

## Security: Sicherheit von Embedded-Systemen im Kontext der funktionalen Sicherheit - Live-Online-Training

### Ziele - Ihr Nutzen

Sie wissen um potentielle Sicherheitslücken in eingebetteten Systemen (embedded systems), wie z.B. IoT und können daraus entstehende Gefahren einschätzen (Risikobewertung).

Effiziente Lösungsansätze erlauben, diese Lücken mithilfe von ausgewählten IP-Blöcken und/oder Strategien zu schließen.

Ihre Vorteile:

Effektiver und zeitsparender Einstieg in die Gesamthematik

Praktische Tipps zu Security und Safety

Templates auf USB-Stick oder als Download.

### Teilnehmer

Hardware- und Software-Architekten, Hardware- und Software-Entwickler, Testingenieure, Projektmanager, Systemingenieure

### Voraussetzungen

Erfahrung im Zusammenhang mit Embedded-Systemen sowie Grundkenntnisse im Bereich Safety

### Live Online Training

26.01. – 26.01.2023 700,00 € 1 Tage

22.05. – 22.05.2023 700,00 € 1 Tage

13.10. – 13.10.2023 700,00 € 1 Tage

26.01. – 26.01.2024 700,00 € 1 Tage

\* Preis je Teilnehmer, in Euro zzgl. USt.

Anmeldecode: L-SECFUSI

### Präsenz-Training - Deutsch

Termin	Dauer
--------	-------

26.01. – 26.01.2023	1 Tag
---------------------	-------

22.05. – 22.05.2023	1 Tag
---------------------	-------

13.10. – 13.10.2023	1 Tag
---------------------	-------

26.01. – 26.01.2024	1 Tag
---------------------	-------

### Präsenz-Training - Englisch

Dauer

1 Tag

**Security: Sicherheit von Embedded-Systemen im Kontext der funktionalen Sicherheit - Live-Online-Training****Inhalt****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
- The Security Mindset
- The Management Challenge
- Security Development Lifecycle (SDL)
- Threat Models

**Risks and Efforts**

- Procedure
- Classic Approach to Risk Management
- The 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

**HINWEIS: Die Kursunterlagen sind auf Englisch**