



# MIT PRAXISBEISPIELEN FÜR AUTOMOTIVE UND IOT EMBEDDED SECURITY ENGINEERING

**Die Herausforderung: Cybersicherheit für eingebettete Systeme methodisch entwickeln und umsetzen.** Lernen Sie anhand eines konkreten Anwendungsfalls, eine systematische Entwicklungsmethodik anzuwenden, wie es z.B. im Automobilbereich in der ISO/SAE 21434 gefordert wird. Adressiert werden dabei Fragestellungen wie leichtgewichtige Kryptographie mit geeignetem Schlüsselmanagement, Hardware-Sicherheitskonzepte wie TPM 2.0 und die Entwicklung von Protokollen.

## Inhalte des Seminars

### Grundlagen einer systematischen Entwicklungsmethodik

- IT-Sicherheit und Kryptographie
- Entwicklungsprozesse
- Herausforderungen bei der Absicherung eingebetteter Systeme

### Kryptographie für eingebettete Systeme

- Leichtgewichtige Kryptographie und Schlüsselmanagement
- Langzeitsicherheit (z.B. Migrationsstrategien, Post-Quantum-Kryptographie)
- Netzwerksicherheit und Kryptographische Protokolle (z.B. Secure Over-the-air Code Update)

### Hardware-Sicherheit, Plattformintegrität und Geräteidentität

- TPM 2.0, leichtgewichtige Alternativen
- Attestierungsprotokolle
- Secure Boot

### Separations- und Isolationslösungen

- z.B. Mikrokern-Betriebssysteme

### Standardisierung

- ISO/SAE 21434, ISO15118

## Ihr Nutzen

- » Nach dem Seminar können Sie die verschiedenen Arten von Gefährdungen verstehen und bewerten.
- » Sie lernen, grundlegende Begriffe der IT-Sicherheit und Kryptographie zu verstehen und einzuordnen.
- » Sie können Bedrohungs- und Risikoanalysen durchführen.
- » Sie lernen, Sicherheitskonzepte und -protokolle systematisch zu entwickeln, Sicherheitslösungen praktisch umzusetzen und entwickelte Sicherheitslösungen in ihrer Wirksamkeit zu bewerten.

## INFORMATIONEN IM ÜBERBLICK

 Gutes Verständnis technischer Systeme, idealerweise im Bereich eingebettete Systeme

 Entwickler\*innen aus den Bereichen Automotive, IoT und weiteren Domänen im Embedded-Bereich, Technische Leiter\*innen in Entwicklungsprojekten

 2 Tage Präsenz

 1200,-

 Darmstadt

Veranstaltet durch

 **Fraunhofer**  
SIT

Referenten:



Prof. Dr. Christoph Krauß, Abteilungsleiter Fraunhofer SIT

Dr. Roland Rieke,  
wiss. Mitarbeiter  
Fraunhofer SIT



Weitere Infos und aktuelle Termine buchen unter:

[www.cybersicherheit.fraunhofer.de/embedded-security-engineering](http://www.cybersicherheit.fraunhofer.de/embedded-security-engineering)