KIPS Trans. Softw. and Data Eng.
Vol.9, No.12 pp.387~402
ISSN: 2287-5905 (Print), ISSN: 2734-0503 (Online)

https://doi.org/10.3745/KTSDE.2020.9.12.387

A Methodology for Integrating Security into the Automotive Development Process

Seungyeon Jeong† · Sooyoung Kang†† · Seungjoo Kim†††

ABSTRACT

Conventional automotive development has mainly focused on ensuring correctness and safety and security has been relatively neglected. However, as the number of automotive hacking cases has increased due to the increased Internet connectivity of automobiles, international organizations such as the United Nations Economic Commission for Europe(UNECE) are preparing cybersecurity regulations to ensure security for automotive development. As with other IT products, automotive cybersecurity regulation also emphasize the concept of "Security by Design", which considers security from the beginning of development. In particular, since automotive development has a long lifecycle and complex supply chain, it is very difficult to change the architecture after development, and thus Security by Design is much more important than existing IT products. The problem, however, is that no specific methodology for Security by Design has been proposed on automotive development process. This paper, therefore, proposes a specific methodology for Security by Design on Automotive development. Through this methodology, automotive manufacturers can simultaneously consider aspects of functional safety, and security in automotive development process, and will also be able to respond to the upcoming certification of UNECE automotive cybersecurity regulations.

Keywords : Automotive Development, Evidence-based Standards, Secure SDLC, UNECE Cybersecurity Regulation

자동차 개발 프로세스에서의 보안 내재화 방법론

정 승 연† · 강 수 영†† · 김 승 주†††

요 약

기존의 자동차 개발은 주로 정확성(Correctness) 및 안전성(Safety) 확보에 초점을 맞추어 왔으며, 이에 반해 보안성(Security)은 비교적 소홀하게 다루어져 왔다. 하지만 최근 자동차의 인터넷 연결성이 높아짐에 따라 자동차 해킹 사례가 증가하면서, 유엔유럽경제위원회(United Nations Economic Commission for Europe, UNECE)와 같은 국제기관은 자동차 개발에 대한 보안성을 확보하기 위해 사이버보안 규제를 준비하고 있다. 다른 IT 제품과 마찬가지로 자동차 사이버보안 규제에서 또한 개발 초기부터 보안성을 고려하는 "보안 내재화(Security by Design)"의 개념을 강조한다. 특히 자동차 개발은 생명주기가 길고 공급망이 복잡하기 때문에 개발 이후에 아키텍처를 변경하는 것이 매우 어려우므로, 자동차 개발에 있어 보안 내재화는 기존 IT 제품에 비해 훨씬 더 중요시된다. 그러나 문제는 아직 자동차 개발 과정에 보안을 내재화하는 구체적인 방법론이 제시되지 못하고 있다는 것이다. 이에 본 논문에서는 자동차 보안 내재화를 위한 구체적인 방법론을 제안한다. 본 논문에서 제안된 방법론을 통해 자동차 제조사는 자동차 개발 과정에 있어 기능 안전성과 보안성의 측면을 동시에 고려할 수 있으며, 다가오는 UNECE 자동차 사이버보안 규제에 대한 인증에도 대응할 수 있을 것이다.

키워드 : 자동차 개발, 증거 기반 표준, Secure SDLC, UNECE 사이버보안 규제

1. 서 론

전통적으로 자동차 산업에서 개발은 기능 안전성 (Functional Safety)에 초점을 맞추어 왔다. 기능 안전성은 제품이 설계된 대로 정확하게 동작하는지를 판단하는 정확성과 제품 내부에서 발생한 오류가 외부로 표출되어 사용자에게 피해를 줄 수 있는지를 판단하는 안전성을 포함하는 개념이다. 기능 안전성에서는 전기·전자 시스템 내에서 발생한 오작동이 외부로 표출되어 사용자에게 상해를 입히는 상황을 막고자 하며, 기능 안전성이 보장되지 않으면 이는 단순한 시스템 동작 오류뿐만 아니라 인명 피해 사고로 이어질 수 있다[1,2]. 따라서 국제 표준화 기구 ISO(International Organization for Standardization)에서는 ISO 26262라는 자동차 기능 안전성 관련 표준을 제정하여[3] 자동차 개발 프로세스 전반에 걸쳐 기능 안전성을 고려할 수 있도록 하였다.

※ 이 논문은 2020년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(No.2017-0-00184, 자기학습형 사이버 면역 기술 개발).
† 준 회 원 : 고려대학교 자동차융합학과 석사과정
†† 준 회 원 : 고려대학교 정보보호학과 박사과정
††† 종신회원 : 고려대학교 사이버국방학과/정보보호대학원 정교수
Manuscript Received : June 17, 2020
First Revision : August 6, 2020
Accepted : August 25, 2020
* Corresponding Author : Seungjoo Kim(skim71@korea.ac.kr)

이러한 기능 안전성과 다르게 보안성은 자동차 개발에서 중점적으로 다루어지지 않았었다. 보안성은 인가된 사용자만이 시스템의 정보 자산에 접근할 수 있도록 보장하는 기밀성(Confidentiality), 부적절한 정보의 변경이나 파기 없이 시스템이 완전하게 보존됨을 보장하는 무결성(Integrity), 시스템 정보에 대한 접근과 사용을 항상 보장하는 가용성(Availability)을 포함하는 개념이다. 보안성에서는 외부에 존재하는 보안 위협이 시스템 내로 확장되어 사용자가 피해를 보는 상황을 막고자 하며, 보안성이 보장되지 않으면 이는 인명 피해나 프라이버시 유출 등의 다양한 사고로 이어질 수 있다[4]. 최근 커넥티드 카의 등장과 함께 자동차의 소프트웨어 비중 및 인터넷 연결성이 높아지면서[5] 자동차가 보안 위협에 노출될 가능성이 커지고 있고[6], 이에 따라 자동차 해킹 사례 또한 증가하고 있다. 따라서 보안성이 확보된 자동차 개발에 대한 필요성이 높아지고 있으며, 여러 국제기관에서도 자동차 사이버보안 규제를 제정함으로써 이를 강조하려는 노력을 보이고 있다[7]. 특히 UNECE가 제정 중인 자동차 사이버보안 규제의 경우 신차를 기준으로 2022년부터 적용되는데, 이에 따르면 해당 규제에서 정한 기준에 맞춰 평가·인증받지 못한 자동차는 유럽에 수출할 수 없게 된다. 따라서 보안성이 확보된 자동차 개발은 다양한 보안 위협뿐만 아니라 당장 직면하게 될 자동차 수출 및 수입 경제에도 중요한 쟁점이 된다.

UNECE 자동차 사이버보안 규제에서는 핵심 요구사항으로 보안 내재화를 제시하고 있는데, 보안 내재화란 개발 초기부터 제품의 정확성, 안전성, 보안성 등의 요소를 모두 고려하여 신뢰 가능한 제품을 구현하는 개념이다. 특히 자동차 개발은 생명주기가 길고 공급망이 복잡하므로 개발 이후에 아키텍처를 변경하는 것이 매우 어렵다. 따라서 자동차 개발에 있어 보안 내재화는 더욱 중요하게 다루어져야 하는데, 이러한 보안 내재화는 Secure SDLC(System Development Life Cycle)를 통해 달성할 수 있다. Secure SDLC는 제품 개발 생명주기 전반에 적용되는 체계적인 보안 개발 프레임워크로 Microsoft와 같은 기업 또는 NIST와 같은 표준 기관 등에서 활용하고 있으며, 관련 연구 또한 활발하게 이루어지고 있다[8-15].

하지만 기존 Secure SDLC 표준은 주로 소프트웨어를 대상으로 할 뿐만 아니라 체계적인 요구사항 도출, 타사의 구성요소에 대한 획득과 같은 서로 다른 측면의 활동을 강조하기 때문에 자동차 보안 내재화에 대한 전반적이고 구체적인 방법론을 제시하지 못하는 경우가 대부분이다. 또한 앞서 언급한 UNECE 자동차 사이버보안 규제에서도 보안 내재화를 달성하기 위한 구체적인 방법론을 제시하지 않고 있으며, 이는 기존에 연구되었던 논문들에서도 마찬가지이다.

따라서 본 논문에서는 자동차 보안 내재화를 위한 구체적인 방법론으로 Trustworthy Automotive SDLC를 제안하고자 한다. 여기서 Trustworthiness, 즉 신뢰성이란 개발 시스템에 대한 정확성, 안전성, 보안성을 모두 고려함으로써 시스템이 예상대로 동작할 것이라는 신뢰를 제공하는 개념으로[16], 자동차와 같은 기능 안전성이 중요시되는 시스템에서는 특히 강조되어야 한다. Trustworthy Automotive SDLC를 제안하기 위해 본 논문에서는 먼저 4가지 주요 Secure SDLC 표준인 Microsoft SDL(Microsoft Security Development Lifecycle), NIST SSDLC(National Institute of Standards and Technology Secure Software Development Life Cycle), OWASP CLASP(The Open Web Application Security Project Comprehensive, Lightweight Application Security Process), SAE J3061(Society of Automotive Engineers J3061)에서 자동차 개발과 밀접한 관련이 있는 수행 활동들을 도출한다. 이후 각 활동을 IT제품의 보안성 평가 관련 국제 표준인 CC(Common Criteria, ISO/IEC 15408), 정보보호 관리체계 관련 국제 표준인 ISMS(Information Security Management System, ISO/IEC 27001), 프라이버시 관련 국제 표준인 PIMS(Privacy Impact Management System, ISO/IEC 27701)와 자동차 기능 안전성 관련 국제 표준인 FSMS(Functional Safety Management System, ISO 26262)의 세부 항목에 매핑함으로써 상세화된 Trustworthy Automotive SDLC를 도출한다. 또한 이 과정에서 자동차 사이버보안 규제인 UNECE 사이버보안 규제의 요구사항과 UNECE 사이버보안 규제의 기반이 되는 자동차 사이버보안 국제 표준인 ISO/SAE 21434의 요구사항을 우리가 제안하는 Trustworthy Automotive SDLC에 반영한다.

우리가 제안하는 Trustworthy Automotive SDLC는 ISO 26262의 기능 안전성 프로세스를 기반으로 하기 때문에 기존 자동차 기능 안전성 개발 프로세스에 대한 활동 접목이 용이하며, 자동차 개발에서 요구되는 정확성, 안전성, 보안성의 측면을 모두 고려한다. 또한 Trustworthy Automotive SDLC는 자동차 개발에서 요구되는 충분한 보안 수준을 제공함으로써 보안 위협에 대한 경쟁력을 확보하고, 상세화된 활동을 제시함으로써 다가오는 UNECE 자동차 사이버보안 규제에 이를 활용할 수 있도록 한다.

2. 관련 연구

2.1 논문

본 절에서는 기존에 수행된 자동차 보안 개발 관련 연구들을 분석함으로써 Trustworthy Automotive SDLC에 대한 필요성을 부각하고자 한다. 먼저 대상 연구는 2010년부터 2020년까지 발표된 학술 논문을 선정하였으며, 대표적으로 알려진 (i) ACM (ii) IEEE (iii) Springer, (iv) Elsevier의 4가지 출판사(Digital Library)에 게재된 논문만을 고려하였다. 또한 'Automotive' 또는 'CPS'를 키워드로 가지며 'Process', 'Lifecycle', 'Development'와 같은 프로세스 전체나 'Requirements'와 같은 일부 단계 또는 'Fuzz Testing'과 같은 일부 활동을

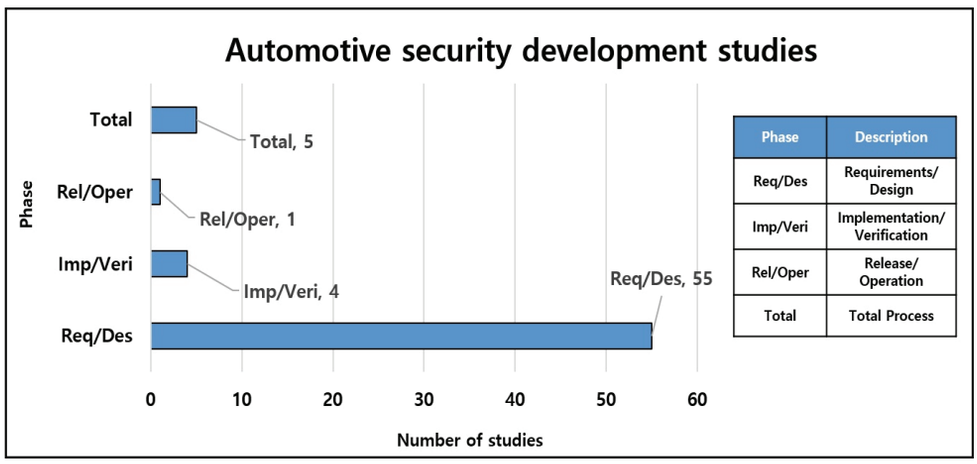

Fig. 1. Automotive Security Development Studies

주제로 가지는 논문을 선별하였다[17-41].

총 65개의 연구를 분석한 결과, Fig. 1에서 볼 수 있듯이 대부분의 연구는 일부 단계에 대해 수행되었으며 이는 주로 요구사항 분석 및 설계 단계에 치중되어 있음을 확인할 수 있었다. 개발 프로세스 전반에 걸친 모델을 제안한 연구도 일부 존재하였으나, 이는 모두 개념적 접근에 그칠 뿐 상세화된 활동을 제시하지는 않았다[18,19,22,29,40]. 따라서 기존 연구에 대한 분석을 통해 개발 프로세스 전반에 걸친 상세화된 자동차 보안 내재화 방법론의 필요성을 느낄 수 있다.

2.2 Secure SDLC 표준

기존 제품 개발의 경우, Secure SDLC를 통해 보안성을 향상시켜왔다[42]. Secure SDLC는 프로세스의 전(全) 단계에 대해 보안 관련 활동을 고려함으로써 보안성이 확보된 제품을 개발할 수 있도록 한다. 하지만 기존에 제시된 Secure SDLC 표준의 경우 실제 구현에 대한 전반적이고 충분한 세부사항을 제공해주지 못하며, 특히 자동차 개발에 대해서는 더욱 그렇다. 따라서 본 논문에서는 기존에 수행되었던 Secure SDLC 표준을 아우르는 보편적인 보안 내재화 방법론을 구축하고, 이를 기반으로 자동차 개발 프로세스에 적합한 활동을 도출하고자 한다. 대상으로 선정하는 Secure SDLC 표준은 소프트웨어 기반의 Microsoft SDL[43], 시스템 기반의 NIST SSDLC[44], 기업에서 수행하는 모범사례(Best Practices) 기반의 OWASP CLASP[45], 자동차 기반의 SAE J3061[46] 총 4가지이며 각 Secure SDLC 표준은 체계적인 보안 요구사항 도출, 타사의 구성요소 획득 등 서로 다른 측면을 강조하기 때문에 이를 통합함으로써 개발 프로세스에 대한 전반적인 활동들을 도출할 수 있다. Table 1은 각 대상에 대한 특징을 보여준다.

2.3 자동차 보안 표준 및 규제

앞서 언급하였듯이 커넥티드 카의 등장과 함께 자동차 소프트웨어의 비중 및 연결성이 높아지면서 자동차 보안의 중요성이 커지고 있다. 이에 따라 여러 국제기관에서도 자동차 개발에 대한 보안성 확보를 위해 규제를 제정 중이다[47]. 특

Table 1. Features of Secure SDLC Standards

	Microsoft SDL	NIST SSDLC	OWASP CLASP	SAE J3061
Target	Software	System	Best Practice	Vehicle
Feature	Focuses on requirements and design phase	Focuses on third-party components acquisition and system disposal	Provides real-world enterprise activities in the form of best practices	Complies with the process of ISO 26262, the automotive functional safety standard
Pros & Cons (P:Pros, C:Cons)	• Provides tools for performing activities like risk analysis(P) • Not include disposal phase(C)	• Can be used to evaluate information systems that require certification when performing certification and accreditation(P) • Lack of activity for implementation phase(C)	• Identifies the role of the person in charge of each activity(P) • Lack of updates and related information(C)	• Easy to apply security-related activities according to the automotive function safety development process(P) • Not include security training and disposal phase(C)

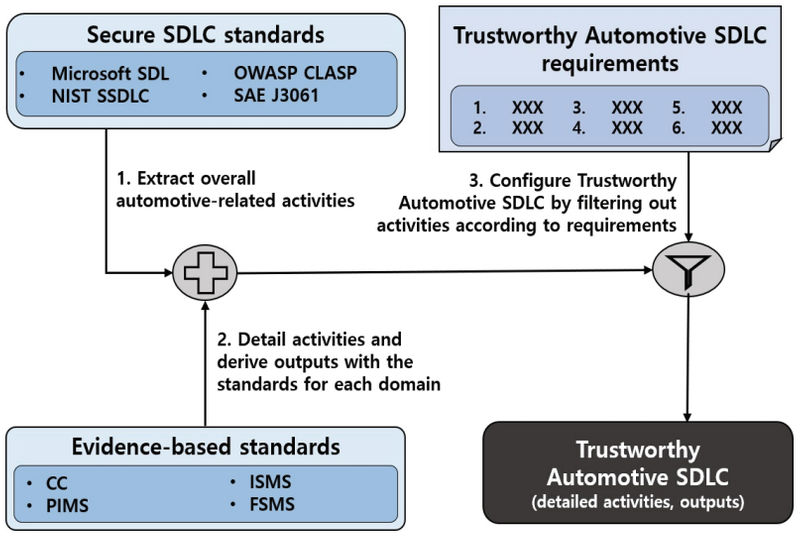

Fig. 2. Procedure of Trustworthy Automotive SDLC Construction

히 UNECE는 개발 프로세스 전반에 대한 보안성 확보를 위해 자동차 사이버보안 규제를 제정 중이며 이는 2022년에 신차를 대상으로, 2024년에는 기존 차를 대상으로 발효될 예정이다[48]. 이때 UNECE 사이버보안 규제는 ISO/SAE 21434라는 국제 표준을 기반으로 한다. ISO/SAE 21434는 자동차 사이버보안 가이드 문서인 SAE J3061을 기반으로 ISO가 제정 중인 자동차 사이버보안 국제 표준으로, 이 또한 2022년에 발간될 예정이다[49]. 따라서 본 논문에서는 UNECE 사이버보안 규제와 ISO/SAE 21434 국제 표준의 요구사항을 모두 반영하여 Trustworthy Automotive SDLC를 제안한다.

3. Trustworthy Automotive SDLC

본 장에서는 기존의 Secure SDLC를 아우르는 보편적인 보안 내재화 방법론을 구축하고, 이를 기반으로 4가지 증거 기반 표준을 활용하여 자동차 개발에 적합한 상세화된 Trustworthy Automotive SDLC를 도출한다. Fig. 2는 본 논문에서 Trustworthy Automotive SDLC를 도출한 과정이다. 이는 자동차의 전체 시스템을 개발하고 완성차를 생산하는 관점에서 제안된 개발 프로세스로 기능 안전성과 보안성을 모두 고려함으로써 신뢰성이 확보된 자동차 개발을 가능하게 한다. 이때 시스템 내 구성요소에 따라 기능 안전성과 보안성이 다르게 적용될 수 있는데, 엔진을 예시로 들었을 때 기능 안전성 측면에서는 엔진과 엔진을 제어하는 소프트웨어를 모두 고려하지만, 보안성 측면에서는 엔진 자체가 아닌 엔진을 제어하는 소프트웨어를 대상으로 프로세스를 수행하게 된다. Trustworthy Automotive SDLC는 침투 테스트와 같은 일부 활동만을 통해 제품의 보안성을 고려하였던 기존 개발 방법론에 비해 보안성이 향상된 제품 개발을 가능하게 한다. 본 장의 세부 절에서는 Trustworthy Automotive SDLC의 요구사항, 설계 방법론, 단계별 수행 활동, 세부 수행 활동 및 단계별 산출물에 관해 서술한다.

3.1 Trustworthy Automotive SDLC의 요구사항

Trustworthy Automotive SDLC가 갖추어야 할 요구사항은 다음과 같다.

1. 시스템(하드웨어 및 소프트웨어) 대상의 프로세스
2. 타사의 구성요소를 획득하는 과정을 포함
3. 신뢰성 관점을 고려
4. 자동차가 필요로 하는 안전성 및 보안성 수준을 충족
5. 단계 수행에 따른 추적성을 확보
6. 프로세스의 모든 단계에 대해 상세화된 활동을 구성 (Depth = 2)

먼저 [50]에 따르면 자동차는 소프트웨어와 하드웨어를 포함하는 시스템의 형태로 개발된다. 따라서 Trustworthy Automotive SDLC는 시스템 기반의 프로세스를 구축해야 한다. 또한 소프트웨어 솔루션 업체 LDRA에 따르면 자동차 제조사는 자동차의 모든 구성요소를 자체적으로 개발하지 않고, 1-Tier, 2-Tier와 같은 협력 업체를 통해 획득한 구성요소를 활용한다[51]. 따라서 타사의 구성요소에 대한 신뢰성을 확보하기 위해 Trustworthy Automotive SDLC는 타사의 구성요소 획득에 대한 활동을 수행해야 한다.

세 번째로 [52]에서도 볼 수 있듯이, 자동차 개발에서는 정확성, 안전성, 보안성의 측면이 모두 포함된 Trustworthy 관점이 고려되어야 한다. 이때 정확성과 안전성 관점은 기존 자동차 기능 안전 개발 표준인 ISO 26262가 제안하는 안전 개발 생명주기와 안전성 수준인 ASIL(Automotive Safety

Integrity Level)을 통해 고려되어 왔기 때문에, 이를 기반으로 보안성을 접목할 수 있는 방법론을 설계해야 한다. 특히 기능 안전성과 보안성의 목표가 상충할 수 있는 부분은 개발 단계 초기에 식별해야 한다[53].

ISO 26262에서 요구하는 ASIL 등급은 자동차의 주요 기능에 따라 다르게 선정되며, 자동차 기능 안전 개발 프로세스에서는 각 기능에 부여된 ASIL 등급을 기반으로 자동차를 개발한다. 미국 보안 업체 Synopsys에 따르면 자동차의 주요 기능에 대해 개발에서 요구되는 ASIL 등급은 평균적으로 C 등급 이상이다[54]. 자동차에 대한 보안성 확보를 위해서는 두 가지 측면을 고려해야 한다. 먼저 자동차 시스템에서 요구하는 EAL 수준을 충족해야 하는데, EAL 수준이란 제품의 보안성 평가 관련 국제 표준인 CC의 보증 수준을 의미한다. [55]에 따르면 ISO 26262의 ASIL C 수준은 CC의 EAL5 수준에 해당한다. 따라서 본 논문에서는 Trustworthy Automotive SDLC가 자동차 개발에 대해 충분한 보안성을 확보하기 위해서 기능 안전성 측면의 ASIL C 수준에 해당하는 EAL5의 보증 수준을 충족해야 한다고 판단하였다. 이에 더해 Trustworthy Automotive SDLC에는 자동차 사이버보안 규제의 요구사항 또한 반영되어야 하는데, 이는 특히 국내뿐만 아니라 해외 시장을 대상으로 하는 자동차 제조사에 필수적이다. 본 논문에서는 앞서 언급하였던 UNECE 사이버보안 규제와 ISO/SAE 21434를 대상으로 하며, UNECE ISO/SAE 21434에 대해서는 필수 수행 요구사항인 RQ(Requirement) 만을 고려한다.

[51,56]에서 언급되었듯이 자동차는 시스템에서 발생 한 문제가 인명 피해로 이어질 수 있는 중요 시스템이기 때문에 Trustworthy Automotive SDLC는 단계 수행에 따른 목표, 요구사항, 아키텍처, 구현체 간의 일치성 및 완전성을 검증함으로써 보다 엄격하게 시스템에 대한 추적성을 확보해야 한다. 또한 Trustworthy Automotive SDLC는 프로세스의 모든 단계에 대해 충분히 상세화된 방법론을 제안함으로써 실제 대상에 이를 적용하기 용이하도록 해야 한다. 본 논문에서는 충분하게 상세화되었다는 의미를 Depth를 통해 나타낸다. Depth는 본 논문에서 정의한 활동의 상세화 정도에 대한 지표로서, 각 단계의 상세화 정도에 따라 Depth를 매길 수 있다. 예를 들어 '요구사항 분석'과 같은 단계는 0의 Depth를, '위험분석'과 같은 활동은 1의 Depth를 가진다. 하지만 프로세스가 세부 단계를 제시하지 않고 모범사례만을 나열했을 경우 해당 프로세스는 모든 활동에 대해 0의 Depth를 가진다고 할 수 있다. 본 논문이 제시하는 Trustworthy Automotive SDLC는 모든 단계의 수행 활동을 2의 Depth까지 상세화함으로써 실제 제품에 활용 가능한 형태를 제시한다.

3.2 Trustworthy Automotive SDLC의 설계 방법론

본 절에서는 3.1 절의 요구사항을 기반으로 Trustworthy Automotive SDLC를 도출하는 방법론을 서술한다. 본 논문에서는 보편적인 보안 내재화 방법론을 구축하기 위해 각 분야(기능 안전성, 보안성, 프라이버시)에서 대표로 활용되고 있는 4가지의 Secure SDLC 표준을 선정한 후 단계별 수행 활동을 도출하였다. 이후 도출된 활동을 증거 기반 표준의 각 요구사항에 매핑하였다. 증거 기반 표준은 개발 프로세스의 단계별 각 수행 활동에 대한 세부 항목을 제시함으로써 프로세스 수행에 대한 구체화된 방법을 제공하는 국제 표준들이다. 개발 프로세스를 여러 증거 기반 표준과 매핑하는 연구는 꾸준히 이루어져 왔지만, 이들은 모두 '요구사항 분석'과 같은 일부 단계에 치중되어 있거나[57], 충분한 구체화가 이루어지지 않았었다[58-67]. 본 논문에서는 CC, ISMS, PIMS, FSMS의 총 4가지 증거 기반 표준의 세부 항목을 Trustworthy Automotive SDLC의 단계별 수행 활동에 매핑하고, 이를 기반으로 단계별 수행 활동을 상세화하였다. Table 2는 Trustworthy Automotive SDLC의 단계에 따른 각 증거 기반 표준의 매핑 결과이다. 이 과정을 통해 Trustworthy Automotive SDLC는 제품과 제품 개발 환경에 대한 기능 안전성, 보안성, 프라이버시의 모든 측면에서 수행 활동을 더욱 구체화할 수 있게 된다(Fig. 3).

이후 구체화된 수행 활동을 기반으로 3.1절의 요구사항을 충족하는 활동을 선정하여 Trustworthy Automotive SDLC를 도출하였다. 최종적으로 도출된 Trustworthy Automotive SDLC는 Fig. 4와 같으며, 이는 10단계에 대한 총 50개의 활동으로 구성된다.

Table 2. Evidence-based Standards

	CC	ISMS	PIMS	FSMS
Target	Product	Environment	Privacy	Functional safety
Description	Standards for evaluating the security and reliability of IT products	Standards for security and reliability certification of an organization's assets	Standards providing detailed criteria for performance of privacy impact assessment	Standards presenting processes for automotive functional safety development
Mapping Phases	2,3,5-10	1-10	2,5,8,10	1-10
Source	ISO/IEC 15408	ISO/IEC 27001	ISO/IEC 27701	ISO 26262

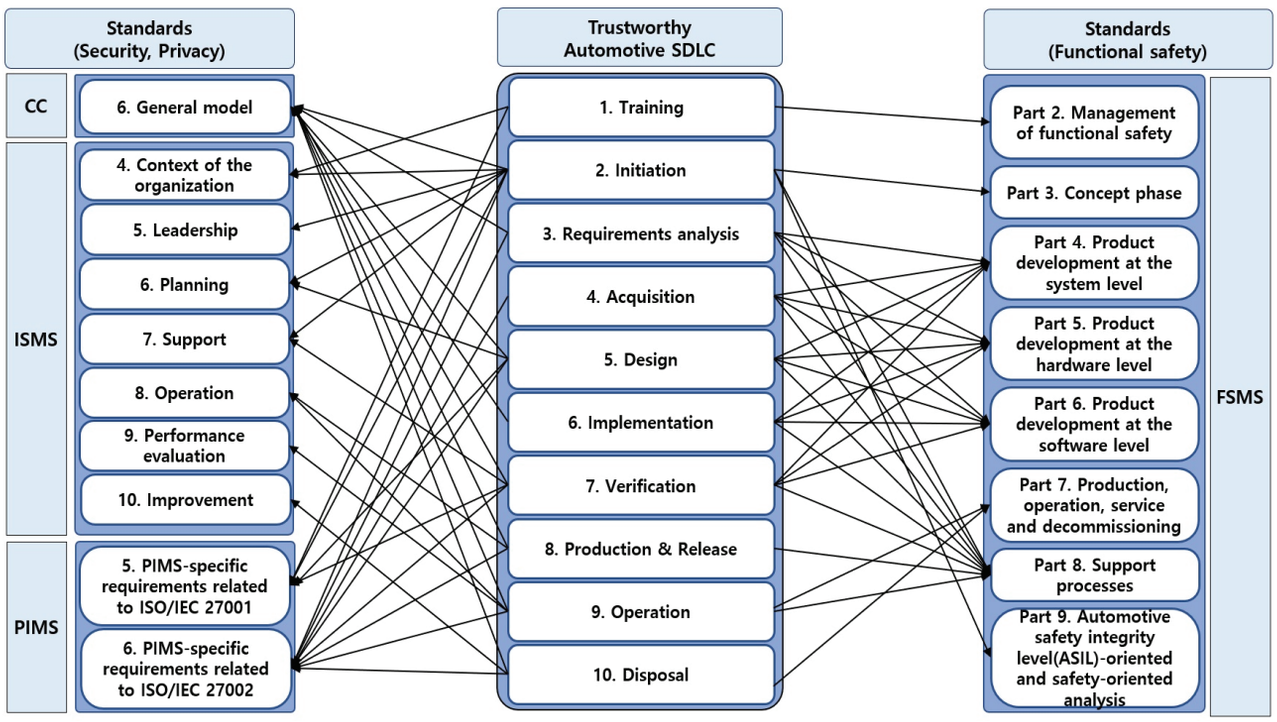

Fig. 3. Mapping between Trustworthy Automotive SDLC and Evidence-based Standards

Trustworthy Automotive SDLC는 앞서 언급하였듯이 시스템을 대상으로 하는 방법론이며, '4. 획득' 단계를 통해 타사의 구성요소에 대한 획득 과정을 수행한다. 또한 Fig. 3에서 볼 수 있듯이 FSMS의 각 Part에 따른 단계 매핑이 가능하므로 기존에 수행하던 기능 안전 개발 프로세스에 병합하여 활용할 수 있다. 이때 보안 개발 프로세스와 기능 안전 개발 프로세스를 병합하면서 발생할 수 있는 기능 안전성과 보안성 간의 목표 충돌 여부는 '3.1.2 분야별 영향평가 결과에 대한 적합성 및 충돌 여부 판단'과 '3.2.2 분야별 요구사항에 대한 적합성 및 충돌 여부 판단', '5.2.3 분야별 완화방안에 대한 적합성 및 충돌 여부 판단'을 통해 해결할 수 있다. 이에 더해 Trustworthy Automotive SDLC는 자동차 개발에서 요구되는 보안 수준인 EAL5 수준을 충족하는 활동으로 구성되어 있으며, ISO/SAE 21434 국제 표준 및 UNECE 사이버 보안 규제의 요구사항을 만족함으로써 UNECE 사이버보안 규제에 대응 가능한 형태를 가진다.

3.3 Trustworthy Automotive SDLC의 단계별 수행 활동

본 절에서는 Trustworthy Automotive SDLC의 10단계와 단계별 수행 활동에 대한 설명을 제시한다.

1) 교육 단계: 교육 단계에서는 조직 구성원을 대상으로 기능 안전성, 보안성, 프라이버시에 대한 인식을 확보하고 개발 프로세스를 수행하면서 필요한 관련 지식을 교육한다. 보안성이나 안전성과 관련된 기능을 개발하거나 관리하는 일부 팀의 경우 이에 대한 배경지식을 가지고 있지만, 개발팀과 같은 그 외의 구성원은 신뢰성에 관한 지식이 부재한 경우가 많다. 따라서 분야별 교육을 통해 프로세스 수행에 요구되는 주제를 교육해야 한다. 먼저 기본 교육에서는 안전성, 보안성 및 프라이버시에 대한 인식 확보를 위한 주제를 다룬다. 이에 더해 위험분석과 같은 개발 프로세스 내에서 다뤄지는 주제에 대한 기본 지식을 교육함으로써 조직의 구성원들이 프로세스를 수행하는데 위화감이 없도록 한다. 심화 교육은 직무에 따라 부여되는 별도의 교육으로, 보안의 측면에서 보면 개발팀 대상의 보안 설계 및 시큐어 코딩, 평가팀 대상의 정적 및 동적 분석, 보안팀 대상의 보안 및 프라이버시 관련 규제 인증과 같은 주제를 통해 각 실무자가 담당한 Trustworthy Automotive SDLC의 활동을 수행하는 방법을 교육한다. 이때 모든 교육은 로드맵을 통해 관리되며, 교육 대상자에 따른 교육 준수 여부를 관리함으로써 교육 수강 여부에 대한 추적성을 확보한다.

2) 착수 및 계획 단계: 착수 및 계획 단계에서는 프로젝트에 대한 개발 환경을 구축하고 프로젝트의 전반적인 계획을 수립하며, 분야별 목표를 설정한다. 먼저 해당 단계에서는 프로젝트에서 취급하는 정보 자산과 제품 유형, 프로젝트 특성을 고려하여 프로젝트 범주화를 수행한다. 또한 이를 기반으로 역할 및 도구, 최소 품질 수준 등을 포함한 프로젝트 전반에 대한 계획을 수립한다. 이때 최소 품질 수준은 프로젝트를

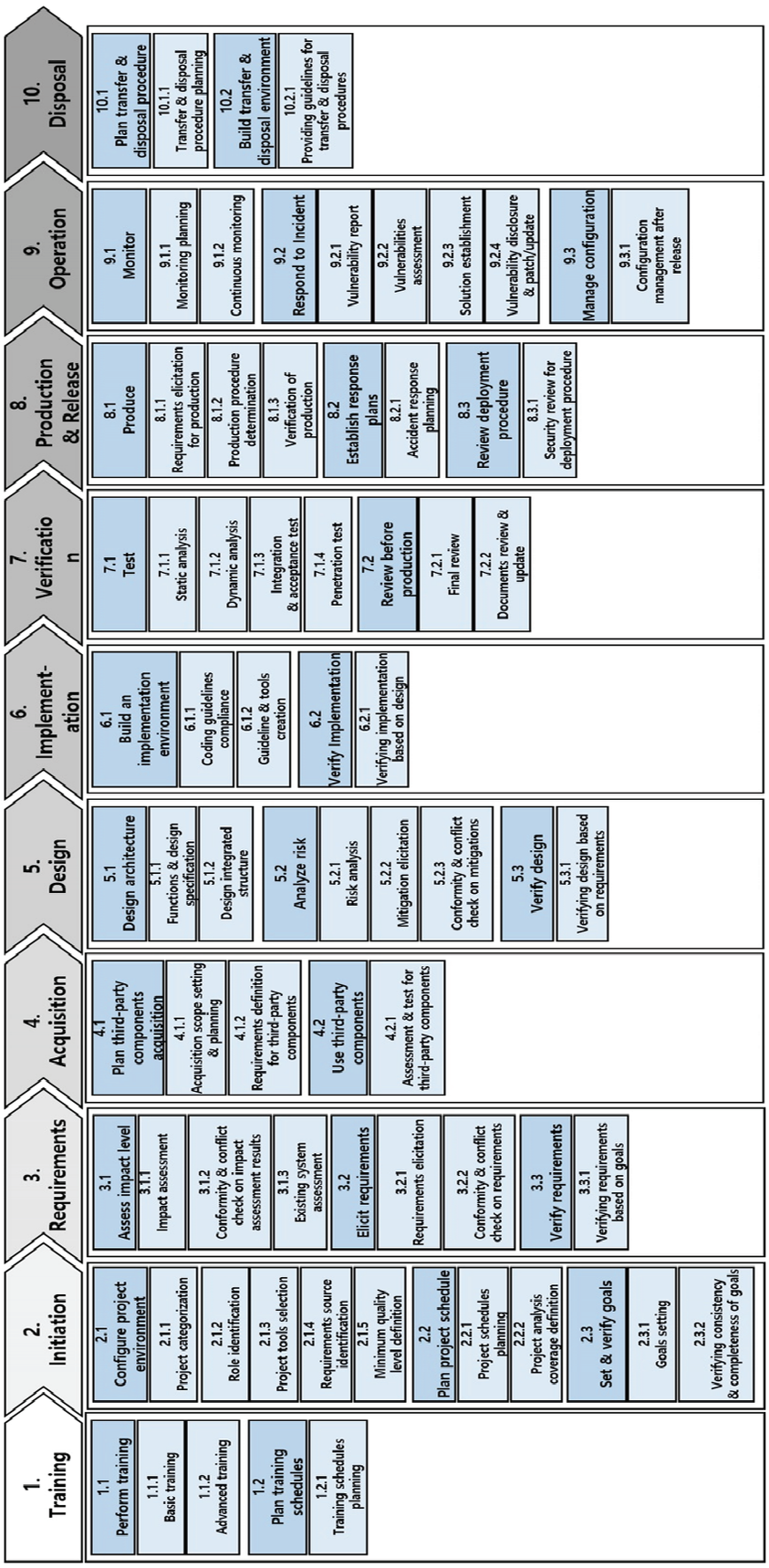

Fig. 4. Trustworthy Automotive SDLC Detailed Activities

수행하면서 반드시 충족시켜야 할 최소한의 보안성, 안전성 및 프라이버시 수준으로, 이를 충족하지 못하면 다음 단계를 수행할 수 없다. 또한 프로젝트에 대한 분야별 목표를 설정하고, 서로 다른 목표 간 일관성 및 완전성을 검증함으로써 이후 단계 수행에 대한 추적성을 확보한다.

자동차 개발의 경우 시스템, 소프트웨어, 하드웨어 수준에 따라 개발이 별도로 수행되기 때문에 해당 단계를 각 수준에 맞춰 진행하게 된다. 이때 시스템 수준의 착수 및 계획 단계에서는 소프트웨어 및 하드웨어 수준을 아우르는 프로젝트 전반의 환경 및 계획을 수립함으로써 소프트웨어 및 하드웨어 개발에 대한 일관성을 확보해야 한다. 이러한 구조는 Fig. 3을 통해 볼 수 있듯이 초기 단계부터 배포 단계까지 동일하게 적용된다.

3) 요구사항 분석 단계: 요구사항 분석 단계에서는 프로젝트의 보안성, 안전성 및 프라이버시 관련 자산에 대한 영향평가를 수행하고 그 결과를 기반으로 분야별 요구사항을 도출한다. 또한 목표와 요구사항 간 일관성 및 완전성을 검증함으로써 착수 및 계획 단계와 요구사항 분석 단계 간의 추적성을 확보한다. 앞서 언급하였듯이 기능 안전성과 보안성의 목표는 충돌할 수 있다[53]. 따라서 해당 단계에서는 '3.1.2 분야별 영향평가 결과에 대한 적합성 및 충돌 여부 판단'을 통해 안전성 및 보안성 영향 수준에 대한 우선순위를 식별한다. 이에 더해 기존 시스템을 재사용하는 경우, 재사용 시스템에 대한 보안성 및 안전성 영향 또한 평가한다. 요구사항을 식별할 때도 마찬가지로 분야별 요구사항에 대한 적합성 및 충돌 여부를 판단함으로써 해당 단계 이후 안전성과 보안성 간의 충돌이 없도록 한다. 마지막으로 앞서 도출한 목표에 따른 요구사항의 일관성 및 완전성을 검증함으로써 착수 및 계획 단계와 요구사항 분석 단계 간의 추적성을 확보한다.

4) 획득 단계: 획득 단계에서는 타사의 구성요소 획득에 대한 범위 및 계획을 수립하고 관련 요구사항을 정의한다. 또한 정의한 요구사항을 기반으로 대상 업체가 제출한 명세에 대해 평가 및 테스트를 수행한다. 이때 타사의 구성요소는 1-Tier, 2-Tier 등의 협력 업체를 통해 획득한 구성요소를 의미한다. 또한 해당 단계에서는 자동차 제조사의 요구사항에 맞추어 제출한 타사의 구성요소의 명세를 기반으로 자동차 제조사가 독립적인 평가 및 테스트를 수행한다. 특히 자동차 개발의 경우 협력 업체를 통한 서브 시스템 개발이 전체 개발에 큰 비중을 차지하므로 해당 단계의 수행은 필수적이다.

5) 설계 단계: 설계 단계에서는 아키텍처를 설계하고 이를 기반으로 한 분야별 위험분석을 수행한다. 자동차 개발의 경우 서브 시스템을 기반으로 하나의 통합 시스템을 구성하기 때문에, 해당 단계에서는 시스템 통합 과정에 대한 아키텍처 설계도 고려한다. 해당 단계에서는 도출된 아키텍처를 기반으로 분야별 위험분석을 수행하여 시스템 내에 발생 가능한 위협에 대해 완화방안을 도출한다. 앞선 단계와 마찬가지로 설계 단계에서는 분야별 완화방안에 대한 적합성 및 충돌 여부를 판단함으로써 이후 기능 안전 개발 프로세스와 보안 개발 프로세스 간의 충돌이 발생하지 않도록 한다. 또한 요구사항에 따라 아키텍처의 일관성 및 완전성을 검증함으로써 요구사항 분석 단계와 설계 단계 간의 추적성을 확보한다.

6) 구현 단계: 구현 단계에서는 앞서 도출한 요구사항 및 아키텍처를 기반으로 시스템을 구현한다. 이때 개발자는 코딩 가이드라인을 통해 시스템을 구현하며, 코딩 가이드라인에는 기존에 확립된 MISRA C 등의 코딩 표준이 포함될 수 있다[68]. 또한 개발자는 배포된 시스템을 사용자가 사용할 때 신뢰성이 확보된 운영 환경을 구축할 수 있도록 배포 가이드라인 또는 도구를 생성한다. 구현 단계에서도 마찬가지로 아키텍처와 구현체 간의 일관성 및 완전성을 검증함으로써 설계 단계와 구현 단계 간의 추적성을 확보한다.

7) 검증 단계: 검증 단계에서는 구현된 시스템을 기반으로 테스트 및 검토를 수행한다. 이때 테스트는 정적 및 동적 분석, 인수 테스트를 포함한다. 또한 자동차는 서브 시스템을 기반으로 구성되는 통합 시스템이므로 해당 단계에서는 시스템을 통합하는 과정에서 문제가 발생하지 않는지를 판단하는 통합 테스트를 수행한다. 이때 통합은 서브 시스템 기반의 통합을 의미하기도 하지만 하드웨어와 소프트웨어 기반의 시스템 통합 또한 포함한다. 이후 통합된 시스템에 대해 보안 위협이 존재하는지를 판단하기 위해 침투 테스트를 수행하며, 시스템을 구현하면서 기존에 설계한 내용과 변경된 사항이 있는지 여부나 변경사항이 보안성, 안전성 및 프라이버시 관련 문제를 발생시키지는 않는지를 프로젝트 최소 품질 수준이나 산출된 문서 측면에서 검토한다.

8) 생산 및 배포 단계: 생산 및 배포 단계에서는 시스템을 생산하고, 배포 후 시스템에서 발생 가능한 사고에 대해 대응계획을 수립한다. 이때 생산은 시스템 생산 공정을 의미하는데, 자동차의 경우 복잡하고 긴 생산 공정을 통해 생산하는 과정을 거치기 때문에 해당 과정에 대한 보안성을 반드시 확보해야 한다. 또한 해당 단계에서는 생산이 완료된 시스템을 배포하는 과정에서도 보안 문제가 발생하는지를 검토한다.

9) 운영 단계: 운영 단계에서는 배포 이후에 시스템에서 발생할 수 있는 취약점을 모니터링하고 발견된 취약점에 대해 대응한다. 이때 모니터링 계획을 수립하여 이를 기반으로 시

스템에 대한 지속적인 모니터링을 수행해야 한다. 또한 사고 발생에 대한 취약점 리포트를 수집하고 이를 평가하여 대응 방안을 도출한다. 이후 해당 대응 방안은 패치 또는 업데이트를 통해 공개 및 배포한다. 특히 자동차의 경우 문제 발생이 인명 피해와 직접 연결될 수 있으므로 24시간 대응 가능한 담당팀을 배치하는 것이 중요하다. 이처럼 운영 중인 시스템에 변경사항이 생겼을 경우, 해당 변경사항에 대해서 형상을 관리함으로써 시스템에 대한 추적성을 확보한다.

10) 폐기 단계: 폐기 단계에서는 시스템에 대한 사용을 종료하고 전이 및 폐기를 수행한다. 이때 시스템 전이는 소유자 이전, 시스템 폐기는 폐차의 경우를 의미한다. 자동차 제조사는 시스템 폐기에 대한 과정을 자체적으로 수행하지는 않지만, 시스템이 전이 또는 폐기될 시 어떤 정보가 보존되거나 소거되어야 하는지에 대한 정보를 가이드 문서를 통해 관련 업체에 제공함으로써 시스템 폐기에 대한 신뢰성을 확보해야 한다.

해당 가이드 문서는 사용자 개인정보에 대한 완전한 소거 방법, 자동차 주행 거리와 같이 이후 활용 가능한 내부 정보에 대한 보존 여부 등을 포함해야 한다. 자동차는 활용도에 따라 중고차 판매와 같은 소유자 이전, 렌터카와 같은 다수의 사용자에 의한 활용 등의 다양한 상황이 고려될 수 있다. 따라서 폐기 단계에서 자동차 제조사는 해당 시스템의 활용도나 특성에 적합한 과정을 수행할 수 있도록 담당 업체에 정보를 제공해야 한다.

3.4 Trustworthy Automotive SDLC의 세부 수행 활동 및 단계별 산출물

본 절에서는 증거 기반 표준을 기반으로 앞서 도출한 Trustworthy Automotive SDLC에 대해 세부 수행 활동 및 단계별 산출물을 제시한다. 이때 Fig. 3을 통해 볼 수 있듯이 Trustworthy Automotive SDLC의 수행 활동을 각 증거 기반 표준의 세부 항목과 매핑한 후 세부 수행 활동과 단계별 산출물을 도출하게 된다.

본 논문에서는 증거 기반 표준의 세부 항목을 CC에서 63개, ISMS에서 104개, PIMS에서 54개, FSMS에서 172개 활용하여 총 393개의 세부 항목들과 50개의 수행 활동 간 매핑을 수행함으로써 세부 수행 활동들을 도출하였다. 하나의 예시로 CC의 AGD 클래스는 사용자에게 제품을 배포할 시 사용자가 사용자 운영 설명서를 통해서 안전하게 운영 환경을 구축할 수 있는지를 판단하는 항목을 포함한다. 이러한 부분은 Trustworthy Automotive SDLC의 6.1.2 가이드라인 및 도구 생성에 매핑할 수 있고, 이를 통해 해당 활동을 수행할 때 AGD 클래스의 사용자 운영 설명서에서 요구하는 항목(예: 사용자 운영 설명서는 각각의 사용자 역할에 대해 안전한 처리환경 내에서 통제되어야 하는 사용자가 접근 가능한 기능 및 특권에 대해 적절한 경고를 포함해서 서술해야 한다.)들을 반영할 수 있게 된다. 결과적으로 해당 과정을 통해 보안성, 안전성, 프라이버시 측면에서 Trustworthy Automotive SDLC의 세부 수행 활동이 도출된다. 또한 이 과정에서 Trustworthy Automotive SDLC의 단계별로 문서를 산출할 수 있으며, 단계별 산출물 목록은 Table 3과 같다.

먼저 교육 단계에서는 기본 및 심화 교육의 목적, 대상자, 각 교육에서 다루어지는 주제 등을 포함하는 교육 계획서를 산출해야 하며, 교육 대상자마다 수강해야 하는 교육 목록, 해당 교육의 수강 여부를 추적할 수 있는 교육 참석 명단을 문서화해야 한다.

착수 및 계획 단계에서는 프로젝트의 분야별 자산, 담당자(보안팀, 개발팀, 설계팀 등)의 수행 역할 및 활용 도구, 최소 품질 수준 등을 포함하는 프로젝트 계획서를 산출해야 한다. 특히 최소 품질 수준의 경우, 프로젝트의 단계 수행 여부에 대한 기준선이 되므로 반드시 포함해야 한다. 이에 더해 프로젝트에 대한 보안성, 안전성, 프라이버시 측면의 목표와 분야별 목표 간 일관성 및 완전성 검증 결과를 산출하여 프로젝트 목표 검증서로 문서화해야 한다.

Table 3. Evidences of Trustworthy Automotive SDLC

Phase		Evidence
1	Training	· Training plan · List of attendance at training
2	Initiation	· Project plan · Project goal verification report
3	Require-ments	· Impact assessment report · Requirements definition report · Project requirements verification report
4	Acquisition	· Acquisition plan · Acquisition inspection report
5	Design	· Design specification · Architecture specification · System Risk Analysis report · Project design verification report
6	Impleme-ntation	· System implementation report · User's manual or tool · Project implementation verification report
7	Verification	· Test plan · Test result report · Vulnerability Analysis report · Final review report
8	Production & Release	· Production plan · Production verification report · Accident response plan
9	Operation	· System monitoring report · Accident response report
10	Disposal	· Guidelines for system transfer and disposal

요구사항 분석 단계에서는 안전성 측면의 ASIL과 같은 분야별 자산의 영향력을 평가한 영향 평가서와 이를 기반으로 하는 요구사항 정의서를 산출해야 한다. 이때 영향 평가서에는 재사용되는 기존 시스템에 대한 영향평가 결과도 포함되어야 한다. 또한 각 분야의 요구사항 간 충돌 여부는 없는지, 요구사항이 프로젝트의 목표를 기반으로 일관되고, 완전하게 도출되었는지 등의 분석 결과를 포함하는 프로젝트 요구사항 검증서를 도출해야 한다.

획득 단계에서는 타사가 개발한 구성요소에 대한 획득 요구사항 및 과정을 포함하는 획득 계획서를 산출해야 한다. 또한 해당 문서를 기반으로 타사가 제공한 구성요소에 대해 별도로 수행한 평가 및 테스트 결과를 포함하는 획득 검수서가 도출되어야 한다.

설계 단계에서는 모듈이나 인터페이스와 같은 단위에 대한 설계 명세서와 이를 모두 포함하는 전체 시스템에 대한 아키텍처 설계서를 도출해야 한다. 또한 위험분석 결과를 기반으로 완화방안을 포함하는 시스템 위험분석서를 산출해야 한다. 이때 해당 문서에는 분야별 완화방안의 적합성 및 충돌 여부 분석 결과가 포함되어야 하며, 별도로 요구사항에 대한 설계의 일관성 및 완전성 분석 결과를 프로젝트 설계 검증서로 산출해야 한다.

구현 단계에서는 코딩 가이드라인을 기반으로 개발한 소스코드를 포함하는 시스템 구현 결과서가 산출되어야 하며, 설치 환경과 관련된 정보를 포함하여 사용자에게 제공되는 사용자 매뉴얼이나 도구에 대해 문서화해야 한다. 해당 단계에서도 동일하게 아키텍처를 기반으로 수행한 구현체의 일관성 및 완전성 분석 결과를 프로젝트 구현 검증서로 문서화해야 한다.

검증 단계에서는 테스트 시나리오와 테스트 케이스를 포함하는 테스트 계획서와 정적 및 동적 분석 수행 결과를 포함하는 테스트 결과서를 산출해야 한다. 독립적인 침투 테스트 수행 결과의 경우 별도의 취약성 분석서를 통해 문서화해야 하며, 제품을 생산하기 전의 모든 단계가 제대로 수행되었는지를 검토하여 최종 검토 결과서를 생성해야 한다.

생산 및 배포 단계에서는 제품의 생산 계획 및 과정을 포함하는 생산 계획서를 산출하고, 실제 생산된 제품에 대한 생산 검증서를 문서화해야 한다. 또한 이후 발생 가능한 사고에 대한 대응 방안을 포함하는 사고 대응 계획서를 산출해야 한다.

운영 단계에서는 서버나 방화벽 등에 대해 수행한 모니터링을 기반으로 시스템 모니터링 결과서를 도출해야 한다. 또한 발견된 취약점의 평가 결과와 해당 취약점의 공개 및 패치/업데이트 관리 방안을 포함하는 사고 대응 결과서를 산출해야 한다.

마지막으로 폐기 단계에서는 사용자 및 관련 업체를 대상으로 하는 시스템의 전이 및 폐기 가이드라인을 산출함으로써 자동차 제조사가 별도로 관리하지 않는 상황에서도 시스템이 안전하게 전이 또는 폐기될 수 있도록 해야 한다.

4. 연구 결과에 관한 비교 및 분석

4.1 Secure SDLC 표준 및 기존 연구와의 비교

Trustworthy Automotive SDLC는 6개의 요구사항을 기반으로 설계된 자동차 보안 내재화 방법론으로, 이는 앞서 언급한 Secure SDLC 표준 및 기존 연구보다 상세한 활동을 제시하며 자동차 개발에 적합하다. Table 4는 Trustworthy Automotive SDLC의 각 요구사항에 대해 기존 Secure SDLC 표준 및 기존 연구의 충족 여부를 비교 분석한 결과이다. 이때 대상 Secure SDLC 표준으로는 Microsoft SDL, NIST SSDLC, OWASP CLASP, SAE J3061를 선정하였고, 기존 연구로는 2.1절에서 언급한 논문 중 개발 프로세스 전체를 대상으로 하는 연구를 선정하였다[18,19,22,29,40]. 비교 분석을 수행한 결과, 기존 연구와 Secure SDLC 표준은 자동차에 적합한 보안 내재화 방법론을 제시함에 있어 본 연구 결과보다 부족함을 알 수 있었다. 특히 모든 비교 대상이 '4. 자동차 개발이

Table 4. Limitations of Secure SDLC Standards and Existing Studies

Requirements		Secure SDLC Standards				Existing Studies					Trustworthy Automotive SDLC
		Microsoft SDL	NIST SSDLC	OWASP CLASP	SAE J3061	[44]	[45]	[48]	[55]	[66]	
1	Targets on system	X	O	X	O	O	O	O	O	O	O
2	Includes the procedure of third-party components acquisition	X	O	O	O	X	X	X	X	X	O
3	Considers aspect of trustworthiness	X	X	X	O	O	O	O	O	O	O
4	Satisfies the level of safety and security required by automotive development	X	X	X	X	X	X	X	X	X	O
5	Ensures traceability between phases	O	O	X	O	X	X	O	X	X	O
6	Provides detailed activities for every phase of the process	X	X	X	X	X	X	X	X	X	O

Table 5. Mapping between UNECE Regulation Requirements and Trustworthy Automotive SDLC Activities

UNECE Regulation Requirements (7.2. Requirements for the CSMS(Cyber Security Management System))		Trustworthy Automotive SDLC Activities (Activity Number)
1	The vehicle manufacturer shall have a CSMS in place and shall comply with this Regulation.	Total
2	The vehicle manufacturer shall demonstrate that their CSMS applies to the development phase.	Total
3	CSMS shall include the processes used within the manufacturer's organization to manage cyber security.	Total
4	CSMS shall include the processes used for the identification of risks to vehicles.	3.1.1/3.1.2/5.2.1/ 5.2.3
5	CSMS shall include the processes used for the assessment, categorization and treatment of the risks identified.	5.2.2/5.2.3
6	The vehicle manufacturer shall demonstrate how their CSMS will manage dependencies that may exist with contracted suppliers, service providers or manufacturer's sub-organizations.	4.1.1/4.1.2/4.2.1
7	CSMS ensure security shall include the processes used for testing the cyber security of a vehicle.	7.1.1/7.1.2/7.1.3/7.1.4
8	CSMS ensure security shall include the processes in place to verify that the risks identified are appropriately managed.	7.2.1/9.1.1/9.1.2/9.3.1
9	The vehicle manufacturer shall demonstrate that their CSMS applies to the production phase.	8.1.1/8.1.2/8.1.3
10	The vehicle manufacturer shall demonstrate that the processes that include the capability to analyze and detect cyber threats, vulnerabilities and cyber-attacks from vehicle data and vehicle logs.	9.1.1/9.1.2/9.2.1
11	CSMS shall include the processes used for ensuring that the risk assessment is kept current.	9.2.4/9.3.1
12	CSMS shall include the processes used to monitor for, detect and respond to cyber-attacks, cyber threats and vulnerabilities on vehicles.	9.1.1/9.1.2/9.2.1/9.2.2/9.2.3/9.2.4/9.3.1
13	CSMS shall include the processes used to assess whether the cyber security measures implemented are still effective in the light of new cyber threats and vulnerabilities that have been identified.	7.2.1/9.2.3
14	The vehicle manufacturer shall demonstrate that the processes used within their CSMS will ensure that cyber threats and vulnerabilities which require a response from the vehicle manufacturer shall be mitigated within a reasonable timeframe.	9.2.1/9.2.2/9.2.3/9.2.4
15	The vehicle manufacturer shall demonstrate that the processes that include vehicles after first registration in the monitoring.	9.1.1/9.1.2
16	The vehicle manufacturer shall demonstrate that their CSMS applies to the post-production phase.	8.1.1/8.1.2/8.1.3/8.2.1/8.3.1/9.1.1/9.1.2/9.2.1/9.2.2/9.2.3/9.2.4/9.3.1/10.1.1/10.2.1

필요로 하는 안전성 및 보안성 수준을 충족'을 만족하지 못함을 확인할 수 있었다. 또한 이는 '6. 프로세스의 모든 단계에 대해 상세화된 활동을 구성'에 대해서도 마찬가지였는데, 기존 Secure SDLC에서는 2의 Depth를 가지는 활동이 최대 36개 도출됐지만 본 논문이 제안하는 Trustworthy Automotive SDLC는 2의 Depth를 가지는 50개의 활동으로 구성되어 있다. 따라서 기존 표준들에 대해 Trustworthy Automotive SDLC의 구성 활동은 충분한 구체화가 이루어졌다고 할 수 있다.

4.2 UNECE 사이버보안 규제 요구사항에 대한 분석

Trustworthy Automotive SDLC는 다가오는 UNECE 사이버보안 규제에 대한 대응을 가능하게 함으로써 국내뿐만 아니라 해외 시장을 목표로 하는 자동차 제조사에 적합한 개발 프로세스를 제공한다. 이를 검증하기 위해 본 논문에서는 UNECE 사이버보안 규제에서 개발 프로세스와 관련이 있는 총 16개의 요구사항을 각 Trustworthy Automotive SDLC의 활동을 매핑하여 그 충족 여부를 파악하였다. 그 결과, Table 5에서 볼 수 있듯이 Trustworthy Automotive SDLC를 통해 UNECE 사이버보안 규제에서 제시하는 요구사항을

Table 6. Trustworthy Automotive SDLC Activities Fulfillment

Phase		Number of Activities (A/TA_SDLC)
1	Training	2/3
2	Initiation	8/9
3	Requirements	3/6
4	Acquisition	3/3
5	Design	5/6
6	Implementation	2/3
7	Verification	3/6
8	Production & Release	4/5
9	Operation	4/7
10	Disposal	0/2
Total		34/50

모두 만족할 수 있음을 확인하였다. 따라서 본 논문이 제시하는 자동차 보안 내재화 방법론이 UNECE 사이버보안 규제에 대해 인증 가능한 형태를 가진다고 할 수 있다.

5. 사례 연구

본 장에서는 앞서 도출한 자동차 보안 내재화 방법론의 실효성을 입증하기 위해 국내 자동차 제조사인 A사를 대상으로 사례 연구를 수행하였다. A사는 국내뿐만 아니라 해외 시장 또한 목표로 하는 자동차 제조사이며, 특히 유럽 시장에 대한 수출을 위해 현재 UNECE 사이버보안 규제에 대한 대응을 준비하고 있다. 본 논문에서는 인터뷰와 설문조사를 기반으로 A사의 현재 개발 프로세스와 수행 활동에 대해 파악한 후, 해당 프로세스가 Trustworthy Automotive SDLC의 활동을 어느 정도 만족하는지를 분석하였다.

A사의 개발 프로세스를 본 연구에서 제안하는 Trustworthy Automotive SDLC(이하 TA_ADLC)의 각 단계 및 수행 활동에 매핑한 결과, Table 6에서와 같이 해당 프로세스가 Trustworthy Automotive SDLC에서 제시하는 50개의 활동 중 총 34개의 활동만을 수행하고 있음을 확인할 수 있었다. 따라서 자동차 보안 내재화를 달성하기 위해 A사는 기존 개발 프로세스에 16개의 활동을 추가적으로 수행해야 함이 도출되었다.

이는 Trustworthy Automotive SDLC를 실제 자동차 제조사에 적용한 결과로, 본 논문에서 제시하는 방법론을 기반으로 자동차 제조사가 해당 기업의 개발 프로세스를 개선하여 UNECE 사이버보안 규제를 만족함과 동시에 신뢰성이 확보된 자동차를 개발할 수 있을 것이라는 가능성을 제시하였다.

6. 결 론

기존의 자동차 개발은 정확성과 안전성 확보에 초점을 맞추어 왔으며, 보안성은 중점적으로 다루지 않았다. 하지만 최근 자동차의 인터넷 연결성이 높아짐에 따라 자동차 해킹 사례가 증가하면서, 여러 국제기관은 자동차 개발에 대한 보안성을 확보하기 위한 사이버보안 규제를 준비하고 있고, 대표적으로 UNECE 사이버보안 규제는 2022년부터 신차를 기준으로 적용될 예정이다. UNECE 사이버보안 규제에서는 개발 초기부터 신뢰성을 고려하는 보안 내재화를 강조하지만, 해당 규제는 보안 내재화를 달성하기 위한 구체적인 방법론은 제시하지 않는다. 또한 이는 기존에 연구되었던 논문들에서도 마찬가지이다. 따라서 본 논문에서는 이를 해결하고자 하기 위해 자동차 보안 내재화를 위한 구체적인 방법론인 Trustworthy Automotive SDLC를 제안하였다.

본 논문에서는 먼저 4개의 주요 Secure SDLC 표준에서 자동차 개발과 관련된 활동을 도출하고 이를 제품 및 개발 환경에 대한 보안성, 프라이버시, 기능 안전성 측면의 증거 기반 표준인 CC, ISMS, PIMS, FSMS의 세부 항목에 매핑한다. 또한 매핑된 결과를 기반으로 자동차 개발에 적합한 상세화된 Trustworthy Automotive SDLC를 구성하였다. 이에 더해 본 논문에서는 사례 연구를 통해 Trustworthy Automotive SDLC 적용에 대한 효과를 입증하였다. Trustworthy Automotive SDLC는 자동차 개발에 중요한 정확성, 안전성, 보안성의 측면을 모두 고려하며, 기존의 Secure SDLC 표준 및 증거 기반 표준을 통해 구체화한 활동으로 구성되어 있으므로 다가오는 자동차 사이버보안 규제에 대응하기 위해 활용할 수 있다.

References

[1] R. Bell, “Introduction to IEC 61508,” *ACM International Conference Proceeding Series,* Vol.162, pp.3-12, 2006.

[2] Amiso M. George, “Japan (Toyota),” in C*ase studies in crisis communication: International perspectives on hits and misses*, Part Ⅲ, pp.227-252, 1997.

[3] R. Debouk, “Overview of the 2nd Edition of ISO 26262: Functional safety-road vehicles,” General Motors Company, Warren, MI, USA, 2018.

[4] Craigen, Dan, Nadia Diakun-Thibault, and Randy Purse., “Defining cybersecurity,” *Technology Innovation Management Review*, Vol.4, No.10, 2014.

[5] J. M ssinger, “Software in automotive systems,” *IEEE Software*, Vol.27, No.2, pp.92-94, 2010.

[6] C. Miller and C. Valasek. “Remote exploitation of an unaltered passenger vehicle,” in *Black Hat USA,* pp.91, 2015.

[7] Mathias Dehm, Markus Tschersich, “Road Vehicles' Life-Cycle: Mapping of relevant standards and regulations for automotive cybersecurity,” in *ESCAR Europe,* 2019.

[8] H. Khattri, N. K. V. Mangipudi, and S. Mandujano, "Hsdl: A security development lifecycle for hardware technologies," *2012 IEEE International Symposium on Hardware-Oriented Security and Trust,* pp.116-121, 2012.

[9] P. Salini and S. Kanmani. "Survey and analysis on security requirements engineering," *Computers & Electrical Engineering,* Vol.38, No.6, pp.1785-1797, 2012.

[10] S. Khou, L. O. Mailloux, J. M. Pecarina, and M. Mcevilley, "A customizable framework for prioritizing systems security engineering processes, activities, and tasks," *IEEE Access*, Vol.5, pp.12878-12894, 2017.

[11] N. M. Mohammed, M. Niazi, M. Alshayeb, and S. Mahmood, "Exploring software security approaches in software development lifecycle: A systematic mapping study," *Computer Standards & Interfaces*, Vol.50, pp.107-115, 2017.

[12] T. Loruenser, H. C. Pöhls, L. Sell, and T. Laenger, "CryptSDLC: Embedding cryptographic engineering into secure software development lifecycle," *Proceedings of the 13th International Conference on Availability, Reliability and Security*, pp.1-9, 2018.

[13] Ruggieri, Maxwell, Tzu-Tang Hsu, and Md Liakat Ali. "Security Considerations for the Development of Secure Software Systems," *2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON),* pp.1187-1193, 2019.

[14] E. Venson, X. Guo, Z. Yan, and B. Boehm, "Costing Secure Software Development: A Systematic Mapping Study," *Proceedings of the 14th International Conference on Availability, Reliability and Security,* pp.1-11, 2019.

[15] V. Casola, A. De Benedictis, M. Rak, and U. Villano, "A novel Security-by-Design methodology: Modeling and assessing security by SLAs with a quantitative approach," *Jounal of Systems and Software*, Vol.163, pp.110537, 2020.

[16] A. Avizienis, J. C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Transactions on Dependable and Secure Computing,* Vol.1, No.1, pp.11-33, 2004.

[17] A. Michailidis, U. Spieth, T. Ringler, B. Hedenetz, and S. Kowalewski, "Test front loading in early stages of automotive software development based on AUTOSAR," *2010 Design, Automation & Test in Europe Conference & Exhibition (DATE 2010),* pp.435-440, 2010.

[18] R. Y. Takahira, L. R. Laraia, F. A. Dias, S. Y. Abraham, P. T. Nascimento, and A. S. Camargo, "Scrum and Embedded Software development for the automotive industry," *Proceedings of PICMET'14 Conference: Portland International Center for Management of Engineering and Technology; Infrastructure and Service Integration,* pp.2664-2672, 2014.

[19] Young, William, and Nancy G. Leveson. "An integrated approach to safety and security based on systems theory," *Communications of the ACM*, Vol.57, No.2, pp.31-35, 2014.

[20] S. Kriaa, L. Pietre-Cambacedes, M. Bouissou and Y. Halgand, "A survey of approaches combining safety and security for industrial control systems," *Reliability Engineering & System Safety*, Vol.139, pp.156-178, 2015.

[21] C. Wolff, L. Krawczyk, R. Höttger, C. Brink, U. Lauschner, D. Fruhner, ... and B. Igel, "AMALTHEA—Tailoring tools to projects in automotive software development," *2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS),* Vol.2, pp.515-520, 2015.

[22] Schmittner, Christoph, Zhendong Ma, and Erwin Schoitsch. "Combined safety and security development lifecylce," *2015 IEEE 13th International Conference on Industrial Informatics (INDIN),* pp.1408-1415, 2015.

[23] Sabaliauskaite, Giedre, Sridhar Adepu, and Aditya Mathur, "A six-step model for safety and security analysis of cyber-physical systems," *International Conference on Critical Information Infrastructures Security*, pp.189-200, 2016.

[24] Pricop, Emil, Sanda Florentina Mihalache, and Jaouhar Fattahi, "Innovative fuzzy approach on analyzing industrial control systems security," *Recent Advances in Systems Safety and Security*, pp.223-239, 2016.

[25] M. Brunner, M. Huber, C. Sauerwein, and R. Breu, "Towards an integrated model for safety and security requirements of cyber-physical systems," *2017 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C),* pp.334-340, 2017.

[26] Y. Zhang, P. Shi, C. Dong, Y. Liu, X. Shao, and C. Ma, "Test and Evaluation System for Automotive Cybersecurity," *2018 IEEE International Conference on Computational Science and Engineering (CSE)*, pp.201-207, 2018.

[27] S. Yi, H. Wang, Y. Ma, F. Xie, P. Zhang, and L. Di, "A safety-security assessment approach for communication-based train control (cbtc) systems based on the extended fault tree," *2018 27th International Conference on Computer Communication and Networks (ICCCN),* pp.1-5, 2018.

[28] H. Abdo, M. Kaouk, J. M. Flaus, and F. Masse, "A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie– combining new version of attack tree with bowtie analysis," *Computers & Security*, Vol.72, pp.175-195, 2018.

[29] Skoglund, Martin, Fredrik Warg, and Behrooz Sangchoolie, "In Search of Synergies in a Multi-concern Development Lifecycle: Safety and Cybersecurity," *International Conference on Computer Safety, Reliability, and Security*, pp.302-313, 2018.

[30] T. Chowdhury, E. Lesiuta, K. Rikley, C. W. Lin, E. Kang, B. Kim, ... and A. Wassyng, "Safe and secure automotive over-the-air updates," *International Conference on Computer Safety, Reliability, and Security*, pp.172-187, 2018.

[31] F. Asplund, J. McDermid, R. Oates, and J. Roberts, "Rapid Integration of CPS Security and Safety," *IEEE Embedded Systems Letters*, Vo.11, No.4, pp.111-114, 2018.

[32] Lisova, Elena, Irfan Šljivo, and Aida Čaušević, "Safety and security co-analyses: A systematic literature review," *IEEE Systems Journal*, Vol.13, No.3, pp.2189-2200, 2018.

[33] Geismann, Johannes, Christopher Gerking, and Eric Bodden, "Towards ensuring security by design in cyber-physical systems engineering processes," *Proceedings of the 2018 International Conference on Software and System Process*, pp.123-127, 2018.

[34] K. Huang, C. Zhou, Y. C. Tian, S. Yang, and Y. Qin, "Assessing the physical impact of cyberattacks on industrial cyber-physical systems," *IEEE Transactions on Industrial Electronics*, Vol.65, No.10, pp.8153-8162, 2018.

[35] D. S. Fowler, J. Bryans, M. Cheah, P. Wooderson, and S. A. Shaikh, "A Method for Constructing Automotive Cybersecurity Tests, a CAN Fuzz Testing Example," *2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C),* pp.1-8, 2019.

[36] Oka, Dennis Kengo, Tommi Makila, and Rikke Kuipers, "Integrating Application Security Testing Tools into ALM Tools in the Automotive Industry," *2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C),* pp.42-45, 2019.

[37] S. Verma, T. Gruber, C. Schmittner, and P. Puschner, "Combined Approach for Safety and Security," *International Conference on Computer Safety, Reliability, and Security*, pp.87-101, 2019.

[38] Apvrille, Ludovic, and Letitia W. Li, "Harmonizing safety, security and performance requirements in embedded systems," *2019 Design, Automation & Test in Europe Conference & Exhibition (DATE),* pp.1631-1636, 2019.

[39] J. Dobaj, C. Schmittner, M. Krisper, and G. Macher, "Towards Integrated Quantitative Security and Safety Risk Assessment," *International Conference on Computer Safety, Reliability, and Security,* pp.102-116, 2019.

[40] M. Koschuch, W. Sebron, Z. Szalay, Á. Török, H. Tschiürtz, and I. Wahl, "Safety & Security in the Context of Autonomous Driving," *2019 IEEE International Conference on Connected Vehicles and Expo (ICCVE),* pp.1-7, 2019.

[41] R. Bramberger, H. Martin, B. Gallina, and C. Schmittner, "Co-engineering of Safety and Security Life Cycles for Engineering of Automotive Systems," *ACM SIGAda Ada Letters*, Vol.39, No.2, pp.41-48, 2020.

[42] B. De Win, R. Scandariato, K. Buyens, J. Grégoire, and W. Joosen, "On the secure software development process: CLASP, SDL and Touchpoints compared," *Information and software technology*, Vol.51, No.7, pp.1152-1171, 2009.

[43] Microsoft, "Security Development Lifecycle - SDL Process Guidance," Ver.5.2, 2012.

[44] United States Congress, "NIST SP 800-64 - Security Considerations in the System Development Life Cycle", Rev.2, 2019.

[45] OWASP, Comprehensive, lightweight application security process [Internet], http://www.owasp.org, 2006.

[46] SAE Vehicle Electrical System Security Committee, "Sae j3061-cybersecurity guidebook for cyber-physical automotive systems," SAE-Society of Automotive Engineers, 2016.

[47] Schmittner, Christoph, and Georg Macher, "Automotive Cybersecurity Standards-Relation and Overview," *International Conference on Computer Safety, Reliability, and Security*, pp.153-165, 2019.

[48] UNECE, "Draft Cyber Security Regulation," final clean version, 2020.

[49] H. Hunjan, "ISO/SAE 21434 Automotive Cyber-Security Engineering," *Presentation, Renessas Electronics LTD*, 2018.

[50] Blyler, John, "Software-Hardware Integration in Automotive Product Development," SAE, pp.i-v, 2014.

[51] LDRA, "Build Security Into The Connected Car Development Life Cycle" [Internet], https://ldra.com/buildsecurity-connected-car-development-life-cycle/?fbclid=IwAR01liF34G0QMtisIVoazTFlDZR2GhVCXOFtg1BkGr7_U9RNwgCfRG02kko, 2017.

[52] E. Schoitsch, C. Schmittner, Z. Ma, and T. Gruber, "The need for safety and cyber-security co-engineering and standardization for highly automated automotive vehicles," *Advanced Microsystems for Automotive Applications 2015,* pp.251-261, 2016.

[53] Sabaliauskaite, Giedre, and Aditya P. Mathur, "Aligning cyber-physical system safety and security," *Complex Systems Design & Management Asia*, pp.41-53, 2015.

[54] Synopsys, What is ASIL? [Internet], https://www.synopsys.com/automotive/what-is-asil.html

[55] Schmittner, Christoph, and Zhendong Ma, "Towards a framework for alignment between automotive safety and security standards," *International Conference on Computer Safety, Reliability, and Security*, pp.133-143, 2014.

[56] Miller, Joseph D, "Automotive System Safety: Critical Considerations for Engineering and Effective Management," *John Wiley & Sons*, 2019.

[57] Mellado, Daniel, Eduardo Fernández-Medina, and Mario Piattini, "A common criteria based security requirements engineering process for the development of secure information systems," *Computer Standards & Interfaces,* Vol.29, No.2, pp.244-253, 2007.

[58] Yin, Lei, and Fang-Liang Qiu, "A novel method of security requirements development integrated common criteria," *2010 International Conference On Computer Design and Applications*, Vol.5, pp.V5-531, 2010.

[59] D. Mellado, C. Blanco, L. E. Sánchez, and E. Fernández-Medina, "A systematic review of security requirements engineering," *Computer Standards & Interfaces,* Vol.32, No.4, pp.153-165, 2010.

[60] S. H. Houmb, S. Islam, E. Knauss, J. Jürjens, and K. Schneider, "Eliciting security requirements and tracing them to design: An integration of Common Criteria, heuristics, and UMLsec," *Requirements Engineering,* Vol.15, No.1 pp.63-93, 2010.

[61] Mesquida, Antoni Lluís, and Antonia Mas, "Implementing information security best practices on software lifecycle processes: The ISO/IEC 15504 Security Extension," *Computers & Security*, Vol.48, pp.19-34, 2015.

[62] H. Li, X. Li, J. Hao, G. Xu, Z. Feng, and X. Xie, "Fesr: A framework for eliciting security requirements based on integration of common criteria and weakness detection formal model," *2017 IEEE International Conference on Software Quality, Reliability and Security (QRS)*, pp.352-363, 2017.

[63] Barafort, Béatrix, Antoni-Lluís Mesquida, and Antonia Mas, "Integrating risk management in IT settings from ISO standards and management systems perspectives," *Computer Standards & Interfaces,* Vol.54, pp.176-185, 2017.

[64] Barafort, Béatrix, Antoni-Lluís Mesquida, and Antònia Mas, "Integrated risk management process assessment model for IT organizations based on ISO 31000 in an ISO multistandards context," *Computer Standards & Interfaces,* Vol.60, pp.57-66, 2018.

[65] Lee, Younghwa, Jintae Lee, and Zoonky Lee, "Integrating software lifecycle process standards with security engineering," *Computers & Security,* Vol.21, No.4, pp.345-355, 2002.

[66] D. Horie, T. Kasahara, Y. Goto, and J. Cheng, "A new model of software life cycle processes for consistent design, development, management, and maintenance of secure information systems,"*2009 Eighth IEEE/ACIS International Conference on Computer and Information Science*, pp.897-902, 2009.

[67] Amara, Naseer, Zhiqui Huang, and Awais Ali, "Modelling Security Requirements for Software Development with Common Criteria," *International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage,* pp.78-88, 2019.

[68] MISRA, C, MISRA C [Internet], https://www.misra.org.uk/

정 승 연

https://orcid.org/0000-0001-8040-2859
e-mail : sodon513@gmail.com
2019년 고려대학교 컴퓨터학과(학사)
2019년 ~ 현 재 고려대학교 자동차융합학과 석사과정
관심분야 : 보안개발생명주기, 자동차 개발

강 수 영

https://orcid.org/0000-0002-4040-9383
e-mail : bbang814@gmail.com
2006년 순천향대학교 컴퓨터공학부(학사)
2008년 순천향대학교 컴퓨터공학부(석사)
2008년 ~ 2010년 한국인터넷진흥원(KISA) 연구원
2010년 ~ 2014년 안랩(Ahnlab) 주임연구원
2013년 ~ 현 재 고려대학교 정보보호대학원 박사과정
관심분야 : 보안개발생명주기, 위협 모델링, 보안성 평가/인증

김 승 주

https://orcid.org/0000-0002-2157-0403
e-mail : skim71@korea.ac.kr

1994년~1999년 성균관대학교 정보공학과(학사, 석사, 박사)
1998년~2004년 한국인터넷진흥원(KISA) 팀장
2004년~2011년 성균관대학교 정보통신공학부 부교수
2004년~현 재 한국정보보호학회 이사
2007년 국가정보원장 국가사이버안전업무 유공자 표창
2010년 방송통신위원회 정보통신망 침해사고 민관합동조사단 위원
2011년~현 재 고려대학교 사이버국방학과/정보보호대학원 정교수
2012년 선관위 디도스 특별검사팀 자문위원
2014년~2015년 육군사관학교 초빙교수
2014년~2016년 다음카카오 프라이버시 정책 자문위원회 위원
2015년~현 재 방위사업청 방산기술보호 자문관
2016년~2018년 개인정보분쟁조정위원회 위원
2016년~현 재 산업통상자원부 전략물자기술 자문위원
2016년~현 재 한국카카오뱅크 정보보호부문 자문교수
2017년~현 재 고려대학교 국방RMF연구센터(AR2C) 센터장
2018년~2020년 4차산업혁명위원회 위원: 대통령직속 4차산업혁명위원회 위원
2018년~현 재 고신뢰 보안운영체제 연구센터(CHAOS) 센터장
2020년~현 재 합동참모본부 정책자문위원회 자문위원
관심분야 : 보안공학 및 보안내재화 방법론, 보안성 평가/인증, RMF A&A, 암호학 및 블록체인