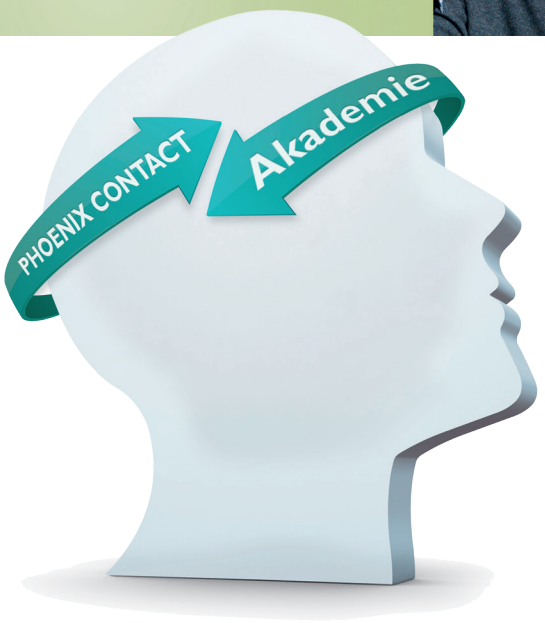
ÖSTERREICH



Schulungs- und Trainings-programm 2025

Phoenix Contact Akademie Österreich

Ihr kompetenter Schulungs- und Trainingspartner

Phoenix Contact ist ein weltweit führendes Unternehmen im Bereich der Elektrotechnik, Elektronik und Automation. Gegründet im Jahr 1923 beschäftigt das Familienunternehmen heute global rund 22.000 Mitarbeiter. In Österreich stehen für Sie 80 Mitarbeiter an unseren drei Standorten (Wien, Linz, Graz) als auch direkt vor Ort als kompetente Ansprechpartner zur Verfügung.

Ob Workshop, ein- oder mehrtägige Schulung, entweder an einer unserer Schulungsstandorte oder direkt bei Ihnen vor Ort: Sie finden bei uns genau das Training, das Sie brauchen.
Praxisnah in der Durchführung, flexibel und aktuell beim Themenangebot, Wissen direkt von der Quelle und ganz in Ihrer Nähe. Referenten, die seit Jahren Erfahrung in ihrem Thema und der Durchführung von Trainings haben, holen Sie dort ab, wo Ihre Anforderungen liegen.
Investieren Sie jetzt in Ihr Wissen!

Auf der Höhe der Zeit

Egal für welche Schulung Sie sich entscheiden – unser Angebot wird Sie überzeugen. Die Themen bauen auf anschaulichen Anwendungsbeispielen auf und sind gut verständlich, nachvollziehbar sowie leicht zu lernen. Unsere Themen sind ebenso vielfältig wie marktorientiert.

Überzeugen Sie sich von unserem Schulungs- und Trainingsangebot in der Sektion „Events & News“ » „Seminare & Trainings“ auf:

www.phoenixcontact.at

Angebotsübersicht 2025

Face-to-Face / Online

Alle Inhalte und Termine zu Schulungen und Trainings finden Sie laufend aktualisiert auf unserer Website in der Sektion „Events & News“ » „Seminare & Trainings“ auf:

www.phoenixcontact.at

Die Anmeldung erfolgt online auf unserer Website
www.phoenixcontact.at

Industrial OT- Security IEC 62443

Training für Einsteiger und Profis (1-tägig)

Als IEC 62443 zertifiziertes Unternehmen können wir das Thema aus erster Hand vermitteln

Die Normenreihe der **IEC 62443** ist ein international anerkannter Standard und beschreibt „Industrial Cyber Security für industrielle Systeme der Steuer- und Leittechnik". Mit der IEC 62443 werden organisatorische bzw. prozessuale Security-Anforderungen an Betreiber, Integratoren und Hersteller von Industrienetzwerken formuliert.
Die Norm enthält aber auch Vorschläge für Maßnahmen (foundational requirements), die bei branchenübergreifenden Sicherheits- bzw. Hardening-Maßnahmen oder Tests zur Anwendung kommen sollen.
Nach erfolgreicher Teilnahme an diesem Training erhalten Sie von Phoenix Contact ein Zertifikat als Besuchsbestätigung.

Ziele:

Wir vermitteln die Grundlagen zur Analyse von potenziellen Cyber-Security-Schwachstellen wie auch Referenzmodelle zur Umsetzung von sicheren Netzen in der industriellen Automatisierungs- und Steuerungstechnik. Die Inhalte dieses Trainings beziehen sich auf die Empfehlungen der internationalen Normenreihe IEC 62443.

Zielgruppe:

Einsteiger wie auch Spezialisten aus den Bereichen der Betriebstechnik (OT) und IT sowie Sicherheitstechniker (Funktionale Sicherheit/Safety). Betreiber von kritischer Infrastruktur (wesentliche Dienste) und ISO 27001 zertifizierte Unternehmen.

Inhalte:

- technische Security
- Firewall, NAT, Netzwerkmaske
- organisatorische Security
- Risiko-Analyse, Segmentierung
- technische Gegenmaßnahmen
- organisatorische Gegenmaßnahmen
- Security Awareness
- Normen, Richtlinien und Gesetze
- weitere Security Aspekte

Schulungstermine auf Anfrage!

Industrial OT- Security IEC 62443

TÜV Rheinland „Cyber Security Program" (4-tägig)

Phoenix Contact Cyber Security GmbH ist anerkannter Kursanbieter für Cyber Security im international etablierten „TÜV Rheinland Functional Safety (FS) & Cyber Security (CySec) Training Program"

Das Training dient der ausführlichen Vermittlung von wichtigem Grundlagenwissen in verschiedenen Themenbereichen von Cyber Security in Industrial Automation and Control Systems (IACS). Die Inhalte dieses Trainings sind eng abgestimmt auf die Inhalte und Anforderungen der Prüfung „Fundamentals of Cyber Security – TÜV Rheinland Cyber Security Training Program" und orientieren sich stark an den Vorgaben und Empfehlungen der internationalen Normenreihe ISA/IEC 62443. Die Prüfung ist Bestandteil des Trainings und wird direkt im Anschluss an das Training durchgeführt.
Voraussetzungen: Kenntnisse in den Bereichen der Elektrotechnik sowie Anwenderkenntnisse im Bereich Software.

Ziele:

- Breit gefächertes Grundlagenwissen im Bereich Cybersicherheit für IACS
- Förderung einer gemeinsamen Sprache von IT und OT in Bezug auf Security und Safety
- Erlangung des notwendigen Wissens zur Ablegung der Prüfung „Fundamentals of Cyber Security – TÜV Rheinland FS & CySec Training Program"

Zielgruppe:

Meister, Techniker, Ingenieure, Software- und Hardware-Entwickler, Berater, etc. die in Design, Entwicklung, Betrieb, Wartung und Management von IACS involviert sind.
Allgemein alle Personen mit einem Interesse daran Anforderungen und Ziele von Cybersicherheit für IACS zu verstehen.

Inhalte:

- Netzwerk Grundlagen
- TCP/IP Grundlagen
- technische Security
- organisatorische Security
- Security Awareness
- Standards, Richtlinien und Gesetze
- technische Gegenmaßnahmen
- weitere Aspekte von Security

TÜVRheinland®

Eine bestandene Prüfung, bestätigt durch eine vom TÜV Rheinland ausgestellte formelle Bescheinigung, dient als Nachweis des erforderlichen Grundlagenwissens auf dem Weg zum „CySec Specialist (TÜV Rheinland)".

Die Anmeldung erfolgt online auf unserer Website
www.phoenixcontact.at

Cyber Security Technician

TÜV Rheinland „Cyber Security Program“ (5-tägig)

Werden Sie zum von TÜV Rheinland zertifizierten Experten für die Implementierung von Cyber Security Funktionen. Erlernen Sie notwendige Grundlagen der Cyber Security für Industrial Automation & Control Systems (IACS) in Theorie und Praxis. Weisen Sie dieses Wissen durch ein international anerkanntes Zertifikat von TÜV Rheinland nach.

Das Training orientiert sich in Inhalt und Umfang an den „Empfehlungen für Fortbildungs- und Qualifizierungsmaßnahmen im ICS-Umfeld“ des Bundesamt für Sicherheit in der Informationstechnik BSI, siehe BSI-CS 123, Kapitel 3: Schulung für Experten der Produktion. Zusätzlich fokussiert das Training auf Anfordungen und Empfehlungen aus der internationalen Normenreise ISA/IEC 62443. Die Prüfung ist Bestandteil des Trainings und wird direkt im Anschluss an das Training durchgeführt.
Voraussetzungen: Kenntnisse in den Bereichen der Elektrotechnik sowie Anwenderkenntnisse im Bereich Software.

Ziele:
Das Seminar dient generell der ausführlichen Vermittlung von wichtigem Grundlagenwissen in verschiedenen Themenbereichen von Cyber Security in Industrial Automation & Control Systems (IACS). Bedingt durch die immer enger werdende Verzahnung von Produktionsumgebungen (OT, Operational Technology) und klassischer EDV (IT, Information Technology), wird eine gemeinsame Sprache von IT und OT gefördert. Die Teilnehmer erlangen Wissen über grundlegende Maßnahmen technischer und organisatorischer Art zur Absicherung einer IACS-Umgebung und setzen verschiedene dieser Kenntnisse zur Erhöhung der Cyber Security an einer realitätsnahen Beispielumgebung praktisch um.

Inhalte:
- Netzwerk Grundlagen
- TCP/IP Grundlagen
- technische Cyber Security
- organisatorische Cyber Security
- wirksame Gegenmaßnahmen
- Standards, Richtlinien und Gesetze
- weitere Aspekte von Security
- praktische Übungen

Zielgruppe:
Meister, Techniker, Ingenieure, Software- und Hardware-Entwickler, Berater, etc. die in Design, Entwicklung, Betrieb, Wartung und Management von IACS involviert sind.

Industrial Cyber Security

Incident Handling für OT-Umgebungen

Umgang mit Sicherheitsvorfällen mit OT-Systemen und Simulation der Angriffsszenarien

Vernetzte IT-Systeme sind fast ständig Angriffen aus dem Internet ausgesetzt. Dies gilt zunehmend auch für industrielle Kontrollsysteme. Zahlreiche Beispiele aus der Vergangenheit haben dies gezeigt. Im Falle eines Cyber-Angriffs ist die richtige Vorbereitung essenziell, um richtig auf einen Angriff reagieren zu können.
In diesem Training wird neben den technischen und organisatorischen Maßnahmen auch ein konkretes Angriffsszenario praktisch in der AIT Cyber Range simuliert. Eine Cyber Range ist eine Simulationsumgebung, die es Teilnehmern von Schulungen und Trainings ermöglicht, Aufgaben in einer möglichst realistischen Umgebung bewältigen und die notwendigen Prozesse erlernen zu können.

Ziele:
- Kennenlernen typischer Bedrohungen von OT-Systemen
- Verständnis entwickeln für die Rolle eines Security Operations Center (SOC) bei der Behandlung von Sicherheitsvorfällen
- In einer praktischen Übung auf der AIT Cyber Range die richtige Vorgehensweise bei Sicherheitsvorfällen exerzieren

Inhalte:
- OT-Bedrohungen
- Security Operations Center
- OT Intrusion Detection
- Security Information and Event Management
- digitale Forensik für OT-Umgebungen
- Einführung in die AIT Cyber Range
- Planspiel OT-Security

Zielgruppe:
Einsteiger wie auch Spezialisten aus den Bereichen der Betriebstechnik (OT) und IT sowie Sicherheitstechniker (Funktionale Sicherheit/Safety). Betreiber von kritischer Infrastruktur (wesentliche Dienste).

AUSTRIAN INSTITUTE OF TECHNOLOGY

PHOENIX CONTACT

Die Anmeldung erfolgt online auf unserer Website
www.phoenixcontact.at

Industrial Cyber Security

Industrielle Cybersicherheit IEC 62443

Grundlagen (ONLINE)

Wissen aus erster Hand – Phoenix Contact ist seit 2020 IEC 62443-2-4 zertifiziert

Im ersten Teil dieses Online-Trainings erhalten Sie einen grundlegenden Überblick zum Thema Informationssicherheit in Industrial Automation and Control Systems (IACS), im zweiten Teil geben wir einen ausführlichen Einblick in die ISA/IEC 62443 und deren Substandards.
Neben der Vermittlung von Informationen zu den einzelnen Substandards werden auch in der Praxis anwendbare Vorgehensweisen vorgestellt, um den verschiedenen Anforderungen aus den Substandards gerecht werden zu können.
Voraussetzungen: Laptop für das Webinar und Internet-Zugang

Ziele:

Teilnehmer dieses Online-Trainings verstehen die grundsätzlichen Belange und Anforderungen im Themengebiet der industriellen Informationssicherheit. Darüber hinaus sind Sie in der Lage, sich als Produktentwickler, Anlagenintegrator oder Anlagenbetreiber in der internationalen Standardreihe ISA/IEC 62443 zurechtzufinden und die für Sie relevanten Dokumente der Standardreihe zu identifizieren und anzuwenden.

Zielgruppe:

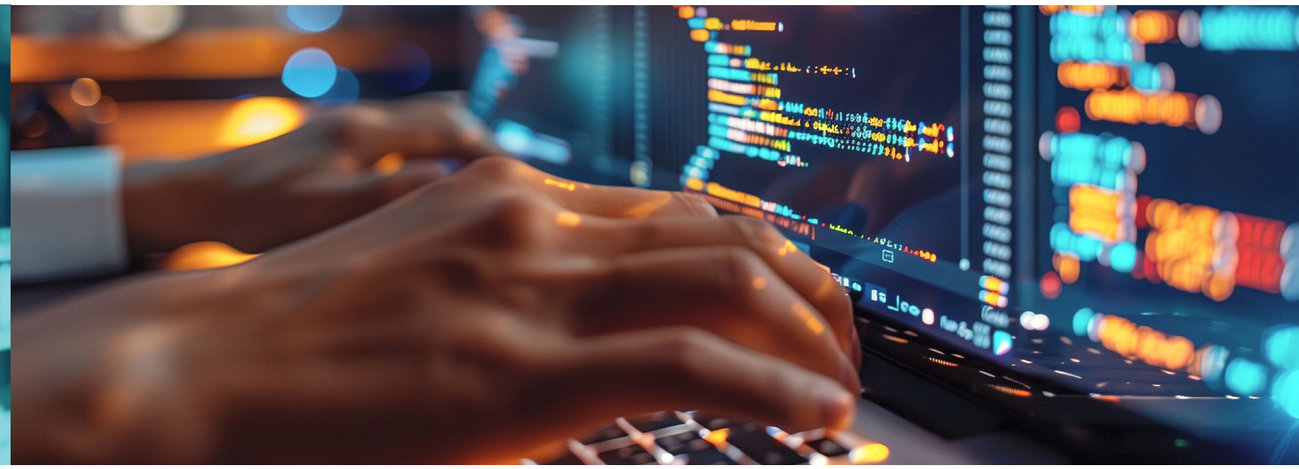
Einsteiger wie auch Spezialisten aus den Bereichen der Betriebstechnik (OT) und IT sowie Sicherheitstechniker (Funktionale Sicherheit/Safety). Betreiber von kritischer Infrastruktur (wesentlichen Diensten) und ISO 27001 zertifizierte Unternehmen.

Inhalte:

Ausführlich behandelt werden insbesondere die grundlegenden Konzepte der ISA/IEC 62443, wie:

- Zones & Conduits
- Security Level
- Foundational Requirements
- Security & Product Lifecycles
- Security Management System
- Security Program Requirements
- Risk Assessment Requirements
- System Requirements
- Secure Development Lifecycle
- Component Requirement

Sichere Produktentwicklung für OT & (I)IoT



Produkte konform zu Cyber Resilience Act, Maschinenverordnung, IEC 62443-4-1 und Co. entwickeln

Wer die Security und damit die Qualität seiner Produkte nicht dem Zufall überlassen möchte, der muss einen proaktiven Zugang wählen. Nur durch die Integration von Security in die Entwicklungsprozesse und durch eine Organisation, die mit dem Thema professionell umzugehen weiß, entstehen hochwertige, dem Markt gerechte Produkte. Das Training „Sichere Produktentwicklung für OT und (I)IoT“ vermittelt den Teilnehmern, wie Security in die Produktentwicklung integriert werden kann, um ihre Produkte nachhaltig sicher zu machen.
Voraussetzungen: Grundlegendes Wissen der Softwareentwicklung

Ziele:

Die TeilnehmerInnen sollten nach der Ausbildung den Zusammenhang von Safety und Security verstehen. Des Weiteren müssen die regulatorischen und normativen Anforderungen angewendet werden können. Die Produktentwicklung und das dazugehörige Verständnis wird in allen Organisationen eine wesentliche Rolle im Teil der Wertschöpfungskette einnehmen. Selbiges gilt für Threat Modelle und der Erarbeitung der dazugehörigen Lösungen, um geeignete Methoden und Maßnahmen zur Integration von Security ableiten zu können. Hierbei können nützliche Tools zur Überprüfung und Verbesserung der Produktsicherheit eingesetzt werden.

Zielgruppe:

Produktmanager, Entwicklungsleiter, Software Architekten, Entwickler, Security-Verantwortliche bei Maschinenbauern, industriellen Komponenten- und Lösungsanbietern sowie Systemintegratoren

Inhalte:

- Überblick Regularien und Normen
- Security Management (Produktklassifizierung, Security Organisation, Security Trainings, Integritätsschutz, Absicherung der Entwicklungsumgebung, Auswahl sicherer Komponenten)
- Spezifikation von Security Requirements
- Secure by Design & Secure Implementation
- Security Verification & Validition Testing
- Schwachstellen-Management
- PSIRT & Security Update Management
- Security Guidelines

LIMES SECURITY

Industrial OT- Security IEC 62443 (4 Tage mit Prüfung)

Datum	Dauer	Ort	Location	Preis*
05.05. – 08.05.2025	4 Tage	Graz	PHOENIX CONTACT GmbH Gasometerweg 47, 8055 Graz	€ 2.550,-

Cyber Security Technician (5 Tage mit Prüfung)

Datum	Dauer	Ort	Location	Preis*
14.07. – 18.07.2025	5 Tage	Wien	PHOENIX CONTACT GmbH Ada-Christen-Gasse 4, 1100 Wien	€ 3.250,-
08.09. – 12.09.2025	5 Tage	Graz	PHOENIX CONTACT GmbH Gasometerweg 47, 8055 Graz	€ 3.250,-
06.10. – 10.10.2025	5 Tage	Linz	PHOENIX CONTACT GmbH Flachenauergutstraße 10, 4020 Linz	€ 3.250,-
10.11. – 14.11.2025	5 Tage	Wien	PHOENIX CONTACT GmbH Ada-Christen-Gasse 4, 1100 Wien	€ 3.250,-

Incident Handling für OT-Umgebungen

Datum	Dauer	Ort	Location	Preis*
18.03. – 19.03.2025	1,5 Tage	Wien	AIT Austrian Institute of Technology GmbH Giefinggasse 4, 1210 Wien	€ 1.500,-
07.10. – 08.10.2025	1,5 Tage	Wien	AIT Austrian Institute of Technology GmbH Giefinggasse 4, 1210 Wien	€ 1.500,-

* alle Preise exkl. MwSt

Ihre Ansprechpartner:

Erich Kronfuss
Industrial IoT-Security Specialist
Industry Management & Automation
Tel: +43 (0)664 6086 7249

Helmut Hagn
Industrial IoT-Security Specialist
Industry Management & Automation
Tel: +43 (0)664 6086 7210

Industrielle Cybersicherheit IEC 62443

Datum	Dauer	Ort	Location	Preis*
26.02.2025	1 Tag Modul 1 08:30 Uhr bis 11:30 Uhr Modul 2 13:00 Uhr bis 16:00 Uhr	online	PHOENIX CONTACT Online Akademie	€ 600,-
20.05.2025	1 Tag Modul 1 08:30 Uhr bis 11:30 Uhr Modul 2 13:00 Uhr bis 16:00 Uhr	online	PHOENIX CONTACT Online Akademie	€ 600,-
10.11.2025	1 Tag Modul 1 08:30 Uhr bis 11:30 Uhr Modul 2 13:00 Uhr bis 16:00 Uhr	online	PHOENIX CONTACT Online Akademie	€ 600,-

Informationen zum Webinar:

Das Webinar „Industrielle Cybersicherheit - Grundlagen IEC62443“ haben wir für Sie in zwei Module unterteilt.
Es besteht die Möglichkeit, diese an verschiedenen Tagen zu wählen.

Die Präsenzdauer steht im Verhältnis 6h +1h (Beratung) pro Webinar. Mit der einstündigen Beratung besteht für Sie die Möglichkeit, nach dem Webinar, innerhalb einer Woche, den Referenten mit Fragen zum Seminar telefonisch zu kontaktieren.

Sichere Produktentwicklung für OT & (I)IoT

Datum	Dauer	Ort	Location	Preis*
02.06. – 04.06.2025	2,5 Tage	Wien	PHOENIX CONTACT GmbH Ada-Christen-Gasse 4, 1100 Wien	€ 2.210,-

* alle Preise exkl. MwSt

Maschinenverordnung (EU) 2023/1230

Anwendung der Maschinenverordnung in der Praxis: In drei Etappen mit der Konformitätsbewertung zur CE-Kennzeichnung.

Lernen Sie als Hersteller von Maschinen die relevanten Artikel und Anhänge der neuen EU-Maschinenverordnung kennen. Speziell nach der Umstellung von der Maschinenrichtlinie zur EU-Maschinenverordnung sind neue Anforderungen dazu gekommen.

Ziele:

Sie können die möglichen Konformitätsbewertungsverfahren und deren praktische Umsetzung für Ihre Art von Maschine anwenden.

Sie wissen, was alles notwendig ist, um eine Maschine verordnungskonform zu konstruieren, zu bauen und in Verkehr zu bringen.

Zielgruppe:

- CE-Verantwortliche
- Händler, Hersteller, Konstrukteure und Importeure von Maschinen, unvollständigen Maschinen und Sicherheitsbauteilen
- Maschinenbetreiber
- Personen, die Maschinen verändern
- Personen, die mehrere Maschinen zu einer Gesamtheit von Maschinen verketten
- Personen, die unvollständige zu vollständigen Maschinen zusammenstellen

Inhalte:

- Anwendungsbereich und Begriffsbestimmungen
- Vollständige und unvollständige Maschinen
- EU-Konformitätsbewertungsverfahren
- Vorstellung der EU-Module für die Bewertung
- „Hochrisiko-Kategorien“ von Maschinen (Anhang I)
- Grundlegende Gesundheits- und Schutzanforderungen (Anhang II)
- EU-Erklärung (Anhang V)
- Montageanleitungen (Anhang IV)
- Technische Unterlagen (Anhang IV)
- Wesentliche Änderung an Maschinen

Neue EU-Maschinenverordnung

Zentrale Veränderungen und Grundlagen (halbtags)

Lernen Sie als Hersteller von Maschinen die relevanten Artikel und Anhänge der neuen Maschinenverordnung kennen.

Zudem: Welche neuen Anforderungen sind nach der Umstellung von der Maschinenrichtlinie zur Maschinenverordnung dazugekommen? Verschaffen Sie sich einen schnellen und fundierten Überblick.

Ziele:

Verstehen und Umsetzen der aktualisierten rechtlichen Anforderungen für Maschinenhersteller und weiterer Wirtschaftsakteure: Änderungen von der Maschinenrichtlinie 2006/42/EG zur neuen Maschinenverordnung (EU) 2023/1230.

Zielgruppe:

- CE-Verantwortliche
- Händler, Hersteller, Konstrukteure und Importeure von Maschinen, unvollständigen Maschinen und Sicherheitsbauteilen
- Maschinenbetreiber
- Personen, die Maschinen verändern
- Personen, die mehrere Maschinen zu einer Gesamtheit von Maschinen verketten
- Personen, die unvollständige zu vollständigen Maschinen zusammenstellen

Inhalte:

- Anwendung der Maschinenverordnung (EU) 2023/1230 und Abgrenzung von anderen Richtlinien
- Übersicht Veränderungen der Maschinenrichtlinie
- Bedeutung harmonisierter Normen bei der Konstruktion und bei der Herstellung
- Organisatorischer Ablauf der Konformitätsbewertungsverfahren für Maschinen und die Vorgehensweise für unvollständige Maschinen
- Praxisorientierte Methoden und Prozesse zum Erreichen der Richtlinienkonformität
- Beispiele zur Erfüllung der Richtlinienanforderungen durch harmonisierte Normen
- Zusammenhang der technischen Unterlagen der Maschine, der Konformitätserklärung und der CE-Kennzeichnung

Risikobeurteilung EN ISO 12100

Wie Sie die Anforderungen der Maschinenrichtlinie 2006/42/EG zur Risikobeurteilung praktisch umsetzen

In diesem Tagesseminar bekommen Sie das Know-how zur praktischen Umsetzung einer Risikobeurteilung in Bezug zur Maschinenrichtlinie 2006/42/EG.
Voraussetzungen: Grundlagenkenntnisse zur Maschinenrichtlinie

Ziele:

Sie wenden die Methoden und Prozesse an einer realen Beispielmaschine an und dokumentieren die Ergebnisse und abgeleiteten Maßnahmen.
Im Anschluss kennen Sie die notwendigen Schritte zur Durchführung und Dokumentation der Risikobeurteilung einer Maschine und wissen, wie Sie diese in Ihrer Praxis umsetzen können.

Zielgruppe:

- Verantwortliche für funktionale Sicherheit
- Elektro- und Maschinenbaukonstrukteure
- Projektleiter

Inhalte:

- Vorstellung der Phasen des Sicherheitslebenszyklus‘ für Maschinen und deren Inhalte
- erforderliche Vorgehensweise für die Risikobeurteilung, die Phase 0 des Sicherheitslebenszyklus‘ für Maschinen in Theorie und Praxis:
  - Ermitteln der Maschinengrenzen
  - Identifizieren der Gefährdungen
  - Bewerten der Risiken
  - Risikominderung durch geeignete Maßnahmen:
    - konstruktiv
    - technisch
    - hinweisend
  - Dokumentation der Ereignisse

Funktionale Sicherheit EN ISO 13849-1:2023

Erlernen Sie die einfache Umsetzung der Anforderungen der EN ISO 13849-1

Die Maschinenrichtlinie 2006/42/EG (Anhang I) und die Maschinenverordnung (MVO) (Anhang III) fordert bezüglich der Sicherheit und Zuverlässigkeit von Steuerungen geeignete Maßnahmen, um Ausfälle zu vermeiden. Auf Basis der in der Risikobeurteilung festgelegten Anforderungen an den Performance-Level (PL) müssen die sicherheitsrelevanten Teile der Steuerung entsprechend geplant und umgesetzt werden.

Die Sicherheitsanforderungsspezifikation (SRS) für jede einzelne Sicherheitsfunktion, die im Rahmen der Risikobeurteilung nach DIN EN ISO 12100 entsteht, bildet die Grundlage für die Arbeit mit der EN ISO 13849-1.
Voraussetzungen: Kenntnisse der Sicherheitstechnik und der Maschinenrichtlinie.

Ziele:

Neben den geeigneten Hardwarestrukturen für Sicherheitssteuerungen lernen Sie die Verfahren zur Erstellung sicherer Software. Nach der Veranstaltung können Sie den erforderlichen Performance Level einer Sicherheitssteuerung bestimmen und kennen die dafür nötigen Schnittstellen zur Mechanik. Sie können Sicherheitssteuerungen optimal aufbauen und kennen die Grundlagen und Verfahren zur Berechnung des erreichten Performance Levels.
Darüber hinaus haben Sie einen Überblick über die Möglichkeiten der Software SISTEMA, ein Tool zur Bewertung von Sicherheitsfunktionen.

Zielgruppe:

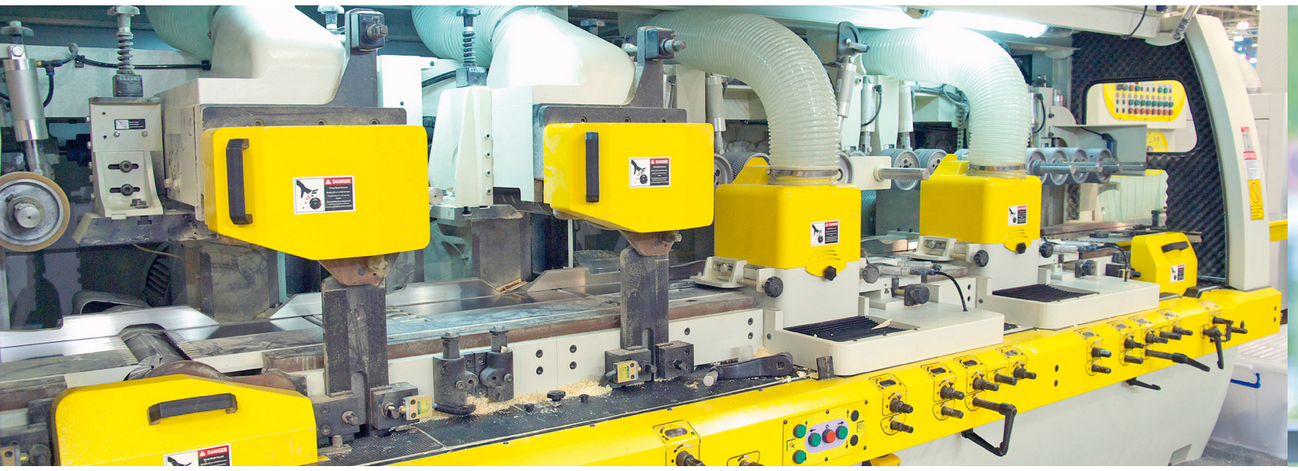
- Konstrukteure von Maschinensteuerungen
- Prüfer & Qualitätsmanager
- Projektleiter, Servicetechniker oder Produktmanager

Inhalte:

- die Begriffe der Norm und ihre Bedeutung
- Konstruieren nach Norm
- Bestimmen des erforderlichen Performance Levels an verschiedenen Beispielen
- Konstruieren von Sicherheitsfunktionen
- Beispiele für das Berechnen des erreichten Performance Levels
- Validieren von Sicherheitsfunktionen

EN ISO 13849-1 reloaded

Sicherheitsbezogene Teile von Steuerungen richtig planen und umsetzen (halbtags)



Sie wollen sicherheitsbezogene Teile von Steuerungen gemäß den Anforderungen der Maschinenrichtlinie bzw. zukünftig gemäß der EU-Maschinenverordnung richtig planen und umsetzen?

Dann nutzen Sie die etablierte Norm EN ISO 13849-1 als technische Hilfestellung, sie wurde gerade erst aktualisiert und erweitert. Erlernen Sie die zentralen Inhalte und Veränderungen der EN ISO 13849-1 direkt zur Anwendung in Ihrer Praxis.

Ziele:
Aktualisierte Sicherheitsstandards verstehen und umsetzen: Änderungen der EN ISO 13849-1 von 2016 zu 2023. Vertiefen Sie Ihr Wissen über die neuesten Sicherheitsanforderungen und -standards, um Ihre Maschinensteuerungen noch sicherer und zuverlässiger zu gestalten.

Zielgruppe:

- CE-Verantwortliche
- Händler, Hersteller, Konstrukteure und Importeure von Maschinen, unvollständigen Maschinen und Sicherheitsbauteilen
- Maschinenbetreiber
- Personen, die Maschinen verändern
- Personen, die mehrere Maschinen zu einer Gesamtheit von Maschinen verketten
- Personen, die unvollständige zu vollständigen Maschinen zusammenstellen

Inhalte:

- Überblick über die Neuerungen der Norm
- Die Begriffe der Norm und ihre Bedeutung
- Anwendung der Norm / Iterativer Prozess zur Gestatung von Sicherheitsfunktionen
- Bestimmen des erforderlichen Performance Levels an verschiedenen Beispielen
- Konstruieren von Sicherheitsfunktionen
- Beispiele für das Berechnen des erreichten Performance Levels
- Validieren von Sicherheitsfunktionen

SISTEMA

Lernen Sie den einfachen Umgang mit dem Softwareassistent SISTEMA zur PL-Bewertung von sicherheitsbezogenen Maschinensteuerungen nach EN ISO 13849

SISTEMA ist ein Tool zur Bewertung von Sicherheitsfunktionen, welches kostenlos von dem IFA zur Verfügung gestellt wird. Es bietet umfassende Hilfestellungen bei der Anwendung der EN ISO 13849-1 zur Ermittlung des Performance Levels. Voraussetzungen: Grundlegende Kenntnisse der Sicherheitstechnik und der EN ISO 13849-1. Den Teilnehmern an diesem Seminar sollten die sicherheitstechnischen Kennwerte PL, MTTFd, Kategorie, DC und CCF geläufig sein.

Ziele:

Nach der Teilnahme an diesem Eintagesseminar haben Sie das erforderliche Wissen für das optimale Arbeiten mit der Sicherheitssoftware SISTEMA.

Zielgruppe:

- Konstrukteure, Prüfer und Entwickler, die für technische Schutzeinrichtungen an Maschinen verantwortlich sind
- Hersteller und Konstrukteure von Maschinen
- Personen, die Maschinen verändern

Inhalte:

- Bedienen der Software, Anlegen des Projektbaums, Erstellen von SUB-Systemen, Eingabe der sicherheitstechnischen Kennwerte und Auswerten der Ergebnisse
- Zusammenfassen und Beschreiben der erforderlichen sicherheitstechnischen Kennwerte wie: PL, MTTFd, Kategorie, DC, CCF
- Umsetzen der EN ISO 13849
- Modellieren einer Sicherheitsfunktion auf Basis der vorgesehenen Strukturen und der sicherheitstechnischen Kennwerte
- Umsetzen dieser Sicherheitsfunktion in Form eines Projektes
- Erstellen von Beispielprojekten, in denen Sie die Auswirkung der sicherheitstechnischen Kennwerte auf den resultierenden PL erkennen
- Nutzen und Erstellen von Bibliotheken
- Nutzen der Software mit mehreren Usern

5 -Tagesseminar
FS Technician for Machinery
mit TÜV Rheinland-Zertifikat

Werden Sie zum TÜV- zertifizierten Experten der funktionalen Sicherheit und lernen Sie alles rund um die CE-Kennzeichnung von Maschinen

Mit erfolgreich bestandener Abschlussprüfung erhalten die Teilnehmer das anerkannte Functional Safety Technician (TÜV Rheinland) Zertifikat und werden namentlich als FS Technician (TÜV Rheinland) for Machinery - CE Practice auf der Seite der TÜV Rheinland Industrie Service GmbH gelistet (www.tuvasi.com). Das Zertifikat ist ein in der Branche international anerkannter Qualifikationsnachweis, der das für die praktische Umsetzung erforderliche Wissen zur Umsetzung der Anforderungen an die Maschinensicherheit belegt.

Ziele:

Sie bekommen das Know-how für die Umsetzung der erforderlichen Aktivitäten für die funktionale Sicherheit von Maschinen und erfahren darüber hinaus, welche weiteren Schritte vor dem Anbringen des CE-Zeichens erforderlich sind.

Zielgruppe:

Maschinenbau-/Elektrokonstrukteure, Software-/Hardware-Entwickler, Projektleiter, Qualitätsmanager, FS Engineers, Techniker, Facharbeiter, Meister

Inhalte:

- Phase 0: Risikobeurteilung der Maschine
- Phase 1: Sicherheitsplanung
- Phase 2: Spezifikation
- Phase 3: Validierungsplanung
- Phase 4: Realisierung
- Phase 5: Verifikation
- Phase 6: Code-Simulation
- Phase 7: Validierung
- Zusammenfassung der Themen
- Beantworten von Teilnehmerfragen
- Prüfung

TÜVRheinland®

Nach Ihrer Anmeldung zu diesem Seminar erhalten Sie ein Formular „Teilnahmevoraussetzungen“ und retournieren dieses ausgefüllt an at_training@phoenixcontact.com

Maschinenverordnung (EU) 2023/1230

Datum	Dauer	Ort	Location	Preis*
17.03.2025	1 Tag	Linz	PHOENIX CONTACT GmbH Flachenauergutstraße 10, 4020 Linz	€ 500,-
08.09.2025	1 Tag	Wien	PHOENIX CONTACT GmbH Ada-Christen-Gasse 4, 1100 Wien	€ 500,-

Neue EU-Maschinenverordnung (halbtags)

Datum	Dauer	Ort	Location	Preis*
20.03.2025	1/2 Tag	Linz	PHOENIX CONTACT GmbH Flachenauergutstraße 10, 4020 Linz	€ 310,-
11.09.2025	1/2 Tag	Wien	PHOENIX CONTACT GmbH Ada-Christen-Gasse 4, 1100 Wien	€ 310,-

Risikobeurteilung EN ISO 12100

Datum	Dauer	Ort	Location	Preis*
18.03.2025	1 Tag	Linz	PHOENIX CONTACT GmbH Flachenauergutstraße 10, 4020 Linz	€ 500,-
09.09.2025	1 Tag	Wien	PHOENIX CONTACT GmbH Ada-Christen-Gasse 4, 1100 Wien	€ 500,-

Funktionale Sicherheit EN ISO 13849-1:2023

Datum	Dauer	Ort	Location	Preis*
19.03.2025	1 Tag	Linz	PHOENIX CONTACT GmbH Flachenauergutstraße 10, 4020 Linz	€ 500,-
10.09.2025	1 Tag	Wien	PHOENIX CONTACT GmbH Ada-Christen-Gasse 4, 1100 Wien	€ 500,-

Ihr Ansprechpartner:

* alle Preise exkl. MwSt

Andreas Paprstein
Spezialist für Maschinen- und Anlagensicherheit
Tel: +43 (0)676 8372 0240

EN ISO 13849-1 reloaded (halbtags)

Datum	Dauer	Ort	Location	Preis*
20.03.2025	1/2 Tag	Linz	PHOENIX CONTACT GmbH Flachenauergutstraße 10, 4020 Linz	€ 310,-
11.09.2025	1/2 Tag	Wien	PHOENIX CONTACT GmbH Ada-Christen-Gasse 4, 1100 Wien	€ 310,-

SISTEMA

Datum	Dauer	Ort	Location	Preis*
21.03.2025	1 Tag	Linz	PHOENIX CONTACT GmbH Flachenauergutstraße 10, 4020 Linz	€ 500,-
12.09.2025	1 Tag	Wien	PHOENIX CONTACT GmbH Ada-Christen-Gasse 4, 1100 Wien	€ 500,-

5-Tagesseminar FS Technician for Machinery
mit TÜV Rheinland-Zertifikat

Datum	Dauer	Ort	Location	Preis*
24.03. – 28.03.2025	5 Tage	Linz	PHOENIX CONTACT GmbH Flachenauergutstraße 10, 4020 Linz	€ 2.550,-
15.09. – 19.09.2025	5 Tage	Wien	PHOENIX CONTACT GmbH Ada-Christen-Gasse 4, 1100 Wien	€ 2.550,-

* alle Preise exkl. MwSt

Ihr Ansprechpartner:

Andreas Paprstein
Spezialist für Maschinen- und Anlagensicherheit
Tel: +43 (0)676 8372 0240

SPT – System Protection Technologies

Überspannungsschutz in Theorie und Praxis

Vorsorge ist besser als Nachsorge, denn das Risiko von Überspannungsschäden ist größer als Sie glauben

In den letzten Jahren ist der Einsatz von Elektrik und Elektronik in Unternehmen und Haushalten massiv gestiegen. Nichtsdestotrotz ist der Blitz- und Überspannungsschutz ein nach wie vor oft vernachlässigtes Thema. Denn im Gegensatz zu einem FI merkt man beim Überspannungsschutz nichts, wenn er aktiviert wird. Gibt es Lücken im Schutzkonzept oder fehlt es sogar komplett, sind die Auswirkungen fatal. Im schlimmsten Fall fällt nicht nur der Strom aus und Geräte oder Anlagen werden beschädigt, sondern es ensteht ein Brand. In allen Fällen bleibt ein schaler Nachgeschmack, denn die Versicherungsentschädigung fällt in der Regel niedriger aus als die tatsächliche Schadenssumme.
Voraussetzungen: Grundkenntnisse der Elektrotechnik

Ziele:

In diesem Seminar frischen wir zuerst die Grundlagen des Überspannungsschutzes auf. Dabei wird unter anderem darauf eingegangen, wie Überspannung entsteht, wie sie in das Leitungssystem gelangt und welche Schäden dabei entstehen. Danach werden die verschiedenen Aspekte der erforderlichen Ableiter-Koordination anhand von praxisorientierten Beispielen ausführlich erörtert. Anschließend vertiefen Sie diese Kenntnisse für die Anwendung der MSR-Technik und bei Photovoltaik-Anlagen. Am Ende der Schulung sind Sie in der Lage, ein Überspannungsschutzkonzept, in Übereinstimmung mit den geltenden rechtlichen Vorschriften, selbst zu erstellen.

Inhalte:

- Wie entstehen Überspannungen
- Wie kommt Überspannung in die Leitungssysteme
- Wie schütze ich vor Überspannung
- Zusammenhang zwischen inneren und äußeren Blitzschutz
- Ableiter-Koordination – Blitzschutzklassen und geeignete Ableiter
- Überspannungsschutz für MSR-Technik
- Überspannungsschutz für Photovoltaik-Anlagen
- Installationshinweise und Praxisbeispiele

Zielgruppe:

Planer, Installateure, Betreiber elektrischer und elektronischer Anlagen, Verantwortliche der Betriebstechnik, Personen mit Lehrtätigkeit

Schulungstermine auf Anfrage!

PLCnext Engineer – Das Programmierwerkzeug

Erlernen Sie die Erstellung von IEC 61131-Projekten mit PLCnext Engineer

Wenn Sie bereits erste Erfahrungen im Bereich der Programmierung von SPS-Systemen haben, dann bietet Ihnen dieser Kurs einen Schnelleinstieg in die IEC 61131 Programmierung mit der Software-Plattform PLCnext Engineer von Phoenix Contact. Dieser Kurs richtet sich sowohl an Anlagen-Programmierer als auch an Inbetriebnahnme-Techniker.
Voraussetzungen: Grundlagen der Automatisierungstechnik, Programmiererfahrungen.

Ziele:

Am Ende des Kurses sind Sie in der Lage, mit PLCnext Engineer IEC61131 Projekte zu realisieren. Sie kennen die Funktionalitäten der Software und gewinnen einen Eindruck in die integrierte Visualisierung. Anhand von Übungen haben Sie die Möglichkeiten der Software verinnerlicht.

Zielgruppe:

Meister, Techniker, Ingenieure, Software- und Hardware-Entwickler, Berater, etc., die in Design, Entwicklung, Betrieb, Wartung und Management von IACS involviert sind.

Inhalte:

- Kennenlernen der Oberfläche des Werkzeugs PLCnext Engineer
- Erstellung eines Projekts
- Handhabung der Editoren
- Kontaktplanprogrammierung
- Funktionsbausteinprogrammierung
- Strukturierter Text-Programmierung
- Schrittkettenprogrammierung
- Benutzerdefinierte Datentypen
- Bibliotheken erstellen und verwenden
- Debugmodus
- eHMI

Schulungstermine auf Anfrage!

PLCnext Technology (inkl. Starterkit)

Tauchen Sie ein in die Welt der modernen SPS-Programmierung mit einer Kombination aus IEC 61131 und Hochsprachen in PLCNext Engineer

Zu diesem Kurztraining erhalten Sie ein vollständig aufgebautes PLCnext Technology-Starterkit, einschließlich PLCnext Steuerung AXC F 2152, I/O-Module AXL Smart Elements DI16/DO16/A14, Schiebepotenziometer, Drucktaster, Steckernetzteil sowie Patch-Kabel.

Ziele:

Wenn Sie bereits erste Erfahrungen im Bereich der Programmierung von SPS-Systemen haben, dann bietet Ihnen dieser Kurs einen Schnelleinstieg in die IEC 61131 Programmierung sowie dem Erstellen von Hochsprachen-Bausteinen mit der Software-Plattform PLCnext Engineer von Phoenix Contact. Des Weiteren wird eine Einführung in den Umgang mit dem offenen Linux System der PLCnext und Containerization (Stichwort Docker) mit podman© gegeben.

Zielgruppe:

Meister, Techniker, Ingenieure, Software- und Hardware-Entwickler, Berater, etc., die in Design, Entwicklung, Betrieb, Wartung und Management von IACS involviert sind.

Inhalte:

- Kennenlernen des PLCnext Ecosystems
- Inbetriebnahme des Starterkits
- erste Schritte mit der Engineering-Software PLCnext Engineer
- Erstellen eines Bausteines mit Visual Studio© in C# und Einbindung in IEC 61131
- Ausführen eines Debian Linux mit podman©

Die Teilnahmegebühr beinhaltet die Seminarunterlagen sowie ein PLCnext Technology Starterkit.

Schulungstermine auf Anfrage!

Die Anmeldung erfolgt online auf unserer Website
www.phoenixcontact.at

Fundamentals of Industrial Ethernet

Industrial Ethernet ist KEIN IT-Netzwerk

Das Training „Fundamentals of Industrial Ethernet“ vermittelt Grundlagenwissen zu Industriellen IP / Ethernet Netzwerken (OSI Layer 1 – 4) sowie zu Industrie Echtzeit-Netzwerken und Netzwerk-Protokollen, wie Profinet, Ethernet/IP, Modbus, u.v.m..
Dieses Training kann auch als Aufbau für das „Fundamentals of Cyber Security“ Training mit TÜV Rheinland Prüfung dienen.
Des Weiteren werden ausführlich wichtige Grundlagen zur digitalen Vernetzung und Kommunikation in der industriellen Automatisierung vermittelt.
Nach Teilnahme an diesem Training erhalten Sie von Phoenix Contact ein Zertifikat als Besuchsbestätigung.
Wir vermitteln Spezialisten aus den Bereichen der Betriebstechnik (OT) und Safety, Sicherheitstechnik (funktionale Sicherheit) Grundlagen zur Analyse von Netzwerkfehlern wie auch zum Aufbau moderner Netze in der industriellen Automatisierungs- und Steuerungstechnik.

Ziele:

Dieses Training dient generell der ausführlichen Vermittlung von wichtigem Grundlagenwissen in verschiedenen Themenbereichen der industriellen Ethernet-Vernetzung im IACS-Bereich. Es orientiert sich eng an dem geforderten Grundlagenwissen für das Training „Fundamentals of Cyber Security“ und dient daher als ideales Vorbereitungstraining für das TÜV Rheinland Cyber Security Training Program, auf dem Weg zum „CySec Specialist (TÜV Rheinland)“.

Zielgruppe:

Instandhalter, Service-Mitarbeiter, Control Software Ingenieure, Technische Entwickler, OT-Systembetreuer, Infrastruktur-Betriebspersonal, Wartungstechniker, Konstrukteure, Software-/Hardware-Entwickler, Projektleiter, Betriebsleiter, Techniker, Facharbeiter, Meister, Ingenieure,…

Inhalte:

Grundlagenwissen zu folgenden Themen wird vermittelt:

- Switch, Router, Firewall
- MAC-Adressen, IP-Adressen
- VLAN-Port, Tagged, Statisch, Dynamisch
- Gateway, Netzwerk-Maske, Broadcast
- ARP, RARP
- IPSec-VPN, OpenVPN
- PKI-Zertifikate
- Firewall-Regelwerke
- Industrie-Protokolle / ProfiNet, Ethernet/IP, ...
- Protokoll-Werkzeuge (WireShark)
- Security-Konzepte (IEC 62443)

Schulungstermine auf Anfrage!

Industrielle Feldbus-Protokolle

Wissenswertes zu Feldbus- & Netzwerk-Technologie

Ein Feldbus ist ein Bussystem, das in einer Anlage Feldgeräte wie Messfühler und Stellglieder zwecks Kommunikation mit einem Automatisierungsgerät verbindet. Dieses weiterführende Training baut auf das Training „Fundamentals of Industrial Ethernet“ oder vergleichbares Grundlagenwissen auf.
Voraussetzungen: Vorkenntnisse im Umfeld von Netzwerken, Grundlagen nach IEEE-Norm 802.3 - OSI Layer 1/2, Affinität zur Netzwerktechnik

Ziele:

Ziel dieses Trainings ist es, Teilnehmern, die bereits über Grundlagenwissen von konventionellen IP-Netzwerken verfügen, weiterführendes Wissen zu Feldbus-Protokollen zu vermitteln. Es behandelt die konkrete Umsetzung der Feldbus-Vernetzung in aktuellen (industriellen) Netzwerken. Es umfasst den Aufbau von CAN-Netzwerken bis hin zu OPC-UA-FX-Netzwerken auf Basis der TSN-Technologie.

Zielgruppe:

Instandhalter, Service-Mitarbeiter, Control Software Ingenieure, Technische Entwickler, OT-Systembetreuer, Infrastruktur-Betriebspersonal, Wartungstechniker, Konstrukteure, Software-/Hardware-Entwickler, Projektleiter, Betriebsleiter, Techniker, Facharbeiter, Meister, Ingenieure, …

Inhalte:

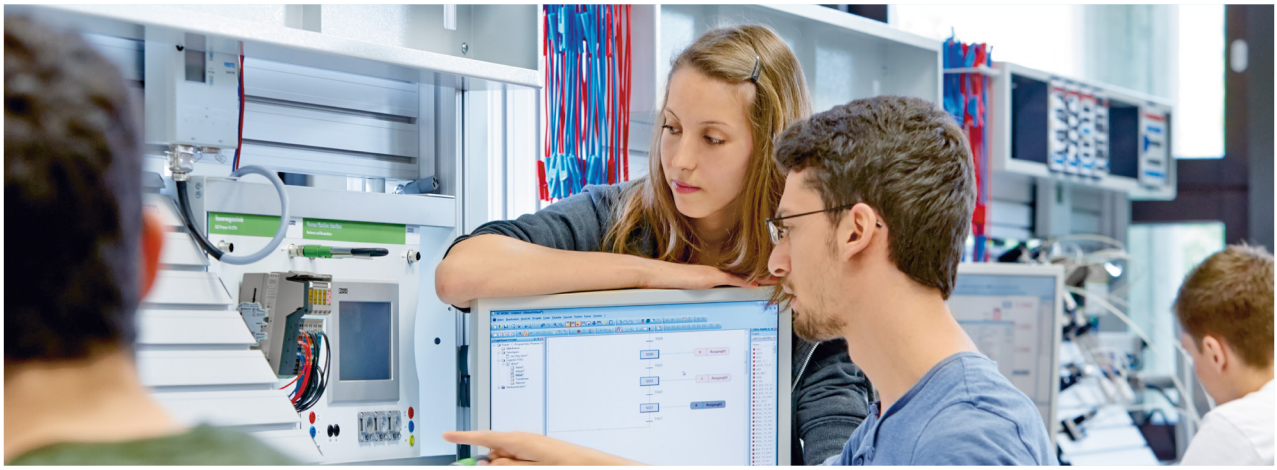
Wissen und Kenntnisse zu folgenden Themen:

- RS485, RS232, RS422, …
- CAN Bus
- TSN, APL, SPE, ...
- OPC DA, OPCHDA, OPC UA /FX, ...
- ProfiBus-DP, ProfiBus-PA, ProfiNet, ...
- EtherNet/IP, EtherCat, ControlNet, ..
- WTB, MVB, ...
- KNX, BACnet, …
- Protokoll-Werkzeuge (WireShark)
- Security-Konzepte (IEC 62443)

Schulungstermine auf Anfrage!

Schulungs- und Trainingsangebote 2025

Wir führen Schulungen und Trainings sowohl face-to-face als auch online / virtuell durch.
An unseren österreichweiten Standorten verfügen wir über eigene Trainingscenter. Die Veranstaltungen finden in Wien, Graz, und in Linz statt.



Individualtrainings mit eigener Termingestaltung können ebenfalls gebucht werden.

Die Schulungen und Trainings werden durch Mitarbeiter von Phoenix Contact und qualifizierten Partnerunternehmen abgehalten. Prüfungen erfolgen durch zertifizierte Partner wie TÜV Rheinland oder TÜV Süd.

Als Nachweis einer erfolgreichen Teilnahme wird Ihnen durch Phoenix Contact Österreich ein Teilnahmezertifikat ausgestellt.

Die Teilnahmegebühr beinhaltet die Seminarunterlagen sowie die Verpflegung am Seminartag.
Für sämtliche Bestellungen gelten unsere Geschäftsbedingungen, die Sie auf unserer Website einsehen können.

Wir sind für Sie da!

Bei Fragen zu allen Belangen unserer Schulungen und Trainings kontaktieren Sie uns bitte unter:

PHOENIX CONTACT GmbH
Tel. **+43 (0)1 / 68076**
E-Mail: **at_training@phoenixcontact.com**
Adresse: Ada-Christen-Gasse 4, 1100 Wien