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

Have you wondered **how** to analyse **Cybersecurity** Threats and Risks in your **Automotive** context?

Have you ever thought about **Cybersecurity Principles** and best practise?

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

Do you understand the **relationship** between **Functional Safety** and **Cybersecurity**?

Join our training and learn more about Automotive Cybersecurity

DE0601 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 applica**tion 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 ISO262626 and Automotive Cybersecurity ISO/SAE 21434 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).

DE0601 Automotive Cybersecurity

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:	1.5 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-Straße 1 D-85579 Neubiberg / Germany
Certificate:	Each participant gets a letter of attendance.

For more information, please contact:
Kerstin Tietel
+49 89 44118232
kerstin.tietel@exida.com

DE0601 Automotive Cybersecurity

Agenda and Content

- Cybersecurity Awareness & Motivation
- Cybersecurity & Functional Safety
- Cybersecurity Goals
- Cybersecurity Standards Overview
- Cybersecurity Management
- Analysis of cybersecurity risks (TARA)
- Cybersecurity Measures
- Cybersecurity Attack Principles