자동차 사이버보안
가이드라인

국토교통부

한국교통안전공단
자동차안전연구원

자동차 사이버보안 가이드라인

국토교통부

한국교통안전공단
자동차안전연구원

자동차 사이버보안
가이드라인

2020.12.

목차

01.

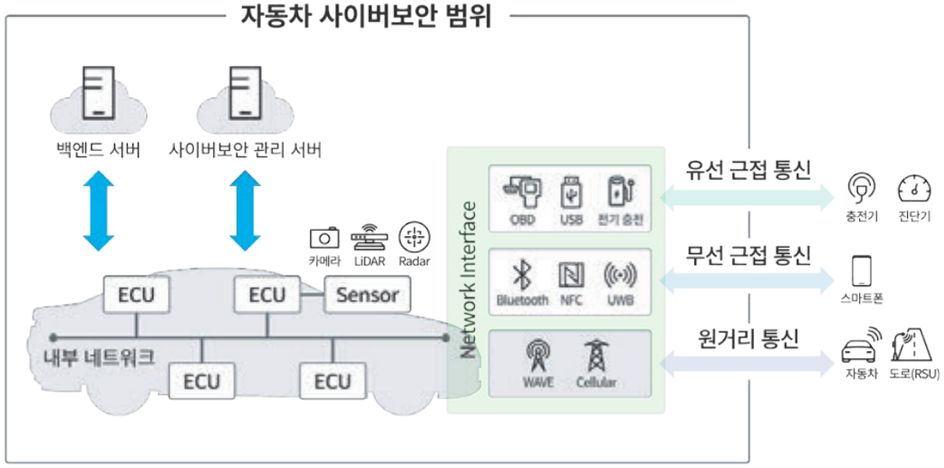
개요

1 자동차 사이버보안 가이드라인 제정 개요

1. 자동차 사이버보안 가이드라인 제정 배경

■ **사이버보안 위협 증대** 자동차에 전자제어장치가 증가하고 통신과 연결되면서 자동차 불법제어 및 프라이버시 침해 등 사이버보안 취약점과 위협이 증대됨에 따라 대응방안을 강구할 필요가 있음

● 자동차에 대한 사이버공격 등 해킹의 피해는 최악의 경우 사망에 이르는 인명사고로 직접 이어질 수 있으므로 자동차 사이버보안 확보가 필수적임



자동차에서 사이버보안 고려 환경

■ **국제기준의 제정** 자동차 사이버보안 중요성에 대한 국제적인 공감대를 바탕으로 UNECE WP.29 (국제 자동차기준 조화 회의체)에서 자동차 사이버보안에 관한 최초의 국제기준*이 채택되었음

* UN Regulation No.155 (2020년 6월 채택, 2021년 1월 발효, 이하 UNR)

● 국내 자동차의 안전성을 확보함과 동시에 원활한 자동차 수출입이 이루어질 수 있도록 우리나라도 자동차 사이버보안에 대한 국제 논의에 발맞춰 관련 제도를 준비해야할 것으로 보임

2. 가이드라인 제정 목적

■ 우리나라는 이번 사이버보안 국제기준을 대체로 받아들일 계획이지만, 이를 우리나라 법체계에 맞게 제도화하기 위해서는 다음의 사항들을 먼저 검토할 필요가 있어 이번에 채택된 국제기준을 전부 반영하여 즉시 국내 기준화 하기는 어려움

● **자기인증** 우리나라는 자기인증제도를 취하여 안전기준도 자기인증에 부합하도록 체계화 되어있는 반면, 이번에 채택된 UN 사이버보안 기준은 형식승인제도에 맞추어져 있어 국내 사이버보안 기준 제정을 위해서는 우리 제도에 맞게 기준화 될 수 있도록 더 많은 검토가 필요함

● **사이버보안 특성** 제작사들이 자동차 자기인증을 하려면 자동차의 성능 평가를 위한 기준이 먼저 주어져야 하는데, 사이버 공격(해킹)의 지속적인 진화와 다양성 등을 감안할 때, 사이버보안에 대한 성능평가 기준을 마련하는 데에는 보다 많은 연구가 필요함

■ 국내 기준이 제정되기 까지는 아직 시간이 있지만, 자동차 사이버보안의 중요성이 나날이 강조되고 있다는 점과 사이버보안 국제 기준까지 이미 제정되었다는 점을 고려한다면 우리나라 제작사들도 자동차 사이버보안 확보를 위한 준비에 돌입할 필요가 있음

■ 이에, 자동차 제작사 등 관련자들이 국내기준 제정 전까지의 참조자료로 활용할 수 있도록 국제기준을 기반으로 만들어진 ▲ 자동차 사이버보안 권고안, ▲ 사이버보안 관련 기준마련 계획, ▲ 인프라 구축 계획 등을 담은 “자동차 사이버보안 가이드라인”을 마련함

3. 가이드라인 제정 경위

■ UNECE WP.29(국제 자동차기준 조화 회의체) 사이버보안전문가기술그룹(CS/OTA IWG)* 사이버보안 논의 참여 中

* 사이버보안전문가기술그룹(CS/OTA IWG, Informal Working Group on Cyber Security & OTA)

** UNECE WP.29은 2016.12월부터 사이버보안전문가기술그룹을 결성하여 자동차 사이버보안 신규 UN 기준을 개발하였음(‘20.06 채택, ‘21.01발효)

제12차 UN 사이버보안 전문가기술그룹 회의, 2018.4.17.-19, 서울

- 국제기준회의체(UNECE WP.29) 의 사이버보안 기준(안) 검증을 위한 테스트단계 참여 ('19.01~ '19.08)

■ 자동차 사이버보안 전문가회의를 통한 사전 의견수렴('19.11)

* 자동차보안 전문가, 자율차산업발전협의체 등 관련 전문가 의견수렴

■ 자동차 사이버보안 지침(안) 발표를 위한 세미나 개최('19.11.15)

* 자동차 제작사, 부품사, 보안 업체 등 관산학연 약150명 참여

■ 자동차 사이버보안 지침 이해관계자 회의 및 의견 수렴

- 자동차 사이버보안 지침 관련 전문가 회의 5회('20.05~09)
- 국내제작사 및 수입차제작사 회의('20.9.24, 10.28) 및 의견 수렴

02.

자동차 사이버보안 국제기준

1 자동차 사이버보안 국제기준 제정 배경

■ **연구 본격화 이전, '15~'16.11** WP.29는 자율주행차와 커넥티드 카를 위한 일반적인 요구사항을 담은 '자율주행자동차 및 커넥티드 카의 사이버보안 및 데이터 보호를 위한 가이드라인'을 개발하였음

■ **연구그룹 결성, '16.12** 사이버보안 대책 마련을 위한 세부 논의를 위하여 WP.29산하에 사이버보안전문가기술그룹*을 결성하였음

* 사이버보안전문가기술그룹(CS/OTA IWG, Informal Working Group on Cyber Security and software updates (Over-The-Air))

● 한국, 영국, 일본, 독일, 네덜란드, 프랑스, 미국 등의 국가와 세계자동차제작사협회(OICA), ISO, ITU 등의 국제표준기구, 국제자동차연맹(FIA), 유럽자동차 공급업체협회(CLEPA) 및 자동차 애프터마켓 공급자 유럽연합(FIGIEFA) 등 관련 단체가 참여하였음

■ **사이버보안 기준안 제안, '18.9** 사이버보안 원칙 및 사이버보안 위협 완화조치 수준의 권고안을 도출하고 부록으로 기준안을 제안하였음

■ **기준안 테스트, '19** 사이버보안 기준(안)의 효과성 및 강건성을 검증하기 위하여 테스트단계(Test Phase)를 진행하였음

● 각 국가(한국, 영국, 네덜란드, 독일, 일본, 프랑스, 스페인 등)의 승인기관 및 시험기관(평가/검증)과 자동차 제작사들(자료 준비)이 참여하였으며, 구체적인 설명과 예시 등의 정보제공을 위한 해석서*도 개발하였음

* '2021년3월 WP.29총회에서 채택을 위한 공식논의 예정

■ **기준 채택, '20.6** 사이버보안 권고안에서 기준 부분을 분리하여 제안하고, WP.29총회에서 사이버보안 기준(UNR No.155)을 채택함

■ **GTR 개발 논의, '20.10~** UNR 기준(형식승인)기반으로 GTR(자기인증) 개발을 위한 사이버보안 전문가기술그룹 논의가 시작됨('20.10~)

2 자동차 사이버보안 국제기준의 주요 내용

1. 개요

■ **적용대상** 승용차·상용차·전자제어 장치가 장착된 트레일러·자율주행기능이 장착된 초소형차, 이와 관련된 **자동차제작사 등**

■ **주요내용** 제작사들은 ▲ 차량 **사이버보안 관리를 위한 체계**(CSMS*)를 갖추고, ▲ 차량 **형식에 대한 위험평가·관리**를 수행하여야 함

* CSMS(Cyber Security Management System, 사이버보안관리체계)

● 승인/시험기관은 ▲ 제작사가 **CSMS를 갖춘 경우 인증서 발급, ▲ 차량 위험평가·관리**가 CSMS에 따라 적절히 시행된 경우 **형식 승인**

2. 세부 내용

■ **CSMS 인증서 발급요건** 제작사가 **자동차 사이버보안에 필요한 각종 프로세스*** 등 관리체계를 적절히 갖추었음을 **입증해야 함**

* (주요내용) ①보안 위협을 식별·평가·분류·관리하기 위한 프로세스, ②차량 보안성 시험을 위한 프로세스, ③보안 위협을 모니터링하고 탐지·대응하는 프로세스

■ **형식승인 요건** 제작사는 ▲ **CSMS 인증서를 보유**하고, ▲ 차량에 대한 **위험평가·관리, ▲ 보안조치* 및 충분한 검증시험** 등을 수행해야 함

* (주요내용) ① 사이버 공격의 탐지 및 예방 조치, ② 제작사의 모니터링 기능 지원 조치, ③ 사이버 공격에 대한 분석을 위한 "데이터 포렌식" 지원 조치

● 아울러, ▲ 해당 차량의 부품, ▲ 애프터마켓 소프트웨어 등 **제작사 외부의 공급업체·시스템에 대한 위험도 관리**하여야 함

■ **모니터링/보고** 제작사는 보안 **모니터링 결과를 승인기관에 보고**해야 함

■ **정보 공유** 본 기준을 채택한 **회원국의 승인기관**들은 형식승인 관련 정보 교류를 위한 **DB* 에 정보**를 공유**하여야 함

* DETA(Database for the Exchange of Type Approval, 형식승인 교환을 위한 DB)

** (주요내용) ①승인기관이 제작사의 보안조치 적절성을 평가하기 위한 방법·기준, ②이에 대한 타 승인기관의 검토의견 등

참고 UN 사이버보안 기준 관련 참고자료

■ UN 기준(UNR No.155)의 구성

형식승인		자기인증
UN 사이버보안 기준		국내 도입 대상
1.	범위	○
2.	정의	○
3.	승인 신청	△
4.	마킹	(형식승인 관련)
5.	승인	△
6.	사이버보안 관리체계(CSMS) 준수 인증서	
7.	사양서 - 사이버보안 관리체계(CSMS) 요구사항 - 자동차 형식에 대한 요구사항 - 보고 조항	○
8.	자동차 형식의 변경 및 연장	△ (형식승인 관련)
9.	생산 적합성	
10.	생산 부적합성에 대한 벌칙	
11.	생산 중지	
12.	형식승인기관 및 승인시험 담당 시험기관 명과 주소	
부속서		국내 도입 대상
1.	정보 문서	○
2.	통신	형식승인 관련
3.	승인 마크의 배치	
4.	사이버보안 관리체계(CSMS) 준수인증서 모델	
5.	위협 및 대응 완화조치 목록	○

■ 주요 국가들의 사이버보안 기준 관련 동향

주요국가	사이버보안 기준 관련 동향	비 고
한 국	■ '22.7 기준시행 목표로, 다음의 단계적 조치를 거칠 예정 • (1단계) 가이드라인 발간 (2단계) 관련 법규/안전기준 제정	자기인증
미 국	■ 사이버보안 기술전문가그룹에 참여하여 GTR 개발 중 • 2016.10 첨단자동차를 위한 사이버보안 모범사례 발행	자기인증
유 럽	■ UNR No.155를 채택, '22.7부터 기준 시행예정 • (적용대상) 새로운 차량형식:'22.7~ / 모든 차량형식:'24.7~	형식승인
일 본	■ UNR No.155를 채택 • (적용대상) 자율주행시스템 : '21.1~ / 새로운 차량형식:'22.7~ / 모든 차량형식:'24.7~	형식승인

03.

자동차 사이버보안 확보를 위한 권고안

1 권고안과 국제기준의 비교

1. 권고안의 기본방향

■ 제작사 등이 **현 UNR*을 바탕으로 제정될 국내기준에 대비**할 수 있도록 **제작사 권고사항** 및 **보안 승인/시험기관의 역할** 등을 제시

* UNR(UN Regulation, 여기서는 UN Regulation No.155 사이버보안 기준을 의미)

● **UNR**을 기반으로, 향후 **국내기준으로 제정될 가능성이 높은 사항**에 대해서 **권고안으로 우선 제시**

* 권고안과 국내기준이 크게 상이할 경우 제작사 등의 혼선이 초래될 우려가 있어 국내기준화가 어려울 것으로 검토되는 일부 조항들은 권고안에 미포함

2. 국제기준 중 국내 기준화가 어려운 조항

■ 현 **사이버보안 UNR**에는 기준 **미채택국에게 배타적인 조항**이 있어 충분한 검토를 거쳐 향후 **법제화시 국내기준 반영여부 결정** 예정

배타적 조항	채 택 국	미 채택국
CSMS 인증서	• CSMS를 갖춘 제작사에게 국제 기준을 채택한 **가입국 사이에서만 통용되는 CSMS 인증서 발급**	• **자체 인증서** 발급은 가능하나, **기준 가입국에 대한 효력 없음**
승인기관 간 정보공유	• 사이버보안 관련 데이터 교류를 위한 **DB(DETA) 열람권한 부여**	• DETA **열람권한 제한적 부여**

* 한국은 UNR(1958협정) 가입국이지만, 자기인증제도를 취하고 있기 때문에 형식승인 기반의 UNR No.155을 채택하지 않음

3. 주요사항의 비교

비교사항	국제기준	권 고 안
성 격	• 채택 시 의무규정	• 의무·강제성 없는 권고안
기 반	• 형식승인	• 자기인증·형식승인 등의 체계와 무관하게 제시될 수 있는 내용만 포함
주요 내용	• 총칙(범위·정의 등)	• 좌동
	• 사이버보안 요건 (CSMS, 자동차 형식의 보안요건)	• 좌동
	• 제작사 보고의무 규정	• 제작사 정보공유에 대한 권고 제시
	• 행정사항(절차·서류·벌칙·부칙)	• 미포함
	• 형식승인 특성이 반영된 사항 (CSMS 인증서, DETA 정보공유)	• 미포함

2 자동차 사이버보안 국제기준의 주요 내용

1. 총칙

1-1. 목적

● 본 권고안은 자동차의 사이버보안을 확보하기 위하여 자동차제작사 및 자동차보안전담기관 등에게 권고되는 사항을 규정함을 목적으로 하며, 자동차의 라이프사이클 동안 참여하는 자동차 부품사, 서비스 제공업체, 협력업체 등도 본 권고안을 참고할 수 있다.

자동차보안전담기관이란?

● 사이버보안 국제기준(UNR No.155)에서는 제작사 보안을 평가하여 CSMS 인증서를 발행하는 승인기관을 지정하도록 하고 있으나, 우리나라에는 아직 국제기준에 부합하는 승인기관이 지정되어 있지 않음

▸ 본 권고안에서는 향후 승인기관의 역할 등을 수행하게 될 기관을 자동차보안전담기관(가제)이라고 명명

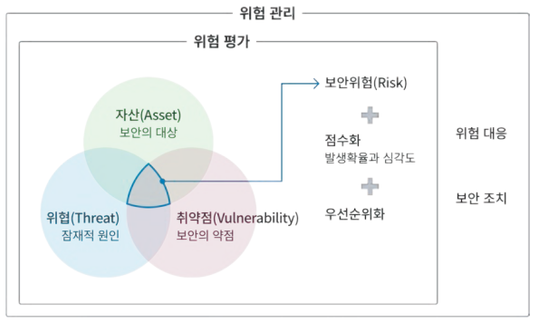
1-2. 용어의 정의

● 이 권고안에서 사용되는 용어의 정의는 다음과 같다.

① **위협** (Threats)	• 시스템/자동차나 조직 또는 사람에게 해를 끼칠 수 있는 사고의 잠재적인 원인
② **취약점** (Vulnerability)	• 위협으로 인해 악용될 수 있는 자산 또는 보안 조치의 약점
③ **위험** (Risk)	• 위협이 취약점을 통해 조직이나 사람에게 해를 끼칠 가능성 * 이하 이 권고안에서는 사이버위협으로부터 발생하는 위험을 의미함

④ **위험 평가**
(Risk Assessment)

- 다음의 절차를 포함하여 위험을 가늠하는 전반적인 과정
  · (위험 식별) 위험의 발견·인지·기술
  · (위험 분석) 위험 특성의 이해 및 위험 수준의 결정(판단)
  · (위험 산정) 위험 분석 결과에 비추어 위험수준의 허용가능 여부를 결정



위험평가 및 위험관리 개념도

⑤ **위험 관리**
(Risk Management)

- 위험 대응을 위하여 조직을 감독하고 통제하는 통합 활동
  * 상기 개념도와 같이 위험평가, 위험대응, 보안 조치 등 자동차를 보호하기 위한 일련의 과정들을 포괄하는 활동

⑥ **사이버보안**
(Cyber Security)

- 자동차와 그 기능이 사이버 위협으로부터 보호되는 상태

⑦ **사이버보안 관리체계**
(CSMS)

- 차량에 대한 위험에 대응 하기 위하여 조직이 구축하는 다음과 같은 관리체계(위험기반 접근법)
  · 대응을 위한 조직의 프로세스
  · 위험 대응과 관련된 조직의 책임·권한 등의 분배

⑧ **보안 조치**
(Mitigation)

- 위험의 제거·감소를 위한 기술적 대책

⑨ **자동차 형식**
(Vehicle Type)

- 다음의 특성에 대해 동일성을 가지는 일련의 차량 종류
  · 자동차의 구조와 장치에 관한 형상, 규격 및 성능(자동차관리법 제2조제4호)
  · 사이버보안 관련 전기·전자 구조 및 외부 연결장치 등

⑩ **라이프사이클**
(생애주기, 수명주기, Lifecycle)

- 자동차 형식의 초기 개발단계에서부터 해당 형식의 폐기에 이르기까지의 전 기간으로, 다음과 같이 구분
  · 개발단계 / 생산단계 / 생산후단계

⑪ **애프터마켓**
(Aftermarket)

- 자동차의 이용이나 운행과 관련하여 제작사의 자동차 판매 이후 형성되는 자동차산업의 2차 시장
  · (예시) 자동차부품, 소프트웨어, 서비스, 화학제품, 장비 및 액세서리의 제조, 재양산, 유통, 판매 및 설치 등

1-3. 적용 대상

● 본 권고안은 자동차 사이버보안 관련하여 「자동차관리법」제3조 제1항 제1호부터 제4호까지의 규정에 해당하는 승용자동차, 승합자동차, 화물자동차, 특수자동차, 전자제어장치가 장착된 피견인 자동차에 적용된다.

사이버보안 이슈와 주된 관련이 있는 자동차

● 전기/전자적 설계요소가 존재하는 모든 자동차는 사이버공격 대상이 될 수 있어 보안에 유의해야 하며, 자율차 및 통신연결 기능이 있는 차량은 보안확보가 필수

UNR에서의 적용범위

● Category M(최소 4륜 승객운송자동차, 승용차), N(최소 4륜 화물 운반 동력 구동 자동차, 화물차), 전자제어장치가 장착된 O(트레일러), 레벨3 이상의 자율주행 기능이 장착된 L^6 및 L^7(초소형 자동차)

2. 사이버보안 관리체계

2-1. 사이버보안 관리체계의 구축

● 자동차제작사는 사이버보안 관리체계(CSMS)를 갖출 것이 권고된다.

관리 주체

● CSMS를 구축하는 주체는 자동차제작사로, 공급업체나 협력업체 등의 공급망에 있어서도 CSMS 관리체계에서 자동차제작사가 관리할 필요가 있음

CSMS와 기타 관리체계와의 관계

● 사이버보안 관리체계는 조직의 품질관리시스템(QMS)의 일부이거나 독립적일 수 있으며, 조직의 품질관리시스템의 일부일 경우에도 명확하게 구분 가능하여야 함

2-2. 사이버보안 관리체계의 적용 범위

● 사이버보안 관리체계는 차량의 라이프사이클 전반에 적합하도록 구축되고 적용될 수 있어야 한다.

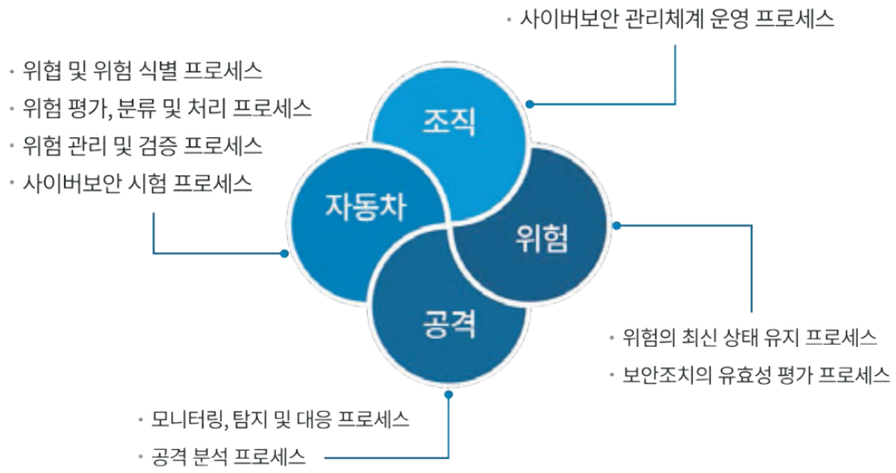
사이버보안의 특성 : 라이프사이클 관리

● 기술발전에 따라 빠르게 변화하는 사이버 위협을 대비하기 위해서는, 특정 시점만 고려한 사이버보안 조치는 유의미한 효과를 거둘 수 없을 것으로 보임

▸ 따라서 제작사는 차량의 라이프사이클(개발 단계, 생산 단계, 생산 후 단계) 전반에 걸쳐 사이버보안 관리체계(CSMS)의 적절한 프로세스를 활용하여 보안조치를 취하는 등 위험을 관리해야 함

2-3. 사이버보안 관리체계의 프로세스

● 사이버보안 관리체계의 구성요소로 다음과 같은 프로세스가 요구된다.



사이버보안 관리체계의 프로세스

① 제작사 조직 내에서 사이버보안 관리체계를 운영하기 위한 프로세스

■ 사이버보안 관리체계의 구축 및 관리체계 자체의 적정성 유지·관리를 위한 활동과 매뉴얼 등을 아우르는 프로세스로, 특히 다음의 사항을 포함

· 사이버보안 관련 조직의 구조화

· 사이버보안 관리에 있어 역할·책임 등의 규정 및 권한 분배

· 자동차 형식 라이프사이클(개발/생산/생산후)에 따른 사이버보안 관리활동 매뉴얼 등

② 자동차에 대한 위험을 식별하기 위한 프로세스

■ 자동차에 대한 위험을 발견·인지할 수 있도록 하는 프로세스로, 최소한 다음의 활동을 포함

· 사이버보안에 대한 시스템의 연관성 식별 활동

· 각 시스템/기능 정의 및 다른 시스템과의 상호작용· 제약 등을 고려한 전체 시스템을 기술/묘사하는 활동

· 자동차의 안전한 운행과 관련하여 보안의 대상이 되는 자산(중요 요소) 식별 활동

· 사이버 위협 및 취약점 식별 활동

※ “부록 1. 자동차에 대한 위협 목록” 참고

③ 식별된 위험을 평가하고 분류 및 처리하기 위한 프로세스

■ ② 에 따라 식별된 위험을 적절히 관리하기 위하여 시행되는 프로세스로, 다음과 같은 절차를 포함

· (위험분석 및 산정) 식별된 위험에 대한 영향평가 및 잠재적 공격 경로 분석, 예상되는 모든 공격 경로에 대한 실행 가능성 판단

· (위험 분류 및 처리) 산정 결과에 따라 위험을 분류하고, 보안조치를 통해 위험수준을 현저하게 낮추는 등 적절하게 처리

④ 식별된 위험이 적절하게 관리되고 있는지 검증하기 위한 프로세스

■ ③ 에 따른 보안조치 등의 처리를 거쳐 잔존한 위험이 향후 자동차에 대한 실제 위험으로 이어지지 않도록 잔존한 위험의 수준 등을 검증하는 프로세스로, 다음 사항을 고려할 것

· 잔존한 위험의 수준을 제작사가 명시한 위험허용범위 이내로 유지할 것

※ “부록 2. 위협에 따른 보안 조치” 참고

⑤ 자동차의 사이버보안 시험을 위한 프로세스

■ 제작사가 개발하는 자동차의 사이버보안에 대하여 자체적인 시험을 하기 위한 프로세스

· 사이버보안의 시험 및 관리는 자동차 라이프사이클 전반에 걸쳐 이루어져야 한다는 점을 감안하여 ⑤프로세스를 구축할 필요가 있음

※ (참고) 생산 단계의 시험 프로세스는 개발 단계에서 사용되는 프로세스와 다를 수 있음

⑥ 위험평가 정보를 최신 상태로 유지하기 위한 프로세스

■ 사이버 공격방법의 진화 또는 자동차 시스템 교체로 인한 사이버 위험의 변화 가능성을 감안하여 변화된 위험에도 대응할 수 있도록 ②,③과 같은 위험평가를 최신화하는 프로세스

· 사이버 위험의 형태·수준 등의 변화 여부를 식별하기 위한 절차와, 사이버 위험의 변화여부가 위험평가 과정에 반영되도록 하는 절차도 ⑥에 포함되어야 함

· 시스템 변경 또는 사이버보안 위협의 변경 등으로 인해 변화된 사이버 위험이 발생할 수 있다고 판단되는 경우 위험평가를 수행하여 정보를 최신화할 것이 권고되며, 이 경우 변경사항을 총체적으로 고려하여 업데이트할 필요가 있음

⑦ 사이버 공격, 위협, 취약점에 대한 모니터링, 탐지 및 대응을 위한 프로세스와 새로운 사이버 위협 및 취약점이 발생한 경우 그에 대한 기존 보안조치의 유효성을 평가하기 위한 프로세스

■ 자동차에 대한 사이버 공격, 위협, 취약점 등을 모니터링하기 위한 프로세스, 모니터링을 통해 식별된(탐지된) 위협에 시기적절하게 대응할 수 있는 프로세스 및 실행된 보안조치가 모니터링을 통해 발견된 새로운 사이버위협 및 취약점에도 여전히 효과적인지 평가하는 프로세스로 다음 사항을 고려

· 생산 후 단계의 자동차에 대한 사이버보안 모니터링 활동

· 제작사 시스템/자동차 관련 수집된 정보와 사이버보안 연관성을 평가하는 활동

· 관련 정보에 대한 위험 판단/평가 활동

· 자동차에 대한 사고 대응 절차

⑧ 자동차에 대한 사이버 공격이나 공격시도 등의 위협이 발생한 경우, 그에 대한 분석을 지원하기 위한 데이터 제공에 사용되는 프로세스

■ 사이버 공격 등으로 인한 위험의 수준, 예상 공격경로, 대응방안 모색 등의 분석(③)을 할 수 있도록 관련 데이터를 제공하기 위한 절차·매뉴얼 등의 프로세스로, 다음을 포함

· 보안사고 등이 발생한 경우 전담 대응팀 활성화 및 대응절차 등에 대한 매뉴얼

· 사고 및 취약점에 대한 정보 획득을 위해 현장을 모니터링하는 절차

· 취약점 발견 시 대응절차 등에 대한 매뉴얼

2-4. 사이버보안 관리체계의 고려사항

● 제작사는 사이버보안의 확보를 위해 다음의 사항을 충분히 고려하여 각 프로세스를 수립할 것이 권장된다.

① 부록에 따른 위협 및 보안 조치와 그밖에 필요한 사항들을 적절히 고려하여 보안을 확보할 수 있을 것

■ 최소한 부록에 제시된 위협 및 보안조치를 고려하되, 부록에 제시되지 않은 위협에 대해서도 조치를 취할 필요가 있음

· 부록에 제시된 위협 및 보안조치의 목록은 부록 작성 당시를 기준으로 보면 최신화 된 것이지만, 기술의 발전과 차량 기능 복잡성의 증가로 인하여 새로운 위협요소가 추가로 발생할 수 있음을 고려하여 프로세스를 수립하는 것이 바람직

② 사이버 위협·취약점으로 인한 피해를 예방·최소화 할 수 있을 정도로 가능한 한 빠른 시간 내에 대응할 수 있도록 할 것

■ 가능한 한 빠른 시간 내에 위험이 관리될 수 있도록 기한(deadline)을 설정하여 대응할 필요가 있음

· 기한 내에 적절한 대응이 이루어졌는지 여부를 확인하기 위한 모니터링 활동도 병행할 것을 권장

③ 차량의 최초 등록 이후 모니터링을 지속적으로 수행하며, 차량의 데이터 등에서 사이버 위협, 취약점 및 공격에 대해 분석하고 탐지할 수 있을 것

■ 사이버보안은 자동차의 라이프사이클 전반에 걸쳐 관리되어야 한다는 점을 감안하여 사이버 공격·위협 및 차량 취약점을 지속적으로 모니터링 할 필요가 있음

· 아울러, 모니터링은 제작사의 사이버보안 관리대상이 되는 모든 차량에 대하여 이루어져야 함

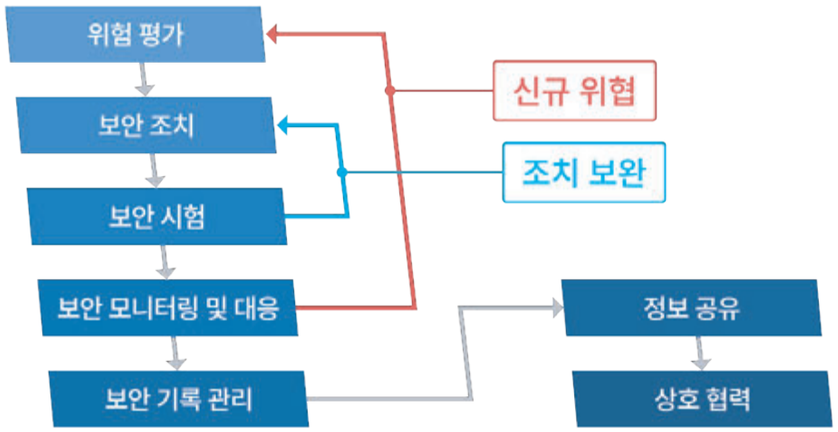
④ 자동차의 부품, 서비스 등 공급망에서 유래하는 사이버보안 위험을 관리할 수 있을 것

- 사이버보안 관리체계를 통해 공급망에서 발생하는 위험도 관리할 수 있도록 하고, 공급망으로부터 초래된 위험에 대해 적절한 조치가 이루어지도록 관리할 필요가 있음
  - 자동차 제작사가 공급망의 보안을 반드시 단독으로 관리해야할 필요는 없으며, 공급업체 간의 상호 합의 및 협력을 통해서도 관리할 수 있음

3. 자동차의 사이버보안 확보를 위한 제작사 권고사항

3-1. 제작사에 대한 권고사항 개요

- 자동차제작사는 자동차의 사이버보안을 확보하기 위하여 사이버보안 관리체계에 따라 다음과 같은 조치들을 취할 것이 권장된다.



사이버보안 관리체계의 활동

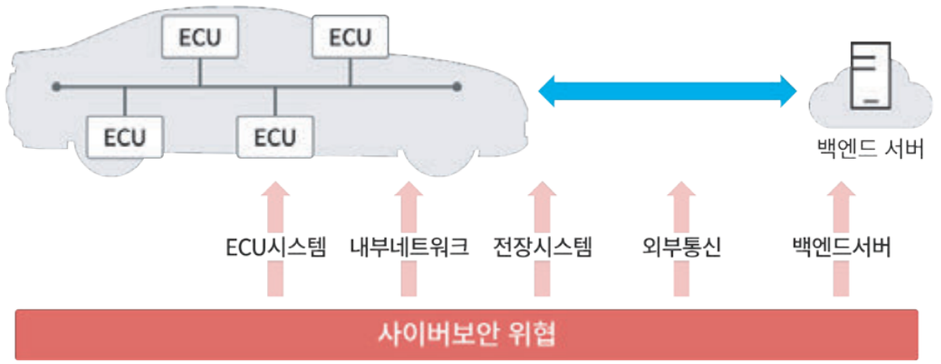
3-2. 위험 평가 및 위험관리

- 자동차제작사는 ▲자동차 사이버보안 관련 중요 요소의 식별 및 ▲위험 평가를 수행하여 ▲식별된 위험을 적절히 처리하고 관리하되, 다음의 사항을 고려할 필요가 있다.

① 위험평가 및 위험관리를 총체적인 관점에서 실시할 것

- 다음의 위협까지 총체적으로 고려하여 위험평가 및 위험관리를 실시할 필요가 있음
  - 자동차 내·외부 시스템들 간의 상호작용(인터페이스)
  - 위험평가 시에 발생할 수 있는 잠재적인 위협
  - 공급망에 존재하는 위협 등

※ “부록 1. 자동차에 대한 위협 목록” 참고하되, 다른 모든 위협들도 고려해야 함



사이버보안 위협의 종류

② 수용/허용 가능한 위험수준 및 위험심각도를 정의하여 위험을 관리할 것

- 위험평가를 통해 산정된 위험, 완화조치 이후 잔존한 위험 등에 대하여 별도의 보안조치가 있어야 하는지를 결정할 수 있도록 판단기준을 사전에 설정할 필요가 있음
- 아울러, 심각한 위험을 우선적으로 탐지·대응하여 위험관리가 효율적으로 이루어질 수 있도록 위험의 심각도를 정의하고, 위험의 우선순위를 정할 수 있어야 함

③ 위험평가 결과를 최신화 할 것

- 프로세스⑥에 따라 최신화된 위험평가 정보를 바탕으로 위험평가 결과를 최신화 할 필요가 있음
  - 특히, 자동차의 사이버보안에 영향을 미치는 위협 발생 시 즉각적으로 이에 대한 위험평가를 수행할 수 있어야 함

자동차 사이버보안 관련 중요 요소란?

- 주로 다음의 사항들이 중요 요소로 간주되나, 제작사가 중요 요소 / 비중요 요소로 식별한 이유에 대한 정당한 근거를 제시할 수 있어야 함

- 차량 안전보호 기능, 전용환경 보호 기능, 도난방지 기능 등과 관련된 차량의 아키텍쳐, 장치 등
- 게이트웨이 등 통신 연결 기능과 관련된 차량의 아키텍쳐, 장치 등

3-3. 보안 조치 / 모니터링 및 대응

- 자동차제작사는 자동차에 대한 사이버 공격·위협 및 취약점 등에 대하여▲탐지 및 예방, ▲모니터링 및 원인분석 등의 보안조치를 취할 수 있어야 하며, 다음의 사항을 고려해야 한다.

① 자동차를 보호하기 위한 적절한 보안조치를 구현할 것

- 자동차의 중요 장치가 식별된 위험으로부터 보호될 수 있도록 적합한 보안 조치들을 마련할 수 있어야 함
  - 제작사는 위험 평가 및 위험 관리 연계하여 보안이 내재화되도록 할 필요가 있음

※ “부록 2. 위협에 따른 보안 조치 참고

② 가능한 한 최단 시간 내에 조치를 마련할 것

- 탐지된 사이버위협과 취약점에 대하여 가능한 한 최단 시간 내에 적합한 조치를 취할 수 있어야 함

③ 자동차 관련 제품의 전용 환경을 마련하고, 이를 보호하기 위한 조치까지 강구할 것

- 자동차에서 애프터마켓 소프트웨어, 서비스, 응용 프로그램, 데이터 등을 안전하게 저장·실행할 수 있도록 보안성을 갖춘 전용환경을 마련할 수 있어야 함

④ 적합한 암호모듈을 사용할 것

- 암호모듈은 충분한 보안 강도를 가진 암호 표준을 따라야 함
  - 만약 제작사가 국제 표준 등에 부합하지 않는 암호모듈을 사용한다면, 그것을 사용하는 정당한 근거를 제시할 수 있어야 함

전용 환경

- 외부에서 제공되는 소프트웨어, 서비스, 응용 프로그램 등을 자동차에서 이용하기 위하여 구축하는 환경
- 차량이 차량 외부에 위치한 서버나 서비스(예: 클라우드)와 상호작용하는 경우, 사이버보안과 관련하여 이들로부터 발생하는 차량에 대한 위험을 고려하여야 함

암호모듈

- 암호화 작업을 처리하는 하드웨어·소프트웨어·펌웨어의 총칭으로, 차량 내외부에서 전송되는 데이터의 암호화 등에 사용되며 여러 국제/국가 표준이 있음(예.FIPS)

3-4. 보안 시험

- 자동차제작사는 보안 조치가 적절한 수준으로 설계되고 구현되었는지를 확인하기 위하여 객관적이고 충분한 시험평가를 수행할 수 있어야 한다.

시험평가 내용

- 시험 대상 및 근거(예: 시험의 성공 척도), 평가 방법론과 근거(예: 시험에 포함된 범위와 노력에 대한 주석), 시험 수행 주체와 근거(예: 사내, 공급업체 또는 외부 조직 및 자격/경력에 관한 모든 관련 정보), 합격/불합격 기준 및 시험 결과를 포함할 수 있음

3-5. 사이버보안 기록 관리

- 자동차제작사는 다음의 사항을 고려하여 자동차의 사이버보안과 관련된 자료를 ▲기록·보존, ▲변경이력을 관리할 필요가 있으며, 향후 자동차보안전담기관이 자료를 필요로 할 경우 충분한 협조를 할 것이 권장된다.

① 다음의 사항을 기록·보존할 것

- 자동차 사이버보안 관리체계와 관련된 정보
- 자동차의 다음 각 항목에 대한 구성 정보
  - 자동차의 사이버보안과 관련된 자동차의 자동차용품, 시스템, 장치, 아키텍쳐
  - 자동차의 사이버보안과 관련된 자동차 시스템 및 차량 내·외부 시스템과의 상호작용(인터페이스)
- 자동차의 위험 평가 정보
- 자동차에 구현한 보안 조치 및 위험 관리 정보
- 자동차의 사이버보안 관련 시험 평가 정보
- 부품 또는 장치, 서비스 등에 대한 공급망에서의 사이버보안에 관한 고려사항
- 사이버보안 관련한 사건/사고 기록 및 분석 정보
- 그 밖에 자동차 사이버보안을 위해 조치한 내역

② 자동차 라이프사이클 동안 기록을 보존할 것

■ 사이버보안 관리가 차량의 라이프사이클에 걸쳐 이루어짐을 감안하여 기록도 최소한 라이프사이클 동안 보존될 필요가 있음

· 아울러, 자동차의 생산이 완전히 중단된 날로부터 최소 10년 이상 보존할 것이 권장됨

■ 기록을 폐기하는 경우에는 적절한 후속조치를 취할 필요가 있음

기록 보존기간 산정 근거

● 자동차 평균 수명주기는 점점 증가하는 추세에 있으며 국내 15년 이상 고령차의 비율은 승용차 11.5%, 화물차 21.6%(오토헤럴드, '20.9.23)로 높은 편

● UNR에서도 자동차 형식의 생산이 완전히 중단된 날로부터 최소한 10년간의 기록 보존을 요구하고 있음

▸ 이러한 점을 고려할 때, 최소 10년 이상의 기록보존이 권장됨

3-6. 정보 공유

● 자동차제작사는 다음을 고려하여 자동차보안전담기관에게 사이버보안 관련 정보를 공유할 수 있어야 한다.

① 다음의 사항을 공유할 것

■ 사이버보안 모니터링 현황
· 사이버 공격
· 자동차에 대한 사이버 위협 및 취약점
· 위협 및 취약점 탐지 및 대응 현황

■ 보안조치 사항
· 자동차에 구현된 보안조치의 유효성 여부
· 추가 보안조치에 대한 필요성
· 보안 조치 결과

② 연간 1회 이상 정보를 공유할 것

■ 제작사의 사이버보안 모니터링 결과를 연간 1회 이상 자동차보안전담기관에게 공유할 필요가 있음

③ 사이버 위험이 발생한 경우 지체없이 공유할 것

■ 새로운 위협이나 취약점이 발견된 경우, 사이버공격이 발생한 경우 자동차보안전담기관에게 지체없이 공유할 필요가 있음

3-7. 상호 협력

● 자동차제작사는 부품제작사, 자동차 사이버보안 관련 사항 등을 시험·인증하는 자동차보안전담기관, 기타 관련자들과 상호 협력할 수 있어야 한다.

● 각 기관은 사이버 위험 관련 정보를 상호 공유할 수 있어야 하며, 위험이 탐지된 경우 신속하게 보안조치를 수립할 수 있도록 긴밀히 협력할 수 있어야 한다.

4. 참고 사이버보안 확보를 위한 자동차보안전담기관의 역할

4-1. 사이버보안 관리체계 인증 확인

- 자동차보안전담기관은 사이버보안 관리체계 인증에 관한 사항에 대해 확인할 수 있다.

4-2. 시정조치 권고

- 자동차보안전담기관은 자동차 사이버보안 위험수준을 관리하기 위하여 제작사로부터 제공된 정보를 확인하고, 필요한 경우 자동차제작사에게 시정을 권고할 수 있다.

4-3. 시험 평가 검증

- 자동차보안전담기관은 제작사의 사이버보안 관리체계 및 자동차의 사이버보안에 대한 시험평가를 수행할 때 3.2~3.4에서 정하는 사항 등에 대하여 적정성을 검증할 수 있다.

04.

자동차 사이버보안 확보를 위한 향후 정책방향

1 제도적 측면에서의 준비

1. 추진 배경

■ 우리나라에서도 해킹 등 **사이버위협에 있어 안전한 자동차**를 **제작**할 수 있도록 **국내기준 마련** 필요

● **국제기준**을 **바탕**으로 **법령 제·개정안**을 마련, **EU 기준 시행**('22.7)에 맞춰 **제·개정 법령이 시행**될 수 있도록 법제화 추진

2. 법제화 관련 검토사항

■ **제·개정 대상 법령 사이버보안 대상이 자동차로 특정**되므로 **자동차 안전 관련 의무사항 등을 규정하는 법령 제·개정** 필요

*「개인정보 보호법」,「위치정보법」,「정보통신기반 보호법」,「정보통신망법」등 네트워크·보안 관련 법령 검토 결과 본 건과 상충될 여지는 적을 것으로 보임

▶ 「자동차관리법」 및 자동차 안전기준 등의 **하위법령 개정**이 타당

* 특히, 제작사에게 보고 의무 등을 부여하기 위해서는 안전기준을 넘어 법률 차원의 개정 필요

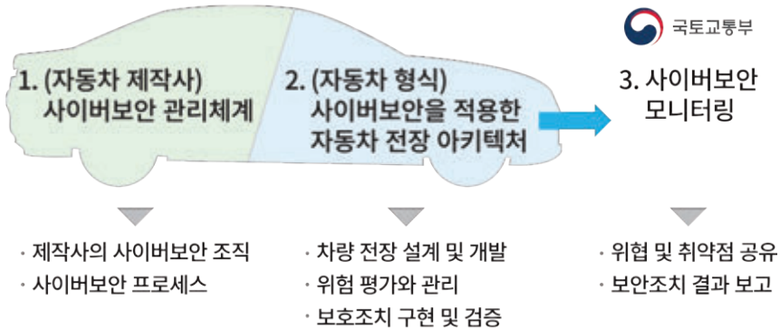
■ **사이버보안성 인증방식 결정 사이버보안의 기술적 특성** 및 현행 **국제기준(UNR)의 제도기반**을 고려, **자기인증/형식승인 방식 결정** 필요

▶ 보다 많은 검토가 필요하나, 현재로서는 **제도적 정합성**을 위하여 **자기인증 방식을 유지하는 것이 타당**할 것으로 보임

구 분	자기인증 방식의 개정	형식승인 방식의 개정
내 용	• CSMS를 자기인증능력 요건으로 규정, 제작사가 차량 보안성 자기인증	• 보안 전담기관이 CSMS 및 차량의 보안성을 직접 검증
장 점	• 자동차 및 자동차부품의 안전성과 관련한 기존 규제방식과 제도적 일관성 유지	• 국내 인증 획득 시 국제기준 채택국에 대해 동일한 효력 발생
단 점	• 국내 제작사의 자동차 수출 시 수출 대상국의 규제 현황에 따른 별도 대응이 필요	• 규제방식의 급격한 변화에 따른 업계의 저항

3. 자동차 사이버보안 법제화 추진안

■ **자기인증 방식을 유지**할 경우「**자동차관리법**」**및 하위법령**에 대해 다음과 같은 방향의 개정이 이루어질 것으로 예상됨



자동차 사이버보안 법제화 방향

■ **법제화 핵심 구조**(예시)

● '자동차 형식에 대한 사이버보안'은 기존 자기인증 대상에 포섭

● '자동차 사이버보안관리체계'에 대한 자기인증제도 신설

● '자동차 사이버보안 관련 보고의무'를 부과하는 법조항 신설

법제화 추진 시 요구사항별 주요 내용(예시) 요약

반영 내용	반영 대상	반영 방안
정의 규정	자동차관리법	‘사이버보안’ 및 ‘사이버보안관리체계’ 정의규정 추가
자동차 형식에 대한 사이버보안 자기인증	자동차관리법 시행령	‘자동차 및 자동차부품의 성능과 기준에 관한 규칙’의 적용대상에 ‘사이버보안을 위한 장치’를 추가
	국토교통부령 (자동차안전기준)	‘자동차 및 자동차부품의 성능과 기준에 관한 규칙’에 상세 준수사항 추가
자동차 사이버보안관리체계에 대한 자기인증	자동차관리법	‘제작사의 CSMS 운영 의무’, ‘CSMS에 대한 자기인증 의무’, ‘CSMS 관련 상세사항의 부령 위임’ 규정을 각 추가
	자동차관리법 시행규칙	‘CSMS에 대한 자기인증제도 운영을 위한 상세사항’을 추가
	국토교통부령(신설)	‘자동차 사이버보안 관리체계의 운영에 관한 규칙(가칭)’을 신설, 상세 준수사항 규정
자동차 사이버보안 관련 보고의무	자동차관리법	‘자동차 형식 중 사이버보안 관련사항 보고의무’ 및 ‘CSMS 관련사항 보고의무’ 추가
	국토교통부령(신설)	‘자동차 사이버보안 관리체계의 운영에 관한 규칙(가칭)’을 신설,상세 준수사항 규정
기타(적용 우선순위)	자동차관리법	‘자동차 사이버보안’ 관련 사항에는 자동차관리법이 우선 적용됨을 규정

법제화 추진 시 관련 법령별 주요 내용 (예시)

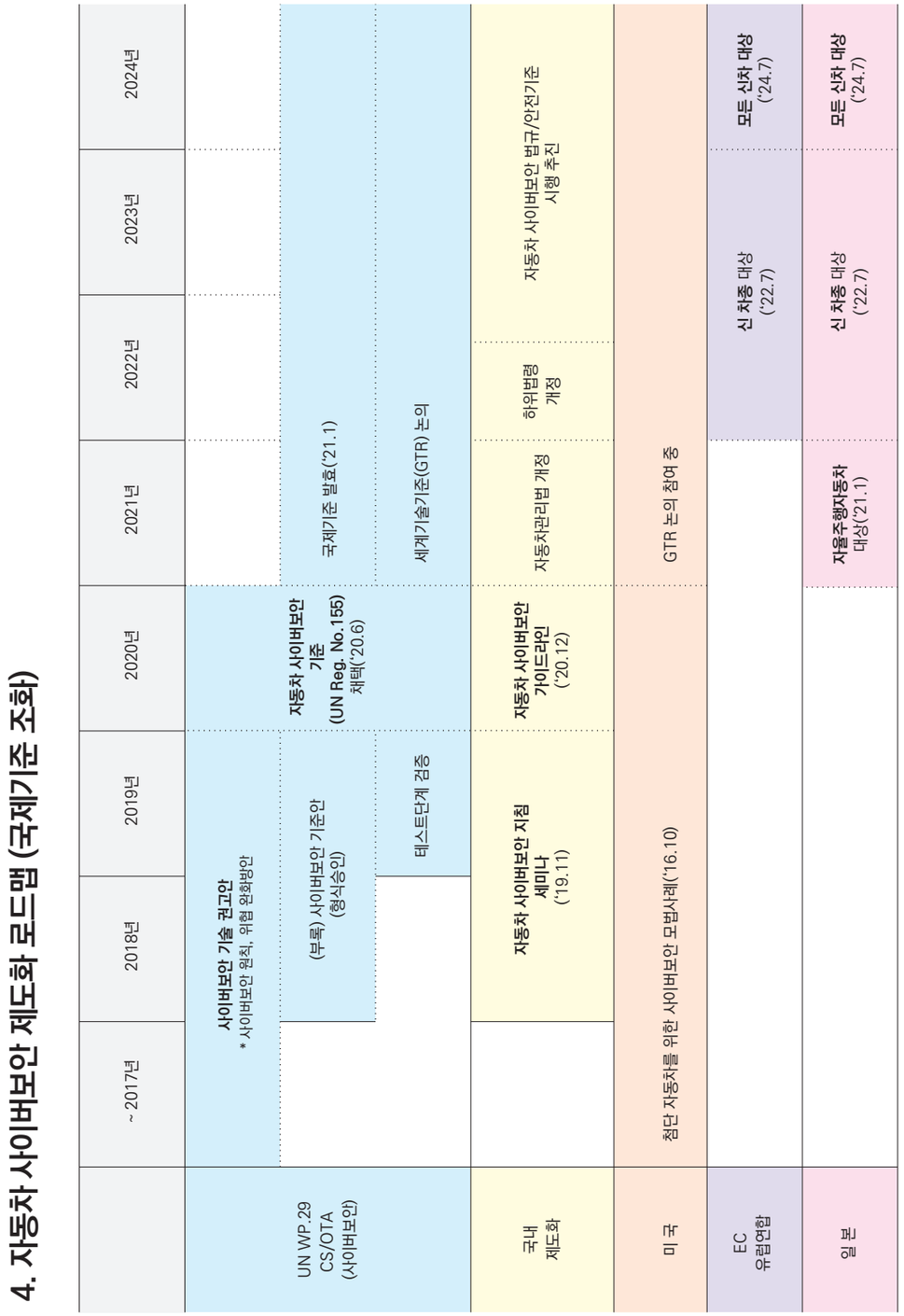
- **「자동차관리법」**에 다음의 사항을 신설함
  - ‘자동차 사이버보안’ 및 ‘자동차 사이버보안관리체계’를 정의하는 규정(동법 제2조 내)
  - 제작사에 ‘자동차 사이버보안관리체계 운영의무’를 부과하는 규정(동법 제29조 내)
  - 국토교통부령으로 ‘자동차 사이버보안 관리기준(가칭)’을 정할 수 있는 근거 규정(동법 제29조 내)
  - ‘자동차 사이버보안관리체계’ 관련 사항을 자기인증 대상에 추가하는 규정(동법 제3장 내)
  - 제작사에 ‘모니터링 및 보고의무’를 부과하는 규정(동법 제3장 내)
  - ‘자동차 사이버보안’과 관련한 사항에 대해서는 동법이 우선 적용됨을 정하는 규정(위치 무관)

- **「자동차관리법 시행령」**에 다음의 사항을 신설함
  - 자동차안전기준의 적용대상에 ‘사이버보안을 위한 장치’를 추가하는 규정(동법 시행령 제8조 제2항 내)

  * 현재 자동차 형식에 대한 자기인증 제도에는 ‘사이버보안을 위한 장치’에 자동차안전기준을 적용할 법령상 근거 규정이 없음

- **「자동차관리법 시행규칙」**에 다음의 사항을 신설함
  - ‘자동차 사이버보안관리체계 자기인증’ 제도 운영을 위한 상세사항을 정하는 규정(동법 시행규칙 제6장의 3추가)

- 국토교통부령으로 다음의 사항을 반영함
  - 「자동차 및 자동차부품의 성능과 기준에 관한 규칙」에 자동차 형식에 대한 사이버보안 관련 준수사항을 추가
  - 「자동차 사이버보안 관리체계의 운영에 관한 규칙(가칭, ‘자동차 사이버보안 관리기준’)」을 신설



2 기반시설 측면에서의 준비

1. 자동차 보안 지원 및 대응 체계 구축 사업 개요

■ 자율차 상용화의 선제 조건인 자동차 사이버보안 확보를 위해 **자동차의 보안 위험수준을 관리·지원**하고 **사이버위협 대응강화**를 위한 **자동차보안 지원 및 대응 체계 구축**

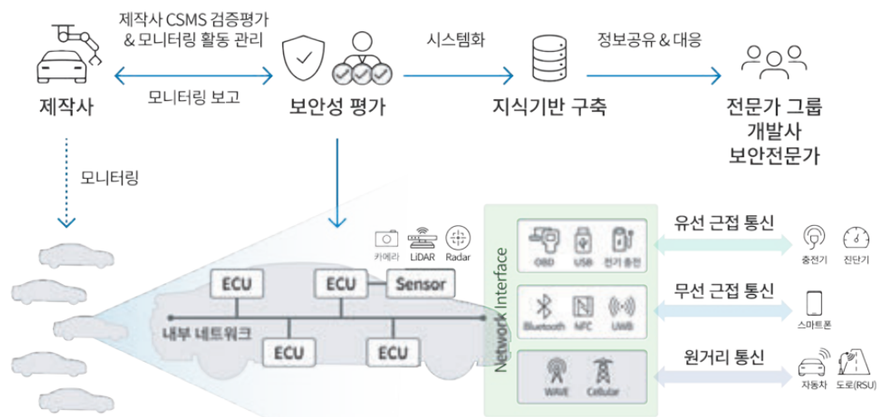
■ **기간/예산** 2021년 ~ 2025년, 약 235억
위 치 경기도 화성시 자동차안전연구원 內

2. 자동차 보안 지원 및 대응 체계 역할(안)

■ 보안 안전기준 검증 자동차 보안 안전 기준 시행을 위한 **자동차 사이버보안 안전성 검증/평가**

- 자동차 **제작사의 사이버보안 관리체계 인증·평가** 및 **사이버보안 모니터링 활동 관리, 차량의 보안 안전성**을 **시험 평가**

- 문제 발견 시 시정 조치 요구 등 **제작결함**(리콜)**과 연계하여 자동차 보안 위험 수준 관리**



자동차 보안 지원 및 대응 체계

■ **보안사고 지원·대응** 자동차 **보안센터** 운영을 통해, **해킹 등 보안사고에 대응**

▶ **국가가 자동차 보안센터(자동차 보안 지원 및 대응체계)를 통해** 사고 등에 대해 **총괄 대응, 업계와 공동 해결책**을 마련하기 위해 **관련기관과 보안 데이터 및 해결책 공유**

보안사고 지원 대응 방안

- 자동차 보안 전문 기구 운영을 통한 보안사고 해결책 마련 및 대응
- 국가차원에서 보안의 위협사례 및 해결방안에 대한 정보 DB구축
- 알림경고 메시지, 해결책 공유, 관제 등을 통해 적극 지원·대응

■ **민간 기술개발 지원** 민간기업 등에 자동차 보안을 실차 수준에서 시험·평가할 수 있는 공간·장비 등을 제공하고, 자동차보안 교육·훈련 및 인식 제고

3. 자동차 보안 지원 및 대응 체계 구축 사업 내용

■ 자동차 보안 센터

- 자동차 보안 지원 및 대응 시스템과 차량을 시험·평가할 수 있는 차고지 등이 포함된 종합적인 자동차 보안 지원 및 대응 공간 구축

■ 자동차 보안 지원 및 대응 시스템

- 자동차 제작사로부터 사이버보안 모니터링 활동을 보고받고, 검증 및 관리하기 위한 시스템 구축

  * 제작사의 사이버보안 관리체계(CSMS) 검증·관리 및 자동차 보안 모니터링 활동 관리

- 자동차에 대한 사이버보안 위협 및 취약점을 수집하고 위험을 분석하여 대응하기 위한 시스템 구축

  * 제작사의 보고 뿐 아니라 보안전문가, 개발사, 연구기관 등을 통한 수집, 연구

- 자동차 사이버보안 위협 및 보안조치 목록에 대한 DB화 등 위협 대응방안에 대한 지식기반 구축

■ **자동차 보안 시험·평가 장비**

- 자동차 실차 및 부품 수준에서 사이버보안 위협 및 취약점 등 자동차의 사이버보안을 검증/평가하기 위하여 자동차 테스트 환경을 조성하는 장비를 구축

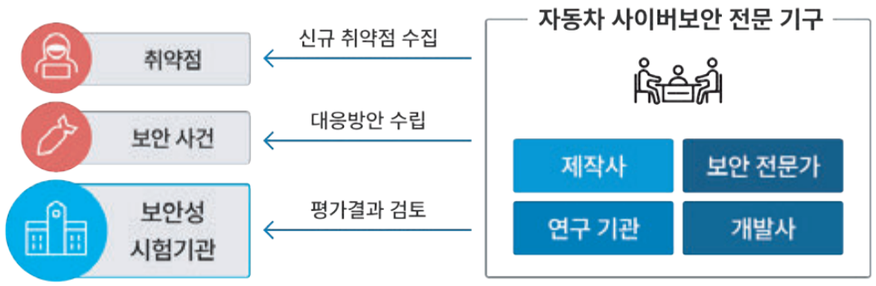
자동차 테스트 환경

① 부품(통신, ECU 등 장비 및 장치) 보안 테스트 환경, ② 차량(실차) 보안 테스트 환경, ③ 보안 시뮬레이션 환경, ④ 보안 주행(도로) 테스트 환경 구축

- 기업 및 학교 등에 자동차 보안 평가환경 지원을 통한 민간 기술개발 지원

■ **자동차 보안 전문 기구**

- 자동차 보안 위협에 대한 정보를 공유·분석하고 공동 대응하여 통합적 해결방법을 찾기 위한 자동차 보안 전문 협의 기구 구성 및 운영



자동차 보안 전문 기구 운영

■ 자동차 보안 지원 및 대응 체계 구축 사업 추진 방안

	2020년	2021년	2022년	2023년	2024년
국내 제도화	자동차 사이버보안 가이드라인 ('20.12)	자동차관리법 개정	하위법령 개정	자동차 사이버보안 법규/안전기준 시행 추진	
자동차보안 지원 및 대응체계	계획 수립	자동차 보안 전문 기구 구성 및 운영			
		자동차 사이버보안 센터 구축 및 실증			고도화
				자동차 보안 지식 기반 구축	

- **1단계** 계획 수립 및 **자동차 보안 전문 기구** 구성/운영

  * 자동차 사이버보안 대응 강화를 위한 포괄적인 계획 수립 및 자동차보안 전문(사이버보안 위협 대응) 기구 구성

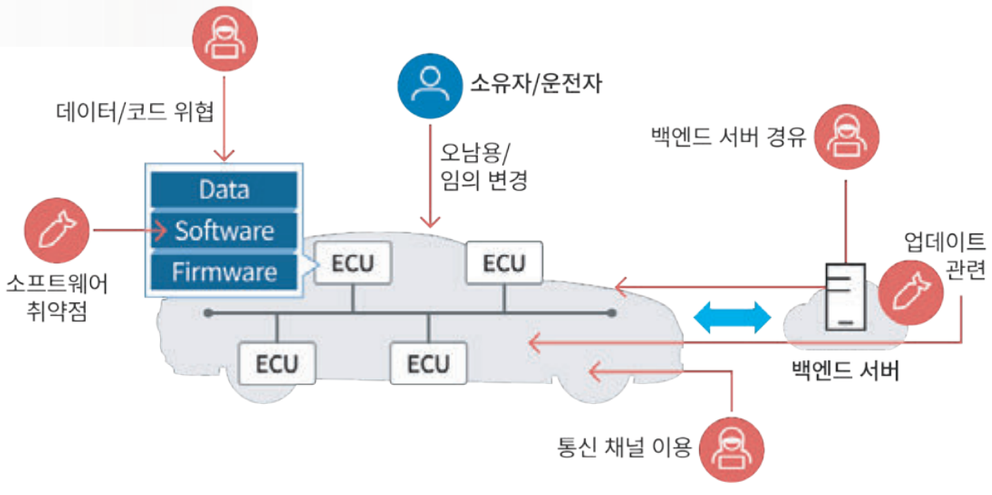
- **2단계 자동차 사이버보안 센터** 구축

  * 자동차 해킹에 대한 정보 공유와 분석 네트워크 구축 및 종합적인 자동차 보안 지원 및 대응 공간 구축

- **3단계 자동차 사이버보안 지식기반** 구축

  * 사이버보안 센터를 통한 사고의 효과적인 대처 및 학습 기반 구축

부록



사이버보안 위협의 예

1. 자동차에 대한 위협

- 실도로 차량과 관련된 백엔드 서버에 대한 위협

취약점/위협에 대한 설명		위협/공격 사례	
1.	자동차를 공격하거나 데이터를 추출하는 수단으로 사용되는 백엔드 서버	1.1	직원의 권한 남용 (내부자 공격)
		1.2	서버에 대한 무단 인터넷 액세스 (백도어, 패치되지 않은 시스템 소프트웨어 취약점, SQL 공격 또는 기타 수단으로 가능)
		1.3	서버에 대한 물리적인 무단 액세스 (서버에 연결된 USB 스틱 또는 기타 매체로 수행됨)
2.	백엔드 서버의 서비스가 중단되어 자동차 동작에 영향을 미침	2.1	백엔드 서버에 대한 공격으로 서버의 기능이 정지됨 (자동차와 서버가 상호작용하지 못하게 되어 자동차에서 요구하는 서비스를 제공하지 못하게 됨)
3.	백엔드 서버에 저장된 데이터 유출 또는 손상	3.1	직원의 권한 남용 (내부자 공격)
		3.2	클라우드 정보 손실. 타사 클라우드 서비스 공급업체에서 데이터를 저장할 때 공격이나 사고로 인해 중요한 데이터가 손실될 수 있음
		3.3	서버에 대한 무단 인터넷 액세스 (백도어, 패치 되지 않은 시스템 소프트웨어 취약점, SQL 공격 또는 기타 수단에 의해 활성화 됨)
		3.4	서버에 대한 물리적인 무단 액세스 (서버에 연결된 USB 스틱 또는 기타 매체로 수행됨)
		3.5	의도하지 않은 데이터 공유로 인한 정보 침해 (관리 오류)

- 통신 채널을 이용한 차량 위협

취약점/위협에 대한 설명		위협/공격 사례	
4.	자동차에서 수신한 메시지나 데이터의 스푸핑	4.1	위장 공격을 이용한 메시지 스푸핑 (군집주행에서 사용되는 802.11p V2X, GNSS 메시지 등)
		4.2	도로에 자동차가 많은 것처럼 다른 자동차를 속이기 위한 시빌 공격
5	차량에 탑재된 데이터/코드에 대한 무단 조작, 삭제 또는 다른 공격을 위해 통신채널을 악용	5.1	통신채널에 악의적인 코드 주입 (변조된 소프트웨어 바이너리를 통신 스트림에 주입)
		5.2	통신채널을 통해 차량에 탑재된 데이터/코드의 변경
		5.3	통신채널을 통해 차량에 탑재된 데이터/코드 덮어쓰기
		5.4	통신채널을 통해 차량에 탑재된 데이터/코드 삭제
		5.5	통신채널에서 자동차에 데이터/코드 끼워넣기 허용 (데이터 코드 작성)
6	통신 채널이 신뢰할 수 없는 메시지를 허용하거나 세션 하이재킹/재생 공격에 취약함	6.1	신뢰할 수 없는 출처의 정보를 수락
		6.2	가로채기(Man in the middle attack) 공격/세션 하이재킹 (session hijacking)
		6.3	재전송 공격 (통신 게이트웨이에 대한 공격을 통해 공격자가 ECU의 소프트웨어 또는 게이트웨이 펌웨어를 다운그레이드 할 수 있음)
7	정보 노출	7.1	정보 가로채기/방해 전파/통신 모니터링 (통신 도청)
		7.2	파일 또는 데이터에 대한 무단 액세스 권한 획득

8	통신채널을 이용한 자동차 기능을 방해하는 서비스 거부(Denial of service) 공격에 취약함	8.1	많은 양의 쓰레기 데이터를 자동차 정보 시스템으로 전송하여 정상적으로 서비스를 이용할 수 없게 함
		8.2	자동차 간의 통신을 교란하기 위해 메시지를 차단할 수 있는 블랙홀 공격
9	자동차 시스템의 액세스 권한 관리 취약점	9.1	권한 없는 사용자가 루트 액세스와 같은 자동차 시스템에 대한 액세스 권한을 탈취할 수 있음
10	통신 매체에 내장된 바이러스를 통해 자동차 시스템이 감염될 수 있음	10.1	통신 매체에 내장된 바이러스를 통해 자동차 시스템을 감염
11	자동차에서 수신된 악의적인 컨텐츠가 포함된 메시지	11.1	악의적인 내부 메시지 (CAN)
		11.2	악의적인 V2X 메시지 (I2V 메시지 또는 V2V 메시지)
		11.3	악의적인 진단 메시지
		11.4	악의적인 고유 메시지 (고유메시지: OEM 또는 구성 요소/시스템/기능 공급업체에서 일반적으로 보낸 메시지)

자동차 업데이트 절차 관련 위협

취약점/위협에 대한 설명		위협/공격 사례	
12	업데이트 절차의 오용 또는 손상	12.1	무선 소프트웨어 업데이트(OTA) 절차의 손상 (조작된 시스템 업데이트 프로그램 또는 펌웨어가 포함됨)
		12.2	로컬/물리적 소프트웨어 업데이트 절차의 손상 (조작된 시스템 업데이트 프로그램 또는 펌웨어가 포함됨)
		12.3	업데이트 프로세스는 손상되지 않았지만 프로세스 전에 소프트웨어가 이미 조작되어 손상됨
		12.4	소프트웨어 공급자의 암호키 손상으로 인한 유효하지 않은 업데이트를 허용
13	정상적인 업데이트 거부	13.1	중요 소프트웨어 업데이트 롤아웃 및 고객별 기능 잠금 해제를 방지하기 위한 업데이트 서버 또는 네트워크에 대한 서비스 거부 공격

의도적이지 않은 인간 행동으로 인한 위협

취약점/위협에 대한 설명		위협/공격 사례	
15	적법한 행위자가 자신도 모르게 사이버 공격을 용이하게 하는 행동을 할수 있음	15.1	합법적인 행위자(소유자, 운영자 또는 유지보수 엔지니어)가 속임수에 당하여 의도하지 않은 악성 프로그램을 실행하거나 공격을 허용하는 행동을 취함
		15.2	정의된 보안 절차를 따르지 않음

차량의 외부 연결 및 접속에 대한 위협

취약점/위협에 대한 설명		위협/공격 사례	
16	자동차의 커넥티비티 관련 기능에 관한 취약점	16.1	리모트 키, 이모빌라이저와 같은 시스템을 원격으로 작동하도록 설계된 기능 조작
		16.2	자동차 텔레매틱스 조작 (민감한 제품의 온도 측정 조작, 화물 도어 원격 잠금 해제)
		16.3	근거리 무선 시스템 또는 센서의 간섭
17	서드파티 소프트웨어에 의한 취약점	17.1	소프트웨어 보안이 취약하거나 손상된 서드파티의 응용 프로그램 (엔터테인먼트 애플리케이션)을 이용하여 자동차 시스템을 공격
18	외부 인터페이스 (USB 포트, OBD 포트)에 연결된 장치가 자동차 시스템을 공격하는 수단으로 사용됨	18.1	외부 인터페이스(USB, 기타 포트 등)가 공격 지점으로 사용
		18.2	바이러스에 감염된 매체가 자동차 시스템에 연결
		18.3	OBD 동글과 같은 진단포트 접근을 이용하여 자동차 매개 변수를 직·간접적으로 조작하는 등의 공격

자동차 데이터/코드에 대한 위협

취약점/위협에 대한 설명		위협/공격 사례	
19	자동차 데이터/코드 추출	19.1	자동차 시스템에서 저작권 또는 독점 소프트웨어 추출 (제품 불법 복제)
		19.2	소유자 개인정보 정보에 대한 무단 액세스 (개인 신상정보, 결제 계좌 정보, 주소록 정보, 위치 정보, 자동차 전자 ID)
		19.3	암호키 추출

20	자동차 데이터/코드 조작	20.1	자동차 전자 ID에 대한 불법/무단 변경사항
		20.2	신원 조작 (사용자가 요금 징수 시스템과 통신할 때 다른 ID를 사용)
		20.3	모니터링 시스템을 우회하는 작업 (ODR 추적기 데이터, 실행 횟수 등 메시지 해킹/수정/차단)
		20.4	자동차 주행 데이터를 변조하기 위한 데이터 조작 (주행 거리, 주행 속도, 주행 방향 등)
		20.5	시스템 진단 데이터에 대한 무단 변경
21	데이터/코드 삭제	21.1	시스템 이벤트 로그 무단 삭제/조작
22	악성코드(malware)의 설치	22.2	악성 소프트웨어 또는 악성 소프트웨어 활동
23	새로운 소프트웨어 설치 또는 기존 소프트웨어 덮어쓰기	23.1	자동차 제어 시스템 또는 정보 시스템의 소프트웨어 위조
24	시스템 운영의 중단	24.1	서비스 거부 (CAN 버스를 플러딩하거나 높은 메시지 전송률을 통해 ECU의 고장을 유발하여 내부 네트워크에서 통신 중단 유발)
25	자동차 매개변수 조작	25.1	무단 액세스를 통해 자동차 주요 기능의 구성 매개변수를 변조 (브레이크 데이터, 에어백 전개 임계값 등)
		25.2	무단 액세스를 통해 충전 매개변수를 변조 (충전 전압, 충전 전력, 배터리 온도 등)

- 충분히 보호되거나 강화되지 않으면 악용될 수 있는 잠재적인 취약점

취약점/위협에 대한 설명		위협/공격 사례	
26	암호 기술이 손상되거나 안전하지 않은 키/알고리즘의 적용	26.1	암호화키의 길이가 짧거나 유효 기간이 길면 공격자가 암호 알고리즘 공격
		26.2	불충분한 용도의 암호 알고리즘을 중요한 시스템을 보호하는 것에 사용
		26.3	더이상 안전하지 않다고 판단되어 이미 사용 중지되었거나 곧 중단될 암호 알고리즘 사용
27	소프트웨어 및 하드웨어 설계상의 취약점	27.1	공격을 가능하게 하도록 설계되었거나 설계 기준을 충족시키지 못하여 사이버 공격에 대응하지 못하는 하드웨어 또는 소프트웨어 사용
28	소프트웨어, 하드웨어 개발 과정에 의한 취약점	28.1	소프트웨어 버그를 이용하여 공격 (알려진 혹은 알려지지 않은 불량 코드/버그가 있는지 소프트웨어 테스트를 하지 않은 경우 특히 위험)
		28.2	개발 과정을 위한 장치 등을 사용하여 공격자가 ECU에 액세스하거나 높은 권한을 획득 (디버그 포트, JTAG 포트, 마이크로프로세서, 개발 인증서, 개발 시 사용된 암호 등)
29	네트워크 설계로 인해 취약점을 허용	29.1	불필요한 포트가 열려 네트워크 시스템에 대한 액세스 허용
		29.2	네트워크 분리를 우회하여 제어권 확보 (보호망을 우회하여 다른 네트워크 세그먼트에 대한 액세스 권한을 획득 등)
31	의도하지 않은 데이터 전송이 발생할 수 있음	31.1	자동차 사용자가 바뀌면 개인정보 및 중요 데이터 유출 가능 (새로운 사용자가 렌트카 사용 또는 자동차의 판매)
32	시스템의 물리적 조작으로 공격이 가능해질 수 있음	32.1	전자 하드웨어 조작 (중간자(man-in-the-middle) 공격을 위해 자동차에 승인되지 않은 하드웨어 설치) 승인된 하드웨어(센서 등)를 승인되지 않은 하드웨어로 교체함 센서가 수집한 정보 조작 (자석을 사용하여 기어 박스에 연결된 홀 효과 센서를 조작)

2. 위협에 따른 보안 조치

- "백엔드 서버"와 관련된 위협 완화조치

"백엔드 서버"에 대한 위협		위협 완화 조치
1.1 & 3.1	직원의 권한 남용 (내부자 공격)	내부자 공격의 위험을 최소화하기 위해 백엔드 시스템에 보안 통제가 적용되어야 한다.
1,2 & 3.3	서버에 대한 무단 인터넷 액세스 (백도어, 패치되지 않은 시스템 소프트웨어 취약점, SQL 공격 또는 기타 수단으로 가능)	무단 액세스를 최소화하기 위해 백엔드 시스템에 보안 통제가 적용되어야 한다.
1.3 & 3.4	서버에 대한 물리적인 무단 액세스 (서버에 연결된 USB 스틱 또는 기타 매체로 수행됨)	시스템 설계 및 액세스 제어를 통해 허가받지 않은 직원이 개인 또는 시스템의 중요 데이터에 접근할 수 없어야 한다.
2.1	백엔드 서버에 대한 공격으로 서버의 기능이 정지됨 (자동차와 서버가 상호작용하지 못하게 되어 자동차에서 요구하는 서비스를 제공하지 못하게 됨)	백엔드 시스템에 보안 통제가 적용되어야 한다. 백엔드 서버가 서비스 제공에 중요할 경우 시스템 정지 시 복구 조치가 있어야 한다.
3.2	클라우드 정보 손실. 타사 클라우드 서비스 공급 업체에서 데이터를 저장할 때 공격이나 사고로 인해 중요한 데이터가 손실될 수 있음	클라우드 컴퓨팅과 관련된 위험을 최소화하기 위해 보안 통제가 적용되어야 한다.
3.5	의도하지 않은 데이터 공유로 인한 정보 침해 (관리 오류)	데이터 침해 방지를 위해 백엔드 시스템에 보안 통제가 적용되어야 한다.

- "자동차 통신 채널"에 대한 완화조치

"자동차 통신 채널"에 대한 위협		위협 완화 조치
4.1	위장 공격을 이용한 메시지 스푸핑 (군집주행에서 사용되는 802.11p V2X, GNSS 메시지 등)	자동차는 수신하는 메시지의 신뢰성 및 무결성을 확인해야 한다.
4.2	도로에 자동차가 많은 것처럼 다른 자동차를 속이기 위한 시빌 공격	암호키 저장을 위한 보안 통제가 구현되어야 함 (예: HSM(하드웨어 보안 모듈) 사용)
5.1	통신채널에 악의적인 코드 주입 (변조된 소프트웨어 바이너리를 통신 스트림에 주입)	자동차는 수신하는 메시지의 신뢰성 및 무결성을 확인해야 한다. 시스템은 위험을 최소화하기 위해 설계별로 보안을구현해야 한다.
5.2	통신채널을 통해 차량에 탑재된 데이터/코드의 변경	시스템 데이터/코드를 보호하기 위해 액세스 제어 기술과 설계가 적용되어야 한다.
5.3	통신채널을 통해 차량에 탑재된 데이터/코드 덮어쓰기	
5.4 21.1	통신채널을 통해 차량에 탑재된 데이터/코드 삭제 시스템 이벤트 로그 무단 삭제/조작	
5.5	통신채널에서 자동차에 데이터/코드 끼워넣기 허용 (데이터 코드 작성)	
6.1	신뢰할 수 없는 출처의 정보를 수락	자동차는 수신하는 메시지의 신뢰성 및 무결성을 확인해야 한다
6.2	가로채기(Man in the middle attack) 공격/세션 하이재킹(session hijacking)	자동차는 수신하는 메시지의 신뢰성 및 무결성을 확인해야 한다
6.3	재전송 공격 (통신 게이트웨이에 대한 공격을 통해 공격자가 ECU의 소프트웨어 또는 게이트웨이 펌웨어를 다운그레이드할 수 있음)	
7.1	정보 가로채기/방해 전파/통신 모니터링 (통신 도청)	자동차와 주고받는 기밀 데이터는 보호되어야 한다.
7.2	파일 또는 데이터에 대한 무단 액세스 권한 획득	시스템 설계 및 액세스 제어를 통해 허가 받지 않은 직원이 개인 또는 시스템의 중요 데이터에 접근할 수 없어야 한다. 보안 통제의 예는 OWASP에서 확인할 수 있다
8.1	많은 양의 쓰레기 데이터를 자동차 정보 시스템으로 전송하여 정상적으로 서비스를 이용할 수 없게 함	서비스 거부 공격을 탐지 및 복구 조치를 취해야 한다.
8.2	자동차 간의 통신을 교란하기 위해 메시지를 차단할 수 있는 블랙홀 공격	서비스 거부 공격을 탐지 및 복구 조치를 취해야 한다.
9.1	권한 없는 사용자가 루트 액세스와 같은 자동차 시스템에 대한 액세스 권한을 탈취할 수 있음	무단 액세스 방지 및 탐지 조치를 취해야 한다
10.1	통신 매체에 내장된 바이러스를 통해 자동차 시스템을 감염	내장된 바이러스/악성 코드로부터 시스템을 보호하기위한 조치를 고려해야 한다
11.1	악의적인 내부 메시지 (CAN)	악의적인 내부 메시지나 활동을 탐지하는 조치를 고려해야 한다
11.2	악의적인 V2X 메시지 (I2V 메시지 또는 V2V 메시지)	자동차는 수신하는 메시지의 신뢰성 및 무결성을 확인해야 한다
11.3	악의적인 진단 메시지	
11.4	악의적인 고유 메시지 (고유메시지: OEM 또는 구성 요소/시스템/기능 공급업체에서 일반적으로 보낸 메시지)	

자동차 업데이트 절차 관련 위협들에 대한 완화조치

“업데이트 프로세스”에 대한 위협		위협 완화 조치
12,1	무선 소프트웨어 업데이트(OTA) 절차의 손상 (조작된 시스템 업데이트 프로그램 또는 펌웨어가 포함됨)	안전한(보안) 소프트웨어 업데이트 절차가 사용되어야 한다
12.2	로컬/물리적 소프트웨어 업데이트 절차의 손상 (조작된 시스템 업데이트 프로그램 또는 펌웨어가 포함됨)	
12.3	업데이트 프로세스는 손상되지 않았지만 프로세스 전에 소프트웨어가 이미 조작되어 손상됨	
12.4	소프트웨어 공급자의 암호키 손상으로 인한 유효하지 않은 업데이트를 허용	암호 키 저장을 위한 보안 통제가 구현되어야 한다
13.1	중요 소프트웨어 업데이트 롤아웃 및 고객별 기능 잠금 해제를 방지하기 위한 업데이트 서버 또는 네트워크에 대한 서비스 거부 공격	백엔드 시스템에 보안 통제가 적용되어야 한다. 백엔드 서버가 서비스 제공에 중요할 경우 시스템 정지 시 복구 조치가 있어야 한다. 보안 통제의 예는 OWASP에서 확인할 수 있다.

의도적이지 않은 인간 행동으로 인한 위협에 대한 완화조치

“의도하지 않은 인간의 행동”에 대한 위협		위협 완화 조치
15.1	합법적인 행위자(소유자, 운영자 또는 유지보수 엔지니어)가 속임수에 당하여 의도하지 않은 악성 프로그램을 실행하거나 공격을 허용하는 행동을 취함	사용자 역할과 액세스 권한을 정의하고 제어하기 위한 조치는 최소한의 액세스 권한 원칙을 기반으로 구현되어야 한다.
15.2	정의된 보안 절차를 따르지 않음	조직은 보안 기능의 관리와 관련된 활동 및 액세스 기록을 포함하여 보안 절차가 정의되고 준수되도록 보장해야 한다.

차량의 외부 연결 및 접속과 관련된 위협에 대한 완화조치

“업데이트 프로세스”에 대한 위협		위협 완화 조치
16,1	리모트 키, 이모빌라이저와 같은 시스템을 원격으로 작동하도록 설계된 기능 조작	보안 통제는 원격 액세스가 가능한 시스템에 적용되어야 한다.
16.2	자동차 텔레매틱스 조작 (민감한 제품의 온도 측정 조작, 화물 도어 원격 잠금 해제)	
16.3	근거리 무선 시스템 또는 센서의 간섭	
17.1	소프트웨어 보안이 취약하거나 손상된 서드 파티의 응용 프로그램(엔터테인먼트 애플리케이션)을 이용하여 자동차 시스템을 공격	소프트웨어는 보안 평가되고, 인증되고 무결성이 보호되어야 함. 자동차에서 호스팅될 예정이거나 예측 가능한 제3자 소프트웨어의 위험을 최소화하기 위해 보안 통제를 적용해야 한다
18.1	외부 인터페이스(USB, 기타 포트 등)가 공격 지점으로 사용	보안 통제가 외부 인터페이스에 적용되어야 한다.
18.2	바이러스에 감염된 매체가 자동차 시스템에 연결	
18.3	OBD 동글과 같은 진단포트 접근을 이용하여 자동차 매개 변수를 직·간접적으로 조작하는 등의 공격	

"공격의 잠재적 대상 또는 동기”와 관련된 위협에 대한 완화조치

“공격의 잠재적 대상 또는 동기”에 대한 위협		위협 완화 조치
19.1	자동차 시스템에서 저작권 또는 독점 소프트웨어 추출 (제품 불법 복제)	시스템 데이터/코드를 보호하기 위해 액세스 제어 기술과 설계가 적용되어야 한다. 보안 통제의 예는 OWASP에서 확인할 수 있다
19.2	소유자 개인정보 정보에 대한 무단 액세스 (개인 신상정보, 결제 계좌 정보, 주소록 정보, 위치 정보, 자동차 전자 ID)	시스템 설계 및 액세스 제어를 통해 허가받지 않은 직원이 개인 또는 시스템의 중요 데이터에 접근할 수 없어야 한다. 보안 통제의 예는 OWASP에서 확인할 수 있다.
19.3	암호키 추출	암호 키 저장을 위한 보안 통제가 구현되어야 함 (예: HSM(하드웨어 보안 모듈) 사용)

20.1	자동차 전자 ID에 대한 불법/무단 변경사항	시스템 데이터/코드를 보호하기 위해 액세스 제어 기술과 설계가 적용되어야 한다. 보안 통제의 예는 OWASP에서 확인할 수 있다.
20.2	신원 조작 (사용자가 요금 징수 시스템과 통신 할 때 다른 ID를 사용)	
20.3	모니터링 시스템을 우회하는 작업 (ODR 추적기 데이터, 실행 횟수 등 메시지 해킹/수정/차단)	시스템 데이터/코드를 보호하기 위해 액세스 제어 기술과 설계가 적용되어야 한다. 보안 통제의 예는 OWASP에서 확인할 수 있다. 센서 또는 전송된 데이터에 대한 데이터 조작 공격은 서로 다른 정보 소스의 데이터를 연관시키는 방법으로 완화조치 할 수 있다.
20.4	자동차 주행 데이터를 변조하기 위한 데이터 조작 (주행 거리, 주행 속도, 주행 방향 등)	
20.5	시스템 진단 데이터에 대한 무단 변경	
21.1	시스템 이벤트 로그 무단 삭제/조작	시스템 데이터/코드를 보호하기 위해 액세스 제어 기술과 설계가 적용되어야 한다. 보안 통제의 예는 OWASP에서 확인할 수 있다.
22.2	악성 소프트웨어 또는 악성 소프트웨어 활동	시스템 데이터/코드를 보호하기 위해 액세스 제어 기술과 설계가 적용되어야 한다. 보안 통제의 예는 OWASP에서 확인할 수 있다.
23.1	자동차 제어 시스템 또는 정보 시스템의 소프트웨어 위조	
24.1	서비스 거부 (CAN 버스를 플러딩하거나 높은 메시지 전송률을 통해 ECU의 고장을 유발하여 내부 네트워크에서 통신 중단 유발)	서비스 거부 공격의 탐지 및 복구를 위한 조치를 취해야 한다.
25.1	무단 액세스를 통해 자동차 주요 기능의 구성 매개변수를 변조 (브레이크 데이터, 에어백 전개 임계값 등)	시스템 데이터/코드를 보호하기 위해 액세스 제어 기술과 설계가 적용되어야 한다. 보안 통제의 예는 OWASP에서 확인할 수 있다.
25.2	무단 액세스를 통해 충전 매개변수를 변조 (충전 전압, 충전 전력, 배터리 온도 등)	

- 충분히 보호되거나 강화되지 않으면 악용될 수 있는 잠재적 취약과 관련된 위협에 대한 완화조치

"충분히 보호되거나 강화되지 않으면 악용될 수 있는 잠재적 취약점"에 대한 위협		위협 완화 조치
26.1	암호화키의 길이가 짧거나 유효 기간이 길면 공격자가 암호 알고리즘 공격	소프트웨어 및 하드웨어 개발을 위한 사이버보안 모범 사례를 따라야 한다.
26.2	불충분한 용도의 암호 알고리즘을 중요한 시스템을 보호하는 것에 사용	
26.3	더이상 안전하지 않다고 판단되어 이미 사용 중지되었거나 곧 중단될 암호 알고리즘 사용	

27.1	공격을 가능하게 하도록 설계되었거나 설계 기준을 충족시키지 못하여 사이버 공격에 대응하지 못하는 하드웨어 또는 소프트웨어 사용	소프트웨어 및 하드웨어 개발을 위한 사이버보안 모범 사례를 따라야 한다.
28.1	소프트웨어 버그를 이용하여 공격 (알려진 혹은 알려지지 않은 불량 코드/버그가 있는지 소프트웨어 테스트를 하지 않은 경우 특히 위험)	소프트웨어 및 하드웨어 개발을 위한 사이버보안 모범 사례를 따라야 한다. 적절한 범위의 사이버보안 테스트
28.2	개발 과정을 위한 장치 등을 사용하여 공격자가 ECU에 액세스하거나 높은 권한을 획득 (디버그포트, JTAG 포트, 마이크로프로세서, 개발인증서, 개발 시 사용된 암호 등)	
29.1	불필요한 포트가 열려 네트워크 시스템에 대한 액세스 허용	
29.2	네트워크 분리를 우회하여 제어권 확보 (보호망을 우회하여 다른 네트워크 세그먼트에 대한 액세스 권한을 획득 등)	소프트웨어 및 하드웨어 개발을 위한 사이버보안 모범 사례를 따라야 한다. 시스템 설계 및 시스템 통합을 위한 사이버보안 모범 사례를 따라야 한다.
31.1	자동차 사용자가 바뀌면 개인정보 및 중요 데이터 유출 가능 (새로운 사용자가 렌트카 사용 또는 자동차의 판매)	개인정보 저장을 위해 데이터 무결성 및 기밀성 보호를 위한 모범 사례를 따라야 한다.
32.1	전자 하드웨어 조작 (중간자(man-in-the-middle) 공격을 위해 자동차에 승인되지 않은 하드웨어 설치)	무단 액세스 방지 및 탐지 조치를 취해야 한다

- 데이터의 물리적인 손상으로 인한 위협에 대한 완화조치

"데이터의 물리적 손상"에 대한 위협		위협 완화 조치
30.1	제3자에 의한 피해. 교통사고 또는 도난 시 물리적 손상으로 인해 중요한 데이터가 손실되거나 손상될 수 있음	개인정보 저장을 위해 데이터 무결성 및 기밀성 보호를 위한 모범 사례를 따라야 한다. 보안통제의 예는 ISO/SC27/WG5에서 확인할 수 있다.
30.2	DRM(디지털 권한 관리) 충돌로 인한 손실. DRM 문제로 인해 사용자 데이터가 삭제될 수 있음	
30.3	IT 구성 요소의 마모 및 파손으로 인해 중요한 데이터(무결성)의 손실이 발생될 수 있으며, 이로 인해 잠재적으로 연쇄적 문제(Cascading Issue)가 발생할 수 있음(예: 키 변경의 경우)	