AUTOCRYPT

UNECE WP.29 체크리스트

2020 년 6 월 UN 은 자동차 사이버 보안에 관한 두 가지 새로운 규정을 공식적으로 채택했습니다. 이에 따라 자동차 산업에 종사하는 경우 조직에서 수행해야 하는 몇 가지 작업 (OEM, Tier-1 공급 업체, 소프트웨어 제공 업체 등)이 있습니다.

CYBER SECURITY MANAGEMENT SYSTEMS (CSMS)

일반 산업 / 부문

- [ ] 차량 설계에서 사이버 보안 위험 식별 및 관리
- [ ] 테스트를 포함한 위험관리 확인
- [ ] 위험평가가 최신 상태로 유지되고 있는지 확인
- [ ] 사이버 공격 모니터링 및 대응
- [ ] 사이버 보안 성공된 사례 분석 지원
- [ ] 새로운 위협 및 취약성 평가

제조업체 부문

- [ ] CSMS 차량적용가능 확인
- [ ] 위험평가 분석 및 주요사항 식별
- [ ] 위험을 줄이기 위한 완화 조치 식별
- [ ] 완화 조치가 의도대로 작동하는지 식별
- [ ] 사이버공격에 대한 예방조치 확인
- [ ] 차량 유형별 활동 모니터링
- [ ] 모니터링 활동 보고서 승인기관 전송

SOFTWARE UPDATE MANAGEMENT SYSTEMS (SUMS)

일반 산업 / 부문

- [ ] 차량유형에 대한 하드웨어 및 소프트웨어 버전 기록
- [ ] 형식승인과 관련된 소프트웨어 식별
- [ ] 소프트웨어 구성요소 확인
- [ ] 소프트웨어 업데이트 및 상호 종속성 확인
- [ ] 차량 표적 식별 및 소프트웨어 업데이트 호환성 확인
- [ ] 소프트웨어 업데이트가 매개변수에 영향을 미치는지 확인
- [ ] 소프트웨어 업데이트가 안전에 영향을 미치는지 확인
- [ ] 차량 소유자에게 소프트웨어 업데이트 알림

제조업체 부문

- [ ] SUMS 차량적용가능 확인
- [ ] 소프트웨어 매커니즘 보호 및 무결성 보장
- [ ] 소프트웨어 식별번호 보호
- [ ] 차량에서 소프트웨어 식별번호 가능여부 확인

출처 : UN 유럽 경제위원회 정보부

OVER-THE-AIR (OTA) SOFTWARE UPDATES

- [ ] 업데이트 실패 시 복원기능
- [ ] 전원이 충분한 경우만 업데이트 실행
- [ ] 안전한 실행 보장
- [ ] 사용자에게 업데이트 완료됨을 확인 필요
- [ ] 차량이 업데이트 실행이 가능한지 확인 필요
- [ ] 정비가 필요할 경우 사용자에게 알림 필요