

BSI Training

Cyber Security Management Systems (CSMS)
(ISO/SAE 21434:2021)

교육 과정



By Royal Charter

bsi.

1. ISO/SAE 21434 이해 및 실무 과정

ISO/SAE 21434은 차량의 라이프 사이클 전체를 통해서 Cybersecurity 활동에 관한 프로세스를 정의하는 것을 목적으로 하고 있으며, 차량의 기획연구부터 시작하여 설계, 제조, 출하, 운용, 폐기 단계에서 발생 할 수 있는 사이버 공격이나 공격에 의한 피해의 발생 리스크를 줄이기 위해 단계별 모든 활동에 있어서 Cybersecurity 대응 체제를 구축 하고 운영 하는 것을 목표로 하고 있는 차량 사이버보안에 대한 규격입니다. 본 과정은 ISO SAE 21434 시스템 및 프로세스를 이해하고 ISO SAE 21434 사이버 보안 관리 시스템 구축 및 적용을 목표로 합니다.

- **교육 목적 및 기대효과**

- ISO SAE 21434 사이버 보안 엔지니어링 요구 사항과 관련된 지식 제공
- ISO SAE 21434 관리 시스템을 구축 및 적용을 위한 역량 강화

기간	교육 대상
2 일	<ul style="list-style-type: none">• CSMS(Cyber security Management System)에 대한 시스템 구축 및 실무 운영관련 담당자• 기업 보안 /프로젝트 개발 담당자• ISO/SAE 21434에 대한 이해를 증진하고자 하는 분

1. ISO/SAE 21434 이해 및 실무 과정

- 커리큘럼

교육내용	
Day 1	<ul style="list-style-type: none">• Vehicle Ecosystem 이해• ISO SAE 21434과 UNECE• 전반적인 사이버보안 관리 -조직 및 프로젝트• 프로젝트 기반의 사이버 보안 관리
Day 2	<ul style="list-style-type: none">• 지속적 사이버보안 관리• 리스크 평가관리• 개발, 생산, 운영, 폐차단계의 사이버보안 관리

2. ISO/SAE 21434 내부심사원 과정

사이버 보안 영역과 ISO SAE 21434의 요구 사항을 이해하고 사이버 보안에서 관련 위험 평가 및 CAL을 학습하고 ISO SAE 21434 내부심사원 양성을 위한 과정입니다.

ISO SAE 21434의 Audit 및 Assessment ? ISO/SAE 21434는 조직의 사이버보안 방침 및 목표 운영의 부합성을 모니터링 검증 하기 위해 다음과 같은 감사와 평가를 요구합니다

✓Cyber security audit : 조직의 사이버 보안 프로세스 운영에 대한 심사

✓Cyber security assessment : 개발 아이템이나 구성부품이 당초 설정한 사이버보안 목표를 달성 하는지 여부를 관련 사이버보안 계획 등을 토대로 운영에 대한 산출물을 검증 평가 하는 것

✓Note : 상기와 같은 Audit/ Assessment는 조직의 기존 시스템 심사와 통합 하여 진행 가능함(ISO9001/IATF16949 등)

• 교육 목적 및 기대효과

- ISO SAE 21434 사이버 보안 시스템 및 프로세스를 내부심사 할 수 있는 전문 인력 양성

기간	교육 대상
3일	<ul style="list-style-type: none">• ISO SAE 21434 내부심사원 및 내부심사원 양성 대상자• ISO SAE 21434 추진 실무자• CSMS(Cyber security Management System)에 대한 시스템 구축 및 실무 운영관련 담당자• 기업 보안 /프로젝트 개발 담당자

2. ISO/SAE 21434 내부심사원 과정

- 커리큘럼

교육내용	
Day 1	심사소개 <ul style="list-style-type: none"> • 심사안내(1자, 2자, 3자 심사), • 심사프로세스, 책임과 권한, 심사기법 • 심사계획/심사시작 • 심사증거, 부적합, 심사회, 종료회의 • 보고서작성
Day 2	<ul style="list-style-type: none"> • 자동차산업 소개 • ISO / SAE 21434 사이버보안경영시스템 (CSMS) 요구 사항 • 전반적인 사이버보안 관리 (Overall Cybersecurity Management) • 프로젝트 연관 사이버보안 관리 (Project dependent cybersecurity management) • 지속적인 사이버 보안 활동 (Continuous cybersecurity activities)
Day 3	<ul style="list-style-type: none"> • 위험 평가 방법 (Risk assessment methods) • 개념(Concept) • 제품 개발 및 사이버 보안 검증 (Product development and cybersecurity validation) • 운영 및 유지 보수 (Operations and maintenance) • 해체(Decommissioning) • 문서심사/ 현장심사/ 보고서작성/부적합보고서/종료회의