정 보 보 호 학 회 지
제29권 제2호, 2019. 4

ITU-T 사이버물리시스템(CPS) 보안 표준화 동향

이 건 희*

요 약

ICT 기술을 이용하여 업무·공정의 효율성을 높이기 위한 사이버물리시스템(CPS)은 구성요소 간 연결성 강화로 인한 사이버 공격 요인이 증가하고 있으며, 이에 따른 보안대책 수립이 CPS 구축 단계에서부터 고려되어야 한다. 본 논문에서는 CPS를 위한 보안대책의 온전한 수립을 위한 국제표준 동향을 ITU-T SG17의 표준화 활동을 중심을 살펴보고자 한다. ITU-T SG17에서 진행되고 있는 IoT 보안 표준, 스마트그리드 보안 표준, ITS 보안 표준 등 CPS 관련 보안 표준화 동향을 기술하고, 향후 표준화 추진 방향에 대해서도 다룬다.

Ⅰ. 서 론

사이버물리시스템(Cyber Physical System, CPS)은 보통 물리적 구성요소와 사이버적 구성요소 간의 상호작용을 통해서 업무, 공정 등을 처리하는 시스템을 의미한다. 즉, 일반적으로는 업무, 공정 등에서 발생하는 정보를 컴퓨팅 장치가 수집·처리·분석하여, 적절하게 물리장치를 움직이도록 함으로써 그 업무 또는 공정이 정상적으로 목적을 달성하도록 하는 시스템을 의미한다. 제품 자동화 생산 공정부터 발전제어시스템까지 다양한 활용 분야가 있으며, 최근에 차세대 먹거리로 떠오르고 있는 스마트공장, 스마트그리드, 자율주행자동차, 스마트시티 등 많은 분야의 핵심 기술로 CPS를 꼽을 수 있다.

실제로 최근 여러 산업현장에서 디지털 트윈(Digital Twin, DT) 기술을 활용하여 실제 현장과 가상의 현장을 동일하게 구성하고, 실제 현장에서 발생하는 정보를 수집·처리·분석하여 동기화된 가상의 현장에서 시뮬레이션 후 판단 및 의사결정을 하는 시스템을 구축하여 운영 중이다.

CPS의 온전한 운영을 위해서 빅데이터 분석, 클라우드, IoT, 5G 등 최신의 ICT 기술을 혼용하여 사용하게 될 것이다. 더불어 현대 사회의 업무, 공정은 더욱 복잡해지고 있고, 서로 다른 공정과의 연계도 발생하게 되므로 서로 다른 CPS 시스템과의 연계도 안정적으로 보장되어야 한다. 예를 들어서 자동차 자체가 하나의 CPS 시스템이라고 할 수 있고, 커넥티드 카 기술은 CPS를 연계하는 기술이라고 할 수 있으며, 지능형 교통 시스템(Intelligent Transportation System, ITS)은 자체로도 CPS이지만 자동차라는 CPS의 복합체로 볼 수도 있다. 따라서 이렇게 복잡하게 변하고 있는 CPS의 안정적인 운영을 위해서는 적용되는 정보통신기술의 상호운용성 확보가 필수적이다. 이를 통해서 서로 다른 CPS 간 유기적 결합이 발생할 수도 있고, 하나의 CPS 내 서로 다른 구성요소 간의 결합도 더욱 유기적으로 만들 수 있다.

이에 ITU, ISO, IEC 등 표준화단체는 물론 IETF, IEEE, 3GPP, oneM2M 등 사실표준화단체에서도 활발하게 CPS에서 대한 표준을 개발하고 있다.

한편, 앞서 밝힌 바와 같이 CPS의 효과적인 운영을 위해 적용되는 ICT 기술로 인해 CPS에 대한 연결성이 높아지므로 다양한 공격 요인이 존재하고, CPS가 주로 활용되는 분야가 산업현장 또는 주요기반시설 등 주요 공격 목표에 해당하므로 CPS에 대한 사이버 보안 강화는 중요한 이슈 중 하나다. 이에 각 표준화단체에서는 CPS 보안 표준도 활발하게 개발 중이다.

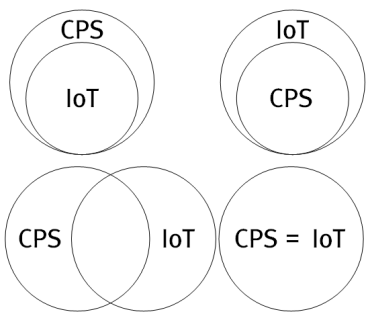
특히 ITU-T SG17 표준화 그룹은 통신 분야 정보보호 표준을 주도하는 표준화 그룹으로 CPS와 관련한 보안 표준을 개발 중이다. 이에 본 논문에서는 ITU-T SG17의 활동을 중심으로 CPS에 대한 보안 표준화 현황을 소개한다.

* ETRI부설연구소 (icezzoco@nsr.re.kr)

Ⅱ. ITU-T SG17 CPS 보안 표준화 분야

CPS가 동작하는데 필수적인 정보 수집·처리·분석 및 물리환경 제어 등에 있어 필수적인 기능은 네트워크 기술이 될 것이며, CPS를 구성하는 많은 요소에 네트워크 기능이 필요하게 된다. 따라서 CPS를 구축하는 데 있어 모든 구성요소 간 연결성을 보장하기 위해 사물인터넷(IoT) 기술은 필수적이다. 이에 최근 미국 국가표준기술원(NIST)에서 발간한 보고서에서는 CPS와 IoT 간의 관계를 그림 1과 같이 포함, 동등 또는 일부 중복 관계로 설명하고 있다.[1] 이는 결국 CPS와 IoT는 서로 분리할 수 없는 관계라는 것을 의미한다. 따라서 CPS 표준화 동향을 살펴볼 때 반드시 함께 고려해야 할 것이 IoT 기술의 보안성 확보를 위한 표준이다. ITU-T SG17에서는 사물인터넷 보안을 중요한 표준화 분야로 간주하고 다양한 표준을 개발하고 있다. 이에 본 논문에서는 ITU-T SG17의 사물인터넷 보안 표준화 동향을 살펴보고자 한다.

또한, CPS의 활용 분야와 관련한 표준화가 ITU-T SG17에서는 이루어지고 있다. 앞서 CPS의 주요 활용 분야로 스마트그리드, 자율주행 자동차 등을 제시하였는데, ITU-T SG17에서는 스마트그리드 분야 보안 표준과 ITS 분야 보안 표준을 개발하고 있다. 특히 ITS 보안에는 많은 관심이 집중되어 별도의 ITU-T SG17 내 별도 표준화 그룹이 존재한다. 이에 본 논문에서는 ITU-T SG17에서 이루어지는 스마트그리드 보안 및 ITS 보안 표준화 동향도 살펴볼 예정이다.



〔그림 1〕 NIST에서 분석한 CPS와 IoT 간의 관계

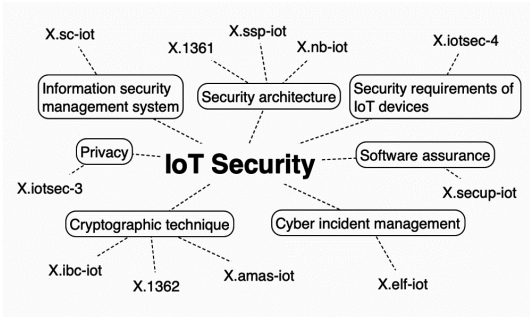
Ⅲ. 사물인터넷 보안 표준화 동향

최근 ITU-T SG17에서는 사물인터넷의 보안성 강화를 위한 표준이 다수 개발되고 있다. 이는 사물인터넷 기술이 다양한 분야에서 사용되면서 그 중요성이 높아진 것과 관련성이 높다고 볼 수 있다. ITU-T SG17에서 사물인터넷 보안은 Question 6(Security aspects of telecommunication services, networks and Internet of Things)에서 주로 다루고 있다.

표 1에서 보는 바와 같이 Q6에서는 현재까지 총 2건의 사물인터넷 보안 표준을 개발하였으며, 현재 총 9개의 표준을 개발 중이다. 개발 중인 표준 중 3건의 표준

〔표 1〕 사물인터넷 보안 표준 목록

Acronym	Title	Timing
X.1362	Simple encryption procedure for Internet of things (IoT) environments	2017/03
X.1361	Security framework for the Internet of things based on the gateway model	2018/09
X.ibc-iot	Security framework for use of identity-based cryptography in support of IoT services over telecom networks	2019/09
X.iotsec-3	Technical framework of PII (Personally Identifiable Information) handling system in IoT environment	2019/09
X.nb-iot	Security requirements and framework for narrow band Internet of Things (IoT)	2019/09
X.secup-iot	Secure software update for IoT devices	2019/09
X.amas-iot	Aggregate message authentication scheme with group authentication capability for IoT environment	2020/03
X.elf-iot	Standard format of IoT error logs for security incident operations	2020/03
X.sc-iot	Security controls for Internet of Things (IoT) systems	2020/03
X.ssp-iot	Security requirements and framework for IoT service platform	2020/03
X.iotsec-4	Security requirements for IoT devices and gateway	2021/09



〔그림 2〕 ITU-T SG17 사물인터넷 보안 표준 동향

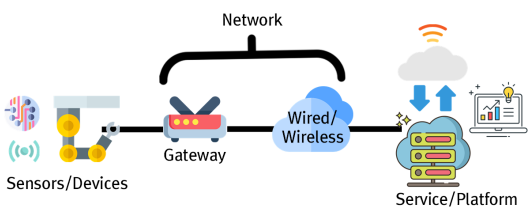
은 다음 회의에서 권고안 개발이 완료될 것으로 예상한다.

해당 권고 및 권고안을 범위와 내용으로 분류하면 그림 2와 같이 사물인터넷 시스템에 대한 보안 아키텍처(Security architecture), 정보보호관리시스템(Information security management system), 사물인터넷 기기에 대한 보안 요구사항(Security requirements for IoT devices), 사물인터넷 기기 내 소프트웨어 보증(Software assurance), 사물인터넷 시스템 사이버 침해 관리(Cyber incident management), 사물인터넷 적용 암호 기술 및 암호기술 활용 요구사항(Cryptographic technique), 개인정보보호(Privacy) 등으로 나눌 수 있다.

3.1. 보안 아키텍처(Security Architecture)

ITU-T SG17 산하 Q6는 IoT 유형별 보안 아키텍처를 다양하게 표준화하고 있다.

지난 2018년 8월 회의에서 최종 승인되어 ITU-T 권고안으로 공표된 X.1361은 IoT 환경 중 IoT 게이트웨이를 사용하는 구성(그림 3 참조)에 대한 보안 아키텍처를 정의한다.[2] 게이트웨이 기반 IoT 시스템에서의 보안 위협, 요구사항을 다루고, 보안 요구사항의 구현을 위해 각 구성요소의 보안 기능을 제시하고 있다. 이 표



〔그림 3〕 게이트웨이 기반 IoT 시스템

준을 통해서 게이트웨이를 사용하는 IoT 시스템이 공통된 보안대책을 수립할 수 있는 계기가 마련되었다.

현재 ITU-T SG17 Q6 내에서는 추가로 2건의 IoT 보안 아키텍처 관련 표준이 개발 중이다.

우선 X.nb-iot는 현재 이동통신 회사에서 서비스하고 있는 NB-IoT(Narrowband IoT) 환경에 대한 보안 요구사항을 정의하는 권고안이다. NB-IoT 구성요소를 단말, 네트워크, 응용으로 구분하고, 각 구성요소에 대한 보안 요구사항 및 보안 기능을 정의함으로써 NB-IoT 기술에 대한 보안성을 높이고자 한다. 2019년 8월 회의에서 표준안 초안 개발을 완료할 예정이다.

다음으로 X.ssp-iot는 지난 2018년 3월 회의에서 신규 워크 아이템으로 채택되어 개발 중인 권고안이다. IoT 서비스 플랫폼에 대한 보안 아키텍처를 제시하는 것이 목표이다. IoT 서비스 플랫폼은 IoT 서비스를 효율적으로 제공하기 위해 기기 관리, 연결 관리, 응용 관리 및 비즈니스 분석 등을 제공하는 통합 플랫폼으로 정의하고 있으며, 이에 대한 응용 보안, 데이터 보안, 시스템 보안, 인프라 보안, 인터페이스 보안 및 운영 보안 등의 관점에서 요구사항이 개발될 것으로 예상된다.

3.2. 정보보호관리시스템(ISMS)

ITU-T SG17 Q6에서는 IoT 시스템에 대한 정보보호관리시스템 구축이 가능하도록 X.sc-iot 표준을 개발 중이다. X.sc-iot는 IoT 시스템이 갖추어야 하는 보안원칙을 제시하고, IoT 시스템 관련 이해당사자(IoT 서비스제공자, IoT 서비스개발자, IoT 서비스사용자 등)들이 제시된 원칙을 올바르게 구현할 수 있도록 보안 통제사항 및 보안 통제사항 준수 가이드라인을 명시하는 표준으로 개발될 예정이다. 해당 권고안은 ISO/IEC JTC 1/SC 27/WG 4에서 개발 중인 ISO/IEC 27030(Guidelines for security and privacy in Internet of Things (IoT)) 표준과 공동 표준으로 개발하기 위한 계획을 세우고 있다.

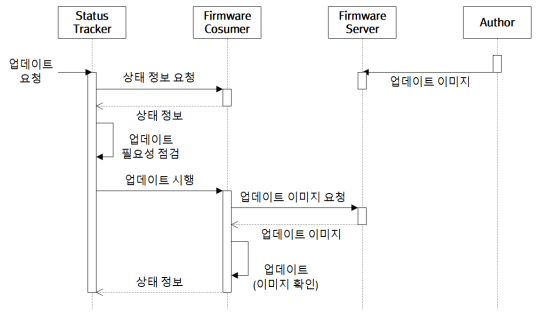
3.3. 소프트웨어 보증

IoT 환경에서는 다양한 형태의 최종 단말이 네트워크 및 시스템에 연계된다. 더불어 각 최종 단말의 관리 주체가 다양할 수 있다. 따라서 최종 단말 장악을 통해

IoT 시스템까지도 장악할 수 있는 공격 시나리오가 주요 위협 요인 중 하나다.

IoT 단말에 대한 다양한 보안 위협 중 큰 관심을 받는 위협요소는 소프트웨어 업데이트 기능을 통한 악성코드 유포를 들 수 있다. IoT 단말의 업데이트가 임의로 발생한다면 공격코드의 설치가 가능하고, 이를 통해 IoT 시스템의 중심으로 침입 전이가 가능하다.

이에 ITU-T SG17에서는 IoT 기기의 안전한 소프트웨어 업데이트 절차에 대해 표준화를 진행 중이다. X.secup-iot는 IoT 환경에서 발생 가능한 소프트웨어 업데이트 프레임워크를 명시하고, 해당 프레임워크에서 소프트웨어 업데이트를 안전하게 시행하기 위한 절차를 정의한다.



〔그림 4〕 IoT 소프트웨어 업데이트 절차

3.4. 사이버 침해 대응

X.elf-iot 권고안은 사이버 침해사고 발생 시 효율적인 사고조사를 위해 IoT 기기의 로그 형식을 단일화하기 위한 표준이다. 로그를 분석하는 보안관제, 보안사고 조사 등의 사례가 늘어가는 시점에서 로그를 단일화함으로써 침해사고 시계열 분석 및 연관성 분석 등의 효과가 증진될 것으로 보인다. 본 권고안은 2020년 3월 회의에서 권고안 개발을 완료하는 것을 목표로 개발 중이며, IoT 기기 로그 형식까지 정의된 상태다.

3.5. 암호 기술

ITU-T SG17은 지난 2017년 3월 IoT 기기를 위한 간단한 암호프로토콜 권고안을 최종 승인하고, X.1362 권고안으로 공개하였다. 해당 표준에는 연산 능력이 약한 IoT 기기에서 암호화로 인한 성능 저하를 최소화하고자 패킷 일부를 암호화함으로써 메시지 기밀성을 보호하기 위한 프로토콜을 정의하였다.

그 외에도 현재 ITU-T SG17 Q6에서는 2건의 암호기술 관련 권고안이 개발 중이다. 첫 번째로 IoT 환경에서 IBC(Identity-based Cryptography)를 사용할 때 보안 위협을 최소화하기 위한 보안 가이드라인을 제시하는 표준이 X.ibc-iot로 개발 중이다. 해당 권고안에서는 IBC를 안전하게 사용하기 위한 요구사항은 물론 IBC를 이용한 인증, 통신 데이터 보호 등을 위한 절차를 사례로 제시한다.

다음으로 X.amas-iot 권고안은 IoT 센서가 IoT 게이트웨이를 통해 서버로 데이터를 전송할 때 메시지 인증값을 종합(aggregation)하되 단일 메시지 인증이 가능하도록 하는 알고리즘을 표준화한다. 이를 통해 10개의 센서가 있을 때 5개의 인증값만 가지고도 10개의 센서 데이터 중 오류가 생긴 센서를 식별할 수 있게 된다.

3.6. 개인정보보호

X.iotsec-3은 개인식별정보를 처리하는 IoT 시스템이 개인식별정보를 안전하게 처리하기 위한 보안 요구사항을 제시하고, 서비스 공급자 구성(단일 또는 복수)에 따른 개인식별정보의 안전한 처리 프레임워크를 정의하는 표준이다. 2019년 1월 회의에서 개발을 완료할 예정이었으나, 일부 수정이 필요하여 다음 회의에서 수정안을 재검토하기로 하였다.

3.7. 기기 보안 요구사항

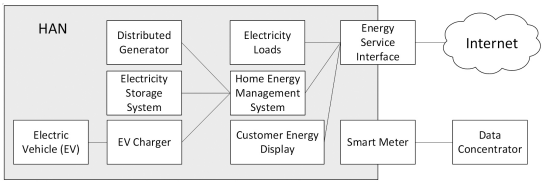
X.iotsec-4는 IoT 기기 및 게이트웨이에 대한 세부 기능 요구사항을 정의하는 표준이다. 이 권고안은 향후 기기 및 게이트웨이에 대한 보안성 평가 표준을 제정하기 위해 첫 단추를 채우는 것이라 평가할 수 있다. X.iotsec-4에서 정의되는 상세 기능에 대해서 시험·평가 방법을 정의하면 IoT 기기 보안성 평가 방법이 될 수 있을 것으로 기대하고 있다. 현재 이 권고안은 X.1361에 정의된 요구사항을 구현하기 위한 기능의 세부사항을 정의하는 중이다.

Ⅳ. 스마트그리드 보안 표준화 동향

스마트그리드는 CPS의 주요한 응용 분야다. 2000년대 후반 온실가스 배출 감소를 위한 신재생에너지 활용 및 노후화된 전력망 개선 등을 위해 스마트그리드가 큰 관심을 받았으며, 그로 인해 전 세계에서 다양한 스마트그리드 응용이 개발·시험운영 되었다.

ITU-T SG17에서는 2016년 3월 회의에서 스마트그리드 보안 기능 아키텍처에 대한 표준 부속서가 개발되었으며, 이후 2017년 9월 회의에서 가정용 스마트그리드 네트워크에 대한 보안 가이드라인이 X.1331로 표준화되었다.

X.1331 권고안은 스마트그리드에 연계되는 소비자 네트워크에 대한 보안 요구사항 및 보안 기능을 정의하는 권고이며, 그림 5[3]에서 보는 것과 같이 소비자 영역에 설치되는 분산전원(DG, ESS), 에너지관리시스템(EMS), 전력 부하(Load), 전기차(EV) 등과 해당 네트워크에 대한 보안 기능의 구현 방안을 명시하였다.



〔그림 5〕 스마트그리드에 연계되는 소비자 네트워크 구성

ITU-T SG17 Q6는 현재 AMI 데이터의 안전한 수집·처리·사용을 위한 스마트미터링 서비스에 대한 보안 가이드라인을 X.sgsec-3 권고안으로 개발 중이며, 해당 권고안은 2019년 8월 회의에서 개발 완료될 예정이다.

Ⅴ. 지능형교통시스템(ITS) 보안 표준화 동향

ITU-T SG17에서 스마트그리드와 함께 보안 표준을 개발하고 있는 주요 CPS로 지능형교통시스템을 들 수 있다. ITS는 차량과 교통시설을 통해 수집한 정보를 이용하여 교통체계 운영을 과학화하고, 교통체계의 효율성을 높이는 기술을 의미한다.[4] 최근에는 차량과 교통시설 간 연계를 넘어 차량과 차량 간 연계는 물론 차량 그룹 간 연계를 통해 더욱 다양한 서비스를 제공함으로써 교통체계를 효율화하기 위해 발전하고 있다.

ITS를 구축하기 위해 교통시설은 물론 차량에까지 네트워크를 기반으로 한 연계성이 증가하고, 다양한 소프트웨어가 추가됨에 따라 차량은 물론 ITS 자체에 대한 사이버 침해 요인이 증가하고 있다.[5] 이로 인해 ITS 구축에 있어 사이버 보안이 중요한 과제로 떠오르며 ITU-T SG17에서도 ITS 보안을 주제로 하는 표준화 그룹인 Question 13(Security aspects for Intelligent Transport System)이 2017년 생성되어 활발히 표준을 개발 중이다.

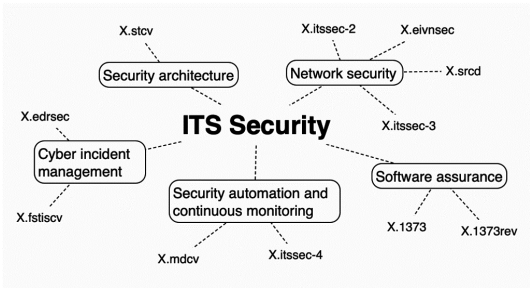
표 2에 명시된 바와 같이 ITU-T SG17에서는 Q13이

〔표 2〕 ITS 보안 표준 목록

Acronym	Title	Timing
X.1373	Secure software update capability for intelligent transportation system communication devices	2017/03
X.itssec-2	Security guidelines for V2X communication systems	2019/09
X.stcv	Security threats in connected vehicles	2019/09
X.itssec-3	Security requirements for vehicle accessible external devices	2020/03
X.itssec-4	Methodologies for intrusion detection system on in-vehicle systems	2020/03
X.mdcv	Security-related misbehaviour detection mechanism based on big data analysis for connected vehicles	2020/09
X.srcd	Security requirements for categorized data in V2X communication	2020/09
X.1373rev	Secure software update capability for intelligent transportation system communication devices	2021/09
X.edrsec	Security guidelines for cloud-based event data recorders in automotive environment	2021/09
X.eivnsec	Security guidelines for the Ethernet-based in-vehicle networks	2021/09
X.fstiscv	Framework of security threat information sharing for connected vehicles	2021/09
X.itssec-5	Security guidelines for vehicular edge computing	2021/09

생성되기 전 ITS 관련 표준 1개를 개발하였으며, 현재 Q13에서 총 11개의 표준을 개발 중이다. 각 권고안에 대한 자세한 내용은 지난 정보보호학회지를 통해 소개된 바 있으므로 생략하도록 하며, 상세 내용이 필요할 경우 해당 논문을 참조하도록 한다.[6]

해당 권고 및 권고안을 범위와 내용으로 분류하면 그림 6과 같이 ITS에 대한 보안 아키텍처(Security architecture), 차량과 ITS 간 네트워크 및 차량 내부 네트워크에 대한 보안(Network security), 차량 및 ITS 기기 내 소프트웨어 보증(Software assurance), ITS 사이버 침해 관리(Cyber incident management), ITS 사이버 침해 보안관제(Security automation and continuous monitoring) 등으로 나눌 수 있다.



〔그림 6〕 ITU-T SG17 ITS 보안 표준화 동향

Ⅵ. 결 론

본 논문에서는 CPS 보안 관련 국제 표준화 현황을 정리하기 위해서 ITU-T SG17에서 진행 중인 IoT 보안 표준, 스마트그리드 보안 표준, ITS 보안 표준 등의 주요 내용과 현황에 관해서 기술하였다.

스마트그리드, ITS 등은 사회 기반시설을 구성하는 주요 시스템이라는 시스템적 특성과 IoT 기술을 기반으로 연결성이 증가하는 환경적 특성으로 인해 CPS에 대한 사이버 위협이 지속적으로 증가하고 있고, 그에 따라 ITU-T SG17에서는 보안 아키텍처부터 사이버 침해사고 관리까지 3종의 표준을 개발하여 공표하였으며 22종에 이르는 보안 표준을 개발 중이다.

하지만 ITU-T SG17에서 이루어지는 표준화 과제들을 살펴보면 아직 다루고 있지 않은 부분이 존재한다. 특히 ITU-T SG17에서는 CPS 구성요소에 대한 물리 보안(Physical security)에 대한 보안 표준을 개발하지 않고 있다. 물론 각 보안 아키텍처, 기기 보안 요구사항 등에서 물리적 보안이 필요함을 요구사항으로 제시하고 있지만, 구체적인 보안 기능에 대한 보안 표준을 개발하지 못하고 있다. 더불어 최근 CPS 환경에서 가장 큰 이슈로 떠오르고 있는 공급망 공격 대응 기술과 관련한 표준이 개발되지 못하고 있다.

이와 함께 개발 중인 표준 기술에 대한 활용도를 높이기 위한 노력도 필요할 것으로 보인다. 이를 위해서는 IEC 등과 같이 실제 표준을 활용할 CPS 보안 분야 제조사 및 산업계에서의 표준화 활동 참여가 시급하다.

참 고 문 헌

[1] C. Greer, M. Burns, D. Wollman, E. Griffor, “Cyber-physical systems and internet of things,” *NIST Special Publication 1900-202*, 2019.

[2] ITU-T, “Security framework for the Internet of things based on the gateway model”, *ITU-T Recommendation X.1361*, pp.4, September 2018.

[3] ITU-T, “Security guidelines for home area network (HAN) devices in smart grid systems”, *ITU-T Recommendation X.1331*, pp.3-4, March 2018.

[4] ITS 소개, Retrieved March, 30, 2019, from http://its.go.kr.

[5] K. Strandberg, T. Olovsson, E. Jonsson, “Securing the Connected Car: A Security-Enhancement Methodology,” *IEEE Vehicular Technology Magazine*, 13(1), pp.56-65, March 2018.

[6] 이상우, 정보흥, 나중찬, “차량 통신 및 ITS 보안 국제 표준화 동향”, *정보보호학회지*, 29(1), pp.8-12, 2019.

〈저 자 소 개〉

이 건 희 (Lee, Gunhee)

정회원

2001년 2월 : 아주대학교 정보 및 컴퓨터공학부 졸업
2003년 2월 : 아주대학교 정보통신전문대학원 석사
2009년 2월 : 아주대학교 정보통신전문대학원 박사
2009년 3월~현재 : ETRI부설연구소 책임연구원
2018년 9월~현재 : ITU-T SG17 Q6/17 Associate Rapporteur
<관심분야> 제어시스템·CPS 보안, M2M 인증