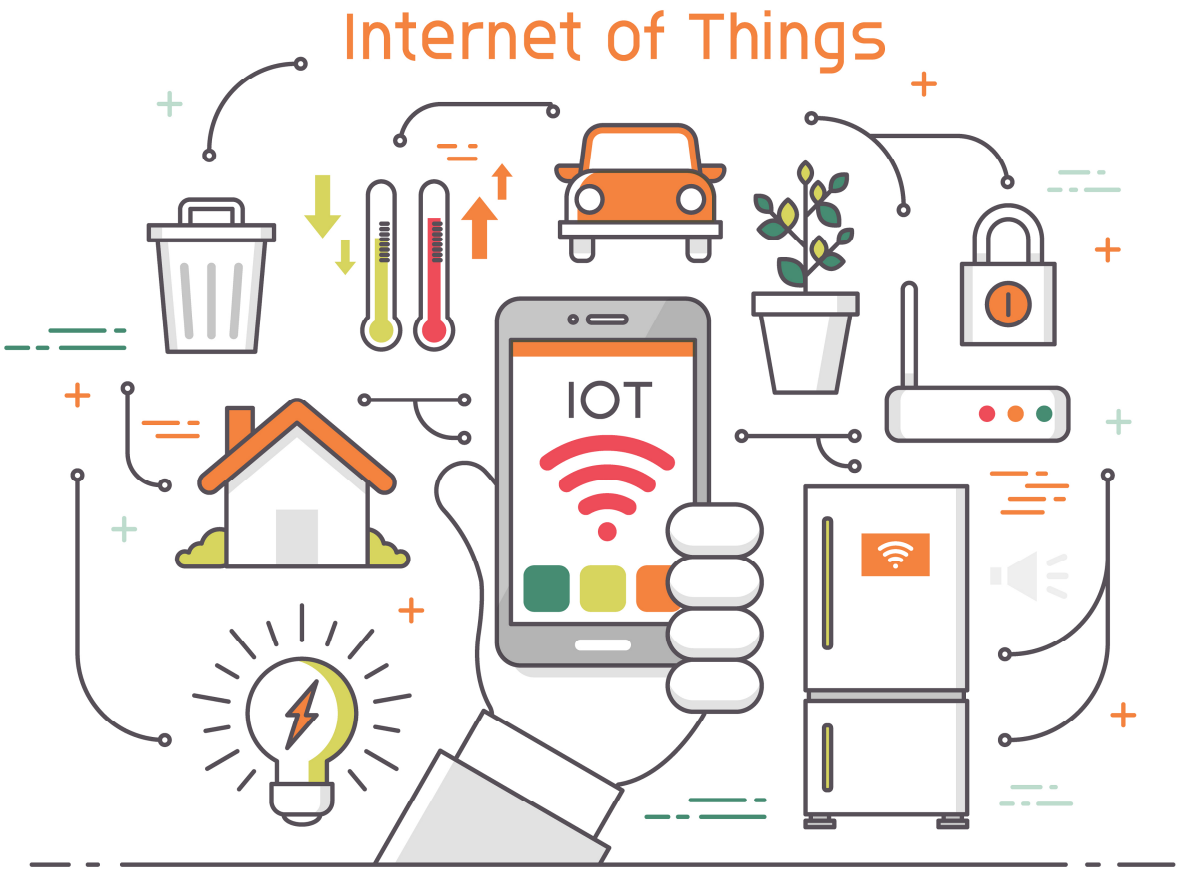
한국지능형사물인터넷협회
Korea Intelligent IoT Association

2023년 3월호

AIoT 월간 동향



〈 목 차 〉

산업 동향 | 1 사물인터넷(IoT) 시대의 도래, 과제와 전망

■ 사물인터넷을 통한 디지털 라이프스타일의 확장

스마트홈과 같은 디지털 라이프스타일이 확장되고, 산업에서도 제조, 의료 및 공공서비스에 광범위하게 적용되는 등 사물인터넷(IoT)은 우리 삶과 일에 점점 더 큰 영향을 미치고 있음. IoT 시장 동향을 발표하는 독일의 시장조사 업체 IoT애널리틱스(IoTAnalytics)에 따르면 2021년 전 세계에서 IoT로 연결된 장치수는 전년대비 8% 증가한 122억개로 파악됨. 코로나19 이전의 성장률에 비해 낮은 수치를 기록하였지만, 이는 IoT장치 및 시스템의 수요를 공급이 따라가지 못하기 때문에 나타난 현상임. IoT애널리틱스는 2023년에 IoT장치가 144억개, 2025년까지 270억개까지 증가할 것으로 예상함

산업 환경의 IoT도 증가하였음. 국제전기전자기술표준협회(IEEE)의 최근조사에 따르면 산업IoT(IIoT)는 2023년에 가장 중요한 기술 영역 중 하나가 될 것으로 전망됨. IoT가 지원되는 공장은 로봇 공학 및 자동화와 결합하여 사람들의 작업을 대신할 수 있음. IoT기반 시스템의 발전과 함께 인간은 점점 더 안전하고 효율적인 공장을 만들 수 있음. 예를 들어, 중국 북부의 텐진 항구는 코로나19로 인한 공급망 중단과 노동력 부족에 대처하기 위해 선박을 수리하고 정비하는 도크 운영을 완전 자동화하는 것을 목표로 3~5년안에 디지털트윈을 개발할 계획임. 항구는 통신기술, 인공지능 및 자율주행회사와 협업을 추진함. 빠르고 안정적인 네트워크 연결을 구축하여 무선기술을 활용해 소프트웨어와 센서를 설치한 자율차량과 로봇을 운행할 계획임

메타버스의 발전은 IoT 트렌드를 가속화 할 것임. 게임과 토큰(Token)을 넘어서 메타버스와 비즈니스 부문이 통합되어 '산업메타버스'를 형성할 것임. 중국의 전자상거래 플랫폼 제이디닷컴(JD.com)은 거래네트워크,

창고 및 유통 네트워크, 서비스 네트워크의 융합을 통해 디지털 전환을 실현하기 위해 노력하고 있음. 여러 기업들이 생산활동을 모니터링하고 제어하는 운영기술(OT)와 정보기술(IT)를 결합하여 디지털 기업의 투명성을 극대화하고 생성된 데이터를 통해 회사안팎에서 사용할 것으로 기대됨

■ IoT시대, 3가지 사회적 과제에 대한 논의 필요

IoT 확장을 위해서는 확장성, 상호 운용성 등 해결해야 할 기술적인 어려움이 많음. 셀룰러 네트워크(Cellular Network)를 통해 데이터를 전송하고 공유하는 셀룰러 IoT는 전 세계적으로 연결이 가능하지만 서로 다른 모바일 네트워크 사업자가 소유하고 있다는 문제가 있음. 따라서 글로벌 IoT솔루션은 전 세계 통신사와 계약을 체결해야 함. 이러한 기술적 문제 외에도 윈스턴마(WinstonMa) 뉴욕대학교 법학대학원 교수는 IoT시대의 3가지 사회적 과제를 제시함

디지털 인프라의 격차

고성능의 안정적인 디지털 인프라는 혁신을 가능하게 하는 중요한 요소임. 중국, 미국, 인도와 같은 국가는 5G 네트워크 및 클라우드 인프라 출시를 가속화하기 위해 막대한 투자를 하고 있음. 그러나, 신흥 시장은 디지털 인프라가 뒤처져 있으며, 저개발 국가의 많은 사람들은 경제성 및 기술 부족과 같은 장벽으로 인해 인터넷 연결의 이점을 얻을 수 없음. 챗GPT와 같은 최신 AI열풍이 보여주듯이 AI는 데이터를 기반으로 실행됨. 데이터가 많을수록 AI는 더욱 개선되며, 성능이 향상될수록 더 많은 사용자를 확보할 수 있음. 또한 더 많은 사용자를 확보할수록 더 많은 데이터를 보유하게 된다는 순환 구조가 있음. 인프라 부족으로 인해 신흥 시장에서 금융, 건강 및 교육이 제한되는 '인터넷격차'가 나타나는 가운데, 윈스턴 마 교수는 산업 부문에서 AI와 IoT 혁명이 발생시킬 'AI 격차'에 대해서도 지금 조치를 취해야 한다고 조언하였음

개인 정보 보호 및 보안 위협

수십억개의 연결된 장치가 민감한 정보를 수집하고 전송하는 IoT는 개인 정보 보호 및 보안이 중요함. 2023년에는 전 세계적으로 장치가 증가함에 따라 스마트 장치에 대한 공격이 대규모로 증가할 수 있음. 산업 IoT는 하드웨어, 소프트웨어, 데이터 전송 및 저장, 네트워크 연결 등과 같은 다양한 기술 요소를 결합하므로 여러 영역을 악용하여 무단 액세스를 얻을 수 있는 보안문제 발생 가능성도 제기됨

이스라엘 산업 사이버 보안 기업인 오토리오(OTORIO)는 산업용 무선 IoT의 보안 취약점이 발견되었다고 발표하였음. 해커는 기업의 내부 운영 기술네트워크에 대한 접근권한을 얻기 위해 산업용 무선IoT 장치의 취약점을 악용할 수 있음. 이러한 취약점을 이용하여 보안 계층을 우회하고 대상 네트워크에 침투하여 중요한 인프라를 위험에 빠뜨리거나 제조를 방해할 수 있음. 산업용 무선 IoT장치는 일반적으로 인터넷과 내부 OT 네트워크 모두에 연결되기 때문에 운영기술 환경에 심각한 위험을 초래할 가능성이 높음. 로니 개블로브(Ronni Gavrlov) 보안 연구원은 확인된 취약점 중 일부는 해커가 인터넷을 통해 수천개의 내부 운영기술 네트워크에 직접 연결할 수도 있다고 함. 해커가 전 세계의 다양한 무선 핫스팟 데이터베이스인 위글(WiGlE)과 같은 플랫폼을 활용하여 고 부가가치 산업 환경을 식별하고 물리적 위치를 파악하여 근접한 접근 포인트로 악용될 가능성도 있다고 지적함 기업이 실행할 수 있는 대책으로는 안전하지 않은 암호화체계를 비활성화하고, 와이파이(Wi-Fi) 네트워크의 이름을 숨길것을 권장함. 사용하지 않는 클라우드 관리 서비스를 비활성하고 장치가 공개적으로 접근이 가능하지 않도록 조치를 취하는 것이 좋음

전자 폐기물 증가로 인한 환경 오염

IoT 사용 확대로 인해 전자 폐기물 증가 문제도 우려되고 있음. 대부분의 IoT장치에는 납, 수은, 카드뮴, 베릴륨과 같은 중금속을 비롯해서 다수의 유해 화학 물질이 포함되어 있음. 세계 전자 폐기물 보고서(Global E-waste Monitor)에 따르면 최근 몇 년 동안 전 세계에서 5,000만톤 이상의 전자폐기물이 발생하였음. 스마트 웨어러블 장치, 스마트 자동차 및 더 많은 산업 IoT장치의 증가는 더 많은 전자폐기물의 발생으로 이어질 것임. 이에 따라 재활용 할 수 있는 지속가능한 솔루션을 찾을 필요가 있음

향후 10년간은 상당한 가능성과 잠재적 위험이 공존하는 가운데, 물리적 디지털 및 생물학적 세계의 융합을 보게 될 것임. 수천억의 비용이 투자되는 디지털 인프라가 필요하고, 실제로 구현될 것임. 산업의 변화는 우리가 10년 동안 목격한 IoT 발전을 뛰어넘을 것으로 전망됨. 마지막으로 윈스턴 마 교수는 새로운 IoT를 위한 충분한 데이터 규제, 개인 정보 보호 및 AI윤리를 준비해야 한다고 조언함

출처: NIPA 글로벌 ICT포털(https://www.globalict.kr), '23. 2

기술 동향

② 산업용 무선 IoT 기기의 OT(Operation Technology) 보안 취약점 및 완화 방안

OT(Operation Technology)팀은 흔히 무선 및 셀룰러 솔루션을 통해 산업 제어 시스템(Industrial Control System, ICS)을 원격 제어 및 모니터링 시스템에 연결한다. 이런 솔루션에는 해당 솔루션 제공업체가 운영하는 클라우드 기반 관리 인터페이스가 포함되기도 한다. 산업용 무선 IoT 기기라고도 하는 이 연결 솔루션은 OT 네트워크의 공격 표면을 늘리고 원격 공격자에게 핵심 컨트롤러가 포함된 네트워크 세그먼트로 들어가는 지름길을 제공할 수 있다.

※ 출처: Getty Images Bank

최근 산업 사이버보안 업체 오토리오(Otorio)가 산업용 무선 IoT 기기를 위험에 빠트릴 수 있는 공격 벡터와 여러 제품에서 발견된 취약점을 정리한 보고서를 발표했다. 오토리오 연구팀은 보고서에서 “산업용 무선 IoT 기기와 클라우드 기반 관리 플랫폼은 비교적 악용이 쉽기 때문에 산업 환경에 침투하기 위한 첫 교두보를 물색하는 공격자에게 매력적인 표적이 된다”라고 경고했다.

전통적인 OT 네트워크 아키텍처의 변화

지금까지 OT 보안은 일반적으로 퍼듀 엔터프라이즈 참조 아키텍처(Purdue Enterprise Reference Architecture, PERA) 모델에 따라 강력한 액세스 제어 계층을 두고 세분화(segmentation)를 수행할 지점을 결정했다. 1990년대에 만들어진 이 모델은 엔터프라이즈 IT와 OT 네트워크를 6단계의 기능 레벨로 분할한다.

레벨 0은 물리적 프로세스에 직접적으로 영향을 미치는 장비다. 밸브, 모터, 액추에이터, 센서 등을 포함한다. 레벨 1 혹은 기본 제어 계층에는 엔지니어가 업로드하는 로직(프로그램)에 따라 레벨 0 센서와 밸브, 액추에이터를 제어하는 PLC(Programmable Logic Controller), RTU(Remote Terminal Unit)과 같은 필드 컨트롤러가 포함된다.

레벨 2는 감시 제어 계층으로, 레벨 1 컨트롤러에서 수신된 데이터를 수집하고 조치를 취하는 SCADA(Supervisory Control and Data Acquisition) 시스템을 포함한다. 사이트 제어 계층인 레벨 3은 엔지니어링 워크스테이션처럼 설비의 운영을 직접적으로 지원하는 시스템을 포함한다. 주로 데이터베이스 서버, 애플리케이션 서버, HMI(Human-machine Interface), 필드 컨트롤러를 프로그램하는 용도 등으로 사용된다. 일반적으로 제어 센터(Control Center)라고 하며, 비무장지대(DMZ)를 통해 기업의 일반 IT 엔터프라이즈 네트워크(레벨 4)에 연결된다.

기업은 네트워크의 IT와 OT 부분을 견고하게 세분화하기 위해 DMZ에 경계 보안의 초점을 맞춰왔다. 또한 제어 센터 침해에서 필드 기기를 보호하기 위해 일반적으로 레벨 3과 레벨 2 사이에 부가적인 제어 수단을 구축한다.

그러나 특성에 따라 중앙 제어 센터에 연결해야 하는 원격 산업용 환경이 존재할 수 있다. 여러 위치에서 유전이나 가스정을 탐사하는 가스 및 석유 산업에서 보편적이며, 다른 업계에서도 흔히 볼 수 있다. 원격 레벨 0~2 기기와 레벨 3 제어 시스템 간 연결은 산업용 셀룰러 게이트웨이 또는 산업용 와이파이 액세스 포인트에 의해 제공되는 경우가 많다.

이런 산업용 무선 IoT 기기는 모드버스(Modbus), DNP3와 같은 여러 프로토콜을 통해 필드 기기와 통신하고, VPN과 같은 다양한 보안 통신 메커니즘을 사용하여 인터넷을 통해 기업의 제어 센터에 다시 연결할 수 있다. 또한 제조업체는 산업용 자산 소유자가 기기를 원격으로 관리할 수 있도록 클라우드 기반 관리 인터페이스를 제공한다.

산업용 무선 IoT 기기의 취약점

인터넷에 연결되는 모든 기기가 그러하듯 산업용 무선 IoT 기기 역시 공격자에게 OT 네트워크의 하위 레벨에 침투하는 우회 경로를 제공해 OT 네트워크의 공격 표면을 늘리고 기업이 구축해 놓은 보안 제어를 약화시킨다. 오토리오 연구팀은 보고서에서 “쇼단(Shodan)과 같은 검색 엔진을 이용해서 산업용 셀룰러 게이트웨이와 라우터가 광범위하게 노출돼 있고 손쉽게 발견할 수 있으며, 위협 행위자의 악용에 잠재적으로 취약한 상태임을 확인했다”라고 말했다. 연구팀이 쇼단에서 발견한 인터넷 접속이 가능한 웹 서버 및 인터페이스 수는 다음과 같다.

업체명	서버 및 인터페이스 수	필터
시에라 와이어리스 (Sierra Wireless)	96,715	http.title:ACEmanager
텔토니카 네트웍스 (Teltonika Networks)	37,100	http.title:Teltonika
인핸드 네트웍스 (InHand Networks)	13,990	http.html:"Login failed! Check your username & password"
목사(Moxa)	1,782	http.html:"MOXA OnCell"
ETIC 텔레콤 (ETIC Telecom)	1,538	http.html:"ETIC TELECOM"

이 중 연구팀은 시에라(Sierra), 인핸드(InHand), ETIC 텔레콤(ETIC Telecom) 기기의 웹 기반 인터페이스에서 24개의 취약점을 발견했다. 테스트 결과, 3사의 기기에 모두 원격 코드 실행 권한을 획득할 수 있었다.

상당수의 결함은 여전히 책임 공개(responsible disclosure) 과정에 있었지만, 이미 패치가 배포된 한 결함(CVE-2022-46649)은 시에라 와이어리스 에어링크(Wireless AirLink) 라우터에 여전히 영향을 미치는 것으로 나타났다. 와이어리스 에어링크에서 사용하는 웹 기반 관리 인터페이스인 ACE매니저(ACEManager)의 IP 로깅 기능에 명령을 주입할 수 있는 취약점으로, 오토리오 연구팀이 2018년 탈로스(Talos)에서 발견한 결함(CVE-2018-4061)의 변형이다.

시에라가 CVE-2018-4061에 대처하기 위해 넣은 필터링은 모든 익스플로잇 시나리오를 차단하지 못했다. 오토리오 연구팀은 이 방화벽을 우회하는 데 성공했다. CVE-2018-4061에서 공격자는 -z 플래그를 사용해서 ACE매니저 iplogging.cgi 스크립트가 실행하는

tcpdump 명령에 부가적인 셸 명령을 붙일 수 있다. 이 플래그는 명령줄 tcpdump 유틸리티에 의해 지원되며, postrotate 명령을 전달하는 데 사용된다. 시에라는 iplogging 스크립트로 전달된 명령에서 공백, 탭, 폼 피드 또는 세로 탭이 뒤따르는 모든 -z 플래그를 제거하는 필터를 강제 실행해서 문제를 수정했다(예를 들어 “tcpdump -z reboot”는 차단됨).

오토리오에 따르면, 시에라가 놓친 것은 -z 플래그는 상기된 문자가 뒤따르지 않아도 동작한다는 점이다. 즉, "tcpdump -zreboot"와 같은 명령은 정상적으로 실행되어 필터링을 우회하게 된다. 이 우회만으로는 공격자가 디바이스에 이미 존재하는 바이너리 파일만 실행할 수 있다는 제약이 있으므로 연구팀은 iplogging_upload.cgi라는 다른 ACE매니저 기능을 통해 디바이스에 업로드되는 PCAP(패키지 캡처) 파일에 페이로드를 숨기는 방법을 고안했다. 이 PCAP 파일은 sh(셸 인터프리터)에 의해 파싱될 때 셸 스크립트로도 작동 가능하며 iplogging.cgi의 -z 취약점을 사용해 파싱 및 실행을 트리거할 수 있다.

클라우드 관리의 위험

기기가 웹 기반 관리 인터페이스를 인터넷에 직접 노출하지 않는다 해도 원격 공격자의 접근이 완벽하게 차단되지는 않는다. 대부분 솔루션 업체가 구성 변경, 펌웨어 업데이트, 기기 재부팅, 기기에 대한 터널 트래픽 등을 수행하기 위해 클라우드 기반 관리 플랫폼을 제공하기 때문이다.

기기는 일반적으로 MQTT와 같은 M2M(machine-to-machine) 프로토콜을 사용해 클라우드 관리 서비스와 통신하는데, 구현에 약점이 존재할 수 있다. 오토리오 연구팀은 업체 3곳의 클라우드 플랫폼에서

공격자가 클라우드로 관리되는 기기에 인증 없이 원격으로 침투할 수 있도록 허용하는 치명적인 취약점을 발견했다.

연구팀은 “원격 공격자는 한 솔루션 업체의 클라우드 기반 관리 플랫폼을 표적으로 삼아 다양한 네트워크와 섹터에 위치한 수천 개의 기기를 노출시킬 수 있다. 클라우드 관리 플랫폼의 공격 표면은 웹 애플리케이션(클라우드 사용자 인터페이스) 악용, M2M 프로토콜 오용, 취약한 액세스 제어 정책, 취약한 등록 프로세스 오용 등 광범위하다”라고 설명했다.

연구팀은 인핸드 네트웍스의 클라우드 플랫폼 디바이스 매니저(Device Manager)와 인라우터(InRouter) 기기의 펌웨어에서 발견한 3가지 취약점 체인을 예로 들었다. 클라우드로 관리되는 모든 인라우터 기기에서 루트 권한으로 원격 코드를 실행할 수 있는 취약점 체인이다.

먼저 연구팀은 기기가 MQTT를 통해 플랫폼과 통신하는 방식과 인증 또는 ‘등록’이 수행되는 방식을 관찰해서 등록에 사용되는 값의 난수화가 충분하지 않아 무차별 대입 공격이 가능하다는 사실을 발견했다. 즉, 연구팀은 3가지 취약점 중에서 2가지를 사용, 인증된 연결을 가장해 호스트이름 변경과 같은 작업을 라우터에 쓰는 방식으로 라우터가 구성 파일을 제공하도록 강제할 수 있었다.

3번째 취약점은 라우터가 MQTT를 통해 구성 파일을 파싱하는 방식, 특히 auto_ping이라는 기능을 위한 매개변수를 파싱하는 데 사용되는 함수에 있었다. 연구팀은 auto_ping을 활성화한 다음 리버스 셸 명령줄을 auto_ping_dst 함수에 연결하면 기기에서 루트 권한으로 실행할 수 있다는 점을 발견했다.

OT 네트워크에 대한 무선 공격

인터넷을 통해 악용할 수 있는 원격 공격 벡터 외에도 문제의 기기는 와이파이와 셀룰러 신호도 로컬로 노출하므로 이런 기술을 통한 공격도 가능하다. 연구팀은 “와이파이 및 셀룰러 통신 채널을 대상으로 다양한 유형의 로컬 공격을 사용할 수 있다. WEP와 같은 약한 암호화에 대한 공격과 취약한 GPRS에 대한 다운그레이드 공격부터 패치하는 데 많은 시간이 걸릴 수 있는 복잡한 칩셋 취약점에 대한 공격까지 가능하다”라고 말했다.

연구팀은 와이파이 또는 셀룰러 기저대역 모뎀 취약점은 조사하지 않았지만, 전 세계 무선 액세스 포인트에 대한 정보를 수집하는 공개 무선 네트워크 매핑 서비스인 WiGLE을 사용해 정찰을 수행했다. 연구팀은 “고급 필터링 옵션을 활용해서 파이썬 스크립트를 작성해 가치가 높은 산업 또는 핵심 인프라 환경을 스캔하면서 약한 암호화로 구성된 환경을 파악했다. 스캔에서는 산업 및 핵심 인프라와 관련된 수천 개의 무선 기기가 발견됐으며, 그중 수백 개는 공개적으로 알려진 약한 암호화로 구성된 상태였다”라고 덧붙였다.

연구팀은 이런 기법을 사용해 실제 제조 설비와 유전, 변전소, 상수 처리 설비 등에서 무선 암호화가 취약하게 구성된 채로 사용되는 기기를 발견했다. 공격자 역시 이와 같은 정찰 기법으로 취약한 기기를 발견한 다음, 사이트로 이동해 악용할 수 있다.

무선 IoT 기기의 취약점을 완화하는 방법

제조 설비와 유전, 변전소, 상수 처리 설비 같은 기기는 OT 네트워크에서 높은 권한을 갖고 핵심 컨트롤러에 직접적으로 액세스할 수 있으므로 취약점이 발견될 때 패치하는 것이 매우 중요하다. 또한

위험을 낮추기 위해서는 패치 외의 부가적인 예방책도 마련해야 한다. 오토리오 연구팀이 제시한 권장 사항은 다음과 같다.

- 안전하지 않은 암호화(WEP, WAP)를 비활성화하거나 사용하지 말고 가능하다면 GPRS와 같은 레거시 프로토콜을 금지한다.
- 네트워크 이름(SSID)을 숨긴다.
- 연결되는 기기에 대해 MAC 기반 화이트리스트 또는 인증서를 사용한다.
- 관리 서비스가 LAN 인터페이스로 제한되는지 또는 IP 화이트리스트에 등록돼 있는지 확인한다.
- 기본 자격 증명을 사용하지 않도록 한다.
- 사용 중인 기기에 배포할 새로운 보안 업데이트가 나오는지 항상 주시한다.
- 사용하지 않는 서비스를 비활성화한다(대부분 기본적으로 활성화된다).
- 별도의 보안 솔루션을 구현하고(VPN, 방화벽 등) IIoT의 트래픽을 신뢰할 수 없는 트래픽으로 취급한다.

출처: IT월드(https://www.itworld.co.kr), '23.2.14(금)

기술 동향 | 3 열차의 안전운행, IoT 데이터에서 답 찾는다

철도에서의 IoT(사물인터넷)는 철도차량, 철도 연변의 각종 시설물, 정거장 및 역사 등 철도와 관련된 사물이 상호 작용을 위한 연결성을 가진 상태에서 다양한 상태 모니터링 및 이를 활용한 고도화된 철도 서비스를 제공하고 있다.

각종 센서(Sensor)와 IoT 기술을 활용해 열차 주요 장치를 실시간으로 원격 감시함으로써, 운행 중 이례사항을 사전 예측·대비하고 데이터를 분석하여 정비주기를 최적화한다. 이를 통해 철도차량의 고장을 방지할 수 있을 뿐만아니라, 안전 정보의 실시간 공유를 통해 열차의 안전운행을 보장할 수 있다.

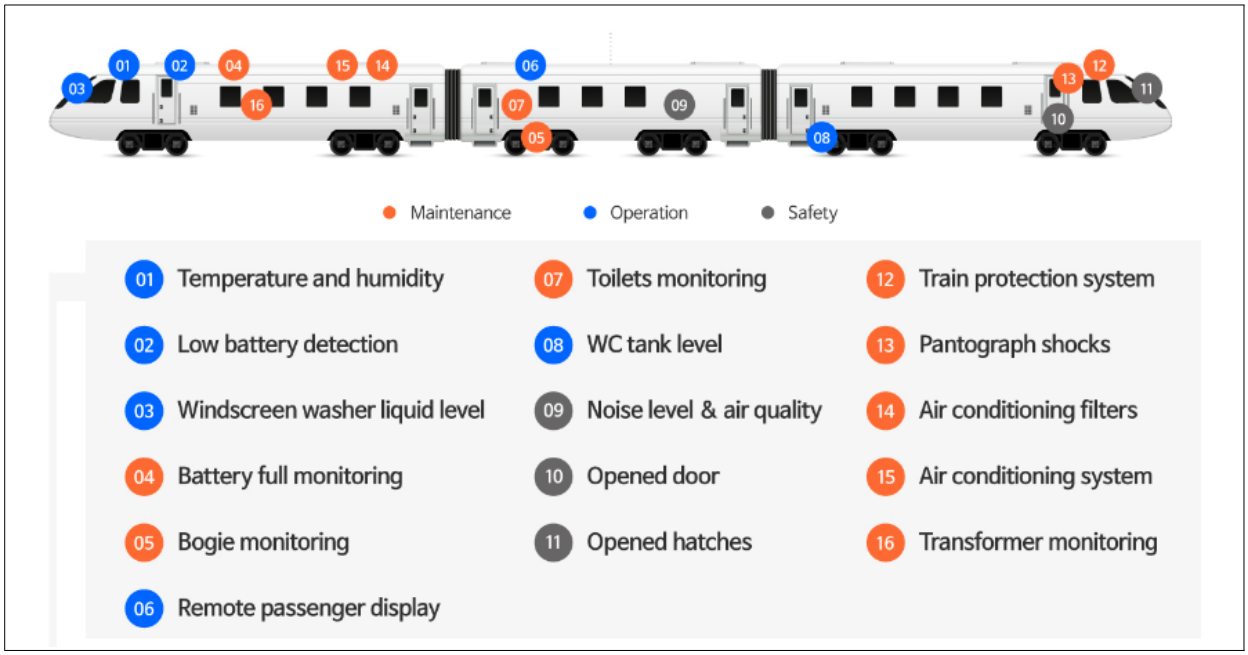
유럽의 철도차량 기술사양인 TSI(European Technical Specification for Interoperability)에서는 철도차량에 대한 실시간 차상 모니터링 방안에 대해 규정함으로써 철도차량의 탈선감지 및 오작동 검측을 강화하고 있다.

독일의 Knorr-Bremse社는 철도차량 제동시스템에 포함된 대차 모니터링 진단시스템인 COMORAN(Condition Monitoring for Railway Application)을 개발하여 안전과 관련된 중요 항목인 윤축 베어링의 손상, 불안정 주행 또는 탈선 등을 모니터링하여 감시제어하고 있다.

특히, 유럽에서는 GSM-R(Global System for Mobile Communication)이라는 무선정보 통신 시스템을 개발하였고, ERTMS-ETCS(European Railway Traffic Managment System-European Train Control System) 및 InteGRail 프로젝트를 통해 철도 운영관리 분야에서 열차-열차간, 열차-인프라간 정보를 공유하고 철도 정보를 통합 관리를 통해 철도 운영의 효율화 및 안전관리의 최적화를 목표로 하고 있다.

우리나라 철도차량제작사인 현대로템은 철도차량의 정보들을 디지털화해 사용자 중심의 유용한 정보로 변환하는 프로세스를 구축 중이다. 앞으로 IoT를 이용한 철도차량의 정보 수집 및 분석을 통한 실시간 진단 모니터링 솔루션 개발 단계를 넘어, 철도차량과 관련된 모든 정보를 자산으로 관리하는 자산 관리 솔루션을 개발해 디지털 서비스의 포트폴리오 완성을 준비하고 있다.

〈 IoT를 통한 철도차량 정보네트워크 구축 예 〉



※ 출처: 현대로템

출처: 철도경제신문(https://www.redaily.co.kr), '23.1.27(금)