APEX
QUALITY ASSURANCE

5-Day

ISO/SAE 21434 Automotive Cybersecurity Certification with UNECE R155 Considerations

Information Security Management Systems

Register by phone

919-635-5581

Register online

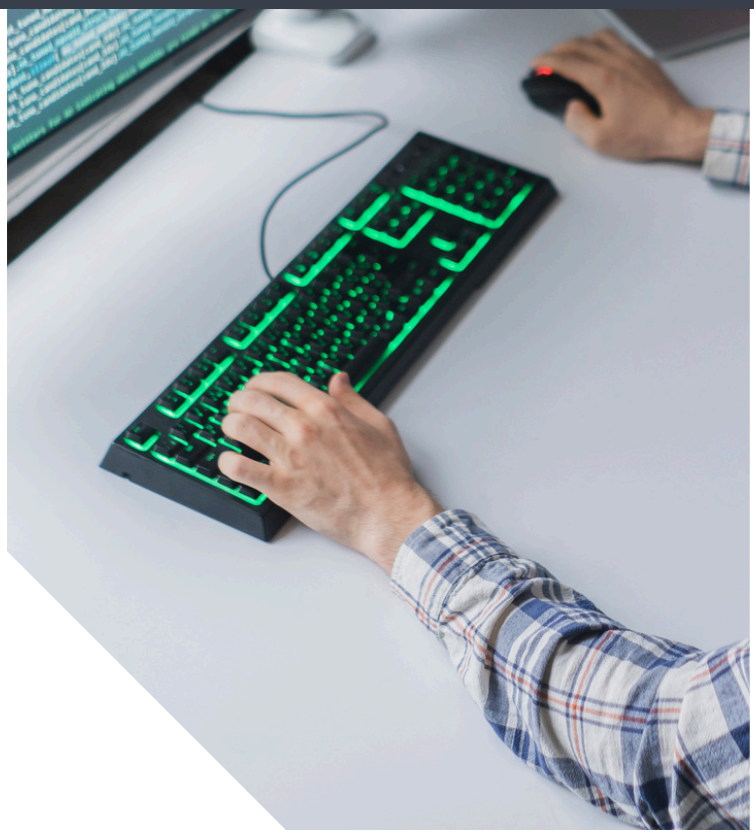
www.apexqualityassurance.com

At A Glance

ISO/SAE 21434 Automotive Cybersecurity Certification with UNECE R155 Considerations for Information Security Management Systems

Gain the knowledge and tools to implement ISO/SAE 21434 in your organization.
This comprehensive seminar equips you with a deep understanding of the ISO/SAE 21434 standard, all in five days. Through a combination of lectures and practical exercises, you'll learn how to achieve compliance and integrate cybersecurity best practices throughout your vehicle development process.
Key benefits:

- Grasp all 14 clauses of ISO/SAE 21434.
- Understand how the standard aligns with UN regulations WP.29, R155 & R156, and VDA ACMS.
- Apply cybersecurity principles to electric/electronic systems, wired and wireless communication networks in modern vehicles.
- Participate in interactive workshops that reinforce learning through real-world applications. (e.g., Airbag system case study covering Item Definition, TARA, Cybersecurity Goals, and Hardware/Software Interface considerations)
- Prepare for the optional ISO/SAE 21434 Certification exam (offered at the end of the course) to validate your expertise.



Learning Objectives

- Determine the Relevance of Automotive Cybersecurity for Specific Products
- Determine the Applicability of ISO/SAE 21434 in Your Organization and Current Products
- Plan and Perform Cybersecurity Management Activities
- Perform a Basic TARA
- Perform Activities of the Concept Phase
- Perform Activities of the Product Development Phases
- List and Describe Applicable Activities of the Production, Operations & Maintenance, and Decommissioning Phases for a Typical Project
- Develop a Plan for Continual Cybersecurity Activities for a Typical Project
- Perform Distributed Cybersecurity Activities for a Typical Project
- Develop a Plan to Implement Automotive Cybersecurity
- Develop a Plan to Implement ISO/SAE 21434 for a Typical Project

Seminar Outline

Chapter 1: Overview of Automotive Cybersecurity and ISO/SAE 21434

- List and describe some automotive cybersecurity issues
- Determine the relevance of some automotive cybersecurity issues for specific products
- Identify and describe some processes in your organization that might benefit from ISO/SAE 21434
- Identify and describe some products/projects in your organization that might benefit from ISO/SAE 21434
- Breakout Exercise 1: Determine the Applicability of Automotive Cybersecurity and ISO/SAE 21434

Chapter 2: Cybersecurity Management (Clauses 5 & 6)

- Plan and perform cybersecurity management activities at the organizational level
- Plan and perform cybersecurity management activities at the product/project level
- Breakout Exercise 2: Define the Cybersecurity Case

Chapter 3: TARA and the Concept Phase (Clauses 15 & 9)

- Develop the Item Definition for a typical project
- Breakout Exercise 3: Create the Item Definition
- Perform an automotive TARA for a typical project
- Breakout Exercise 4: Perform a TARA
- Define cybersecurity goals for a typical project
- Develop the cybersecurity concept for a typical project
- Breakout Exercise 5: Develop the Cybersecurity Goal, Cybersecurity Requirements, and Cybersecurity Concept

Chapter 4: Product Development Phases (Clauses 10 & 11)

- Perform product development activities for a typical project
- Breakout Exercise 6: Derive Flow-down of Hardware and Software Requirements
- Perform cybersecurity validation activities for a typical project

Chapter 5: Post-Development Phases (Clauses 12, 13 & 14)

- Perform activities of the production, operations and maintenance, and decommissioning phases for a typical project

Chapter 6: Continual Cybersecurity Activities (Clause 8)

- Execute a plan for continuous cybersecurity activities for a typical project
- Breakout Exercise 7: Develop Cybersecurity Plans (Continual Cybersecurity Activities and Incidence Response)

Chapter 7: Distributed Cybersecurity Activities (Clause 7)

- Perform distributed cybersecurity activities for a typical project
- Breakout Exercise 8: Develop a Cybersecurity Interface Agreement

Chapter 8: Implementing Automotive Cybersecurity

- Develop a plan to implement automotive cybersecurity for a typical project

Chapter 9: ISO/SAE 21434 Implementation Strategy

- Develop a plan to implement ISO/SAE 21434 for a typical project

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 Cybersecurity which can be verified. The case study should show a broad understanding from Cybersecurity Plan to Cybersecurity 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 the ability to do confirmation measures, and evidence of communication. • Interview. • At least 10 years of relevant industry experience.

Attendees successfully completing the examinations provided in conjunction with this course receive a Certificate of Completion from Apex Quality Assurance.