Stand 29.01.2026

Security Engineering: Security-Fundamente für eingebettete Systeme (Embedded Systems) - Live-Online-Training

**Ziele -
Ihr Nutzen**

Security muss ganzheitlich betrachtet werden. Die Fundamente liegen außerhalb der eigentlichen Umsetzung/Implementierung. Dies spiegelt sich auch im Cyber Resilience Act (CRA) wider, fokussiert auf Verantwortlichkeiten und dem strukturierten Umgang mit dem Thema Security. Wie erkennt man potentielle Sicherheitslücken in eingebetteten Systemen (Embedded Systems) und schließt sie nach entsprechender Bewertung? Dazu gehören die wichtigsten kryptographischen Verfahren und deren Anwendungen ebenso wie ausgewählte Hardware- und Softwarekonzepte. Als wichtigen Vertreter aus dem Normenbereich kennen Sie die ISO/SAE 21434 im Detail und erfüllen entsprechende Anforderungen.

Ihre Vorteile:

Jumpstart in die Security-Thematik mit kompaktem Wissen

Kontext zur Funktionalen Sicherheit (Safety)

Details zur ISO/SAE 21434

Übung: TARA in der Konzeptphase

Kursunterlagen als Kompendium

Teilnehmer

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

Voraussetzungen

Erfahrung im Zusammenhang mit Embedded-Systemen sowie Grundkenntnisse im Bereich Safety sind von Vorteil.

Live Online Training

* Preis je Teilnehmer, in Euro zzgl. USt.

Anmeldecode: L-SECFUSI

Präsenz-Training - Deutsch

Termin	Dauer
15.06. – 16.06.2026	2 Tage
14.09. – 15.09.2026	2 Tage

Präsenz-Training - Englisch

Termin	Dauer
15.06. – 16.06.2026	2 Tage

MICRO CONSULT

Stand 29.01.2026

Security Engineering: Security-Fundamente für eingebettete Systeme (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

HINWEIS: Die Kursunterlagen sind auf Englisch