부 축소가 가시화되고 있으며 실질적인 기여가 이루어져야 할 필요에 대한 현실 인식이 깊어지기 시작하고 있다. 그러나 이런 측면은 주기에 있어 여전히 초기 단계에 불과하며 풀어야 할 과제가 아직도 많다.

7.1.2 바람직한 미래 IoT 표준화 생태계 환경

앞의 절에서 살펴보았듯이 현재의 표준화 환경은 정부, 민간 부문 및 개인을 모두 지원하는 보다 긍정적인 표준화 생태계를 생성하기 위해 IoT 표준화 및 기회를 최적화해야 하는 과제를 던져주고 있다. 이 생태계는 아래 기술하는 것과 같은 SDO와 컨소시엄 범위에 걸쳐 함께 해야 할 협업 중 하나이다.

7.1.2.1 표준

본 분석의 목적상, 표준의 기치 아래 편견없이 공인 SDO의 다양한 결과물들을 함께 통합한다.

- **수평 표준화** – 국제 표준은 도메인 및 지정학적 경계를 넘는 표준 활동의 우선 접근법이 되어야 하며, 국제 수준에 부합하도록 정교하게 만들어진 기능 및 요구사항이어야 한다.
  - ISO, IEC, ITU 및 IEEE의 수평적 표준
  - IETF의 인터넷 표준
  - oneM2M의 수평적 공통 서비스 표준
  - Object Management Group의 모델링 표준
  - W3C의 웹 표준
- **수직 및 전문 표준** – 도메인 특정 또는 지정학적 표준은 관련 기구가 작성한 것이어야 한다. 가능한 한, 관련 기구는 보다 높은 수준의 수평 표준을 작성해야 한다.

7.1.2.2 표준에 대한 요구사항

주요 컨소시엄은 요구사항을 정의하여 그런 요구사항을 기존 표준 기구에 제공해야 한다. 위 표준 접근법과 유사한 2계층 접근법이 권장된다.

수평 기구들은 각 부문을 통솔하여 요구사항 및 피드백 공유를 위한 실무 연대 관계를 수립해야 한다. 이 부문의 예로는 IIC, OpenFog, AIOTI, AllSeen Alliance, OMA 및 NGMN가 있다.

수직 컨소시엄은 각 부문에 대한 요구사항을 정의하고 요구사항 및 피드백 공유를 위한 실무 연대 관계를 수립해야 한다. 이 부문의 예로는 Industrie 4.0, China 2025, AIOTI, Robot Revolution Initiative[50] 및 Industry Value Chain Initiative[51]가 있다.

7.1.2.3 제안된 역할 및 제한사항

정부	▪ 스마트 시티와 같은 공공 부문 IoT의 요구사항에 특별히 중점을 두어야 한다. ▪ 정부 상호 간 및 공개 표준 기구와 산업계 컨소시엄 간에 협력하여 요구사항을 공유해야 한다. ▪ 민간 부문과 공조하고 경쟁 기구 및 이니셔티브 간 공조 증진을 고무해야 한다. ▪ 표준을 직접 정의하거나 표준의 법적 사용을 지시하지 말아야 한다. ▪ 데이터 소유권, 데이터 관리 및 데이터 사용에 대한 지역 정책을 지시하지 말아야 한다.
민간 부문	▪ 국제 공개 표준의 개발 및 사용 극대화를 적극 권장해야 한다. ▪ 공공 부문과 함께 경쟁 표준 기구 및 컨소시엄 간 공조를 촉구해야 한다. ▪ 주요 표준 기구 및 컨소시엄을 중심으로 하나로 뭉쳐 협동해야 한다.
표준 기구 및 컨소시엄	▪ 최대한 다른 조직과의 모범적인 관계(예: IIC/I4.0 파트너십)를 본받아야 한다. ▪ 핵심 표준화 역량에 중점을 두고 단지 조직 생존이나 확장을 위한 표준 혹은 경쟁 표준을 개발하지 말아야 한다.

7. 2 표준 요구사항

제4, 5 및 6절에서 스마트 및 보안 IoT 플랫폼 실현에 필수적인 다수의 특정 표준화 요구사항을 살펴보았다. 다음 표는 그런 요구사항을 정리한 것이다.

연결성	▪ 5G – IoT 네트워크 기능 및 데이터 흐름의 극적인 증가는 5G의 조속한 완결을 좌우한다. 연구 노력과 시제품 배포가 꾸준히 지속되고 있지만 광범위한 배포를 통한 “표준”의 실현은 2020년까지도 어려울 것으로 예측된다. 소비자 수용까지 예상되는 지연 시간을 감안하면 IoT에 활용되기까지 너무 오래 기다려야 할 것이다. ▪ 차세대 위성 연결 – 네트워크 부하 및 지연시간 요구사항에 있어 예상되는 대폭적인 증가를 원활하게 지원하려면 새로운 전송 계층 프로토콜이 위성과 장치 간의 보다 높은 대역폭/요구 지연시간을 지원하는 표준이 요구된다. 6.1절에서 설명한 것과 같이 네트워크의 통신 장비 효율성은 향상된다. ITU-R가 2015년에 개최한 WRC(세계 무선 통신 회의)에서 항공기와 선박처럼 이동하는 지상 기지국의 위성 통신 시스템에 새로운 무선 주파수가 할당되었다. 이동하는 지상 기지국에 대한 무선 주파수 추가 할당은 2019년 WRC에서 논의할 예정이다. ▪ 융통성 – 시스템 복원성, 동적 구성 및 관련 기능에서는 사용 가능한 새로운 연결성 표준으로 업데이트되는 기능을 IoT 장비가 갖추도록 하는 표준을 생성해야 한다.
처리	▪ 장치, 엣지 및 플랫폼 수준에서 도메인 내 및 도메인 간에 데이터 맥락화 기술, 데이터 맥락화 표준 및 의미론 상호운용성 표준이 필요하다. 관련 표준의 개발은 다음 영역에 중점을 두어야 한다. – 정보 교환 모델 – 의미론 메타데이터 정의 표준 및 모델 – 데이터 교환 모델 및 인터페이스와 관련 표준 – 자율 데이터 교환 프로파일 및 교환 메커니즘 – 메타데이터 주석 모델 및 인터페이스 – 맥락화 정보 모델 – 메타데이터 컨텍스트 표준
메모리	▪ 디지털 제품 메모리의 표준화
감지	▪ 메타데이터 ▪ 초정밀 위치 기반 기술에 대한 추상적 개념 ▪ 센서 개인정보보호(최종 소비자/소비자의 옵트인/옵트아웃) ▪ 센서 융합 – 센서 관찰을 추상화하는 센서 메타 모델 개발 표준. 이 표준은 정형화되지 않은 산발적 데이터를 고급 도메인 지식으로 바꿀 수 있는 기반이 된다.
조치	▪ 제어 인터페이스 장치 그룹을 고유하게 식별하는 표준 템플릿 ▪ 시스템 간의 IoT 사용자 I/O를 일반화하는 일반 표준 ▪ 일반적인 인간/컴퓨터 I/O를 뛰어넘는 고급 IoT 서비스를 반영한 고유 IoT 접근성 요구사항

보안	▪ 소셜 시스템의 ID 연합 ▪ 가상 물리 공격 보호 ▪ 동시 연결을 갖는 다중 시스템에서의 장치 ID(예: W3C의 IRI) ▪ 플랫폼 무결성에서의 신뢰 구축을 위한 프로토콜 ▪ 상호 의존적인 시스템 간에 사이버 위협 분석을 교환할 수 있는 협업 보안 프레임워크 ▪ 상호 의존적인 시스템 간에 보안 기능을 평가할 수 있는 성숙 모델

7.2.1 사용 사례에 대한 매핑

		산업				공공		소비자			
		BCM	Anom Detect	CSCM	Pred Maint	Smrt Cty	Soc Sens	Journ Exp	Conn Car	Ski	Smrt Fact
연결성	5G 표준의 실현				•	•			•	•	•
	위성과 장치 간의 보다 높은 대역폭 요구 지연시간을 지원하는 새로운 전송 계층 프로토콜에 대한 표준					•				•	
	IoT 장비가 새로운 연결성 표준으로 업데이트되는 기능을 갖추도록 하는 표준				•	•			•	•	•
처리	정보 교환 모델	•	•	•	•	•	•	•	•	•	•
	의미론 메타데이터 정의 표준 및 모델	•	•	•	•	•	•	•	•	•	•
	데이터 교환 모델 및 인터페이스와 관련 표준	•	•	•	•	•	•	•	•	•	•
	자율 데이터 교환 프로파일 및 교환 메커니즘	•	•	•	•	•	•	•		•	
	메타데이터 주석 모델 및 인터페이스	•	•	•		•				•	
	맥락화 정보 모델	•	•	•	•	•	•	•	•	•	•
	메타데이터 컨텍스트 표준		•			•				•	•
메모리	디지털 제품 메모리의 표준화					•				•	

감지	메타데이터에 대한 표준	•	•	•	•	•	•	•	•	•	•
	초정밀 위치 기반 기술에 대한 추상화 표준					•		•		•	
	센서 개인정보보호 표준					•			•	•	
	센서 융합 표준	•	•	•	•	•				•	•
조치	제어 인터페이스 장치 그룹을 고유하게 식별하기 위한 표준 템플릿					•				•	
	시스템 간의 IoT 사용자 I/O를 일반화하는 일반 표준					•			•	•	
	고유한 IoT 접근성 요구사항에 대한 표준					•			•	•	•
보안	소셜 시스템의 ID 연합 표준	•	•	•		•	•	•		•	•
	가상 물리 공격 보호 표준	•	•	•	•	•	•	•			•
	동시 연결을 갖춘 다중 시스템에서 장치 ID에 대한 표준	•	•	•		•	•	•	•	•	•
	플랫폼 무결성의 신뢰를 구축하기 위한 표준 프로토콜	•	•	•	•	•	•	•	•	•	
	협업 보안 프레임워크	•	•	•		•	•	•		•	
	상호 의존적인 시스템 간에 보안 기능을 평가할 수 있는 성숙 모델	•	•	•		•	•	•		•	

제8절
권고사항

본 백서에 포함된 정보를 토대로 IoT를 발전시키고 스마트 및 보안 IoT 플랫폼 달성을 지원할 수 있는 기회가 많다.

8.1 일반 권고사항

IoT 정의, 개발, 배포 및 운영에 관련된 모든 SDO, 컨소시엄, 지정학적 엔티티 및 기타 주체는 공식적으로 7.1.2절에 기술된 바람직한 미래 IoT 표준화 생태계 환경을 지침으로 채택해야 한다.

또한 IoT 정의, 개발, 배포 및 운영에 관련된 모든 SDO, 컨소시엄, 지정학적 엔티티 및 기타 주체는 공조 및 협업의 수준 강화를 촉진하기 위한 기회를 모색해야 한다.

정부들은 제6절에서 명시한 다양한 기술 요구사항에 대한 제한없는 연구를 위해 재정 지원을 늘려야 한다.

ITU, IEEE 및 3GPP는 2018년까지 5G 개발 완료 및 배포 촉진을 이끌어야 한다.

정부와 민간 부문이 공조하여 상호 의존적인 시스템 간 사이버 위협 분석 교환, 미래 보안 강화 기회의 파악 및 잠재적으로 요구되는 표준화 활동 식별을 활성화하기 위한 합동 협업 보안 프레임워크를 만들어야 한다.

8.2 IEC 및 IEC 위원회에 대한 권고사항

세계 공인 법적 표준 기구 중 하나인 IEC는 IoT 발전을 촉진하고 스마트 및 보안 IoT 플랫폼 실현을 지원해야 할 본연의 임무를 맡고 있다. 그에 따라 IEC는 다음 조치를 취해야 한다.

- 공식적으로 7.1.2절에 기술된 바람직한 미래 IoT 표준화 생태계 환경을 지침으로 채택한다.
- 7.1.2절에 기술된 공인 선두 기관들과 공조하여 잘 알려진 SDO 및 컨소시엄, 유럽 공동체 등의 정부 기구, 개별 정부가 맡는 적정 역할을 규정하는 공식 MoU를 체결한다. 이 MoU에는 참가자들이 바람직한 환경을 조성하기 위해 최대한 공조하는 총괄 MoU 관리 이사회 설립이 포함되어야 한다.
- 제5, 6, 및 7절에 포함된 내용 및 권고사항을 검토하여 IEC 표준화 관리 이사회(SMB)가 구현해야 할 활동을 정한다.
- WG 9 및 WG 10과 공조하여 IoT 요구사항 및 표준을 개발할 책임을 ISO/IEC JTC 1 SC 32에 할당하도록 ISO/IEC JTC 1 대표에게 촉구한다.

  - 정보 교환 모델
  - 의미론 메타데이터 정의 표준 및 모델
  - 데이터 교환 모델 및 인터페이스와 관련 표준

- 메타 데이터 주석 모델 및 인터페이스
- 맥락화 정보 모델
- 메타데이터 컨텍스트 표준

- 제4, 5, 6 및 7절에서 명시한 보안 요구사항과 그에 따른 적정 계획 활동을 검토할 책임을 ISO/IEC JTC 1 SC 27에 할당하도록 ISO/IEC JTC 1 대표에게 촉구한다.
- 다음을 정의하여 자율 데이터 교환에 대한 표준화 활동을 시작할 책임을 적정 SC/WG에 할당하도록 ISO/IEC JTC 1 대표에게 촉구한다.

  - 자율 데이터 교환 프로파일(ADECP)을 제어하는 프로파일

  - ADECP를 관리 및 강화하는 시스템 메커니즘

  - IoT 장치, 엣지 장치 및 클라우드에서 ADECP를 강화하기 위해 요구되는 인터페이스와 메커니즘

- IEC 결과물에서 관계자들의 관심사를 반영하도록 정부 기구와 공조하여 참여 및 요구사항 식별 수준을 강화한다.
- 보다 큰 ITU-R 무선 주파수 할당을 지원한다.

부록A - 사용 사례

비즈니스 연속성 관리(BCM)

1. 사용 사례의 기술

1.1 사용 사례의 명칭

비즈니스 연속성 관리(BCM)

1.2 사용 사례의 범위 및 목적

1.2.1 범위

- 부문: 제조, 물류, 공급망관리
- 아키텍처 수준: IoT 플랫폼, 장치, 엣지, 클라우드.

1.2.2 목적

- 사건 정보 수집 및 공유를 통한 고급 위험도 평가
- 보안 대책의 자동 및 즉각 구현
- 사이버 위협에 대응한 최적의 생산 재계획

1.3 사용 경험담

1.3.1 사용 사례의 요약

- 감지: 현장 상태를 감지하여 데이터로 변환한다.

  - 다양한 보안 시스템으로부터 데이터를 IoT 플랫폼으로 수집한다.

  - 생산 제어 시스템으로부터 데이터를 IoT 플랫폼으로 수집한다.

- 사고: 데이터를 분석하고 조치 계획을 작성한다.

  - 위에서 수집된 데이터를 분석하여 위험도 분석을 수행한다.

  - 위에서 수집된 데이터를 분석하여 최적의 생산 계획을 다시 수립한다.

- 조치: 조치 계획을 구현한다.

  - 보안 대책을 구현한다.

  - 생산 계획을 구현한다.

1.3.2 본 사용 사례의 특성

- 서로 다른 시스템으로부터 통합되는 데이터를 분석하고 비즈니스 연속성 실현을 위한 조치 계획을 작성하기 위한 협업 보안 프레임워크
- 생산 활동에 대한 영향을 최소화하는 가운데 IoT 플랫폼이 필요한 보안 대책을 구현하는 대응 보안 프레임워크[52]

1.3.3 전체 기술

- IoT 플랫폼은 다양한 보안 시스템에서 사건 정보를 수집할 뿐만 아니라 생산 제어 시스템에서도 실제 및 계획 생산 데이터를 수집한다.
- IoT 플랫폼은 사건 정보를 분석하고 사건 위험도 분석을 수행한다. 또한 생산 활동에 대한 영향을 최소화하는 위험도 완화 계획과 같은 보안 대책도 마련한다.
- IoT 플랫폼은 통신선 단절 및 생산 라인 일시 중단과 같은 보안 대책을 구현한다.

- 한편, IoT 플랫폼은 생산 데이터를 분석하여 각 생산 현장에서 영향을 받는 제품 기능에 대응한 최적의 생산 계획을 작성한다[53].

1.4 사용 사례 도표

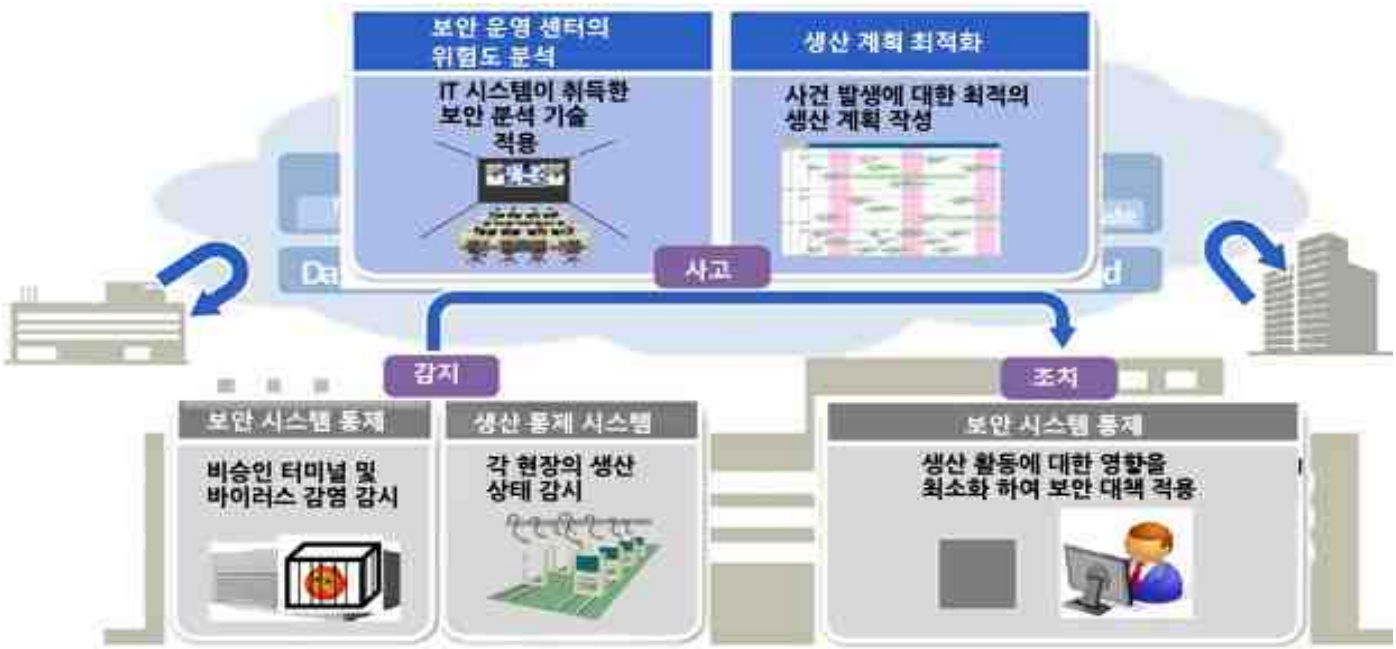


표 – 비즈니스 연속성 관리

1.5 사용 사례의 조건

1.5.1 전제

서로 다른 운영자가 운영하는 다중 시스템이 연관된다.

1.5.2 선결요건

없음

1.6사용 사례에 대한 추가 정보

1.6.1 최신 상태

- 현재 상태
  - 생산 제어 시스템의 준 실시간 데이터 수집 및 분석(일반적인 분석 주기는 월별임)
  - 생산 활동으로부터 독립적인 보안 대책 마련
- 최신 상태
  - 생산 활동에 대한 데이터 수집 및 실시간 분석을 통해 생산 활동에 대한 영향을 고려하는 다양한 보안 시스템의 사건 정보를 토대로 보안 대책 마련
- 보안 시스템 및 생산 제어 시스템의 데이터를 통합하기 위해 현재 상태를 최신 상태 기술/표준으로 전환하는 것이 필요하다.

1.6.2 다른 관련 사용 사례(하위 및 상위 사용 사례 포함)

협업 SCM 사용 사례는 다중 시스템의 데이터 통합에 중점을 두고 있기 때문에 본 사용 사례와 관련이 있다.

2. 특징적 기능에 대한 매핑

2.1 연결성

기능		비고
실시간 상황 처리	X	실시간 감지수행 포함
다중 시스템 연결성	X	여러 시스템에 연결
원격 기능	X	제품 외부에 상주하는 기능
모든 대역폭/프로토콜에 대한 적용성		제공 대역폭/프로토콜에 맞춰 재구성 → HW에서 SW로 전환
새로운 연결성 표준으로 업그레이드 가능성	X	SW를 통해 새로운 연결성 표준으로 업그레이드할 수 있는 기능
합법적 감청 기능		
원격 액세스	X	
인증 및 액세스 제어	X	
신뢰성 및 무결성	X	

2.2 처리

기능		비고
온보드 분석	X	
오프보드 분석	X	
기계 학습	X	
맥락화	X	
익명화		
정보 매시업	X	
의미론 상호 운용성	X	
장치의 동적 구성	X	자가 치유/복원성을 위한 장치의 동적 구성
동적 구성가능성		변경 요구사항에 따라 장치가 자체적으로 또는 시스템을 통해 동적으로 구성 가능해질 필요
데이터 소유권 추적		
집단 인지		

2.3 메모리

기능		비고
디지털 제품 메모리		전체 수명주기, 제품 내력
패턴 인지	X	인공 지능/기계 학습 기반
기능 데이터	X	분석용

2.4 감지

기능		비고
감지 기능을 갖춘 장치 수 증가에 대응	X	
감지 데이터의 중재 교환	X	
데이터의 신뢰성	X	
원시 데이터의 정리	X	
초정밀 위치 기반 기능		
개인정보보호		
데이터의 무결성	X	
인증을 요하는 복잡한 센서	X	
센서 재구성 기능		

2.5 작업

제어 인터페이스 장치

기능		비고
교정		
장치 그룹의 제어		런타임 및 구성
장치의 동적 구성		동적 장치 온보딩/그룹에 지정
컨텍스트에 따라 장치가 제어되는 방식 적용		
안전성 요구사항	X	
인증 및 액세스 제어 및 권한 부여	X	
플로어 제어	X	시스템을 실제로 제어하도록 허락된 사람들과 그 인계 메커니즘
집단/자체 최적화 제어 지능 보안의 집단 제어		
컨텍스트 인지 제어		

사용자 I/O

기능		비고
촉각 인터페이스		
다중 장치 사용자 인터페이스		
가상 모델링		
시뮬레이션	X	
접근성		장애인용
증강 현실		예: 안경
사용성 및 사용자 경험	X	

2.6 보안성

기능		비고
엔드 투 엔드 정책 관리	X	모든 정책 통합
가용 물리적 자원 및 보안성에 대해 최적화된 프레임워크	X	가용 물리적 자원/보안 강건성에 대해 최적화된 프레임워크(ISO 27001에서는 계획-실천-확인-조치) ISO 27001)
복원성	X	가상 물리 공격 포함
장애 허용 능력	X	가상 물리 공격 포함
시스템 위협 탐지 및 대응	X	OODA 관찰-방향설정-결정-실행
장치의 모니터링	X	
협조 및 위협 분석	X	
ID 관리	X	연합 ID 관리, 시스템 간 ID 상관관계, …
장치의 ID 보안	X	
인증 관리	X	데이터의 책임/부인 방지
이상 탐지	X	

3. 차세대 지원 기술

	차세대 지원 기술		비고
연결성	차세대 위성 연결을 위한 전송 계층 프로토콜		보다 높은 대역폭, 높은 지연시간
	5세대 셀룰러 액세스(5G)		
	저전력 무선 액세스(LPWAN)		
처리	시스템 구성 및 동적 구성	X	
	데이터 맥락화	X	
	자율 데이터 교환	X	
	센서 융합 기술	X	
	기계 학습	X	
	가상화		
메모리	디지털 제품 메모리		
감지	초정밀 위치 기술		
조치	증강 현실		
	가상 현실		
	촉각 인터넷		
보안	사물의 ID		
	준동형 암호화		
	검색 가능 암호화		
	신뢰 구축		
	보안화 시스템 협업 기술	X	
	사용 제어를 통한 개인정보보호		
	지속적인 보안 감사		
	IoT용 IAM 기술	X	ID 및 액세스 관리
	애플리케이션 격리 및 보안 경계 기술	X	

4. 필요한 미래 표준

	표준 요구사항		비고
연결성	5G 표준의 실현		
	위성과 장치 간의 보다 높은 대역폭/요구 지연시간을 지원하기 위한 새로운 전송 계층 프로토콜에 대한 표준		
	IoT 장비가 새로운 연결성 표준으로 업데이트하는 기능을 갖추도록 하는 표준		
프로세싱	정보 교환 모델	X	
	의미론 메타데이터 정의 표준 및 모델	X	
	데이터 교환 모델 및 인터페이스와 관련 표준	X	
	자율 데이터 교환 프로파일 및 교환 메커니즘	X	
	메타데이터 주석 모델 및 인터페이스	X	
	맥락화 정보 모델	X	
	메타데이터 컨텍스트 표준		
메모리	디지털 제품 메모리의 표준화		
감지	메타데이터에 대한 표준	X	
	초정밀 위치 기반 기술에 대한 추상화 표준		
	센서 개인정보보호 표준		개인정보보호(최종 소비자/소비자의 옵트인/옵트아웃)
	센서 융합 표준	X	센서 관찰을 추상화하는 센서 메타 모델 개발 표준. 이 표준은 정형화되지 않은 산발적 데이터를 고급 도메인 지식으로 바꿀 수 있는 기반이 된다.
조치	제어 인터페이스 장치 그룹 고유 식별 표준 템플릿		
	시스템 간의 IoT 사용자 I/O를 일반화하는 일반 표준		
	고유한 IoT 접근성 요구사항에 대한 표준		일반적인 인간/컴퓨터 I/O를 뛰어넘는 고급 IoT 서비스 반영

	표준 요구사항		비고
허브	소셜 시스템의 ID 연합 표준	X	
	가상 물리 공격 보호 표준	X	
	동시 연결을 갖춘 다중 시스템에서 장치 ID에 대한 표준	X	예: W3C의 국제화 자원 식별자(IRI)
	플랫폼 무결성의 신뢰를 구축하기 위한 표준 프로토콜	X	
	협업 보안 프레임워크	X	상호 의존적인 시스템 간의 사이버 위협 분석 교환 활성화
	상호 의존적인 시스템 간에 보안 기능을 평가할 수 있는 성숙 모델	X	

부록 B – 사용 사례

고급 유지보수 서비스용 이상 탐지 시스템

1. 사용 사례의 기술

1.1 사용 사례의 명칭

고급 유지보수 서비스용 이상 탐지 시스템[54]

1.2 사용 사례의 범위 및 목적

1.2.1 범위

- 부문: 제조 부문의 유지보수 등
- 아키텍처 수준: IoT 플랫폼, 장치, 엣지, 클라우드.

1.2.2 목적

- 이전에 전문 지식을 갖춘 엔지니어를 요구했던 장비 상태 진단의 자동화를 활성화한다.
- 예상치 못한 생산 시설 중단으로 인한 손실 방지 및 정밀도가 높은 이상 탐지를 통해 가용성을 개선한다.
- 장비 상태에 적합한 유지보수를 수행하여 유지보수 관리 시간 및 비용을 절감한다.

1.3 사용 경험담

1.3.1 사용 사례의 요약

이상 탐지 시스템(압축 가스 엔지 발전기에 적용)이 온도, 압력 및 엔지 속도와 같은 매개변수에 대해 수십 개의 센서로부터 데이터를 자동으로 수집한다.

이 시스템은 데이터를 데이터베이스에 저장하고 원격 모니터링 기능 및 데이터 마이닝 기능을 사용하여 자동으로 진단을 수행한다. 진단 결과는 장비 각각에 대한 상태를 색상으로 구분 표시한 목록 화면을 사용하여 유지보수 서비스 인력에게 제공할 수 있다.

1.3.2 사용 사례의 특성

- 데이터 마이닝 기술을 사용하여 빅 데이터로부터 유의한 정보를 추출하여 이상 하드웨어 상태의 변경에 대한 고급 정보를 제공하도록 설계되었다.
- 수십 개의 센서로부터 데이터를 자동으로 수집한다.
- 원격 모니터링 기능과 데이터 마이닝 기능을 사용하여 진단 프로세스를 자동으로 수행한다.
- 장비 각각에 대한 상태를 색상으로 구분 표시한 목록 화면을 사용하여 진단 결과를 표시한다.

1.3.3 전체 기술

- 압축 가스 엔진 발전기에 적용되는 이상 탐지 시스템의 예는 다음과 같다.
- 이 이상 탐지 시스템은 온도, 압력 및 엔지 속도와 같은 매개변수에 대해 수십 개의 센서로부터 데이터를 데이터베이스에

저장하고 원격 모니터링 기능 및 데이터 마이닝 기능을 사용하여 자동으로 진단을 수행한다. 진단 결과는 장비 각각에 대한 상태를 색상으로 구분 표시한 목록 화면을 사용하여 유지보수 서비스 인력에게 제공할 수 있다(1.4 참조).

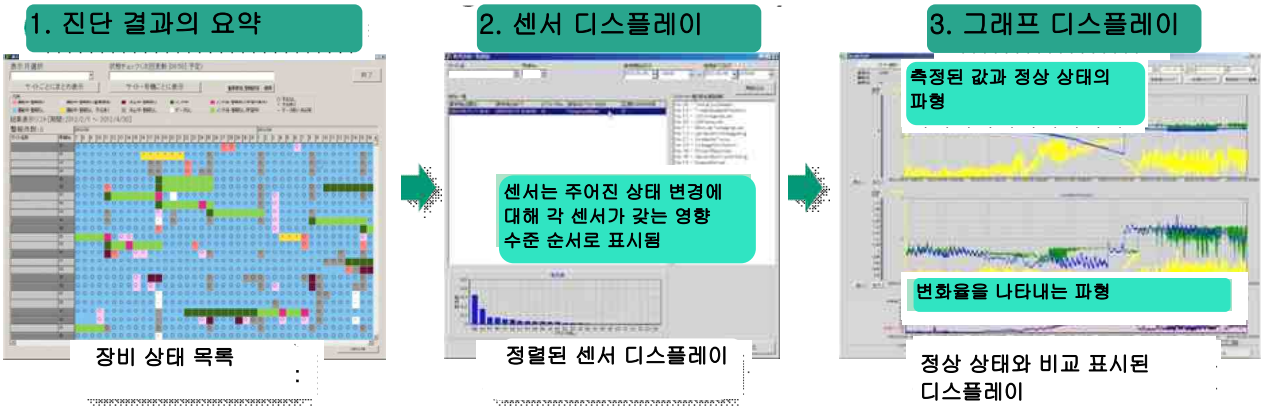
- 원격 모니터링 기능은 운영자 경험 및 지식을 토대로 장비로부터 수집된 각 센서 신호에 대한 상한/하한 값 및 변화율 평가 기준이 설정되고 난 뒤 상태 변경을 탐지하는 물리적 기반 진단 기능이다. 평가는 각 센서에 대한 이상 탐지 한도 값을 설정하여 구현된다. 각 센서 신호에 단일 평가 한도 값이 있어서 발생하는 오류 및 장애를 쉽게 설명할 수 있으나 다중 센서 신호와 관련된 경우에는 상태 변경 탐지가 어려워진다. 장비 설치 환경에 계절적 변화나 차이가 있으면 각 변화 여건에 따른 별도의 설정이 필요하다. 서로 다른 장애 유형이 다수이고 각 유형의 발생 빈도가 서로 다를 경우 항상 최적의 설정값을 결정하는 게 어려울 수 있다. 또 다른 문제는 동일 유형의 장애 중에도 장애로 이어진 프로세스나 장애 원인이 각기 다를 수 있어서 각 장애 유형에 대해 단일 설정값을 정하는 것이 불가능할 수 있다는 점이다.
- 데이터 마이닝 기능은 정상적인 상태 데이터로 통계적인 참조점을 습득하도록 훈련되는 예제 기반 진단 기능이다. 이 기능은 통계적인 데이터 공간에서의 측정 지점과 참조점 간 거리를 기반으로 장비 상태 변경을 탐지한다. 데이터 마이닝 기능은 원격 모니터링 기능보다 민감도가 높으므로 상태 변경의 조기 탐지를 지원할 수 있다.

그러나 기존 데이터 마이닝 기능의 단점은 진단 결과가 복잡한 센서 신호 상관관계로부터 도출될 때 원인이 무엇인지 설명하기가 어렵다는 것이다. 이 시스템은 탐지된 상태 변경에 상응하는 정렬된 센서 신호 목록을 출력하여 상태 모니터링과 원인 분석을 지원하도록 설계되었다.

- 이상 탐지 시스템은 장비로부터 센서 신호 데이터를 수신하는 데이터 수집 장치(기존 데이터 수집 메커니즘 사용 가능), 수집된 데이터를 저장하는 데이터 저장 장치, 저장된 데이터를 분석하는 진단 처리 장치 및 분석 결과를 출력하는 디스플레이 장치로 구성된다(1.4 참조). 위의 각 기능은 애플리케이션에 따라 IoT 플랫폼의 적정 위치에 자리한다.
- 이상 탐지 알고리즘으로 사용되는 데이터 마이닝 기술(진단 엔진)은 정상 상태 센서 데이터에 대한 기계 학습을 수행하여 모니터링 대상 데이터 간의 차이에 대한 지표를 만들고 정상 데이터 그룹을 습득하며, 결과가 정상 데이터와 동일하여 정상인지 또는 정상 데이터와 다른 이상인지 여부를 평가한다.
- 진단 엔진은 비매개변수 방법이며 센서 데이터에 대한 통계적인 제약에 내성이 있다. 모델 없이 알고리즘을 사용할 수 있으면 장치나 시스템 운영 상태에 중대한 변경이 있을 때에도 모델을 구축할 필요 없이 또는 각 상태 변경에 대한 시뮬레이션 없이 융통성 있게 대응할 수 있다.
- 모니터링할 장치 또는 시스템에 따라 또는 탐지할 비정상 상태의 특성에 따라 개별적으로 각 진단 엔진을 사용하여 최적의 시스템 구성을 생성할 수 있다.

1.4 사용 사례의 도표

● 진단 결과 디스플레이로부터 상태 점검



●이상 탐지 시스템의 운영

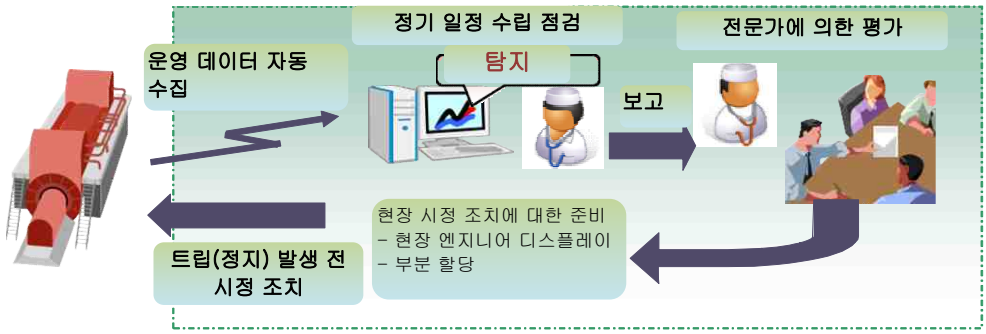


그림 B-1 | 사용 사례 도표 – 고급 유지보수 서비스용 이상 탐지 시스템

1.5 사용 사례의 조건

1.5.1 전제

대용량의 운영 레코드 데이터와 센터 데이터를 수집 및 저장할 수 있다.

1.5.2 선결요건

없음

1.6 사용 사례에 대한 추가 정보

1.6.1 최신 상태

- 현재 상태
  - 국
    가 전체에 걸쳐 압축 가스 엔진 발전기의 원격 모니터링 실시
  - 제한된 수의 모니터링 대상에 시스템 적용
  - 몇십 초 주기로 측정되는 몇십 개의 서로 다른 센서 신호 일일 진단 실시
- 최신 상태
  - 세계 전체에 걸쳐 압축 가스 엔진 발전기의 원격 모터링 수행
  - 다양한 유형의 장비에 대한 원격 모니터링 수행
  - 방대한 수의 장비에 시스템 적용

- 더 적은 초 단위 주기로 측정되는 더 많은 서로 다른 센서 신호의 실시간 진단 수행
- 탐지뿐만 아니라 다양 기타 목적으로 저장된 데이터 분석

- 현재 상태에서 최신 상태로 전환하려면 IoT 플랫폼 전체에 걸쳐 기능을 개선하기 위한 기술 /표준이 필요하다.

1.6.2 다른 관련 사용 사례(하위 및 상위 사용 사례 포함)

예측 유지보수와 서비스 사용 사례는 이 사용 사례와 관련이 있다.

2. 특징적 기능에 대한 매핑

2.1 연결성

기능		비고
실시간 상황 처리	X	실시간 감지수행 포함
다중 시스템 연결성	X	여러 시스템에 연결
원격 기능	X	제품 외부에 상주하는 기능
모든 대역폭/프로토콜에 대한 적용성		제공 대역폭/프로토콜에 맞춰 재구성 → HW에서 SW로 전환
새로운 연결성 표준으로 업그레이드 가능성		SW를 통해 새로운 연결성 표준으로 업그레이드할 수 있는 기능
합법적 감청 기능		
원격 액세스	X	
인증 및 액세스 제어	X	
신뢰성 및 무결성	X	

2.2 프로세싱

기능		비고
온보드 분석	X	
오프보드 분석	X	
기계 학습	X	
맥락화	X	
익명화		
정보 매시업	X	
의미론 상호 운용성	X	
장치의 동적 구성	X	자가 치유/복원성을 위한 장치의 동적 구성

기능		비고
동적 구성가능성		변경 요구사항에 따라 장치가 자체적으로 또는 시스템을 통해 동적으로 구성 가능해질 필요
데이터 소유권 추적	X	
집단 인지	X	

2.3 메모리

기능		비고
디지털 제품 메모리	X	전체 수명주기, 제품 내력
패턴 인지	X	인공 지능/기계 학습 기반
기능 데이터	X	분석용

2.4 감지

기능		비고
감지 기능을 갖춘 장치 수 증가에 대응	X	
감지 데이터의 중재 교환	X	
데이터의 신뢰성	X	
원시 데이터의 정리	X	
초정밀 위치 기반 기능	X	
개인정보보호		
데이터의 무결성	X	
인증을 요하는 복잡한 센서	X	
센서 재구성 기능		

2.5 작업

제어 인터페이스 장치

기능		비고
교정	X	
장치 그룹의 제어	X	런타임 및 구성
장치의 동적 구성	X	동적 장치 온보딩/그룹에 지정
컨텍스트에 따라 장치가 제어되는 방식 적용	X	
안전성 요구사항		

기능		비고
인증 및 액세스 제어 및 인증	X	
플로어 제어	X	시스템을 실제로 제어하도록 허락된 사람들과 그 인계 메커니즘
집단/자체 최적화 제어 지능	X	
보안의 집단 제어	X	
컨텍스트 인지 제어	X	

사용자 I/O

기능		비고
촉각 인터페이스	X	
다중 장치 사용자 인터페이스	X	
가상 모델링	X	
시뮬레이션	X	
접근성	X	장애인용
증강 현실		예: 안경
사용성 및 사용자 경험	X	

2.6 보안성

기능		비고
엔드 투 엔드 정책 관리	X	모든 정책 통합
가용 물리적 자원 및 보안성에 대해 최적화된 프레임워크	X	가용 물리적 자원/보안 강건성에 대해 최적화된 프레임워크(ISO 27001에서는 계획-실천-확인-조치) ISO 27001)
복원성	X	가상 물리 공격 포함
장애 허용 능력	X	가상 물리 공격 포함
시스템 위협 탐지 및 대응	X	OODA 관찰-방향설정-결정-실행
장치의 모니터링	X	
협조 및 위협 분석	X	
ID 관리	X	연합 ID 관리, 시스템 간 ID 상관관계…
장치의 ID 보안		
인증 관리	X	데이터의 책임/부인 방지
이상 탐지	X	

3. 차세대 지원 기술

	차세대 지원 기술		비고
연결성	차세대 위성 연결을 위한 전송 계층 프로토콜		보다 높은 대역폭, 높은 지연시간
	5세대 셀룰러 액세스(5G)		
	저전력 무선 액세스(LPWAN)		
처리	시스템 구성 및 동적 구성	X	
	데이터 맥락화	X	
	자율 데이터 교환	X	
	센서 융합 기술	X	
	기계 학습	X	
	가상화		
메모리	디지털 제품 메모리		
감지	초정밀 위치 기술		
조치	증강 현실		
	가상 현실		
	촉각 인터넷		
보안	사물의 ID		
	준동형 암호화		
	검색 가능 암호화		
	신뢰 구축		
	보안화 시스템 협업 기술	X	
	사용 제어를 통한 개인정보보호		
	지속적인 보안 감사		
	IoT용 IAM 기술	X	ID 및 액세스 관리
	애플리케이션 격리 및 보안 경계 기술	X	

4. 필요한 미래 기술

	표준 요구사항		비고
연결성	5G 표준의 실현		
	표준 위성과 장치 간의 보다 높은 대역폭/요구 지연시간을 지원하기 위한 새로운 전송 계층 프로토콜에 대한 표준		
	IoT 장비가 새로운 연결성 표준으로 업데이트하는 기능을 갖추도록 하는 표준		
프로세싱	정보 교환 모델	X	
	의미론 메타데이터 정의 표준 및 모델	X	
	데이터 교환 모델 및 인터페이스와 관련 표준	X	
	자율 데이터 교환 프로파일 및 교환 메커니즘	X	
	메타데이터 주석 모델 및 인터페이스	X	
	맥락화 정보 모델	X	
	메타데이터 컨텍스트 표준	X	
메모리	디지털 제품 메모리의 표준화		
감지	메타데이터에 대한 표준	X	
	초정밀 위치 기반 기술에 대한 추상화 표준		
	센서 개인정보보호 표준		최종 소비자/소비자의 옵트인/옵트아웃)
	센서 융합 표준	X	센서 관찰을 추상화하는 센서 메타 모델 개발 표준. 이 표준은 정형화되지 않은 산발적 데이터를 고급 도메인 지식으로 바꿀 수 있는 기반이 된다.
조치	제어 인터페이스 장치 그룹을 고유하게 식별하는 표준 템플릿		
	시스템 간의 IoT 사용자 I/O를 일반화하는 일반 표준		
	고유한 IoT 접근성 요구사항에 대한 표준		일반적인 인간/컴퓨터 I/O를 뛰어넘는 고급 IoT 서비스 반영

	표준 요구사항		비고
허브	소셜 시스템의 ID 연합 표준	X	
	가상 물리 공격 보호 표준	X	
	동시 연결을 갖춘 다중 시스템에서 장치 ID에 대한 표준	X	예: W3C의 국제화 자원 식별자(IRI)
	플랫폼 무결성의 신뢰를 구축하기 위한 표준 프로토콜	X	
	협업 보안 프레임워크	X	상호 의존적인 시스템 간의 사이버 위협 분석 교환 활성화
	상호 의존적인 시스템 간에 보안 기능을 평가할 수 있는 성숙 모델	X	

부록 C – 사용 사례

협업 공급망관리(SCM)

1. 사용 사례의 기술

1.1 사용 사례의 명칭

협업 공급망관리(SCM)

1.2 사용 사례의 범위 및 목적

1.2.1 범위

- 부문: 제조, 물류, 공급망관리
- 아키텍처 수준: IoT 플랫폼, 엣지, 클라우드.

1.2.2 목적

- 기지 관리 및 최적의 물류 계획 수립
- 기지 배치 최적화
- 전세계 공급 및 수요 조정

1.3 사용 경험담

1.3.1 사용 사례의 요약

- 감지: 현장 상태를 감지하여 데이터로 변환
  - PSI(제품, 판매, 재고) 시스템으로부터 IoT 플랫폼으로 데이터를 수집한다.
  - 제품 제어 시스템으로부터 IoT 플랫폼으로 데이터를 수집한다.
- 사고: 데이터를 분석하고 조치 계획을 작성한다.
  - 위에서 수집된 데이터를 분석하여 기지 관리 및 최적의 물류 계획을 작성한다.
  - 위에서 수집된 데이터를 분석하여 기지 배치 최적화 계획을 작성한다.
- 조치: 조치 계획을 구현한다.
  - IoT 플랫폼에서 작성하여 전세계 공급 및 수요 조정 계획을 구현한다.

1.3.2 사용 사례의 특성

- IoT 플랫폼이 서로 다른 시스템에서 통합된 데이터를 분석하여 다양한 유형의 전례없는 혜택/애플리케이션을 실현하기 위한 조치 계획을 작성한다.
- 독립부문 밖으로 확장[52]

1.3.3 전체 기술

- IoT 플랫폼이 전세계 PSI를 시각화하는 PSI 관리 시스템으로부터 실제 및 예상 PSI(제품, 판매, 재고) 데이터를 감지하고 생산 진행을 시각화하는 생산 제어 시스템으로부터 실제 및 계획 생산 데이터를 감지하여 최선의 생산 계획을 수립한다[55].
- IoT 플랫폼이 시뮬레이터를 이용하여 위에서 수집된 데이터를 분석하고 높은 정밀도로 비즈니스 가치를 평가하여 기지 관리 및 최적의 물류 계획을 도출한다.
- IoT 플랫폼이 위에서 수집된 데이터를 분석하여 공장/물류 기지 배치를 최적화함으로써 글로벌 시장으로 확장하기 위한 기지 배치 최적화 계획을 준비한다.
- IoT 플랫폼이 위에서 수집된 데이터를 분석한 후 전세계 공급 및 수요 조정 계획을 실행(구현)하여 수요 변동에 대응한 적정 수량의 재고를 배치하고 재고를 서로 교환한다.

1.4 사용 사례 도표

협업 SCM(공급망관리)

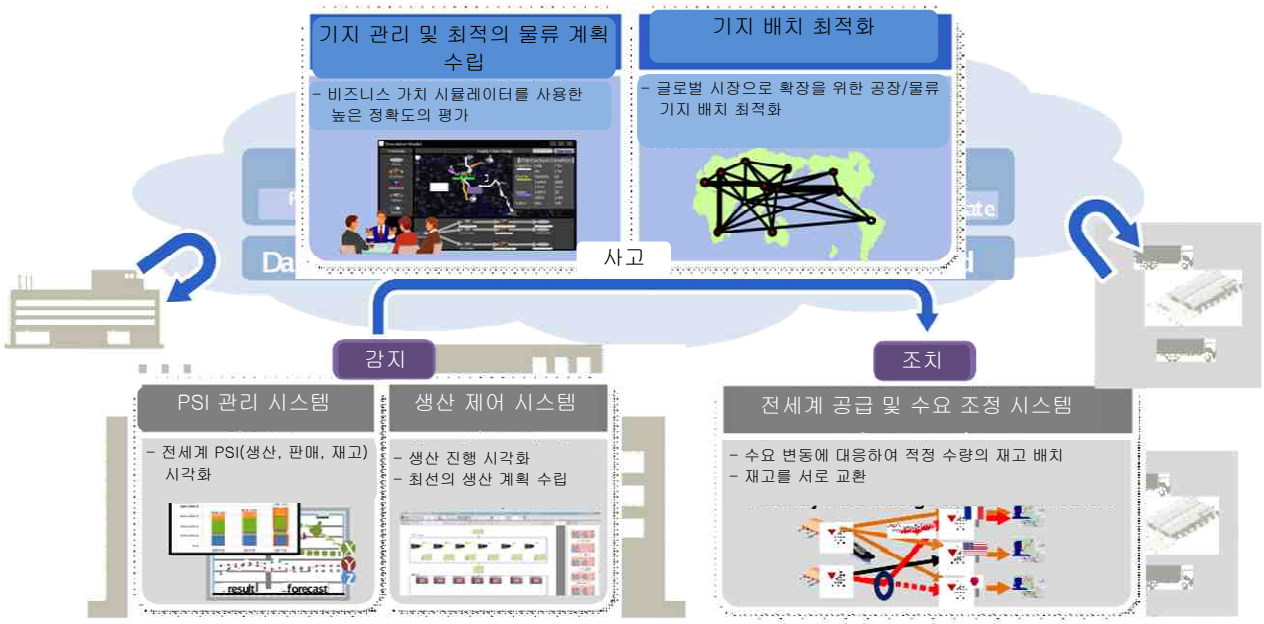


그림 C-1 | 사용 사례 도표 – 협업 공급망관리

1.5 사용 사례의 조건

1.5.1 전제

서로 다른 당사자가 연관된다.

1.5.2 선결요건

2.3, 2.4 및 2.5 참조

1.6 사용 사례에 대한 추가 정보

1.6.1 최신 상태

- 현재 상태

  – 단일 엔터프라이즈의 시스템 간 협업을 실현한다.

  – 주요 엔터프라이즈와 종속 엔터프라이즈의 시스템 간 협업을 실현한다.

- 최신 상태

  – 이전에 전혀 관계를 맺지 않았던 서로 다른 엔터프라이즈의 시스템 간 협업을 실현한다.

- 현재 상태를 최신 상태로 전환하려면 서로 다른 엔터프라이즈의 데이터를 통합하고 서로 다른 엔터프라이즈의 시스템에 연결하기 위한 기술/표준이 필요하다.

1.6.2 다른 관련 사용 사례(하위 및 상위 사용 사례 포함)

BCM(비즈니스 연속성 관리) 사용 사례가 본 사용 사례와 관련이 있다. BCM 사용 사례의 IoT 플랫폼은 이 사용 사례와 유사하게 감지, 사고 및 조치한다.

2. 특징적인 기능에 대한 매핑

2.1 연결성

기능		비고
실시간 상황 처리	X	실시간 감지수행 포함
다중 시스템 연결성	X	여러 시스템에 연결
원격 기능	X	제품 외부에 상주하는 기능
모든 대역폭/프로토콜에 대한 적용성		제공 대역폭/프로토콜에 맞춰 재구성→ HW에서 SW로 전환
새로운 연결성 표준으로 업그레이드 가능성		SW를 통해 새로운 연결성 표준으로 업그레이드할 수 있는 기능
합법적 감청 기능		
원격 액세스	X	
인증 및 액세스 제어	X	
신뢰성 및 무결성	X	

2.2 처리

기능		비고
온보드 분석	X	
오프보드 분석	X	
기계 학습	X	
맥락화	X	
익명화		
정보 매시업	X	
의미론 상호 운용성	X	
장치의 동적 구성	X	자가 치유/복원성을 위한 장치의 동적 구성
동적 구성가능성		변경 요구사항에 따라 장치가 자체적으로 또는 시스템에 의해 동적으로 구성 가능할 필요가 있다.
데이터 소유권 추적	X	
집단 인지	X	

2.3 메모리

기능		비고
디지털 제품 메모리	X	전체 수명주기, 제품 내력
패턴 인지	X	인공 지능/기계 학습 기반
기능 데이터	X	분석용

2.4 감지

기능		비고
감지 기능을 갖춘 장치 수 증가에 대응	X	
감지 데이터의 중재 교환	X	
데이터의 신뢰성	X	
원시 데이터의 정리	X	
초정밀 위치 기반 기능	X	
개인정보보호		
데이터의 무결성	X	
인증을 요하는 복잡한 센서	X	
센서 재구성 기능		

2.5 조치

제어 인터페이스 장치

기능		비고
교정	X	
장치 그룹의 제어	X	런타임 및 구성
장치의 동적 구성	X	동적 장치 온보딩/그룹에 지정
컨텍스트에 따라 장치가 제어되는 방식 적용	X	
안전성 요구사항		
인증 및 액세스 제어와 권한 부여	X	
플로어 제어	X	시스템을 실제로 제어하도록 허락된 사람들과 그 인계 메커니즘
집단/자체 최적화 제어 지능	X	
보안의 집단 제어	X	
컨텍스트 인지 제어	X	

사용자 I/O

기능		비고
촉각 인터페이스	X	
다중 장치 사용자 인터페이스	X	
가상 모델링	X	
시뮬레이션	X	
접근성	X	장애인용
증강 현실		예: 안경
사용성 및 사용자 경험	X	

2.6 보안

기능		비고
엔드 투 엔드 정책 관리	X	모든 정책 통합
가용 물리적 자원 및 보안성에 대해 최적화된 프레임워크	X	가용 물리적 자원/보안 강건성에 대해 최적화된 프레임워크(ISO 27001에서는 계획-실천-확인-조치) ISO 27001)
복원성	X	가상 물리 공격 포함
장애 허용 능력	X	가상 물리 공격 포함
시스템 위협 탐지 및 대응	X	OODA 관찰-방향설정-결정-실행
장치의 모니터링	X	
협조 및 위협 분석	X	
ID 관리	X	연합 ID 관리, 시스템 간 ID 상관관계,…
장치의 ID 보안		
인증 관리	X	데이터의 책임/부인 방지
이상 탐지	X	

3. 차세대 지원 기술

	차세대 지원 기술	비고
연결성	차세대 위성 연결을 위한 전송 계층 프로토콜	보다 높은 대역폭, 높은 지연시간
	5세대 셀룰러 액세스(5G)	
	저전력 무선 액세스(LPWAN)	

	차세대 지원 기술		비고
처리	시스템 구성 및 동적 구성	X	
	데이터 맥락화	X	
	자율 데이터 교환	X	
	센서 융합 기술	X	
	기계 학습	X	
	가상화		
메모리	디지털 제품 메모리		
감지	초정밀 위치 기술		
조치	증강 현실		
	가상 현실		
	촉각 인터넷		
보안	사물의 ID		
	준동형 암호화		
	검색 가능 암호화		
	신뢰 구축		
	보안화 시스템 협업 기술	X	
	사용 제어를 통한 개인정보보호		
	지속적인 보안 감사		
	IoT용 IAM 기술	X	ID 및 액세스 관리
	애플리케이션 격리 및 보안 경계 기술	X	

4. 필요한 미래 기술

	표준 요구사항	비고
연결성	5G 표준의 실현	
	표준 위성과 장치 간의 보다 높은 대역폭/요구 지연시간을 지원하기 위한 새로운 전송 계층 프로토콜에 대한 표준	
	IoT 장비가 새로운 연결성 표준으로 업데이트하는 기능을 갖추도록 하는 표준	

	표준 요구사항		비고
프로세싱	정보 교환 모델	X	
	의미론 메타데이터 정의 표준 및 모델	X	
	데이터 교환 모델 및 인터페이스와 관련 표준	X	
	자율 데이터 교환 프로파일 및 교환 메커니즘	X	
	메타데이터 주석 모델 및 인터페이스	X	
	맥락화 정보 모델	X	
	메타데이터 컨텍스트 표준	X	
메모리	디지털 제품 메모리의 표준화		
감지	메타데이터에 대한 표준	X	
	초정밀 위치 기반 기술에 대한 추상화 표준		
	센서 개인정보보호 표준		최종 소비자/소비자의 옵트인/옵트아웃
	센서 융합 표준	X	센서 관찰을 추상화하는 센서 메타 모델 개발 표준. 이 표준은 정형화되지 않은 산발적 데이터를 고급 도메인 지식으로 바꿀 수 있는 기반이 된다.
조치	제어 인터페이스 장치 그룹을 고유하게 식별하는 표준 템플릿		
	시스템 간의 IoT 사용자 I/O를 일반화하는 일반 표준		
	고유한 IoT 접근성 요구사항에 대한 표준		일반적인 인간/컴퓨터 I/O를 뛰어넘는 고급 IoT 서비스 반영
보안	소셜 시스템의 ID 연합 표준	X	
	가상 물리 공격 보호 표준	X	
	동시 연결을 갖춘 다중 시스템에서 장치 ID에 대한 표준	X	예: W3C의 국제화 자원 식별자(IRI)
	플랫폼 무결성의 신뢰를 구축하기 위한 표준 프로토콜	X	
	협업 보안 프레임워크	X	상호 의존적인 시스템 간의 사이버 위협 분석 교환 활성화
	상호 의존적인 시스템 간 보안 기능 평가를 활성화하는 성숙 모델	X	

부록 D - 사용 사례

예측 유지보수 및 서비스

1. 사용 사례의 기술

1.1 사용 사례의 명칭

예측 유지보수 및 서비스: 상태 기반 유지보수 및 일정 수립

1.2 사용 사례의 목적 및 범위

1.2.1 범위

예측 유지보수 및 서비스는 유지보수 일정과 자원 사용(예: 예비 부품) 최적화를 위한 자산 건전성과 결정 지원의 전체적인 관리를 제공한다.

이 최적화는 건전성 점수, 이상 탐지, 스펙트럼 분석 및 기계 학습을 기반으로 한다. 최적화는 방대한 양의 융합 IT 및 OT 데이터를 처리할 수 있는 확장 가능한 고기능 데이터 처리 IoT 플랫폼에서 실행된다. 이 최적화는 정교한 데이터 공학 방법과 다양한 자산 제어/자동화 시스템의 데이터를 조합하여 자산 장애의 숨겨진 패턴을 찾아서 완화하게 한다.

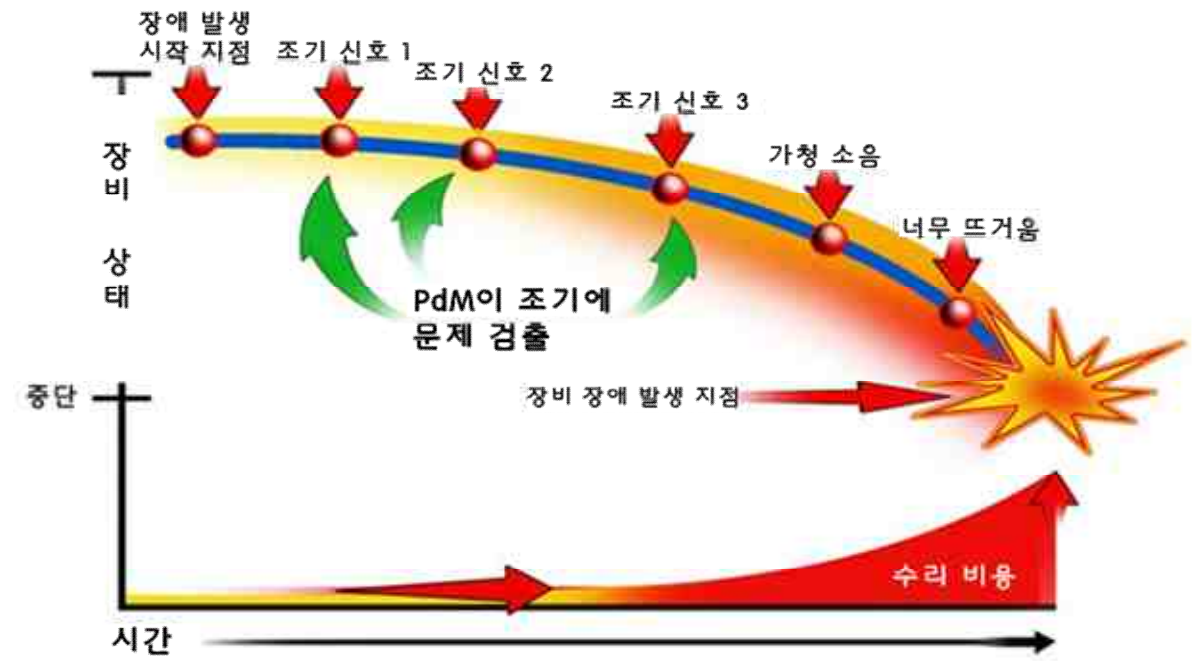


그림 D-1 | 예측 유지보수 및 서비스 시간[56]

그림 D-1에서 볼 수 있듯이 예측 유지보수 및 서비스를 통해 대상 자산이나 기계를 지속적으로 모니터링 및 분석할 수 있다. 이는 기계 운영자가 기계 장애를 사전에 파악하고 기계가 실제로 중단되기 전에 필요한 조치를 취할 수 있도록 지원한다. 이를 통해 비계획 중단 시간이 감소하고 유지보수 효율이 개선되며 운영비가 절감될 것이다.

이 절에서 살펴보는 사용 사례의 범위는 다음과 같다.

- OT에 의해 생성되는 운영 데이터와 함께 비즈니스 데이터(IT) 융합
- IoT플랫폼의 데이터 공학 기능
- 분석 결과를 의미 있는 조치로 전환

1.2.2 목적

예측 유지보수 및 서비스의 기본 목적은 유지보수 및 서비스의 품질 및 일정을 개선하기 위한 데이터 중심의 접근법 활성화를 통해 예방 유지보수 제공자가 혁신적인 소비자 서비스와 유지보수 성과를 제공하여 비즈니스를 경쟁력 있는 차별화 요소로 전환하도록 지원하는 것이다.

1.3 사용 경험담

1.3.1 사용 사례의 요약

이 사용 사례는 주로 데이터 융합(다양한 데이터 소스로부터 진정한 단일 소스로), 데이터 분석 및 찾아낸 정보를 의미있는 조치로 변환하는 현재 과제에 직면하기 위해 사용 가능한 IoT 플랫폼 기능에 중점을 둔다. 이 사용 사례에 있어 철도 운영자가 수행하는 상태 기반 유지보수와 일정 수립 및 예측 유지보수 및 서비스가 서비스 요구에 생산적으로 대응하고 유지보수 효율성을 개선하며 운영비를 절감하는 데 도움이 되는 방식에 대해 살펴본다.

1.3.2 사용 사례의 특성: 유지보수 최적화

자산 운영자의 중요한 목표는 운영비 절감이며 이에 대해 유지보수는 상당한 비중을 차지한다. 유지보수 최적화는 최소 예산 및 자원만으로 최고의 가용성을 지원하여 유지보수 운영의 최대 효율성을 보장한다. 예측 유지보수 및 서비스는 데이터 중심 분석, 계획 수립 및 우선순위 지정을 통해 이런 목표를 지원할 수 있다.

1.3.3 전체 기술

1.3.3.1: 과제: 다중 데이터 소스 결합으로 “방대한 데이터”를 “꼭 필요한만큼의 충분한 데이터”로 축소

IoT 플랫폼의 핵심 기능 중 하나이고 중추적인 요소는 다양한 소스의 데이터를 통합하여 진정한 단일 소스로 병합하기 위해 사용되는 데이터 융합 기능이다. 그러나 Gartner는 2020년대에 부적합한 데이터 수집 방법으로 인해 모든 IoT 프로젝트의 80%가 구현 단계에서 실패할 것 이라고 예측한다[4].

운영 데이터는 품질 보증, 컴포넌트 추적성, 프로세스 제어 등의 특정 사용 사례를 위해 항상 캡처되지만 그렇다고 해서 다른 운영 데이터와 통합되지는 않는다. 강력한 IoT 플랫폼 구축에 있어 초거대 데이터 세트에 대한 데이터 통합(IT/OT 통합) 및 데이터 품질은 주요 과제이며 고비용 요소이다.

항상 그렇듯이 데이터가 다중 소스에 상주하면 유용한 인사이트를 도출하기 위해서 데이터를 병합하여 분석할 필요가 있다. 여기에는 벤더 내역, 컴포넌트 마스터 데이터 등과 더불어 각기 다른 목적으로 사용되는 다중 센서의 운영 데이터가 포함된다. 단순히 이런 데이터를 결합하거나 융합하면 잘못된 결과로 이어지거나

쓸모없거나 품질이 더 낮을 것이다. 이를 극복하려면 데이터 관리 방법을 재고하는 것이 중요하다. 기능 제약을 극복하기 위해 인메모리 데이터 처리, 분산 컴퓨팅 및 인간 중심 데이터 마이닝을 통한 초 대규모 데이터를 지원하는 IoT 플랫폼이 선호될 것이며 데이터 통합, 표준화 및 관리를 위한 혁신적인 접근법이 요구된다.

1.3.3.2 과제: 빅 데이터 및 데이터 분석

프로젝트 및 상업적 구현 중에 다음 몇 가지 경향이 일관되게 관찰된다.

- 인간이 단독으로 또는 오늘날의 중간 규모 기계조차도 기계 및 센서에 의해 생성되는 방대한 분량의 데이터를 처리할 수 없다. 이 사실은 기계 생성 데이터의 0.5 페타바이트가 포함되는 최대 데이터 세트를 갖는 현재까지 수행된 모든 프로젝트에 있어 분명했다. 고기능 컴퓨팅이 지원되지 않으면 인간은 그런 데이터를 처리할 수 없다.
- 현재까지 컴퓨터 알고리즘은 정확하고 신뢰성 있게 임의적인 기계 또는 컴포넌트 장애를 예측할 수 없다. 이 문서를 작성하는 시점에 개별 기계나 기계 그룹에 있어 모든 부문에 통용되는 장애를 예측하는 신뢰성 있고 강력한 일반적인 방법은 발견되지 않았다.
- 인간은 기계에 의해 생성되는 방대한 용량의 데이터를 처리할 수 없기 때문에 동시에 알고리즘을 효과적으로 사용하여 인간 사용자에게 의미있는 정보를 제공하는 것도 필수불가결하다.
- 더욱이 데이터의 품질이 낮거나 오류가 있기 때문에 데이터 레이크(data lake)에서 기계 데이터의 50% – 60%는 기계 학습에 사용할 수 없다.
- IT/OT 통합을 위한 단일 산업 간 표준 데이터 모델이 없다. 또한 소비자는 자신들의 특정 형식으로 데이터를 조회 및 분석하길 원한다.

1.3.3.3 새로운 접근법이 요구되는 IoT의 현재 및 미래 요구

새로운 접근법에 사용되는 개념 모델은 가추 추론(잠정적 가설 → 이론)과 연역적 추론(이론 → 가설 → 관찰 → 확인) 중 하나여야 하며, 여기서 이런 프로세스에 대한 입력을 제공할 수 있는 데이터 공학은 귀납적 추론(관찰 → 패턴 → 잠정적 가설 → 이론)으로 간주될 수 있다. 대화형이고 (대부분의 경우) 반복적인 이 프로세스(그림 D-2 참조)는 부문 전문가와 데이터 공학 간에 요구되는 협업(관찰 – 이론 – 관찰)을 보여준다.

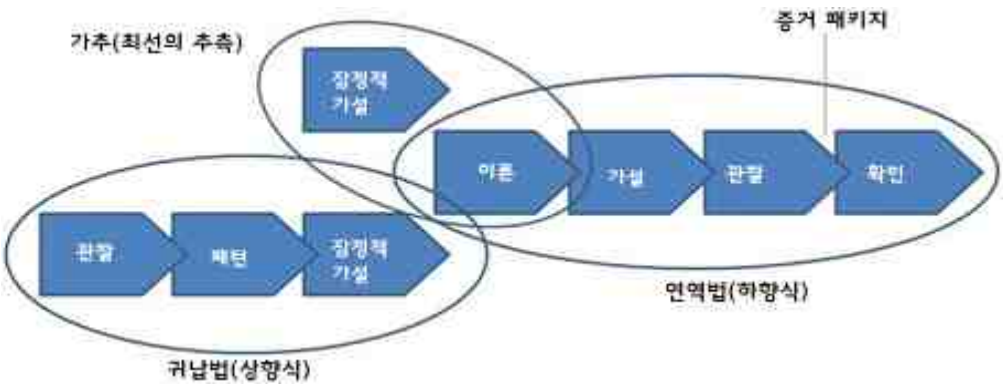


그림 D-2 | 새로운 접근법에 대한 개념 모델

IoT 플랫폼은 인메모리 데이터 처리, 분산 컴퓨팅 및 비용 효율적인 스토리지를 이용한 초대규모 데이터 세트를 지원할 준비가 되어 있어야 한다. 고급 데이터 공학 기능 및 예측 시나리오를 적용하면 해당 조직에 대한 전체적인 프로세스 효율이 향상될 것이다. 데이터를 "있는 그대로" 검색하고 가능한 한 그 처리를 유예하기 위한 데이터 관리가 준비되어야 한다. 데이터를 처리 중일 때만 데이터가 정리되며, 대응 필요가 있는 비즈니스 문제에 특정적인 형식으로 데이터가 통합되어야 한다.

산업 간 IoT 플랫폼의 대상 사용자는 주로 기계 엔지니어링, 화학 엔지니어링 또는 기타 엔지니어링 및 제조 기반 활동을 전문적으로 하는 비즈니스 사용자와 부문 전문가이다.

업체의 핵심 비즈니스나 비즈니스 라인에 있어 유지보수, A/S, 품질 보증, 총수익, 에너지 효율, 제품 개선 및 프로세스 개선과 같은 복잡한 프로세스 관리는 이런 사람들의 역할이 될 것이다. IoT 플랫폼의 또 다른 중요한 설계 개념은 부문 전문가들에게 데이터 공학자 또는 전처리(예: 검색 프로세스에 도움이 될 수 있는 복잡한 주요 지표의 계산)의 기타 소스로부터 정보 조각이 제공될 수 있다는 점이다(그림 D-3 참조).

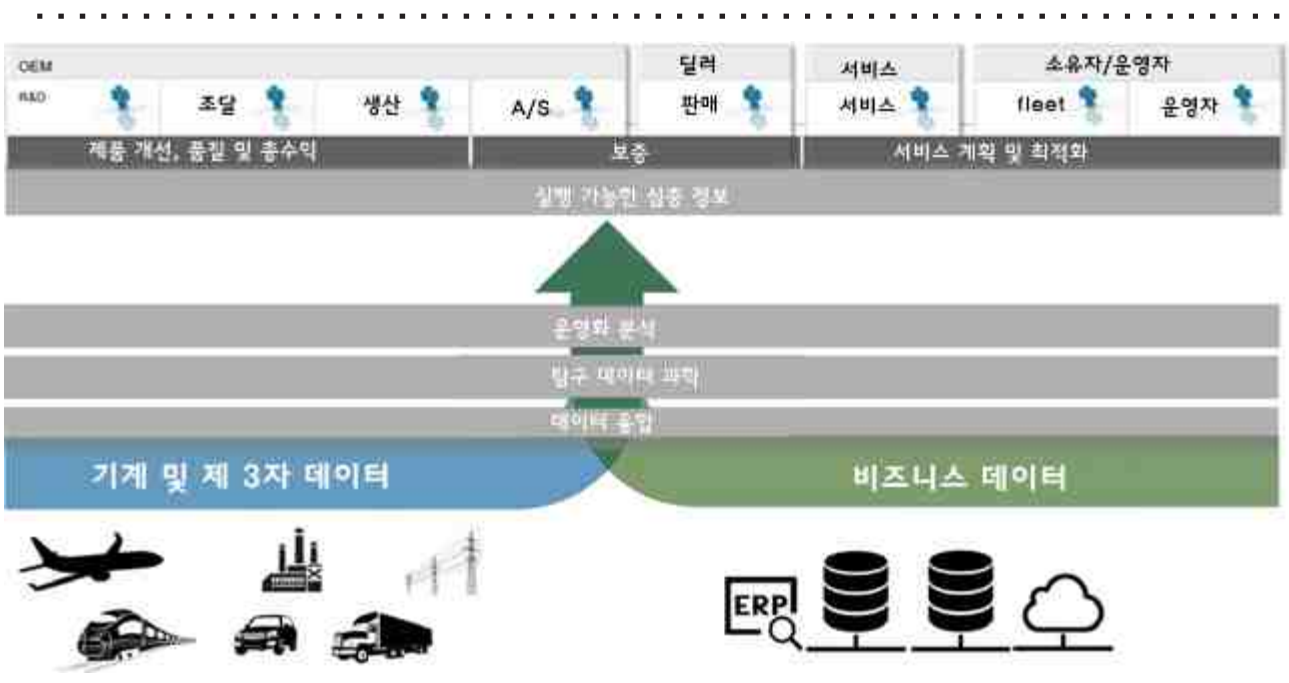


그림 D-3 | 산업 간 IoT 플랫폼

1.3.3.4 사용 사례: 철도 운영자의 유지보수 최적화

예측 유지보수 기법은 유지보수 일정과 자원 사용(예: 예비 부품) 최적화를 위한 자산 건전성과 결정 지원의 전체적인 관리를 제공한다. 이 최적화는 건전성 점수, 이상 탐지, 스펙트럼 분석 및 기계 학습을 기반으로 한다.

아래에서 살펴보는 사용 사례는 철도 운영자가 예측 유지보수 및 서비스 솔루션을 사용하여 기관차 수준에서 플릿(fleet) 또는 컴포넌트의 유지보수를 관리하는 방법에 대한 간략한 개요를 제공한다. 이 예에서는 차량에 사용되는 일단의 배터리 또는 열차 조명, 엔진 시동, 신호, 전기 통신, 다중 전자 장치 등에서 기계 수준에서 사용되는 특정 배터리를 분석한다. 배터리는 차량의 핵심 자산이며 배터리 문제는 예상치 못한 가동 중지 시간으로 이어질 수 있다. 고장난 배터리의 조기 발견은 가동 중지 시간 절감에 상당한 영향을 준다.

1.3.3.6 현재 상황

기관차 한 대에 정기 유지보수가 요구되는 구성부품이 50,000개 이상 존재한다. 현재 이런 구성부품에 대한 유지보수 활동은 압연재 공급자가 제공하는 일정을 근거로 계획된다. 이런 일정은 마일리지나 시간별로 계산되며 특정 부품의 실제 또는 예상 장애에 대응(시정 유지보수)하는 것을 목적으로 한다. 데이터 마이닝은 적용되지 않는다.

1.3.3.6 목적

- 기술 지원 유지보수 운영의 개선 및 발전을 위해 강력한 확장형 개방 플랫폼을 구축한다.
- 보다 복잡한 알고리즘을 갖는 규칙 기반 접근법을 추가 패턴 및 이상 탐지가 가능하도록 확장한다.
- 각 구성부품의 특정 패턴을 토대로 유지보수 일정에 대한 보다 융통성 있는 효율적인 새로운 접근법을 추진한다.

1.3.3.7 거리 기반 악성 행위자 분석

거리 기반 악성 행위자 분석을 수행하려면 장비의 센서 데이터가 시계열 스토리지로부터 추출되어야 한다. 추출된 데이터는 학습 모델 정의를 위해 구문 분석, 보강 및 변환되어야 한다. 이는 토공기계의 거리 알고리즘과 시계열 스토리지의 저장 거리를 사용하여 각 구성부품(예: 배터리)이 참조 구성부품에 대해 이미 커버한 마일리지를 산출하여 수행될 수 있다. 특정 한도를 초과하는 배터리 수명이 불량한 상태로 간주될 수 있다. 그림 D-4와 같이 유지보수 및 서비스에 대한 비즈니스 시스템에서 경고와 서비스 통보가 생성된다.

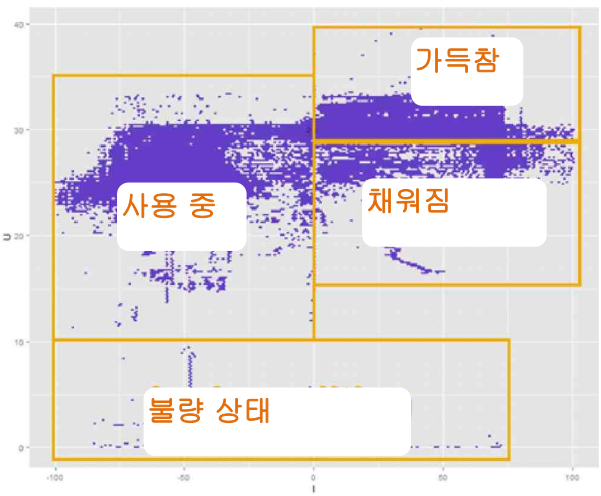


그림 D-4 | 거리 기반 악성 행위자 분석을 위해 추출된 데이터의 예

위 예측 유지보수 접근법은 운영자가 적정 시간에 요구되는 모든 유지보수 대책만을 수행하여 적정 자원의 가용성을 보장함으로써 운영비를 절감하고 계획하지 않은 가동 중지 시간을 줄이는 데 도움이 될 것이다.

1.3.3.8 IoT 플랫폼의 미래 전망

IoT 플랫폼은 시간, 소스, 네트워크 및 형식에 구애받지 않고 데이터 수집을 인스턴스화하여 실시간 데이터 융합을 지원해야 한다. 이 플랫폼은 인접 플랫폼 및 시스템의 의미론과 언어를 통합할 수 있어야 한다. 그러면 다중 플랫폼 간의 데이터 전송을 활성화하여 Platform of Platforms(플랫폼을 위한 플랫폼) 개념을 실현할 것이다.

이 플랫폼은 온보드 분석, 자가 치유 및 경험에 근거한 자체 학습을 지원해야 한다. 이는 비정상 항목의 취급을 개선하고 이를 반복하지 않도록 지원할 것이다.

이 플랫폼에는 고급 기계 학습 기능, 사용 준비 완료된 내장 애플리케이션, 알기 쉬운 시각화 및 디자인 개념과 함께 실시간으로 비즈니스 인사이트를 제공하는 데 필요한 실시간 데이터 수집, 처리 및 데이터 변환을 수행하도록 지원하는 (장소에 구애없이 매끄러운) 데이터 전송 기능을 갖춰야 한다.

안전과 보안에 중점을 둔 이 플랫폼의 원격 모니터링 및 원격 실행 제어 기능은 인간에게 액세스 권한이 없거나 제한적인 상황(예: 석유 굴착 장치)에서 보다 나은 장치 수명 주기 관리가 가능하도록 지원한다. 장치 수명 주기 관리는 위에서 언급한 부문에 제한될 뿐만 아니라 신규 자산의 설치와 구성, 유지보수 및 운영주기 종료 시점에 도달한 후 서비스 해제와 같은 광범위한 부분을 다룬다.

1.3.3.9 미래 IoT 플랫폼에 대한 기술적 요구사항

첨단 IoT 플랫폼은 플랫폼 간에 정보를 공유하는 다중 플롯폼에 연결하여 장치 연결성과 확장성을 지원하고 쉬운 데이터 전송을 지원해야 한다.

더 나아가 IoT 플랫폼은 규칙 엔진과 모델 관리자와 같은 고급 기능을 갖춰야 한다. 규칙 엔진은 이전의 데이터 탐색을 근거로 한 학습 프로세스의 표준을 정의 및 설정하고 모델 관리자는 인지되거나 학습된 패턴을 분석 라이브러리로 포함하는 것을 담당한다. 그러면 인공 지능과 기계 학습 알고리즘이 학습된 패턴을 활용하여 개별 모델을 도출할 수 있다.

엣지 네트워크에서 통합 보안 및 원격 관리에 연관된 플랫폼의 상호 운용성은 IoT 솔루션이 엣지 네트워크에서 처리 기능을 활용할 수 있도록 지원한다. 또한 이는 IoT 센서 네트워크가 데이터 전송을 위해 상호 연결할 수 있는 생태계를 제공하며 엣지 네트워크에서 인사이트를 조치로 전환하는 실시간 컨텍스트를 제공한다. 엣지에서 실시간 인사이트를 실행하면 왕복 지연시간에 대한 필요가 방지된다.

IoT 플랫폼은 실시간 트랜잭션 데이터에 대한 고기능 메시지 처리 시스템을 지원하여 안정적이지 못한 네트워크에서 데이터 무결성을 보장해야 한다. 또한 고급 플랫폼 기능은 분석 애플리케이션 및 마이크로 서비스의 매끄러운 구축과 배포를 지원해야 한다. 동시에 만족스러운 사용자 경험을 이끌어내려면, 플랫폼이 가상 모델링 및 증강 현실과 같은 고급 인터페이스를 제공하는 플랫폼이 필요하다.

Platform of Platforms(플랫폼을 위한 플랫폼)의 미래와 성공은 오늘날 엣지 네트워크에서 IoT 플랫폼 및 장치 연결성에 대해 설정된 표준에 좌우된다.

2. 특징적인 기능에 대한 매핑

2.1 연결성

기능		비고
실시간 상황 처리	X	실시간 감지수행 포함
다중 시스템 연결성	X	여러 시스템에 연결
원격 기능	X	제품 외부에 상주하는 기능
모든 대역폭/프로토콜에 대한 적용성	X	제공 대역폭/프로토콜에 맞춰 재구성 → HW에서 SW로 전환
새로운 연결성 표준으로 업그레이드 가능성	X	SW를 통해 새로운 연결성 표준으로 업그레이드할 수 있는 기능
합법적 감청 기능		
원격 액세스	X	
인증 및 액세스 제어	X	
신뢰성 및 무결성	X	

2.2 처리

기능		비고
온보드 분석	X	
오프보드 분석	X	
기계 학습	X	
맥락화	X	
익명화		
정보 매시업	X	
의미론 상호 운용성	X	
장치의 동적 구성	X	자가 치유/복원성을 위한 장치의 동적 구성
동적 구성가능성		변경 요구사항에 따라 장치가 자체적으로 혹은 시스템을 통한 동적인 구성이 가능해질 필요
데이터 소유권 추적	X	
집단 인지		

2.3 메모리

기능		비고
디지털 제품 메모리	X	전체 수명주기, 제품 내력
패턴 인지	X	인공 지능/기계 학습 기반
기능 데이터	X	분석용

2.4 감지

기능		비고
감지 기능을 갖춘 장치 수 증가에 대응	X	
감지 데이터의 중재 교환	X	
데이터의 신뢰성	X	
원시 데이터의 정리	X	
초정밀 위치 기반 기능		
개인정보보호		
데이터의 무결성	X	
인증을 요하는 복잡한 센서		
센서 재구성 기능	X	

2.5 조치

제어 인터페이스 장치

기능		비고
교정	X	
장치 그룹의 제어	X	런타임 및 구성
장치의 동적 구성	X	동적 장치 온보딩/그룹에 지정
컨텍스트에 따라 장치가 제어되는 방식 적용	X	
안전성 요구사항	X	
인증 및 액세스 제어 및 인증	X	
플로어 제어		시스템을 실제로 제어하도록 허락된 사람들과 그 인계 메커니즘
집단/자체 최적화 제어 지능		
보안의 집단 제어		
컨텍스트 인지 제어		

사용자 I/O

기능		비고
촉각 인터페이스		
다중 장치 사용자 인터페이스	X	
가상 모델링	X	
시뮬레이션	X	
접근성		장애인용
증강 현실	X	예: 안경
사용성 및 사용자 경험	X	

2.6 보안

기능		비고
엔드 투 엔드 정책 관리	X	모든 정책 통합
가용 물리적 자원 및 보안성에 대해 최적화된 프레임워크	X	가용 물리적 자원/보안 강건성에 대해 최적화된 프레임워크(ISO 27001에서는 계획-실천-확인-조치) ISO 27001)
복원성	X	가상 물리 공격 포함
장애 허용 능력	X	가상 물리 공격 포함
시스템 위협 탐지 및 대응	X	OODA 관찰-방향설정-결정-실행
장치의 모니터링	X	
협조 및 위협 분석	X	
ID 관리	X	연합 ID 관리, 시스템 간 ID 상관관계, …
장치의 ID 보안	X	
인증 관리	X	데이터의 책임/부인 방지
이상 탐지	X	

3. 차세대 지원 기술

	차세대 지원 기술		비고
연결성	차세대 위성 연결을 위한 전송 계층 프로토콜		보다 높은 대역폭, 높은 지연시간
	5세대 셀룰러 액세스(5G)	X	
	저전력 무선 액세스 (LPWAN)		

	차세대 지원 기술		비고
처리	시스템 구성 및 동적 구성	X	
	데이터 맥락화	X	
	자율 데이터 교환	X	
	센서 융합 기술	X	
	기계 학습	X	
	가상화	X	
메모리	디지털 제품 메모리	X	
감지	초정밀 위치 기술		
조치	증강 현실	X	
	가상 현실		
	촉각 인터넷		
보안	사물의 ID	X	
	준동형 암호화	X	
	검색 가능 암호화		
	신뢰 구축	X	
	보안화 시스템 협업 기술	X	
	사용 제어를 통한 개인정보보호		
	지속적인 보안 감사		
	IoT용 IAM 기술	X	ID 및 액세스 관리
	애플리케이션 격리 및 보안 경계 기술	X	

4. 필요한 미래 표준

	표준 요구사항		비고
연결성	5G 표준의 실현	X	
	표준 위성과 장치 간의 보다 높은 대역폭/요구 지연시간을 지원하기 위한 새로운 전송 계층 프로토콜에 대한 표준		
	IoT 장비가 새로운 연결성 표준으로 업데이트하는 기능을 갖추도록 하는 표준	X	

	표준 요구사항		비고
프로세싱	정보 교환 모델	X	
	의미론 메타데이터 정의 표준 및 모델	X	
	데이터 교환 모델 및 인터페이스와 관련 표준	X	
	자율 데이터 교환 프로파일 및 교환 메커니즘	X	
	메타데이터 주석 모델 및 인터페이스		
	맥락화 정보 모델	X	
	메타데이터 컨텍스트 표준		
메모리	디지털 제품 메모리의 표준화		
감지	메타데이터에 대한 표준	X	
	초정밀 위치 기반 기술에 대한 추상화 기술		
	센서 개인정보보호 표준		최종 소비자/소비자의 옵트인/옵트아웃
	센서 융합 표준	X	센서 관찰을 추상화하는 센서 메타 모델 개발 표준. 이 표준은 정형화되지 않은 산발적 데이터를 고급 도메인 지식으로 바꿀 수 있는 기반이 된다.
조치	제어 인터페이스 장치 그룹을 고유하게 식별하는 표준 템플릿		
	시스템 간의 IoT 사용자 I/O를 일반화하는 일반 표준		
	고유한 IoT 접근성 요구사항에 대한 표준		일반적인 인간/컴퓨터 I/O를 뛰어넘는 고급 IoT 서비스 반영
보안	소셜 시스템의 ID 연합 표준		
	가상 물리 공격 보호 표준	X	
	동시 연결을 갖춘 다중 시스템에서 장치 ID에 대한 표준		예: W3C의 국제화 자원 식별자(IRI)
	플랫폼 무결성에서 신뢰를 구축하기 위한 표준 프로토콜	X	
	협업 보안 프레임워크		상호 의존적인 시스템 간의 사이버 위협 분석 교환 활성화
	상호 의존적인 시스템 간 보안 기능 평가를 활성화하는 성숙 모델		

부록 E - 사용 사례

스마트 및 보안 IoT 플랫폼을 이용한 스마트 시티

1. 사용 사례의 기술

1.1 사용 사례의 명칭

스마트 및 보안 IoT 플랫폼을 이용한 스마트 시티

1.2 사용 사례의 범위 및 목적

1.2.1 범위

스마트 시티의 범위에서는 감지, 처리, 작동, 통신 및 보안 관점에서 다양한 ICT 기술을 통합하여 스마트하고 안전한 방식으로 자원 관리, 정보 투명성 및 작동 효율을 향상시킨다.

1.2.2 목적

유럽 스마트 시티 프로젝트[57]는 스마트 거버넌스, 스마트 이동, 스마트 공공시설, 스마트 빌딩, 스마트 환경 등의 서로 다른 서비스 부문을 고려하여 유럽 도시의 스마트 수준을 평가해 왔다. 도메인 간 기술 통합과 정보 매시업은 고급 스마트와 보안 기술을 이용하는 차세대 IoT 플랫폼에 있어 필수 요구사항일 것이다. 그러므로 여기에서는 공공 안전, 도시 성과, 도시 이동, 모바일 운영 센터 및 스마트 공공시설 사용을 포함한 다양한 서비스 유형의 스마트 시티가 차세대 스마트 및 보안 IoT 플랫폼의 구체적인 사용 사례를 제공하기 위해 고려된다.

1.3 사용 경험담

공공 부문

1.3.1 사용 사례의 요약

스마트 시티 사용 사례에 있어 온도, 습도, 소음, 가스, 동작 센서, 카메라, 모바일 장치, 네트워크 스니퍼, 스마트 계량기 및 수도 계량기와 같은 다양한 유형의 센서와 데이터 소스가 도시의 동태(dynamics) 감지를 위해 배포된다. 다중 모델 감지 정보는 의미론적 상호 운용성을 이용하여 도메인 간 및 실시간 정보 매시업으로 변환된다. 더 나아가 이런 정보 매시업은 다양한 고급 데이터 마이닝 및 기계 학습 기법을 위해 쉽게 액세스되어 주민 및 여러 기관을 위한 애플리케이션을 제공하여 지능형 작업이 수행될 수 있을 것이다. 이 스마트 시티 사용 사례에서는 공공 안전, 도시 성과, 도시 이동, 모바일 운영 센터 및 모바일 공공시설 이용을 포함한 다양한 대표적인 도시 애플리케이션을 검토한다. 또한 감지, 처리, 메모리, 연결성 및 작동에 있어 차세대 IoT 플랫폼의 고급 기능이 도시 지역에서 보다 스마트하고 안전한 거주 환경을 조성할 수 있는 방식에 대해 살펴본다.

1.3.2 사용 사례의 특성

1.3.3 전체 기술

스마트 및 보안 IoT 플랫폼을 이용한 스마트 시티는 그림 E-1과 같이 다수의 유력한 IoT 서비스가 가능하게 지원한다. 먼저 공공 안전 향상을 위해 비상 대응 기술이 대피 인원 밀도와 추가 수색 및 구조를 위해 기관으로부터 요구되는 자원을 예측한다. 둘째로 스마트 환경 구축을 위해 도시 성과 조사에 필요한 교통, 대기의 질, 소음 및 혼잡 수준에 대한 데이터를 제공한다.

셋째, 스마트 이동 활성화를 위해 혼잡도 탐지 기술이 인간 이동을 캡처하여 도시에서 인간 이동 및 행동 방식을 분석하여 대중 교통 서비스를 개선하여 지나치게 혼잡한 교통 수단 탑승 경험이 생기는 것을 방지한다. 넷째, 스마트 공공시설 이용 및 스마트 빌딩 구축을 위해 스마트 계량 시스템이 자동으로 수도와 전기 사용량을 기록하고 이를 공공시설 기관에 보고한다. 동시에 에너지 절약을 위한 몇 가지 권고사항도 알려준다. 다섯째, 도시 안전 향상을 위한 스마트 정부 활성화를 위해 이미지 처리 및 인지 기술이 범죄 조사를 촉진하고 범죄나 도난 차량 식별 등을 통해 보다 많은 범죄 해결을 지원한다. 마지막으로 스마트 시티의 동적 필요에 대응하기 위해 모바일 운영 센터가 다중 기관 및 사용자 간의 데이터 소유권을 통제하는 보안화 인증을 통해 서로 다른 기관 간에 실시간 센서 데이터 스트림을 동적으로 교환할 수 있다. 이상의 모든 스마트 시티 서비스는 연결된 개체, 장치, 클라우드 및 기관의 감지 데이터에 대한 각 매시업 수준에 크게 의존하며 이런 데이터는 주민들 및 여러 기관에 전달되어 스마트 서비스(작동 포함)를 가능하게 한다.

스마트 시티 이야기: 스마트 시티의 구체적인 이야기는 이런 스마트 서비스들이 스마트하고 안전한 방식으로 상호 협업하는 방식을 설명하기 위해 제공된다. 구체적인 예제 시나리오는 다음과 같은 중요 상황 탐지 및 대응이다. 도시에서 화학물질 사고 또는 테러 공격으로 인한 대형 폭발 사고와 같은 비상 사태가 발생할 때 혼잡 탐지, 도시 이동 및 도시 성과 조사 기법이 관련 인원 대피를 위한 혼잡 수준, 인간 이동 흐름, 대중 교통 이용 및 교통 상태에 대한 투명한 정보를 제공할 것이다. 한편 동적 모바일 운영 센터가 설치되어 현장 구조 작업을 지원한다. 그런 모바일 운영 센터는 다중 기관과 공조하여 자원(예: 앰뷸런스, 자율 주행 차, 소방차 및 경찰 차량)을 관리 및 파견한다.

또한 수색 및 구조 로봇과 자율 주행 차가 희생자 구조를 위해 파견된다. 비상 대응 중 사이버 공격을 방지하기 위해 모바일 운영 센터는 데이터와 데이터 소유권에 대한 액세스를 통제한다. 테러 공격 발생 시 도시 감시 기능이 용의자를 색출하여 얼굴 인식을 통해 경찰과 비상 대응 기관 간의 기관 간 공조를 촉진한다. 얼굴 인식은 실종 아동과 가족 찾기에도 사용될 수 있다. 또한 고급 기술을 통해 정보 매시업은 도시의 세련됨, 안전성, 보안성을 높여줄 수 있다. 차세대 플랫폼에서 정보 매시업을 활성화하려면 개체, 장치, 엣지 노드, 작동기, 기관 및 서비스 간의 연결이 기존의 다대일 또는 일대다 연결이 아니라 다대다가 될 것이다. 단일 데이터 소스는 단일 엔터프라이즈 클라우드뿐만 아니라 다중 연결 클라우드에 대한 정보도 제공할 것이다.

1.4 사용 사례의 도표

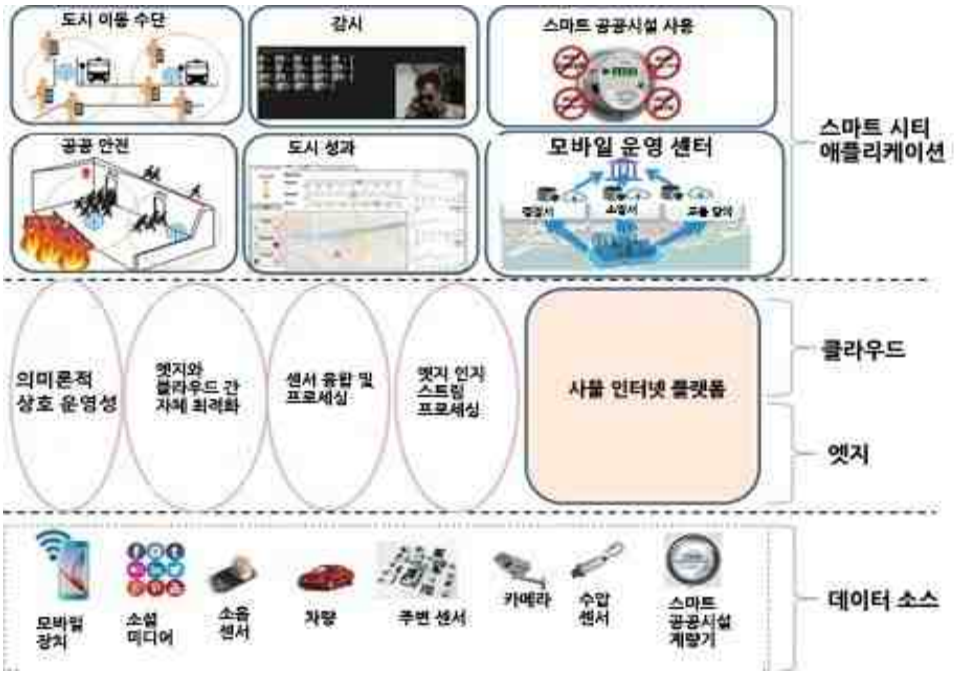


그림 E-1 | 스마트 및 보안 IoT 플랫폼을 이용한 스마트 시티

그림 E-2 | 스마트 및 보안 IoT 플랫폼을 이용한 스마트 시티의 비전

1.5 사용 사례의 조건

1.5.1 전제

미래 도시에 스마트 개체가 배포되는 것을 전제로 한다. 그런 스마트 개체는 그림 E-2와 같이 메모리, 연결성, 감지, 처리 및 조치의 기본 기능을 갖추고 있다. 기본 기능과 함께 도시의 주변 정보, 이동, 에너지 또는 수도 사용량, 동영상 스트림, 교통 정보 등이 감지될 수 있다. 한편, 각 스마트 개체는 다중 스마트 개체와 다중 엔티티(즉, 스마트 시티 활성화를 위한 애플리케이션 및 서비스 플랫폼 등)에 연결될 수 있다.

1.5.2 선결요건

기존 IoT 플랫폼은 엣지와 협업하여 서로 다른 소스로부터 데이터를 수집한다. 차세대 IoT 플랫폼의 발전은 (1) 의미론적 상호 운용성, (2) 엣지와 클라우드 간 자체 최적화, (3) 센서 융합과 처리 및 (4) 엣지 인지 스트림 처리를 포함한 다수의 다른 고급 기능으로 지원될 것이다.

1.6 사용 사례에 대한 추가 정보

1.6.1 최신 상태

센서 융합 및 처리: 센서 융합 및 처리 기법은 대상 정보의 강력하고 전체적인 기술을 제공하기 위해 다중 센서로부터의 관찰을 결합하는 프로세스를 나타낸다. 일반적인 센서 융합 기법은 센서 데이터 스트리밍을 단일 모델로 통합하고 로봇 제어, 로컬라이제이션 및 환경 모니터링 영역에서 공통적으로 고려되었던 확률적 추론 모델링(예: 입자 여과기 또는 칼만 필터)[58]을 기반으로 한다. 인간 이동에 대한 분석과 관련하여 이미지 기반 기법이 이미지 프레임으로 발견되는 사람 모형을 사용하여 사람 수를 계산하고[59] 센서 기반 접근방법이 실내 장소의 점유 혼잡 수준을 판별하기 위해 다중 모델 센서 데이터를 근거로 특징을 추출한다[60].

IoT 표준: 목표 비전은 IoT 및 스마트 시티 플랫폼에서 의미론적 상호 운용성을 지원하는 것이다. 이 비전을 달성하기 위해 M2M 시스템(아마도 oneM2M 표준에 기반)에서 수신되는 정보 스트림이 FIWARE에서 표준으로 정의되어 사용되는 차세대 서비스 인터페이스(NGSI) 기반 맥락화 정보 모델로 자동으로 매핑될 수 있다. 이 변환 프로세스는 의미론적 중재 게이트웨이(SMG)에 의해 취급되어 의미론적 정보뿐만 아니라 변환 루틴의 라이브러리를 사용하여 서로 다른 정보 모델을 공통적인 모델로 매핑할 수 있다. 변환된 메타데이터는 가용 자원, 자동 정보 매시업 및 개선된 빅 데이터 분석 기능의 빠른 발견을 위해 사용될 수도 있다.

2. 특징적 기능에 대한 매핑

의미론적 상호 운용성: 상호 운용성은 “둘 이상의 시스템이나 구성요소가 데이터를 교환하고 정보를 사용하는 기능”이다[61]. 의미론적 상호 운용성은 상호작용을 하는 시스템이 개별 데이터 형식에 관계없이 시스템 간 데이터의 일관성을 보장하면서 교환되는 데이터와 동일한 의미를 갖게 될 때 달성된다. 의미론은 온톨로지에서 지정되는 것과 같은 공유된 어휘를 사용하여 명시적으로 정의될 수 있다. 의미론적 상호 운용성은 IoT 시스템의 모든 부분(즉, 클라우드 내의 IoT 플랫폼)에 적용될 수 있지만 엣지 구성요소와 IoT 장치에까지 도달할 수도 있다.

엣지와 클라우드 간 자체 최적화: 스마트 시티 애플리케이션은 일반적으로 서로 다른 수준에서 다양한 데이터 처리 작업에 의존하여 지리적으로 분산된 IoT 데이터 소스로부터 실시간 인사이트를 추출한다. 클라우드-엣지 기반 환경에서

그런 작업은 특정 최적화 목적 충족(예: 엣지와 클라우드 간의 대역폭 소모를 절감, 원시 센서 데이터로부터 분석 결과를 추출하기 위한 지연시간의 최소화)을 위해 클라우드 또는 엣지에 동적으로 할당될 수 있다. 엣지와 클라우드 간 작업 배포의 최적화는 애플리케이션 개발자가 제공하는 표준에 기반하여 설계 시(배포 전) IoT 플랫폼에 의해 이행되거나 시스템 플랫폼 자체로부터 측정된 실시간 시스템 정보를 기반으로 런타임 시(배포 후) IoT 플랫폼에 의해 이행될 수 있다. 예를 들어 영상 감시 시스템에서는 카메라 영상을 근거로 용의자를 발견하기 위한 네 가지 처리 작업(즉, 영상 스트림 판독기, 이미지 추출, 얼굴 추출 및 얼굴 인식)이 필요할 것이다. 대역폭 소모 절감을 위해 앞의 3가지 작업 유형을 엣지에 할당하고 발견된 얼굴만 클라우드로 전송하여 얼굴 인식을 할 수 있다. 그러나 연관된 엣지 노드에 과부하가 걸리면 런타임 중에 일부는 엣지에서 클라우드로 마이그레이션될 수 있다.

센서 융합 및 처리: 고급 센서 융합 및 처리 기법은 지나치게 과중한 사전 교육 간접비를 들이지 않고 실시간 스트리밍을 취급하고 실시간 이상의 예측을 수행할 수 있어야 한다. 예를 들어 경량 장치가 소규모의 관찰된 데이터 내에서 온보드 학습을 수행하여 추가 작업을 위해 인사이트를 스마트 시티 애플리케이션으로 전송할 수 있다. 한편 차세대 IoT 플랫폼에서는 스마트 시티 애플리케이션을 효과적으로 활성화하기 위해 경량 예측 모델이 선호된다.

엣지 인지 스트림 처리: 엣지 인지 스트림 처리는 애플리케이션 실행을 촉진 및 관리하기 위해 병렬 네트워크 연결 시스템에서 실행되는 소프트웨어 솔루션(또는 "처리 토폴로지")을 필요로 한다. 엣지 인지 스트림 처리가 실행되는 시스템은 전통적으로 서버 클러스터이지만 어떤 조합의 네트워크 연결 장치가 될 수도 있다. 예를 들어 클러스터를 수정하는 장치는 이종이고 물리적으로 분산될 수 있다.

서버 클러스터의 일반적인 시나리오는 대부분의 빅 데이터 스트림이 웹 분석 애플리케이션에서 수신된 것이었다는 사실에 근거하지만 이종 및 지역적 분산 노드에서 엣지 인지 스트림 처리를 실행하는 최근 시나리오는 IoT에서 생성 및 분석될 수 있는 거대한 스트림에 기인한다. 엣지 인지 스트림 처리에 대한 중요한 과제는 이른바 처리 토폴로지의 배포를 최적화하는 것이다. 기존 솔루션은 토폴로지 작업 간의 데이터 트래픽 및 호스팅 서버와 네트워크 연결에 대한 상태 정보를 기반으로 배포를 최적화하려고 노력해 왔다. 그러나 다수의 IoT 시나리오에서, 중요한 낮은 지연시간 요구사항은 처리 토폴로지의 엣지(즉, 처리 단계와 외부 IT 또는 IoT 엔티티(예: 작동기 또는 데이터베이스) 사이)에서 나타난다. 그러므로 "엣지-인지" 처리 기법은 배포 최적화 중에 일정한 양질의 서비스 요구사항을 목표로 한다.

표준-호환 IoT 플랫폼: 표준 호환 IoT 플랫폼은 애플리케이션에서 IoT 설치의 복잡성을 숨김으로써 스마트 애플리케이션의 쉬운 개발을 가능하게 지원할 것이다. 그러므로 표준 호환 미들웨어 구성요소는 애플리케이션에 단일 접촉점을 제공하고 기본 장치 설치와 분리되도록 설계될 수 있다. 한편 이들은 대용량 IoT 장치 및 게이트웨이와 활발하게 통신을 주고 받으며 IoT 애플리케이션 실행을 위한 정보를 취득할 수 있다. 효율적인 데이터 모델(예: NGSI)에 대한 일부 기술 표준은 표준 호환 미들웨어 구성요소의 이행을 촉진할 수 있다.

2.1 연결성

기능		비고
실시간 상황 처리	X	실시간 감지수행 포함
다중 시스템 연결성	X	여러 시스템에 연결
원격 기능	X	제품 외부에 상주하는 기능
모든 대역폭/프로토콜에 대한 적용성	X	제공 대역폭/프로토콜에 맞춰 재구성→ HW에서 SW로 전환
새로운 연결성 표준으로 업그레이드 가능성		SW를 통해 새로운 연결성 표준으로 업그레이드할 수 있는 기능
합법적 감청 기능	X	
원격 액세스	X	
인증 및 액세스 제어	X	
신뢰성 및 무결성	X	

2.2 처리

기능		비고
온보드 분석	X	
오프보드 분석	X	
기계 학습	X	
맥락화	X	
익명화	X	
정보 매시업	X	
의미론적 상호 운용성	X	
장치의 동적 구성	X	자가 치유/복원성에 대한 장치의 동적 구성
동적 구성가능성	X	변경 요구사항에 따라 장치가 자체적으로 또는 시스템을 통해 동적으로 구성 가능해질 필요
데이터 소유권 추적	X	
집단 인지	X	

2.3 메모리

기능		비고
디지털 제품 메모리		전체 수명주기, 제품 내력
패턴 인지	X	인공 지능/기계 학습 기반
기능 데이터	X	분석용

2.4 감지

기능		비고
감지 기능을 갖춘 장치 수 증가에 대응	X	
감지 데이터의 중재 교환	X	
데이터의 신뢰성	X	
원시 데이터의 정리	X	
초정밀 위치 기반 기능	X	
개인정보보호	X	
데이터의 무결성	X	
인증을 요하는 복잡한 센서	X	
센서 재구성 기능	X	

2.5 조치

제어 인터페이스 장치

기능		비고
교정	X	
장치 그룹의 제어	X	런타임 및 구성
장치의 동적 구성	X	동적 장치 온보딩/그룹에 지정
컨텍스트에 따라 장치가 제어되는 방식 적용	X	
안전성 요구사항	X	
인증 및 액세스 제어와 권한 부여	X	
플로어 제어	X	시스템을 실제로 제어하도록 허락된 사람들과 그 인계 메커니즘
집단/자체 최적화 제어 지능	X	
보안의 집단 제어	X	
컨텍스트 인지 제어	X	

사용자 I/O

기능		비고
촉각 인터페이스		
다중 장치 사용자 인터페이스	X	
가상 모델링	X	
시뮬레이션	X	
접근성	X	장애인용
증강 현실	X	예: 안경
사용성 및 사용자 경험	X	

2.6 보안

기능		비고
엔드 투 엔드 정책 관리	X	모든 정책 통합
가용 물리적 자원 및 보안성에 대해 최적화된 프레임워크	X	가용 물리적 자원/보안 강건성에 대해 최적화된 프레임워크(ISO 27001에서는 계획-실천-확인-조치) ISO 27001)
복원성	X	가상 물리 공격 포함
장애 허용 능력	X	가상 물리 공격 포함
시스템 위협 탐지 및 대응	X	OODA 관찰-방향설정-결정-실행
장치의 모니터링	X	
협조 및 위협 분석	X	
ID 관리	X	연합 ID 관리, 시스템 간 ID 상관관계, …
장치의 ID 보안	X	
인증 관리	X	데이터의 책임/부인 방지
이상 탐지	X	

3. 차세대 지원 기술

	차세대 지원 기술		비고
연결성	차세대 위성 연결을 위한 전송 계층 프로토콜	X	보다 높은 대역폭, 높은 지연시간
	5세대 셀룰러 액세스(5G)	X	
	저전력 무선 액세스 (LPWAN)	X	
처리	시스템 구성 및 동적 구성	X	
	데이터 맥락화	X	
	자율 데이터 교환	X	
	센서 융합 기술	X	
	기계 학습	X	
	가상화	X	
메모리	디지털 제품 메모리	X	
감지	초정밀 위치 기술	X	

	차세대 지원 기술		비고
조치	증강 현실	X	
	가상 현실	X	
	촉각 인터넷	X	
보안	사물의 ID	X	
	준동형 암호화	X	
	검색 가능 암호화	X	
	신뢰 구축	X	
	보안화 시스템 협업 기술	X	
	사용 제어를 통한 개인정보보호	X	
	지속적인 보안 감사	X	
	IoT용 IAM 기술	X	ID 및 액세스 관리
	애플리케이션 격리 및 보안 경계 기술	X	

4. 필요한 미래 표준

	표준 요구사항		비고
연결성	5G 표준의 실현	X	
	표준 위성과 장치 간의 보다 높은 대역폭/요구 지연시간을 지원하기 위한 새로운 전송 계층 프로토콜에 대한 표준	X	
	IoT 장비가 새로운 연결성 표준으로 업데이트하는 기능을 갖추도록 하는 표준	X	
처리	정보 교환 모델	X	
	의미론 메타데이터 정의 표준 및 모델	X	
	데이터 교환 모델 및 인터페이스와 관련 표준	X	
	자율 데이터 교환 프로파일 및 교환 메커니즘	X	
	메타데이터 주석 모델 및 인터페이스	X	
	맥락화 정보 모델	X	
	메타데이터 컨텍스트 표준	X	
메모리	디지털 제품 메모리의 표준화	X	

	표준 요구사항		비고
감지	메타데이터에 대한 표준	X	
	초정밀 위치 기반 기술에 대한 추상화 기술	X	
	센서 데이터 개인정보보호 표준	X	최종 소비자/소비자의 옵트인/옵트아웃
	센서 융합 표준	X	센서 관찰을 추상화하는 센서 메타 모델 개발 표준. 이 표준은 정형화되지 않은 산발적 데이터를 고급 도메인 지식으로 바꿀 수 있는 기반이 된다.
조치	제어 인터페이스 장치 그룹을 고유하게 식별하는 표준 템플릿	X	
	시스템 간의 IoT 사용자 I/O를 일반화하는 일반 표준	X	
	고유한 IoT 접근성 요구사항에 대한 표준	X	일반적인 인간/컴퓨터 I/O를 뛰어넘는 고급 IoT 서비스 반영
보안	소셜 시스템의 ID 연합 표준	X	
	가상 물리 공격 보호 표준	X	
	동시 연결을 갖춘 다중 시스템에서 장치 ID에 대한 표준	X	예: W3C의 국제화 자원 식별자(IRI)
	플랫폼 무결성에서 신뢰를 구축하기 위한 표준 프로토콜	X	
	협업 보안 프레임워크	X	상호 의존적인 시스템 간의 사이버 위협 분석 교환 활성화
	상호 의존적인 시스템 간 보안 기능 평가를 활성화하는 성숙 모델	X	

부록 F – 사용 사례

소셜 센서

1. 사용 사례의 기술

1.1 사용 사례의 명칭

소셜 센서

1.2 사용 사례의 목적 및 범위

1.2.1 범위

이 사용 사례는 데이터 수집, 데이터 집계 및 사용자에 대한 데이터 제공에 대해 기술한다. 이 사용 사례에서는 분석을 다루지 않는다.

1.2.2 목적

신뢰, 개인정보보호, 데이터 소유권 및 상호 운용성에 대해 설명한다.

1.3 사용 경험담

1.3.1 사용 사례의 요약

소셜 센서 서비스의 목적은 풍부한 사용자 생성 데이터를 수집하는 것이며, 이 데이터는 익명화되고 편집되어 전체 커뮤니티에 대한 (개인적인 행동 대비) 효용성을 나타낼 수 있다. 이 사용 사례는 [62]에서 제시하는 IoT 시나리오에서 도출된 것이다.

1.3.2 사용 사례의 특성

정부 중점

1.3.3 전체 기술

날이 갈수록 사람이 가정이나 주변 환경에서 중요 매개변수를 모니터링할 가능성이 커져간다. 이에 대한 한 가지 예는 bwired.nl 웹 사이트에서 제공되며 여기에서는 각 사용자별로 다수의 센서 모니터링 및 가정 및 주변 지역의 기능(예: 지역의 실외 온도, 습도 또는 오염, 소음 및 기타 요소에 대한 다양한 매개변수)에 관련된 측정 매개변수를 사용할 수 있다.

소셜 센서 서비스의 목적은 풍부한 사용자 생성 데이터를 수집하는 것이며, 이 데이터는 익명화되고 편집되어 전체 커뮤니티에 대한 (개인적인 행동 대비) 효용성을 나타낼 수 있다. 예를 들어 일부 매개변수에 대한 중간 또는 평균값을 계산하고 시민들이 매개변수 값 모음을 “평균 값 모음”과 비교할 수 있도록 지원할 수 있다. 이런 방식으로 개인이 적정 전력 소비 범위를 확립하는 것과 같은 “모범 시민 행동방식”의 표준 양식을 준수하는 지점을 확인할 수 있다. 사실 이런 유형의 데이터 분석 가용성은 선의의 경쟁을 촉진하고 전체로서 공동체에 기여할 수 있는 것으로 여겨지는 기존 및 새로운 실행 방법을 개선하고 준수하도록 고무할 수 있다. 또 다른 잠재적인 유용성은 사용자 생성 데이터를 통합하여 시민들이 직접 수집한 데이터 및 매개변수와 공공 당국이 제공하는 공식적인 데이터를 비교하도록 하는 것이다. 한 가지 중요한 사례는 대도시에서 모니터링하는 공식적인 데이터와 비교하여 지역 오염을 제어하는 것이다. 이 소셜 서비스는 환경 모니터링, e-정부 및 지능형 가정에 적용될 수 있다.

“소셜 센서” 서비스는 특정 환경(예: 가정)에서 센서에 의해 수집된 측정값 및 정보를 집계하고 대규모 컨텍스트(예: 지역)에서 공유하는 것을 목적으로 한다.

데이터, 측정값 및 정보는 환경 운영 방식과 관련된 지식(예: 패턴 분석)을 도출하기 위해 사용될 수 있다. 중요한 특징이라면 사용자와 센서 네트워크의 소유자가 대규모 커뮤니티에서 데이터를 공유하는 데 동의한다는 것이다. 이 서비스의 특징은 서로 다른 관리 영역(예: 가정, 회사, 공공 당국 및 정부, 소셜 네트워크)의 센서에서 발생한 데이터의 액세스/사용 필요성 및 가능성이다. 이 서비스는 대규모 커뮤니티에서 사용하기 위해 광범위한 독립적인 센서 네트워크가 공조할 수 있는 방식의 예를 보여준다.

이 사용 사례의 3가지 행위자는 다음과 같다.

1. 센서 제공자는 일상 생활이나 비즈니스의 수 많은 측면을 모니터링하는 가정이나 사무실 네트워크를 실제로 소유하고 관리하는 행위자이다. 여기에는 수도와 전기 사용량에서부터 홍보전단을 뿌리기 위해 사람이 문을 두드리는 빈도 및 “가정”을 중심으로 하는 기타 다수의 활동까지의 일들이 포함된다. 데이터는 사람이 집에서 생활하는 행동을 나타내며 이 데이터를 저장하고 분석하면 가족의 사회 생활과 비즈니스 운영이 일정 시간에 걸쳐 어떻게 발전하는지에 대한 매우 유용한 정의를 얻을 수 있다. 데이터는 센서 제공자에 의해 집계자에게 푸시되거나 집계자가 직접 가져올 수 있다.

2. 집계자(aggregator)는 실제로 풍부한 데이터를 수집하여 적절하게 취급하는 행위자이다. 집계자의 임무는 데이터 표현 간의 차이를 통제하고 데이터를 익명화한 후 의미 있는 방식으로 데이터를 구성하는 것이다. 집계자는 분산 센서 네트워크의 제공자이거나 공공시설, 네트워크 운영자 또는 공공 당국/정부 기관과 같은 기타 데이터 수집 네트워크의 소유자일 수 있다.

3. 사용자가 최종적으로 모든 정보를 이용한다. 또한 사용자는 시민 또는 매우 특정한 개인 하위 집단(예: 특정 지역의 주민)의 사회적 행동방식을 판별하기 위해 소싱된 데이터를 사용하는 회사나 프로그래머일 수 있다.

이 서비스의 개념은 간단하다(그림 F-1 참조). 센서 제공자가 정보 생성자이고 집계자가 이를 수집 및 익명화하여 다양한 데이터 형식 및 정보를 맞춤화한다. 서로 다른 센서 제공자로부터 수집된 데이터가 집계되고 사용자에게 서로 다른 뷰 및 추론된 정보가 제공될 수 있다. 데이터 세트 또한 일반화되어 가용화(즉, 서로 다른 데이터 형식을 일반화하여 생성할 수 있음)된다. 사용자는 이 데이터에 액세스하거나 이를 행동방식에 대한 벤치마크로 활용할 수 있다. 집계자는 또한 자체 센서 인프라를 통합하여 보다 광범위한 데이터 세트를 생성할 수 있다. 애플리케이션의 범위는 평균 도시 온도 파악을 위해 시민들의 온도계 눈금을 이용하는 것과 같이 매우 단순한 것부터 도시에서 군중의 이동을 추적하는 동작 센서 또는 모바일 운영자 데이터와 같이 매우 복잡한 것까지 걸쳐 있다.

소셜 센서 서비스는 개념적으로는 단순하지만 3가지 요인 때문에 복잡하다. 첫째, 이종 소스(즉, 기능, 데이터 표현 및 형식이 각기 다른 서로 다른 센서)를 일반화할 필요가 있다. 둘째, 개인 부문(즉, 사용자가 데이터 값을 특정 사용자에게 매핑하도록 허용하는 데이터)에 속한 데이터를 익명화할 필요가 있다. 셋째, 서로 다른 컨텍스트 및 부문에서 데이터를 통합하여 통신, 상호 연동 및 데이터 신뢰성에 관련된 문제에 대응할 필요가 있다.

1.4 사용 사례의 도표

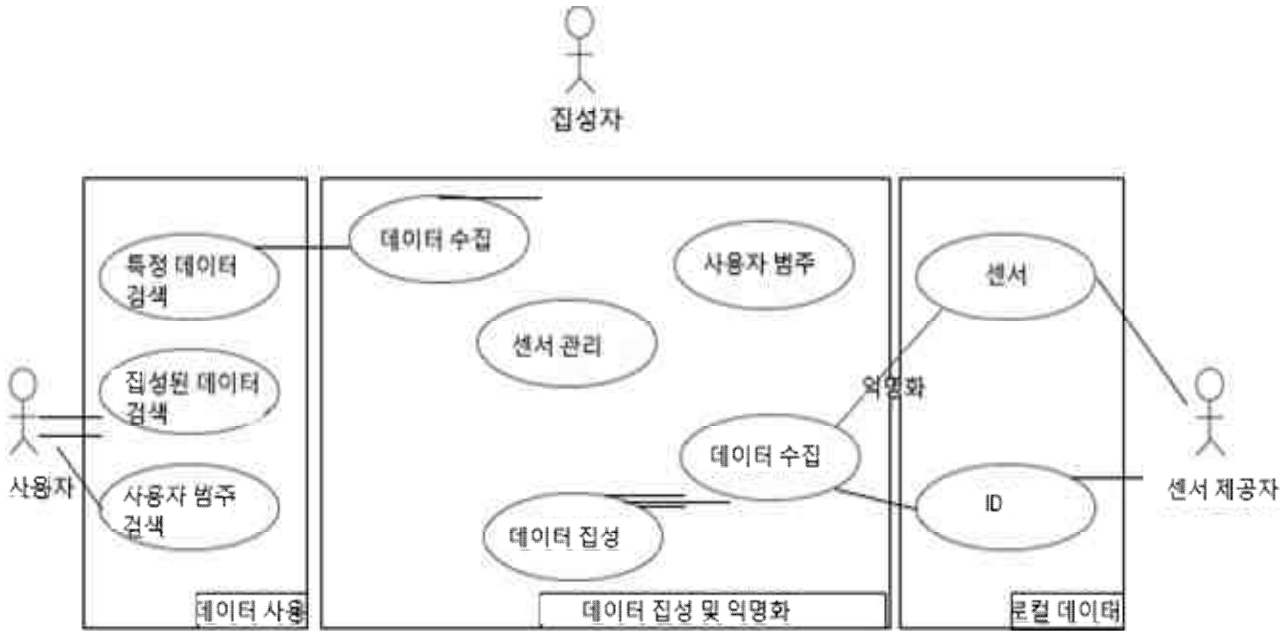


그림 F-1 | 소셜 센서 서비스의 행위자와 사용 사례

1. 사용 사례의 조건

1.5.1 전제

센서 제공자가 데이터 집계자에게 자신들의 데이터를 정직하게 제공할 의향이 있다.

1.5.2 선결요건

- 서로 다른 센서 제공자에 의해 생성된 데이터가 통합될 수 있다.
- 수집된 데이터에 대해 적정 익명화를 이행할 수 있다.
- 센서 제공자가 그들이 제공하는 데이터를 추적 및 통제하는 기능이 제공될 필요가 있을 수 있다.

1.6 사용 사례에 대한 추가 정보

1.6.1. 최신 상태

가정과 사무실의 고정 센서로부터 데이터를 수집하는 통신 기술은 현재 사용이 가능하지만 이 통신 기술은 주택이나 사무실 상공을 비행하는 드론에 설치된 센서 등의 다른 센서에서 데이터를 수집하기에는 충분하지 않을 수 있다.

2. 특징적 기능에 대한 매핑

2.1 연결성

기능		비고
실시간 상황 처리		실시간 감지수행 포함
다중 시스템 연결성	X	여러 시스템에 연결
원격 기능		제품 외부에 상주하는 기능
모든 대역폭/프로토콜에 대한 적용성		제공 대역폭/프로토콜에 맞춰 재구성→ HW에서 SW로 전환
새로운 연결성 표준으로 업그레이드 가능성		SW를 통해 새로운 연결성 표준으로 업그레이드할 수 있는 기능
합법적 감청 기능		
원격 액세스	X	
인증 및 액세스 제어	X	
신뢰성 및 무결성	X	

2.2 처리

기능		비고
온보드 분석	X	
오프보드 분석	X	
기계 학습	X	
맥락화	X	
익명화	X	
정보 매시업	X	
의미론적 상호 운용성	X	
장치의 동적 구성		자가 치유/복원성을 위한 장치의 동적 구성
동적 구성가능성		변경 요구사항에 따라 장치가 자체적으로 또는 시스템을 통해 동적으로 구성 가능해질 필요
데이터 소유권 추적	X	
집단 인지		

2.3 메모리

기능	비고
디지털 제품 메모리	전체 수명주기, 제품 내력
패턴 인지	인공 지능/기계 학습 기반
기능 데이터	분석용

2.4 감지

기능		비고
감지 기능을 갖춘 장치 수 증가에 대응	X	
감지 데이터의 중재 교환	X	
데이터의 신뢰성	X	
원시 데이터의 정리	X	
초정밀 위치 기반 기능		
개인정보보호	X	
데이터의 무결성	X	
인증을 요하는 복잡한 센서		
센서 재구성 기능		

2.5 조치

제어 인터페이스 장치

기능		비고
교정	X	
장치 그룹의 제어		런타임 및 구성
장치의 동적 구성	X	동적 장치 온보딩/그룹에 지정
컨텍스트에 따라 장치가 제어되는 방식 적용		
안전성 요구사항		
인증 및 액세스 제어 및 인증	X	
플로어 제어	X	시스템을 실제로 제어하도록 허락된 사람들과 그 인계 메커니즘
집단/자체 최적화 제어 지능		
보안의 집단 제어		
컨텍스트 인지 제어		

사용자 I/O

기능	비고
촉각 인터페이스	
다중 장치 사용자 인터페이스	
가상 모델링	
시뮬레이션	
접근성	장애인용
증강 현실	예: 안경
사용성 및 사용자 경험	

2.6 보안

기능		비고
엔드 투 엔드 정책 관리	X	모든 정책 통합
가용 물리적 자원 및 보안성에 대해 최적화된 프레임워크		가용 물리적 자원/보안 강건성에 대해 최적화된 프레임워크(ISO 27001에서는 계획-실천-확인-조치) ISO 27001)
복원성		가상 물리 공격 포함
장애 허용 능력		가상 물리 공격 포함
시스템 위협 탐지 및 대응	X	OODA 관찰-방향설정-결정-실행
장치의 모니터링	X	
협조 및 위협 분석		
ID 관리	X	연합 ID 관리, 시스템 간 ID 상관관계, …
장치의 ID 보안	X	
인증 관리	X	데이터의 책임/부인 방지
이상 탐지		

2. 차세대 지원 기술

	차세대 지원 기술		비고
인터넷 접속	차세대 위성 연결을 위한 전송 계층 프로토콜		보다 높은 대역폭, 높은 지연시간
	5세대 셀룰러 액세스(5G)		
	저전력 무선 액세스 (LPWAN)	X	

	차세대 지원 기술		비고
처리	시스템 구성 및 동적 구성		
	데이터 맥락화	X	
	자율 데이터 교환	X	
	센서 융합 기술	X	
	기계 학습	X	
	가상화		
메모리	디지털 제품 메모리		
감지	초정밀 위치 기술		
조치	증강 현실		
	가상 현실		
	촉각 인터넷		
보안	사물의 ID	X	
	준동형 암호화	X	
	검색 가능 암호화	X	
	신뢰 구축	X	
	보안화 시스템 협업 기술	X	
	사용 제어를 통한 개인정보보호	X	
	지속적인 보안 감사		
	IoT용 IAM 기술	X	ID 및 액세스 관리
	애플리케이션 격리 및 보안 경계 기술		

4. 필요한 미래 표준

	표준 요구사항	비고
연결성	5G 표준의 실현	
	표준 위성과 장치 간의 보다 높은 대역폭/요구 지연시간을 지원하기 위한 새로운 전송 계층 프로토콜에 대한 표준	
	IoT 장비가 새로운 연결성 기준으로 업데이트하는 기능을 갖추도록 하는 표준	

	표준 요구사항		비고
프로세싱	정보 교환 모델	X	
	의미론 메타데이터 정의 표준 및 모델	X	
	데이터 교환 모델 및 인터페이스와 관련 표준	X	
	자율 데이터 교환 프로파일 및 교환 메커니즘	X	
	메타데이터 주석 모델 및 인터페이스		
	맥락화 정보 모델	X	
	메타데이터 컨텍스트 표준		
메모리	디지털 제품 메모리의 표준화		
감지	메타데이터에 대한 표준	X	
	초정밀 위치 기반 기술에 대한 추상화 기술		
	센서 데이터 개인정보보호 표준		최종 소비자/소비자의 옵트인/옵트아웃
	센서 융합 표준	X	센서 관찰을 추상화하는 센서 메타 모델 개발 표준. 이 표준은 정형화되지 않은 산발적 데이터를 고급 도메인 지식으로 바꿀 수 있는 기반이 된다.
조치	제어 인터페이스 장치 그룹을 고유하게 식별하는 표준 템플릿		
	시스템 간의 IoT 사용자 I/O를 일반화하는 일반 표준		
	고유한 IoT 접근성 요구사항에 대한 표준		일반적인 인간/컴퓨터 I/O를 뛰어넘는 고급 IoT 서비스 반영
보안	소셜 시스템의 ID 연합 표준	X	
	가상 물리 공격 보호 표준	X	
	동시 연결을 갖춘 다중 시스템에서 장치 ID에 대한 표준	X	예: W3C의 국제화 자원 식별자(IRI)
	플랫폼 무결성의 신뢰를 구축하기 위한 표준 프로토콜	X	
	협업 보안 프레임워크	X	상호 의존적인 시스템 간의 사이버 위협 분석 교환 활성화
	상호 의존적인 시스템 간에 보안 기능을 평가할 수 있는 성숙 모델	X	

부록 G - 사용 사례

특수한 도움이 필요한 사람들을 포함하는 승객들의 대중 교통 탑승경험 개선

1. 사용 사례의 기술

1.1 사용 사례의 명칭

특수한 도움이 필요한 사람들을 포함하는 승객들의 대중교통 탑승경험 개선

1.2 사용 사례의 범위 및 목적

1.2.1 범위

본 사용 사례는 IoT 시스템의 적용성을 취급한다.

1.2.2 목적

분석, 기계 학습 및 개인정보보호에 관한 요구사항을 기술한다.

1.3 사용 경험담

1.3.1 사용 사례의 요약

IoT 시스템은 특수한 도움이 필요한 사람들을 포함하여 승객이 필요 및 선호를 토대로 목적지까지의 경로를 선택하고 승객이 예정 경로대로 이동 중인지 확인할 수 있도록 지원한다. 또한 승객에게 보다 나은 서비스를 제공하기 위해 버스 및 기차와 같은 대중교통의 운행을 조정할 수 있다. 본 사용 사례는 [63]에서 제시하는 IoT 시나리오를 확장한 것이다.

1.3.2 사용 사례의 특성

소비자 중심

1.3.3 전체 기술

본 사용 사례는 보다 자율적인 방식으로 발전 및 실행되어 보다 신뢰성이 있고 스마트한 IoT 시스템을 취급한다.

이 IoT 시스템은 특수한 도움이 필요한 사람들을 포함한 승객에 대한 서비스를 지원한다. 승객은 시스템에 출발지, 목적지 및 탑승 일자와 시간을 입력한다. 그러면 시스템이 승객이 제공한 정보와 필요 및 선호사항을 토대로 경로를 검색한다. 이 시스템은 또한 승객이 예정대로 이동 중인지를 확인하는 데 사용되는 검사 지점도 선택한다. 예정대로 이동하지 않는 것이 발견되면 IoT 시스템에 의해 알림 경보가 생성된다. 검사 지점에서 확인을 위해 실제 사용자 데이터와 버스 운영자, 철도 운영자 및 경찰과 같은 교통 관련 이해당사자로부터 취득된 데이터를 분석하여 평균 이동 시간에 대한 데이터가 취합된다. IoT 시스템에 의해 사용되는 데이터에는 승객의 교통 스케줄, 위치 및 수단이 포함되며 이들은 개인정보보호 관련 데이터이다. IoT 시스템은 대중 교통 시스템과 협업하여 그런 시스템에 의한 승객 필요 서비스 개선을 도모할 수 있다. 예를 들어 버스 운영자는 IoT 시스템과 협업하여 휠체어 승차 가능 버스 경로를 재조정하여 휠체어를 탄 승객에게 대중교통 서비스를 제공할 수 있다.

IoT 시스템은 운영 경험을 토대로 학습할 수 있을 것이며 상황별 지식 취득 및 분석을 통해 동작 방식에 영향을 줄 가능성이 있는 상황 및 사건을 시스템이 인지하도록 한다. 적응 선택 접근방법은 현실세계의 동태로 인해 유입되는 불확실성과 휘발성을 관리할 것이다.

관리 결정과 런타임 적용성은 IoT 시스템을 구성하는 사물의 보안, 신뢰, 관리 측면, 위치, 관계, 정보 및 컨텍스트별 속성을 토대로 할 것이다.

1.4 사용 사례의 도표

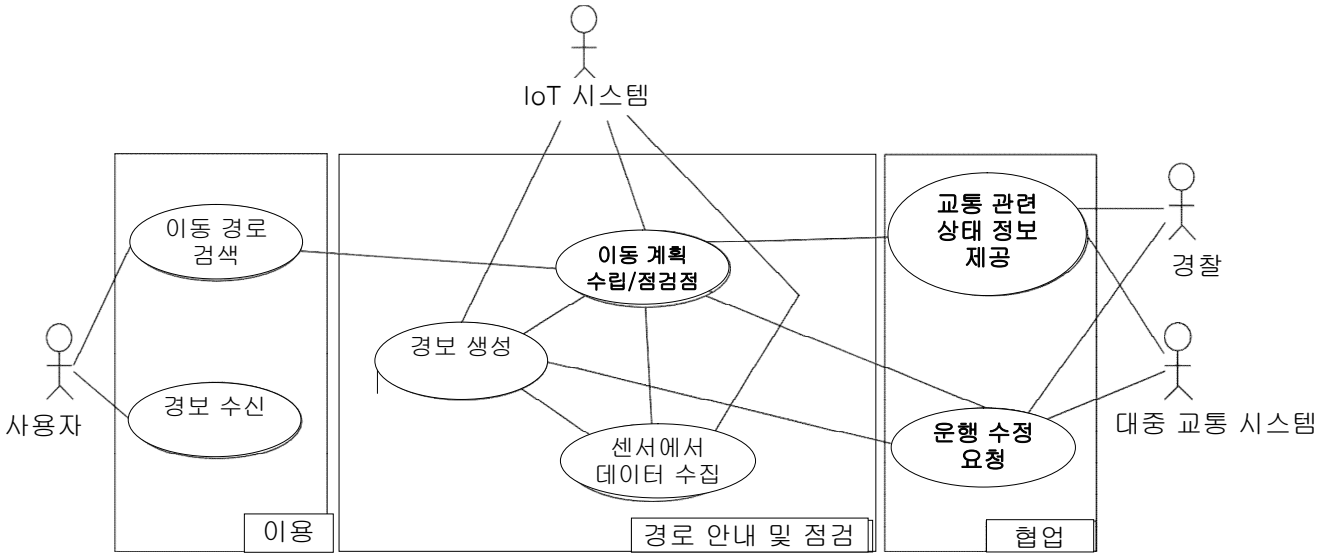


그림 G-1 | 탑승 경험의 개선의 행위자 및 사용 사례

1.5 사용 사례의 조건

1.5.1 전제

각 검사 지점에서 승객의 통과를 탐지하기 위해 센서와 같은 적정 장비가 이미 배포되어 있다. 승객의 스마트폰만으로 충분할 수 있다.

1.5.2 선결요건

승객의 개인정보보호 필요가 있다.

1.6 사용 사례에 대한 추가 정보

1.6.1 최신 상태

승객의 선호(최저 운임, 최단 이동 시간)에 따른 승객의 경로 검색 시스템이 이미 존재한다. 현재 경로 검색 시스템에서 평균 이동 시간 데이터가 데이터 분석에 의해 유지되는지 여부는 확실하지 않다.

2. 특징적인 기능에 대한 매핑

2.1 연결성

기능		비고
실시간 상황 처리	X	실시간 감지수행 포함
다중 시스템 연결성		여러 시스템에 연결
원격 기능		제품 외부에 상주하는 기능
모든 대역폭/프로토콜에 대한 적용성		제공 대역폭/프로토콜에 맞춰 재구성→ HW에서 SW로 전환
새로운 연결성 표준으로 업그레이드 가능성		SW를 통해 새로운 연결성 표준으로 업그레이드할 수 있는 기능
합법적 감청 기능		
원격 액세스	X	
인증 및 액세스 제어	X	
신뢰성 및 무결성	X	

. . . . . .

2. 처리

기능		비고
온보드 분석	X	
오프보드 분석	X	
기계 학습	X	
맥락화	X	
익명화	X	
정보 매시업	X	
의미론적 상호 운용성	X	
장치의 동적 구성		자가 치유/복원성을 위한 장치의 동적 구성
동적 구성가능성		변경 요구사항에 따라 자체 및 시스템에 의해 장치가 동적으로 구성 가능할 필요가 있다.
데이터 소유권 추적	X	
집단 인지		

. . . . . .

2.3 메모리

기능	비고
디지털 제품 메모리	전체 수명주기, 제품 내력
패턴 인지	인공 지능/기계 학습 기반
기능 데이터	분석용

. . . . . .

2.4 감지

기능		비고
감지 기능을 갖춘 장치 수 증가에 대응	X	
감지 데이터의 중재 교환	X	
데이터의 신뢰성	X	
원시 데이터의 정리	X	
초정밀 위치 기반 기능	X	
개인정보보호	X	
데이터의 무결성	X	
인증을 요하는 복잡한 센서		
센서 재구성 기능		

2.5 조치

제어 인터페이스 장치

기능		비고
교정	X	
장치 그룹의 제어		런타임 및 구성
장치의 동적 구성	X	동적 장치 온보딩/그룹에 지정
컨텍스트에 따라 장치가 제어되는 방식 적용	X	
안전성 요구사항	X	
인증 및 액세스 제어 및 인증	X	
플로어 제어		시스템을 실제로 제어하도록 허락된 사람들과 그 인계 메커니즘
집단/자체 최적화 제어 지능		
보안의 집단 제어		
컨텍스트 인지 제어	X	

사용자 I/O

기능		비고
촉각 인터페이스		
다중 장치 사용자 인터페이스	X	
가상 모델링		
시뮬레이션	X	
접근성	X	장애인용
증강 현실		예: 안경
사용성 및 사용자 경험		

2.6 보안

기능		비고
엔드 투 엔드 정책 관리	X	모든 정책 통합
가용 물리적 자원 및 보안성에 대해 최적화된 프레임워크		가용 물리적 자원/보안 강건성에 대해 최적화된 프레임워크(ISO 27001에서는 계획-실천-확인-조치) ISO 27001)
복원성		가상 물리 공격 포함
장애 허용 능력	X	가상 물리 공격 포함
시스템 위협 탐지 및 대응	X	OODA 관찰-방향설정-결정-실행
장치의 모니터링	X	
협조 및 위협 분석	X	
ID 관리	X	연합 ID 관리, 시스템 간 ID 상관관계, …
장치의 ID 보안	X	
인증 관리	X	데이터의 책임/부인 방지
이상 탐지		

3. 차세대 지원 기술

	차세대 지원 기술		비고
연결성	차세대 위성 연결을 위한 전송 계층 프로토콜		보다 높은 대역폭, 높은 지연시간
	5세대 셀룰러 액세스(5G)		
	저전력 무선 액세스 (LPWAN)		
처리	시스템 구성 및 동적 구성		
	데이터 맥락화	X	
	자율 데이터 교환	X	
	센서 융합 기술		
	기계 학습	X	
	가상화		
메모리	디지털 제품 메모리		
감지	초정밀 위치 기술	X	

	차세대 지원 기술		비고
조치	증강 현실	X	
	가상 현실		
	촉각 인터넷		
보안	사물의 ID	X	
	준동형 암호화	X	
	검색 가능 암호화	X	
	신뢰 구축	X	
	보안화 시스템 협업 기술	X	
	사용 제어를 통한 개인정보보호	X	
	지속적인 보안 감사	X	
	IoT용 IAM 기술	X	ID 및 액세스 관리
	애플리케이션 격리 및 보안 경계 기술		

4. 필요한 미래 표준

	표준 요구사항		비고
연결성	5G 표준의 실현		
	표준 위성과 장치 간의 보다 높은 대역폭/요구 지연시간을 지원하기 위한 새로운 전송 계층 프로토콜에 대한 표준		
	IoT 장비가 새로운 연결성 표준으로 업데이트하는 기능을 갖추도록 하는 표준		
프로세싱	정보 교환 모델	X	
	의미론 메타데이터 정의 표준 및 모델	X	
	데이터 교환 모델 및 인터페이스와 관련 표준	X	
	자율 데이터 교환 프로파일 및 교환 메커니즘	X	
	메타데이터 주석 모델 및 인터페이스		
	맥락화 정보 모델	X	
	메타데이터 컨텍스트 표준		
메모리	디지털 제품 메모리의 표준화		

	표준 요구사항		비고
감지	메타데이터에 대한 표준	X	
	초정밀 위치 기반 기술에 대한 추상화 기술	X	
	센서 데이터 개인정보보호 표준		최종 소비자/소비자의 옵트인/옵트아웃
	센서 융합 표준		센서 관찰을 추상화하는 센서 메타 모델 개발 표준. 이 표준은 정형화되지 않은 산발적 데이터를 고급 도메인 지식으로 바꿀 수 있는 기반이 된다.
조치	제어 인터페이스 장치 그룹을 고유하게 식별하는 표준 템플릿		
	시스템 간의 IoT 사용자 I/O를 일반화하는 일반 표준		
	고유한 IoT 접근성 요구사항에 대한 표준		일반적인 인간/컴퓨터 I/O를 뛰어넘는 고급 IoT 서비스 반영
보안	소셜 시스템의 ID 연합 표준	X	
	가상 물리 공격 보호 표준	X	
	동시 연결을 갖춘 다중 시스템에서 장치 ID에 대한 표준	X	예: W3C의 국제화 자원 식별자(IRI)
	플랫폼 무결성에서 신뢰를 구축하기 위한 표준 프로토콜	X	
	협업 보안 프레임워크	X	상호 의존적인 시스템 간의 사이버 위협 분석 교환 활성화
	상호 의존적인 시스템 간 보안 기능 평가를 활성화하는 성숙 모델	X	

부록 H – 사용 사례

커넥티드 카

1. 사용 사례의 기술
1.1 사용 사례의 명칭

커넥티드 카

1.2 사용 사례의 범위 및 목적

1.2.1 범위

본 사용 사례의 범위는 통신 액세스 기술을 고려하여 V2X 서비스에 대한 사용 사례 및 연관된 잠재적 요구사항을 기술하는 것이다.

1.2.2 목적

목적은 SDO에 정의된 것과 같은 통신 액세스 기술을 고려하여 V2X 서비스에 대한 사용 사례 및 연관된 잠재적 요구사항을 기술하는 것이다. 조사 대상 V2X(V2V, V2I 및 V2P)에 대한 필수 사용 사례 및 정의되는 요구사항은 다음과 같다.

- V2V: 차량 간 무선 통신 취급
- V2P: 차량과 개인 휴대 장치(예: 보행자, 사이클 선수, 운전자 또는 승객이 휴대하는 휴대용 단말기) 간 무선 통신 취급
- V2I: 차량과 도로변 장치 간의 무선 통신 취급

본 사용 사례에는 안전 및 비안전 측면이 포함된다.

1.3 사용 경험담

1.3.1 사용 사례의 요약

본 조사에서 차량 대 만물(V2X)이라고 하는 차량 관련 통신유형은 다음의 3가지이다.

- 차량대차량(V2V) 통신
- 차량대인프라(V2I) 통신
- 차량대보행자(V2P) 통신

1.3.2 차량대차량(V2V)

스마트 및 보안 IoT 플랫폼에서 권한, 권한 부여 및 근접 기준이 충족될 때 상호 근접한 스마트 개체가 스마트 및 보안 IoT 플랫폼을 이용하여 V2V 관련 정보를 교환할 수 있다. 서비스 제공자가 근접 기준을 구성한다. 그러나 V2V 서비스를 지원하는 스마트 개체가 스마트 및 보안 IoT 플랫폼에 의해 제공되거나 제공되지 않을 때 그런 정보를 교환할 수 있다.

V2V 애플리케이션을 지원하는 스마트 개체는 애플리케이션 계층 정보(예: 위치, 동태 및 V2V 서비스의 일부인 속성)를 전송한다. V2V 페이로드는 서로 다른 정보 콘텐츠를 수용하기 위해 융통성이 있어야 하며 그런 정보는 서비스 제공자가 제공하는 구성에 따라 주기적으로 전송될 수 있다.

V2V는 대부분 브로드캐스트 기반이다. V2V에는 각 스마트 개체 간에 직접적인 V2V 관련 애플리케이션 정보 교환과, V2V의 직접적인 통신 범위 제한으로 인해 인프라(예: 도로변 장치(RSU))를 통한 각 스마트 개체 간에 V2V 관련 애플리케이션 정보 교환이 이뤄진다.

1.3.3 차량대인프라(V2I)

V2I 애플리케이션을 지원하는 스마트 개체는 애플리케이션 계층 정보를 RSU로 전송한다. RSU는 애플리케이션 계층 정보를 V2I 애플리케이션을 지원하는 스마트 개체 그룹 또는 개별 스마트 개체에 전송한다.

또한 V2N는 한쪽 당사자가 스마트 개체이고 상대측이 서비스 제공 엔티티일 때 양측 모두 V2N 애플리케이션을 지원하고 통신 네트워크를 통해 서로 통신하는 경우 도입된다.

1.3.4 차량대보행자(V2P)

스마트 및 보안 IoT 플랫폼에서 권한, 권한 부여 및 근접 기준이 충족될 때 상호 근접한 스마트 개체가 스마트 및 보안 IoT 플랫폼을 이용하여 V2P 관련 정보를 교환할 수 있다. 서비스 제공자가 근접 기준을 구성한다. 그러나 V2P 서비스를 지원하는 스마트 개체가 스마트 및 보안 IoT 플랫폼에 의해 제공되지 않을 때에도 그런 정보를 교환할 수 있다.

V2P 애플리케이션을 지원하는 스마트 개체는 애플리케이션 계층 정보를 전송한다. 그런 정보는 V2P 서비스를 지원하는 스마트 개체를 이용하는 차량(예: 보행자 경고) 또는 V2P 서비스를 지원하는 스마트 개체를 이용하는 보행자(예: 차량에 대한 경고)가 전송할 수 있다.

V2P에는 각 스마트 개체 간에 직접적인 V2P 관련 애플리케이션 정보 교환과, V2V의 직접적인 통신 범위 제한으로 인해 인프라(예: 도로변 장치(RSU))를 통한 각 스마트 개체 간에 V2P 관련 애플리케이션 정보 교환이 있다.

1.4 사용 사례의 도표

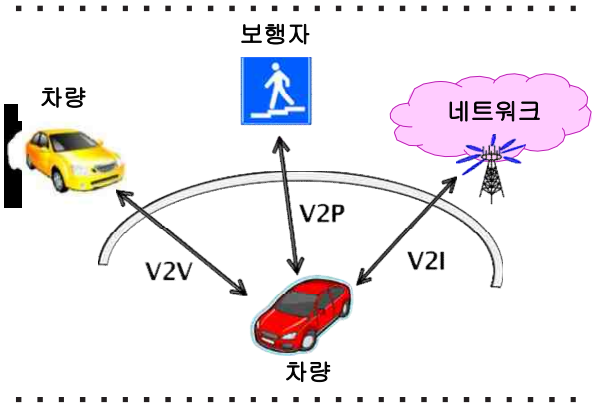


그림 H-1 | 사용 사례의 도표 – 차량대만물

1.5 전방 추돌 경고(FCW)

1.5.1 설명

FCW 애플리케이션은 동일 차선 및 주행 방향에서 교통 흐름의 앞에 있는 원격 차량(RV)과 후미 추돌이 임박한 경우 호스트 차량(HV)의 운전자에게 경고하는 것을 목적으로 한다. V2V 서비스를 사용하는 FCW는 운전자가 주행의 전방 경로에서 후미 차량 추돌을 피하거나 추돌을 완화시키는 것을 목적으로 한다.

1.5.2 선결요건

RV와 HV 모두 V2V 서비스를 지원하고 V2V 서비스를 사용하여 상호 통신을 주고 받을 수 있다.

1.5.3 서비스 흐름

RV V2V 서비스 계층은 현재 위치, 속도, 가속 및 선택적인 예상 궤도를 표시하는 메시지를 주기적으로 브로드캐스팅한다.

RV는 차선 준수 여부 및 추돌 예상 시간을 판별하며 이는 브로드캐스팅 메시지에 반영된다.

통신 액세스 노드가 애플리케이션 계층의 요청에 따라 서로 다른 메시지를 브로드캐스팅한다.

HV와 RV는 메시지를 브로드캐스팅하고 조치를 취할지 여부를 결정한다.

1.5.4 사후 요건

HV 운전자에게 주행 차선 내 전방 차량 존재에 대해 경보를 보내고 주행 경로 전방에서 후미 차량 추돌을 피하거나 완화하기 위한 시정 조치를 취할 수 있도록 한다.

1.5.5 잠재적 요구사항

본 사용 사례에서 도출된 잠재적 요구사항은 다음과 같다.

- 서비스 제공자 네트워크는 V2V 서비스를 지원하는 스마트 개체가 V2V 서비스에 대한 필요에 따라 메시지 전송을 사용할 수 있도록 승인해야 한다.
- V2V 서비스를 지원하는 스마트 개체는 V2V 서비스 계층에 의해 요구될 경우 브로드캐스트 V2V 메시지를 주기적으로 전송할 수 있어야 한다.
- V2V 서비스를 지원하는 스마트 개체는 주기적인 브로드캐스 메시지를 수신할 수 있어야 한다.
- 스마트 및 보안 IoT 플랫폼은 높은 이동 기능(예: 최대 절대 속도 160km/h)을 지원할 수 있어야 한다.
- 스마트 및 보안 IoT 플랫폼은 운전자에게 충분한 응답 시간(예: 4초)을 제공하기에 충분한 통신 범위를 지원할 수 있어야 한다.
- 스마트 및 보안 IoT 플랫폼은 최대 1,200바이트가 될 수 있는 50-300바이트의 메시지 크기를 지원할 수 있어야 한다.
- 스마트 및 보안 IoT 플랫폼은 최대 100ms의 지연시간을 지원할 수 있어야 한다.
- 스마트 및 보안 IoT 플랫폼은 최대 10건의 V2V 메시지/초를 지원할 수 있어야 한다.
- 스마트 및 보안 IoT 플랫폼은 애플리케이션 계층 메시지 재전송을 요구하지 않고도 높은 신뢰성을 지원할 수 있어야 한다.
- V2V 서비스는 사용자/차량 익명성과 전송의 무결성 보호를 지원해야 한다.
- V2V 서비스를 지원하는 스마트 개체는 V2V 메시지 전송과 서로 다른 공공 육상 모바일 네트워크(PLMN)에서 V2V 서비스를 지원하는 다른 스마트 개체 및 서로 다른 국가로부터 이 메시지 수신을 지원할 수 있어야 한다.

1.6 제어 상실 경고(CLW)

1.6.1 설명

CLW 애플리케이션은 HV가 주변 RV에 자체 생성 제어 상실 사건을 브로드캐스팅할 수 있도록 지원한다. 그런 사건 정보를 수신하는 즉시 RV는 사건과의 관련성을 판별한 후 해당할 경우 운전자에게 경고를 보낸다.

1.6.2 선결 요건

RV와 HV 모두 V2V 서비스를 지원하고 V2V 서비스를 사용하여 상호 통신을 주고 받을 수 있다.

1.6.3 서비스 흐름

RV는 현재 위치, 속도, 가속 및 선택가능한 예상 궤도를 표시하는 메시지를 주기적으로 브로드캐스팅한다.

RV는 차선 준수 여부 및 추돌 예상 시간과 함께 제어 상실을 자체적으로 판별할 때 V2V 서비스를 사용하여 브로드캐스팅을 통해 이 정보를 사건으로 전송한다.

HV는 그 RV 사건 메시지를 수신하여 조치가 필요한지 여부를 판별한다.

1.6.4 사후 요건

HV 운전자에게 동일 주행 차선의 제어 상실된 차량 존재에 대해 경보를 보내고 주행 경로 전방에서 후미 차량 추돌을 피하거나 완화하기 위한 시정 조치를 취할 수 있도록 한다.

1.6.5 잠재적인 요구사항

본 사용 사례에서 도출된 잠재적 요구사항은 다음과 같다.

- 스마트 및 보안 IoT 플랫폼은 높은 이동 기능(예: 최대 절대 속도 280km/h)을 지원할 수 있어야 한다.
- 스마트 및 보안 IoT 플랫폼은 운전자에게 충분한 응답 시간(예: 4초)을 제공하기에 충분한 통신 범위를 지원할 수 있어야 한다.
- 스마트 및 보안 IoT 플랫폼은 최대 100ms의 지연시간을 지원할 수 있어야 한다.
- 서비스 제공자 네트워크는 통신의 익명성과 무결성 보호를 지원할 수 있어야 한다.
- V2V 서비스를 지원하는 스마트 개체는 V2V 서비스 계층의 호출로 시작된 후 즉시 사건 중심의 V2V 메시지를 전송할 수 있어야 한다.
- V2V 서비스를 지원하는 스마트 개체는 사건 중심의 V2V 메시지를 수신할 수 있어야 한다.
- 스마트 및 보안 IoT 플랫폼은 최대 1,200바이트가 될 수 있는 50-300바이트의 메시지 크기를 지원할 수 있어야 한다.
- 스마트 및 보안 IoT 플랫폼은 최대 10건의 V2V 메시지/초를 지원할 수 있어야 한다.
- 스마트 및 보안 IoT 플랫폼은 애플리케이션 계층 메시지 재전송을 요구하지 않고도 높은 신뢰성을 지원할 수 있어야 한다.

1.7 긴급 차량 경고에 대한 V2V 사용 사례

1.7.1 설명

긴급 차량 경고 서비스는 각 차량이 주변 긴급 차량(예: 앰뷸런스)의 위치, 속도 및 방향 정보를 얻어 앰뷸러스 주행 차선을 비워주는 등 안전을 도모할 수 있도록 지원한다.

1.7.2 선결요건

도로에서 앰뷸런스가 빠르게 달리고 있다고 하자. 그 앰뷸런스에는 V2V 서비스를 지원하는 근접 서비스(ProSe) [64] 활성 스마트 개체가 장착되어 있다.

그 앰뷸런스 주변에는 V2V 서비스를 지원하는 ProSe 활성 스마트 개체를 갖춘 몇 대의 차량이 있다.

1.7.3 서비스 흐름

그 앰뷸런스는 주기적으로 이전에 통보된 것과 비교하여 사전 정의된 한도를 기준으로 위치, 속도 또는 방향이 변경되었는지 점검한다. 위 매개변수 중 하나가 점검 기준을 충족할 경우 차량의 명세가 포함된 협업 인지 메시지(CAM)가 브로드캐스팅된다.

CAM에는 방향 및 속도와 같은 차량의 동적 상태 정보와 제원, 외부 라이트 상태 및 경로 이력과 같은 차량의 정적 데이터를 포함한 기본 차량 정보가 포함되어 있다. CAM 메시지의 크기는 50바이트-300바이트 사이이다.

앰뷸런스에서 긴급 차량 경고 메시지는 초당 최대 10건의 메시지 빈도로 전송된다.

생성된 CAM은 브로드캐스팅된다. 가시 경로가 없는 코너의 차량을 포함하여 앰뷸런스로부터 300m-500m 범위 내에 있는 모든 차량이 이 메시지를 수신할 수 있어야 한다,

메시지 수신 지연시간은 100ms 미만이어야 한다.

1.7.4 사후 요건

앰뷸런스 주변의 차량은 차량 운전자에게 정보를 제공하여 앰뷸러스가 지나가는 길을 열어줘야 한다는 사실을 알린다.

1.7.5 잠재적인 요구사항

- 스마트 및 보안 IoT 플랫폼은 50바이트-300바이트의 가변 메시지 페이로드를 허용하는 V2V 애플리케이션을 지원하는 두 스마트 개체 간에 V2V 서비스 메시지를 전송할 수 있어야 한다.
- 스마트 및 보안 IoT 플랫폼은 초당 최대 10건의 메시지 빈도를 허용하는 V2V 애플리케이션을 지원하는 두 스마트 개체 간에 V2V 서비스 메시지를 전송할 수 있어야 한다.
- 스마트 및 보안 IoT 플랫폼은 최대 100ms의 지연시간을 허용하는 V2V 애플리케이션을 지원하는 두 스마트 개체 간에 V2V 서비스 메시지를 전송할 수 있어야 한다.
- 스마트 및 보안 IoT 플랫폼은 운전자에게 충분한 응답 시간(예: 4초)을 제공하는 데 충분한 통신 범위를 지원할 수 있어야 한다.
- 스마트 및 보안 IoT 플랫폼은 280km/h의 최대 상대 속도를 허용하는 V2V 애플리케이션을 지원하는 스마트 개체 간에 V2V 서비스 메시지를 전송할 수 있어야 한다.

1.8 V2V 긴급 정지 사용 사례

1.8.1 설명

본 사용 사례에서는 정지 차량 근처의 다른 차량에 대한 보다 안전한 동작방식을 촉발하기 위해 비상 정지하는 경우 사용되는 V2V 통신을 기술한다.

1.8.2 선결 요건

어떤 사람이 도로에서 차량을 운전하고 있다고 하자. 그 차에는 V2V 서비스를 지원하는 ProSe-활성 스마트 개체가 장착되어 있다.

그 차 근처에는 동일하게 V2V 서비스를 지원하는 ProSe-활성 스마트 개체가 장착된 몇 대의 차량이 있다.

1.8.3 서비스 흐름

차량의 엔진이 고장나 도로 한복판에서 갑자기 정지한다. 차량의 안전 서비스가 이 사건을 통보하고 분산 환경 통보 메시지(DENM)를 통해 “정지 차량 경고”를 생성한다. DENM의 크기는 3000바이트 미만이다.

그 차량의 전송 범위 내에 있는 모든 차량이 이 메시지를 수신할 수 있다.

1.8.4 사후 요건

그 차량 근처에 있는 차량들이 정보를 운전자에게 제공하여 적절한 조치를 취할 수 있도록 한다.

1.8.5 잠재적 요구사항

- 스마트 및 보안 IoT 플랫폼은 최대 1,200바이트의 메시지 크기를 허용하는 V2V 애플리케이션을 지원하는 두 스마트 개체 간에 V2V 서비스에 의해 요청될 때 V2V 서비스 메시지를 전송할 수 있어야 한다.
- 스마트 및 보안 IoT 플랫폼은 초당 최대 10건의 메시지 빈도를 허용하는 V2V 애플리케이션을 지원하는 두 스마트 개체 간에 V2V 서비스 메시지를 전송할 수 있어야 한다.
- 스마트 및 보안 IoT 플랫폼은 100ms 최대 지연시간을 허용하는 V2V 애플리케이션을 지원하는 두 스마트 개체 간에

V2V 서비스 메시지를 전송할 수 있어야 한다.

- 스마트 및 보안 IoT 플랫폼은 운전자에게 충분한 응답 시간(예: 4초)을 제공하는 데 충분한 통신 범위를 지원할 수 있어야 한다.
- 스마트 및 보안 IoT 플랫폼은 160km/h의 최대 상대 속도를 허용하는 V2V 애플리케이션을 지원하는 스마트 개체 간에 V2V 서비스 메시지를 전송할 수 있어야 한다.

1.9 협업 순응 주행 제어(CACC)

1.9.1 설명

본 사용 사례에서는 V2V 기능을 갖춘 차량이 협업 순응 주행 제어(CACC) 차량 그룹에 합류 및 이탈하는 시나리오에 대해 기술한다. 이 그룹은 합류 차량에 편리성과 안전성 혜택을 제공하며 도로 정체 해소와 연비 향상이라는 범사회적 차원의 혜택도 제공한다.

1.9.2 선결 요건

차량 A와 B 모두 V2V 애플리케이션을 지원한다.

차량 A와 B는 근접하여 주행 중이고 V2V 통신 범위 내에 있다.

차량 A는 차량 B가 포함되어 있는 CACC 그룹에 속하지 않은 채 주행 중이고 해당 CACC 그룹에 합류하기를 원한다.

1.9.3 서비스 흐름

차량 B와 다른 참여 차량들은 주기적으로 CACC 그룹의 규모, 속도, 간격 정책, 위치 등의 정보를 포함한 메시지를 브로드캐스팅한다.

차량 A가 CACC 그룹 회원으로부터 메시지를 수신하고 특정 기준(예: 속도와 간격 정책, 규모)을 토대로 적정 CACC 그룹을 찾는다.

차량 A가 해당 CACC 그룹 회원들에게 합류 요청 메시지를 전송한다.

차량 B는 CACC 그룹 앞에서 필요할 경우 거리 간격을 허용하여 A가 합류할 수 있도록 결정하고 확정 수락 의사를 응답한다.

CACC 그룹의 다른 모든 참여 차량이 차량 A로부터 메시지를 수신하고 참여 차량들이 자체 지역에서 보유하고 있는 CACC 그룹 정보를 업데이트한다.

이후 차량 A의 운전자가 CACC 그룹에서 이탈하고 차량 A의 제어권을 되찾는다.

차량 A는 CACC 그룹의 다른 참여 차량들에게 작별 메시지를 브로드캐스팅한다.

차량 B는 차량 A로부터 메시지를 수신하여 회원들이 자체 지역에서 보유하고 있는 CACC 그룹 정보를 업데이트한다.

1.9.4 사후 요건

차량 A가 CACC 그룹에서 이탈한다.

1.9.5 잠재적 요구사항

- 스마트 및 보안 IoT 플랫폼은 최대 1초의 지연시간을 지원할 수 있어야 한다.
- 스마트 및 보안 IoT 플랫폼은 초당 최대 1건의 V2V 메시지 빈도를 지원할 수 있어야 한다.
- 스마트 및 보안 IoT 플랫폼은 애플리케이션 계층 메시지 재전송 없이도 높은 신뢰성을 지원할 수 있어야 한다.
- 스마트 및 보안 IoT 플랫폼은 V2V 서비스를 지원하는 높은 밀도의 스마트 개체(예: 교통 체증 상태인 4차선 자동차 도로)를 지원할 수 있어야 한다.

1.10 V2I 긴급 정지 사용 사례

1.10.1 설명

이 사용 사례에서는 보다 안전한 동작방식을 촉발하기 위해 서비스 RSU가 근접하여 주행 중인 차량에 긴급 정지를 통보하는 V2I 통신에 대해 기술한다.

1.10.2 선결 요건

도로에서 차량이 주행 중이다. 이 차량에는 V2X 서비스를 지원하는 ProSe-활성 스마트 개체가 장착되어 있다.

그 차량 근처에 동일하게 V2X 서비스를 지원하는 ProSe-활성 스마트 개체가 장착된 몇 대의 RSU가 있다.

1.10.3 서비스 흐름

차량의 엔진이 고장나 도로 한복판에서 갑자기 정지한다. 차량의 안전 서비스가 이 사건을 통보하고 “정지 차량 경고” DENM 메시지를 생성한다.

그 차량의 근처에 있는 서비스 RSU가 이 메시지를 수신할 수 있다.

서비스 RSU는 이 메시지를 주변 차량에 중계한다.

서비스 RSU의 전송 범위 내에 있는 모든 차량이 이 메시지를 수신할 수 있다.

1.10.4 사후 요건

서비스 RSU 주변 차량이 그 정보를 운전자들에게 제공하여 적정 조치를 이행할 수 있도록 한다.

1.10.5 잠재적 요구사항

- 스마트 및 보안 IoT 플랫폼은 1,200바이트 미만의 가변 메시지 페이로드를 허용하는 V2I 애플리케이션을 지원하는 두 스마트 개체 간에 V2I 서비스 메시지를 전송할 수 있어야 한다.
- 스마트 및 보안 IoT 플랫폼은 초당 최대 10건의 메시지 빈도를 허용하는 V2I 애플리케이션을 지원하는 스마트 개체와 도로변 장치 간에 V2I 서비스 메시지를 전송할 수 있어야 한다.
- 스마트 및 보안 IoT 플랫폼은 100ms 이하의 지연시간과 낮은 제공 손실을 허용하는 V2I 애플리케이션을 지원하는 스마트 개체와 도로변 장치 간에 V2I 서비스 메시지를 전송할 수 있어야 한다.
- 스마트 및 보안 IoT 플랫폼은 운전자에게 충분한 응답 시간(예: 4초)을 제공하는 데 충분한 V2I 애플리케이션을 지원하는 스마트 개체와 도로변 장치 간에 통신 범위를 지원할 수 있어야 한다.
- 스마트 및 보안 IoT 플랫폼은 최대 160km/h의 상대 속도를 허용하는 V2I 애플리케이션을 지원하는 스마트 개체와 도로변 장치 간에 V2I 서비스 메시지를 전송할 수 있어야 한다.

1.11 대기 행렬 경고

1.11.1 설명

많은 상황에서, 도로에 길게 늘어선 차량 대기 행렬은 잠재적 위험 요인이 되거나 교통 정체를 유발할 수 있다(예를 들어, 좌회전 대기 행렬이 다른 차선까지 차지하고 있는 경우). V2I 서비스를 사용하면 다른 운전자들이 대기 행렬 정보를 미리 수신하게 할 수 있다. 이는 충돌 발생 가능성을 최소화하고 그 위험을 완화하는 조치를 가능하게 한다.

1.11.2 선결 요건

차량 A, B, C 및 D 모두 V2X 애플리케이션을 지원하고 V2V 서비스를 사용하여 상호 통신을 주고 받을 수 있으며 V2I 서비스를 통해 인프라 엔티티인 RSU와 통신을 주고 받을 수 있다.

차량 A, B 및 C가 교차로에서 대기 중이고 차량 A는 대기 행렬의 선두에 있으며 차량 C는 대기 행렬의 끝에 있다. 차량 D는 멀리에서 접근 중이다.

1.11.3 서비스 흐름

이 서비스 흐름은 두 측면(즉, 대기 행렬 판별 및 대기 행렬 정보 전파)과 연관된다. 전자는 V2V 서비스를 사용하고 후자는 V2I 서비스를 사용한다.

세부적인 서비스 흐름은 다음과 같다.

차량 A, B 및 C 각각은 V2V 서비스를 사용하여 주기적으로 다른 차량에 메시지를 브로드캐스팅한다. 이 메시지는 위치, 차량 제원, 방향, 속도, 제동 상태, 기어 단 및 기타 환경 정보와 같은 차량 상태 정보를 나타낸다.

차량 C가 브로드캐스팅된 메시지를 수신하여 대기 행렬의 끝인지 확인하고 V2I 서비스를 사용하여 주기적으로 RSU에 대기 행렬 정보(예: 대기 행렬의 규모, 대기 행렬의 상태, 관련 차선 대기 행렬의 최종 위치 등)를 통보한다.

RSU는 V2I 서비스를 사용하여 차량 C로부터 수신된 정보를 근거로 근접 차량에 대기 행렬에 대한 정보를 브로드캐스팅한다.

RSU에 접근할 때 차량 D는 V2I 서비스를 사용하여 RSU로부터 메시지를 수신하여 운전자가 대기 행렬 및 관련 정보를 인지하여 그 대기 행렬에 다다르기 전에 자신의 주행 방향을 결정할 수 있다.

차량 D는 차량 C의 뒤에서 대기 행렬에 합류한다. 차량 D가 V2V 서비스를 이용하여 해당 대기 행렬의 맨뒤에 합류한 것을 식별한 후 차량 C를 대신하여 해당 대기 행렬에 대해 RSU를 업데이트한다.

1.11.4 사후 요건

차량 D의 운전자가 미리 대기 행렬을 인지하여 그에 따라 적시에 조치를 취할 수 있다.

1.11.5 잠재적 요구사항

- V2I 서비스를 지원하는 스마트 개체는 RSU에 메시지를 전송할 수 있어야 한다.
- V2I 서비스를 지원하는 스마트 개체는 RSU로부터 메시지를 수신할 수 있어야 한다.
- 스마트 및 보안 IoT 플랫폼은 160km/h의 최대 상대 속도를 지원할 수 있어야 한다.
- 스마트 및 보안 IoT 플랫폼은 운전자에게 충분한 응답 시간(예: 4초)을 제공하는 데 충분한 통신 범위를 지원할 수 있어야 한다.
- 스마트 및 보안 IoT 플랫폼은 최대 1,200바이트일 수 있는 50바이트-400바이트 크기의 메시지를 지원할 수 있어야 한다.
- 스마트 및 보안 IoT 플랫폼은 100ms의 최대 지연시간을 지원할 수 있어야 한다.
- V2I 서비스는 사용자/차량 익명성과 전송의 무결성 보호를 지원할 수 있어야 한다.

2. 특징적인 기능에 대한 매핑

2.1 연결성

기능		비고
실시간 상황 처리	X	실시간 감지수행 포함
다중 시스템 연결성	X	여러 시스템에 연결
원격 기능	X	제품 외부에 상주하는 기능
모든 대역폭/프로토콜에 대한 적용성	X	제공 대역폭/프로토콜에 맞춰 재구성→ HW에서 SW로 전환
새로운 연결성 표준으로 업그레이드 가능성	X	SW를 통해 새로운 연결성 표준으로 업그레이드할 수 있는 기능
합법적 감청 기능		
원격 액세스	X	
인증 및 액세스 제어	X	
신뢰성 및 무결성	X	

2.2 처리

기능		비고
온보드 분석	X	
오프보드 분석	X	
기계 학습		
맥락화	X	
익명화	X	
정보 매시업	X	
의미론적 상호 운용성	X	
장치의 동적 구성	X	자가 치유/복원성을 위한 장치의 동적 구성
동적 구성가능성	X	변경 요구사항에 따라 장치가 자체적으로 또는 시스템을 통해 동적으로 구성 가능해질 필요
데이터 소유권 추적	X	
집단 인지		

2.3 메모리

기능		비고
디지털 제품 메모리		전체 수명주기, 제품 내력
패턴 인지		인공 지능/기계 학습 기반
기능 데이터	X	분석용

2.4 감지

기능		비고
감지 기능을 갖춘 장치 수 증가에 대응	X	
감지 데이터의 중재 교환	X	
데이터의 신뢰성	X	
원시 데이터의 정리	X	
초정밀 위치 기반 기능	X	
개인정보보호		
데이터의 무결성	X	
인증을 요하는 복잡한 센서	X	
센서 재구성 기능	X	

2.5 조치

제어 인터페이스 장치

기능		비고
교정		
장치 그룹의 제어	X	런타임 및 구성
장치의 동적 구성	X	동적 장치 온보딩/그룹에 지정
컨텍스트에 따라 장치가 제어되는 방식 적용	X	
안전성 요구사항		
인증 및 액세스 제어 및 인증	X	
플로어 제어		시스템을 실제로 제어하도록 허락된 사람들과 그 인계 메커니즘
집단/자체 최적화 제어 지능		
보안의 집단 제어		
컨텍스트 인지 제어		

사용자 I/O

기능		비고
촉각 인터페이스	X	
다중 장치 사용자 인터페이스	X	
가상 모델링		
시뮬레이션		
접근성		장애인용
증강 현실		예: 안경
사용성 및 사용자 경험		

2.6 보안

기능		비고
엔드 투 엔드 정책 관리	X	모든 정책 통합
가용 물리적 자원 및 보안성에 대해 최적화된 프레임워크	X	가용 물리적 자원/보안 강건성에 대해 최적화된 프레임워크(ISO 27001에서는 계획-실천-확인-조치) ISO 27001)
복원성	X	가상 물리 공격 포함
장애 허용 능력	X	가상 물리 공격 포함
시스템 위협 탐지 및 대응		OODA 관찰-방향설정-결정-실행
장치의 모니터링	X	
협조 및 위협 분석	X	
ID 관리	X	연합 ID 관리, 시스템 간 ID 상관관계, …
장치의 ID 보안	X	
인증 관리	X	데이터의 책임/부인 방지
이상 탐지		

3. 차세대 지원 기술

	차세대 지원 기술		비고
연결성	차세대 위성 연결을 위한 전송 계층 프로토콜	X	보다 높은 대역폭, 낮은 지연시간
	5세대 셀룰러 액세스(5G)	X	
	저전력 무선 액세스(LPWAN)	X	
처리	시스템 구성 및 동적 구성		
	데이터 맥락화		
	자율 데이터 교환		
	센서 융합 기술		
	기계 학습	X	
	가상화	X	
메모리	디지털 제품 메모리		
감지	초정밀 위치 기술	X	

	차세대 지원 기술		비고
조치	증강 현실		
	가상 현실		
	촉각 인터넷	X	
보안	사물의 ID	X	
	준동형 암호화		
	검색 가능 암호화		
	신뢰 구축		
	보안화 시스템 협업 기술	X	
	사용 제어를 통한 개인정보보호		
	지속적인 보안 감사		
	IoT용 IAM 기술	X	ID 및 액세스 관리
	애플리케이션 격리 및 보안 경계 기술	X	

4. 필요한 미래 표준

	표준 요구사항		비고
연결성	5G 표준의 실현	X	
	표준 위성과 장치 간의 보다 높은 대역폭/요구 지연시간을 지원하기 위한 새로운 전송 계층 프로토콜에 대한 표준		
	IoT 장비가 새로운 연결성 표준으로 업데이트하는 기능을 갖추도록 하는 표준	X	
처리	정보 교환 모델	X	
	의미론 메타데이터 정의 표준 및 모델	X	
	데이터 교환 모델 및 인터페이스와 관련 표준	X	
	자율 데이터 교환 프로파일 및 교환 메커니즘 메타데이터 주석 모델 및 인터페이스		
	맥락화 정보 모델	X	
	메타데이터 컨텍스트 표준		
메모리	디지털 제품 메모리의 표준화		

	표준 요구사항		비고
감지	메타데이터에 대한 표준	X	
	초정밀 위치 기반 기술에 대한 추상화 기술		
	센서 데이터 개인정보보호 표준	X	최종 소비자/소비자의 옵트인/옵트아웃
	센서 융합 표준		센서 관찰을 추상화하는 센서 메타 모델 개발 표준. 이 표준은 정형화되지 않은 산발적 데이터를 고급 도메인 지식으로 바꿀 수 있는 기반이 된다.
조치	제어 인터페이스 장치 그룹을 고유하게 식별하는 표준 템플릿		
	시스템 간의 IoT 사용자 I/O를 일반화하는 일반 표준	X	
	고유한 IoT 접근성 요구사항에 대한 표준	X	일반적인 인간/컴퓨터 I/O를 뛰어넘는 고급 IoT 서비스 반영
보안	소셜 시스템의 ID 연합 표준		
	가상 물리 공격 보호 표준		
	동시 연결을 갖춘 다중 시스템에서 장치 ID에 대한 표준	X	예: W3C의 국제화 자원 식별자(IRI)
	플랫폼 무결성에서 신뢰를 구축하기 위한 표준 프로토콜	X	
	협업 보안 프레임워크		상호 의존적인 시스템 간의 사이버 위협 분석 교환 활성화
	상호 의존적인 시스템 간 보안 기능 평가를 활성화하는 성숙 모델		

부록 I – 사용 사례

WISE 스키잉

1. 사용 사례의 기술

1.1 사용 사례의 명칭

스마트 및 보안 IoT 플랫폼을 이용한 WISE 스키잉

1.2 사용 사례의 범위 및 목적

1.2.1 범위

WISE 스키잉의 비전은 스키타는 것과 같은 일상 활동 특히 그러한 일상 생활에서 사용하는 스포츠 제품에 IoT 기술을 통합하는 것이다. 이런 시스템에 사용자 가입을 유도하기 위해 보상 기법 및 게임화가 사용된다. 유사 시, 그 위험에 더 빨리 대처하는 데에 동일 정보가 활용될 수 있다. 넓은 의미에서 본 사용 사례는 효율적인 응급 상황 대응과 공공 안전 대책의 개선을 목표로 한다.

1.2.2 목적

WISE 스키잉은 예제 애플리케이션이며 여기에서는 IoT 기술이 다목적용이다. 이런 기술은 물감 축제, 마라톤, 골프 행사 등의 대도시 행사의 공공 안전 관리에 적용할 수 있다.

이 비전 실현을 위해서는 감지, 처리, 통신, 작동, 보안성, 게임화 및 보상 체계의 고급 기술 기능이 필요하다. 더 나아가 투명한 정보 공유, 정보 매시업 기회 발견, 의미론적 상호 운용성 및 응급 상황 관리에 대한 표준화 노력도 요구될 것이다. 간단히 말해 이 사용 사례는 차세대 IoT 플랫폼의 필수 요구사항을 정의한다.

1.3 사용 경험담

1.3.1 사용 사례의 요약

WISE 스키잉 사용 사례에 있어 각 스키어는 그 사람의 스키잉 궤적, 동작 정보, 빛의 강도 및 주변 소리 수준을 포착하는 다양한 내장 기능을 갖춘 스마트폰을 소지하고 있다. 한편 스키 장비에는 진동 센서가 장착되어 있어 스키어의 동작과 제스처를 추적한다. 시스템은 이런 감지 데이터를 이용하여 실시간 사건 탐지, 응급상황 대응 및 난이도별 슬로프 권장 등의 다양한 기능을 수행할 것이다.

WISE 스키잉 시나리오를 실현하려면 미래 IoT 서비스의 다음 특성으로 인해 일부 고급 기술 기능이 요구된다.

(a) 시나리오에 서로 매우 다른 장비(다양한 장치)가 포함될 필요가 있다.

(b) 다수의 애플리케이션에서 데이터가 사용된다(다양한 소모 애플리케이션).

수직 부문에 있어 미래 IoT 플랫폼은 서로 매우 다른 출처의 데이터를 수용하고 연결성 관리 및 자원 컨텍스트 관리를 제공한다. 수평 부문에 있어서는 엣지 측의 의미론 기반 검색과 컨텍스트 변환, 클라우드 측의 데이터 맥락화와 시장성 있는 데이터 스트림 관리가 요구된다. 그러나 수직 및 수평 기능은 데이터 소스의 정보 통합 및 더 나아가 미래의 의미론 통합을 위한 표준화 노력에 큰 영향을 받는다.

1.3.2 사용 사례의 특성

개인 소비자

1.3.3 전체 기술

스마트 및 보안 IoT 플랫폼을 이용한 WISE 스키잉 사용 사례는 그림 I-1과 같다. 각 스키어는 스키 장비에 달린 센서 모음과, 일부 내장 센서가 달린 모바일 장치를 착용할 것이다. 이런 센서는 스키 이동 궤적(위치 센서), 동작 정보(중력, 방향 및 가속도계 센서), 빛 강도(빛 센서) 및 주변 소리의 수준(마이크)을 캡처한다. 스키어의 적극적인 감지 데이터 수집 참여를 독려하기 위해 WISE 스키잉 시스템에는 게임화 기반 보상 체계가 있으며 스키어가 더 많은 데이터를 제공하거나 더 높은 품질의 데이터를 제공하면 점수나 실시간 쇼핑 상품권 등으로 보상받는다. 수집된 데이터가 차세대 IoT 플랫폼에서 컨텍스트별 정보와 함께 공통적인 형태로 변환되고 나면 안전성 향상을 위해 스키어에게 실시간 사건 탐지, 응급 상황 대응 및 슬로프 권고가 제공된다.

그러나 WISE 스키잉 사용 사례는 스마트 및 보안 IoT 플랫폼의 상호 운용성 및 상호 네트워킹에 지나치게 의존한다. IoT 플랫폼 맥락의 수직 부문에서, 연결성 관리 및 자원 컨텍스트 관리는 서로 다른 엔티티 간의 정보 투명성을 활성화하고 정보 매시업에 대한 기회를 제공한다. 특히 연결성 관리는 의미론적 상호 운용성 및 의미론 중재의 기능을 나타내며 자원 컨텍스트 관리는 자체 최적화 및 자원 엔티티 매핑을 나타낸다. 수평 부문에 있어서는 엣지와 클라우드의 고급 기능이 서로 다른 자원과 엔티티의 데이터 스트림을 통합하여 수색 및 구조 작업(예: 사고 및 부상자 위치 파악)을 수행할 것이다. 특히 엣지 측의 의미론 기반 검색과 컨텍스트 변환은 조기 매시업에 대한 기회를 모색하는 반면, 클라우드 측의 데이터 맥락화와 확장 가능 데이터 스트림 관리는 비상 대응 향상을 위한 복잡한 컴퓨팅을 수행한다. 한편 정상적인 상황에서 수평 기능은 보상 체계를 통해 슬로프 권고와 게임화를 활성화한다. 수직 및 수평 기능 모두 엣지와 클라우드를 연결하는 FIWARE NGSI 및 서로 다른 유형의 장치와 엣지를 연결하는 oneM2M과 같은 사용 사례를 실현하기 위한 표준화 노력에 의존할 것이다.

1.4 사용 사례의 도표

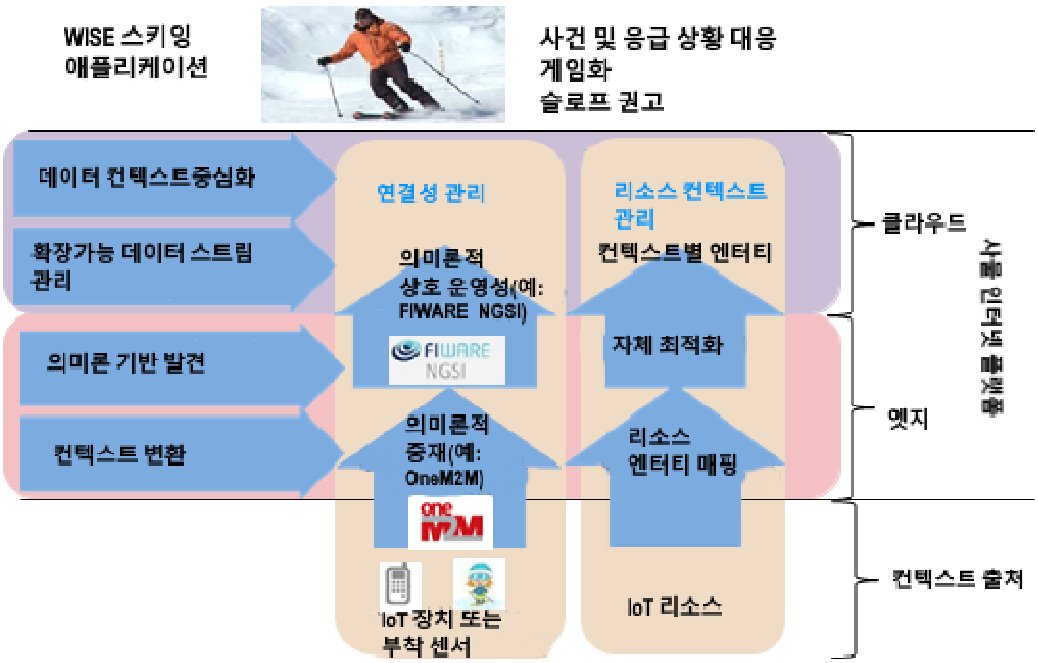


그림 I-1 | 스마트 및 보안 IoT 플랫폼을 이용한 WISE 스키잉

그림 I-2 | 스마트 및 보안 IoT 플랫폼을 이용한 WISE 스키잉의 비전

1.5 사용 사례의 조건

1.5.1 전제

WISE 스키잉 사용 사례는 스키 리조트에 입장하는 사람이 이미 IoT 센서로 장비를 활성화하거나 스키를 타기 전에 장치를 대여/구매하는 것을 전제로 한다.

1.6 사용 사례에 대한 추가 정보

1.6.1 최신 상태

IoT 표준: 본 사용 사례는 데이터 통신을 위해 oneM2M 표준을 채택한다. 이 표준은 다수의 애플리케이션의 정보에 대한 맥락화 액세스를 제공하는 Open Mobile Alliance(OMA) 차세대 서비스 인터페이스(NGSI) 9/10 API를 사용한다. 본 사용 사례의 비전은 다양한 시스템의 데이터에 대한 의미론적 상호 운용성을 위한 지원의 통합과 같은 추가적인 표준화된 구성요소를 필요로 한다. M2M 시스템(아마도 oneM2M 표준 기반)에서 수신되는 정보 스트림은 FIWARE에서 표준으로 정의되어 사용되는 NGSI 기반 맥락화 정보 모델로 자동 매핑될 필요가 있다. 이 변환 프로세스는 의미론 중재 게이트웨이(SMG)에 의해 취급되어 의미론적 정보와 변환 루틴 라이브러리를 이용하여 서로 다른 정보 모델을 공통 모델에 매핑할 수 있다. 가용 자원, 정보의 자동 매시업 및 개선된 빅 데이터 분석 기능을 보다 신속하게 발견하기 위해 변환된 메타데이터가 사용될 것이다. 정보의 자동 통합 및 자동 매시업 생성을 위한 스마트 기능이 필요하다. 더 나아가 수집 및 추론된 데이터는 서로 다른 제3자가 제공할지도 모르는 여러 신규 애플리케이션에서 가용할 수 있도록 지원된다. 보안 및 개인정보보호 정책을 엄격히 통제할 필요가 있다.

2. 특징적인 기능에 대한 매핑

의미론적 상호 운용성: 상호 운용성은 "둘 이상의 시스템 또는 구성요소가 데이터를 교환하고 정보를 사용하는 기능"이다[61]. 의미론적 상호 운용성은 상호작용하는 시스템이 개별 데이터 형식에 관계없이 시스템 전체에 걸쳐 데이터의 일관성을 보장하여 교환된 데이터와 동일한 의미를 채택할 때 달성된다. 의미론은 온톨로지에서 지정되는 것과 같은 공유 어휘를 사용하여 명시적으로 정의될 수 있다. 의미론적 상호 운용성은 IoT 시스템의 모든 부품(즉, 클라우드의 IoT 플랫폼뿐만 아니라 엣지 구성요소와 IoT 장치 등)에 적용될 수 있다[65].

의미론 중재: 의미론 중재는 서로 다른 장치로부터 수신되는 데이터를 매끄럽게 변환하여 서로 다른 IoT 시스템에 대해 상호 운용되는 지식을 제공한다. 차세대 IoT 플랫폼의 비전은 광범위한 서로 다른 애플리케이션과 사용자에 걸쳐 개별 수직 부분에서 발생한 데이터를 공유하는 것이다. 그러므로 지능형 의미론 중재 게이트웨이는 서로 다른 연결성 옵션(WiFi, Bluetooth, ZigBee, 3GPP, LoRaWAN)을 가질 수 있는 서로 다른 장치를 연결하기 위한 기능을 갖출 것이다.

자원 엔티티 매핑: 기존 IoT 플랫폼에서는 다중 자원이 단일 컨텍스트(예: 상황)에 매핑되었다. 그러나 미래에는 자원 또한 두어개의 컨텍스트 엔티티가 될 수 있다. 예를 들어 눈오는 날과 달력의 공휴일에 대한 컨텍스트별 정보는 권장 슬로프를 변경할 수 있는 공유 자원과 연관될 수 있다. 그러므로 자원 컨텍스트 관리 면에서 자원과 컨텍스트 엔티티 간의 매핑은 보다 복잡해질 것이다.

자체 최적화: 클라우드-엣지 기반 환경에서 엣지와 클라우드 간 대역폭 소모 절감 또는 원시 센서 데이터에서 분석 결과를 추출하기 위한 지연시간 최소화와 같은 특정 최적화 목적을

충족하기 위해 데이터 처리와 컨텍스트별 데이터 마이닝 작업이 클라우드나 엣지에 동적으로 할당될 수 있다.

컨텍스트 변환: 컨텍스트 변환은 초기 단계에 의미론 기반 검색과 정보 매시업을 활성화하기 위해 엣지에서 초기 및 경량 데이터 분석(예: 데이터 필터링 및 전처리)을 수행한다.

의미론 기반 검색: 의미론 기반 검색은 사용자의 작업 및 지원 필요를 없애고 웰드와이드 IoT 애플리케이션이 초기화 단계에서 자동화 설치, 배포 및 정보 매시업을 완료할 수 있도록 허용한다.

확장 가능한 데이터 스트림 관리: 확장 가능 데이터 스트림 관리의 기능은 실시간 및 대규모 데이터 공유와 데이터 배포를 취급하는 것이다. 한편 데이터 흐름, 보안 및 빅 데이터 분석과의 통합을 조율한다.

데이터 맥락화: 데이터 맥락화는 투명한 정보 또는 수집된 데이터 뒤에 숨겨진 정보를 추출하여 컨텍스트별 마이닝과 분석 알고리즘을 통해 특정 지식 부문에서 의미있는 형태로 표시하는 정보 변환 프로세스이다. 데이터 맥락화의 새로운 기법은 이력 데이터 분석, 실시간 상황 인지 및 상황 예측 등 3가지 작업을 지속적으로 수행할 것이다.

2.1 연결성

기능		비고
실시간 상황 처리	X	실시간 감지수행 포함
다중 시스템 연결성	X	여러 시스템에 연결
원격 기능	X	제품 외부에 상주하는 기능
모든 대역폭/프로토콜에 대한 적용성	X	제공 대역폭/프로토콜에 맞춰 재구성→ HW에서 SW로 전환
새로운 연결성 표준으로 업그레이드 가능성	X	SW를 통해 새로운 연결성 표준으로 업그레이드할 수 있는 기능
합법적 감청 기능		
원격 액세스	X	
인증 및 액세스 제어	X	
신뢰성 및 무결성	X	

2.2 처리

기능		비고
온보드 분석	X	
오프보드 분석	X	
기계 학습	X	
맥락화	X	
익명화	X	
정보 매시업	X	
의미론적 상호 운용성	X	
장치의 동적 구성	X	자가 치유/복원성을 위한 장치의 동적 구성
동적 구성가능성	X	변경 요구사항에 따라 장치가 자체적으로 또는 시스템을 통해 동적으로 구성 가능해질 필요
데이터 소유권 추적	X	
집단 인지		

2.3 메모리

기능		비고
디지털 제품 메모리	X	전체 수명주기, 제품 내력
패턴 인지	X	인공 지능/기계 학습 기반
기능 데이터	X	분석용

2.4 감지

기능		비고
감지 기능을 갖춘 장치 수 증가에 대응	X	
감지 데이터의 중재 교환	X	
데이터의 신뢰성	X	
원시 데이터의 정리	X	
초정밀 위치 기반 기능	X	
개인정보보호	X	
데이터의 무결성	X	
인증을 요하는 복잡한 센서	X	
센서 재구성 기능	X	

2.5 조치

제어 인터페이스 장치

기능		비고
교정	X	
장치 그룹의 제어	X	런타임 및 구성
장치의 동적 구성	X	동적 장치 온보딩/그룹에 지정
컨텍스트에 따라 장치가 제어되는 방식 적용	X	
안전성 요구사항	X	
인증 및 액세스 제어 및 인증	X	
플로어 제어	X	시스템을 실제로 제어하도록 허락된 사람들과 그 인계 메커니즘
집단/자체 최적화 제어 지능	X	
보안의 집단 제어		
컨텍스트 인지 제어	X	

사용자 I/O

기능		비고
촉각 인터페이스	X	
다중 장치 사용자 인터페이스	X	
가상 모델링	X	
시뮬레이션	X	
접근성		장애인용
증강 현실	X	예: 안경
사용성 및 사용자 경험	X	

2.6 보안

기능		비고
엔드 투 엔드 정책 관리	X	모든 정책 통합
가용 물리적 자원 및 보안성에 대해 최적화된 프레임워크	X	가용 물리적 자원/보안 강건성에 대해 최적화된 프레임워크(ISO 27001에서는 계획-실천-확인-조치) ISO 27001)
복원성	X	가상 물리 공격 포함
장애 허용 능력	X	가상 물리 공격 포함
시스템 위협 탐지 및 대응	X	OODA 관찰-방향설정-결정-실행
장치의 모니터링	X	
협조 및 위협 분석	X	
ID 관리	X	연합 ID 관리, 시스템 간 ID 상관관계, …
장치의 ID 보안	X	
인증 관리	X	데이터의 책임/부인 방지
이상 탐지	X	

3. 차세대 지원 기술

	차세대 지원 기술		비고
연결성	차세대 위성 연결을 위한 전송 계층 프로토콜	X	보다 높은 대역폭, 높은 지연시간
	5세대 셀룰러 액세스(5G)	X	
	저전력 무선 액세스(LPWAN)	X	
처리	시스템 구성 및 동적 구성	X	
	데이터 맥락화	X	
	자율 데이터 교환	X	
	센서 융합 기술	X	
	기계 학습	X	
	가상화	X	
메모리	디지털 제품 메모리	X	
감지	초정밀 위치 기술	X	

	차세대 지원 기술		비고
조치	증강 현실	X	
	가상 현실	X	
	촉각 인터넷		
보안	사물의 ID	X	
	준동형 암호화	X	
	검색 가능 암호화	X	
	신뢰 구축	X	
	보안화 시스템 협업 기술	X	
	사용 제어를 통한 개인정보보호	X	
	지속적인 보안 감사		
	IoT용 IAM 기술	X	ID 및 액세스 관리
	애플리케이션 격리 및 보안 경계 기술	X	

4. 필요한 미래 표준

	표준 요구사항		비고
연결성	5G 표준의 실현	X	
	표준 위성과 장치 간의 보다 높은 대역폭/요구 지연시간을 지원하기 위한 새로운 전송 계층 프로토콜에 대한 표준	X	
	IoT 장비가 새로운 연결성 표준으로 업데이트하는 기능을 갖추도록 하는 표준	X	
처리	정보 교환 모델	X	
	의미론 메타데이터 정의 표준 및 모델	X	
	데이터 교환 모델 및 인터페이스와 관련 표준	X	
	자율 데이터 교환 프로파일 및 교환 메커니즘	X	
	메타데이터 주석 모델 및 인터페이스	X	
	맥락화 정보 모델	X	
	메타데이터 컨텍스트 표준	X	
메모리	디지털 제품 메모리의 표준화	X	

	표준 요구사항		비고
감지	메타데이터에 대한 표준	X	
	초정밀 위치 기반 기술에 대한 추상화 기술	X	
	센서 데이터 개인정보보호 표준	X	최종 소비자/소비자의 옵트인/옵트아웃
	센서 융합 표준	X	센서 관찰을 추상화하는 센서 메타 모델 개발 표준. 이 표준은 정형화되지 않은 산발적 데이터를 고급 도메인 지식으로 바꿀 수 있는 기반이 된다.
조치	제어 인터페이스 장치 그룹을 고유하게 식별하는 표준 템플릿	X	
	시스템 간의 IoT 사용자 I/O를 일반화하는 일반 표준	X	
	고유한 IoT 접근성 요구사항에 대한 표준	X	일반적인 인간/컴퓨터 I/O를 뛰어넘는 고급 IoT 서비스 반영
보안	소셜 시스템의 ID 연합 표준	X	
	가상 물리 공격 보호 표준		
	동시 연결을 갖춘 다중 시스템에서 장치 ID에 대한 표준	X	예: W3C의 국제화 자원 식별자(IRI)
	플랫폼 무결성의 신뢰를 구축하기 위한 표준 프로토콜	X	
	협업 보안 프레임워크	X	상호 의존적인 시스템 간의 사이버 위협 분석 교환 활성화
	상호 의존적인 시스템 간 보안 기능 평가를 활성화하는 성숙 모델	X	

부록 J – 사용 사례

홈 디바이스 스마트 팩토리

1. 사례의 기술

1.1 사용 사례의 명칭

홈 디바이스 스마트 팩토리

1.2 사용 사례의 범위 및 목적

1.2.1 범위

본 사용 사례는 중국의 가정용 기기 제조업체 내 팩토리 프로세스를 취급한다. 즉, 팩토리 프로세스 데이터를 취득하여 이 데이터를 백 오피스에서 실시간으로 사용할 수 있게 한다.

1.2.2 목적

이 사용 사례를 통하여 팩토리 툴, 기구, 센서, PLC 및 장치에서 관련 프로세스 데이터를 취득하는 것을 볼 수 있다. 개선 효과는 물론 클라우드 내에서 팩토리 프로세스 데이터를 가용하게 만들고 관련 정보의 가용성을 개선하는 데스크 클라우드 클라이언트를 통한 팩토리 프로세스 관리 애프리케이션에 대한 액세스를 제공하여 가능한 비용 절감 방법도 보여준다.

1.3 사용 경험담

1.3.1 사용 사례의 요약

본 사용 사례는 장치 상태, 에너지 소비량 등의 데이터를 조회하기 위해 서로 다른 프로토콜을 지원하는 산업 게이트웨이인 IoT 게이트웨이를 통해 팩토리 프로세스 데이터를 취득하는 방법을 기술한다.

또한 본 사용 사례에서는 클라우드 내의 팩토리 프로세스 애플리케이션 제공에 대해 기술하고 사용되는 전사적 자원 관리(ERP), 제품 수명주기 관리(PLM) 및 제조 실행 시스템(MES)에 액세스하기 위한 클라우드 터미널을 배포한다. 이런 액세스는 품질 통제(QC) 테스트 결과, 생산 프로세스 정보 등의 정보에 대한 실시간 쿼리 기회를 제공할 것이다.

1.3.2 사용 사례의 특성

본 사용 사례는 Platform of Platforms(플랫폼을 위한 플랫폼) 원칙의 예인 IoT 에이전트와 IoT 플랫폼의 상호 네트워킹을 소개한다.

1.3.3 전체 기술

이 가정용 기기 제조업체는 생산 프로세스 내의 비효율성을 발견하여 생산 비효율성을 파악하기 위해 제조 프로세스에서 보다 많은 정보를 수집하기로 결정했다. 또한 공장 외부의 영업부 및 관리부 내에서 생산 프로세스 정보에 대한 접근성을 개선할 필요도 확인하였다.

시스템이 서로 다른 센서의 유선/버스/무선 연결을 경유하는 산업 게이트웨이를 통해 생산 라인 내의 제조 프로세스 및 공장의 프로세스에서 데이터를 자동으로 수집한다. 데이터에는 장치 상태, 에너지 소비량, 환경 모니터링 데이터, 센서 데이터 및 생산 프로세스 데이터가 있다. 이 데이터는 공장 클라우드 인프라 내 IoT 플랫폼에 제공되고

ERP, PLM, MES 및 빅 데이터 분석과 같은 서로 다른 비즈니스/제조 프로세스에 분산된다.

비즈니스 및 제조 통계와 정보는 몇 가지 애플리케이션이 통합된 클라우드 터미널에서 클라우드 인프라를 통해 이용이 가능해진다. 이 제조업체의 경영층은 이제 터미널에서 경영 처리에 대한 핵심 프로세스 정보를 즉시 수신하고 비즈니스 및 제조 프로세스에 대한 필요한 시정 조치를 도입하여 폐기물 및 장애를 방지할 수 있다. 그 결과 효율성이 30% 증가하고 비용은 20% 절감되었다.

1.5 사용 사례의 조건

1.5.1 전제

사용되는 기술은 제조 프로세스에 있어 상당히 새로운 기술을 요하지는 않지만 필요한 장소 및 시간과 같은 필요한 비즈니스 및 제조 정보를 제공하는 데 초점을 둔다. 그러므로 취득된 정보가 비즈니스 및 제조 프로세스 관리에 필요하다는 것을 전제로 한다.

본 사용 사례는 공장 내 제조 정보를 관리, R&D 및 영업부의 비즈니스 프로세스에 통합하는 데 중점을 둔다.

1.4 사용 사례의 도표

그림 J-1 | 사용 사례의 도표 – 가정용 기기의 스마트 팩토리

1.5.2 선결요건

이 솔루션에서는 서로 다른 통신 기술(예: 무선 및 유선과 서로 다른 프로토콜)을 사용하여 센서와 작동기에 연결할 수 있는 산업 게이트웨이가 필요하다.

이 솔루션은 보안성 관리, 장치 관리 및 데이터 관리 기능과 같은 산업 게이트웨이 내의 일부 공통 기능을 포함하여 산업 게이트웨이 내에 통합되는 IoT 에이전트를 필요로 한다.

보안성 관리에는 장치 인증, 시간 기반 인증, 데이터 소스 점점 및 장치 가용성과 같은 기본 보안 액세스 기능이 포함된다.

장치 관리에는 장애 관리, 서비스 추적, 존재 관리 및 도난 방지/복제 관리와 같은 기본 기능이 포함된다.

데이터 관리에는 통지 전송하거나 혹은 특정 조건이 부합되면 경보기를 작동시키는 등의 대처를 자동으로 시작할 수 있는 규칙 엔진이 포함될 것이다. 이 규칙 엔진은 장치마다 개별적으로 또는 장치 그룹에 대해 특정 규칙을 지원할 것이다. 규칙은 선언 프로그램을 사용하여 프로그래밍할 수 있다.

1.6 사용 사례의 추가 정보

1.6.1 최신 상태

제조 산업 내에서 정보 지식의 도입 변화(즉, 스마트 제조)가 이미 진행 중이다. 통신 기술(CT), IT, OT 등의 서로 다른 산업 내에서 산업 게이트웨이에 대한 기본 기술을 사용할 수 있다.

그러나 일부 특정 사용 사례는 무선 통신 기술의 상당한 개선을 요하는 10ms 미만 등의 낮은 지연시간 서비스를 요구할 것이다. 기타 기술에는 데이터 관리 기능 개선과 더불어 하드웨어 가속을 통해 플랫폼 기능 기준 충족을 보장하는 자체 학습 기능이 포함될 수 있다.

2. 특징적인 기능에 대한 매핑

2.1 연결성

기능		비고
실시간 상황 처리	X	실시간 감지수행 포함
다중 시스템 연결성	X	여러 시스템에 연결
원격 기능	X	제품 외부에 상주하는 기능
모든 대역폭/프로토콜에 대한 적용성	X	제공 대역폭/프로토콜에 맞춰 재구성 HW에서 SW로 전환
새로운 연결성 표준으로 업그레이드 가능성	X	SW를 통해 새로운 연결성 표준으로 업그레이드할 수 있는 기능
합법적 감청 기능		
원격 액세스	X	
인증 및 액세스 제어	X	
신뢰성 및 무결성	X	

2.2 처리

기능		비고
온보드 분석	X	
오프보드 분석	X	
기계 학습		
맥락화	X	
익명화	X	
정보 매시업	X	
의미론적 상호 운용성	X	
장치의 동적 구성	X	자가 치유/복원성을 위한 장치의 동적 구성
동적 구성가능성	X	변경 요구사항에 따라 장치가 자체적으로 또는 시스템을 통해 동적으로 구성 가능해질 필요
데이터 소유권 추적	X	
집단 인지		

2.3 메모리

기능		비고
디지털 제품 메모리		전체 수명주기, 제품 내력
패턴 인지	X	인공 지능/기계 학습 기반
기능 데이터	X	분석용

2.4 감지

기능		비고
감지 기능을 갖춘 장치 수 증가에 대응	X	
감지 데이터의 중재 교환	X	
데이터의 신뢰성	X	
원시 데이터의 정리	X	
초정밀 위치 기반 기능	X	
개인정보보호		
데이터의 무결성	X	
인증을 요하는 복잡한 센서	X	
센서 재구성 기능	X	

2.5 조치

제어 인터페이스 장치

기능		비고
교정		
장치 그룹의 제어	X	런타임 및 구성
장치의 동적 구성	X	동적 장치 온보딩/그룹에 지정
컨텍스트에 따라 장치가 제어되는 방식 적용	X	
안전성 요구사항		
인증 및 액세스 제어 및 인증	X	
플로어 제어		시스템을 실제로 제어하도록 허락된 사람들과 그 인계 메커니즘
집단/자체 최적화 제어 지능		
보안의 집단 제어		
컨텍스트 인지 제어		

사용자 I/O

기능		비고
촉각 인터페이스	X	
다중 장치 사용자 인터페이스	X	
가상 모델링		
시뮬레이션		
접근성		장애인용
증강 현실		예: 안경
사용성 및 사용자 경험		

2.6 보안

기능		비고
엔드 투 엔드 정책 관리	X	모든 정책 통합
가용 물리적 자원 및 보안성에 대해 최적화된 프레임워크		가용 물리적 자원/보안 강건성에 대해 최적화된 프레임워크(ISO 27001에서는 계획-실천-확인-조치) ISO 27001)
복원성	X	가상 물리 공격 포함
장애 허용 능력	X	가상 물리 공격 포함
시스템 위협 탐지 및 대응		OODA 관찰-방향설정-결정-실행
장치의 모니터링	X	
협조 및 위협 분석	X	
ID 관리	X	연합 ID 관리, 시스템 간 ID 상관관계, …
장치의 ID 보안	X	

기능		비고
인증 관리	X	데이터의 책임/부인 방지
이상 탐지		

2. 차세대 지원 기술

	차세대 지원 기술		비고
연결성	차세대 위성 연결을 위한 전송 계층 프로토콜		보다 높은 대역폭, 높은 지연시간
	5세대 셀룰러 액세스(5G)	X	
	저전력 무선 액세스 (LPWAN)	X	
처리	시스템 구성 및 동적 구성	X	
	데이터 맥락화	X	
	자율 데이터 교환		
	센서 융합 기술	X	
	기계 학습	X	
	가상화		
메모리	디지털 제품 메모리		
감지	초정밀 위치 기술	X	
조치	증강 현실		
	가상 현실		
	촉각 인터넷	X	
보안	사물의 ID	X	
	준동형 암호화		
	검색 가능 암호화		
	신뢰 구축		
	보안화 시스템 협업 기술	X	
	사용 제어를 통한 개인정보보호		
	지속적인 보안 감사		
	IoT용 IAM 기술		ID 및 액세스 관리
	애플리케이션 격리 및 보안 경계 기술		

4. 필요한 미래 표준

	표준 요구사항		비고
연결성	5G 표준의 실현	X	
	표준 위성과 장치 간의 보다 높은 대역폭/요구 지연시간을 지원하기 위한 새로운 전송 계층 프로토콜에 대한 표준		
	IoT 장비가 새로운 연결성 표준으로 업데이트하는 기능을 갖추도록 하는 표준	X	
프로세싱	정보 교환 모델	X	
	의미론 메타데이터 정의 표준 및 모델	X	
	데이터 교환 모델 및 인터페이스와 관련 표준	X	
	자율 데이터 교환 프로파일 및 교환 메커니즘		
	메타데이터 주석 모델 및 인터페이스		
	맥락화 정보 모델	X	
	메타데이터 컨텍스트 표준	X	
메모리	디지털 제품 메모리의 표준화		
감지	메타데이터에 대한 표준	X	
	초정밀 위치 기반 기술에 대한 추상화 기술		
	센서 데이터 개인정보보호 표준		최종 소비자/소비자의 옵트인/옵트아웃
	센서 융합 표준	X	센서 관찰을 추상화하는 센서 메타 모델 개발 표준. 이 표준은 정형화되지 않은 산발적 데이터를 고급 도메인 지식으로 바꿀 수 있는 기반이 된다.
조치	제어 인터페이스 장치 그룹을 고유하게 식별하는 표준 템플릿		
	시스템 간의 IoT 사용자 I/O를 일반화하는 일반 표준		
	고유한 IoT 접근성 요구사항에 대한 표준	X	일반적인 인간/컴퓨터 I/O를 뛰어넘는 고급 IoT 서비스 반영

	표준 요구사항		비고
허브	소셜 시스템 내 ID 연합 표준	X	
	가상 물리 공격 보호 표준	X	
	동시 연결을 갖춘 다중 시스템에서 장치 ID에 대한 표준	X	예: W3C로부터 국제화된 자원 식별자(IRI)
	플랫폼 무결성의 신뢰를 구축하기 위한 표준 프로토콜		
	협업 보안 프레임워크		상호 의존적인 시스템 간의 사이버 위협 분석 교환 활성화
	상호 의존적인 시스템 간에 보안 기능을 평가할 수 있는 성숙 모델		

참고문헌

[1] International Data Corporation (IDC), Explosive Internet of Things Spending to Reach $1.7 Trillion in 2020, According to IDC, 02 June 2015, [Online]. Available: http://www.idc.com/getdoc.jsp?containerId=prUS25658015. [Accessed 22 August 2016].

[2] Gartner Inc., The Internet of Things Is a Revolution Waiting to Happen, 30 April 2015. [Online]. Available: http://www.gartner.com/smarterwithgartner/the-internet-of-things-is-a-revolution-waitingto-happen. [Accessed 22 August 2016].

[3] McKinsey Global Institute, Unlocking the Potential of the Internet of Things, June 2015. [Online]. Available: http://www.mckinsey.com/business-functions/business-technology/our-insights/the-internet-of-thingsthe-value-of-digitizing-the-physical-world. [Accessed 22 August 2016].

[4] Gartner Inc., Infrastructure and Operations Leaders: Prepare for the IoT Rush, 2016.

[5] Wikipedia, Kevin Ashton, [Online]. Available: https://en.wikipedia.org/wiki/Kevin_Ashton. [Accessed 22 August 2016].

[6] ISO/IEC JTC 1, Internet of Things (IoT), Geneva, 2014.

[7] ISO/IEC 30141, Information technology – Internet of Things Reference Architecture, Working Draft.

[8] Industrial Internet Consortium, Industrial Internet Reference Architecture, [Online]. Available: http://www.iiconsortium.org/IIRA.htm. [Accessed 22 August 2016].

[9] ISO/IEC/IEEE 42010, Systems and software engineering – Architecture description, 2011.

[10] ITU-T Study Group 13, Next Generation Networks – Frameworks and Functional Models: Overview of the Internet of Things, International Telecommunication Union, Geneva, 2012.

[11] ZVEI – German Electrical and Electronic Manufacturers' Association, Industrie 4.0: The Reference Architectural Model Industrie 4.0 (RAMI 4.0), Frankfurt am Main, 2015.

[12] Internet of Things – Architecture Consortium, The IoT Architectural Reference Model (ARM) – D1.3, European Commission, Luxembourg, 2012.

[13] Industrial Internet Consortium, Industrial Internet Reference Architecture (Version 1.7), Object Management Group, Needham, MA, US, 2015.

[14] TAKABI, H., JOSHI, J. B. D., AHN, G. J., Security and Privacy Challenges in Cloud Computing Environments, IEEE Security and Privacy, vol. 8, no. 6, pp. 24-31, 2010.

[15] Gartner Inc., Digital Ethics, or How to Not Mess Up With, 2016.

[16] Industrial Internet Consortium, Industrial Internet Systems Volume G8: Vocabulary, 2016.

[17] Hitachi Ltd., Information and Control Systems – Open Innovation Achieved through Symbiotic Autonomous Decentralization, Hitachi Review Vol.65 (2016), No.5, 2016.

[18] Cisco, Global Cloud Index.

[19] BRANDHERM, B., KROENER, A., Digital Product Memories and Product Life Cycle, in Seventh International Conference on Digital Environments, 2011.

[20] Hitachi Ltd., Hitachi's Concept for Social Infrastructure Security, Hitachi Review Vol.63 (2014), No.5, 2014.

[21] CHAN, H., PERRIG, A., Security and privacy in sensor networks, Computer, vol. 36, no. 10, pp. 103- 105, 2003.

[22] McDANIEL, P., McLAUGHLIN, S., Security and Privacy Challenges in the Smart Grid, IEEE Security and Privacy, vol. 7, no. 3, pp. 75-77, 2009.

[23] WEIS, S. A., SARMA, S. E., RIVEST, R. L., ENGELS, D. W., Security and Privacy Aspects of LowCost Radio Frequency Identification Systems, in Security in Pervasive Computing, 1st International Conference, Boppard, Germany, 2004.

[24] MIMURA, M., Ph.D. ARAI, T., Ph.D. NAKANO, T., Ph.D. HATTORI, R., SATO, A., Hitachi's Concept for Social Infrastructure Security, Hitachi Review, 63 (5), 222-229, 2014.

[25] Machina Research, [Online]. Available: https://machinaresearch.com/news/global-m2m-market-togrow-to-27-billion-devices-generating-usd16-trillion-revenue-in-2024. [Accessed 22 August 2016].

[26] Gartner Inc., When Smart Things Rule the World - Introducing Autonomous Business, 2015.

[27] Gartner Inc., Internet of Things Scenario: When Things Become Customers, 2015.

[28] RODE, J., SCHMIDT, M., O'ROURKE, J., GERDSMEIER, S., SemProM: Semantic Product, 2009.

[29] GRANGEL-GONZALES, I., HALILAJ, L., COSKUN, G., AUER, S., COLLARANA, D., HOFFMEISTER; M., Towards a Semantic Administrative Shell for Industry 4.0 Components, 2016, [Online]. Available: https://arxiv.org/pdf/1601.01556.pdf. [Accessed 22 August 2016].

[30] Forrester Inc., Master Mobile Moments To Win In The IoT World, 2016.

[31] The Library of the Congress, What is a GPS? How does it work?, 2016.

[32] U.S. Coast Guard Navigation Center, GPS Frequently Asked Questions, 2016.

[33] U.S. Air Force, GPS Accuracy, 2016. [34] U.S. Air Force, GPS Modernization, 2016.

[35] GRAHAM, M., ZOOK, M., BOULTON, A., Augmented reality in urban places: contested content and the duplicity of code, Transactions of the Institute of British Geographers, vol. 38, no. 3, pp. 464-479, 2013.

[36] FETTWEIS, G., The Tactile Internet: Applications and Challenges, IEEE Vehicular Technology Magazine, pp. 64-70, March 2014.

[37] ITU-T Technology Watch, The Tactile Internet, International Telecommunication Union, Geneva, August 2014.

[38] SANS Institute, Tools and Standards for Cyber Threat Intelligence Projects, [Online]. Available: https:// www.sans.org/reading-room/whitepapers/warfare/tools-standards-cyber-threat-intelligenceprojects-34375. [Accessed 22 August 2016].

[39] Internet Engineering Task Force, Security Assertion Markup Language (SAML) 2.0 Profile for OAuth 2.0 Client Authentication and Authorization Grants, May 2015, [Online]. Available: https://tools.ietf. org/html/rfc7522. [Accessed 22 August 2016].

[40] OpenID Connect Core 1.0, November 2014, [Online]. Available: http://openid.net/specs/openid-connect-core-1_0.html. [Accessed 22 August 2016].

[41] Internet Engineering Taskforce, The OAuth 2.0 Authorization Framework, October 2012, [Online]. Available: https://tools.ietf.org/html/rfc6749. [Accessed 22 August 2016].

[42] Internet Engineering Task Force, System for Cross-domain Identity Management: Protocol, September 2015, [Online]. Available: https://tools.ietf.org/html/rfc7644. [Accessed 22 August 2016].

[43] Authentication and Authorization for Constrained Environments, [Online]. Available: https://datatracker.ietf.org/wg/ace/documents. [Accessed 22 August 2016].

[44] RFC 7252 Constrained Application Protocol, [Online]. Available: http://coap.technology. [Accessed 22 August 2016].

[45] [Online]. Available: http://mqtt.org. [Accessed 22 August 2016].

[46] [Online]. Available: https://www.predix.io/docs#Jig2gorb. [Accessed 22 August 2016].

[47] OAuth 2.0 Proof-of-Possession (PoP) Security Architecture draft-ietf-oauth-pop-architecture-07.txt, December 2015, [Online]. Available: https://tools.ietf.org/html/draft-ietf-oauth-pop-architecture. [Accessed 22 August 2016].

[48] Cloud Security Alliance, SDP Specification 1.0, 2014.

[49] KAWAI, H. et al., Access Authentication Solutions – Providing Flexible and Secure Network Access, NEC Technical Journal, 2014, vol. 8, no.2.

[50] Robot Revolution Initiative, [Online]. Available: https://www.jmfrri.gr.jp/english/info/256.html. [Accessed 22 August 2016].

[51] Industrial Value Chain Initiative, Industrial Value Chain Initiative Flyer English, [Online]. Available: https://www.iv-i.org/en/docs/IVI_Flyer_English.pdf. [Accessed 22 August 2016].

[52] IEC MSB, IEC White Paper Factory of the future, 2015, [Online]. Available: http://www.iec.ch/whitepaper/pdf/iecWP-futurefactory-LR-en.pdf. [Accessed 22 August 2016].

[53] Hitachi Ltd., Production Control System to Visualize Future Effects by Production Trouble, Hitachi Review Vol.61 (2012), No.6, 2012.

[54] Hitachi Ltd., An Anomaly Detection System for Advanced Maintenance, Hitachi Review, vol. 63, no. 4, 2014.

[55] Hitachi Ltd., TSCM Cloud Services for Implementing the Global Mother Factory Center Concept, Hitachi Review Vol.64 (2015), No.5, 2015.

[56] Reliability Centered Energy Management, Failure Mode Driven Maintenance Strategy, 2011.

[57] European Smart Cities, [Online]. Available: http://www.smart-cities.eu. [Accessed 22 August 2016].

[58] SICILIANO, B., KHATIB, O., Springer Handbook of Robotics, ISBN: 978-3-319-32550-7.

[59] CHRIYADAT, A., RADKE, R. J., Detecting Dominant Motions in Dense Crowds, Topics Signal Processing 2, 4, pp. 568-581, 2008.

[60] HAILEMARIAM, E., GOLDSTEIN, R., ATTAR, R., KHAN, A., Real-Time Occupancy Detection using Decision Trees with Multiple Sensor Types, in Proceedings of Symposium on Simulation for Architecture and Urban Design (SimAUD'11), 2011.

[61] VAN DER VEER, H., WILES, A., Achieving Technical Interoperability – the ETSI Approach, ETSI, 2008, 3rd Ed.

[62] IEEE, IoT Scenario and Use Cases: Social Sensors, IEEE IoT Scenario submitted by IEEE, 2016.

[63] IEEE, IoT improving journey experience in public transport for passengers with special needs, IEEE IoT Scenarios submitted by ATOS Research and Innovation.

[64] 3GPP, Service requirements for the Evolved Packet System (EPS), Version 13.3.0, 2016-06.

[65] NEC becomes first supplier to integrate semantic interoperability for IoT platforms, [Online]. Available: https:// www.fiware.org/press-coverage/nec-becomes-first-supplier-to-integrate-semantic-interoperabilityfor-iot-platforms-technology-to-be-demonstrated-at-the-etsi-m2m-workshop-2015-from-9-11- december-sophia-antipolis-france. [Accessed 22 August 2016].

IEC 백 서

발행일 2018년 9월
발행인 김동섭
지은이 IEC 산하 MSB(Market Strategy Board)
옮긴이 한국전력공사 기술기획처
발행처 한국전력공사 기술기획처
주 소 전남 나주시 전력로 55
전 화 061-345-4925
팩 스 061-345-4929

ISBN 978-2-8322-6117-0

International Electrotechnical Commission

3 rue de Varembe
PO Box 131
CH-1211 Geneva 20
Switzerland

T +41 22 919 0211
info@iec.ch
www.iec.ch