

## Security of Embedded Systems in the Context of Functional Safety - Face-to-Face Training

### Objectives

You know about potential security vulnerabilities in embedded systems, such as in the context of IoT, and you learn how to assess the related risks (risk assessment).

Efficient solutions help you minimize these vulnerabilities by means of specific IP blocks and/or strategies.

Your benefit:

Efficient and compact jump-start into the overall topic

Practical tips on safety and security

Templates on USB stick or as download.

### Participants

Hardware and software architects, hardware and software developers, test engineers, project managers, system engineers

### Requirements

Experience with embedded systems as well as basic knowledge of safety

## Security of Embedded Systems in the Context of Functional Safety - Face-to-Face Training

### Content

#### Threats and Attack Scenarios

- Security incidents
- Concerns
- Applications
- Authentication
- Communication protocols
- Terms and definitions
- Vulnerabilities
- Impacts
- A case study
- Defense in depth
- Classes of attackers
- Security - an ongoing process
- Security by design
- Security mindset
- Management challenge
- Security development lifecycle (SDL)
- Threat models

#### Risks and Efforts

- Procedure
- Classic approach to risk management
- Assurance matrix
- Risk matrix concept

- TARA
- Determining a generic method for risk assessment
- New approach to risk management
- A glimpse into IT security risk assessment
- Security goals
- Selected TARA methods and vulnerability analysis
- EVITA
- TVRA

**Generic Application of Countermeasures**

- Security principles
- List of exemplary countermeasures
- Countermeasures as requirements
- Industry and government security initiatives
- Cryptography
- Defense in depth
- Security zones
- Security conduits
- EVITA
- HIS - SHE
- ARM security
- Security development lifecycle (SDL)
- Software security matters
- Trusted platform module
- Security testing methods

**Selected Vulnerabilities and Countermeasures**

- Stack based buffer overflow
- Code reuse
- Countermeasures
- Boundary error vulnerabilities
- Memory management and security
- Debugging and security

**Norms and Standards****Partial ISO/IEC List**

- Other standards and work
- IEC 62443
- Certification
- SAE J3061™

**Security in a Safety Context**

- Safety and security differences
- Subsets of product assurance
- Relations between safety and security
- Leveraging commonalities
- Security in safety norms
- Rules for industrial control systems (ICS)
- Inheritance of safety principles
- Comparisons
- Communication paths

**FACE-TO-FACE TRAINING**

**Price \***                      **Duration**

700,00 €                      1 day

Training code: E-SECFUSI

\* Price per attendee, in Euro plus VAT

**Face-To-Face - German**

**Date**                              **Duration**

26.01. – 26.01.2023 1 day

22.05. – 22.05.2023 1 day

13.10. – 13.10.2023 1 day

26.01. – 26.01.2024 1 day

### **Live Online - German**

<b>Date</b>	<b>Duration</b>
-------------	-----------------

26.01. – 26.01.2023	1 day
---------------------	-------

22.05. – 22.05.2023	1 day
---------------------	-------

13.10. – 13.10.2023	1 day
---------------------	-------

26.01. – 26.01.2024	1 day
---------------------	-------

### **Coaching**

Our coaching services offer a major advantage: our specialists introduce their expertise and experience directly in your solution process, thus contributing to the success of your projects.

We will be happy to provide you with further information or submit a quotation tailored to your requirements.