SAE J3061 and ISO/SAE 21434:2021 Automotive Cybersecurity Certification

Course Duration: 5 Days - 8 Hours/day

SAE J3061 and ISO/SAE 21434:2021 Automotive Cybersecurity Certification

Course Duration: 5 Days - 8 Hours/day

This five-day seminar covers all 14Clauses of the ISO/SAE 21434 standard to give those attending the information necessary to understand the standard, and move your organization toward conformance.. An overview of ISO 27001, United Nations (UN) regulation WP.29, and VDA ACMS (Automotive Cybersecurity Management System) will also be provided. ISO/SAE 21434 is the cybersecurity standard that is applied to Cybersecurity Related Systems that include electric/electronic, wired and wireless communication systems installed in production passenger vehicles. The course combines presentations with hands-on work and is conducted in English. There is an optional ISO/SAE 21434 Certification exam at the end of the class for those wanting to demonstrate and document their knowledge.

This course combines presentations, along with in-class group exercises to put what you are learning into practice. Concepts are reinforced by a running case study of an air bag system. Forms are used to complete the exercises as a part of the integrated workshops that include Item Definition, Threat Analysis and Risk Assessment (TARA), Cybersecurity Goals, CAL levels, Cybersecurity Concept, and Hardware/Software Interface.

Learning Objectives

- Tailor the necessary activities to support vehicle cybersecurity lifecycle management, development, production, operation, service, and decommissioning
- Information provided in the class can be used for ISO/SAE 21434 implementation

- Understand cybersecurity aspects of the entire development process including requirements specification, design, implementation, integration, verification, validation, and configuration.
- Understand the risk-based approach for determining risk classes cybersecurity assurance levels (CALs)
- Use CALs for achieving an acceptable residual risk
- Provide requirements for validation and confirmation measures to ensure a sufficient and acceptable level of cybersecurity is being achieved.

Seminar Outline

Daily Agenda (approximate, based on class discussions)

Day One

- Chapter 1: Introduction and Overview to ISO/SAE 21434, ISO 27001, WP.29, and VDA ACMS.
- ISO/SAE 21434 Purpose, Scope and Framework
- Chapter 2: Overall Cybersecurity Management (Clause 5)
- Cybersecurity Governance
- Cybersecurity Culture
- Cybersecurity Risk Management
- Cybersecurity Audit
- Information sharing
- Confirmation Measures
- Chapter 3: Project Dependent Cybersecurity Management (Clause 6)
- Tailoring of Cybersecurity Activities
- System or Component out of Context
- Cybersecurity Planning
- Cybersecurity Case

CONSULTING · TRAINING · SOFTWARE

SAE J3061 and ISO/SAE 21434:2021 Automotive Cybersecurity Certification

Course Duration: 5 Days - 8 Hours/day

- Breakout Exercise 1: Safety Case Outline
- Chapter 4: Post-Development Phases (Clauses 10-13)
- Production, Operation, Maintenance, and Decommissioning
- Chapter 5: Concept Phase (Clause 8)
- Cybersecurity Relevance
- Item Definition
- Breakout Exercise 2: Item Definition

Day Two

- Chapter 5: Concept Phase (Clause 8) *(cont'd)*
- Threat Analysis and Risk Assessment (HARA)
- **Breakout Exercise 3: Threat and Risk Analysis**
- Cybersecurity Goals
- Cybersecurity Concept
- **Breakout Exercise 4: Cybersecurity Requirements**
- Chapter 6: CAL-Oriented and Cybersecurity-Oriented Analyses (Annex F)
- Cybersecurity Assurance Levels (CAL)
- Usage of CALs
- Chapter 7: Risk Assessment Methods (Clause 7)
- Asset Identification
- Vulnerability Analysis
- **Breakout Exercise 5: Vulnerability Analysis**
- Attack Feasibility Analysis
- Risk Determination
- Risk Treatment

Day Three

- Chapter 8: Product Development I (Clause 9.1)
- Introduction to Design & Verification
- Structure of Cybersecurity Requirements
- Refined Cybersecurity Design
- Cybersecurity Controls
- Design Principles
- Chapter 9: Product Development II (Clause 9.1)
- Hardware Development
- Reference Model
- Hardware Design Principles
- Chapter 10: Product Development III (Clause 9.1)
- Software Development I
- Design Principles
- **Breakout Exercise 6: Walkthrough vs. Inspection**
- Design Verification

Day Four

- Chapter 11: Product Development IV (Clause 9.1)
- Software Development II
- Verification Compliance
- Testing Environments
- Item Integration and Testing
- System Integration and Testing
- Test Cases
- Chapter 12: Validation at Vehicle Level & Release for Post-Development (Clauses 9.2 & 9.3)
- Cybersecurity Validation
- Cybersecurity Assessment

CONSULTING • TRAINING • SOFTWARE

SAE J3061 and ISO/SAE 21434:2021 Automotive Cybersecurity Certification

Course Duration: 5 Days - 8 Hours/day

- Breakout Exercise 6: Developing a Cybersecurity Case
- Release for Post-Development

Day Five

- Chapter 13: Supporting Processes (Clause 14)
- Quality Management Systems
- Change Management
- Documentation Management
- Configuration Management
- Requirements Management
- Verification
- Breakout Exercise 8: Confidence in Management Systems
- Tool Management
- Distributed Cybersecurity Activities
- Chapter 14: ISO/SAE 21434 Implementation Strategy

Optional ISO/SAE 21434 Certification Exam
– Final 3 hours of Day Five

Note: The materials will include SAE J3061 content as applicable. Contact Omnex for the Auditor and Assessor Competencies and Learning Objectives of this course.

Three Levels of Certification

Level 1

Cybersecurity Engineer

Knowledge Requirements:

- 1 week of Cybersecurity training and candidates must pass a three hour final exam.

Prerequisites:

- At least 3 years of relevant professional experience,

Level 2

Cybersecurity Engineer Professional

Knowledge Requirements:

- 1 week of Cybersecurity training and candidates must pass a three hour final exam.

Prerequisites:

- One case study demonstrating experience in Automotive Cybersecurity which can be verified. The case study should show a broad understanding from Safety Planto Safety Case (work products)
- Interview
- At least 5 years of relevant industry experience.

Level 3

Cybersecurity Expert

Knowledge Requirements:

- 1 week of Cybersecurity training and candidates must pass a three hour final exam.

Prerequisites:

- Two case studies demonstrating ability to do confirmation measures, evidence of communication.
- Interview
- At least 10 years of relevant industry experience.

Who Should Attend

Those involved in the design, development, and production of electrical and electronic based vehicle products, including the systems, software and hardware engineers, and managers.

CONSULTING ★ TRAINING ★ SOFTWARE

SAE J3061 and ISO/SAE 21434:2021 Automotive Cybersecurity Certification

Course Duration: 5 Days - 8 Hours/day

Basically, all those responsible for the development and implementation of hardware and software systems in motor vehicles.

Participants should be, or plan to be, actively managing, or involved in, or aware of electrical and/or electronic items, systems, or elements that are incorporated in motor vehicles. And have the abilities, education, and experience required for the above roles.

Seminar Materials

Each participant will receive a seminar manual including case studies.

Pre-Requisite

Participants should be involved in or aware of software and hardware development as it relates to the motor vehicle industry.

CONSULTING · TRAINING · SOFTWARE