



Security by Design für Maschinen und Anlagen

IT-Sicherheit nach IEC 62443 von Beginn an mitdenken

Lernen Sie, Sicherheitslücken in Maschinen und Anlagen frühzeitig zu identifizieren und durch Security by Design abzusichern. Mit praxisorientiertem Wissen aus diesem Seminar können Sie Sicherheitsmaßnahmen direkt in der Produktentwicklung umsetzen.

Sicherheitsrisiken in Maschinen und Anlagen von Beginn an minimieren

Durch die fortschreitende Digitalisierung in der Industrie werden Maschinen und Anlagen zunehmend vernetzter und durch Embedded Software gesteuert.

Diese Vernetzung bringt zahlreiche Vorteile, birgt jedoch auch erhebliche Sicherheitsrisiken, die im schlimmsten Fall die gesamte Produktion lahmlegen können.

Das Seminar „Security by Design für Maschinen und Anlagen“ soll Verantwortliche aus Entwicklung und Konstruktion dabei unterstützen, potenzielle technische Sicherheitsrisiken frühzeitig zuverlässig zu erkennen und bereits in der Produktentwicklung geeignete Maßnahmen gezielt zu ergreifen – Ziel ist Security by Design.

Kursdetails auf einen Blick

- Für **Product Security Officer, Produktentwickler*innen, Servicetechniker*innen**
- **Offene Schulung** oder **Inhouse Training**
- Dauer: **2 Tage**
- Format: **Präsenz**
- Kosten: 1.790,00 Euro (zzgl. MwSt.)

IT-Sicherheit frühzeitig in die Entwicklung von Maschinen und Anlagen integrieren

Gemeinsam mit unseren Partnern, dem [VDMA-Arbeitskreis Industrial Security](#), zeigen das Fraunhofer IOSB und Fraunhofer IEM auf, wie IT-Sicherheit bereits in der Entwicklungsphase von Maschinen und Anlagen zu berücksichtigen ist, um Risiken vorzubeugen.

Addressiert werden hier Fachkräfte, die in der Produktentwicklung und Konstruktion tätig sind, insbesondere an Produktentwickler von Maschinenherstellern, Product Security Officer (ProSO), Verantwortliche für Industrial Security, Servicetechniker bei Integratoren und Systemintegratoren für Automatisierungstechnik.

Nach dem Seminar können Sie:

- das Prinzip »Secure by Design« entlang Ihres **Entwicklungsprozesses** gewinnbringend einsetzen, um sichere Maschinen und Anlagen zu produzieren.
- relevante **Sicherheitsrisiken frühzeitig erkennen**, bewerten und geeignete **Schutzmaßnahmen ableiten**.
- die **IEC 62443-Normenreihe anwenden**, um die Industrial Security in Ihrem Unternehmen zu verbessern.

Industrial Security von Beginn an mitdenken

Das Seminar wurde auf Basis der IEC 62443 entwickelt und verfolgt das Ziel, Security im Entwicklungsprozess von Maschinen und Anlagen zu berücksichtigen. Entlang des Produktlebenszyklus gilt es hierbei unterschiedliche Methoden und Ansätze zu beachten.

Alle Kursdetails und die Anmeldung finden Sie hier:



<https://s.fhg.de/Security-Design>

Kursinhalte

Das Spektrum der behandelten Themen umfasst:

Initialisierung

- Wichtige Begriffe, Schutzziele und Bedrohungen
- Grundlagen zu IEC 62443 und Security by Design

Analyse

- Bedrohungen und Risiken analysieren. Prozessbetrachtung
- Sicherheitsrisiken mit Security Assessments aufdecken

Entwurf

- Grundsätze für sichere System- und Softwarearchitekturen
- Sichere Vernetzung von Maschinen und Anlagen
- Sichere Komponenten: Anforderungen und Beschaffung
- Risiken von Fernzugriffen einschätzen und Konzepte zur sicheren Umsetzung anwenden

Realisierung

- Grundsätze für die sichere Implementierung
- Prinzipien für manuelle und automatische Code-Reviews

Veröffentlichung

- Fail Securely und (In)Secure Defaults – Grundsätze für sicheres Deployment
- Systemhärtung – Vorgehensweisen und Fallstricke

Nutzung

- Aufgespürte Schwachstellen – Tipps
- Patch Management – Fehler beheben und Sicherheitslücken schließen

Fachlicher Ansprechpartner am Fraunhofer IOSB

Dr.-Ing. Christian Haas
Tel. +49 721 6091-605
christian.haas@iosb.fraunhofer.de

Fraunhofer IOSB
Fraunhoferstraße 1
76131 Karlsruhe

