ISO/SAE 21434 사이버보안 산출물

LKAS (Lane Keeping Assist System)

시스템 버전 1.0 | 작성일: 2025년 12월 11일 | 문서 분류: 기밀

2조 | 강현우, 구교웅, 김소영, 박세리, Agaliu Enrik, 황진영

1. 프로젝트 개요 및 범위

1.1 LKAS 소개 및 목적

프로젝트명	전방 카메라를 통한 **LKAS** 개발
목적	차선 유지 보조를 통한 운전자의 편의 및 안전 증대
ASIL 레벨	ASIL B (중간 수준의 안전 무결성 수준)
적용 차량	승용차, SUV (레벨 2 자율주행 지원)

LKAS(Lane Keeping Assist System)는 차량이 주행 중 차로를 벗어날 위험이 감지되었을 때, 운전자 개입 없이 스티어링을 보조하여 차로 중앙을 유지하도록 지원하는 능동 안전 시스템입니다.
본 시스템은 전방 카메라와 차선 인식 알고리즘을 기반으로 차선의 위치·곡률·차량 편차 등을 실시간으로 추정하며, 도로 구조가 직선·곡선 여부에 관계없이 차로 유지에 필요한 조향 보조 토크를 제공합니다.
이를 통해 운전자의 피로도를 줄이고 차로 이탈로 인한 사고 위험을 완화할 수 있습니다.

1.2 시스템 아키텍처

LKAS 시스템은 다음과 같은 주요 구성요소로 이루어져 있습니다.

- 감지 센서 : 전방 카메라 (12MP)
- 제어 유닛 : LKAS ECU
- 액추에이터 : 전동식 파워 스티어링(EPS) 모터, 조향 보조 액추에이터
- 통신 인터페이스 : Automotive Ethernet , V2X, CAN-FD

1.3 개발 단계 및 일정

단계	기간	주요활동	산출물
컨셉 단계	2025	요구사항 정의, TARA 수행	사이버보안 컨셉
제품 개발	2025	설계, 구현, 통합	사이버보안 구현
검증/검수	2025	테스트, 평가, 승인	사이버보안 검증
생산	2025	양산, 모니터링	사이버보안 모니터링

2. 아이템 정의

2.1 LKAS 경계 및 외부 인터페이스

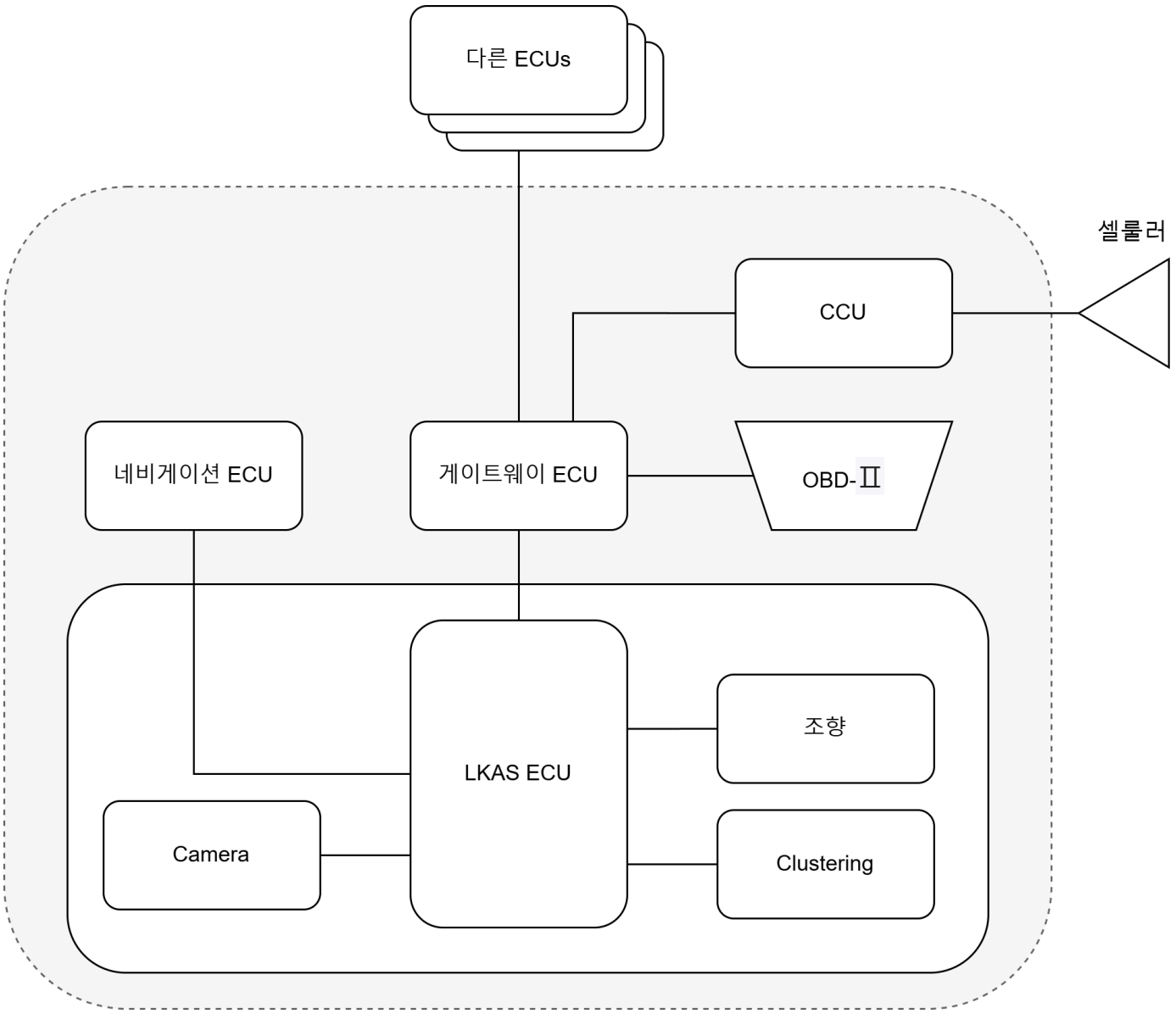
시스템 경계	전방 카메라 입력부터 조향 보조(EPS 액추에이터) 제어까지
제외 항목	● 종방향 제어 시스템(ACC, AEB) ● 엔진 제어 ● 변속기 제어 ● 차량 자세 제어 장치(Electronic Stability Control, ESC) ● 기타 차선 유지와 직접 관련 없는 기능
운영 조건	● 속도 60-180km/h ● 명확한 차선이 존재하는 도로 ● 전천후 조건(극단적 시야 제한 제외)

2.2 외부 인터페이스

인터페이스	프로토콜	데이터 유형	보안 요구사항
전방 카메라	LVDS 또는 Automotive Ethernet	영상 데이터, 차선 인식 정보	데이터 무결성/가용성: 센서 데이터 인증 및 이상 탐지
조향 모듈	CAN-FD 또는 내부 통신	조향 제어 명령 (토크)	명령 무결성/인증: LKAS ECU로부터의 제어 명령 인증 및 재생 방지
게이트웨이 ECU	CAN-FD, Automotive Ethernet	차량 상태 (차속, 요율 등), 센서/제어 신호	접근 제어/통신 무결성: 비정상 트래픽 필터링, 방화벽, 메시지 인증 및 암호화
네비게이션 ECU	CAN/Ethernet	지도 기반 보조 정보, 도로 곡률	데이터 무결성: 수신하는 도로 예측 정보의 인증 및 무결성 검증
CCU/셀룰러 모듈	셀룰러 (LTE/5G), V2X	OTA 업데이트, 원격 진단 요청, V2X 정보	원격 접근 인증/인가/기밀성: 원격 통신 채널 종단 간 암호화, 접근 제어, 안전한 OTA 메커니즘
OBD-II 포트	UDS on CAN / DoIP	진단 데이터, 펌웨어	접근 제어/인증: 물리적 연결 시 강력한 인증 및 인가, 진단 세션 관리
GNSS 수신기	별도 GNSS 통신	차량 위치/속도 데이터	데이터 무결성/인증: 위치 정보 스푸핑 방지 및 신호 인증

2.3 주요 기능

- 차선 인식: 전방 카메라 및 Clustering을 통한 차선 중심 및 도로 형상 인식
- 조향 제어: LKAS ECU가 차선 유지 제어 알고리즘을 실행하여 조향각 명령 생성
- 운전자 경고: 시각·청각·햅틱 경고를 통한 차선 이탈 위험 알림
- 차량 정보 수집: 게이트웨이를 통해 속도·요율 등 주행 정보 수집
- 시스템 감시: 센서 상태, 조향 모듈 동작, 통신 품질을 실시간 모니터링 및 Fail-safe 수행
- 원격 연동: CCU를 통한 OTA 업데이트 및 진단 지원



2.4 ASIL 레벨 요구사항

LKAS 시스템의 오작동은 차량의 차로 유지 기능 저하나 경미한 차선 이탈을 초래할 수 있으나, 즉각적으로 치명적인 사고로 이어질 가능성은 상대적으로 낮습니다.
또한, 시스템 고장 시 운전자가 조향을 통해 상황을 일정 수준 제어할 수 있는 여지가 존재합니다. 이러한 점을 고려할 때 LKAS는 중간 수준의 안전 무결성이 요구되는 기능으로 분류되며, 이에 따라 ASIL B가 적용됩니다.

3. 자산 식별(Asset Identification)

자산 **ID**	자산명	기밀성	무결성	가용성	설명
A-01	Camera(전방 카메라 센서)	Very High	High	High	LKAS 차선 인식, 객체 탐지를 위한 핵심 센서
A-02	LKAS ECU	Very High	High	High	차선 유지 제어, 조향 명령 생성
A-03	조향 모듈(Steering Actuator)	Low	High	High	LKAS 제어 명령을 실제 조향으로 변환
A-04	Clustering 모듈	Medium	Very High	High	영상/센서 기반 Lane/Edge/클러스터 분석
A-05	게이트웨이 ECU	Very High	High	High	차량 내부망과 LKAS ECU 연결, CAN·Ethernet 라우팅
A-06	내비게이션 ECU	Medium	Very High	Medium	지도 기반 보조 정보 제공
A-07	OBD-II 포트	Medium	High	Very High	진단용 인터페이스. 공격자가 내부 네트워크 진입 가능
A-08	CCU (텔레매틱스 ECU) + 셀룰러 모듈	Very High	High	High	원격 통신, OTA, V2X 정보 수신. 외부 공격에 가장 많이 노출
A-09	CAN / Ethernet 메시지	Very High	Low	High	차량 상태/센서 데이터/제어 신호 전달
A-10	LKAS ECU 내부 SW/알고리즘	Very High	High	High	차선 판단 알고리즘, 제어 로직, 파라미터
A-11	차량 위치/속도 데이터	Medium	High	High	LKAS 제어의 필수 입력(차속, 요율 등)

3.1 자산별 상세 설명

A-01: Camera (전방 카메라 센서**)**
LKAS의 차선 인식 및 객체 탐지를 위한 핵심 센서 자산입니다. 환경 인식을 위한 원본 영상 데이터와 처리된 차선 정보를 제공하며, 이 데이터의 무결성과 가용성은 LKAS 제어의 정확성과 안전에 결정적입니다. 센서 기만(Spoofing) 공격에 취약할 수 있으며, 고장 시 운전자에게 차선 유지 기능을 제공할 수 없어 Critical한 무결성 및 가용성이 요구됩니다.

A-02: LKAS ECU
LKAS 시스템의 주 제어 유닛입니다. 전방 카메라 데이터를 입력받아 차선 유지 제어 알고리즘(A-10)을 실행하고 조향 모듈(A-03)로 조향 명령을 생성하여 전송합니다. 시스템의 핵심 제어 로직을 담고 있어, 이 자산의 기밀성, 무결성, 가용성 모두가 Critical하게 관리되어야 합니다. 무단 접근이나 펌웨어 변조는 즉각적인 차량 제어 오작동으로 이어질 수 있습니다.

A-03: 조향 모듈**(Steering Actuator)**
LKAS ECU로부터 수신된 조향 제어 명령(토크)을 실제 물리적인 조향 보조 액추에이터 동작으로 변환하는 최종 실행 장치입니다. 제어 명령의 무결성과 기능의 가용성이 Critical하며, 비인가된 명령이 주입되면 운전자의 의도와 무관하게 차량이 급격히 조향될 수 있습니다.

A-04: Clustering 모듈
전방 카메라 센서(A-01)에서 수신한 영상/센서 데이터를 기반으로 차선(Lane), 도로 경계(Edge), 객체 클러스터 등을 분석하는 소프트웨어 모듈입니다. LKAS의 판단에 필수적인 분석 정보를 제공하며, 특히 시스템의 상태를 운전자에게 알리는 경고 신호와 연관되어 있어 무결성(High)과 가용성(Critical)이 중요합니다.

A-05: 게이트웨이 **ECU**
차량 내부 통신망(CAN·Ethernet)의 중심 허브로서, LKAS ECU와 다른 도메인 ECU들을 연결하고 트래픽을 라우팅합니다. 외부 네트워크(CCU, OBD-II)에서 유입되는 트래픽을 필터링하여 LKAS 도메인을 보호하는 보안 핵심 자산입니다. Critical한 무결성과 가용성 확보를 통해 네트워크 DoS 공격 및 보안 정책 우회 위협을 방지해야 합니다.

A-06: 내비게이션 **ECU**
LKAS 제어를 보조하기 위해 지도 기반의 전방 도로 곡률, 제한 속도 등의 예측 정보를 제공합니다. 제공되는 데이터의 무결성(High)이 보장되어야 급커브 구간에서의 직선 주행 오판과 같은 위험을 방지할 수 있습니다.

A-07: OBD-II 포트

차량의 진단 및 펌웨어 업데이트를 위한 물리적 인터페이스입니다. 차량 내부 네트워크로의 잠재적 진입점이 될 수 있어, 공격자가 이를 통해 내부 네트워크에 침입하여 메시지 주입이나 ECU 펌웨어 변조를 시도할 수 있습니다. 진단 중에도 Critical한 명령 무결성 관리가 요구됩니다.

A-08: CCU (텔레매틱스 **ECU) +** 셀룰러 모듈

OTA 업데이트, 원격 진단 요청, V2X 정보 수신 등 외부와의 무선 통신을 담당하는 자산입니다. 외부 네트워크에 가장 많이 노출되어 원격 명령 실행 등 원격 공격의 진입점이 될 위험이 높습니다. 통신 채널의 기밀성, 무결성, 가용성 모두 Critical하게 관리되어야 합니다.

A-09: CAN / Ethernet 메시지

차량 내부에서 LKAS ECU, 조향 모듈, 카메라 등이 주고받는 센서 데이터, 제어 신호, 차량 상태 정보 등의 통신 메시지 자체입니다. 이 메시지들의 무결성과 가용성이 훼손되면(도청 및 재생, DoS 공격 등) LKAS 기능이 직접적으로 오작동하거나 마비되므로 Critical한 보호가 필요합니다.

A-10: LKAS ECU 내부 **SW/**알고리즘

차선 판단 알고리즘, 조향 제어 로직, 파라미터 등 LKAS의 핵심 기능을 구현하는 소프트웨어 및 데이터를 포함합니다. 이 자산의 무결성이 훼손되면 시스템의 근본적인 제어 로직이 공격자 의도대로 변경되어 심각한 위험을 초래할 수 있으므로 Critical하게 관리되어야 합니다.

A-11: 차량 위치**/**속도 데이터

GNSS 수신기 및 다른 ECU로부터 수신되는 차량의 현재 위치(GPS), 속도, 요율 등의 주행 정보입니다. LKAS 제어의 필수 입력 데이터이며, 스푸핑(Spoofing) 공격 등으로 이 데이터의 신뢰성(무결성/가용성)이 훼손될 경우 LKAS의 작동 조건 판단이나 제어에 치명적인 오류를 유발할 수 있습니다.

4. 위협 시나리오 식별

위협 ID	위협 시나리오	대상 자산	위협 설명
T-01	카메라 센서 기만 (Spoofing)	A-01 (Carmera)	공격자가 카메라 센서에 강한 빛(레이저)를 비추거나 가짜 차선 이미지(프로젝터 등)를 투사하여, LKAS가 차선을 오인식하게 만들어 의도치 않는 조향을 유발함
T-02	네비게이션 예측 정보 변조	A-06, A-11 (내비게이션 ECU, 차량 위치/속도 데이터)	네비게이션이 제공하는 전방 도로의 곡률이나 제한 속도 정보를 변조하여, 급커브 구간에서 LKAS가 감속하지 않고 직선 주행하도록 유도함
T-03	위치 정보 스푸핑	A-11 (차량 위치/속도 데이터)	외부에서 위조된 GPS 신호를 송신하여 차량이 자신의 위치를 고속도로가 아닌 일반 도로로 착각하게 만들어, LKAS 작동 조건을 강제로 해제하거나 오작동시킴.
T-04	게이트웨이 보안 정책 우회	A-05 (게이트웨이 ECU)	CCU나 OBD-II에서 유입되는 비정상 트래픽을 차단해야 할 게이트웨이의 필터링 규칙을 우회하거나 무력화하여, 외부의 공격 패킷을 LKAS 도메인으로 침투시킴.
T-05	CAN 메시지 도청 및 재생 (Sniffing & Replay)	A-09 (CAN / Ethernet 메시지)	공격자가 내부 네트워크에 침투하여 정상적인 조향 명령 패킷을 도청(Sniffing)한 뒤, 이를 나중에 재전송(Replay)하여 운전자 의도와 무관하게 핸들을 조작함.
T-06	차량 네트워크 DoS 공격	A-05	공격자가 대량의 더미 데이터를 네트워크에 폭주

		(게이트웨이 ECU)	시켜 Camera에서 LAKS ECU로 가는 차선 정보나 LKAS ECU에서 조향 장치로 가는 제어 신호 전달을 지연 또는 차단함
T-07	원격 명령 실행	A-08 (CCU)	셀룰러 네트워크를 통해 CCU(Communication Control Unit)의 취약점을 공격하여, 외부에서 원격으로 차량 내부 네트워크에 접근하고 악성 명령을 전달
T-08	클러스터 경고 알림 차단	A-04 (Clustering)	LKAS 시스템의 고장 또는 해제 상태를 알리는 경고등 신호를 차단하여, 운전자가 시스템이 정상 작동 중이라고 오인하게 만듦
T-09	LKAS ECU 제어 명령 변조	A-02 (LKAS ECU)	CAN/Ethernet을 통해 LKAS ECU로 전달되는 조향 제어 신호를 공격자가 변조하여, 차량이 의도치 않은 방향으로 조향되도록 함. 유지 조향 기능이 공격자 의도대로 조작될 수 있음
T-10	LKAS ECU 펌웨어 무결성 변조	A-02 (LKAS ECU), A-10 (LKAS ECU 내부 알고리즘)	공격자가 OTA 또는 진단 포트(OBD-II)를 통해 LKAS ECU의 펌웨어(SW/알고리즘)를 변조하거나 악성 코드를 주입하여, 차선 유지 제어 로직을 영구적으로 변경하거나 오작동을 유발함.
T-11	조향 모듈 제어 명령 권한 우회	A-03 (조향 모듈), A-09 (CAN/Ethernet 메시지)	게이트웨이 ECU를 우회하거나 조향 모듈과의 통신 채널에 접근한 공격자가 LKAS ECU의 인증된 명령 없이 직접 조향 명령(토크)을 주입하여 차량을 무단 조작함.
T-12	V2X 정보 변조를 통한 제어	A-08 (CCU), A-09	V2X (차량-사물 통신) 채널을 통해 수신되는 주변

	오작동	(CAN/Ethernet 메시지)	차량/인프라 정보를 변조하여, LKAS 시스템이 차로 상황이나 주변 환경을 잘못 판단하게 만들어 불필요하거나 급격한 조향을 유발함.
T-13	운전자 경고등 작동불가	A-04 (Clustering 모듈), A-09 (CAN/Ethernet 메시지)	(T-08과 유사하나 근본적인 원인 공격) LKAS 시스템은 고장 시 운전자에게 경고해야 하나, 공격자가 HMI(Human-Machine Interface) 시스템과 통신하는 메시지를 차단하거나 조작하여, LKAS 시스템이 고장 났음에도 운전자가 이를 인지하지 못하게 만듦. (T-08은 경고 알림 차단, T-12는 고장 알림 자체를 방지하는 더 포괄적인 공격)
T-14	LKAS 내부 제어 알고리즘 변조	A-10 (LKAS ECU 내부 SW/알고리즘)	악성 업데이트 또는 내부자 공격으로 LKAS 알고리즘이 조작되면, 조향 판단 로직 자체가 공격자 의도대로 동작하여 매우 높은 위험을 초래함
T-15	OBD-II 포트 불법 접근 및 메시지 주입	A-07 (OBD-II 포트)	공격자가 차량 내부에 접근해 OBD 포트를 통해 진단 프로토콜(UDS)을 이용하면, ECU 정보 조회·제어 명령 주입 등이 가능해 차량의 정상 주행을 방해할 수 있음

4.1 주요 위협 시나리오 상세 분석

T-01 카메라 센서 기만:

공격자가 고해상도 프로젝터, 레이저, 또는 도로 위 위조 표시(테이프, 페인트)를 사용하여 전방 카메라 센서에 가짜 차선 이미지를 주입하거나 강한 광원으로 시각 정보를 교란합니다. 이로 인해 LKAS 시스템이 실제 주행 차선이 아닌 허위 차선을 정상 경로로 오인식하게 만들어, 의도치 않은 급격한 조향을 유발하여 차선 이탈 및 충돌 사고를 야기하거나, 곡선로에서 차선을 감지하지 못해 조향 보조 기능을 무력화시킬 수 있습니다.

T-02 내비게이션 예측 정보 변조:

공격자는 네비게이션 ECU가 사용하는 도로 곡률, 경사, 제한 속도, 차선 수 등의 예측 정보가 저장된 내부 DB 또는 외부 지도 서버에 접근하여, 전방 도로 형상 정보를 의도적으로 변조합니다.
이 과정은 차량 내부 네트워크 침투, OTA 업데이트 경로 탈취, 네비게이션 맵 데이터 위변조, 혹은 통신 구간(예: TCU ↔ 지도 서버) 공격을 통해 이루어질 수 있습니다.

T-03 위치 정보 스푸핑:

공격자는 차량 주변에 GNSS(GPS) 신호 발생 장치를 설치하거나 이동식 스푸퍼를 사용하여, 차량이 실제 주행 위치와 다른 좌표를 수신하도록 조작합니다.
이 공격은 GNSS가 기본적으로 암호화되지 않은 민간 신호를 사용하는 구조적 취약점을 이용하며, 비교적 낮은 비용으로도 실행 가능한 위험한 유형입니다.

T-04 게이트웨이 보안 정책 우회:

게이트웨이 ECU(A-05)는 차량 내부 네트워크의 중심 허브로, 외부에서 유입되는 CAN/Ethernet 트래픽을 필터링하고, LKAS와 같은 안전 도메인으로의 접근을 차단하는 핵심 보안 기능을 담당합니다다.
그러나 공격자는 CCU(텔레매틱스 ECU) 또는 OBD-II 포트와 같이 게이트웨이 외부 인터페이스와 연결된 지점을 악용하여, 게이트웨이의 필터링 정책을 우회하거나 비활성화하도록 조작할 수 있습니다.

T-05 CAN 메시지 도청 및 재생 :

공격자가 텔레매틱스 유닛(CCU) 해킹이나 OBD-II 포트 접근을 통해 차량 내부 네트워크에 침투한 후, LKAS ECU가 전송하는 정상적인 조향 제어 패킷을 도청하여 수집합니다. 이후 공격자는 수집된 조향 명령을 악의적인 시점에 재전송하며, 별도의 신선도(Freshness) 검증이 없는 조향 액추에이터가 이를 현재의 유효한 명령으로 수락하게 만듭니다. 이로 인해 운전자의 제어 의도와 무관하게 핸들이 급격히 조작되어, 고속 주행 중 차량이 차선을 이탈하거나 장애물과 충돌하는 심각한 사고를 야기할 수 있습니다.

T-06 차량 네트워크 DoS 공격:

공격자가 게이트웨이 ECU의 취약점을 악용하거나, 차량 내부의 취약한 ECU 혹은 OBD-II 포트를 통해 물리적으로 침입하여 차량 내부 통신망에 접근합니다. 침입 후, 공격자는 CAN / Ethernet 메시지버스를 대상으로 대량의 더미 데이터를 지속적으로 주입하거나, 높은 우선순위를 가진 메시지를 악의적으로 반복 전송하여 네트워크 대역폭을 고갈시킵니다. 이로 인해 전방 카메라에서 LKAS ECU로 전송되는 실시간 차선 인식 데이터, 그리고 LKAS ECU에서 조향 장치로 전송되는 긴급한 제어 명령이 지연되거나 완전히 손실됩니다. 결과적으로 LKAS 시스템의 실시간 제어 기능이 마비되어 차선 유지 또는 조향 보조 기능이 제때 작동하지 못하고 운전자가 차량 제어권을 상실하는 심각한 상황이 발생할 수 있습니다.

T-07 원격 명령 실행:

공격자가 셀룰러 네트워크를 통해 차량의 CCU에 원격으로 접속하여 통신 프로토콜의 취약점이나 인증 메커니즘을 우회합니다. 차량 내부 네트워크에 대한 제어 권한을 획득한 공격자는 게이트웨이를 거쳐 LKAS ECU로 위조된 조향 제어 명령을 전송합니다. 이는 운전자의 의지와 무관하게 핸들을 임의로 조작하거나 고속 주행 중 차선 유지 기능을 강제로 해제시켜, 도로 이탈 또는 주변 차량과의 충돌과 같은 심각한 사고를 야기할 수 있습니다.

T-08 클러스터 경고 알림 차단:

공격자는 LKAS 기능의 고장, 비정상 상태, 또는 임의 해제가 발생했을 때 계기판(Cluster)에 표시되어야 하는 경고등·경고 메시지를 의도적으로 차단하여, 운전자가 시스템 이상을 즉시 인지하지 못하게 만듭니다다.
이 공격은 차량 내부 네트워크(CAN/Ethernet)를 통한 메시지 변조, 게이트웨이 필터링 우회, Cluster ECU 자체 공격, 또는 LKAS ECU에서 Cluster로 전달되는 경고 신호의 ID/데이터 페이로드 조작을 통해 수행될 수 있습니다.

T-09 LKAS ECU 펌웨어 무결성 변조:

공격자는 차량의 CCU(텔레매틱스 ECU) 또는 OBD-II 포트 와 같은 외부 인터페이스를 진입점으로 사용하여, LKAS ECU의 펌웨어 업데이트 채널이나 진단 채널에 접근합니다. 공격자는 이 채널의 보안 취약점을 악용하여 LKAS ECU 의 제어 알고리즘이나 운영 소프트웨어 를 악성 코드가 포함된 변조된 펌웨어로 교체합니다. 이로 인해 LKAS 시스템이 차선 인식 및 조향 제어 로직을 오작동하게 만들거나, 특정 조건에서 운전자의 개입을 무시하고 차량을 위험하게 조작할 수 있는 백도어를 시스템에 영구적으로 심을 수 있습니다.

T-10 조향 모듈 제어 명령 권한 우회:

LKAS ECU 는 차선 유지 제어를 위해 조향 모듈(Steering Actuator) 로 조향 제어 명령(토크)을 전송합니다. 공격자는 내부 네트워크(CAN/Ethernet 메시지) 에 침투한 후, LKAS ECU의 명령이 아닌 위조된 조향 명령 패킷을 조향 모듈로 직접 주입합니다. 만약 조향 모듈이 수신된 명령의 출처(LKAS ECU) 또는 적법성을 검증하지 못한다면, 운전자의 의지와 무관하게 조향 보조 액추에이터가 작동하여 차량이 급격하게 차로를 이탈하거나 충돌 사고를 야기할 수 있습니다.

T-11 V2X 정보 변조를 통한 제어 오작동:

LKAS 시스템은 CCU/셀룰러 모듈 을 통해 V2X(차량-사물 통신) 정보를 수신하여 주행 보조에 활용할 수 있습니다. 공격자는 무선 통신 채널 을 통해 전송되는 주변 차량의 위치, 속도, 또는 도로 인프라가 제공하는 차선 및 교통 정보를 가로채거나 위조하여 CCU에 주입합니다. LKAS ECU는 변조된 V2X 정보 를 신뢰하고 잘못된 차로 유지 판단(예: 실제로는 안전하지만, V2X 정보 변조로 인해 급격한 조향 회피를 시도)을 내리게 되어, 불필요하거나 위험한 수준의 조향 보조 를 유발하여 사고 위험을 높입니다.

T-12 운전자 경고등 작동 불가 (HMI 무력화):

LKAS 시스템은 시스템 고장, 센서 상태 이상, 또는 통신 품질 저하 발생 시 운전자에게 시각/청각/햅틱 경고 를 통해 위험을 알려야 합니다. 공격자는 게이트웨이 ECU 나 내부 네트워크 를 경유하여, LKAS ECU 또는 Clustering 모듈 에서 운전자 경고등 신호를 담당하는 CAN/Ethernet 메시지 를 목표로 공격합니다. 이 메시지들을 차단하거나 조작하여, 시스템이 위험한 상태(예: 차선 인식 알고리즘 고장, 센서 기만 상황)임에도 불구하고 운전자에게 경고 신호가 도달하는 것을 완전히 방지합니다. 이는 운전자가 시스템이 정상 작동 중이라고 오인하게 만들어 위험 상황에 대한 적절한 조치를 취할 기회를 박탈함으로써 사고 위험을 증대시킵니다.

T-13 운전자 경고등 작동불가:

공격자는 LKAS 시스템의 고장이나 비정상 상태를 운전자에게 전달해야 하는 HMI(Human-Machine Interface) 경고 체계 전체를 무력화하여, 운전자가 시스템이 고장났거나 비활성화된 사실을 전혀 인지하지 못하게 만듭니다다.

이는 단순히 특정 경고 메시지만 차단하는 T-08보다 더 광범위하며, 경고를 생성하는 상위 로직, Cluster 모듈, 그리고 HMI로 전달되는 CAN/Ethernet 메시지를 포괄적으로 조작하여 이루어집니다.

T-14 LKAS 내부 제어 알고리즘 변조:

공격자는 OTA 업데이트 서버 공격, ECU 내부 플래시 메모리 조작, 악성 소프트웨어 주입, 혹은 내부자 접근 권한을 악용하여 LKAS ECU 내부의 조향 알고리즘(차선 인식 로직, 조향 토크 계산, Track-keeping 로직 등)을 변조합니다.

변조된 알고리즘은 정상적인 차량 주행 조건에서도 의도적으로 과도한 조향 값을 출력하거나, 특정 상황에서 조향 보조 기능을 비활성화하도록 설계될 수 있습니다.

T-15 OBD-II 포트 불법 접근 및 메시지 주입:

공격자가 물리적으로 차량 내부에 접근해 OBD-II 진단 포트에 장비를 연결하면, 표준 진단 프로토콜(UDS, KWP2000 등)을 사용하여 ECU 상태 조회뿐 아니라 특정 조건에서 ECU 제어 명령까지 직접 주입할 수 있습니다.

5. 영향도 평가

위협ID	위협 시나리오	Safety	Financial	Operational	Privacy	전체 심각도
T-01	카메라 센서 기만	Severe	Major	Severe	Moderate	Severe
T-02	네비게이션 예측 정보 변조	Severe	Moderate	Major	Moderate	Severe
T-03	위치 정보 스푸핑	Severe	Moderate	Major	Moderate	Severe
T-04	게이트웨이 보안 정책 우회	Severe	Major	Severe	Moderate	Severe
T-05	CAN 메시지 도청 및 재생	Severe	Major	Severe	Moderate	Severe
T-06	차량 네트워크 DoS 공격	Severe	Major	Severe	Moderate	Severe
T-07	원격 명령 실행	Severe	Severe	Severe	Severe	Severe
T-08	클러스터 경고 알림 차단	Severe	Moderate	Moderate	Moderate	Severe
T-09	LKAS ECU 제어 명령 변조	Severe	Severe	Severe	Severe	Severe
T-10	LKAS ECU 펌웨어 무결성 변조	Severe	Severe	Severe	Moderate	Severe
T-11	조향 모듈 제어 명령 권한 우회	Severe	Severe	Severe	Severe	Severe
T-12	V2X 정보	Severe	Moderate	Severe	Severe	Severe

	변조를 통한 제어 오작동					
T-13	운전자 경고등 작동불가	Severe	Severe	Severe	Severe	Severe
T-14	LKAS 내부 제어 알고리즘 변조	Severe	Moderate	Severe	Severe	Severe
T-15	OBD-II 포트 불법 접근 및 메시지 주입	Severe	Severe	Severe	Severe	Severe

5.1 영향도 평가 기준

- Safety

Impact Rating	Criteria for Safety Impact Rating	Value
극심함(Severe)	Life-threatening injuries (survival uncertain), fatal injuries	100
심각함(Major)	Severe and life-threatening injuries (survival probable)	10
보통(Moderate)	Light and moderate injuries	1
무시할만함(Negligible)	No injuries	0

- Financial

Impact Rating	Criteria for Financial Impact Rating	Value
극심함(Severe)	The financial damage leads to catastrophic consequences which the affected stakeholder might not overcome.	100
심각함(Major)	The financial damage leads to substantial consequences which the affected stakeholder will be able to overcome.	10
보통(Moderate)	The financial damage leads to inconvenient consequences which the affected stakeholder will be able to overcome with limited resources.	1
무시할만함(Negligible)	The financial damage leads to no effect, negligible consequences or is irrelevant to the stakeholder	0

- Operational

Impact Rating	Criteria for Operational Impact Rating	Value
극심함(Severe)	The operational damage leads to a vehicle not working, from non-intended operation up to the vehicle being non-operational.	100
심각함(Major)	The operational damage leads to the loss of a vehicle function.	10
보통(Moderate)	The operational damage leads to partial degradation of a vehicle function or performance.	1
무시할만함(Negligible)	The operational damage leads to no effect or indiscernible degradation of a vehicle function or performance.	0

- Privacy

Impact Rating	Criteria for Privacy Impact Rating	Value
극심함(Severe)	The privacy damage leads to significant or even irreversible impact to the road user. In this case, the information regarding the road user is highly sensitive and easy to link to a PII principal.	100
심각함(Major)	The privacy damage leads to serious impact to the road user. In this case, the information regarding the road user is: a) highly sensitive and difficult to link to a PII principal, or b) sensitive and easy to link to a PII principal.	10
보통(Moderate)	The privacy damage leads to significant inconveniences to the road user. In this case, the information regarding the road user is: a) sensitive but difficult to link to a PII principal, or b) not sensitive but easy to link to a PII principal.	1
무시할만함(Negligible)	The privacy damage leads to no effect or can create few inconveniencies to the road user. In this case, the information regarding the road user is not sensitive and difficult to link to a PII principal.	0

총 심각도	최소 점수
없음(None)	0
무시할만함(Negligible)	1
보통(Moderate)	20
심각함(Major)	100
극심함(Severe)	1000

6. 공격 경로 분석

6.1 주요 공격 시나리오별 상세 경로

공격 시나리오	1단계: 진입점	2단계: 측면 이동	3단계: 목표 접근	4단계: 영향 실행
T-01: 카메라 센서 기만	차량 근처에서 시각적 공격 장비 배치	전방 카메라 센서 시야 확보	고강도 빛(레이저) 또는 가짜 이미지 투사	LKAS의 차선 인식 오작동 유발
T-02: 네비게이션 예측 정보 변조	네비게이션 맵 업데이트 경로 침투	지도 DB 변조 / 속도·곡률 정보 조작	LKAS 경로 예측 모듈 접근	급커브 구간에서 직선 주행 오판 유도
T-03: GPS 위치 스푸핑	외부 GNSS 스푸핑 장치 설치	차량 GPS 수신 신호를 위조	차량 위치·속도 판단 로직 교란	LKAS 작동 조건 변경/오작동 유발
T-04: 게이트웨이 보안 정책 우회	CCU or OBD-II 진입	게이트웨이 필터링 우회	LKAS 도메인 통신 접근	악성 패킷 LKAS ECU 전달
T-05: CAN 메시지 도청 및 재생	OBD-II 포트를 통한 CAN 버스 접근	LKAS 관련 CAN 메시지 식별	도청된 메시지 분석 및 위조/재전송	운전자 의도와 무관한 조향 제어 명령 재실행
T-06: 차량 네트워크 DoS 공격	CCU 또는 OBD-II 포트 접근	CAN/FlexRay 포트로 대량 메시지 주입	LKAS 데이터 경로 포화	LKAS 제어 신호 지연·차단
T-07: 원격 명령 실행	CCU 셀룰러 네트워크 침투	게이트웨이 보안 정책 우회	LKAS ECU 네트워크 접근	위조된 조향 명령 전송으로 무단 조향 실행
T-08: 클러스터 경고 알림 차단	OBD-II 또는 게이트웨이 우회	HMI 관련 메시지 가로채기	Cluster 모듈 접근	경고등 표시 차단 → 운전자 오인

T-09: LKAS ECU 제어 명령 변조	OBD-II 또는 내부 네트워크 침투	CAN 조향 신호 위·변조	LKAS ECU 명령 채널 접근	비의도적 조향 명령 실행
T-10: LKAS ECU 펌웨어 무결성 변조	OTA 서버 침투 / OBD-II 접근	악성 펌웨어 파일 주입	LKAS ECU 플래시 메모리 접근	조향 알고리즘 영구 변조·오작동 발생
T-11: 조향 모듈 제어 권한 우회	게이트웨이 우회 또는 물리 접근	조향 모듈 통신 채널 장악	액추에이터 명령 인터페이스 접근	직접 조향 토크 주입 → 차량 무단 조작
T-12: V2X 정보 변조	외부 V2X 송신 장치 설치	CCU가 수신하는 V2X 메시지 위조	LKAS 판단 로직 접근	잘못된 주변 상황 인지 → 급격한 조향 유도
T-13: 운전자 경고등 작동불가	게이트웨이 우회 또는 OBD-II	HMI 메시지 조작·차단	Cluster/HMI 모듈 접근	LKAS 고장 숨김 → 운전자 오판으로 사고 위험 증가
T-14: LKAS 내부 제어 알고리즘 변조	OTA 서버 해킹 / 진단 포트 접근	악성 SW 주입 경로 확보	LKAS 알고리즘 메모리 접근	조향 로직 변조 → 지속적 오작동 발생
T-15: OBD-II 포트 불법 접근	물리적으로 OBD-II 포트 연결	UDS 명령 및 CAN 메시지 주입	LKAS ECU/조향 모듈 접근	조향 신호 변조·제어 방해

6.2 공격 표면(Attack Surface) 분석

- 물리적 접근 경로: OBD-II 포트, USB 포트, 진단 커넥터
- 무선 통신 경로: 셀룰러(4G/5G), V2X(DSRC/5G), OTA 업데이트 채널
- 센서 공격 경로: 시각적 스푸핑(가짜 차선 이미지), 광학 교란(레이저/LED), GPS 스푸핑
- 네트워크 통신 경로: CAN-FD 메시지, Automotive Ethernet, Gateway ECU 경유 통신
- 소프트웨어 업데이트 경로: OTA 업데이트 서버, ECU 펌웨어 업데이트 채널
- HMI 정보 전달 경로: 클러스터 경고 메시지, 상태 표시 데이터 흐름

7. 공격 가능성 평가

위협ID	전문성	지식	장비	시간	전체 가능성
T-01	Medium	Medium	Low	Medium	Medium
T-02	Medium	Medium	Low	High	Medium
T-03	Low	Medium	Medium	Medium	Medium
T-04	High	High	Medium	High	High
T-05	Medium	Medium	Medium	Medium	Medium
T-06	Medium	Low	Medium	Low	Medium
T-07	High	High	High	Medium	High
T-08	Medium	Medium	Low	Medium	Medium
T-09	High	High	Medium	High	High
T-10	High	High	High	High	Very High
T-11	High	High	Medium	High	High
T-12	Medium	High	Medium	Medium	High
T-13	Medium	Medium	Low	Medium	Medium
T-14	Very High	Very High	High	High	Very High
T-15	Low	Medium	Low	Low	Medium

7.1 평가 기준 정의

- 전문성 (Expertise): 공격 수행에 필요한 기술적 전문성 수준
- 지식 (Knowledge): 대상 시스템에 대한 구체적 지식 요구 수준
- 장비 (Equipment): 공격 수행에 필요한 장비의 접근성 및 비용
- 시간 (Time): 공격 수행에 소요되는 시간 및 지속성

8. 리스크 결정

8.1 리스크 매트릭스

위협ID	영향도	공격 가능성	리스크 레벨	우선순위
T-01	Severe	Medium	High	3
T-02	Severe	Medium	High	3
T-03	Severe	Medium	High	3
T-04	Severe	High	Very High	2
T-05	Severe	Medium	High	3
T-06	Severe	Medium	High	3
T-07	Severe	High	Very High	2
T-08	Severe	Medium	High	3
T-09	Severe	High	Very High	2
T-10	Severe	Very High	Very High	1
T-11	Severe	High	Very High	2
T-12	Severe	High	Very High	2
T-13	Severe	Medium	High	3
T-14	Severe	Very High	Very High	1
T-15	Severe	Medium	High	3

8.2 고위험 항목 상세 분석

재평가된 리스크 분석 결과, LKAS 시스템의 기능 안전(Safety)과 운영(Operational)에 치명적인 영향을 미치는 Severe 영향도를 가지면서, 공격 가능성이 High 또는 Medium 이상인 위협들이 고위험 항목으로 분류되었습니다. 이들 항목은 완화 조치 구현에 있어 최우선 순위를 가집니다.

8.2.1 최우선 대응 필요 항목 (Very High Risk, P1)

이 위협들은 공격 수행이 비교적 용이(High Possibility)하며, 성공 시 운전자에게 치명적인 결과(Severe Impact)를 초래하므로 가장 시급한 대응이 필요합니다. 물리적 접근 경로(OBD-II), 통신 메시지 무결성 위협, 운전자 경고 무력화 등 핵심 보안 요소에 대한 공격이 여기에 포함됩니다.

위협 **ID**	위협 시나리오	핵심 위험 및 필요 대응 방안
T-04	게이트웨이 보안 정책 우회	위험**:** 게이트웨이 필터링 규칙을 무력화하여 CCU나 OBD-II 등 외부 진입점을 통한 악성 패킷이 LKAS 도메인으로 침투하도록 허용합니다. 대응**:** 게이트웨이 ECU의 방화벽(Filtering) 규칙 강화, 비정상 트래픽 모니터링 및 필터링 (CSR-03)
T-07	원격 명령 실행	위험**:** 셀룰러 네트워크를 통해 CCU의 취약점을 공격하여 원격으로 차량 내부 네트워크에 접근해 악성 조향 제어 명령을 전달합니다. 대응**:** 원격 통신 채널(CCU) 종단 간 암호화(End-to-End Encryption), 강력한 접근 인증 및 인가 (CSR-05)
T-09	LKAS ECU 제어 명령 변조	위험**:** LKAS ECU로 전달되는 조향 제어 신호를 변조하여 차량이 의도치 않은 방향으로 조향되도록 합니다.대응**:** CAN/Ethernet 메시지 인증 코드(MAC) 및 수신 패킷의 신선도 검증 적용, E2E 보호 프로토콜 구현 (CSR-02, CSR-06)
T-10	LKAS ECU 펌웨어 무결성 변조	위험**:** OTA나 진단 포트를 통해 펌웨어를 변조하여 LKAS 제어 로직을 영구적으로 변경하거나 악성 코드를 심습니다.대응**:** HSM 기반 안전 부팅 적용, 펌웨어 디지털 서명 검증, JTAG/디버그 포트의 물리적/소프트웨어적 비활성화 (CSR-07)
T-11	조향 모듈 제어 명령 권한 우회	위험**:** LKAS ECU의 인증 없이 조향 모듈(액추에이터)로 직접 조향 명령(토크)을 주입하여 차량을 무단 조작합니다.대응**:** 게이트웨이 방화벽을 통한 비인가 메시지 필터링, 조향 모듈단에서의 소스 인증, 비정상 토크 명령에 대한 임계치 제한 구현 (CSR-03)

T-12	V2X 정보 변조를 통한 제어 오작동	위험: V2X 통신을 통해 수신되는 주변 환경 정보를 위조하여 LKAS가 잘못된 판단을 내리고 불필요하거나 위험한 조향을 유발합니다.대응: V2X 메시지 서명 검증 및 인증서 관리(PKI), 내부 센서 데이터와 V2X 데이터 간 정합성 확인, V2X 정보를 보조 수단으로만 한정 (CSR-04)
T-14	LKAS 내부 제어 알고리즘 변조	위험: 악성 SW 주입이나 내부자 접근 등으로 LKAS 알고리즘 자체를 조작하여 조향 로직이 공격자 의도대로 동작하게 만듭니다. 대응: 런타임 메모리 무결성 체크, MPU를 통한 코드/데이터 영역 분리 및 쓰기 방지, 중요 파라미터 영역에 대한 주기적 체크섬 검증 (CSR-07)

8.2.2 높은 우선순위 대응 필요 항목 (High Risk, P2)

이 위협들은 결과적으로 치명적인 영향(Severe Impact)을 가져오지만, 공격을 성공시키기 위한 전문성이나 장비, 지식의 요구 수준이 높아 공격 가능성이 상대적으로 낮게 평가되었습니다. P1 항목을 완화하는 동시에 이들에 대한 대응을 진행해야 합니다.

위협 **ID**	위협 시나리오	핵심 위험 및 필요 대응 방안
T-01	카메라 센서 기만 (Spoofing)	위험: 가짜 차선 이미지 투사 등으로 LKAS가 차선을 오인식하여 의도치 않은 급격한 조향을 유발하거나 기능이 무력화됩니다. 대응: 센서 데이터 무결성 인증, 영상 품질 모니터링, 다중 센서(예: 레이더) 교차 검증을 통한 스푸핑 탐지 (CSR-01)
T-02	네비게이션 예측 정보 변조	위험: 도로 곡률, 제한 속도 등의 예측 정보를 변조하여 급커브 구간에서 LKAS가 직선 주행을 시도하게 유도하는 등 치명적인 오판을 초래합니다. 대응: 네비게이션 도로 예측 정보에 대한 디지털 서명 및 무결성 검증 로직 구현 (CSR-04)
T-03	위치 정보 스푸핑	위험: GNSS 신호 조작을 통해 LKAS의 작동 조건(예: 고속도로/일반 도로)을 오인하게 만들어 시스템의 강제 해제나 오작동을 유발합니다. 대응: GNSS 신호 인증 메커니즘 적용, 위치 스푸핑 탐지 및 경고/Fail-safe 로직 구현 (CSR-04/08)
T-05	CAN 메시지 도청 및 재생	위험: 내부 네트워크 침투 후 정상적인 조향 명령을 도청/재전송하여 운전자 의도와 무관하게 핸들을 급격히 조작하게 만듭니다. 대응: CAN/Ethernet 통신에 메시지 인증 코드(MAC) 적용 및 시퀀스 번호를 통한 재생 공격 방지 로직 구현 (CSR-02, CSR-06)
T-06	차량 네트워크 DoS 공격	위험: 대량의 더미 데이터 주입으로 실시간 차선 인식 데이터 및 긴급 제어 명령의 지연/손실을 유발하여 LKAS 시스템을 마비시킵니다. 대응: 네트워크 세그먼트 분리, 트래픽 속도 제한(Rate Limiting), DoS 공격 탐지/차단 로직 구현 (CSR-03, CSR-08)

T-08	클러스터 경고 알림 차단	위험: LKAS 고장/해제 상태를 알리는 경고 신호를 차단하여 운전자가 시스템 이상을 인지하지 못하게 만듭니다. 대응: 클러스터 경고 신호에 대한 메시지 인증 적용, HMI 시스템의 무결성 보장 (CSR-10)
T-13	운전자 경고등 작동불가	위험: LKAS 고장 발생 시 HMI(Human-Machine Interface) 경고 체계 전체를 무력화하여 운전자의 인지 기회를 박탈합니다. 대응: 클러스터 통신 메시지에 대한 E2E 보호 적용, 주기적 상태 확인 신호 모니터링, 통신 두절 시 클러스터 자체 로직으로 강제 경고등 점등 (CSR-10)
T-15	OBD-II 포트 불법 접근 및 메시지 주입	위험: 공격자가 OBD-II 포트를 통해 내부 네트워크에 접근하여 ECU 정보 조회 및 조향 제어 명령을 직접 주입할 수 있습니다. 대응: 진단 서비스(UDS) 진입 시 강력한 Security Access 인증 절차 강제, 보안 게이트웨이를 통한 외부 트래픽 차단, 주행 중 진단 세션 활성화 차단 로직 적용 (CSR-09)

9. 리스크 처리 결정

위협ID	리스크 레벨	처리 전략	구체적 대응 방안
T-01	High	수용(Accept)	센서 데이터 무결성 인증, 영상 품질 모니터링, 다중 센서 (예: 레이더) 교차 검증
T-02	High	완화(Mitigate)	네비게이션 도로 예측 정보에 대한 디지털 서명 및 무결성 검증 로직 구현
T-03	High	완화(Mitigate)	GNSS 신호 인증 메커니즘 적용, 위치 스푸핑 탐지 및 경고/Fail-safe 로직
T-04	Very High	완화(Mitigate)	게이트웨이 ECU의 방화벽(Filtering) 규칙 강화, 비정상 트래픽 모니터링 및 필터링
T-05	High	수용(Accept)	CAN/Ethernet 통신에 메시지 인증 코드(MAC) 적용, 시퀀스 번호를 통한 재생 공격 방지
T-06	High	수용(Accept)	네트워크 세그먼트 분리, 트래픽 속도 제한(Rate Limiting) 및 DoS 공격 탐지/차단
T-07	Very High	완화(Mitigate)	원격 통신 채널(CCU) 종단 간 암호화(End-to-End Encryption), 강력한 접근 인증 및 인가

T-08	High	수용(Accept)	클러스터 경고 신호에 대한 메시지 인증 적용, HMI 시스템의 무결성 보장
T-09	Very High	완화(Mitigate)	CAN/Ethernet 메시지 인증 코드(MAC) 적용, 수신 패킷의 신선도 검증, E2E 보호 프로토콜 구현
T-10	Very High	완화(Mitigate)	HSM 기반의 안전 부팅 적용, 펌웨어 디지털 서명 검증, JTAG/디버그 포트의 물리적/소프트웨어적 비활성화
T-11	Very High	완화(Mitigate)	게이트웨이 방화벽을 통한 비인가 메시지 ID 필터링, 조향 모듈단에서의 소스 인증, 비정상 토크 명령에 대한 임계치 제한
T-12	Very High	완화(Mitigate)	V2X 메시지 서명 검증 및 인증서 관리(PKI), 내부 센서(카메라) 데이터와 V2X 데이터 간 정합성 확인, V2X 정보를 보조 수단으로만 한정
T-13	High	완화(Mitigate)	클러스터 통신 메시지에 대한 E2E 보호 적용, 주기적 상태 확인 신호 모니터링, 통신 두절 시 클러스터 자체 로직으로 강제 경고등 점등
T-14	Very High	완화(Mitigate)	런타임 메모리 무결성 체크, MPU를 통한 코드/데이터 영역 분리 및 쓰기 방지, 중요 파라미터 영역에 대한 주기적 체크섬 검증
T-15	High	완화(Mitigate)	진단 서비스(UDS) 진입 시 Security Access(Seed & Key) 인증 절차 강제, 보안 게이트웨이를 통한 외부 트래픽 차단, 주행 중 진단 세션 활성화 차단 로직 적용

10. 사이버보안 목표

자산	위협	사이버보안 목표	보안 속성	**CAL** 레벨
Camera(A-01)	T-01	영상 데이터 무결성 및 스푸핑 방지	무결성 가용성	CAL-3
LKAS ECU (A-02)	T-05, T-07, T-09, T-13, T-14, T-15	제어 소프트웨어 무결성 및 무단 접근 방지	기밀성 무결성 가용성	CAL-4
조향 모듈(A-03)	T-05, T-11, T-14	제어 명령 무결성 및 적법성 검증	무결성 가용성	CAL-4
Clustering 모듈(A-04)	T-08, T-12 ,T-15	시스템 상태 경고 신호의 무결성 보장	무결성 가용성	CAL-3
게이트웨이 ECU(A-05)	T-04, T-06, T-14	네트워크 접근 제어 및 통신 가용성 유지	기밀성 무결성 가용성	CAL-4
CCU(A-08)	T-07	원격 통신 채널의 기밀성 및 인증	기밀성 무결성 가용성	CAL-3
CAN/Ethernet 메시지(A-09)	T-05, T-06	통신 메시지의 무결성 및 재생 방지	무결성 가용성	CAL-3
LKAS 알고리즘 (A-10)	T-10, T-13	펌웨어·알고리즘 무결성 검증 및 위변조 방지	기밀성 무결성 가용성	CAL-4
차량 위치/속도 데이터(A-11)	T-02, T-03, T-15	위치/속도 데이터의 신뢰성 및 인증	무결성 가용성	CAL-3

11. 사이버보안 컨셉

11.1 보안 아키텍처 계층

LKAS 시스템은 '심층 방어(Defense in Depth)' 원칙을 적용하여 다중 보안 계층을 구축하고, 단일 실패점을 제거합니다. 주요 계층은 다음과 같습니다.

- 센서/데이터 계층: 센서 데이터의 무결성을 실시간으로 검증하고, 스푸핑/재밍과 같은 외부 공격을 탐지합니다.
- 통신 계층: CAN-FD 및 Automotive Ethernet 통신에 메시지 인증(MAC)을 적용하여 위조 및 재생 공격을 방지합니다.
- 제어/ECU 계층: LKAS ECU 소프트웨어의 무결성을 보장하고, 런타임 검증을 통해 무단 변경을 탐지합니다.
- 원격 접근 계층: CCU를 통한 외부 통신에 강력한 인증과 종단 간 암호화를 적용하여 원격 명령 실행 위협을 방지합니다.

11.2 주요 방어 메커니즘

- Zero Trust 원칙: 모든 내부 및 외부 통신에 대해 '절대 신뢰하지 않고 항상 검증한다'는 원칙을 적용하여 접근 권한을 최소화합니다.
- CAN 메시지 인증: LKAS 제어에 사용되는 모든 CAN/CAN-FD 메시지에 MAC (Message Authentication Code)을 적용합니다.
- 무결성 검증 (Integrity Check): ECU 부팅 시 및 런타임에 LKAS 소프트웨어 및 주요 파라미터의 무결성을 주기적으로 검증합니다.
- 이상 탐지 시스템 (IDS): 게이트웨이 및 주요 ECU에 비정상적인 트래픽 패턴이나 제어 명령을 탐지하고 안전 모드로 전환하는 로직을 구현합니다.

12. 사이버보안 요구사항

요구사항 ID	요구사항 설명	카테고리	CAL	우선순위	검증 방법
CSR-01	전방 카메라 데이터는 인증 및 이상 탐지 알고리즘으로 무결성이 검증되어야 함	센서 보안	CAL-4	보통	동적 테스트
CSR-02	LKAS ECU는 수신하는 조향 제어 명령에 대해 메시지 인증 및 재생 방지 기능을 수행해야 함	제어 무결성	CAL-4	매우 높음	침투 테스트
CSR-03	게이트웨이 ECU는 비정상 트래픽에 대한 심층 패킷 필터링을 수행해야 함	네트워크 보안	CAL-4	매우 높음	침투 테스트
CSR-04	네비게이션/GNSS에서 수신하는 데이터는 디지털 서명으로 무결성 검증을 거쳐야 함	데이터 무결성	CAL-4	보통	동적 테스트
CSR-05	CCU를 통한 원격 통신 채널은 종단 간 암호화 및 강력한 인증을 적용해야 함	원격 통신 보안	CAL-4	낮음	침투 테스트
CSR-06	CAN/Ethernet 메시지는 MAC으로 인증되어야 하며, 시퀀스 번호로 재생 공격을 방지해야 함	통신 보안	CAL-4	매우 높음	침투 테스트
CSR-07	LKAS ECU 펌웨어 무결성은 런타임에 주기적으로 검증되어야 하며 안전 부팅을 지원해야 함	시스템 보안	CAL-4	높음	정적 분석 …
CSR-08	시스템은 센서 데이터, 통신 품질 등 이상 행위 탐지 시	모니터링/ Fail-safe	CAL-4	매우 높음	시나리오 …

	운전자에게 경고하고 안전 모드로 전환해야 함				
CSR-09	OBD-II 포트 접근 시 강력한 인증 및 인가 절차를 요구해야 함	접근 제어	CAL-4	매우 높음	침투 테스트
CSR-10	운전자 경고등 신호는 메시지 인증을 통해 조작 및 차단을 방지해야 함	HMI 보안	CAL-3	보통	동적 테스트

13. 결론 및 다음 단계

본 문서에서는 LKAS(Lane Keeping Assist System) 개발 프로젝트의 ISO/SAE 21434 기반 사이버보안 활동의 첫 단계인 TARA(위협 분석 및 리스크 평가) 및 사이버보안 컨셉 수립 결과를 요약합니다.

13.1 결론 요약

- 위협 분석 및 리스크 식별: LKAS 시스템에 대한 8가지 위협 시나리오를 식별하고 영향도(Critical/Major)와 공격 가능성을 평가했습니다.
- 고위험 위협 (High Risk): 분석 결과, T-01(카메라 센서 기만), T-05(CAN 메시지 도청 및 재생), T-06(차량 네트워크 DoS 공격), T-08(클러스터 경고 알림 차단) 4가지 위협이 고위험(High Risk)으로 결정되어 즉각적인 완화 조치가 필요한 것으로 확인되었습니다.
- 보안 목표: 핵심 자산(A-01, A-02, A-05, A-08, A-09, A-11 등)에 대해 최고 등급인 CAL-4 수준의 사이버보안 목표를 수립하였으며, 이는 데이터 무결성 및 통신 가용성 확보에 중점을 둡니다.
- 보안 컨셉: '심층 방어(Defense in Depth)' 및 'Zero Trust' 원칙에 기반하여 센서 데이터 무결성 인증, CAN/Ethernet 메시지 인증(MAC), 런타임 펌웨어 무결성 검증, 이상 탐지 시스템(IDS) 구현 등의 주요 방어 메커니즘을 적용하는 것으로 결정되었습니다.

13.2 다음 단계

도출된 결과를 바탕으로 프로젝트의 다음 단계는 다음과 같습니다.

1. 사이버보안 구현 (제품 개발 단계):
    - 도출된 High 우선순위 사이버보안 요구사항(CSR-01 ~ CSR-08)을 시스템 및 컴포넌트 설계에 반영합니다.
    - 특히 고위험 위협(T-01, T-05, T-06, T-08)의 완화를 위한 구체적 대응 방안(센서 데이터 인증, 메시지 인증/재생 방지, 트래픽 속도 제한 등)을 최우선적으로 구현합니다.
2. 사이버보안 검증 (검증/검수 단계):
    - 각 요구사항에 지정된 침투 테스트, 동적 테스트, 시나리오 테스트 등의 검증 방법을 통해 구현된 보안 메커니즘의 효과성을 철저히 확인합니다.
3. 지속적인 문서화 및 관리:
    - ISO/SAE 21434 표준 요구사항에 따라 '사이버보안 구현', '사이버보안 검증', '사이버보안 모니터링' 관련 후속 산출물을 지속적으로 개발하고 관리합니다.
4. 리스크 재평가:
    - 완화 조치 구현 후, 잔존 리스크를 평가하고 허용 가능한 수준인지 확인하는 절차를 진행합니다.