VDI Wissensforum

Bildquelle: © mit KI erstellt

VDI-Fachkonferenz

Industrielle Cybersicherheit

Die Top-Themen:

- **Schutz industrieller Anlagen durch Segmentierung, sichere Fernzugriffe und wirksame OT-Sicherheitsarchitekturen**
- **Erkenntnisse aus realen Cyberangriffen, Security-Assessments und praxisnahen Live-Hacking-Szenarien**
- **Umsetzung von NIS 2, CRA und relevanten Standards für Produkte, Anlagen und industrielle Prozesse**
- **Neue Sicherheitsrisiken durch KI, KI-Agenten und vernetzte Produktionsumgebungen**
- **Aufbau von Cyberresilienz durch klare Prozesse, Governance, Monitoring und Incident Response**
- **Praxisbeispiele zu OT-Monitoring, Schwachstellenmanagement, Security-Assessments, Audits und Incident Response**

+ **Buchbarer Spezialtag**
Sichere drahtlose industrielle Kommunikation mit LTE, 5G und LoRa

+ **Fachausstellung**

+ **Ihre Konferenzleitung**
Prof. Dr. Martin Henze, Security and Privacy in Industrial Cooperation (SPICe), Fakultät für Informatik, RWTH Aachen University, Aachen

Höre Expert*innen folgender Unternehmen:

ABB · BASF · BOSCH · CGI · Fraunhofer · gaia-x · Greenbone · INNOMOTICS · paloalto · PHOENIX CONTACT · PILZ · SCHAEFFLER ENGINEERING · SCHAEFFLER · Sichere Industrie · SIEMENS · more security. usd · ZEISS · ZF

Veranstaltung der VDI Wissensforum GmbH
Jetzt online anmelden!
www.vdi-wissensforum.de/02K0021026
Telefon +49 211 6214-201 • Fax +49 211 6214-154

09. und 10. Dezember 2026, Aachen

1. Konferenztag
Mittwoch, 09. Dezember 2026

08:45 Registrierung

09:45 Begrüßung und Eröffnung
Prof. Dr. Martin Henze, Security and Privacy in Industrial Cooperation (SPICe), Fakultät für Informatik, RWTH Aachen University, Aachen
Caroline Körber, Produktmanagement, VDI Wissensforum GmbH

Industrielle Cybersicherheit in der Praxis: Angriff, Resilienz und Umsetzung

10:00 Gehacked: Ein Praxisbericht über Cyberangriff, Resilienz und Regulierung
- Die ersten Tage nach dem Angriff und was wir konkret getan haben: Krisenkommunikation, Systemabschaltung, Datensicherung
- Konsequenzen aus dem Angriff – Maßnahmen zur Stärkung der Resilienz: Netzwerksegmentierung, Entwicklungsisolation, Rechtekontrolle
- Wie beeinflusst diese Erfahrung unsere Sicht auf aktuelle Gesetze und Normen zur Cybersecurity heute?

Dr. Hartmut Paulus, Product Development, Network Systems, Senior Manager, Pilz GmbH & Co. KG, Ostfildern

10:30 Nachhaltige OT Security Implementierung in großen Produktionsumgebungen
- Konzept: Organisation, Prozesse, Tools, kontinuierliche Verbesserung
- Einbeziehung relevanter Normen und Industriestandards
- Risikomanagement (Produktionsausfälle a) durch Cyber-Bedrohungen versus b) durch Patchen)

Rainer Rodler, Head of OT Security, ZF Friedrichshafen AG, Friedrichshafen

11:00 Kaffeepause mit Besuch der Fachausstellung

Umgang mit Cybersicherheitsanforderungen: Von Compliance zu wirksamer OT-Security

11:30 Von Compliance zu Resilienz
- Von regulatorischen Pflichten zu belastbaren Sicherheitspraktiken
- ISA/IEC 62443 und andere Standards als gemeinsame Sprache für Controls, Risiken und Nachweise
- Ein skalierbares Rahmenwerk für Governance, Umsetzung und kontinuierliche Verbesserung

Dipl.-Ing. (FH) Gustav Martin Bartel, Senior Expert, Cybersecurity Governance & Enabling Industrial IT, Robert Bosch GmbH, Stuttgart

12:00 Durchblick im Regulierungsdschungel: Umgang mit regulatorischer Komplexität in der Cybersecurity
- Zusammenspiel europäischer und nationaler Cybersecurity-Regulierungen
- Herausforderungen bei der Harmonisierung und Umsetzung regulatorischer Vorgaben
- Best Practices und Lessons Learned aus der Umsetzung

Dr.-Ing. Raphael Fritz, Head of Cyber Security Governance, Regulatory and ISMS, BASF Digital Solutions GmbH, Ludwigshafen am Rhein

12:30 Mittagspause mit Besuch der Fachausstellung

OT-Security wirksam umsetzen: Von Richtlinien zu Sicherheitsmaßnahmen

14:00 360° Security als Erfolgsfaktor: Richtlinien sicher erfüllen
- Technische Anforderungen von NIS 2 und CRA verstehen und Auswirkungen auf Produkte und Anlagen einordnen
- CRA-Umsetzung bei Phoenix Contact: Einblicke in Standards, Entwicklung und technische Compliance.
- Risiken, Prozesse und Schutzmaßnahmen verzahnen und Security-Anforderungen ganzheitlich umsetzen

Dr.-Ing. Lutz Jänicke, Corporate Product & Solution Security Officer, PHOENIX CONTACT GmbH & Co. KG, Blomberg

14:30 Cyberresilienz unter neuen Rahmenbedingungen – von Anforderungen zu wirksamen Security Operations
- Cyberresilienz im Wandel: Auswirkungen neuer regulatorischer Anforderungen auf Unternehmen und Security
- Von Vorgaben zur Umsetzung: Regulatorische Anforderungen in Prozesse und Sicherheitsmaßnahmen übersetzen
- Security Operations für Resilienz: Mit Detection, Response und Recovery Widerstandsfähigkeit nachhaltig stärken

Dipl.-Inform. Sebastian Jansen, Director Consulting Services, CGI Deutschland B.V. & Co. KG, Köln

15:00 OT-Asset Management in echt und aus der Praxis
- Zielsetzung von OT-Asset Management als Enabler für Use-Cases wie Netzwerksegmentierung, Remote Access und Risikobewertung
- Praxiserprobtes Phasenmodell zur Inventarisierung industrieller Umgebungen
- Abstieg in technische Details z.B. aktive vs. passive Erkennung und die jeweiligen Vor- und Nachteile

Dr. Markus Dahlmanns, Solution Engineer OT-Security, SI | Sichere Industrie GmbH, Hamburg

15:30 Kaffeepause mit Besuch der Fachausstellung

Produktionsnetze unter Kontrolle: Security Assessments, Netzwerksegmentierung und Remote Access

16:00 Netzwerksicherheit in der Industrie 4.0: Segmentierung und kontrollierter Remote-Zugriff in der Praxis
- Industrielle Netzwerke und Herausforderungen für Segmentierung und Remote-Zugriff
- Sicherer Remote Zugriff für Maschinenhersteller für Maintenance-Aufgaben in der Praxis
- Regelmäßige Überprüfung der Sicherheitsmaßnahmen: Automatisierte Scans, Inventory Management mit Vulnerability Detection, Audits mit externen Dienstleistern

David Schachtschneider, M.Sc., Cybersecurity Professional, Innomotics GmbH, Tübingen

16:30 Zwischen Legacy und Next Gen: Wie strikte Segmentierung und cleverer Remote Access skalierbare Cybersecurity in der Produktion ermöglichen
- Strikte Segmentierung als Voraussetzung für wirksame Cybersecurity
- Zielkonflikt zwischen Sicherheitstiefe und Produktionsrealität im Rahmen von Segmentierungsprojekten
- Cleverer Remote Access als Enabler für effiziente Produktion innerhalb der Segmentierung

Thorsten Schmitt, Vice President Operations IT Security, **Vivien Rose**, Director Operations IT Security, Operations Digitalization & IT, Schaeffler Technologies AG & Co. KG, Herzogenaurach

17:00 Hacker im Schaltschrank - OT-Security-Assessments in der Praxis

- Ablauf eines OT-Security-Assessments in der Praxis: Threat Model, passive Asset- und Netzwerkerkennung im Produktionsnetz, Analyse industrieller Protokolle, kontrolliert durchgeführte aktive Tests
- Exemplarische (anonymisierte) Findings aus realen Assesments, z.B. unsicher konfigurierter SPS-Zugriff
- Live-Hacking: Auswirkungen von Netzwerkzugriff in OT-Netzen

Samir Benzammour, M. Sc., Senior Consultant IT Security, usd HeroLab, **Robin Plugge, B. Sc.,** Senior Consultant IT Security, usd HeroLab, usd AG, Köln

17:30 Zusammenfassung und Ausblick durch die Konferenzleitung

17:45 Ende des Fachprogramms des ersten Veranstaltungstages

Get-together

18:30 Zum Ausklang des ersten Veranstaltungstages lädt das VDI Wissensforum zu einem Get-together ein. Nutze die entspannte Atmosphäre, um dein Netzwerk zu erweitern und mit anderen Teilnehmenden und Referierenden vertiefende Gespräche zu führen.

2. Konferenztag
Donnerstag, 10. Dezember 2026

OT Sicherheitswerkzeuge: Schwachstellenmanagement, Frimwaresicherheit und Monitoring

08:45 Open Source OT-Netzwerkmonitoring mit Malcolm, von low hanging fruits zu incident response

- „Man kann nicht absichern, wenn man nicht kennt": Zuerst Sichtbarkeit im Netzwerk herstellen
- OT-Netzwerke kann man gut bereinigen, was Resilienz stärkt und nicht teuer sein muss
- Anomalien erkennen ist der erste Schritt, aber was dann?

Dipl.-Phys. Jens Wiesner, Referatsleiter, Referat C25 - Industrielle Steuerungs- und Automatisierungssysteme, Bundesamt für Sicherheit in der Informationstechnik, Bonn

09:15 Schwachstellen-Management in Heterogenen Umgebungen: Möglichkeiten und Herausforderungen

- Schwachstellen-Management: Erkennung & Compliance
- IT/OT Scanbeispiele, Tradeoffs des Was und Wie
- Zukunftsaussicht OT

Olav Lamberts, M.Sc., Vulnerability Test Automation Developer, Greenbone AG, Osnabrück

09:45 Effektive Integration von Firmware-Sicherheitsanalysen an kritischen Punkten der Software-Lieferkette

- Vertrauenswürdigkeit von Drittanbieter-Komponenten in der Software-Lieferkette überprüfen und sicherstellen
- Methoden und Werkzeuge der Firmware-Analyse: Stand der Technik in statischer und dynamischer Analyse
- Firmwareanalyse zur Erhöhung des Sicherheitsniveaus effektiv einsetzen: Risiken identifizieren und bewerten

Johannes vom Dorp, M.Sc., Wissenschaftlicher Mitarbeiter, Abteilung Cyber Analysis and Defense, Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE, Wachtberg-Werthhoven

10:15 Kaffeepause mit Besuch der Fachausstellung

Absicherung von KI und Daten: Sichere Datenräume und Integration von AI

11:00 Sichere Architektur für das Datenteilen in Datenräumen und digitalen Ökosystemen

- Generelle Architektur: Daten-Plattformen, Datenräume, und (Service-)Ökosysteme
- Zwei Ebenen von Trust: verifizierte Identitäten der Datenraum-Teilnehmenden sowie Integrität, Herkunft und Verlässlichkeit bereitgestellter Daten und Services von Fremden
- Sicheres Datenteilen zwischen Datenräumen: Wie sich zwei oder mehrere autonome Datenräume ohne aufwändige und nicht-skalierende bilaterale Verhandlungen auf eine gemeinsame Vertrauensbasis „einigen"

Dr. Christoph F. Strnadl, CTO, Gaia-X European Association for Data and Cloud, Brüssel, Belgien

11:30 Sicherheit von KI-Workloads in der OT: Lösungsansätze im industriellen Umfeld

- Grenzen klassischer Architektur: Warum KI-Workloads in der Fertigung neue Anforderungen an die Defense-in-Depth-Strategie stellen
- Methodik & Standards: Wie die sichere Interaktion zwischen KI-Applikationen und kritischen OT-Komponenten umgesetzt wird
- Risikomanagement in der Praxis: Identifikation und Absicherung spezifischer Gefahren bei der Integration von KI-Systemen in vernetzten Produktionsumgebungen

Dipl.-Inform. Med. Christian Götz, Director, SE Programs, Palo Alto Networks (Germany) GmbH, München

12:00 Digitale Identitäten für AI-Agenten im Shopfloor: Können etablierte Sicherheitskonzepte aus der IT auf die OT übertragen werden?

- Analyse der Identitäts- und Autorisierungsanforderungen autonom handelnder AI-Agenten in industriellen Produktionsumgebungen und deren Unterschiede zu klassischen IT-Systemen
- Kritische Bewertung etablierter Sicherheitsansätze wie Zero Trust, kurzlebiger Tokens, föderierter Berechtigungen und Workload Identities hinsichtlich ihrer Anwendbarkeit auf OT-Geräte und industrielle Netzwerke
- Diskussion neuer Risiken durch Agent-to-Agent-Kommunikation, delegierte Entscheidungen und physische Auswirkungen auf Anlagen (Physical AI) sowie möglicher Lösungsansätze für Nachvollziehbarkeit, Governance und sichere Autorisierung

Dipl.-Ing. Vadim Gamidov, Cybersecurity Architect, **Nicolas Baumann, M.Eng.**, Cybersecurity Professional, Siemens AG, Digital Industries, Karlsruhe und Erlangen

12:30 Mittagspause mit Besuch der Fachausstellung

KI zur Erhöhung der Cybersicherheit: LLMs und Agentic AI

14:00 KI-gestützte Risikoanalyse und Entwicklung von Cybersecurity-Konzepten für Industrieprodukte im Kontext des Cyber Resilience Act (CRA)

- Sichere Verarbeitung sensibler Cybersecurity-Daten durch On-Premise-Lösungen auf Basis lokaler Large Language Modelle (LLMs)
- Automatisierbare Risikobewertung und Maßnahmenableitung für Produkte in variablen industriellen Einsatzumgebungen
- Transparente Abgrenzung zwischen KI-gestützten Empfehlungen und menschlicher Expertenentscheidung

Dipl.-Inf. (FH) Dennis Baron, TC Officer Product Cybersecurity Schaeffler Engineering Europe, Engineering Support & Consulting, SCHAEFFLER Engineering GmbH, Werdohl

14:30 KI-gestützte Behandlung von Netzwerk-Vorfällen (Incidents): von der Erkennung bis zur Ursachenanalyse

- Erkennung von Anomalien und Incidents durch intelligente Mustererkennung jenseits starrer Regelwerke
- Automatisierte Ursachenanalyse ohne tieferes Fachwissen
- Nachvollziehbarkeit und Selbstanpassung durch Agenten-gestützte generative KI

Dr. Dirk Schulz, Senior Principal Scientist - Communication Architecture, ABB AG Forschungszentrum Deutschland, Mannheim

15:00 Agentic Threat Modelling für Industrieprodukte

- Frühzeitige und effiziente Risikoerkennung: Bedrohungen bereits in der Entwicklung systematisch erkennen und dokumentieren
- Kontextbasierte Priorisierung: Deployment-, Daten- und Nutzerkontext reduzieren Fehlalarme und rücken geschäftskritische Risiken in den Fokus
- Integration ins Schwachstellen- und Patchmanagement: Erkannte Risiken direkt in die Pipeline für Schwachstellen- und Patchmanagement von Industrieprodukten überführen

Johannes Lang, M.Sc., Business Information Security Officer (BISO), Carl Zeiss Microscopy GmbH, Oberkochen

15:30 Zusammenfassung der Konferenz und Schlusswort

15:45 Ende der Veranstaltung

Separat buchbar

VDI-Spezialtag, 08. Dezember 2026, Aachen

Sichere drahtlose industrielle Kommunikation mit LTE, 5G und LoRa

09:00 - ca. 17:00 Uhr

Prof. Dr.-Ing. Michael Rademacher, Professur für Informatik, Hochschule Bonn-Rhein-Sieg, Sankt Augustin & Forschungsgruppenleiter „Secure Mobile Communication", Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE), Bonn

Inhalte des Spezialtags

Drahtlose Netze verstehen: Funkausbreitung und Software Defined Radio

- Bedeutung drahtloser Netze für Smart City, kritische Infrastrukturen und Industrie
- Grundlagen der Funkausbreitung: Freiraumdämpfung, Reflexion, Beugung und Frequenzbänder
- Zusammenhang von Bandbreite, Datenrate und Reichweite
- Software Defined Radio (SDR): flexible Funksysteme mit Signalverarbeitung in Software
- Kurze Vorführung: Empfang und Visualisierung realer Funksignale mit einem SDR

LoRa und LoRaWAN

- Einordnung von LPWAN im Vergleich zu WLAN, Bluetooth und Mobilfunk
- LoRa auf der Bitübertragungsschicht: Chirp Spread Spectrum und Empfang unter dem Rauschpegel
- LoRaWAN-Architektur: Sensor, Gateway, Network Server und Application Server
- Rahmenbedingungen: lizenzfreie ISM-Bänder und Duty-Cycle-Beschränkungen
- Sicherheit in LoRaWAN: Aktivierung (OTAA/ABP), Schlüssel und Ende-zu-Ende-Verschlüsselung

Mobilfunknetze der 4. und 5. Generation

- Von 1G bis 5G: Entwicklung der Standards und ihrer Fähigkeiten
- Die drei 5G-Nutzungsszenarien eMBB, mMTC und URLLC
- Architektur von Funkzugangsnetz (RAN) und Kernnetz (Service Based Architecture)
- Schlüsseltechnologien: Massive MIMO, Beamforming, mmWave und Carrier Aggregation
- 5G-Campusnetze / private Netze für Industrie und kritische Infrastrukturen

Sicherheit von Mobilfunknetzen

- Angriffsflächen im Vergleich: Funkzugangsnetz (RAN) versus Kernnetz
- Passive Angriffe: Mitschneiden von Kontroll- und Nutzdaten, Metadaten
- Aktive Angriffe: Jamming und intelligentes, selektives Stören einzelner Signale
- Gefälschte Basisstationen und das Einschleusen von Nachrichten – Funktionsweise, Erkennung und Abwehr
- Schutzmaßnahmen, deren Grenzen sowie rechtliche Rahmenbedingungen

Demonstrationen und Abschluss

- Live-Demonstration mit Software Defined Radio: Empfang und Spektrum-Visualisierung realer Funksignale
- Demonstration einer gefälschten Basisstation im abgeschirmten Laboraufbau: Funktionsweise und Erkennungsmerkmale
- Diskussion, offene Fragen und Transfer in die eigene Praxis

Konferenzleitung

Prof. Dr. Martin Henze, Security and Privacy in Industrial Cooperation (SPICe), Fakultät für Informatik, RWTH Aachen University, Aachen

Als Professor leitet er die Forschungsgruppe Security and Privacy in Industrial Cooperation (SPICe) und beschäftigt sich intensiv mit der Absicherung industrieller Netzwerke sowie sicherem Datenaustausch insbesondere im Automatisierungs- und Produktionssektor. Zusätzlich bringt er seine Expertise als Co-Leiter der Forschungsgruppe Secure Production & Energy Networks am Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE und Fraunhofer-Zentrum Digitale Energie ein.
Er verbindet aktuelle Forschung mit hoher Praxisrelevanz. Durch seine fachliche Tiefe den Bereichen Sicherheit von industriellen Netzwerken und Daten, Angriffserkennung und Absicherung von industriellen 5G/6G-Netzwerkene schafft er als Konferenzleiter den passenden Rahmen, um zentrale Herausforderungen, wirksame Schutzkonzepte und neue Ansätze für mehr Cyberresilienz im Anlagen- und Maschinenbau fundiert zu diskutieren.

Gründe für den Konferenzbesuch

· Lerne mehr über moderne OT-Sicherheitsarchitekturen, Netzwerksegmentierung und sichere Fernzugriffe für industrielle Anlagen.
· Informiere dich über aktuelle Cyberbedrohungen, reale Angriffsszenarien und wirksame Schutzmaßnahmen für Produktionsumgebungen.
· Erhalte aktuelle Informationen zu NIS 2, Cyber Resilience Act (CRA) sowie relevanten Normen und Standards für industrielle Systeme.
· Erfahre alles über neue Sicherheitsrisiken durch KI, KI-Agenten und die sichere Vernetzung von OT-, IoT- und Industrie-4.0-Umgebungen.
· Baue dein Wissen zu Security Assessments, Schwachstellenmanagement, Audits und der Erkennung sowie Behandlung von Cybervorfällen aus.

Ausstellung & Sponsoring

Du möchtest Kontakt zu den hochkarätigen Teilnehmenden dieser VDI-Konferenz aufnehmen und deine Produkte und Dienstleistungen einem Fachpublikum deines Marktes ohne Streuverluste präsentieren? Vor, während und nach der Veranstaltung bieten wir dir vielfältige Möglichkeiten, rund um das Konferenzgeschehens „Flagge zu zeigen“ und mit deiner potenziellen Zielgruppe ins Gespräch zu kommen. Informationen zu Ausstellungsmöglichkeiten und zu individuellen Sponsoringangeboten erhältst du von:

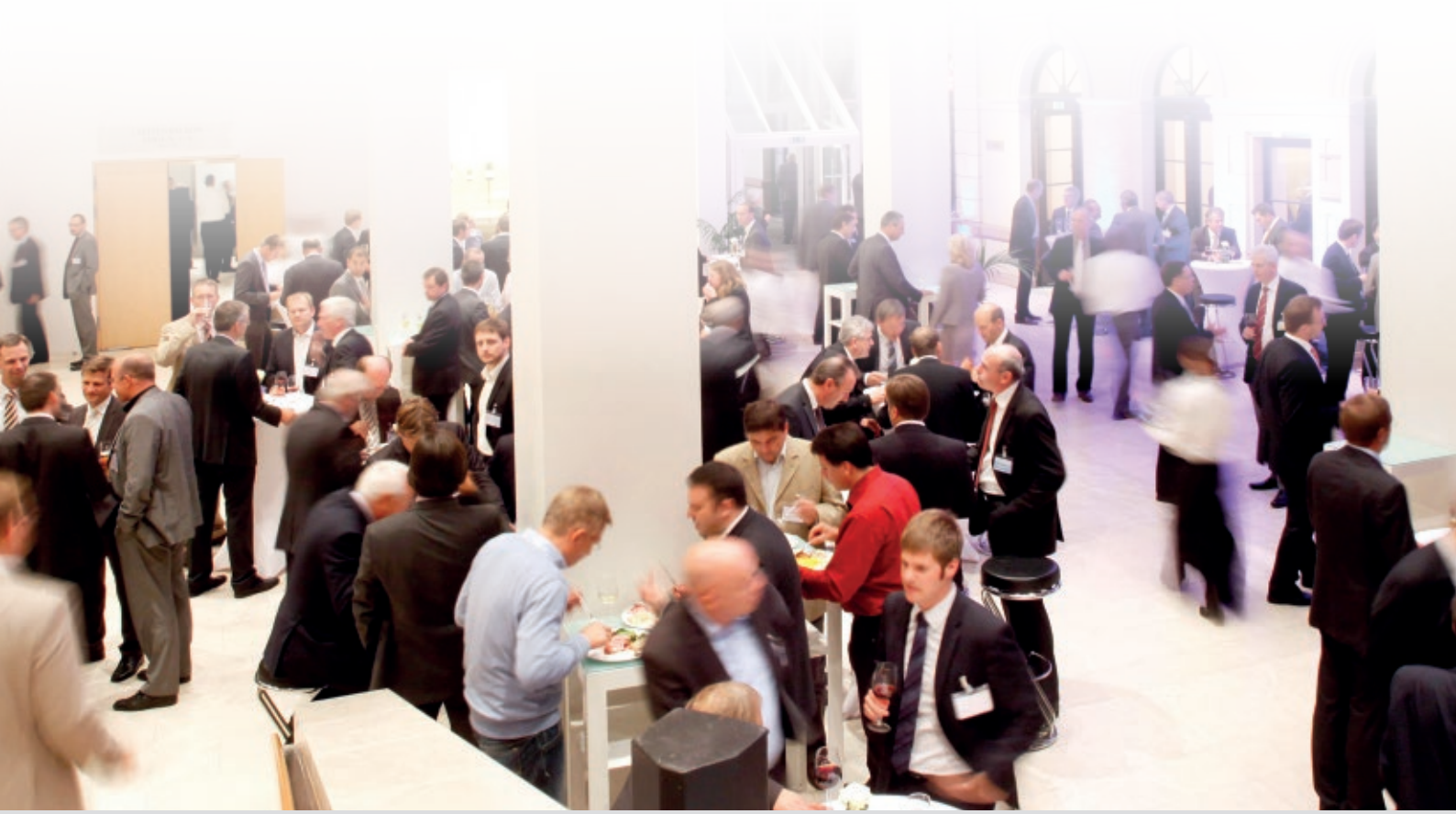
Sandra Schreiner
Projektreferentin Ausstellungen & Sponsoring
Telefon: +49 211 6214-188
E-Mail: schreiner@vdi.de

Weitere interessante Veranstaltungen

Seminar
Kommunikationssysteme für Industrie 4.0
30. Nov. und 01. Dez. 2026, Online-Seminar

Seminar
Künstliche Intelligenz und Maschinelles Lernen in der Instandhaltung
16. und 17. März 2027, Online-Seminar

VDI-Fachtagung
28. VDI-Kongress AUTOMATION 2027
08. und 09. Juni 2027, Stuttgart



VDI Wissensforum

VDI-Fachkonferenz
Industrielle Cybersicherheit

Jetzt online anmelden
www.vdi-wissensforum. de/
02K0021026

OT-Systeme und Produktionsanlagen wirksam vor Cyberangriffen schützen

VDI Wissensforum GmbH | VDI-Platz 1 | 40468 Düsseldorf | Deutschland

Sie haben noch Fragen?
Kontaktieren Sie uns einfach!

VDI Wissensforum GmbH
Kundenzentrum
Postfach 10 11 39
40002 Düsseldorf
Telefon: +49 211 6214-201
Telefax: +49 211 6214-154
E-Mail: wissensforum@vdi.de

www.vdi-wissensforum.de

✓ **Ich nehme wie folgt teil (zum Preis p. P. zzgl. MwSt.):**

VDI-Konferenz Industrielle Cybersicherheit	VDI Spezialtag Sichere drahtlose industrielle Kommunikation	Kombipreis Konferenz + 1 Spezialtag
☐ **09. und 10. Dezember 2026** **Aachen** (02K0021026)	☐ **08. Dezember 2026** **Aachen** (02ST238026)	☐ **08. bis 10. Dezember 2026** Aachen (02K0021026 + 02ST238026)
EUR 1.690,-	EUR 990,-	EUR 2.530,-

www

☐ Ich bin VDI-Mitglied und erhalte **pro Veranstaltungstag EUR 50,– Rabatt** auf die Teilnahmegebühr: Mitgliedsnr.*

* Für den VDI-Mitglieder-Rabatt ist die Angabe der VDI-Mitgliedsnummer erforderlich.

☐ **Ich interessiere mich für Ausstellungs- und Sponsoringmöglichkeiten**

Meine Kontaktdaten:

Nachname _____ Vorname _____

Titel _____ Funktion/Jobtitel _____ Abteilung/Tätigkeitsbereich _____

Firma/Institut _____

Straße/Postfach _____

PLZ, Ort, Land _____

Telefon _____ Mobil _____ E-Mail _____ Fax _____

Abweichende Rechnungsanschrift _____

_____

Datum Unterschrift

Teilnehmer mit einer Rechnungsanschrift außerhalb Deutschlands, Österreichs oder der Schweiz bitten wir, mit Kreditkarte zu zahlen. Bitte melden Sie sich über www.vdi-wissensforum.de an. Auf unserer Webseite werden Ihre Kreditkartendaten verschlüsselt übertragen, um die Sicherheit Ihrer Daten zu gewährleisten.

Die allgemeinen Geschäftsbedingungen der VDI Wissensforum GmbH finden Sie im Internet:
www.vdi-wissensforum.de/de/agb/

Veranstaltungsort(e) Spezialtag & Konferenz
Aachen: Mercure Hotel Aachen Europaplatz, Joseph-von-Görres-Str. 21 Am Europaplatz, 52068 Aachen, Tel. +49 241/16870, E-Mail: h0482@accor.com
Zimmerkontingent
Ein begrenztes Zimmerkontingent steht zur Verfügung im Mercure Hotel Aachen Europaplatz, Joseph-von-Görres-Straße 21, Tel. +49 241 1687 0, E-Mail: h0482@accor.com
Weitere Infos zur Hotelbuchung finden Sie auf der Website der Konferenz.

Weitere Hotels in der Nähe des Veranstaltungsortes finden Sie auch über unseren kostenlosen Service von HRS, www.vdi-wissensforum.de/hrs

HRS Das Hotelportal

Leistungen: Im Leistungsumfang sind die digitalen Veranstaltungsunterlagen, Pausengetränke, das Mittagessen sowie die Abendveranstaltung enthalten. Im Leistungsumfang des Spezialtages sind die Pausengetränke und das Mittagessen enthalten.

Exklusiv-Angebot: Als Teilnehmer*in dieser Veranstaltung bieten wir Ihnen eine 3-monatige, kostenfreie VDI-Probemitgliedschaft an (dieses Angebot gilt ausschließlich bei Neuaufnahme).

Datenschutz: Die VDI Wissensforum GmbH verwendet die von Ihnen angegebene E-Mail-Adresse, um Sie regelmäßig über ähnliche Veranstaltungen der VDI Wissensforum GmbH zu informieren. Wenn Sie zukünftig keine Informationen und Angebote mehr erhalten möchten, können Sie der Verwendung Ihrer Daten zu diesem Zweck jederzeit widersprechen. Nutzen Sie dazu die E-Mail Adresse wissensforum@vdi.de oder eine andere der oben angegebenen Kontaktmöglichkeiten.
Auf unsere allgemeinen Informationen zur Verwendung Ihrer Daten auf https://www.vdi-wissensforum.de/datenschutz-print weisen wir hin.
Hiermit bestätige ich die AGBs der VDI Wissensforum GmbH sowie die Richtigkeit der oben angegebenen Daten zur Anmeldung.

Ihre Kontaktdaten haben wir basierend auf Art. 6 Abs. 1 lit. f) DSGVO (berechtigtes Interesse) zu Werbezwecken erhoben. Unser berechtigtes Interesse liegt in der zielgerichteten Auswahl möglicher Interessenten für unsere Veranstaltungen. Mehr Informationen zur Quelle und der Verwendung Ihrer Daten finden Sie hier: www.wissensforum.de/adressquelle

Mit dem FSC® Warenzeichen werden Holzprodukte ausgezeichnet, die aus verantwortungsvoll bewirtschafteten Wäldern stammen, unabhängig zertifiziert nach den strengen Kriterien des Forest Stewardship Council® (FSC). Für den Druck sämtlicher Programme des VDI Wissensforums werden ausschließlich FSC-Papiere verwendet.

FSC www.fsc.org
MIX
Papier aus verantwortungsvollen Quellen
FSC® C124933