

자동차 및 자동차부품의 성능과 기준에 관한
규칙 일부개정령안

기 관 명 (부 서 명)	국무위원 ○○○ (국토교통부장관)
연 월 일	20 . . .

법제처 심사 전

1. 개정이유 및 주요내용

최근 자동차의 핵심 기술이 하드웨어에서 소프트웨어 기반으로 급속히 전환되고 통신을 활용한 외부와의 연결 기능이 확산됨에 따라, 해킹 등의 사이버공격·위협으로부터 자동차의 사이버보안을 확보하고 자동차 안전에 영향을 줄 수 있는 소프트웨어 업데이트를 관리할 필요성이 증대되고 있음.

이와 관련, 자동차 사이버보안 관리체계 인증제도를 도입하고 자동차 소프트웨어 업데이트 준수사항을 신설하는 내용으로 「자동차관리법」이 개정(법률 제20298호, 2024. 2. 13. 공포, 2025. 8. 14. 시행)됨에 따라, 자동차 사이버보안의 안전기준 및 무선 업데이트 시 소프트웨어 업데이트 장치의 안전기준을 정하려는 것임.

2. 참고사항

가. 관계법령 : 생략

나. 예산조치 : 별도조치 필요 없음

다. 합 의 : 0000부 등과 합의되었음

라. 기 타 : 1) 신·구조문대비표, 별첨

2) 입법예고(9999. 12. 31. ~ 12. 31.) 결과, 특기할 사항
없음

3) 행정규제 :

자동차 및 자동차부품의 성능과 기준에 관한 규칙 일부개정령안

자동차 및 자동차부품의 성능과 기준에 관한 규칙 일부를 다음과 같이 개정한다.

제2조에 제65호를 다음과 같이 신설한다.

65. “무선 업데이트”란 케이블 등의 연결 없이 무선으로 데이터를 전송하는 방법으로 자동차의 소프트웨어를 변경하는 것을 말한다.

제18조의5 및 제18조의6을 각각 다음과 같이 신설한다.

제18조의5(자동차 사이버보안) 자동차는 법 제30조의9제1항에 따른 자동차 사이버보안 관리체계 인증 내용에 따라 다음 각 호를 준수하여 제작되어야 한다.

1. 자동차의 부품 및 시스템과 관련된 사이버공격·위협이 식별될 것
2. 다음 각 목의 사항을 고려하여 자동차 사이버공격·위협이 평가될 것
 - 가. 자동차의 각 구성요소 및 구성요소 간 상호작용
 - 나. 자동차와 외부 시스템과의 상호작용
 - 다. 별표 5의38을 포함한 자동차 사이버공격·위협
3. 제1호에 따라 식별된 자동차 사이버공격·위협이 제2호에 따른 평

가 결과에 따라 적절하게 관리될 것

4. 제3호에 따라 관리하는 자동차 사이버공격·위협을 완화하기 위하여 별표 5의39의 조치가 적용될 것. 다만, 별표 5의39의 조치가 제1호에 따라 식별된 사이버공격·위협과 관련이 없거나 충분하지 않은 경우 별도의 적절한 보안 조치가 적용되어야 한다.

5. 자동차 판매 후 서비스·응용 프로그램 실행 등을 목적으로 인터페이스 등 전용 환경을 제공하는 경우 제공된 전용 환경을 자동차 사이버공격·위협으로부터 보호하기 위한 보안 조치가 적용될 것

6. 제4호 및 제5호에 따른 보안 조치의 효과를 확인하기 위하여 국토교통부장관이 고시하는 사항을 포함하여 적절하고 충분한 검증이 수행될 것

7. 자동차 사이버보안이 적정하게 유지되고 있는지 확인하기 위해 다음 각 목의 기능을 갖출 것

가. 자동차 사이버공격·위협 및 이와 관련된 취약점을 탐지하고 방지하는 기능

나. 탐지된 자동차 사이버공격·위협 및 취약점을 제작자등이 모니터링할 수 있도록 지원하는 기능

다. 자동차 사이버공격·위협의 시도나 성공 여부 등에 대한 분석이 가능한 데이터 포렌식 기능

8. 자동차의 부품 또는 자동차부품을 제작·조립 또는 수입하는 자(이하 “부품제작자등”이라 한다)와 관련된 위험이 식별·관리될 것

제18조의6(소프트웨어 업데이트) ① 자동차의 소프트웨어는 그 버전을 확인할 수 있어야 한다.

② 제작자등이 자동차에 무선 업데이트를 실시할 경우 다음 각 호의 기준에 적합해야 한다.

1. 업데이트가 실패 또는 중단된 경우 업데이트를 실시하기 이전 버전으로 되돌리거나 자동차를 안전한 상태로 전환할 것

2. 업데이트 완료에 필요한 전력 및 업데이트가 실패 또는 중단된 경우 제1호에 따른 조치를 취하는데 필요한 전력이 있는 경우에만 업데이트가 실행될 것

3. 업데이트 실행이 자동차의 안전에 영향을 주는 경우 기술적 수단 등을 통해 업데이트를 실행하는 동안 자동차를 안전한 상태로 유지할 수 있음을 입증할 것

4. 업데이트 실행 전 다음 각 목의 정보를 운전자에게 제공할 것

가. 업데이트 목적(리콜, 안전 또는 보안상의 중요성 등을 포함)

나. 업데이트로 인한 자동차 기능의 변경 내용

다. 업데이트 완료까지의 예상 소요 시간

라. 업데이트 실행 중 사용이 불가능한 자동차의 기능

마. 운전자가 업데이트를 실행할 때 참고해야 할 사항

5. 운전 중 업데이트 실행 시 안전운행을 위협할 우려가 있는 경우 다음 각 목의 어느 하나를 만족할 것

가. 차량 운행 중 업데이트 실행이 불가능할 것

나. 운전자가 자동차의 안전 또는 업데이트 실행에 영향을 주는 기능을 이용할 수 없도록 할 것

6. 업데이트 실행 후 다음 각 목의 정보를 운전자에게 제공할 것

가. 업데이트의 성공 또는 실패 정보

나. 업데이트로 변경된 사항

별표 5의38 및 별표 5의39를 각각 별지와 같이 신설한다.

부 칙

제1조(시행일) 이 규칙은 2025년 8월 14일부터 시행한다.

제2조(일반적 적용례) 이 규칙의 개정규정은 이 규칙 시행 이후 제작·조립 또는 수입되는 자동차부터 적용한다.

제3조(자동차 사이버보안에 관한 적용례) 제18조의5의 개정규정은 이 규칙 시행 당시 제작·조립 또는 수입되고 있는 형식의 자동차에 대해서는 2027년 8월 14일부터 적용한다.

제4조(소프트웨어 업데이트에 관한 적용례) 제18조의6의 개정규정은 이 규칙 시행 당시 제작·조립 또는 수입되고 있는 형식의 자동차에 대해서는 2027년 8월 14일부터 적용한다.

자동차 사이버공격·위협(제18조의5 관련)

1. 자동차와 관련된 백엔드 서버에 대한 사이버공격·위협

사이버공격·위협에 대한 분류		사이버공격·위협 또는 취약점의 예시	
1	백엔드 서버를 통해 자동차를 공격하거나 데이터를 추출 *백엔드 서버란 자동차에 서비스를 제공하기 위해 연산, 조회 등의 처리를 하는 제작사의 서버를 말함	1.1	내부 직원의 권한 남용(내부자 공격)
		1.2	백엔드 서버에 대한 무단 인터넷 접근 *백도어, 패치되지 않은 시스템 소프트웨어 취약점, SQL 공격 또는 기타 수단에 의해 활성화될 수 있음
		1.3	백엔드 서버에 대한 물리적인 무단 접근 *서버에 연결된 USB, 기타 매체 등으로 수행될 수 있음
2	백엔드 서버의 서비스를 중단시켜 자동차 작동에 영향	2.1	백엔드 서버에 대한 공격으로 인한 기능중단 *자동차와 상호작용하거나 자동차에서 요구하는 서비스를 제공하지 못하게 됨
3	백엔드 서버에 저장된 자동차 관련 데이터 손실 또는 손상	3.1	내부 직원의 권한 남용(내부자 공격)
		3.2	클라우드 정보 손실 *타 클라우드 서비스 공급업체에 데이터를 저장할 때, 중요한 데이터가 공격이나 사고로 인해 손실될 수 있음
		3.3	백엔드 서버에 대한 무단 인터넷 접근 *백도어, 패치되지 않은 시스템의 소프트웨어 취약점, SQL공격, 기타 수단에 의해 활성화될 수 있음
		3.4	백엔드 서버에 대한 물리적인 무단 접근 *서버에 연결된 USB, 기타 매체 등으로 수행될 수 있음
		3.5	의도하지 않은 데이터 공유로 인한

		정보 침해(관리 오류 등)
--	--	----------------

2. 자동차 통신채널과 관련된 사이버공격 · 위협

사이버공격 · 위협에 대한 분류		사이버공격 · 위협 또는 취약점의 예시	
4	자동차가 수신하는 메시지 또는 데이터를 스푸핑 *스푸핑이란 데이터 위·변조를 통해 합법적 사용자인 것처럼 위장하여 공격 대상을 속이는 공격 기술을 말함	4.1	위장 공격을 이용한 메시지 스푸핑 *군집 주행 중 802.11p V2X, GNSS 메시지 등
		4.2	시빌 공격 *시빌 공격이란 도로에 자동차가 많은 것처럼 다른 자동차를 속이는 공격 기술을 말함
5	통신채널을 통해 자동차의 데이터 및 코드를 무단 조작, 삭제하거나 다른 공격을 위해 사용	5.1	통신채널에 코드 주입을 허용 *변조된 소프트웨어가 통신 스트림에 주입될 수 있음
		5.2	통신채널을 통한 자동차의 데이터/코드 조작을 허용
		5.3	통신채널을 통한 자동차의 데이터/코드 덮어쓰기를 허용
		5.4	통신채널을 통한 자동차의 데이터/코드 삭제를 허용
		5.5	통신채널을 통한 자동차의 데이터/코드 주입을 허용(데이터 코드 작성)
6	통신채널이 신뢰할 수 없는 메시지를 수신하거나, 가로채기 공격 또는 세션 하이재킹, 재전송 공격 *가로채기 공격이란 송·수신자 사이에 공격자가 끼어들어 데이터를 도청하거나 조작하는 공격 기술을 말함 *세션 하이재킹이란 공격자가 유효한 통신 세션(시스템 간 연결이 활성화된 상태) 등을 가로채어 접근하는 공격 기술을 말함	6.1	신뢰할 수 없는 출처의 정보를 수신
		6.2	가로채기 공격/세션 하이재킹
		6.3	재전송 공격 *통신 게이트웨이에 대한 공격을 통해 공격자가 ECU의 소프트웨어 또는 게이트웨이 펌웨어를 다운그레이드할 수 있음

7	통신 도청, 중요한 파일 또는 폴더에 대한 무단 접근 허용 등에 의한 정보 추출	7.1	정보 가로채기/방해 전파/통신 모니터링
		7.2	파일 또는 데이터에 대한 무단 접근 권한 획득
8	통신채널을 통한 서비스 거부 공격으로 자동차 기능 방해	8.1	서비스 거부 공격 *서비스 거부 공격이란 많은 수의 공격 데이터를 자동차로 전송하여 정상적으로 서비스를 제공할 수 없도록 하는 공격 기술을 말함
		8.2	블랙홀 공격 *블랙홀 공격이란 자동차 간 통신을 교란하기 위하여 자동차 간의 메시지를 차단하는 공격 기술을 말함
9	권한이 없는 사용자가 자동차 시스템에 대한 접근 권한 획득	9.1	권한이 없는 사용자가 자동차 시스템에 대한 관리자 권한을 탈취
10	통신 매체에 내장된 바이러스를 통한 자동차 시스템 감염	10.1	통신 매체에 내장된 바이러스가 자동차 시스템을 감염
11	자동차가 수신하는 메시지에 악성 콘텐츠가 포함	11.1	악성 내부(CAN 등) 메시지
		11.2	악성 V2X 메시지 *I2V 메시지(RSA 등) 또는 V2V 메시지(BSM 등)
		11.3	악성 진단 메시지
		11.4	악성 전용 메시지 *OEM 또는 관련 부품사들이 정의하여 사용하는 고유 메시지

3. 업데이트 절차와 관련된 사이버공격·위협

사이버공격·위협에 대한 분류		사이버공격·위협 또는 취약점의 예시	
12	업데이트 절차와 관련된 오류	12.1	무선 소프트웨어 업데이트(OTA) 절

	또는 공격		차와 관련된 공격 *조작된 시스템 업데이트 프로그램 또는 펌웨어가 포함됨
		12.2	OBD 등 진단 인터페이스, USB 등 유선으로 실시하는 소프트웨어 업데이트 절차와 관련된 공격 *조작된 시스템 업데이트 프로그램 또는 펌웨어가 포함됨
		12.3	업데이트 절차와 관련된 공격은 아니지만, 소프트웨어가 이미 조작됨
		12.4	소프트웨어 공급자의 암호키가 훼손되어 잘못된 업데이트를 실행
13	정상적인 업데이트 거부	13.1	업데이트 서버 또는 네트워크의 서비스 거부 공격을 통해 중요 소프트웨어 업데이트 배포 및 특정 기능의 활성화 등을 방해

4. 의도하지 않은 행동으로 인한 사이버공격·위협

사이버공격·위협에 대한 분류		사이버공격·위협 또는 취약점의 예시	
15	자동차 소유자, 운영자 또는 유지보수 엔지니어 등(이하 “합법적 사용자”라 한다)이 의도치 않게 사이버공격을 용이하게 행동	15.1	합법적 사용자가 속임을 당하여 의도하지 않게 악성 프로그램을 실행하거나 사이버공격을 허용
		15.2	자동차 사이버보안 확보를 위해 내부에 규정된 보안 절차를 따르지 않음

5. 자동차의 외부 연결에 대한 사이버공격·위협

사이버공격·위협에 대한 분류		사이버공격·위협 또는 취약점의 예시	
16	텔레매틱스, 원격 시스템, 근거리 무선 통신 시스템 등의 자동차의 외부 연결 관련 기능을 조작하여 사이버공격을 가능하게	16.1	원격 잠금장치, 이모빌라이저 등 원격으로 작동하도록 설계된 시스템의 기능을 조작
		16.2	차량 텔레매틱스 조작

	함		*민감한 제품의 온도 측정 조작, 원격으로 차문 잠금 해제
		16.3	근거리 무선 시스템 또는 센서와의 간섭
17	엔터테인먼트, 애플리케이션 등의 제삼자 소프트웨어에 의한 공격	17.1	손상되거나 소프트웨어 보안이 취약한 애플리케이션을 이용하여 자동차 시스템을 공격
18	외부 인터페이스(USB, OBD 등)에 연결된 장치를 통한 자동차 시스템 공격	18.1	외부 인터페이스를 통해 공격
		18.2	바이러스에 감염된 매체가 자동차 시스템에 연결
		18.3	OBD 등 진단 인터페이스를 통해 사이버공격을 용이하게 함 *직·간접적인 자동차 매개 변수 조작 등

6. 자동차 데이터/코드에 대한 사이버공격 · 위협

사이버공격 · 위협에 대한 분류		사이버공격 · 위협 또는 취약점의 예시	
19	자동차 데이터/코드 추출	19.1	자동차 시스템에서 저작권이 있거나 독점하고 있는 소프트웨어 추출(제품 불법 복제)
		19.2	소유자의 개인 정보에 대한 무단 접근 *개인 신상정보, 결제 계좌 정보, 주소록 정보, 위치 정보, 자동차 전자 ID 등
		19.3	암호키 추출
20	자동차 데이터/코드 조작	20.1	자동차 전자 ID에 대한 불법/무단 변경
		20.2	신원 조작 *요금징수 시스템과 통신 시 다른 ID 사용 등
		20.3	모니터링 시스템을 우회하는 작업 *ODR 추적기 데이터, 실행 횟수 등 메시지 해킹/수정/차단
		20.4	자동차 주행데이터를 변조하기 위한

			데이터 조작 *주행거리, 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	멀웨어 유입	22.2	악의적으로 소프트웨어를 조작
23	새로운 소프트웨어 설치 또는 기존 소프트웨어에 덮어쓰기	23.1	자동차 제어 시스템 또는 정보시스템의 소프트웨어가 위조
24	시스템 또는 운영의 중단	24.1	서비스 거부 *CAN 버스를 플러딩하거나 메시지 전송률을 높여 ECU의 고장을 유발하여 내부 네트워크에서 통신 중단 유발
25	자동차 매개변수 조작	25.1	무단 접근을 통해 자동차 주요 기능의 구성 매개변수를 변조 *브레이크 데이터, 에어백 전개 임계값 등
		25.2	무단 접근을 통해 충전 기능과 관련된 전압, 전력, 배터리 온도 등과 같은 매개변수를 변조

7. 악용될 수 있는 잠재적 취약점

취약점에 대한 분류		사이버공격·위협 또는 취약점의 예시	
26	암호 기술이 손상되거나 제대로 적용되지 않음	26.1	암호키의 길이가 짧고 암호의 변경 주기가 긴 암호 알고리즘을 사용
		26.2	중요한 시스템을 보호하기 위한 암호 알고리즘을 적절히 사용하지 않음
		26.3	이미 사용 중지되었거나 곧 중단될 암호 알고리즘 사용
27	부품이나 소모품 등이 손상되어 자동차가 공격받음	27.1	사이버공격에 대응하기 위한 설계 기준을 충족하지 못하는 하드웨어 또는 소프트웨어 사용
28	소프트웨어 또는 하드웨어 개발	28.1	소프트웨어 버그

	과정에서의 취약점		*소프트웨어 버그의 존재는 잠재적으로 공격 가능한 취약점이 될 수 있으며, 알려진 불량 코드/버그의 존재 여부 확인을 위한 테스트 혹은 알 수 없는 불량 코드/버그의 존재 위험을 줄이기 위한 테스트를 하지 않는 경우 발생할 수 있음
		28.2	개발용 인터페이스 등을 사용하여 공격자가 ECU에 접근하거나 상위 권한을 획득 *디버그 포트, JTAG 포트, 마이크로프로세서, 개발 인증서, 개발자 암호 등
29	네트워크 설계로 인한 취약점	29.1	불필요한 인터넷 포트가 열려있어 네트워크 시스템에 대한 접근 허용
		29.2	네트워크 망분리를 우회하여 제어권 확보 *보호망을 우회하여 다른 네트워크 세그먼트에 대한 접근 권한을 획득하여, 임의의 CAN 메시지 전송과 같은 악의적인 행위를 수행하기 위하여 보호되지 않은 게이트웨이 또는 접근 지점을 공격 *특장 자동차(트럭 트레일러 게이트웨이 등)를 사용하는 경우를 예로 들 수 있음
31	의도하지 않은 데이터 전송	31.1	정보 침해 *렌터카로 사용·판매되는 등 자동차 사용자가 바뀌면서 개인 정보가 누출될 수 있음
32	물리적 조작으로 인한 시스템 공격 가능성	32.1	하드웨어 조작 *메세지 가로채기 공격 등을 위해 승인된 하드웨어(센서 등)를 승인되지 않은 하드웨어로 교체하거나, 자석을 사용하여 기어 박스에 연결된 홀 효과 센서를 조작하는 방식 등으로 센서가 수집한 정보를 조작

※ 비교 : 위 표는 개정 당시 “UN Regulation No. 155, Annex 5의 Part A. Vulnerability or attack method related to the threats”를 참조하였음.

자동차 사이버공격·위협에 대한 보안 조치(제18조의5 관련)

1. 자동차 통신채널과 관련된 위협에 대한 보안 조치

사이버공격·위협 또는 취약점의 예시		보안 조치	
4.1	위장 공격을 이용한 메시지 스푸핑 *군집 주행 중 802.11p V2X, GNSS 메시지 등	M10	자동차는 수신하는 메시지의 신뢰성 및 무결성을 확인해야 함
4.2	시빌 공격 *시빌 공격이란 도로에 자동차가 많은 것처럼 다른 자동차를 속이는 공격 기술을 말함	M11	암호키를 저장하기 위한 보안 조치가 구현되어야 함 *하드웨어 보안 모듈(HSM) 사용
5.1	통신채널에 코드 주입을 허용 *변조된 소프트웨어가 통신 스트림에 주입될 수 있음	M10	자동차는 수신하는 메시지의 신뢰성 및 무결성을 확인해야 함
		M6	시스템은 위협을 최소화하기 위해 설계 단계부터 보안 조치를 고려해야 함
5.2	통신채널을 통한 자동차의 데이터/코드 조작을 허용	M7	자동차의 데이터/코드를 보호하기 위해 접근 통제 기술 및 설계가 적용되어야 함
5.3	통신채널을 통한 자동차의 데이터/코드 덮어쓰기를 허용		
5.4 & 21.1	통신채널을 통한 자동차의 데이터/코드 삭제를 허용		
5.5	통신채널을 통한 자동차의 데이터/코드 주입을 허용(데이터 코드 작성)		
6.1	신뢰할 수 없는 출처의 정보를 수신	M10	자동차는 수신하는 메시지의 신뢰성 및 무결성을 확인해야 함
6.2	가로채기 공격/세션 하이재킹 *가로채기 공격이란 송·수신자 사이에 공격자가 끼어들어 데이터를 도청하거나 조작하는 공격 기술을 말함 *세션 하이재킹이란 공격자가 유효한 통신 세션(시스템 간 연결이 활성화된 상태) 등을 가		

	로채어 접근하는 공격 기술을 말함		
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	M12	자동차와 주고받는 기밀 정보는 보호되어야 함
7.2	파일 또는 데이터에 대한 무단 접근 권한 획득	M8	시스템 설계 및 접근 제어를 통해 권한이 없는 사용자가 개인 또는 시스템의 중요 데이터에 접근할 수 없어야 함 *보안 조치의 예는 OWASP(the Open Web Application Security Project)에서 찾을 수 있음
8.1	서비스 거부 공격 *많은 수의 공격 데이터를 자동차로 전송하여 정상적으로 서비스를 제공할 수 없음	M13	서비스 거부 공격을 감지하고 복구 조치를 취해야 함
8.2	블랙홀 공격 *자동차 간 통신을 교란하기 위하여 자동차 간의 메시지를 차단할 수 있음		
9.1	권한이 없는 사용자가 자동차 시스템에 대한 관리자 권한을 탈취	M9	무단 접근을 방지하고 탐지하는 대책을 취해야 함
10.1	통신 매체에 내장된 바이러스가 자동차 시스템을 감염	M14	내장된 멀웨어로부터 시스템을 보호하기 위한 조치를 고려해야 함
11.1	악성 내부(CAN 등) 메시지	M15	악성 내부 메시지나 활동을 탐지하는 조치를 고려해야 함
11.2	악성 V2X 메시지 *I2V 메시지(RSA 등) 또는 V2V 메시지(BSM 등)	M10	자동차는 수신하는 메시지의 신뢰성 및 무결성을 확인해야 함
11.3	악성 진단 메시지		
11.4	악성 전용 메시지 *OEM 또는 관련 부품사들이 정의하여 사용		

	하는 고유 메시지		
--	-----------	--	--

2. 업데이트 절차와 관련된 위협에 대한 보안 조치

사이버공격·위협 또는 취약점의 예시		보안 조치	
12.1	무선 소프트웨어 업데이트(OTA) 절차와 관련된 공격 *조작된 시스템 업데이트 프로그램 또는 펌웨어가 포함됨	M16	소프트웨어 업데이트가 안전하게 실행되어야 함
12.2	OBD 등 진단 인터페이스, USB 등 유선으로 실시하는 소프트웨어 업데이트 절차와 관련된 공격 *조작된 시스템 업데이트 프로그램 또는 펌웨어가 포함됨		
12.3	업데이트 절차와 관련된 공격은 아니지만, 소프트웨어가 이미 조작됨		
12.4	소프트웨어 공급자의 암호키가 훼손되어 잘못된 업데이트를 실행	M11	암호키를 저장하기 위한 보안 조치가 구현되어야 함 *하드웨어 보안 모듈(HSM) 사용
13.1	업데이트 서버 또는 네트워크의 서비스 거부 공격을 통해 중요 소프트웨어 업데이트 배포 및 특정 기능의 활성화 등을 방해	M3	백엔드 서버가 서비스 제공에 중요한 경우 중단에 대비한 복구 대책 등의 보안 조치가 적용되어야 함. *보안 조치의 예는 OWASP에서 찾을 수 있음

3. 의도하지 않은 행동으로 인한 위협에 대한 보안 조치

사이버공격·위협 또는 취약점의 예시		보안 조치	
15.1	합법적 사용자가 속임을 당하여 의도하지 않게 악성 프로그램을 실행하거나 사이버공격을 허용	M18	최소 권한 원칙에 따라 사용자별 접근 권한을 정의하고, 정의된 접근 권한대로 제어해야 함
15.2	자동차 사이버보안 확보를 위해 내부에 규정된 보안 절차를 따르지 않음	M19	보안 기능 관리와 관련된 작업 및 접근 기록을 포함한 보안 절차를 정의하고 준수

		해야 함
--	--	------

4. 자동차의 외부 연결과 관련된 위협에 대한 보안 조치

사이버공격 · 위협 또는 취약점의 예시		보안 조치	
16.1	원격 잠금장치, 이모빌라이저 등 원격으로 작동하도록 설계된 시스템의 기능을 조작	M20	원격 접근이 가능한 시스템에 보안 조치가 적용되어야 함
16.2	차량 텔레매틱스 조작 *민감한 제품의 온도 측정 조작, 원격으로 차문 잠금 해제		
16.3	근거리 무선 시스템 또는 센서와의 간섭		
17.1	손상되거나 소프트웨어 보안이 취약한 애플리케이션을 이용하여 자동차 시스템을 공격	M21	소프트웨어의 보안과 관련된 사항들이 평가되어야 하고, 인증 및 무결성이 보호되어야 하며, 제삼자 소프트웨어로부터의 위협을 최소화하기 위한 보안 조치가 적용되어야 함
18.1	외부 인터페이스를 통해 공격	M22	외부 인터페이스에 보안 조치가 적용되어야 함
18.2	바이러스에 감염된 매체가 자동차 시스템에 연결		
18.3	OBD 등 진단 인터페이스를 통해 사이버공격을 용이하게 함 *직·간접적인 자동차 매개 변수 조작 등		

5. 자동차 데이터/코드와 관련된 위협에 대한 보안 조치

사이버공격 · 위협 또는 취약점의 예시		보안 조치	
19.1	자동차 시스템에서 저작권이 있거나 독점하고 있는 소프트웨어 추출(제품	M7	시스템 데이터/코드를 보호하기 위해 접근 통제 기술 및

	불법 복제)		설계가 적용되어야 함 *보안 조치의 예는 OWASP에서 참조 가능
19.2	소유자의 개인 정보에 대한 무단 접근 *개인 신상정보, 결제 계좌 정보, 주소록 정보, 위치 정보, 자동차 전자 ID 등	M8	시스템 설계 및 접근 제어를 통해 권한이 없는 사용자가 개인 또는 시스템의 중요 데이터에 접근할 수 없어야 함 *보안 조치의 예는 OWASP에서 참조 가능
19.3	암호키 추출	M11	암호키를 저장하기 위한 보안 조치가 구현되어야 함 *하드웨어 보안 모듈(HSM) 사용
20.1	자동차 전자 ID에 대한 불법/무단 변경	M7	시스템 데이터/코드를 보호하기 위해 접근 통제 기술 및 설계가 적용되어야 함 *보안 조치의 예는 OWASP에서 참조 가능
20.2	신원 조작 *요금징수 시스템과 통신 시 다른 ID 사용 등		
20.3	모니터링 시스템을 우회하는 작업 *ODR 추적기 데이터, 실행 횟수 등 메시지 해킹/수정/차단	M7	시스템 데이터/코드를 보호하기 위해 접근 통제 기술 및 설계가 적용되어야 함 *보안 조치의 예는 OWASP에서 참조 가능 *센서 또는 전송된 데이터에 대한 데이터 조작 공격은 서로 다른 정보 소스의 데이터를 연관시키는 방법으로 보안 조치 가능
20.4	자동차 주행데이터를 변조하기 위한 데이터 조작 *주행거리, 주행 속도, 주행 방향 등		
20.5	시스템 진단 데이터에 대한 무단 변경		
21.1	시스템 이벤트 로그 무단 삭제/조작	M7	시스템 데이터/코드를 보호하기 위해 접근 통제 기술 및 설계가 적용되어야 함 *보안 조치의 예는 OWASP에서 참조 가능
22.2	악의적으로 소프트웨어를 조작		

23.1	자동차 제어 시스템 또는 정보시스템의 소프트웨어가 위조		
24.1	서비스 거부 *CAN 버스를 플러딩하거나 메시지 전송률을 높여 ECU의 고장을 유발하여 내부 네트워크에서 통신 중단 유발	M13	서비스 거부 공격을 감지하고, 복구 조치를 취해야 함
25.1	무단 접근을 통해 자동차 주요 기능의 구성 매개변수를 변조 *브레이크 데이터, 에어백 전개 임계값 등	M7	시스템 데이터/코드를 보호하기 위해 접근 통제 기술 및 설계가 적용되어야 함 *보안 조치의 예는 OWASP에서 참조 가능
25.2	무단 접근을 통해 충전 기능과 관련된 전압, 전력, 배터리 온도 등과 같은 매개변수를 변조		

6. 악용될 수 있는 잠재적 취약점에 대한 보안 조치

사이버공격 · 위협 또는 취약점의 예시		보안 조치	
26.1	암호키의 길이가 짧고 암호의 변경 주기가 긴 암호 알고리즘을 사용	M23	소프트웨어 및 하드웨어 개발 시 사이버보안 모범사례를 따라야 함
26.2	중요한 시스템을 보호하기 위한 암호 알고리즘을 적절히 사용하지 않음		
26.3	이미 사용 중지되었거나 곧 중단될 암호 알고리즘 사용		
27.1	사이버공격에 대응하기 위한 설계 기준을 충족하지 못하는 하드웨어 또는 소프트웨어 사용		
28.1	소프트웨어 버그 *소프트웨어 버그의 존재는 잠재적으로 공격 가능한 취약점이 될 수 있으며, 알려진 불량 코드/버그의 존재 여부 확인을 위한 테스트 혹은 알 수 없는 불량 코드/버그의 존재 위험을 줄이기 위한 테스트를 하지 않는 경우 발생할 수 있음	M23	소프트웨어 및 하드웨어 개발 시 사이버보안 모범사례를 따라야 함 *적절한 범위의 사이버보안 테스트 포함
28.2	개발용 인터페이스 등을 사용하여 공격자가 ECU에 접근하거나 상위 권한을 획득		

	*디버그 포트, JTAG 포트, 마이크로프로세서, 개발 인증서, 개발자 암호 등		
29.1	불필요한 인터넷 포트가 열려있어 네트워크 시스템에 대한 접근 허용		
29.2	네트워크 망분리를 우회하여 제어권 확보 *보호망을 우회하여 다른 네트워크 세그먼트에 대한 접근 권한을 획득하여, 임의의 CAN 메시지 전송과 같은 악의적인 행위를 수행하기 위하여 보호되지 않은 게이트웨이 또는 접근 지점을 공격 *특장 자동차(트럭 트레일러 게이트웨이 등)를 사용하는 경우를 예로 들 수 있음	M23	소프트웨어 및 하드웨어 개발 시 사이버보안 모범사례를 따라야 함

7. 차량 데이터 손실 및 데이터 유출과 관련된 위협에 대한 보안 조치

사이버공격 · 위협 또는 취약점의 예시		보안 조치	
31.1	정보 침해 *렌터카로 사용·판매되는 등 자동차 사용자가 바뀌면서 개인정보가 유출될 수 있음	M24	개인정보의 보관은 데이터 무결성 및 기밀성 보호를 위한 모범사례를 따라야 함

8. 시스템의 물리적 조작과 관련된 위협에 대한 보안 조치

사이버공격 · 위협 또는 취약점의 예시		보안 조치	
32.1	하드웨어 조작 *메세지 가로채기 공격 등을 위해 승인된 하드웨어(센서 등)를 승인되지 않은 하드웨어로 교체하거나, 자석을 사용하여 기어박스에 연결된 홀 효과 센서를 조작하는 방식 등으로 센서가 수집한 정보를 조작	M9	무단 접근을 방지 및 감지할 수 있는 대책을 취해야 함

9. 자동차와 관련된 백엔드 서버의 위협에 대한 보안 조치

사이버공격 · 위협 또는 취약점의 예시		보안 조치	
1.1 & 3.1	내부 직원의 권한 남용(내부자 공격)	M1	내부자 공격 위험을 최소화하기 위해 백엔드 서버에 보안 조치가 적용되어야 함
1.2 &	백엔드 서버에 대한 무단 인터넷 접근 *백도어, 패치되지 않은 시스템 소프트웨어 취약점, SQL 공격 또는 기타 수단에 의해 활성화	M2	무단 접근을 최소화하기 위해 백엔드 서버에 보안 조치가 적용되어야 함

3.3	화될 수 있음		
1.3 & 3.4	백엔드 서버에 대한 물리적인 무단 접근 *서버에 연결된 USB, 기타 매체 등으로 수행될 수 있음	M8	시스템 설계 및 접근 제어를 통해 권한이 없는 사용자가 개인 또는 시스템의 중요 데이터에 접근할 수 없어야 함 *보안 조치의 예는 OWASP에서 참조 가능
2.1	백엔드 서버에 대한 공격으로 인한 기능중단 *자동차와 상호작용하거나 자동차에서 요구하는 서비스를 제공하지 못하게 됨	M3	백엔드 서버가 서비스 제공에 중요한 경우 중단에 대비한 복구 대책 등의 보안 조치가 적용되어 있어야 함. *보안 조치의 예는 OWASP에서 찾을 수 있음
3.2	클라우드 정보 손실 *타 클라우드 서비스 공급업체에 데이터를 저장할 때, 중요한 데이터가 공격이나 사고로 인해 손실될 수 있음	M4	클라우드 컴퓨팅과 관련된 위험을 최소화하기 위한 보안 조치가 적용되어야 함 *보안 조치의 예는 OWASP 및 NCSC에서 참조 가능
3.5	의도하지 않은 데이터 공유로 인한 정보 침해(관리 오류 등)	M5	데이터 유출을 방지하기 위한 보안 통제가 백엔드 서버에 적용되어야 함 *보안 조치의 예는 OWASP에서 참조 가능

10. 데이터의 물리적 손실에 대한 보안 조치

사이버공격·위협 또는 취약점의 예시		보안 조치	
30.1	제삼자에 의한 피해, 교통사고, 도난 등 물리적인 손상으로 민감 데이터가 손실되거나 손상	M24	개인정보의 보관은 데이터 무결성 및 기밀성 보호를 위한 모범사례를 따라야 함 *보안 조치의 예는 ISO/SC27/WG5에서 참조 가능
30.2	DRM(디지털 권한 관리) 충돌 등으로 사용자 데이터가 손실되거나 손상		

30.3	IT 컴포넌트의 손상으로 민감 데이터의 무결성이 훼손되어 연쇄적인 문제가 발생 *키 변경의 경우		
------	--	--	--

※ 비교 : 위 표는 개정 당시 “UN Regulation No. 155, Annex 5의 Part B. Mitigations to the threats intended for vehicles” 및 “Part C. Mitigations to the threats outside of vehicles”를 참조하였음.

신 · 구조문 대비표

현 행	개 정 안
제2조(정의) 이 규칙에서 사용하는 용어의 뜻은 다음과 같다. 1. ~ 64. (생략) <u><신 설></u>	제2조(정의) ----- -----. 1. ~ 64. (현행과 같음) <u>65. “무선 업데이트”란 케이블 등의 연결 없이 무선으로 데이터를 전송하는 방법으로 자동차의 소프트웨어를 변경하는 것을 말한다.</u> <u>제18조의5(자동차 사이버보안) 자동차는 법 제30조의9제1항에 따른 자동차 사이버보안 관리체계 인증 내용에 따라 다음 각 호를 준수하여 제작되어야 한다.</u> <u>1. 자동차의 부품 및 시스템과 관련된 사이버공격·위협이 식별될 것</u> <u>2. 다음 각 목의 사항을 고려하여 자동차 사이버공격·위협이 평가될 것</u> <u>가. 자동차의 각 구성요소 및 구성요소 간 상호작용</u> <u>나. 자동차와 외부 시스템과의 상호작용</u> <u>다. 별표 5의38을 포함한 자</u>
<u><신 설></u>	

동차 사이버공격·위협

3. 제1호에 따라 식별된 자동차
사이버공격·위협이 제2호에
따른 평가 결과에 따라 적절
하게 관리될 것

4. 제3호에 따라 관리하는 자동
차 사이버공격·위협을 완화
하기 위하여 별표 5의39의 조
치가 적용될 것. 다만, 별표 5
의39의 조치가 제1호에 따라
식별된 사이버공격·위협과
관련이 없거나 충분하지 않은
경우 별도의 적절한 보안 조
치가 적용되어야 한다.

5. 자동차 판매 후 서비스·응
용 프로그램 실행 등을 목적
으로 인터페이스 등 전용 환
경을 제공하는 경우 제공된
전용 환경을 자동차 사이버공
격·위협으로부터 보호하기
위한 보안 조치가 적용될 것

6. 제4호 및 제5호에 따른 보안
조치의 효과를 확인하기 위하
여 국토교통부장관이 고시하
는 사항을 포함하여 적절하고
충분한 검증이 수행될 것

<신 설>

7. 자동차 사이버보안이 적정하
게 유지되고 있는지 확인하기
위해 다음 각 목의 기능을 갖
출 것

가. 자동차 사이버공격·위협
및 이와 관련된 취약점을
탐지하고 방지하는 기능

나. 탐지된 자동차 사이버공
격·위협 및 취약점을 제
작자등이 모니터링할 수
있도록 지원하는 기능

다. 자동차 사이버공격·위협
의 시도나 성공 여부 등에
대한 분석이 가능한 데이
터 포렌식 기능

8. 자동차의 부품 또는 자동차
부품을 제작·조립 또는 수입
하는 자(이하 “부품제작자등”
이라 한다)와 관련된 위험이
식별·관리될 것

제18조의6(소프트웨어 업데이트)

① 자동차의 소프트웨어는 그
버전을 확인할 수 있어야 한다.

② 제작자등이 자동차에 무선
업데이트를 실시할 경우 다음
각 호의 기준에 적합해야 한다.

1. 업데이트가 실패 또는 중단
된 경우 업데이트를 실시하기
이전 버전으로 되돌리거나 자
동차를 안전한 상태로 전환할
것

2. 업데이트 완료에 필요한 전
력 및 업데이트가 실패 또는
중단된 경우 제1호에 따른 조
치를 취하는데 필요한 전력이
있는 경우에만 업데이트가 실
행될 것

3. 업데이트 실행이 자동차의
안전에 영향을 주는 경우 기
술적 수단 등을 통해 업데이
트를 실행하는 동안 자동차를
안전한 상태로 유지할 수 있
음을 입증할 것

4. 업데이트 실행 전 다음 각 목
의 정보를 운전자에게 제공할
것

가. 업데이트 목적(리콜, 안전
또는 보안상의 중요성 등
을 포함)

나. 업데이트로 인한 자동차
기능의 변경 내용

다. 업데이트 완료까지의 예

	<u>상 소요 시간</u> <u>라. 업데이트 실행 중 사용이 불가능한 자동차의 기능</u> <u>마. 운전자가 업데이트를 실행할 때 참고해야 할 사항</u> <u>5. 운전 중 업데이트 실행 시 안전운행을 위협할 우려가 있는 경우 다음 각 목의 어느 하나를 만족할 것</u> <u>가. 차량 운행 중 업데이트 실행이 불가능할 것</u> <u>나. 운전자가 자동차의 안전 또는 업데이트 실행에 영향을 주는 기능을 이용할 수 없도록 할 것</u> <u>6. 업데이트 실행 후 다음 각 목의 정보를 운전자에게 제공할 것</u> <u>가. 업데이트의 성공 또는 실패 정보</u> <u>나. 업데이트로 변경된 사항</u>
--	--