# ISO/SAE 21434 – Cybersecurity im Automotive: Theorie und Praxis.

**Automotive Cybersecurity verstehen und in der Entwicklung anwenden**

| | | |
|---|---|---|
| Seminar | Zurzeit keine Termine | Teilnahmebescheinigung |
| Präsenz / Virtual Classroom | 16 Unterrichtseinheiten | |

Seminarnummer: 31165

Stand: 09.11.2026. Alle aktuellen Informationen finden Sie unter https://akademie.tuv.com/s/31165

Vom Wissen zur Anwendung: Cybersecurity greifbar machen!

In diesem zweitägigen Workshop bekommen Sie ein Fresh-Up der theoretischen Grundlagen zur ISO/SAE 21434 Cybersecurity Automotive.
Anhand eines konkreten Best-Practise-Beispiels aus der automobilen Entwicklung wenden Sie das zuvor Gelernte direkt an und lernen, wie Sie die Norm effizient und zielgerichtet in Ihre Projekte im Produktentwicklungszyklus integrieren. Interaktive Arbeit mit direktem Expertenfeedback.

## Nutzen

Ziel dieses Workshops ist es, Ihnen die Anforderungen der **ISO/SAE 21434** nicht nur theoretisch zu vermitteln, sondern direkt in Ihre Entwicklungsrealität zu übertragen.

Sie lernen, wie Sie **Automotive Cybersecurity** strukturiert und effizient in Ihre Projekte integrieren und typische Herausforderungen im Automotive-Umfeld sicher bewältigen.

Nach dem Seminar sind Sie in der Lage:

- die Anforderungen der **ISO SAE 21434** sicher zu interpretieren
- Cybersecurity systematisch in den Entwicklungsprozess zu integrieren
- Risiken in vernetzten Fahrzeugsystemen frühzeitig zu erkennen und zu bewerten
- Sicherheitsanforderungen effektiv mit Lieferanten umzusetzen
- Ihre Rolle im Kontext moderner **Automotive Cyber Security Jobs** fachlich fundiert auszufüllen

**Kurz gesagt:** Sie bringen Cybersecurity dorthin, wo sie im Automotive wirklich wirkt – in die Entwicklung.

® TÜV, TUEV und TUV sind eingetragene Marken. Eine Nutzung und Verwendung bedarf der vorherigen Zustimmung.

# Zielgruppe

- Betriebsverantwortliche
- Qualitätsbeauftragte
- Cybersecurity-Verantwortliche
- Fahrzeughersteller
- Zulieferer in der Automobilindustrie
- Software- und Hardwaredienstleister in der Automobilindustrie

# Abschluss

**Teilnahmebescheinigung**

Teilnahmebescheinigung der TÜV Rheinland Akademie

# Inhalte des Seminars

**1. Tag: Theorietag – ISO/SAE 21434 Cybersecurity Automotive**

- Einführung in die **ISO/SAE 21434** und ihre Rolle in der **Automotive Cybersecurity**
- Grundlagen der Cybersecurity: Zusammenhang mit ISO 27001, typische Angriffsarten
- Spezifische Herausforderungen im Automotive-Bereich: Vernetzung, Software-defined Vehicles, autonomes Fahren
- Regulatorisches Umfeld: Normierung, Homologation und deren Bedeutung für **Cybersecurity Automotive**
- Anforderungen der **ISO SAE 21434** an Organisationen (CSMS):
  - Verteilte Sicherheitsaktivitäten
  - Lieferantenmanagement und Absicherung der Supply Chain
- Überblick über konkrete Umsetzungsmöglichkeiten in Entwicklungsprojekten

**2. Tag: Praxistag – Anwendung im Entwicklungsprozess**

**Automotive Cybersecurity konkret umsetzen**

- Anwendung der Anforderungen der **ISO/SAE 21434** anhand eines Best-Practice-Projekts
- Integration von Cybersecurity in den Produktentwicklungszyklus (V-Modell, agile Ansätze)
- Durchführung typischer Security-Aktivitäten (z. B. Risikoanalysen, Threat Modeling)

® TÜV, TUEV und TUV sind eingetragene Marken. Eine Nutzung und Verwendung bedarf der vorherigen Zustimmung.

- Zusammenarbeit zwischen Entwicklung, Security und Lieferanten
- Ableitung konkreter Maßnahmen für eigene Projekte

Durch interaktive Übungen und **direktes Expertenfeedback** entwickeln Sie ein sicheres Verständnis für die praktische Umsetzung von **Automotive Cyber Security**.

## Terminübersicht und Buchung

Buchen Sie Ihren Wunschtermin jetzt direkt online unter https://akademie.tuv.com/s/31165 und profitieren Sie von diesen Vorteilen:

- Schneller Buchungsvorgang
- Persönliches Kundenkonto
- Gleichzeitige Buchung für mehrere Teilnehmer:innen

Alternativ können Sie das Bestellformular verwenden, um via Fax oder E-Mail zu bestellen.

® TÜV, TUEV und TUV sind eingetragene Marken. Eine Nutzung und Verwendung bedarf der vorherigen Zustimmung.