Veranstaltungsnummer: VA-01522

IEC 62443 – Grundlagen der sicheren Softwareentwicklung

Sichere Softwareentwicklung nach IEC 62443-4-1 – von Security-by-Design bis Schwachstellenmanagement



Termin

Mo. 08.03.2027, 08:30 Uhr –
Di. 09.03.2027, 12:30 Uhr

Veranstaltungsort

hdt+ digitaler Campus

Teilnahmegebühren

Online-Teilnahme 1.210,00 €*
Für HDT-Mitglieder 1.089,00 €*

* mehrwertsteuerfrei, einschließlich veranstaltungsgebundener Arbeitsunterlagen

Weitere Informationen und die Möglichkeit zur Online-Buchung **Ihrer Teilnahme finden Sie auf** der Veranstaltungs-Webseite.

Stand: 18.11.2026, 13:16 Uhr

IEC 62443 – Grundlagen der sicheren Softwareentwicklung

Die zunehmende Vernetzung industrieller Systeme, die steigende Komplexität softwarebasierter Produkte und neue regulatorische Anforderungen stellen Unternehmen vor wachsende Herausforderungen bei der Entwicklung sicherer Software. Gerade in sicherheitskritischen Bereichen wie industrieller Automatisierung, Maschinenbau, Medizintechnik oder Infrastruktur reicht funktionale Software allein nicht mehr aus. Software und softwarebasierte Produkte müssen über ihren gesamten Lebenszyklus hinweg sicher, robust und gegen Manipulationen geschützt entwickelt und betrieben werden.

Das Onlineseminar vermittelt praxisorientierte Grundlagen der sicheren Softwareentwicklung für industrielle Systeme. Die Inhalte orientieren sich am international anerkannten Standard IEC 62443-4-1 und betrachten den gesamten sicheren Produkt- und Softwarelebenszyklus – von Risikomanagement und sicherem Design über Implementierung und Dokumentation bis zur Supportphase und zum Schwachstellenmanagement.

Behandelt werden außerdem aktuelle Bedrohungen wie Ransomware und Supply-Chain-Angriffe sowie regulatorische Anforderungen durch den EU Cyber Resilience Act (CRA) und NIS2. Die Teilnehmenden erhalten einen Überblick über Unterschiede zwischen IT- und OT-Security, relevante Schutzziele sowie Methoden zur systematischen Risikoanalyse, beispielsweise TARA und STRIDE.

Weitere Schwerpunkte bilden Security-by-Design, sichere Architekturen, Anforderungen an Lieferanten sowie die Umsetzung und Dokumentation geeigneter Sicherheitsmaßnahmen. Ziel ist es, robuste, regelkonforme und auditierbare Softwarelösungen entwickeln, bewerten und über den gesamten Lebenszyklus hinweg betreiben zu können.

Zum Thema
Mit der zunehmenden Digitalisierung und Vernetzung industrieller Produkte und Anlagen gewinnt Cybersicherheit über den gesamten Produktlebenszyklus an Bedeutung. Schwachstellen in Software, Angriffe auf industrielle Systeme und Risiken in der Lieferkette können Daten, Produktionsabläufe und die Verfügbarkeit technischer Systeme gefährden.

IEC 62443-4-1 beschreibt Anforderungen an einen sicheren Entwicklungslebenszyklus für industrielle Automatisierungs- und Steuerungssysteme. Dazu zählen Security Management, Sicherheitsanforderungen, sicheres Design, Implementierung, Verifikation, Dokumentation und Schwachstellenmanagement.

Zusätzlich erhöhen Vorgaben wie der EU Cyber Resilience Act und NIS2 den Handlungsdruck. Ein systematischer Secure-Development-Prozess hilft, Risiken frühzeitig zu bewerten und nachvollziehbare, auditierbare Sicherheitsmaßnahmen umzusetzen.

Zielsetzung
Das Onlineseminar vermittelt einen strukturierten Überblick über sichere Softwareentwicklung im industriellen Umfeld nach IEC 62443-4-1. Im Fokus stehen Security-by-Design, Risikomanagement, sichere Architektur und Implementierung, Lieferantenmanagement sowie Dokumentation und Schwachstellenmanagement. Ziel ist die Entwicklung robuster, nachvollziehbarer und regelkonformer Softwarelösungen über den gesamten Produktlebenszyklus hinweg.

Programm

08.03.2027

08:30–12:30 IEC 62443 - 1.Tag

1. Grundlagen der industriellen Cybersicherheit und sicheren Softwareentwicklung
- Aktuelle Bedrohungslage für industrielle Systeme
- Ransomware und Angriffe auf industrielle Infrastrukturen
- Supply-Chain-Risiken
- Unterschiede zwischen IT- und OT-Security
- Zentrale Schutzziele: Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität
- Überblick über den sicheren Produkt- und Softwarelebenszyklus

2. Normative und regulatorische Anforderungen
- Einführung in IEC 62443
- Schwerpunkt IEC 62443-4-1
- Anforderungen an sichere Entwicklungsprozesse
- EU Cyber Resilience Act (CRA)
- NIS2
- Zusammenspiel von Normen, Regulierung und betrieblicher Umsetzung

3. Lieferantenmanagement und Supply-Chain-Security
- Sicherheitsanforderungen an Lieferanten und externe Komponenten
- Risiken durch Drittanbieter und Softwarekomponenten
- Integration von Cybersecurity-Anforderungen in Beschaffungsprozesse
- Bewertung und Nachverfolgung von Lieferantenrisiken
- Berücksichtigung der Lieferkette im sicheren Produktlebenszyklus

4. Risikomanagement für industrielle Produkte und Software
- Grundlagen eines systematischen Cybersecurity-Risikomanagements
- Bedrohungen und Schwachstellen identifizieren
- Threat Analysis and Risk Assessment (TARA)
- Bedrohungsmodellierung mit STRIDE
- Risiken bewerten und priorisieren
- Sicherheitsanforderungen aus Risiken ableiten

5. Sicheres Design und Security-by-Design
- Security-by-Design als Entwicklungsprinzip
- Sicherheitsanforderungen frühzeitig berücksichtigen
- Sichere System- und Softwarearchitekturen
- Angriffsflächen reduzieren
- Sicherheitsfunktionen und Schutzmechanismen festlegen
- Nachvollziehbare Designentscheidungen treffen

09.03.2027

08:30–12:30 IEC 62443 - 2.Tag

6. Sichere Implementierung
- Sicherheitsanforderungen in der Softwareentwicklung umsetzen
- Secure-Coding-Prinzipien
- Vermeidung typischer Schwachstellen
- Umgang mit Softwarebibliotheken und Komponenten
- Sicherheitsmaßnahmen in bestehende Entwicklungsprozesse integrieren
- Anforderungen an Verifikation und Qualitätssicherung

7. Dokumentation und Nachweisführung
- Anforderungen und Sicherheitsentscheidungen nachvollziehbar dokumentieren
- Dokumentation über den Softwarelebenszyklus
- Nachweis von Sicherheitsmaßnahmen
- Auditierbarkeit von Entwicklungsprozessen
- Bedeutung einer konsistenten Dokumentation im regulatorischen Umfeld

8. Supportphase und Schwachstellenmanagement
- Sicherheit nach der Produktfreigabe
- Schwachstellen identifizieren und bewerten
- Umgang mit gemeldeten Sicherheitslücken
- Priorisierung und Bearbeitung von Schwachstellen
- Sicherheitsupdates und Patches
- Kommunikation und Dokumentation im Schwachstellenprozess
- Kontinuierliche Verbesserung während der Supportphase

9. Zusammenführung zum sicheren Produktlebenszyklus
- Zusammenspiel von Risikomanagement, Design und Implementierung
- Lieferanten und externe Komponenten einbinden
- Dokumentation und Nachweisführung sicherstellen
- Schwachstellen über den gesamten Produktlebenszyklus berücksichtigen
- Voraussetzungen für robuste, regelkonforme und auditierbare Softwarelösungen

Referenten

DM

Dipl.-Ing. Heinz Marien

OTSecure GmbH

Heinz Marien ist Dipl.-Ing. (FH) Elektrotechnik und M.Sc. Applied IT-Security sowie zertifizierter ISA/IEC 62443 Cybersecurity Expert. Er verfügt über langjährige Erfahrung in der Softwareentwicklung für industrielle Automatisierung, unter anderem in der Stahl- und Prozessindustrie sowie im Umfeld kritischer Infrastrukturen.

Ein Schwerpunkt seiner Tätigkeit liegt in der sicheren Entwicklung industrieller Produkte und Systeme nach IEC 62443. Er leitete Entwicklungsprojekte gemäß IEC 62443-4-1 und war am Aufbau sowie an der Einführung zertifizierter Prozesse für sichere Produktentwicklung beteiligt. Darüber hinaus engagiert er sich in Verbänden und Normungsgremien und ist als Lehrbeauftragter für sichere Softwareentwicklung an Hochschulen tätig. Damit verbindet er praktische Industrieerfahrung, fundiertes Normenwissen und didaktische Erfahrung in besonderer Weise.