CPS 안전·신뢰성 표준 동향

임태형 CPS 프로젝트 그룹(PG609) 위원, 한국정보통신기술협회 AI융합기술팀 책임연구원

1. 머리말

1조 센서 시대(Trillion sensor)가 온다. 과학기술정보통신부는 지난 1월 21일 '스마트 센서 연구개발 투자전략' [1]을 발표하면서 2025년 전 세계 센서 사용량이 1조 개를 돌파할 것으로 예측했다. 정확한 시기는 조금씩 다르지만 [2], 1조 센서 시대가 반드시 올 것이라는 점에 대해서는 기관 및 전문가 모두 이견이 없다.

1조 센서 시대는 물리적인 모든 것이 디지털 정보가 된다는 것을 의미한다. 1조 센서 시대는 사이버 물리 시스템(CPS, Cyber-Physical Systems)을 실현하는 이상적인 환경이다. CPS는 지능형 서비스를 제공하는 컴퓨팅으로 데이터 기반의 피드백 제어를 수행한다. CPS는 주변 환경에서 수집한 데이터를 근거로 시스템 스스로 상황을 판단하고 목적에 맞게 대상을 제어한다.

CPS의 대표적인 예는 자율주행자동차이다. 자율주행자동차는 라이다(LIDAR, Light Imaging Detection and Ranging), 레이더(RADAR, Radio Detection and Ranging), 카메라, GPS(Global Positioning System) 같은 센서로 도로와 자동차 상태, 운전자의 요청을 비롯한 전반적 상황을 파악한다. 그다음 최적의 주행 방향, 속도를 계산해 조향장치, 가속장치, 브레이크를 알아서 조정한다. CPS는 인간의 개입을 최소화하며 수행의 정확도와 정밀도, 효율성, 안전성, 신뢰성을 향상하는 편익을 가져올 것이다.

그러나 CPS의 장밋빛 미래를 꿈꾸기에는 아직 이르다. 2019년 발표된 기사에 따르면 자율주행에 대한 사람들의 신뢰도는 약 50% 수준에 그친다. [3] 2명 중 1명은 자율주행차를 안전하지

1 제15회 과학기술관계장관회의, 과학기술정보통신부, 2021년 1월 21일.

2 센서 분야 권위자인 야누즈 브라이젝(Janusz bryzek) 교수는 2014년 미국에서 개최된 'Trillion Sensor Summit'에서 1조 센서 시대의 시작을 2024년으로 전망했다.

3 "딜로이트, 자율주행차 안전성 소비자 신뢰 정체", 연합뉴스, 2019년 1월 9일.

않다고 생각한다. 신기술에 느끼는 막연한 불신일 수도 있으나, 불안감을 종식하지 못하면 자율주행차가 팔리지 않을 것이라는 점은 분명하다. CPS의 성공적 확산은 단지 1조 센서 시대가 도래하는 것만으로는 불충분하다. CPS가 자율적으로 피드백 제어를 하는 전 과정이 안전하고 신뢰할 수 있음을 보장해야 한다.

CPS 시대를 준비하고자 주요국은 CPS의 요소기술과 더불어 안전·신뢰성 확보 기술을 함께 연구·개발하고 있다. 본고에서는 미국, 유럽, 국내의 CPS 안전·신뢰성 확보 기술과 관련된 표준 동향을 차례로 살펴본다.

2. CPS 안전·신뢰성 표준 동향

2.1 미국: NIST CPS 프레임워크

미국은 2007년부터 대통령과학기술자문위원회[4]와 대통령혁신펠로우[5]를 통해 CPS를 국가의 미래를 결정하는 혁신기술로 지정하고, 미국국립표준기술연구소(NIST)[6]를 통해 구체적 실행 프로젝트를 추진했다. 2014년에 NIST는 다양한 분야의 CPS 전문가를 모아 5개 서브 그룹[7]으로 구성된 개방형 포럼인 CPS pwg(public working group)를 조직해 활동을 개시했다. 2017년 CPS PWG는 CPS를 물리 컴포넌트와 계산 컴포넌트가 긴밀히 상호작용해 '스마트 서비스'를 제공하는 SoS(System of Systems)로 정의하고, CPS 개발 단계에서 다양한 관심사를 어떻게 다룰지 분석하는 방법론인 CPS 프레임워크를 제시했다[1]. CPS 프레임워크는 CPS의 생명주기를 '설계-개발-검증'이라는 3단계로 구분하고 CPS 구축 시 고려할 관심사들을 기능, 비즈니스, 인간, 안전·신뢰성, 타이밍, 데이터, 경계, 복합성, 생명주기의 총 9가지 그룹으로 분류했다. 이에 따라 이해관계자들은 CPS 프레임워크의 CPS 생명주기와 관심사를 교차하는 두 축으로 놓고 어느 CPS라도 동일하게 접근할 수 있는 공통의 개념적 토대를 갖게 됐다.

NIST는 CPS 구축 시 고려할 관심사들을 종합적으로 제시했는데, 그중에서도 안전·신뢰성을 강조했다. 기존 시스템은 IT 영역인 사이버 환경에만 한정됐다. 반면에 CPS는 사이버와 물리 환경을 모두 포함해 시스템이 오작동할 경우 그 파급력이 훨씬 커졌기 때문이다. 원격 의료나 스마트 교통처럼 CPS가 응용되는 주요 분야는 안전이 필수이기 때문에 잠재 위험요소까지 꼼꼼하게 대비해야 한다. NIST는 안전·신뢰성(trustworthiness)의 개념을 보안성(security), 프라이버시(privacy), 안전성(safety), 신뢰성(reliability), 회복성(resilience)이 모두 포함된 포괄적인 것[8]으로 정의했다. 또한 이들 사이의 미묘한 차이를 구별할 뿐만 아니라 이들 사이의 상충 관계(trade off)까지 분석해 CPS를 설계, 개발, 검증해야 한다고 권한다[2].

---

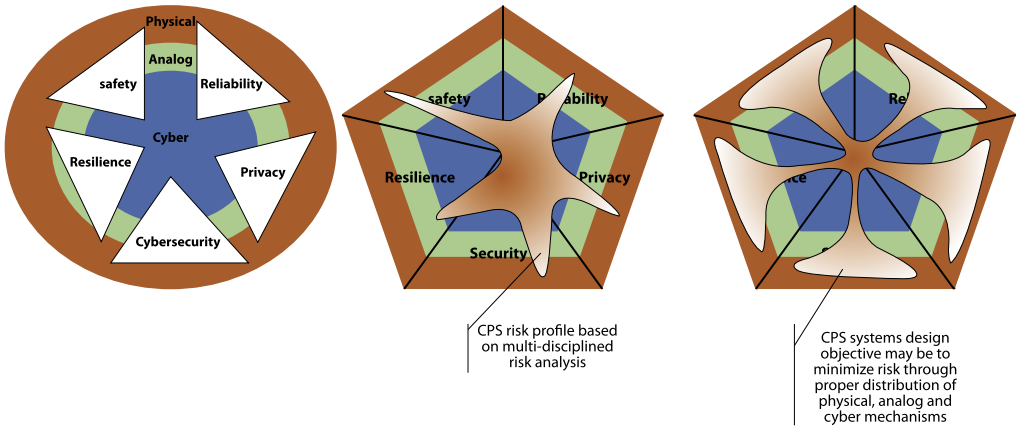
4 PCAST(President's Council Advisors on Science and Technology): 과학, 공학 분야의 전문가로 구성된 자문위원회로 각종 국가 정책방안 마련을 지원한다.

5 PIFs(Presidential Innovation Fellows): 민간, 비영리, 학계와 정부의 혁신가들을 한 팀으로 묶어서 진행하는 협업 백악관 산하의 혁신 프로그램.

6 NIST(National Institute of Standards and Technology): 산업의 기술 발전을 보조하고자 각종 기술과 측정 분야의 미국 국가 표준을 선정, 개발, 적용하는 미국 상무부 산하기관.

7 용어 및 참조 아키텍처 서브 그룹, 유즈케이스 그룹, 타이밍 및 동기화 그룹, 사이버 보안 및 프라이버시 그룹, 데이터 상호운용성 그룹

8 'trustworthiness'와 'reliability'는 모두 '신뢰성'으로 번역될 수 있지만 개념 차이를 나타내기 위해 'trustworthiness'를 '안전·신뢰성'으로 표기했다. 'reliability'는 HW 또는 SW가 고장으로 중단되지 않고 정상 운용되는 특성을 뜻하며, 'trustworthiness'는 보안, 안전, 고장, 유지보수, 가용성을 모두 포함한 상위 개념이다. 2.2절에 소개하는 AMASS에서는 'trustworthiness'와 대응되는 용어로 'dependability'를 사용한다.



[그림 1] NIST의 CPS 안전·신뢰성 확보 방안: 교차 위험분석 모델[2]

2018년 NIST는 미국의 밴더빌트 대학(Vanderbilt University)과 협력해 CPS 설계와 통합을 실험하는 오픈 소스 도구 'UCEF(Universal CPS Environment for Federation)'를 개발해 배포했다[3]. UCEF는 Java, C++, MATLABTM, OMNeT++, GridLAB-D, LabVIEWTM 같은 다양한 프로그래밍 언어와 모델링 도구를 통합한 가상 머신을 제공한다. 스마트 그리드, 스마트 교통, 스마트 시티 등 여러 분야의 개별 CPS를 UCEF의 가상 머신에서 통합할 수 있다. 또한 이종 CPS 간 메시지 교환 같은 통합 실험을 한 곳에서 구성, 조정, 관리할 수 있다.

CPS의 공적 표준이 부재한 현 시점에서 NIST의 CPS 프레임워크는 CPS 개념을 정립하고 이해관계자가 소통할 수 있는 출발점을 최초로 제시했다. 다만 2018년 이후 공식 산출물이 아직 나오지 않고 있으며 후속 작업이 더디게 진행되는 점은 아쉽다. 이는 기술이 융복합하는 추세가 가속화되면서 CPS의 고유 색깔이 희미해지고 사물인터넷, 디지털 트윈 같은 다른 개념과 통합되고 있기 때문으로 추측한다.

2.2 유럽: AMASS[9)]

유럽도 2007년부터 연구기금 지원 프로그램 'Frame Programme 7'을 통해 CPS 및 임베디드 시스템 연구 프로젝트 'ARTEMIS'에 70억 달러(약 8조 원)를 투자했다. 이와 더불어 후속 프로그램 'Horizon 2020'을 통해 CPS 연구 투자를 이어갔다. 대표적으로 2016년부터 2019년까지 약 266억 원의 예산을 투입한 AMASS(Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems) 프로젝트가 있다.

AMASS는 CPS의 안전성과 보안성을 보장하고 인증을 하기 위한 유럽의 표준 플랫폼 개발을 목표로 수행됐다. AMASS의 표준 플랫폼에는 다음과 같은4가지 세부 목표가 있다.

아키텍처 기반 보장(Architecture-driven Assurance)
다중 관심사 보장(Multi-Concern Assurance)
끊김 없는 상호운용성(Seamless Interoperability)
도메인 내·외 인증 재활용(Cross-and Intra-Domain Reuse)

아키텍처 기반 보장은 안전성을 담보하는

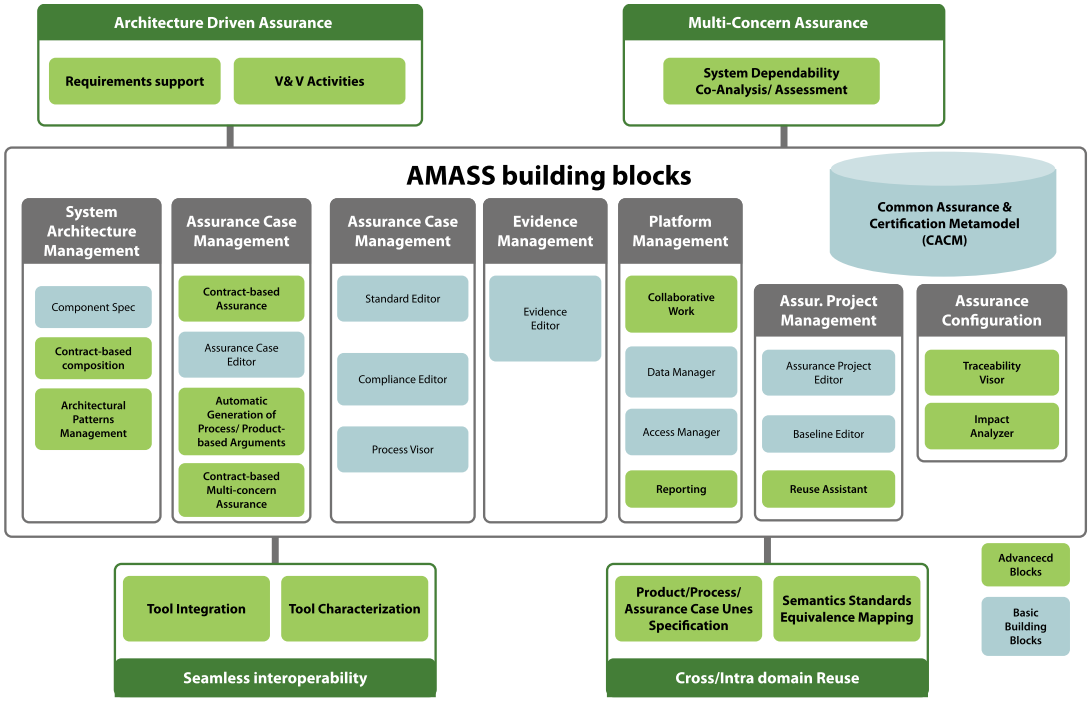
9 프로젝트 산출물 참고: https://cordis.europa.eu/project/id/692474/results

CPS의 구조를 패턴화하고, 이를 활용해 검증된 패턴으로 설계된 모듈은 재활용하는 것이다. 이를 위해 AMASS는 자동화된 정형분석을 지원하는 계약 기반 설계(Contract-based Design) 방식을 플랫폼에 도입했다.

다중 관심사 보장은 NIST의 접근방식과 유사하다. CPS의 안전·신뢰성 관련된 여러 속성 간의 상호의존성을 분석하고 이를 계약 기반 설계에 적용하는 것이다. AMASS는 안전과 보안이라는 2가지 속성을 상호 분석하고 공동 설계하는 데 집중했다.

끊김이 없는 상호운용성이란 서로 다른 분야의 안전 관리 도구, 설계와 개발 도구, 시험 도구 간의 데이터 교환을 제공하는 것이다. AMASS 플랫폼은 다른 분야, 다른 시스템 사이의 안전성 보장 증거의 추적성 관리와 영향 분석 결과까지 공유할 수 있다. 또한 CPS 분야별 안전 관리, 시험 및 인증 도구가 모두 AMASS의 플랫폼을 통해 연결된다. 그 결과 서로 다른 도메인에서 CPS 표준 호환성이 이뤄진다. 따라서 인증 결과를 재활용함으로써 인증 비용을 절감하고 효율성도 향상할 수 있다.

상위 수준의 CPS 개념을 정립하는 일에 초점을 맞춘 NIST의 프레임워크에 비해 AMASS는 좀 더 구체적이고 현실적인 부분에 초점을 맞췄다. 이는 항공, 철도, 자동차처럼 기존의 기능 안전 분야를 주도하는 유럽 제조 산업의 경험이 반영된 것으로 해석된다. AMASS는 CPS를 완전히 새로운 컴퓨팅 패러다임으로 규정하기보다는 기존 임베디드 시스템의 확장으로 봤다. 그렇기에 기존 안전 공학 기술과 호환 가능한 CPS 안전 공학 체계를 만들고자 했다. AMASS가 레거시를 잘 활용하는 것은 현명한 결정으로 보인다. 다만 인공지능, 물리 영역의 불확실성 같은



[그림 2] AMASS 플랫폼의 기능 블록[4]

<표 1> PG609의 CPS 안전·신뢰성 확보지침

표준번호	표준명	제/개정년도
TTAK.KO-11.0268-Part 1	사이버-물리 시스템(CPS)의 안전·신뢰성 확보지침 제1부: CPS 사고분석 모델	2019년
TTAK.KO-11.0268-Part 2	사이버 물리 시스템(CPS)의 안전·신뢰성 확보 지침 제2부: CPS 안전·신뢰성 프로필 저장소 참조 모델	2020년

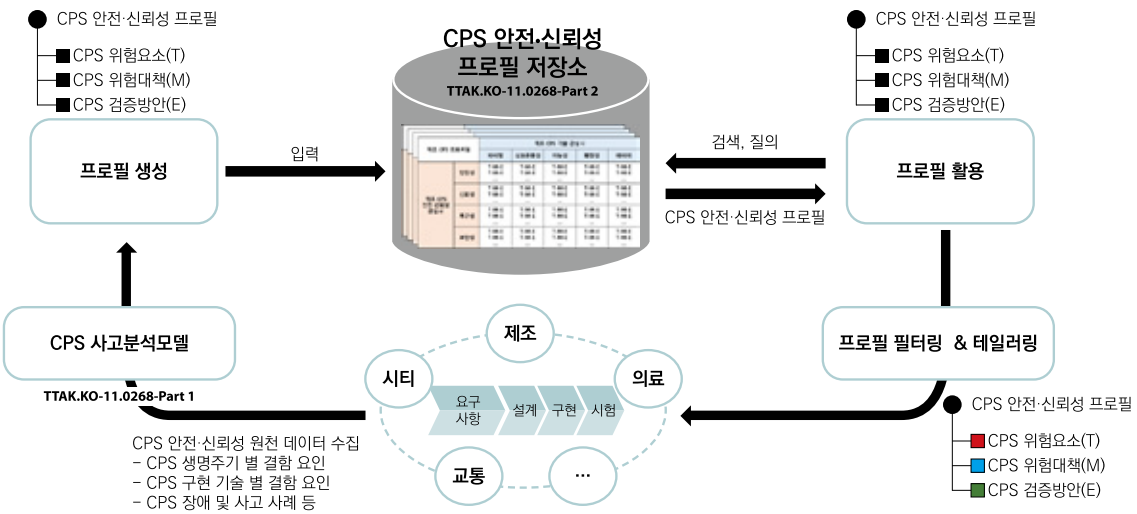
기존 기능 안전의 영역 밖에서는 여전히 많은 숙제가 남아 있다는 점을 상기할 필요가 있다.

2.3 국내: 사이버-물리 시스템의 안전·신뢰성 확보 지침

TTA CPS 프로젝트 그룹(PG609)은 2011년 신설돼 CPS 관련 국내 표준화 활동을 전담한다. 초기에는 주로 CPS 공통 기술에 대한 표준을 제정했다. 이후 CPS가 다양한 응용 분야로 확산되면서 제조, 국방, 조선을 비롯한 여러 분야에서 CPS 응용 기술 표준을 정립하는 데 주력하고 있다. 본 절에서는 PG609에서 최근 제정된 '사이버-물리 시스템의 안전·신뢰성 확보지침'의 내용을 간략히 살펴본다.

CPS의 안전·신뢰성에 영향력을 끼치는 요인은 CPS의 응용 분야와 적용 기술에 따라 다양하다. 모든 요인을 분석하고 대응하는 것은 개별 조직이나 도메인의 역량을 넘어선다. CPS의 안전·신뢰성을 확보하는 것은 특정 분야에서 이뤄지는 독자적인 노력보다는 전 분야가 협력해 달성해야 한다. 또한 광범위한 CPS의 안전·신뢰성 데이터를 전체 산업이 체계적으로 공유해야 한다.

이러한 맥락에서 2019년 '사이버-물리 시스템의 안전·신뢰성 확보 지침'의 제1부[5]가 제정됐다. 제1부는 CPS의 기술관심사(예: 지능성, 실시간성, 확장성, 상호운용성 등) 관점에서 CPS의 안전·신뢰성 사고와 원인 관계를 체계적으로 분석하는 모델을 정의했다. CPS 사고분석 모델의 산출물은 CPS 안전·신뢰성 프로필이며 이는 CPS 안전·신뢰성과 관련된 사고의 융복합적 기술 원인과 이에 대한 대책, 그리고 검증 방안을 정리한



[그림 3] CPS 안전·신뢰성 확보지침의 프로필 생성과 활용[5]

데이터이다. 후속 표준인 제2부[6]는 CPS 안전·신뢰성 프로필을 산업 전반에서 활용하기 위한 일종의 데이터 공유 플랫폼이다. CPS 이해관계자들은 CPS의 생명주기 단계에서 수행할 안전·신뢰성을 확보하는 활동에 유용한 정보를 저장소에서 쉽게 획득할 수 있다. TTAK.KO-11.0268 표준은 시리즈 표준으로 기획돼 계속 추진될 예정이다. 2021년도에는 CPS 안전·신뢰성 프로필 개념 모델에 대한 표준화가 논의 중이다.

3. 맺음말

ICT 융합 시대의 표준은 시장을 선도하기 위한 기술 진화에 초점을 맞추는 동시에 공공의 안전을 보장하는 안전·신뢰성 확보에도 심혈을 기울여야 한다. 아무리 뛰어난 성능을 가진 기술이라도 안전·신뢰성을 확보하지 못하면 결국 시장에서 통용될 수 없다. 그래서 CPS 안전·신뢰성의 표준화가 중요하다.

그러나 CPS 안전·신뢰성 표준화는 결코 쉽지 않다. CPS는 다양한 기술의 융복합으로 만들어져 매우 복잡하기 때문이다. 사물인터넷과 센서, 클라우드 컴퓨팅, 인공지능, 빅데이터, 디지털 트윈 같은 최신 기술이 복합된 CPS가 다뤄야 할 기술적 이슈는 매우 광범위하다. 또한 개별 기술이 변화하는 속도도 매우 빠르다. 개별 요소 기술마다 독자 표준이 있고 자체적인 기술 생태계가 있다. 일부 기술 분야의 노력만으로 CPS 안전·신뢰성은 결코 확보할 수 없다. NIST의 CPS 프레임워크나 H2020의 AMASS도 국가 차원에서 많은 예산을 장기적으로 투자한 표준 연계 활동이다. 그렇기에 우리도 국가 차원에서 더 많은 투자와 지원을 아끼지 않아야 한다. CPS 안전·신뢰성 표준화는 다학제 간 협력이 필수라는 것을 상기해 개별 기술의 혁신과 더불어 안전·신뢰성을 함께 추구해야 한다.

주요 용어 풀이

- **피드백 시스템**(Feedback system): 처리 결과가 주어진 조건과 목적대로 수행됐는지를 검사하고 확인해 자동적으로 자기 수정하거나 제어하는 회로로 된 시스템. 예를 들면 어느 달의 출고량 정보에 따라 생산을 조절하고, 다음 달의 출고량을 증가시키거나 감소시키는 것이다.

참고문헌

[1] NIST, Framework for Cyber-Physical Systems: Volume 1, Overview, 2017. URL: https://doi.org/10.6028/NIST.SP.1500-201 (2021.3.19 접속)

[2] NIST, Framework for Cyber-Physical Systems: Volume 2, Working Group Reports, 2017. URL: https://doi.org/10.6028/NIST.SP.1500-202 (2021.3.19 접속)

[3] Burns, M., et al., Universal CPS Environment for Federation, 2018 Winter Simulation Innovation Workshop, URL: https://par.nsf.gov/biblio/10076182 (2021.3.19 접속)

[4] AMASS, Deliverable D2.4 - Reference Architecture (C), 2018. URL: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5bb30efe4&appId=PPGMS (2021.3.19 접속)

[5] 정보통신단체표준, TTAK.KO-11.0268-Part 1, 사이버-물리 시스템(CPS)의 안전·신뢰성 확보지침 제1부: CPS 사고분석 모델, 2019.

[6] 정보통신단체표준, TTAK.KO-11.0268-Part 2, 사이버 물리 시스템(CPS)의 안전·신뢰성 확보 지침 제2부: CPS 안전·신뢰성 프로필 저장소 참조 모델, 2020.