Stand 28.04.2026

Security Engineering: Security Fundamentals for Embedded Systems - Live Online Training

**Ziele -
Ihr Nutzen**

Security requires a holistic view. The foundations lie outside the actual implementation. This is also reflected in the Cyber Resilience Act (CRA), focusing on reliabilities and a structured handling of security issues. How do you identify potential security vulnerabilities in embedded systems, and how can you assess and eliminate them efficiently? This includes the most significant cryptographic processes and their application as well as specific hardware and software concepts. You know the details of ISO/SAE 21434, one of the most essential security standards, and can comply with the related requirements.

Your benefit:

Jump-start into the security topic with compact knowledge

Functional security (safety) context

Details on ISO/SAE 21434

Exercise: TARA in the concept phase

Training documentation as a kompendium

Teilnehmer

The Security Engineering seminar addresses managers (project, security/ safety), process & method engineers as well as system analysts/ system designers/ system architects

Voraussetzungen

Experience with embedded systems as well as basic safety knowledge of are an advantage.

Live Online Training

* Preis je Teilnehmer, in Euro zzgl. USt.

Anmeldecode: LE-SECFUSI

Präsenz-Training - Englisch

Termin	Dauer
15.06. – 16.06.2026	2 Tage

Live-Online - Deutsch

Termin	Dauer
14.09. – 15.09.2026	2 Tage

Präsenz-Training - Deutsch

MICRO CONSULT

Stand 28.04.2026

Termin	Dauer
15.06. – 16.06.2026	2 Tage

Security Engineering: Security Fundamentals for Embedded Systems - Live Online Training

Inhalt

Threats and Attack Scenarios

- Security incidents
- Terms and definitions
- Vulnerability databases
- Impacts
- Classes of attackers
- Case study
- Defense in depth
- Security process/ mindset/ design
- Security development lifecycle (SDL)
- Threat models

Risks and Efforts

- Classic risk management
- Security risk management
- Threat analysis and risk assessment TARA
- IT security risk assessment
- Examples of TARA methods

Generic Application of Countermeasures

- Security attributes
- Cryptography (symmetric, asymmetric, hash, MAC, signatures)
- Example of memory encryption
- Security modules (SHE, HSM, TPM)
- CPU core security
- Secure software
- Security testing

Selected Vulnerabilities and Countermeasures

- Code injection
- Code reuse
- Countermeasures
- Boundary error vulnerabilities
- Side channel attacks
- Debug interface aspects

Norms and Standards

- References
- Extracts from IEC 62443

Security in Safety Context

- Differences and similarities
- Security in safety norms

Cybersecurity Engineering

- ISO/SAE 21434:2021
- Exercises: headlamp system