Updated 10/10/2024

Sign up

Automotive cybersecurity standard training (ISO 21434)

2 days (14 hours)

Presentation

Our ISO 21434 Automotive Cybersecurity training course will help you understand and apply the requirements of this essential standard in the automotive industry. This training is designed to help you integrate robust cybersecurity practices into the early design phases of your vehicles and systems.

During this training course, you will learn about the critical issues of cybersecurity in the automotive industry, the relevant international regulations and risk analysis methods specific to the automotive sector.

On completion of this course, you will be able to effectively manage cybersecurity throughout the life cycle of your products, from design to decommissioning, while meeting the requirements of current regulations.

Objectives

- Understand the challenges of cybersecurity in the automotive industry and the main threats and vulnerabilities.
- Acquire in-depth knowledge of ISO 21434
- Mastering cybersecurity management phases, from design to decommissioning
- Apply risk analysis and threat management (TARA) methodologies
- Manage cybersecurity incidents and implement update and continuous improvement strategies
- Keep abreast of technological developments and standards to ensure cybersecurity proactive

Target audience

- Cybersecurity engineers
- Risk management managers
- Embedded software developers
- Automotive project managers
- Quality and compliance managers
- Anyone involved in the design, development and maintenance of automotive systems

Prerequisites

- No on-board safety experience required
- Knowledge of automotive infrastructure is a plus

OUR AUTOMOTIVE CYBERSECURITY STANDARD TRAINING PROGRAM

INTRODUCTION TO AUTOMOTIVE CYBERSECURITY AND THE ISO 21434 STANDARD

- Presentation of cybersecurity issues in the automotive industry
- General introduction to ISO 21434
- Distinction between safety and cybersecurity
- The impact of new technologies on automotive cybersecurity
- Overview of major threats and vulnerabilities

FUNDAMENTALS OF CYBERSECURITY MANAGEMENT ACCORDING TO ISO 21434

- Understanding the structure and objectives of the standard
- Organizational cybersecurity management
- The importance of integrating cybersecurity right from the design stage
- Cybersecurity management phases: from design to decommissioning
- Roles and responsibilities in implementing the standard

INTERNATIONAL REGULATIONS AND CERTIFICATION

- Overview of UN Regulations n°155 and n°156
- Certification process and requirements for cybersecurity management systems (CSMS)
- Cybersecurity management in the supply chain
- Implications of these regulations for current practices

RISK ANALYSIS AND ASSESSMENT METHODS (TARA)

- Introduction to risk analysis and threat management methodology (TARA)
- Approaches to identifying and assessing cybersecurity risks
- Practical examples and case studies
- Application of TARA in the automotive development cycle

INCIDENT MANAGEMENT AND CYBERSECURITY UPDATES

- Principles of cybersecurity incident management
- Strategies for updating systems in response to discovered vulnerabilities
- Standard requirements for continuous monitoring and improvement
- Case studies on managing security updates and patches

TECHNOLOGY AND STANDARDS WATCH

- Recent developments in ISO 21434
- Impact of the Internet of Things (IoT), AI and the digital twin on automotive cybersecurity
- Discussion on future updates and evolutions of the standard
- The importance of technology and standards monitoring to stay up to date

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire enabling us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives with regard to the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.