


Sicherheitsgerichtete Systeme entwickeln

Grundlagen der funktionalen Sicherheit in der Praxis

Beginn: 16.11.2026 - 09:00 Uhr	 Ostfildern	Veranstaltungsnr.: 36256.00.003	Präsenz EUR 1.310,00 (MwSt.-frei)
Ende: 17.11.2026 - 16:30 Uhr		Leitung <u>Dr. Thomas Liedtke</u>	Mitgliederpreis ⓘ EUR 1.179,00 (MwSt.-frei)
Dauer: 2,0 Tage			

in Zusammenarbeit mit:



BESCHREIBUNG



Die Entwicklung **sicherheitsgerichteter** Produkte stellt den Schutz von **Leben und Gesundheit** in den Mittelpunkt. Ziel ist es, Risiken auf ein **akzeptables Restrisiko** zu minimieren. Um dies zu erreichen, müssen Entwicklungsprozesse lückenlos dokumentiert, überwacht und optimiert werden.

Gerade in sicherheitskritischen Branchen und im Umfeld von KRITIS (kritischen Infrastrukturen) – etwa in Energieversorgung, Verkehr, Industrie oder Gesundheitswesen – sind strukturierte Safety-Prozesse eine zentrale Voraussetzung für Resilienz und Betriebssicherheit.

Dieses Seminar vermittelt die Prinzipien der funktionalen Sicherheit, zeigt Methoden zur Fehlervermeidung auf und beleuchtet, wie systematische und zufällige Fehler reduziert werden können.

Ziel der Weiterbildung

- Verständnis der Prinzipien der funktionalen Sicherheit und ihrer Umsetzung in der Praxis (z. B. Traceability, 4-Augen-Prinzip, Rollen, Safety-Level, Risikobegriff, Safety-Kultur, Validierung, Planung, ...).
- Grundlagen der Sicherheits- und Zuverlässigkeitstechnik sowie zentraler Normen – insbesondere mit Blick auf Anwendungen in sicherheitskritischen Systemen und KRITIS-Umgebungen.
- Planung und Dokumentation sicherheitsgerichteter Entwicklungsprozesse (inkl. RAMS, QA, Toolqualifikation).
- Umgang mit spezifischen Herausforderungen wie COTS-/Open-Source-Komponenten und der Verknüpfung von Safety und Security.
- Unterschied zwischen Safety und Security erkennen und verstehen
Abgrenzung und Gemeinsamkeiten (Gefahr versus Bedrohung, Gefahr für Menschen, Bedrohung für technische Systeme)
Codierung versus Verschlüsselung
Wieviel Safety braucht Security? – „better safe than sorry“
- Beispielhaft werden wir gemeinsam einen Safety-Plan entwickeln – auch unter Berücksichtigung typischer Anforderungen aus dem KRITIS-Umfeld.

IMMER TOP!

Unser Qualitätsversprechen



Seit über 65 Jahren gehört die Technische Akademie Esslingen (TAE) mit Sitz in Ostfildern – nahe der Landeshauptstadt Stuttgart – zu Deutschlands größten Weiterbildungs-Anbietern für berufliche und berufsvorbereitende Qualifizierung im technischen Umfeld. Unser Ziel ist Ihr Erfolg. Egal ob Seminar, Zertifikatslehrgang oder Fachtagung, unsere Veranstaltungen sind stets abgestimmt auf die Bedürfnisse von Ingenieuren sowie Fach- und Führungskräften aus technisch geprägten Unternehmen. Dabei können Sie sich stets zu 100 Prozent auf die Qualität unserer Angebote verlassen. Warum das so ist?

PROGRAMM

1 | Grundlagen der Sicherheits- und Zuverlässigkeitstechnik

- Sicher(heitsgerichtet)e Systeme: Überblick und Motivation
- Techniken: FMEA, RBD, FTA, Markov, CCA, HAZOP, ...
- Definitionen – IEC 61508
- Risikoakzeptanz: Risiko | MEM | Risikograf | Risikoparameter | Sicherheitsintegritätslevel
- Relevante Safety-Normen verschiedener Branchen (z.B. Bahnumfeld, Automotive, ...)
- Übung zur Gefahrenanalyse und Risikobewertung in der Praxis
 - Walkthrough durch ein Beispiel
 - Aufstellen von Sicherheitszielen

2 | Entwicklungsprozess und deren Wechselwirkungen

- Der Kernprozess im Überblick: Vorgehensmodelle (inkl. Beispiele)
- Kernprozess zur Entwicklung von elektronischen Systemen und Software
- Unterstützungsprozesse für die Embedded Software Entwicklung
- Planung von Safetyaktivitäten
- Prinzip des Dreiklangs: Planung – Spezifikation – Ergebnisbericht
- Übung zur HAZOP-Analyse von Softwarearchitekturen

3 | Unterstützungsprozesse

- RAMS
- QA
- Validierung
- Änderungsmanagement

4 | Arbeitsergebnisse und Dokumentation

- Wichtige Dokumente
- Dokumentationsplan
- Dokumentenprüfung

5 | Anforderungen aus Normen

- Überblick der Sicherheitsnormen und deren Eigenschaften
- Anforderungen an Organisation, Lebenszyklus und Dokumentation
- Anforderungen an Konfigurationsmanagement
- SW-Sicherheitszyklus, SW-Anforderungen, SW-Entwurf, SW-Architektur, SW-Implementierung
- SW-Integrationstest, SW-Modifikation, SW-Verifikation

6 | Toolqualifikation

- Werkzeuge in der normengetriebenen Software Entwicklung
- Qualifikation von Werkzeugen (Automotive, Avionics, Bahn ...)

7 | Einsatz COTS-Software/ Open Source

- Unterschiede im V-Modell
- Qualifikation von Software Komponenten

8 | Entwurfs- und Codier-Standards

- Beispiele von OEMs
- MISRA, SEI CERT, ...

9 | Software-Verifikation und Test

- Grundlagen und Anforderungen an die Softwareprüfung
- Maßnahmen, Methoden und Vorgehensweisen der Softwareprüfung
- Beispiel aus der Praxis

10 | Safety vs. Security

- Sicherheit = Safety + Security
- Security | Normen | Methoden
- Unterschiede, Widersprüche
- Kombination von Risikoanalysen
- Übung: Aufstellen eines Fehlerbaums, Vergleich mit einem Angriffsbaum

- **Fachkräfte**/(Produkt-) Entwickler (System, Software, Hardware) im Umfeld der funktionalen Sicherheit
- **Projektleiter** mit der Verantwortung für die Sicherheit ihrer zu entwickelnden Produkte
- **Manager**, Interessensvertreter zum Erwerb von Bewusstsein für funktionale Sicherheit
- **Rollenverantwortliche** wie Safety Manager oder Safety Engineer

REFERENT:INNEN



Dr. Thomas Liedtke

Dr. Thomas Liedtke ist

- seit vielen Jahren beratend tätig für funktionale Sicherheit, Informations- und Produktsecurity. Er ist Mitglied der deutschen DIN-AK-Spiegelgruppe, welche für die Definition ISO/SAE 21434, ISO/PAS 5112 und weitere Cybersecuritystandards verantwortlich ist
- Mitglied des intacs Advisory Boards und Leiter der SPICE Cybersecurity Arbeitsgruppe Leiter der ZVEI Arbeitsgruppe Datensicherheit im Automobil
- Leadauditor für CSMS; ISMS; TISAX
- Berater für die Implementierung der Cybersecurity in Unternehmen Publikationen
- Informationssicherheit: Möglichkeiten und Grenzen; SpringerLink publisher:
link.springer.com/book/10.1007/978-3-662-63917-7
- The New Cybersecurity Challenges and Demands for Automotive Organisations and Projects
 - an Insight View link.springer.com/chapter/10.1007/978-3-031-42307-9_21

Weitere Veranstaltungen

[Cyber Resilience Act \(CRA\) erfolgreich umsetzen](#)

[Cyber-Sicherheit für kritische Infrastrukturen: NIS2 & CER verstehen und umsetzen](#)

[Intelligente Systeme in der Industrie: Architektur, Einsatz und Wirtschaftlichkeit](#)

[Einführung in die Kryptographie: Methoden und praktische Anwendungen](#)

VERANSTALTUNGSORT UND HOTEL

Technische Akademie Esslingen

An der Akademie 5
73760 Ostfildern



[Anfahrt](#)

Die TAE befindet sich im Südwesten Deutschlands im Bundesland Baden-Württemberg – in unmittelbarer Nähe zur Landeshauptstadt Stuttgart. Unser Schulungszentrum verfügt über eine hervorragende Anbindung und ist mit allen Verkehrsmitteln gut und schnell zu erreichen.

Hotelübernachtung benötigt?

Über den nachfolgenden Link finden Sie nahegelegene Hotels in direkter Umgebung zu TAE-Konditionen:

[🔗 Hotelbuchung](#)

GEBÜHREN UND FÖRDERMÖGLICHKEITEN

Die Teilnahme beinhaltet [Verpflegung](#) sowie ausführliche Unterlagen.

Preis:

Die Teilnahmegebühr beträgt:

1.310,00 € (MwSt.-frei)

Fördermöglichkeiten:

Für den aktuellen Veranstaltungstermin steht Ihnen die [ESF-Fachkursförderung](#) leider nicht zur Verfügung.

Für alle weiteren Termine erkundigen Sie sich bitte vorab bei unserer [Anmeldung](#).

Andere Bundesland-spezifische Fördermöglichkeiten finden Sie [hier](#).

Inhouse Durchführung:

Sie möchten diese Veranstaltung firmenintern bei Ihnen vor Ort durchführen? Dann fragen Sie jetzt ein individuelles [Inhouse-Training](#) an.