

가상물리시스템(CPS)의 보증 및 인증 기술 동향

- 유럽(H2020-ECSEL)의 AMASS 프로젝트 -



서준호 TTA 지능정보융합소프트웨어단 전임연구원

1. 머리말

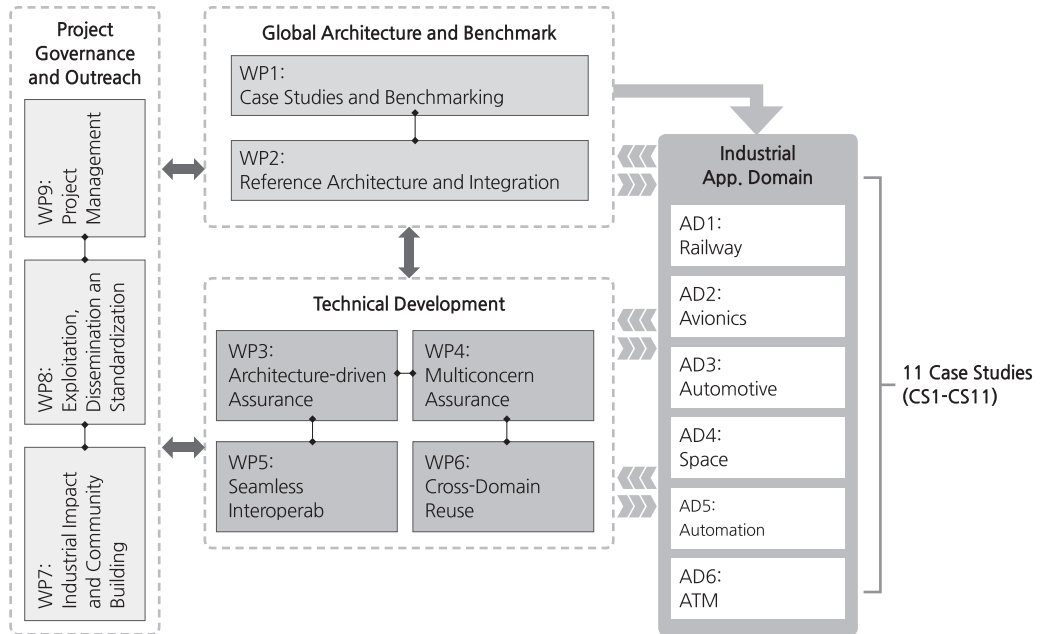
정보통신기술(ICT)의 융·복합적인 발전으로 인한 4차 산업 혁명 시대로 접어들면서 가상물리시스템(CPS, Cyber Physical Systems)이 핵심 기술로 부각되고 있다. 가상물리시스템은 물리 세계에서 수집된 정보를 인공지능(AI), 빅데이터(Big Data) 등 지능정보기술을 활용하여 처리하고 다시 물리 세계로 피드백함으로써 가상 세계와 물리 세계가 상호 작용하는 시스템이다. 이러한 가상물리시스템은 교통, 전력, 제조와 같이 사회 전반적인 분야에서 수많은 시스템과 연결되어 있어 문제가 발생했을 때 사회적 혼란 및 안전사고와 직결될 수 있기 때문에 안전성 확보가 중요하다.

이에 유럽 연합은 연구 및 혁신 기금 지원 계획인 Horizon 2020[1]의 전자 소자 및 시스템 개발 사업인 ECSEL JU[2]의 일환으로 다양한 교차 도메인 간에서 가상물리시스템의 안전성(Safety), 신뢰성(Reliability), 보안성(Security) 등을 확보할 수 있는 ‘개방형 통합 보증 및 인증 체계’를 개발하고 있다.

이 프로젝트는 AMASS(Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems)라는 명칭으로 2016년 4월 시작되었으며(2016~2019년 3월, 총 기간 36개월) 8개국, 29개의 협력사와 함께 진행 중이다.

2. 프로젝트 목표

AMASS 프로젝트의 목표는 다양한 도메인 간 (재)활용 가능한 통합된 도구 플랫폼을 개발하여 전 생명 주기에 걸쳐 보증 및 인증을 통해 비용을 절감하고자 하는 것이다. AMASS 프로젝트에서 정의하는 보증(Assurance)은 시스템이 안전성, 보안성, 신뢰성, 가용성(Availability), 유지보수성(Maintainability)에 대한 요구사항을 준수하기 위한 체계적인 활동이며 인증(Certification)은 의도된 서비스를 안전하게 제공하기 위해 명시된 표준, 규정 및 정책 등을 준수하는 (법적)승인을 말한다.



[그림 1] 프로젝트의 구성[3]

프로젝트의 목표는 다음과 같다.

- 복잡한 가상물리시스템의 설계 효율 향상
- 컴포넌트 및 제품에 대해 기존에 취득한 보증 결과를 재사용함으로써 비용 절감
- 기술적인 혁신을 통해 새로운 가상물리시스템 인증 시 잠재적인 위험 요인 감소
- 가상물리시스템의 보증·인증 도구를 개발하고 상호운용성을 향상시켜 가상물리시스템 산업의 지속가능한 성장 기반 마련

3. AMASS 프로젝트 내용

AMASS 프로젝트는 [그림 1]과 같이 크게 3개의 그룹으로 나뉘며 총 9개의 워크 패키지(Work Package, WP)로 구성된다. 첫 번째 그룹(Global Architecture and Benchmark)은 산업별 사례 조사를 통해 요구사항을 도출하고 프로젝트 결과에 대한 평가를 위해 산업별 유스케이스 개발(WP1)하며 AMASS 참조 도구 아키텍처(ARTA, AMASS Reference Tool

Architecture)를 통합 및 개발(WP2)한다. 두 번째 그룹(Technical Development)은 AMASS 프로젝트의 핵심적인 기술 작업을 수행한다. 아키텍처 주도의 보증(WP3)과 다중의 관심 보증(WP4)을 만족시키고 교차 도메인간의 재사용 가능(WP5)하며 원활한 상호운용성을 보장(WP6)할 수 있도록 하는 기능을 개발한다. 마지막 그룹(Project Governance and Outreach)은 주요 산업에 대한 확장 및 커뮤니티 구축(WP7)과 교육 및 보급, 표준화(WP8), 컨소시엄이나 프로젝트 관리, 지원 등(WP9)을 수행한다.

3.1 아키텍처 통합과 벤치마크(Global Architecture and Benchmark) 그룹

3.1.1 (WP1) 사례 연구 및 벤치마크

WP1은 <표 1>과 같이 6개의 도메인에 대해 총 11개의 사례 연구를 수행한다. 사례 연구를 통해 도메인별 가상물리시스템의 사용자 요구사항을 도출

<표 1> AMASS 사례 연구[4]

분야	사례 연구명	협력사
자동차 (Automotive)	Advanced driver assistance function with electric vehicle	Infineon
	Collaborative automated fleet of vehicles	Berner & Mattner
	Telematics function	SP Sveriges Tekniska Forskningsinstitut
우주 (Space)	Design and safety assessment of on-board software	GMV Aerospace and Defence, S.A.U.
	Certification basis to boost the usage of MPSoC architectures	Thales Alenia Space
	Design and efficiency assessment of model-based Attitude	OHB Sweden AB
철도 (Railway)	Platform Screen Doors Controller	CLEARSY SAS
	Automatic Train Control Formal Verification	Alstom Transport SA
항공 전자 공학 (Avionics)	Safety assessment of multi-modal interactions in cockpits	Honeywell
항공 교통 관리 (Air Traffic Management)	Telematics function	SP Sveriges Tekniska Forskningsinstitut
산업 자동화 (Industrial Automation)	Industrial and Automatin Control System	Schneider Electric Espana S.A.

하며 프로젝트를 통해 도출되는 결과를 적용 및 평가, 벤치마킹할 수 있다.

3.1.2 (WP2) 참조 아키텍처 및 통합

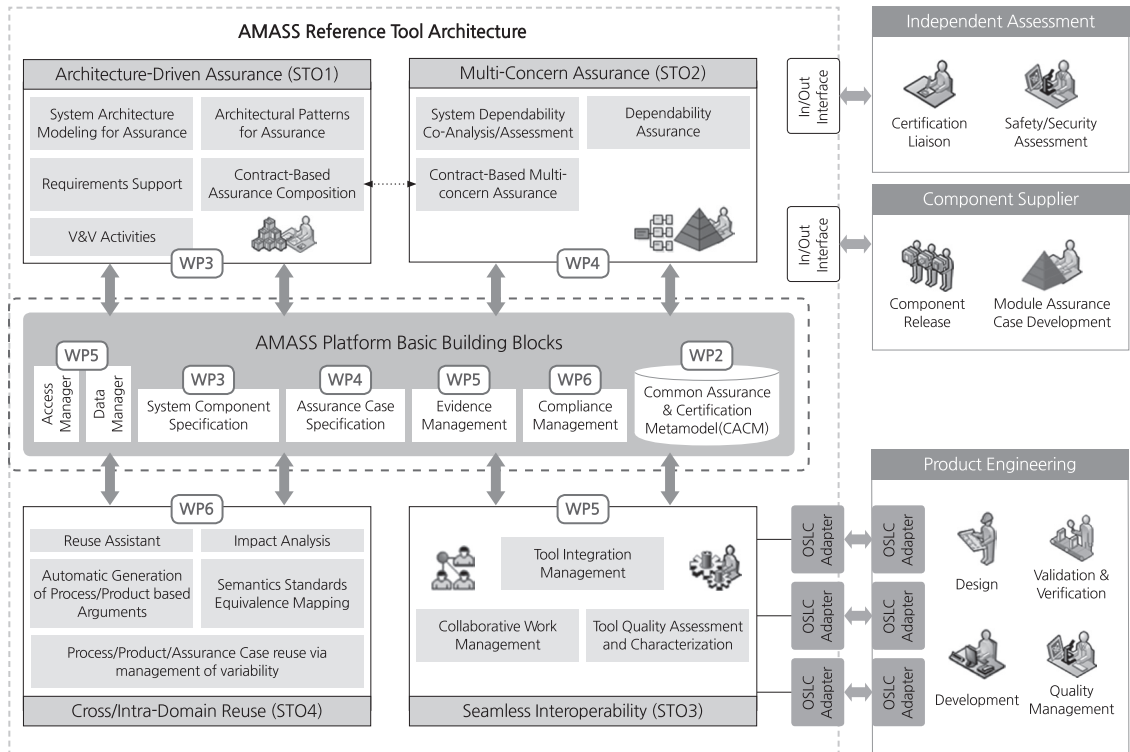
AMASS 참조 도구 아키텍처(ARTA)는 가상물리 시스템의 보증 및 인증을 위해 공통적으로 활용 가능한 참조용 도구 아키텍처이다. ARTA는 기존의 OPENCOS[6]와 SafeCer[7] 프로젝트에서 개발된 기술과 CHESS[8]와 같은 관련 프로젝트들의 내용을 결합 및 발전시킨 7개의 기본 요소(Basic Building Blocks)로 구성함으로써 가상물리시스템의 보증 및 인증을 공통적으로 사용할 수 있도록 한다. 7개의 기본 요소는 데이터 관리(Data Management)와 접근 관리(Access Management), 시스템 컴포넌트 명세(System Component Specification), 보

증 지침 명세(Assurance Case Specification), 근거 관리(Evidence Management), 규정 준수 관리(Compliance Management), 공통 보증 및 인증 메타모델(Common Assurance & Certification Metamodel, CACM)¹⁾로 구성된다.

3.2 기술 개발(Technical Development) 그룹

AMASS 프로젝트는 AMASS 메타모델과 보증 및 인증을 수행하기 위한 방법, 도구들이 개발되는 WP(WP3~WP6)가 있으며, 각 WP는 4개의 기술 목표(STO, Scientific and Technical Objectives)를 설정하여 수행한다. 설정된 기술 목표에 대해 프로젝트는 3번의 개발 및 적용 과정을 거쳐 기본 요소(Basic Building Blocks)를 개발하고 통합한다. 각각의 기술 목표를 달성하기 위한 WP 및 구현되는 기

1) 공통 보증 및 인증 메타모델(CACM, Common Assurance & Certification Metamodel): OPENCOS와 SafeCer 프로젝트의 결과를 병합 및 발전시킨 것으로 보증 및 인증 명세를 위한 메타모델이며 보증에 대한 정보를 구조화된 데이터베이스로 저장할 수 있다. 이를 통해 서로 다른 도메인의 보증을 위해 '공통된 개념 언어'를 사용하여 '공통된 형식'으로 인증 자산을 관리하고 기술 및 아키텍처를 공유하고 다양한 도메인 및 표준 프레임워크 간의 효율적인 재사용을 수행한다.



[그림 2] 참조 아키텍처 및 도구 플랫폼 구성[5]

능은 [그림 3]과 같다.

3.2.1 (WP3) 아키텍처 주도의 보증(Architecture-Driven Assurance)

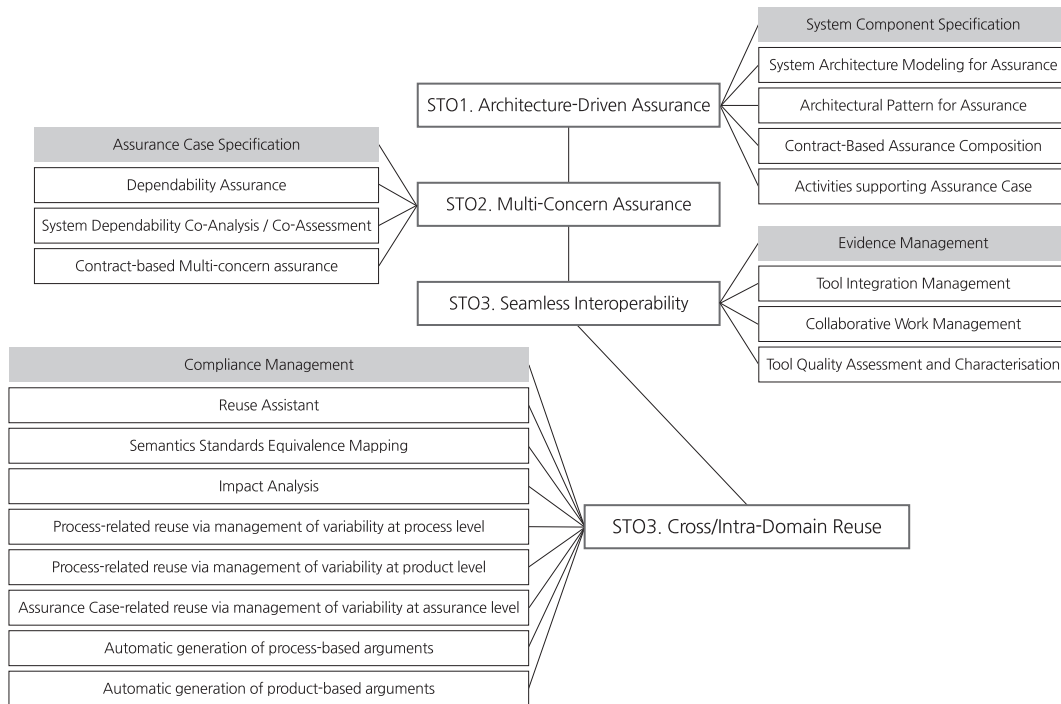
‘아키텍처 주도의 보증(STO1)’은 가상물리시스템 개발 시 보증 및 인증을 위해 도메인 사례를 기반으로 시스템 구성 및 명세 등의 통합을 목표로 한다. 이러한 목표로 개발되는 AMASS의 기능에는 기본 요소인 시스템 컴포넌트 명세(System Component Specification)를 포함하여 보증을 위한 시스템 아키텍처 모델링(System Architecture Modeling for Assurance), 보증을 위한 구성 패턴(Architectural Patterns for Assurance), 계약 기반의 보증 구성(Contract-Based Assurance Composition), 보증을 지원하는 활동(Activities supporting Assurance Case) 등의 기능이 있다.

3.2.2 (WP4) 다중 관심 보증(Multi-concern Assurance)

‘다중 관심 보증(STO2)’은 시스템이 갖춰야 하는 여러 특성(안전성과 보안성을 중심으로 가용성, 견고성, 신뢰성과 같은 고신뢰성 측면의 특성 포함)을 다루는 보증 지침 개발, 공동 평가 및 계약 기반의 보증을 위한 도구 개발을 목표로 한다. 이러한 목표로 개발되는 AMASS의 기능에는 기본 요소인 보증 지침 명세(Assurance Case Specification)를 포함하여 고신뢰성 보증(Dependability Assurance), 시스템 고신뢰성 공동분석/공동평가(System Dependability Co-Analysis/Co-Assessment), 계약 기반의 다중 관심 보증(Contract-based Multi-concern assurance) 등의 기능이 있다.

3.2.3 (WP5) 원활한 상호운용성(Seamless Interoperability)

‘원활한 상호운용성(STO3)’은 가상물리시스템의



[그림 3] 과학 기술 목표(STO)를 통해 도출되는 기능[5]

모델링, 분석 및 개발 시(특히 보증 및 인증 시 이해 관계자 간의 공동 작업) 상호운용성을 보장하기 위해 공통적으로 적용 가능한 기능을 개발한다. 이러한 목표로 개발되는 AMASS의 기능에는 기본 요소인 근거 관리(Evidence management)를 포함하여 도구 통합 관리(Tool Integration Management), 협업 작업 관리(Collaborative Work Management), 도구 품질 평가 및 특성화(Tool Quality Assessment and Characterization) 등의 기능이 있다.

3.2.4 (WP6) 교차/내부-도메인에서 재사용(Cross/Intra-Domain Reuse)


‘교차/내부-도메인에서 재사용(STO4)’은 보증 및 인증된 자산들을 관리하고 자산들을 명세화한 프레임워크를 기반으로 교차/내부 도메인에서 재사용을 제공하는 것을 목표로 한다. 이러한 목표로 개발되

는 AMASS의 기능에는 기본 요소인 규정 준수 관리(Compliance Management)를 포함하여 재사용 지원(Reuse Assistant), 시맨틱 표준 평가 매핑(Semantics Standards Equivalence Mapping), 영향 분석(Impact Analysis), 프로세스 레벨에서의 변경 관리를 통한 프로세스 관련 재사용(Process-related reuse via management of variability at process level), 제품 레벨에서의 변경 관리를 통한 제품 관련 재사용(Product-related reuse via management of variability at product level), 보증 레벨에서의 변경 관리를 통한 보증 지침 관련 재사용(Assurance Case-related reuse via management of variability at assurance level), 프로세스 기반 인자 자동 생성(Automatic generation of process-based arguments), 제품 기반 인자 자동 생성(Automatic generation of product-based arguments) 등의 기능이 있다.

3.3 AMASS 프로젝트 관리 및 지원 활동(Project Governance and Outreach) 그룹

프로젝트 홍보, AMASS 커뮤니티의 구축 및 관리(WP7)를 하며 컨소시엄 협력사와 수행자를 포함하여 프로젝트 관리 및 홍보 등(WP9)을 한다. 또한 프로젝트 결과에 대한 교육이나 보급, 표준화(안전 및 보안·상호운용성) 등(WP8)을 수행한다.

4. 맺음말

가상물리시스템은 인공지능, 빅데이터 등의 최신 기술이 융합되어 다양한 도메인에서 활용되고 있다. 더욱이 사회의 밀접한 분야에 적용되어 안전사고 발생 시 파급효과가 상당하기 때문에 가상물리시스템의 기술적인 발전에 대한 연구뿐만 아니라 안전성, 보안성과 같은 고신뢰성(Dependability) 확보를 위한 연구 역시 필요하다. 본고에서 소개한 AMASS 프로젝트는 다중의 고신뢰성을 고려하고 상호운용성 및 교차·내부-도메인에서 재사용 등을 위한 작업으로 통합된 보증 및 인증을 위한 도구 플랫폼을 개발하여 비용을 절감하고 기술적·사회적 효율성을 높이는 효과를 가져왔다. 국내에서도 가상물리시스템은 스마트시티, 스마트공장 등의 분야로 응용되어 효율성을 높이는 연구가 수행되고 있다. 하지만 사회와 밀접한 분야임에도 불구하고 기술 개발 연구에 비해 안전이나 보안에 대한 연구가 미비한 만큼 도메인별 참조 아키텍처 개발과 안전·신뢰성 확보에 대한 연구가 확대될 필요가 있다. 

[참고문헌]

- [1] Horizon 2020, <https://ec.europa.eu/programmes/horizon2020/>
- [2] ECSEL JU, <https://www.ecsel.eu/>
- [3] AMASS, Organization, <https://www.amass-ecsel.eu/content/organization>
- [4] AMASS, Deliverable D1.1 Case studies description and business impact, 2018.
- [5] AMASS, Deliverable D2.4 AMASS Reference Architecture(c), 2018.
- [6] FP7, OPENCOS, <http://www.opencoss-project.eu/>
- [7] ARTEMIS, SafeCer, <http://www.safecer.eu/>
- [8] ARTEMIS, CHESS, <http://www.chess-project.org/>

[주요 용어 풀이]

- 사이버 물리 시스템(CPS, Cyber-Physical Systems): 센서 네트워크(sensor networks), 사이버네틱스(cybernetics) 및 메카트로닉스(mechatronics) 시스템을 결합 설계한 임베디드 시스템(embedded systems)이 진화되고 있는 시스템을 의미함. 현실 세계의 다양한 물리, 화학 및 기계공학 시스템(physical systems)을 컴퓨터와 네트워크(cyber systems)를 통해 자율적, 지능적으로 제어하기 위해 등장하였다. 크게 연산(computation), 통신(communication), 제어(control) 기술로 구성되며, 대규모 융복합 시스템(system of systems) 구축을 위한 여러 전문 분야가 관련된 다학제적(多學際的, multidisciplinary and interdisciplinary)이다. 스마트 공장(smart factory), 스마트 그리드(smart grid), 자동차, 항공, 국방 등 광범위한 분야에 응용됨.

※ 본고는 2018년도 정부(과학기술정보통신부)의 재원으로 정보통신산업진흥원의 지원을 받아 수행됨[S1014-18-1002, CPS 안전·신뢰성 확보체계 연구]