





Informationen im Überblick


 Zertifikat

 Einsteiger*innen mit geringem und ohne Vorwissen

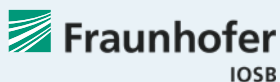
 Entscheider*innen, Ingenieur*innen und Fachkräfte aus technischen Unternehmensbereichen, insbesondere Entwicklung und Konstruktion, Verantwortliche für die IT-Sicherheit

 3 Tage

 2475,-

 Karlsruhe

Veranstaltet durch
**Maschinenbau-Institut
GmbH in Kooperation
mit Fraunhofer IOSB**




Referenten:



Dr.-Ing. Christian Haas, Gruppenleiter
Fraunhofer IOSB



M.Sc. David Meier,
wiss. Mitarbeiter
Fraunhofer IOSB

 Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/IEC-62443-it-sicherheitskonzept

Cybersecurity nach IEC 62443 – IT-Sicherheitskonzept

Sicherheitsanforderungen für vernetzte Maschinen und Anlagen definieren

Basierend auf einer fundierten Bedrohungs- und Risikoanalyse (Thread Risk Assessment) kann ein IT-Sicherheitskonzept für industrielle Automatisierungs- und Steuerungssystemen (IACS) entwickelt werden. Das Seminar zeigt speziell für Hersteller, Betreiber und Integrierte von Maschinen und Anlagen, wie ein solches Konzept mit entsprechenden Sicherheitsmaßnahmen und Testplänen erstellt werden kann.

Die IT-Sicherheit von vernetzten Maschinen und Anlagen wird immer mehr zu einem Schlüsselthema für produzierende Unternehmen, vor allem aber für den Maschinenbau. Neben Produktionsausfällen fallen hohe Kosten an und entstehen immense Imageschäden. Um dies zu vermeiden, müssen Maschinenbauer mehr in die Cybersicherheit ihrer industriellen Produktionssysteme investieren. In diesem Seminar werden das notwendige Wissen und die Fähigkeiten vermittelt, um aufbauend auf einer Risikoanalyse Sicherheitsmaßnahmen für neue und bestehende IACS auswählen und umsetzen zu können. Darüber hinaus wird gezeigt, wie Testpläne zur Überprüfung von umgesetzten Maßnahmen in Verbindung mit den Sicherheitsanforderungen erstellt werden.

Inhalte des Seminars

- Ergebnisse einer Bedrohungs- und Risikoanalyse (Thread Risk Assessment) interpretieren
- Entwicklung einer Cybersecurity Requirements Specification (CRS) und darauf basierenden Konzepten
- Den Security Development Lifecycle und dessen Bestandteile verstehen
- Durchführung einer grundlegenden Konfiguration und Inbetriebnahme einer Firewall
- Eine sichere Lösung für den Remote-Zugang entwickeln
- Entwicklung einer Spezifikation zur Systemhärtung
- Umsetzung eines einfachen Intrusion Detection Systems (IDS)
- Entwicklung und Durchführung eines Cybersecurity Acceptance Test Plan (CFAT/CSAT)

Ihr Nutzen

- Sie lernen den Standard IEC 62443 mit Blick auf die Entwicklung eines IT-Sicherheitskonzepts kennen.
- Sie lernen an Hand von Praxisbeispielen aus dem Maschinenbau und Demonstratoren.
- Sie lernen erste Konzepte in Übungen in Kleingruppen anzuwenden.
- Sie lernen durch den Austausch mit den Teilnehmenden und durch das Feedback der Trainer.

