한국ITS학회논문지 J. Korea Inst. Intell. Transp. Syst.

차량 사이버보안 법규 준수를 위한 프레임워크 개발: Cybersecurity Requirement Finder

Development of Framework for Compliance with Vehicle Cybersecurity Regulations: Cybersecurity Requirement Finder

오 준 희* · 송 윤 근** · 박 경 록*** · 권 혁**** · 우 사 무 엘*****

* 주저자 : 단국대학교 컴퓨터학과 석사과정
** 공저자 : 단국대학교 컴퓨터학과 박사과정
*** 공저자 : 단국대학교 컴퓨터학과 석사과정
**** 공저자 : 한국인터넷진흥원 책임연구원
***** 교신저자 : 단국대학교 소프트웨어학과 교수

Jun hee Oh* · Yun keun Song** · Kyung rok Park*** · Hyuk Kwon**** · Samuel Woo*****

* Dept. of Conputer Science, Univ. of Dankook
** Dept. of Conputer Science, Univ. of Dankook
*** Dept. of Conputer Science, Univ. of Dankook
**** Korea Internet & Security Agency (KISA)
***** Dept. of Software, Univ. of Dankook

† Corresponding author : Samuel Woo, samuelwoo@dankook.ac.kr

Vol. 22 No.6(2023)
December, 2023
pp.299~312

pISSN 1738-0774
eISSN 2384-1729
https://doi.org/10.12815/kits.2023.22.6.299

Received 18 September 2023
Revised 6 October 2023
Accepted 6 November 2023

요 약

최근 ECU(Electronic Control Unit)는 단순한 편의 기능을 넘어 여러 기능이 하나로 통합되고 있다. 이에 따라 ECU는 이전보다 더 많은 기능과 외부 인터페이스를 갖게 되었고, 다양한 사이버 보안 문제가 발생하고 있다. UNECE(United Nations Economic Commission for Europe) WP. 29는 증가하는 차량 사이버보안에 대한 위협을 고려해 UN Regulation No.155를 발표하여 차량 사이버 보안 관리 체계에 대한 국제 기준을 마련했다. 국제 기준에 따르면 차량 제조업체는 2022년 7월부터 CSMS(Cybersecurity Management System)를 구축하고, VTA(Vehicle Type Approval)를 받아야 한다. 그러나 국내에서는 이에 대한 준비가 미흡해 시행 시기를 조정해야 한다는 의견이 제기되었다. 따라서 본 논문에서는 요구사항의 CSMS 현황을 확인하기 위한 체크리스트와 식별된 갭(Gap)을 완화하기 위한 다양한 차량 보안 솔루션을 매핑 시켜주는 웹 기반의 솔루션을 제안한다.

핵심어 : 차량 사이버보안, 사이버보안 관리 체계, 사이버보안 요구사항, UN Regulation No.155, ISO/SAE 21434

ABSTRACT

Recently, the electronic control unit (ECU) has been integrating several functions into one beyond simple convenience functions. Accordingly, ECUs have more functions and external interfaces than before, and various cybersecurity problems are arising. The United Nations Economic Commission for Europe (UNECE) World Forum for Harmonization of Vehicle Regulations (WP.29) issued UN

Regulation No.155 to establish international standards for vehicle cybersecurity management systems in light of the growing threats to vehicle cybersecurity. According to international standards, vehicle manufacturers are required to establish a Cybersecurity Management System (CSMS) and receive a Vehicle Type Approval (VTA). However, opinions were raised that the implementation period should be adjusted because domestic preparations for this are insufficient. Therefore, in this paper, we propose a web-based solution that maps a checklist to check the status of CSMS in the requirement and various vehicle security companies and solutions to mitigate the identified gap.

Key words : Vehicle Cybersecurity, Cybersecurity Management System, Cybersecurity Requirement, UN Regulation No.155, ISO/SAE 21434

Ⅰ. 서 론

1. 연구 배경

차량에는 수많은 ECU[1]가 탑재되어 있으며, CAN[2]을 통해 연결되어 있다. 차량과 스마트 기기를 연결하는 커넥티비티(Connectivity) 기능이나 자율주행과 같은 편의 기능에 비중을 두었던 예전의 ECU에 비해 오늘날은 단순한 편의 기능을 넘어 여러 기능이 하나로 통합되는 추세이다. 이는 ECU가 예전보다 더 많은 기능과 외부 인터페이스를 가지게 된다는 것을 의미하며, 차량 해킹과 같은 사이버보안 문제를 발생시키기도 한다. 실제로 국내외에서 차량 해킹 사례가 계속해서 보고되고 있는데, 차량의 액셀(Accelerator), 핸들(Steering Wheel), 브레이크(Brake) 등과 관련된 기능을 비활성화하거나 마음대로 조작하는 것이 가능하다. 다양한 유형의 사이버 공격이 등장하고 있으며, 차량의 사이버 공격 및 취약점은 심각한 인명 사고 및 리콜 사태로 이어질 수 있으므로 차량 사이버보안에 대한 중요성이 높아지고 있다. <Table 1>은 CVE[3]에서 제공하고 있는 연도별 사이버보안 사고 수와 차량 사이버보안에 관련된 위협의 수를 보여준다(EE Times, 2023). 구체적인 차량 사이버보안 위협에 관한 내용은 CVE 홈페이지에서 제공하고 있다.

<Table 1> Automotive Cybersecurity Trends

Note	2010-2015	2016	2017	2018	2019	2020	2021
Incidents per year	12	24	52	80	160	410	485
Yearly new CVEs	n/a	n/a	n/a	n/a	24	33	139
Cumulative CVEs	n/a	n/a	n/a	53	77	110	249

2. 연구 목적

UNECE[4]의 산하 국제 자동차 기준 조화 회의체인 WP. 29에서는 증가하고 있는 차량 사이버보안 위협을 고려해 2020년 6월 UN Regulation No.155를 발표하여 차량 사이버보안 관리 체계에 관한 국제 기준을 마련

1) ECU: Electronic Control Unit
2) CAN: Controller Area Network
3) CVE: Common Vulnerabilities and Exposures
4) UNECE: United Nations Economic Commission for Europe

했다(Boannews, 2023a). 국제 기준에 따르면 차량 제조업체는 CSMS[5]를 구축하고 VTA[6]를 받아야 하며(Dong Sung Im, 2022), 새롭게 출시되는 차량에 대해서는 2022년 7월부터, 기존 차량에 대해서는 2024년 7월까지 VTA를 받아야 한다(Boannews, 2023b). 만약 CSMS 구축을 위한 요구사항을 준수하지 못할 경우, 차량 제조업체는 UNECE에 가입되어 있는 국가 내에서 차량을 판매할 수 없게 된다(Korea Internet & Security Agency, 2023a). 그러나 모든 국가가 국제 기준을 따르고 있는 것은 아니다. 유럽의 경우에는 형식 승인 제도를 운영하고 있으며, 북미의 경우에는 사이버보안 관리 체계 인증에 관한 국제 기준을 적용하고는 있지만, 자기 인증 제도를 운영하고 있으므로 사이버보안 관리 체계에 대한 가이드라인만 제시하고 있다. 한국은 국제 기준을 국내 실정에 맞추어 도입하기 위해 2023년 4월 제204회 국회 제1차 국토교통위원회를 통해서 사이버보안 관리 체계 인증 도입과 관련된 자동차관리법 개정안을 발의했다(Land Infrastructure and Transport Committee, 2023). 발의된 개정안에 의하면 사이버보안 관리 체계 구축을 위한 준비 및 차량 제조업체의 상황과 대응 등을 종합 고려하여 시행 시기를 신차의 경우에는 2025년 1월부터 적용하고, 기존 차의 경우에는 2026년 7월부터로 조정해야 한다는 의견이 제기되었다(Land Infrastructure and Transport Committee, 2023). 국내에서는 이처럼 개정안이 발의됨에 따라 차량 사이버보안 관리 체계가 필수가 되었다. UN Regulation No.155에서는 CSMS를 구축하기 위한 요구사항을 나열하고 있지만 체계적으로 적용하는 방법에 대해서는 정의하고 있지 않다. 때문에 CSMS를 처음 준비하는 기업의 보안 담당자는 방대한 양의 요구사항을 파악하기에 어려움이 있으며 VTA를 위해 제출해야 하는 WP[7]는 여러 사람이 작성하기 때문에 사람에 따라서 다르게 작성될 수 있다. 따라서 CSMS를 구축하고, 인증을 취득하기 위해 참고할 수 있는 구체적인 가이드라인과 솔루션이 필요하며 WP에 필수적으로 작성되어야 하는 내용이 모두 작성되었는지 점검해 볼 수 있도록 하는 방법이 필요하다.

이에 본 논문에서는 WP에 필수적으로 들어가야 하는 내용을 스스로 확인할 수 있도록 하는 체크리스트와 손쉬운 접근법을 제공하기 위한 웹 기반의 프로그램을 제안한다. ISO/SAE 21434는 총 15개의 챕터로 구성되어 있으며, 각 챕터별로 요구사항과 WP가 명시되어 있다. 각 챕터별로 3~31개의 요구사항이 나열되어 있으며, 총 42개의 WP가 명시되어 있다(ISO/SAE, 2021). 본 논문에서는 CSMS를 처음 준비하는 기업의 보안담당자가 42개의 WP에 필수적으로 작성해야 하는 내용을 스스로 확인할 수 있도록 하는 체크리스트를 제안한다. 또한 현재 차량 업계에서는 자사의 CSMS 현황을 확인할 때 표준 문서를 통해 직접 CSMS 요구사항을 확인하거나 엑셀(Excel) 프로그램을 통해 정리하는 방법을 사용하고 있다. 따라서 본 논문에서는 손쉬운 접근법을 제공하기 위한 웹 기반의 솔루션을 제안한다.

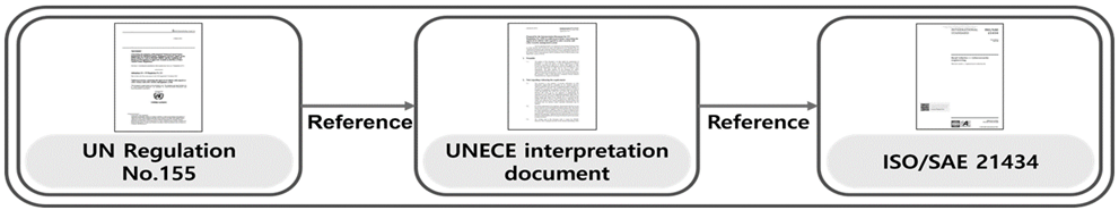
Ⅱ. 본 론

1. UN Regulation No.155와 ISO/SAE 21434의 상관관계 분석

UN Regulation No.155는 차량 라이프사이클 전반에 걸쳐 사이버보안을 보장하기 위한 요구사항을 포함하고 있다(UNECE WP.29, 2021). ISO/SAE 21434는 차량 라이프사이클 전반에 걸쳐 사이버보안 활동에 관한 프로세스를 정의하는 것을 목적으로 하는 국제 표준이다(ISO/SAE, 2021). UN Regulation No.155에 대한 해설서에 의하면 ISO/SAE 21434는 UN Regulation No.155의 요구사항을 준수하기 위한 활동들을 구체적으로 명시하

5) CSMS: Cybersecurity Management System
6) VTA: Vehicle Type Approval
7) WP: Work Product

고 있으며, UN Regulation No.155의 요구사항을 준수했다는 증거로 ISO/SAE 21434의 WP를 활용하도록 권장하고 있다(UNECE WP29, 2020). 따라서 UN Regulation No.155의 요구사항은 ISO/SAE 21434의 요구사항과 매핑될 수 있으며, 차량 사이버보안 법규 준수를 위한 프레임워크를 개발하기 위해서는 먼저 두 개의 표준 문서 간의 상관관계를 분석해야 한다(Korea Internet & Security Agency, 2022). <Fig. 1>은 사이버보안 관리 체계에 관련된 표준 문서 간의 상관관계에 대한 그림이다.



<Fig. 1> Correlation between standard documents

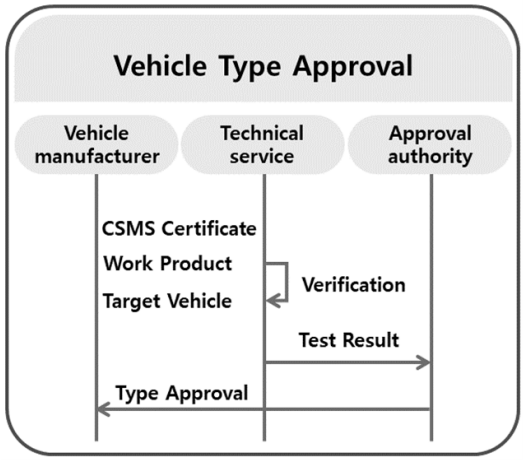
UN Regulation No.155의 요구사항은 7.2.2.1.부터 7.2.2.5.까지 있으며 각 요구사항에서 수행해야 하는 활동으로 항목을 분류한다. Requirement No. 7.3부터는 차량 형식 승인에 대한 요구사항으로 승인기관 및 기술 서비스 기관에 해당하는 내용이기 때문에 ISO/SAE 21434의 범위를 벗어난다. 따라서 본 논문에서는 Requirement No. 7.2.2.1부터 7.2.2.5에 해당하는 요구사항에 대해서만 분석한다. Requirement No. 7.2.2.1부터 7.2.2.5까지의 요구사항 개수는 총 15개이며 각각의 요구사항은 부록의 <Table A1>의 Type과 같이 12개의 활동들로 나눌 수 있다. ISO/SAE 21434에서는 필수적으로 적용되어야 하는 요구사항에 대해서 RQ(Requirement)로 표기하고 있다. 따라서 본 논문에서는 RQ로 표기된 요구사항에 대해서만 분석하며, UN Regulation No.155의 12개의 활동과 요구사항을 매핑한다. <Table A1>의 ISO/SAE 21434 Requirement No.는 UN Regulation No.155의 요구사항을 준수하기 위한 구체적인 활동들을 매핑한 내용이며, ISO/SAE 21434에서 표기하고 있는 Requirement No.를 나타낸다.

2. 체크리스트 작성

차량 제조업체는 CSMS 인증을 취득한 후 VTA를 신청할 수 있다. 또한 VTA를 위해 CSMS 인증서를 제출한 차량 제조업체는 사이버보안 활동에 관한 결과를 문서로 남겨야 하며, 문서로 만들어진 자료는 형식승인 기관 및 기술 서비스 기관에 제출한다. 이러한 자료는 ISO/SAE 21434에 명시된 WP를 의미한다. <Fig. 2>는 VTA에 대한 전체적인 구조에 대한 그림이다.

모든 WP는 한 사람이 작성하는 것이 아니라 여러 사람이 나누어 작성하기도 하며, 작성하는 사람마다 다른 퀄리티로 작성되는 문제가 발생할 수 있다. 또한 WP를 처음 작성하는 사람은 VTA를 위해 WP에 필수적으로 들어가야 하는 항목이 무엇인지 판단하기 어렵다. 따라서 UN Regulation No.155와 ISO/SAE 21434의 상관관계를 파악한 후에는 WP의 일정한 퀄리티 유지와 필수로 들어가야 하는 항목을 스스로 점검할 수 있도록 하는 체크리스트를 도출한다. 자동차 산업에서 OEM을 대표하는 캐나다 협회인 APMA Cybersecurity Committee에서는 ISO/SAE 21434의 WP에 대한 체크리스트를 제공하고 있다(APMA cybersecurity committee, 2021). 그러나 APMA Cybersecurity Committee의 체크리스트는 2021년 3월 ISO/SAE 21434의 WP에 대해 작성된 것으로 ISO/SAE 21434의 Draft 버전에 관한 내용이다(SAE, 2020). 따라서 본 논문에서는 APMA Cybersecurity Committee의 체크리스트에 ISO/SAE 21434:2021을 기준으로 내용을 추가해 체크리스트를 작성

한다. 부록의 <Table A2>는 개발 단계(Development Phase) 활동에 관한 체크리스트를 나타낸다. UN Regulation No.155의 요구사항 중 7.2.2.1.(a)는 개발 단계 활동에 관한 내용이다. 이러한 개발 단계 활동에서 작성되어야 하는 WP 항목은 매핑되는 ISO/SAE 21434 요구사항을 통해 알 수 있다. CSMS 인증을 준비하면서 작성되어야 하는 WP는 총 42개이며 개발 단계에서 작성되어야 하는 WP는 21개이다.



<Fig. 2> VTA Procedure for UNR No. 155

3. 차량 보안 솔루션 매핑

차량 제조업체가 체크리스트를 통해 체크한 후에는 부족한 부분에 대한 도움을 받아 CSMS를 구축하고, VTA 인증을 취득할 수 있도록 차량 보안 솔루션을 매핑한다. 매핑한 차량 보안 솔루션은 한국 인터넷진흥원에서 제공하고 있는 차량 보안 솔루션 맵(Vehicle Security Solution Map)이다. 한국인터넷진흥원에서 제공하고 있는 차량 보안 솔루션 맵에 의하면 차량 보안 솔루션은 크게 차량 보안 솔루션(Vehicle Security Solution), 백엔드 보안 솔루션(Back-end Security Solution), 사이버보안 관리 체계(Cybersecurity Management System)에 대한 범주로 나눌 수 있다. 차량 보안 솔루션은 8가지의 솔루션으로 구성되어 있으며, 백엔드 보안 솔루션은 2가지의 솔루션, 사이버보안 관리 체계는 3가지의 솔루션으로 구성되어 있다(Korea Internet & Security Agency, 2023b). 각각의 솔루션은 <Table A1>의 12개의 활동과 매핑할 수 있다.

차량 보안 솔루션 범주는 <Table 2>와 같이 8개의 범주로 구성되며, <Table A1>의 12개의 활동 중 '위험 평가 최신 상태로 유지 확인', '하위 조직과의 종속성', '테스트를 포함한 위험 관리 확인', '사이버보안 위험 식별 및 관리' 활동과 매핑된다. 백엔드 보안 솔루션 범주는 <Table 3>와 같이 2개의 솔루션으로 구성되며, <Table A1>의 12개의 활동 중 '테스트를 포함한 위험 관리 확인', '위험 평가 최신 상태로 유지 확인', '사이버보안 공격 모니터링 및 대응' 활동과 매핑된다. 사이버보안 관리 체계 솔루션 범주는 <Table 4>와 같이 3개의 솔루션으로 구성되며, <Table A1>의 12개의 모든 활동과 매핑된다.

예를 들어 차량 보안 솔루션 맵에서 사이버보안 관리 시스템 범주에 속해있는 TARA 솔루션은 <Table A1>의 12개의 활동 중 개발 단계에 매핑된다. 따라서 개발 단계의 체크리스트를 수행한 결과에서 부족한 부분이 있다면 개발 단계와 매핑되는 사이버보안 관리 시스템의 TARA 솔루션 목록을 보여준다. <Fig. A1>은 각각의 보안 솔루션 범주를 <Table A1>의 Type과 매핑한 그림이다.

<Table 2> Types of Vehicle Security

No.	Vehicle Security Solution
1	OTA Update
2	SBOM
3	Security Testing
4	HSM
5	V2X
6	Keyless entry
7	IDS/IDPS
8	Cryptography Library

<Table 3> Types of Back-end Security

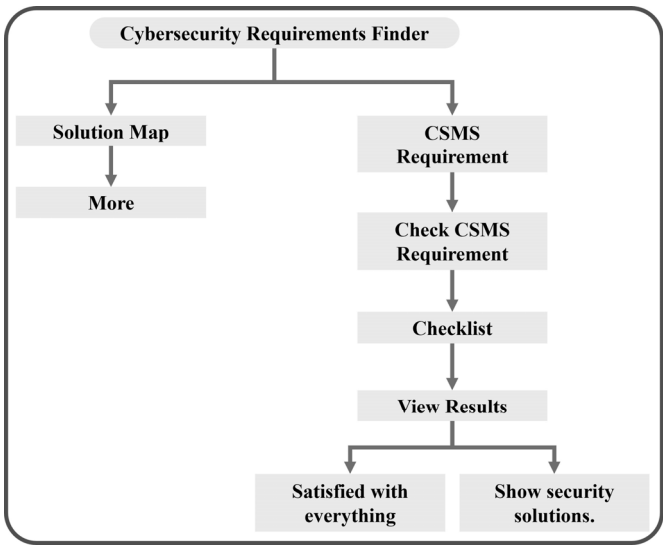
No.	Back-end Security Solution
1	V2X-CSMS
2	V-SOC

<Table 4> Types of Caybersecurity Management System

No.	Cybersecurity Management System
1	Security Consulting
2	TARA
3	Security Training

4. 차량 보안 솔루션 맵

차량 제조업체 및 CSMS를 처음 준비하는 기업의 보안담당자가 CSMS 요구사항을 쉽게 확인하고, VTA를 준비할 수 있도록 하기 위해 앞서 설명한 기능을 포함하는 웹 기반의 솔루션을 개발했다. 프로그램의 이름은 Cybersecurity Requirement Finder로 정의했으며, CSS와 JavaScript를 사용하여 개발했다. <Fig. 3>은 제안하는 웹 기반 솔루션의 전체 흐름도에 대한 그림이다.



<Fig. 3> Flowchart for Web-based solutions

프로그램의 사용자는 Cybersecurity Requirement Finder의 홈 화면에서 솔루션 맵(Solution Map)과 사이버보안 관리 시스템 요구사항(CSMS Requirement) 중 한 가지 메뉴를 선택한다. 홈 화면에서 사용자가 차량 보안에 관한 솔루션을 확인하기 위해 좌측 메뉴인 솔루션 맵을 실행하면 한국인터넷진흥원에서 제공하고 있는 차량 사이버보안 솔루션 맵이 화면에 출력된다. 사용자는 화면에 마우스를 올리면 활성화되는 '더 보기(more)' 버튼을 통해 솔루션을 자세히 확인할 수 있다. 솔루션은 차량 보안 솔루션, 백엔드 보안 솔루션, 사이

버보안 관리 시스템으로 분류되어 있으며 차량 보안 업체명과 차량 보안 업체에서 제공하고 있는 솔루션 명을 확인할 수 있다. <Fig. 4>는 좌측 메뉴인 솔루션 맵 실행 시 나타나는 화면이다.

▷ Security Training

- 사이버 해킹 위협으로부터 차량 ECU 및 차량 내부 네트워크를 보호하는 방법에 대한 교육

기업 명	솔루션 명
BSI	• TISO/SAE 21434 차량 사이버보안 이해 및 실무 과정 • ISO/SAE 21434 차량 사이버보안 내부심사원 과정 • ISO/SAE 21434 차량 사이버보안 심사원/선임심사원 교육과정
DNV	• UN regulation, ISO/SAE 21434:2021 기반의 자동차 사이버보안 엔지니어 양성교육 • ISO/SAE 21434:2021 기반의 자동차 사이버보안 내부심사원 양성 교육
ETAS	• Security product design • Automotive security •threat analysis and risk assessment coaching
FESCARO	• 보안 교육
Karamba	• Security Training

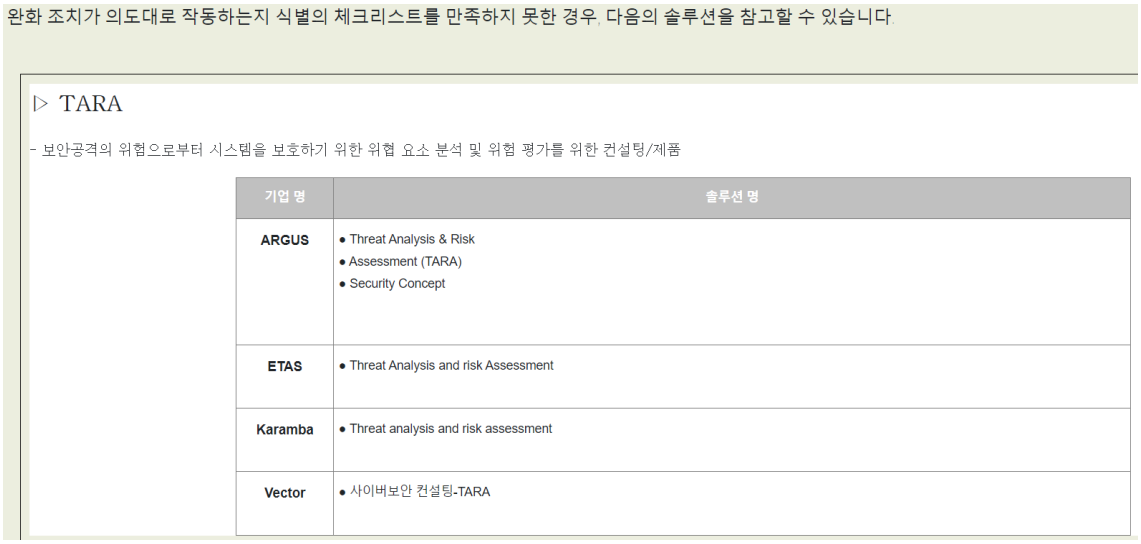
<Fig. 4> Security Solution Map Screen (Learn More)

Cybersecurity Requirement Finder에서 사용자가 CSMS에 대한 요구사항을 모두 만족했는지에 대한 여부를 확인하기 위해 우측 메뉴인 사이버보안 관리 체계 요구사항을 실행하면 CSMS에 대한 UN Regulation No.155의 요구사항과 ISO/SAE 21434의 요구사항이 매핑되어 화면에 출력된다. CSMS 요구사항은 개발, 생산, 생산 후 과정에서 수행해야 하는 활동을 항목별로 확인할 수 있다. 활동은 총 12개의 활동으로 구성되어 있으며, 부록의 <Table A1>에서 작성한 내용과 같다. 사용자가 CSMS 요구사항을 확인한 후 체크리스트를 실행하면 활동별로 CSMS 요구사항을 준수하는지에 대한 여부를 확인하기 위한 체크리스트를 실행할 수 있다. <Fig. 5>은 CSMS 요구사항에 대한 체크리스트 화면이다. 사용자가 체크리스트를 모두 실행한 후 결과 보기를 실행하면 CSMS 요구사항을 모두 만족하는지에 대한 여부를 확인할 수 있다. 결과 확인은 2가지로 구분된다. CSMS 요구사항을 모두 만족할 때는 모든 요구사항을 만족했다는 문구가 화면에 출력되며, 부족한 부분이 있을 때는 참고할 수 있는 보안 솔루션 명과 차량 보안 업체명이 화면에 출력된다. <Fig. 6>은 부족한 부분이 있을 때 나타나는 결과에 대한 그림이다(ITSSL, 2023).

Cybersecurity Interface agreement

- ☐ [1] 조직은 공급업체의 역량을 분석하여 모든 공급업체의 사이버보안 역량을 평가하였는가?
- ☐ [2] 모든 견적 요청에는 공급업체의 사이버보안 책임에 대한 기대가 포함되어 있는가?
- ☐ [3] 조직의 모든 공급업체와 사이버보안 인터페이스 계약을 이행하고 있는가?
- ☐ [4] 사이버보안 인터페이스 계약에는 고객과 공급업체의 역할과 책임이 모두 포함되어 있는가?
- ☐ [5] 고객과 공급업체 간의 사이버보안 역할과 책임을 확실하게 전달하기 위한 커뮤니케이션 계획이 있는가?

<Fig. 5> Checklist screen



<Fig. 6> Checklist Results screen

본 논문에서 제안하는 웹 기반 솔루션의 효과성을 검증하기 위해 가상의 회사가 있다고 가정한다. CSMS를 준비하고 있는 A사는 글로벌 자동차부품 업체이며, B사는 국외로 차량을 수출하는 글로벌 OEM이다.

<Table 5> Company A's information

Company A (Global Automotive parts manufacturer)	
company size	less than 100 people
Cybersecurity Department	Yes
Incident Response Department	No
production facilities	Yes
Acquisition of certification	ISO 27001

<Table 6> Company B's information

Company B (Global OEM)	
company size	More than 100 people
Cybersecurity Department	Yes
Incident Response Department	Yes
production facilities	Yes
Acquisition of certification	ISO 27001 ISO 26262 IATF 16949 A-SPICE

A사는 CSMS 인증을 받기 전 자사의 CSMS가 인증 기준에 부합하는지에 대한 여부를 확인하려고 한다. A사의 CSMS 담당자는 Cybersecurity Requirement Finder에 접속한 후 사이버보안 관리 체계 요구사항 메뉴를 클릭했다. A사의 CSMS 담당자는 UN Regulation No.155의 12개의 활동에 대한 질문사항을 모두 확인한 후 결과보기를 클릭했다. A사는 침해사고 대응에 관한 부서가 없으므로 '사이버보안 공격 모니터링 및 대응'에 관한 질문사항에서 부족한 부분이 발견되었다. 따라서 차량 수명 주기 전반에 걸쳐 사이버 공격을 모니터링 및 분석하고, 효과적으로 대응할 수 있도록 하는 백엔드 보안 솔루션인 V-SOC에 관련된 보안 업체명과 보안 솔루션 명이 결과 화면에 나타났다. A사는 결과 화면에 있는 V-SOC에 관한 솔루션을 통해 부족한 부분에 대한 도움을 받기로 했다.

B사는 국외로 차량을 수출하는 글로벌 OEM이다. 따라서 국제 기준을 만족하기 위해 CSMS를 취득하려고 한다. B사의 CSMS 담당자는 자사의 CSMS가 국제 기준에 만족하는지에 대한 여부를 확인하려고 한다. B사

의 CSMS 담당자는 Cybersecurity Requirement Finder에 접속한 후 사이버보안 관리 체계 요구사항 메뉴를 클릭했다. B사의 CSMS 담당자는 UN Regulation No.155의 12개의 활동에 대한 질문사항을 모두 확인한 후 결과보기를 클릭했다. B사는 사이버보안 부서와 침해사고 대응에 관한 부서를 통해 차량 사이버 공격 및 취약점에 대해 대비를 하고 있었다. 따라서 모든 질문사항을 만족했으며, 모든 요구사항을 만족했다는 문구가 결과 화면에 나타난다.

Ⅲ. 결 론

현재 국내에서는 2021년 1월부터 UN Regulation No.155가 발효되었음에도 CSMS에 대한 준비가 미흡한 상황이며, 자동차관리법에 적합한 방식으로 CSMS를 도입하기 위한 준비를 하고 있다. CSMS를 구축하기 위해서는 UN Regulation No.155의 요구사항을 따라야 한다. UN Regulation No.155에서는 CSMS를 구축하기 위한 요구사항을 나열하고 있지만 체계적으로 적용하는 방법에 대해서는 정의하고 있지 않다. 또한 VTA를 위해 제출해야 하는 WP는 여러 사람이 나누어 작성하기 때문에 작성하는 사람에 따라서 다르게 작성된다는 문제가 있으며, CSMS를 처음 준비하는 기업의 보안담당자의 관점에서 보았을 때 방대한 양의 요구사항을 모두 파악하고, WP를 준비하기에 어려움이 있다고 판단된다. 이에 본 논문에서는 UN Regulation No.155와 ISO/SAE 21434에서 CSMS와 관련된 요구사항을 매핑하고 상관관계를 분석했다. 이 과정을 통해 차량 제조업체가 VTA를 위해 제출해야 하는 WP의 목록을 파악할 수 있었고, WP를 작성할 때 필수적으로 작성해야 하는 내용을 점검할 수 있도록 하는 체크리스트를 도출 했다. 체크리스트를 도출하는 과정에서 ISO/SAE 21434의 Draft 버전에 관한 내용으로 작성된 APMA Cybersecurity Committee의 체크리스트를 참고했으며, ISO/SAE 21434:2021 버전에 관한 내용으로 질문사항을 추가하는 작업이 필요했다. 이러한 기능을 모두 포함하는 웹 기반의 솔루션을 제안했으며, 사용자가 체크리스트를 통해 부족한 부분을 확인하고, 부족한 부분에 대해 국내 차량 보안기업에서 제공하는 솔루션을 받을 수 있도록 하는 기능을 추가했다. 차량 제조업체는 웹 기반 솔루션을 참고해 CSMS 요구사항과 VTA를 위해 제출해야 하는 WP를 효과적으로 확인할 수 있을 것으로 기대된다. 또한 CSMS를 처음 접하는 모든 기업의 보안담당자가 이 웹 기반의 솔루션을 통해 UN Regulation No.155와 ISO/SAE 21434의 상관관계를 쉽게 이해하고, CSMS를 준비할 수 있을 것으로 예상된다.

ACKNOWLEDGEMENTS

본 연구는 산업통상자원부 한국산업기술평가관리원(KEIT) 자율주행기술개발혁신사업 “자율주행 시스템의 내부 네트워크 및 무선 소프트웨어 업데이트 보안 평가기술 개발” 과제(과제번호: 20022229)의 지원을 받아 수행되었습니다.

본 연구는 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(No.2022-0-01022, 이벤트 기반 실험시스템 구축을 통한 자동차 내·외부 아티팩트 수집 및 통합 분석 기술 개발)

REFERENCES

APMA(Automotive Parts Manufacturers Association) Cybersecurity Committee(2021), *Apma Cyberkit ISO 21434*.

Boannews(2023a), https://m.boannews.com/html/detail.html?idx=94054, 2023.09.08.

Boannews(2023b), https://m.boannews.com/html/detail.html?idx=94213, 2023.09.04.

EE(Electronic Engineering) Times, https://www.eetimes.com/automotive-cybersecurity-more-than-in-vehicle-and-cloud/, 2023.09.04.

Im, D. S.(2022), "An Analysis of the Relative Importance of Security Level Check Items for Autonomous Vehicle Security Threat Response", *The Journal of the Korea Institute of Intelligent Transportation Systems*, vol. 21, no. 4, pp.145-156.

ISO/SAE(2021), *ISO/SAE 21434:2021, Road vehicles-Cybersecurity engineering*.

ITSSL(Intelligent Transport Systems security Lab)(n.d.), *Cybersecurity Requirements Finder*, http://43.201.15.38/, 2023.09.04.

Korea Internet & Security Agency(2022), *Self-driving car security model Part 2: CSMS*.

Korea Internet & Security Agency(2023a), *An Explanation and Application of Security Model for Autonomous Vehicles*.

Korea Internet & Security Agency(2023b), https://www.kisa.or.kr/2060205/form?postSeq=18&page=1, 2023.09.04.

Land Infrastructure and Transport Committee(2023), *Report on the review of partial amendments to the Automobile Management Act*.

SAE(Society of Automotive Engineers)(2020), https://www.sae.org/standards/content/iso/sae21434.d1/, 2023.09.04.

Song, Y. K., Woo, S., Lee, J. and Lee, Y. S.(2019), "Deriving Essential Security Requirements of IVN through Case Analysis", *The Journal of the Korea Institute of Intelligent Transport Systems*, vol. 18, no. 2, pp.144-155.

UNECE WP(United Nations Economic Commission for Europe Working Party).29.(2021), *UN Regulation No.155-Cyber Security and Cyber Security Management System*.

UNECE WP(United Nations Economic Commission for Europe Working Party)29.(2020), *Proposal for the Interpretation Document for UN Regulation No. [155] on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system*.

UPSTREAM(2023), *Upstream 2023 Global Automotive Cybersecurity Report*.

APPENDIX

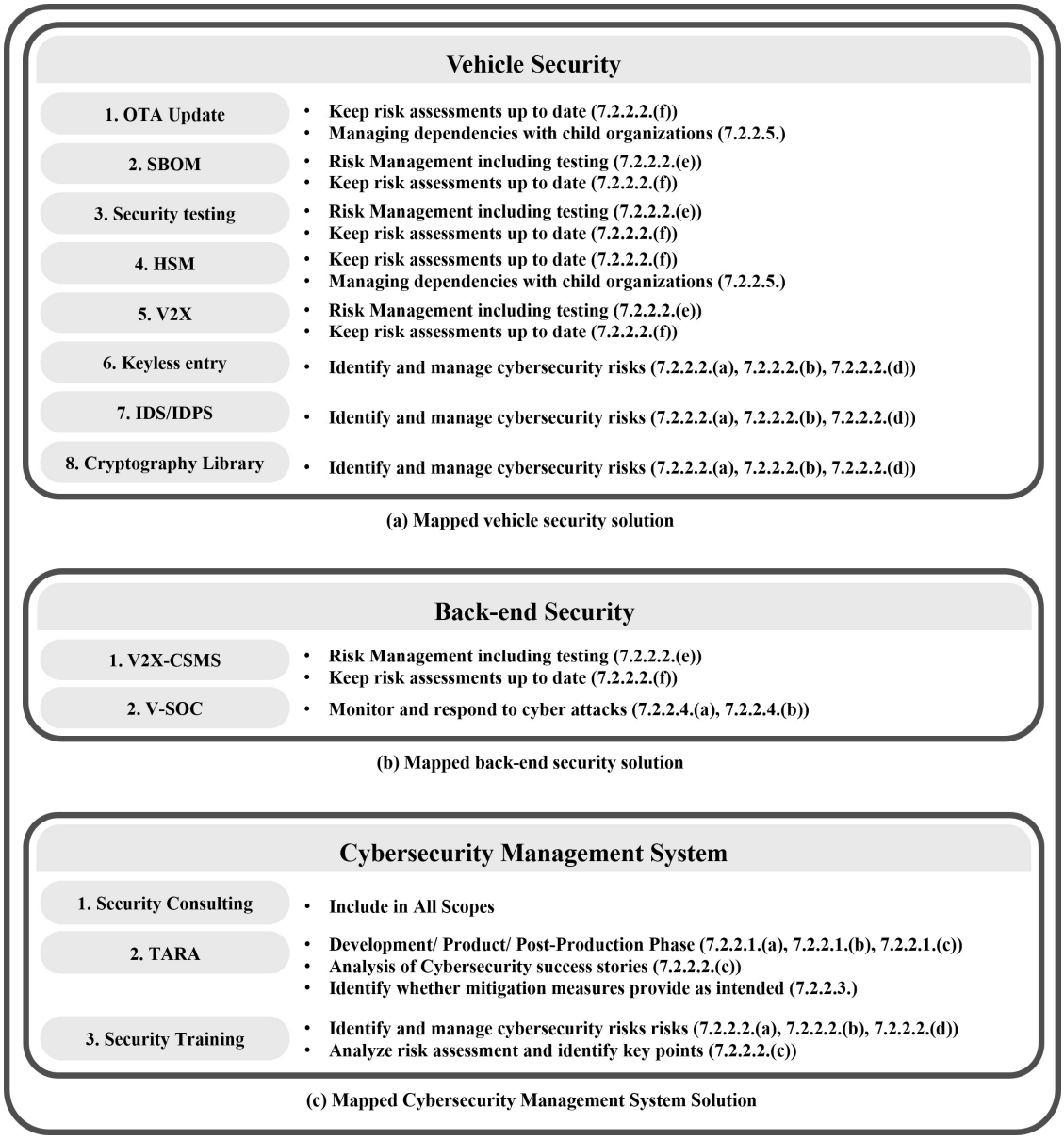
<Table A1> Classification of requirements in UN Regulation No.155 and mapping with ISO/SAE 21434

Type	Requirement No.	ISO/SAE 21434 Requirement No.
Development Phase	7.2.2.1.(a)	RQ-07-01, RQ-07-03, RQ-07-04, RQ-07-06, RQ-07-07, RQ-09-01, RQ-09-02, RQ-09-03, RQ-09-04, RQ-09-05, RQ-09-06, RQ-09-07, RQ-09-08, RQ-09-09, RQ-09-10, RQ-09-11, RQ-10-01, RQ-10-02, RQ-10-03, RQ-10-04, RQ-10-05, RQ-10-06, RQ-10-07, RQ-10-08, RQ-10-09, RQ-10-10, RQ-10-11, RQ-10-13, RQ-11-01, RQ-11-02, RQ-12-01, RQ-12-02, RQ-12-03, RQ-15-01, RQ-15-02, RQ-15-03, RQ-15-04, RQ-15-05, RQ-15-06
Product Phase	7.2.2.1.(b)	RQ-12-01
Post-Production Phase	7.2.2.1.(c)	RQ-07-04, RQ-07-06, RQ-07-07, RQ-08-01, RQ-08-02, RQ-08-03, RQ-08-04, RQ-08-05, RQ-08-06, RQ-08-07, RQ-08-08, RQ-13-01, RQ-13-02, RQ-13-03, RQ-14-01, RQ-14-02, RQ-15-01, RQ-15-02, RQ-15-03, RQ-15-04, RQ-15-05, RQ-15-06
Identify and manage cybersecurity risks	7.2.2.2.(a) 7.2.2.2.(b) 7.2.2.2.(d)	RQ-05-01, RQ-05-02 ,RQ-05-03, RQ-05-06, RQ-05-07, RQ-05-08, RQ-05-09, RQ-08-01, RQ-08-02, RQ-08-03, RQ-08-06, RQ-08-08, RQ-09-03, RQ-09-04, RQ-09-05, RQ-09-06, RQ-09-07, RQ-09-09, RQ-15-01, RQ-15-02, RQ-15-03, RQ-15-08, RQ-15-09
Analyze risk assessment and identify key points	7.2.2.2.(c)	RQ-05-01, RQ-05-02, RQ-05-06, RQ-08-04, RQ-08-06, RQ-09-03, RQ-09-04, RQ-09-05, RQ-09-06, RQ-09-07, RQ-09-08, RQ-15-04, RQ-15-05, RQ-15-06, RQ-15-10, RQ-15-15, RQ-15-16, RQ-15-17
Risk management including testing	7.2.2.2.(e)	RQ-09-08, RQ-09-09, RQ-09-10, RQ-09-11, RQ-10-01, RQ-10-02, RQ-10-03, RQ-10-06, RQ-11-01, RQ-11-02, RQ-12-01, RQ-12-02, RQ-12-03
Keep risk assessments up to date	7.2.2.2.(f)	RQ-06-02, RQ-06-03, RQ-06-04, RQ-06-05, RQ-06-06, RQ-06-07, RQ-06-09, RQ-06-10, RQ-06-11, RQ-06-12, RQ-07-06, RQ-08-07, RQ-08-08
Identify preventive measure against cyber attacks	7.2.2.2.(g)	RQ-07-01, RQ-07-02, RQ-07-03, RQ-07-04, RQ-07-06, RQ-07-07, RQ-08-01, RQ-08-02, RQ-08-03, RQ-08-04, RQ-08-05, RQ-08-06, RQ-08-07, RQ-08-08, RQ-11-01, RQ-11-02, RQ-13-01, RQ-13-02, RQ-13-03, RQ-15-03, RQ-15-04, RQ-15-05
Analysis of Cybersecurity success stories	7.2.2.2.(h)	RQ-07-03, RQ-08-04
Identify whether mitigation measures provide as intended	7.2.2.3.	RQ-13-01, RQ-13-02
Monitor and respond to cyber attacks	7.2.2.4.(a) 7.2.2.4.(b)	RQ-05-09, RQ-08-01, RQ-08-02, RQ-08-03, RQ-08-04, RQ-08-05, RQ-08-06
Managing dependencies with child organizations	7.2.2.5.	RQ-06-02, RQ-06-03, RQ-06-04, RQ-06-05, RQ-06-06, RQ-06-07, RQ-06-09, RQ-06-10, RQ-06-11, RQ-06-12, RQ-07-01, RQ-07-03, RQ-07-04, RQ-07-06, RQ-07-07, RQ-15-02, RQ-15-03

<Table A2> Questions about the development phase

Development Phase		
Requirements No.	Work Product (21)	Question
RQ-07-04 RQ-07-06 RQ-07-07	Cybersecurity interface agreement	Has the organization analyzed the capabilities of the vendors to assess the cybersecurity capabilities of all vendors?
		Does every quote request include expectations of vendor cybersecurity liability?
		Do you fulfill cybersecurity interface agreements with all vendors in your organization?
		Does a cybersecurity interface contract include both customer and vendor roles and responsibilities?
		Is there a communication plan to ensure that the cybersecurity roles and responsibilities between customers and suppliers are communicated?
RQ-09-01 RQ-09-02	Item definition	Are item definitions performed to ensure implementation of cybersecurity best practices?
		Does the item definition include item boundaries, features, and architecture?
		Does the item definition include the operating environment of the item in relation to cybersecurity?
		Does the item definition include constraints and compliance requirements?
		Does the item definition reflect the assumptions made during the item definition process?
RQ-09-03 RQ-09-04	TARA	Has a TARA been performed that includes all assets for the specified item?
RQ-09-05	Cybersecurity goals	Are cybersecurity objectives such as CAL defined based on risk, threat planning for each specific item?
RQ-09-06	Cybersecurity claims	Are cybersecurity claims mentioned for operating environments that lead to reduced risk of threat scenarios?
		Are cybersecurity claims mentioned for risk handling options that share or transfer risk?
RQ-09-07	Verification report for cybersecurity goals	Has documented reports validated the process of determining cybersecurity objectives and cybersecurity claims?
RQ-09-08 RQ-09-09 RQ-09-10	Cybersecurity concept	Has the Sailor Security Concept been documented that embodies the cybersecurity requirements needed to meet the cybersecurity objectives of a particular item?
RQ-09-11	Verification report of cybersecurity concept	Has the cybersecurity concept been validated through the report?
RQ-10-01 RQ-10-02	Cybersecurity specifications	Are cybersecurity requirements defined for product development based on cybersecurity requirements allocated at a high level?
		Are cybersecurity requirements defined for product development based on higher-level architectural design?
		Does your cybersecurity requirements include applicable cybersecurity controls?
		Is the architecture designed to ensure the applicability of various cybersecurity requirements improved?
		Are contact points identified between refined architectural design components applicable to meet cybersecurity requirements?

Development Phase		
Requirements No.	Work Product (21)	Question
RQ-10-03	Cybersecurity requirements for post-development	Did you consider the impact of cybersecurity on the development stage while listing the cybersecurity requirements?
		Are specific cybersecurity requirements documented to ensure cybersecurity in the post-development phase?
RQ-10-04 RQ-10-05	Documentation of the modelling, design, or programming languages and coding guidelines	Are standards established for appropriate design, modeling, and programming languages for cybersecurity?
RQ-10-07	Weaknesses found during produc development	Has a vulnerability analysis been performed to identify weaknesses in improved architectural design and cybersecurity requirements?
		Is the vulnerability analysis presented as a final documented report?
RQ-10-08	Verification report for the cybersecurity specifications	Are refined cybersecurity requirements and architectural designs identified in documented reports?
RQ-10-09 RQ-10-11	Integration and verification report	Are verification activities carried out to ensure compliance with refined cybersecurity requirements?
		Are integration and validation activities summarized in a documented report?
RQ-10-10	Integration and verification specification	Are integration and validation specifications defined for the development phase?
RQ-11-01 RQ-11-02	Validation report	Has a verification report been produced detailing the risks and acceptance grounds identified for a particular item during the concept and product development phase?
RQ-12-01 RQ-12-02	Production control plan	Has a production management plan been established to apply cybersecurity requirements during the development phase?
		Does the production management plan include the cybersecurity requirements listed for the post-development phase?
		Does the production management plan include details on how to achieve cybersecurity requirements during production?
		Does the production management plan contain details on how to configure items or components in case of unauthorized changes?
		Does the production management plan include activities to ensure that cybersecurity requirements have been met during production?
RQ-15-01	Damage scenarios	Is a process in place to identify damage scenarios for assets related to the functioning of road vehicles?
RQ-15-02	Assets with cybersecurity properties	Is there a list of assets that identified all assets associated with road vehicles in the organization?
		Does the asset list detail assets with cybersecurity attributes that result in damage scenarios?
RQ-15-03	Threat scenarios	Can threat scenarios be applied to organizational assets?
RQ-15-04 RQ-15-05 RQ-15-06	Impact ratings with associated impact categories	Is the impact on the organization evaluated in safety, financial, operational and personal information (S, F, O, P) for various damage scenarios?
		Are impact ratings identified for different damage scenarios for each independent category (e.g., safety, finance, operations, personal information (S, F, O, P))?



<Fig. A1> Categories of security solutions mapped to the type in <Table A1>