

UN Regulation No. 155: 자동차 사이버 보안의 글로벌 표준

20210741 황정현

제1장: 적용 범위(Scope)

- **카테고리 M & N:** 일반 승용차, 버스, 화물차 전반 적용
- **카테고리 O:** 전자제어장치(ECU)가 1개 이상 장착된 트레일러
- **카테고리 L₆ & L₇:** 레벨 3 이상의 자율주행 기능 탑재 시 적용

제2장: 정의(Definitions)

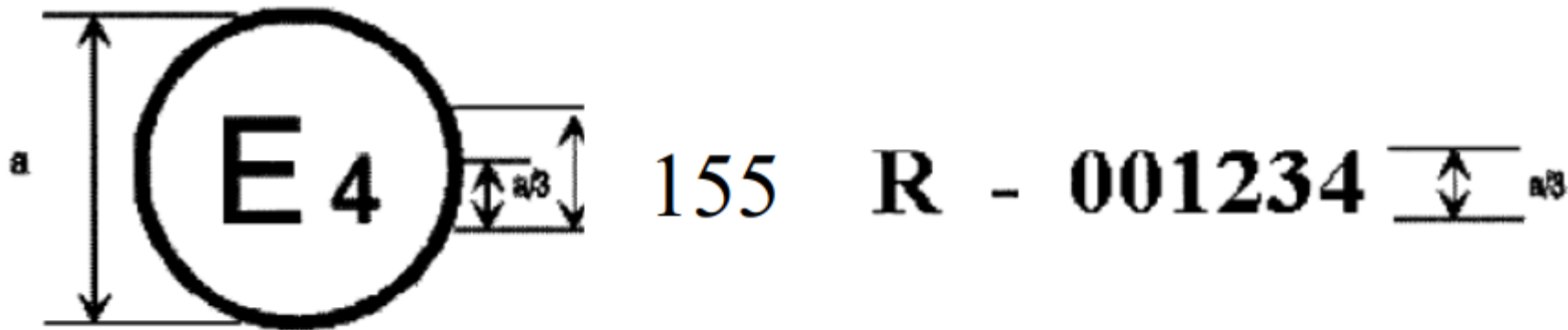
- **차량 형식(Vehicle type):** 제조사 명칭 및 전기/전자 아키텍처의 핵심적 특징이 동일한 차량군
- **CSMS(사이버 보안 관리 체계):** 사이버 위협에 대응하기 위한 조직적 프로세스와 거버넌스를 정의한 체계적인 접근 방식
- **생애 주기:** 개발 단계, 생산 단계, 그리고 차량 폐기 시까지의 생산 후 단계로 구분
- **위험 관리 용어:** 위협(Threat), 취약점(Vulnerability), 위험(Risk), 완화(Mitigation) 등 핵심 보안 용어를 정의

제3장: 승인 신청(Application for approval)

- 신청 주체:** 차량 제조사 또는 정식 대리인이 신청
- 필수 서류:** 차량 형식 설명서와 제6항에 따른 CSMS 적합성 인증서가 포함되어야 함.
- 문서 보관:** 승인 기관과 제조사는 생산이 중단된 후에도 최소 10년 동안 관련 서류를 유지해야 함.

제4장: 마킹(Marking)

- **E 마크:** 승인된 차량에는 문자 'E'와 국가 번호가 포함된 원형 국제 승인 마크가 부착됨.
- **부착 방식:** 마크는 판독 가능하고 지워지지 않아야 하며, 제조사 데이터 플레이트 근처에 위치해야 함.



$a = 8 \text{ mm min.}$

제5장: 승인(Approval)

- 검증 방법:** 승인 기관은 서류 검토 및 실차 시험을 통해 보안 조치의 구현 여부를 확인
- 거부 사유:** 위험 평가가 불충분하거나 보안 조치의 효과 검증이 부족할 경우 승인 거부
- 정보 공유:** 승인 정보와 기준은 유엔의 DETA 데이터베이스를 통해 국제적으로 공유

제6장: CSMS 적합성 인증서 (Certificate of Compliance for CSMS)

- 선행 조건:** 개별 차량 형식 승인을 위해 제조사는 유효한 CSMS 인증서를 보유
- 유효 기간:** 인증서의 유효 기간은 최대 3년
- 인증 철회:** 요구 사항을 충족하지 못해 CSMS 인증이 철회되면 해당 차량의 형식 승인도 취소될 수 있음

제7장: 요구 사항(Specifications)

- 전 생애주기 관리:** CSMS는 개발, 생산, 생산 후 단계 모두를 아우러야 함
- 위험 평가 및 관리:** 제조사는 공급망 위험을 관리하고, 부속서 5의 위협을 고려한 철저한 위험 평가를 수행
- 지속적 모니터링:** 운행 중인 차량에 대해서도 지속적으로 모니터링하고 결과를 연 최소 1회 보고

제8~12장: 행정 절차

- **수정 및 연장:** 사이버 보안에 영향을 주는 차량의 수정 사항은 승인 기관에 통지
- **생산 적합성:** 제조사는 생산 차량의 보안 적합성을 기록하고 관리해야 하며, 기관은 3년마다 이를 점검할 수 있음
- **처벌 및 통보:** 요건 미달 시 승인이 취소되며, 생산 중단 시에도 이를 다른 체약국에 알려야 함

Annex 5 개요: 위협 및 완화 조치

- **Part A: 위협 및 취약점 기준 (위험 평가 체크리스트)**
- Part B: 차량 자체에 적용되는 완화 조치
- Part C: 백엔드 서버 등 차량 외부 영역 완화 조치

주요 위협 (1): 백엔드 서버 위협

- **공격 통로:** 서버를 경유하여 차량을 제어하거나 데이터를 탈취
- **주요 위협:** 내부자 권한 남용, 미패치 취약점(SQL 공격 등) 활용, 물리적 서버 접근
- **서비스 중단:** 서버 공격을 통한 차량 필수 서비스 및 상호작용 마비
- **데이터 유출:** 클라우드 사고 및 관리자 실수로 인한 민감 정보 유출

주요 위협 (2): 차량 통신 채널 위협

- **메시지 조작:** V2X, GNSS 메시지 사칭(스푸핑) 및 시빌 공격(Sybil attack)
- **데이터 침해:** 통신 스트림 내 코드 주입, 데이터 삭제 및 무단 수정
- **세션 공격:** 중간자 공격(MITM), 세션 하이재킹 및 재전송 공격(Replay attack)
- **서비스 거부(DoS):** 대량의 쓰레기 데이터 전송 및 메시지 차단(블랙홀 공격)
- **악성 콘텐츠:** 내부 통신(CAN), V2X, 진단 메시지 내 악성 코드 포함

주요 위협 (3): 업데이트 절차 위협

- **업데이트 변조:** 무선(OTA) 및 물리 업데이트 시 펌웨어 위조 및 조작
- **권한 탈취:** 소프트웨어 공급자의 암호화 키 탈취를 통한 무효 업데이트 승인
- **업데이트 방해:** 업데이트 서버 DoS 공격으로 보안 패치 배포 차단

주요 위협 (4): 인간 행위 관련 위협

- **사회공학적 기법:** 소유자나 정비사를 속여 의도치 않게 악성코드 로드 유도
- **절차 미준수:** 규정된 보안 프로토콜 및 절차를 따르지 않아 보안 구멍 발생

주요 위협 (5): 외부 연결성 및 인터페이스 위협

- **원격 제어 조작:** 원격 키, 이모빌라이저, 텔레매틱스(공조, 문 잠금 등) 조작
- **제3자 앱:** 보안이 취약한 외부 앱(인포테인먼트 등)을 통한 시스템 공격
- **물리적 포트:** USB, OBD 단자를 통한 코드 주입 및 파라미터 조작

주요 위협 (6): 차량 데이터 및 코드 위협

- **무단 추출:** 저작권 소프트웨어 불법 복제 및 개인정보/암호화 키 탈취
- **조작 및 사기:** 차량 ID(VIN) 변경, 신원 사칭, 주행 데이터(마일리지 등) 위조
- **안전 파라미터:** 브레이크, 에어백, 충전 설정값 등 핵심 기능 파라미터 변조

주요 위협 (7): 잠재적 취약점 및 물리 조작

- **암호화 결함:** 짧은 키 길이, 폐기된 알고리즘 사용 등 불충분한 암호화 적용
- **개발 잔재물:** 제거되지 않은 디버그 포트(JTAG), 개발자 패스워드 악용
- **네트워크 설계:** 불필요한 포트 개방 및 네트워크 분리 우회
- **물리적 방해:** 무단 하드웨어 추가 및 자석 등을 이용한 센서 정보 조작

정리

- 조직과 제품의 이중 인증(CSMS & VTA)
- 전 생애주기 책임
- 위험 기반의 선제적 방어
- 지속적인 모니터링 및 보고