

DE0610 Road Vehicle Cybersecurity in context of ISO/SAE 21434 – in depth

This training will support to lay a basis for the **understanding of Automotive Cybersecurity** which is one of the most important topics for the future of highly automated and connected vehicles.

It will provide **guidance and suggestions** for the topics:

- Understanding and interpreting the ISO/SAE 21434
- TARA (Threat-Analysis-and-Risk-Assessment) and Vulnerability Analysis
- Cybersecurity Mitigations and Controls
- Secure SW Development
- Security Verification and Validation

Prerequisites: an understanding of engineering in road-vehicle industry (OEM, TIER1, TIER2) is recommended.

Notes:

- The training is a compilation of DE0602 and DE0604. More details can be looked up in those flyers
- Participation is recommended before applying for CACE/S-automotive speciality personal certification

DE0610 Road Vehicle Cybersecurity in context of ISO/SAE 21434 – in depth

Who should attend?

- ♦ Automotive Cybersecurity responsible persons
- ♦ Functional Safety Engineers – who wants to understand how they are impacted by Cybersecurity
- ♦ Development Engineers (System, Hardware and Software)
- ♦ Product Managers
- ♦ Project Leaders of cybersecurity related development projects
- ♦ Process Managers
- ♦ Quality Managers

Duration:

3.5 days (or in-house, jointly agreed, please contact us for more information)

Language:

Depending on the participants the training will be given in German or English. The training material will be in English.

Location:

exida.com GmbH office
Prof.-Messerschmitt-Str. 1
85579 Neubiberg / Germany
or online

Certificate:

Each participant gets a letter of attendance.

For more information, please contact:

Kerstin Tietel

☎ +49 89 44118232

✉ kerstin.tietel@exida.com

DE0610 Road Vehicle Cybersecurity in context of ISO/SAE 21434 – in depth

Agenda and Content

Intro

- Awareness & Motivation
- Cybersecurity & Functional Safety
- Standards overview

ISO/SAE 21434

- General
- Cybersecurity Management
 - Organizational
 - Project dependent
 - Post-development related
- Concept Phase
- Product Development

Cybersecurity Analysis

- Assets/Properties/Impacts -> Risks
- TA-RA
- TARA vs VA
- ATA vs TMEA (STRIDE Analysis)

Beyond ISO/SAE 21434

- Measures & Mitigations
 - Cryptography, why?
 - Architectural considerations
 - Quality Measures
- Brainstorm on Attacks

Secure by Design

- Design principles & patterns
- Attack surface analysis
- Supply chain security considerations

- Programming language selection & toolchains

◆ **Secure Coding**

- Memory safety & type safety
- Coding guidelines & industry best practices
- Understanding programming mistakes and their security impact
- Avoiding & detecting common software vulnerabilities for selected software weaknesses (CWE)

◆ **Secure Verification**

- Static & dynamic analysis
- Secure code review
- Fuzzing & other security testing techniques
- Introduction to penetration testing

