Automotive Cybersecurity (Based on ISO/SAE 21434)

Foundations of Secure Development for Connected Vehicles

About SANEON

SANEON is an engineering-driven consulting company specializing in automotive functional safety and safety-critical system development. Our trainers are active practitioners with experience in complex OEM and supplier programs, covering system architecture, hardware metrics, software safety, and safety analyses.

Our training programs are derived from real project experience and designed to bridge the gap between standard interpretation and practical implementation.

Why This Training Matters

Modern vehicles are increasingly connected, software-driven systems that interact with external networks and services. This connectivity introduces new cybersecurity risks that must be addressed throughout the development lifecycle. Cybersecurity incidents can lead to:

- Unauthorized access to vehicle systems
- Manipulation of vehicle functions
- Data breaches and privacy violations
- Safety risks resulting from malicious attacks

ISO/SAE 21434 provides a structured framework for managing cybersecurity risks in automotive systems.

Training Overview

This training introduces the fundamentals of automotive cybersecurity and the development processes defined in ISO/SAE 21434. Participants learn how cybersecurity considerations integrate into system development and how organizations can identify, assess, and mitigate cybersecurity risks.

The training provides a practical understanding of cybersecurity activities across the engineering lifecycle.

Detailed Agenda – [1 day**]

Part 1- Foundations of Automotive Cybersecurity	
▪ Introduction to cybersecurity in connected vehicles ▪ Overview of automotive cybersecurity standards ▪ Interaction between cybersecurity, functional safety, and engineering processes ▪ Project-dependent & continual cybersecurity activities ▪ Cybersecurity activities across the development lifecycle	09:00 – 12:00
Part 2- Secure Development & Risk Management	
▪ Secure system and software architecture principles ▪ Secure onboard communication ▪ Threat Analysis and Risk Assessment (TARA) ▪ Verification & validation of cybersecurity requirements ▪ Practical examples of automotive cybersecurity scenarios	13:00 – 17:00

Practical Focus

- Identification of typical attack surfaces in vehicle architectures
- Discussion of cybersecurity risks in connected vehicle functions
- Example of a simplified TARA exercise
- Analysis of interactions between automotive safety & cybersecurity

Target Audience

- System Engineers
- Software Engineers
- Cybersecurity Engineers
- Functional Safety Engineers
- Quality and Project Managers

Learning Outcomes

Participants will be able to:

- Understand the principles of automotive cybersecurity and ISO/SAE 21434
- Identify typical cyber threats and attack surfaces in connected vehicles
- Perform a threat analysis and risk assessment (TARA) concepts
- Integrate cybersecurity activities into system development processes
- Fundamentals of secure onboard communication

Pre-requisites

- Basic understanding of system or software development in automotive environments.

Participants Receive:

- Professional training material*
- Certificate of participation

Delivery Format

- Onsite | Live Online | Hybrid

Training & Coaching Language

- English

Additional Services

Do you need a personalized offer about this course? Feel free to contact us at contacting@saneon.de

We also offer further services beyond the scope of this training:

- Safety concept review workshops
- ISO 26262 Gap Analysis
- Project-specific coaching
- Assessment preparation support

* Printed material offered for onsite trainings only.
** Extended 2-day version available upon request.