

Have you ever asked yourself how to develop a Cybersecure System in an Automotive context?

Have you ever wondered how to analyse Cybersecurity Threats and Risks?

Have you ever thought about Cybersecurity principles and best practise?

Do you know about the situation and status of Automotive and other Cybersecurity Standards?

Join our training and learn more about Automotive Cybersecurity

DE0206 Automotive Cybersecurity

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 critical topics such as threat analysis and risk assessment, cybersecurity related requirements, architecture and design or verification & validation.

The learning success will be supported by practical examples and exercises.

The training will also include the **interpretation and application** of standards such as the upcoming Automotive Cybersecurity standard ISO/SAE 21434, recommended practise like SAE J30161 or other like IEC 62443.

Also the relationship between Automotive Functional Safety and Cybersecurity will be discussed.

General approach:

- The *exida* approach is to explain **how** the requirements of various standards and regulations can be fulfilled, and not only to show and introduce their requirements.
- The standards and guidelines define a route, typical **solutions** are exemplified using e.g. tools delivered or recommended by *exida.com* (SafetyCaseDB, FMEDA-Tools, Enterprise Architect and other).

DE0206 Automotive Cybersecurity

Who should attend?

- ◆ Automotive Cybersecurity responsible persons
- ◆ Development Engineers (System, Hardware and Software)
- ◆ Product Managers
- ◆ Project Leaders of cybersecurity related development projects
- ◆ Process Managers
- ◆ Quality Managers

Duration:

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

Language:

Can be chosen between German or English, training material will be in English

Location:

exida.com GmbH office
Prof.-Messerschmitt-Straße 1
D-85579 Neubiberg / Germany

Certificate:

Each participant gets a letter of attendance.

For more information, please contact:

Kerstin Tietel

☎ +49 89 44118232

✉ trainings.germany@exida.com

DE0206 Automotive Cybersecurity

Agenda and Content

- ◆ Introduction to Automotive Cybersecurity
 - Current situation and status of standards and guidelines
 - Definitions and terms
 - Cybersecurity principles
 - Relationship between Safety and Security
- ◆ Management of Functional Safety
- ◆ Cybersecurity Lifecycles and process overview
- ◆ Cybersecurity analysis techniques
 - Asset Analysis
 - Threat Analysis and Risk Assessment
 - Goals
 - Introduction to best practise methods
 - Identification of Cybersecurity Goals
 - Vulnerability Analysis
- ◆ Cybersecurity Concepts and Requirements
- ◆ Product development incl. design and architecture, principles and practise, integration and testing on
 - System level
 - Hardware level
 - Software level
- ◆ Vulnerability and penetration testing
- ◆ Cybersecurity Assessment
- ◆ Supporting Processes
 - Change Management
 - Configuration Management
 - Documentation Management
 - Tool Management