

# DE0602 Road Vehicle Cybersecurity in context of ISO/SAE 21434

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 including an understanding of its main aspects and work-products (CSMS, planning, audit, assessment, TARA, Vulnerability analysis, ....)
- Cybersecurity Mitigations and Controls
- Understanding some attacks

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

Notes:

- The training prepares for taking the A-CSP (Automotive-Cybersecurity-Practitioner) Exam. It does not prepare for the CACE/S automotive personal certification.

# DE0602 Road Vehicle Cybersecurity in context of ISO/SAE 21434

## Who should attend?

- ♦ Automotive Cybersecurity responsible persons
- ♦ Functional Safety Engineers – who want 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:

2,5 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](mailto:kerstin.tietel@exida.com)

# DE0602 Road Vehicle Cybersecurity in context of ISO/SAE 21434

## 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