

Cybersecurity nach IEC 62443 – Grundlagen

Seminar zur Einführung in die Industrial Security im Maschinenbau

Schützen Sie industrielle Systeme mit IEC 62443: Lernen Sie Risikoanalyse, sichere Architekturen und CSMS-Implementierung. Praxisnahe Übungen und aktuelle Forschung sorgen für nachhaltigen Wissenstransfer.

Industrial Security im Maschinenbau – praxisnah nach IEC 62443 umsetzen

Der IT-Sicherheit von industriellen Automatisierungs- und Steuerungssystemen (IACS) kommt im Maschinenbau eine besondere Bedeutung zu. Denn Cyberangriffe verursachen Produktionsausfälle, hohe Kosten und immense Imageschäden.

Das Seminar zeigt Hersteller*innen, Betreiber*innen und Integrator*innen von

vernetzten Maschinen und Anlagen auf, wie Industrial Security nach IEC 62443 für den Maschinenbau umgesetzt werden kann. Dabei wird die Theorie an zahlreichen Beispielen und Demonstratoren veranschaulicht.

Der Kurs richtet sich an Ingenieurinnen, IT-Sicherheitsverantwortliche und Entscheiderinnen, unabhängig von Vorkenntnissen.

Kursdetails auf einen Blick

- Für **Ingenieur*innen, Fachkräfte der IT-Sicherheit, Entscheider*innen**
- **Offene Schulung** oder **Inhouse Training**
- Dauer: **3 Tage à 8 Stunden**
- Format: **Präsenz**
- Kosten: 2.995,00 Euro (zzgl. MwSt.)

Von der Theorie zur Praxis: ISA/IEC 62443 anwenden

Über drei Tage werden die Grundlagen der ISA/IEC 62443-Norm vermittelt, die Sicherheitsanforderungen für industrielle Systeme definiert.

Wichtige Themen sind IT- vs. OT-Security, Defense-in-Depth, Zonen- und Conduit-Modelle sowie die Implementierung eines Cyber Security Management Systems (CSMS). Zudem werden Risikoanalyse und sicheres Systemdesign behandelt.

Das Seminar kombiniert Theorie mit Praxis: Anhand von Fallbeispielen und Demonstratoren aus dem Maschinenbau werden reale Bedrohungsszenarien analysiert. Bei Übungen in Kleingruppen können die Teilnehmenden erste Konzepte anwenden und von Expert*innen-Feedback profitieren.

Die enge Verbindung zur aktuellen Forschung gewährleistet den Zugang zu neuesten Erkenntnissen und Best Practices.

Nach dem Seminar können Sie:

- die relevanten **Teile der IEC 62443-Normreihe identifizieren** und in industriellen Netzwerken anwenden.
- **Cyber Security Management Systeme** nach den Vorgaben der Norm **entwickeln**, einschließlich Risikoanalyse und Systemüberwachung.
- **Sicherheitsrisiken** in der Industrie erkennen und mit geeigneten Maßnahmen zur **Risikominderung** proaktiv umgehen.

Alle Kursdetails und die Anmeldung finden Sie hier:



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

Kursinhalte

Das Spektrum der behandelten Themen umfasst:

- Einführung in den IEC 62443 Standard
- Unterschiede zwischen IT- und OT-Security
- Einführung grundlegender Konzepte wie
 - Defense-in-Depth,
 - Zonen,
 - Conduits
 - Security-Levels
- Aufbau eines Cyber Security Management Systems (CSMS)
- Einführung in die Themen Risikoanalyse und sicheres Systemdesign

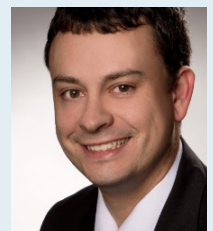
Zugangsvoraussetzung:

Das Seminar richtet sich an Einsteigerinnen und Einsteiger mit und ohne Vorwissen sowie an Fortgeschrittene.

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



Lernlabor
Cybersicherheit