DE0604 Secure Software Development – in context of ISO/SAE 21434

This training will support to lay a basis for **understanding and performing secure software development in context of road vehicles** which is one of the key topics for the future of highly automated and connected vehicles.

This training delves into the crucial aspects of secure software development, equipping you to protect components of modern road vehicles from evolving threats.

Prerequisites: The training builds on DE0602-Road Vehicle Cybersecurity in context of ISO/SAE 21434. Participants which already bring an understanding of ISO/SAE 21434 and its work-products might consider skipping DE0602.

What You'll Gain

- Comprehensive understanding of ISO/SAE 21434 and its implications for software security
- Practical skills to identify and mitigate software vulnerabilities in automotive systems
- Techniques to integrate secure practices throughout the software development lifecycle
- Confidence in delivering road-vehicle cybersecurity solutions that align with industry standards

DE0604 Secure Software Development – in context of ISO/SAE 21434

Who should attend?

- Software Development Engineers (System, Hardware and Software)
- Project and Product Managers in automotive and embedded systems
- Software Architects overseeing vehicle software design
- Software Developers of automotive applications
- Functional Safety Engineers – who want to understand how they are impacted by Cybersecurity
- Process Managers
- Quality Managers

Duration: 1 day (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

DE0604 Secure Software Development – in context of ISO/SAE 21434

Agenda and Content

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