



► Industrial Security

Denn auf Sicherheit kommt es an

PILZ
THE SPIRIT OF SAFETY

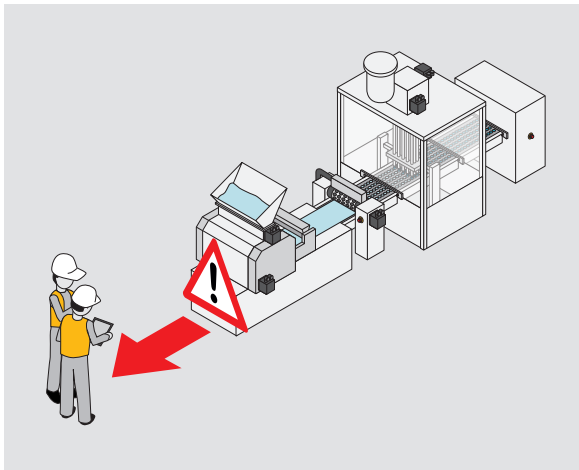


► Maschinensicherheit und Industrial Security

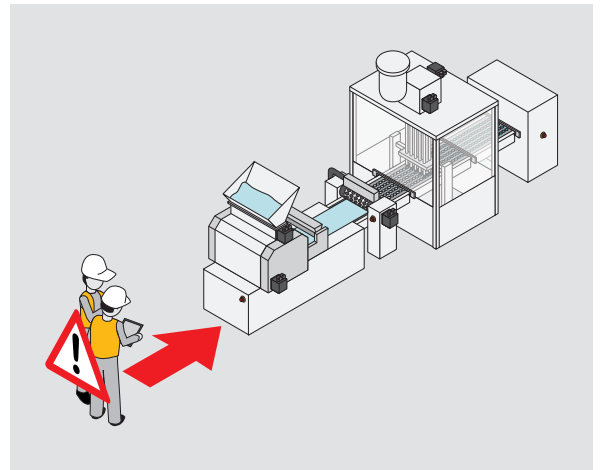
Ein wichtiger Zusammenhang mit weitreichenden Folgen

Neben der Maschinensicherheit gewinnt auch die Industrial Security zunehmend an Bedeutung. Es geht heute nicht mehr nur darum, Mitarbeiter vor Gefahr bringenden Maschinen zu schützen, sondern auch darum, Maschinen vor Manipulation, z. B. durch Cyberangriffe, zu bewahren. Durch Digitalisierung und Vernetzung entstehen neue Schwachstellen, die wirtschaftliche und körperliche Schäden verursachen können.

Besonders schützenswerte Bereiche in Maschinen und Anlagen müssen abgesichert werden, um ungewollte Zugriffe auf das Steuerungsnetzwerk zu verhindern. Sicherheitslücken können zu Unfallrisiken, Qualitätsverlust oder Produktionsausfällen führen. Beide Aspekte – Safety und Security – sind für den sicheren Umgang mit Maschinen in der Produktion notwendig.



Safety: Schutz vor Maschinen



Security: Schutz für Maschinen



Safety und Security – ein ganzheitlicher Ansatz

Dank unserer langjährigen Erfahrung in der Maschinensicherheit (Safety) wissen wir genau, wie man Safety und Industrial Security zu einem leistungsstarken, nahtlosen Konzept zusammenbringt. Ein umfassendes Verständnis der Sicherheitsfunktionen einer Maschine ist notwendig, um die richtigen Schutzmaßnahmen festzulegen. Ein vollständiger Maschinenschutz ist nur dann erreichbar, wenn beide Perspektiven harmonisch zusammenwirken. Daher sollten Safety und Security stets gemeinsam betrachtet werden.

Gut zu wissen:

Pilz prüft die Einhaltung der Konformität sowohl im Bereich Safety als auch für Security – für jede Maschine und in jeder Umgebung.



Erfahren Sie mehr
über unseren Ansatz!
www.pilz.com/safety-security

► Industrial Security – von Anfang an

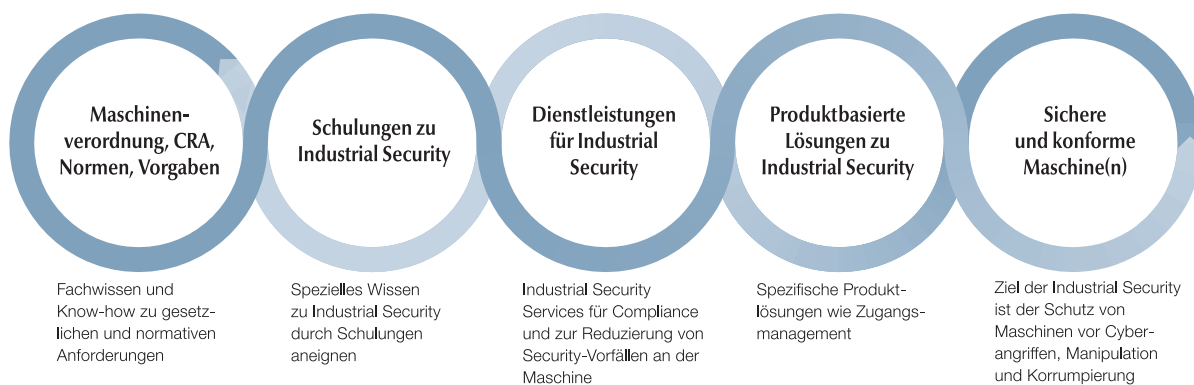
Industrial Security spielt eine entscheidende Rolle für die Gewährleistung einer zuverlässigen Maschinensicherheit sowie einer effizienten Produktion. Das frühzeitige Erkennen von Schwachstellen hilft, unbefugten Zugriff oder Manipulationen an Maschinen zu verhindern.

Um Risiken von Anfang an zu minimieren, sollte Industrial Security bereits in der Planungs- und Konstruktionsphase in das Gesamtkonzept der Maschine integriert werden.

Sie spielt zudem eine zentrale Rolle für das Bedienungspersonal und unterstützt jeden Tag einen sicheren, unterbrechungsfreien und zukunftsfähigen Anlagenbetrieb.

Schützen Sie Ihre Maschinen vor Manipulationen!

Bei Pilz unterstützen wir Sie mit maßgeschneiderten Lösungen in jeder Phase Ihrer Industrial-Security-Umsetzung – für Schutz, Zuverlässigkeit und langfristigen Erfolg.



Gut zu wissen: Industrial Security wird in Europa zur Pflicht

In Europa wurden Safety und Security durch neue Vorschriften wie die NIS-2-Richtlinie, die EU-Maschinenverordnung und den Cyber Resilience Act (CRA) eng miteinander verknüpft. Dadurch wird eine Industrial-Security-Risikobetrachtung für Unternehmen, Maschinen und Produkte mit digitalen Elementen verpflichtend. Ab 2027 dürfen Maschinen ohne Einhaltung dieser Anforderungen in der EU nicht mehr in Verkehr gebracht werden. Unter www.pilz.com/trainings finden Sie entsprechende Trainings dazu.

Weitere Informationen:



Alles, was Sie zur EU-Maschinenverordnung wissen müssen:
www.pilz.com/mr



Wichtige Informationen zu Normen und Richtlinien im Bereich Industrial Security:
www.pilz.com/security

► Grundlagen Industrial Security

Wissen schützt! Security Know-how aufbauen. Für mehr Sicherheit.



Grundlagen



Sind Sie bereit? Tauchen Sie ein in die Welt der Industrial Security:

Cyberangriffe, OT-Security und neue Anforderungen – jetzt gilt pflüg sein und vorsorgen:

Profitieren Sie von Basiswissen durch die Schulung „Grundlagen Industrial Security“ von Pilz und schützen Sie sich und Ihre Maschinen vor Cyberattacken und Manipulation auf maschineller Produktionsebene.

Digitalisierung, Vernetzung von Maschinen und digitale Elemente in der Automation fordern die Berücksichtigung von Industrial Security zum Schutz der Maschinen. Ziel dieser Schulung ist, Basiswissen zu Industrial Cyber Security aufzubauen: Grundlegende Begrifflichkeiten, Konzepte und regulatorische Anforderungen ermöglichen Teilnehmenden in anschaulichen Beispielen aus der Praxis einen Zugang zum Thema und vermitteln grundlegende Fachkenntnisse zu Cybersicherheit im Maschinenbereich.

Ihre Vorteile auf einen Blick

- schneller Einstieg in das Thema Industrial Security
- kompakter Wissensaufbau zu Terminologie und Anforderungen
- Cybersicherheit im Kontext von Maschinen- und Netzwerksicherheit verstehen
- Best Practices zum Verständnis von Cybersicherheitsrisiken in der eigenen Produktion

Diese Schulung zu Industrial Cyber Security ist daher eine optimale Grundlage zur Wissensaneignung, um die Sicherheit in eigenen industriellen Maschinen und Anlagen zu verbessern.

Weitere Informationen zu Industrial-Security-Schulungen finden Sie auf unserer Webseite unter:
www.pilz.com/security-trainings

Grundlagen Industrial Security

Details zur Schulung	Dauer 1 Tag, online oder in Präsenz Inhalte ▶ Einführung in Industrial Security - Unterschiede zwischen Operational Technology (OT) und Information Technology (IT) - Defence in Depth als Schutzprinzip - Überblick über schützenswerte Anlagen, Personen und Werte - Maschinensicherheit und Industrial Security - Überblick über verschiedene Angreifergruppen - Grundlagen Malware ▶ Grundlagen der Netzwerksicherheit - Netzwerktopologien, Gerätearten und industrielle Protokolle - Netzwerksegmentierung - Unterschied zwischen sicherer und unsicherer Kommunikation ▶ Bedrohungen, Schutzmaßnahmen und bewährte Lösungen - mögliche Bedrohungsszenarien und Best Practise - Cyber Kill Chain Modell - Allgemeine Schwachstellen und spezifische Sicherheitslücken ▶ Gesetzgebung und Normen - EU-Maschinenverordnung - Cyber Resilience Act (CRA) - NIS-2-Richtlinie - relevante Rechtsvorschriften außerhalb der EU - Überblick über Normen zu Industrial Security - Grundlagen IEC 62443 - Einführung in die EN 50742 - Einführung in die ISO 27000 ▶ Auswirkungen von Cyberangriffen auf OT-Systeme ▶ Grundlagen der Security Risikobeurteilung
Zielgruppe	Diese Schulung richtet sich an alle Mitarbeitenden von Maschinenherstellern, Integratoren und Betreibern, die nach einer Einführung in das Thema Industrial Security suchen. Sie ist insbesondere für Personen geeignet, die für die Maschinensicherheit im täglichen Betrieb verantwortlich sind. Dazu zählen folgende Personen: ▶ Konstrukteure ▶ Projektmanager ▶ Planer ▶ Systemintegratoren ▶ Sicherheitsbeauftragte ▶ Produktionsleiter bzw. Produktionsverantwortliche ▶ Verantwortliche für Umbauten und die Instandhaltung von Maschinen und Anlagen ▶ Technische Einkäufer

Jetzt anmelden –
weil Wissen
schützt!



Online-Info unter
[www.pilz.com/
security-trainings](http://www.pilz.com/security-trainings)



► CESA – Certified Expert for Security in Automation

Empowerment für Industrial Security in der Automation



TÜVNORD

Bedrohungen in Form von Cyberangriffen auf die industrielle Umgebung von Unternehmen nehmen stetig zu und stellen eine große Herausforderung für die sogenannte Industrial Security dar. Diese beschreibt den Schutz der Maschine vor Menschen, z. B. durch Cyberangriffe, Manipulation oder auch Fehlbedienung. Es wird daher zunehmend wichtiger, Maschinen und Anlagen nicht nur unter dem Gesichtspunkt von Sicherheit im Sinne von „Safety“, sondern auch im Hinblick auf „Security“ zu betrachten. Speziell auf diese Herausforderungen haben wir die Qualifizierung zum „CESA – Certified Expert for Security in Automation“ ausgerichtet.

Ihre Vorteile auf einen Blick

- Die Qualifizierung vermittelt umfangreiches Fachwissen zu normativen Anforderungen, zu Grundlagen der Risikoanalyse sowie zu technischen und organisatorischen Security-Maßnahmen im industriellen Umfeld.
- Sie lernen die korrekte Anwendung und Implementierung der Norm IEC 62443 und erfahren, welche Anforderungen Maschinen erfüllen müssen, um den Standards der modernen Industrial Security zu entsprechen.
- Wir zeigen Ihnen, wie Sie Ihre Maschinen hinsichtlich der Cybersicherheit beurteilen und optimieren können.
- Vertiefen Sie Ihre Kenntnisse über das Management von Sicherheitsrisiken, die durch die Vernetzung und Anwendung von IT und industriellen Maschinen in der Produktionshalle entstehen.
- Die kompakte Zusammenstellung und die auf Vorkenntnissen aufbauenden Inhalte ermöglichen eine Zertifizierung in nur zwei Tagen.
- Bei bestandener Prüfung erhalten Sie das weltweit anerkannte TÜV NORD-Zertifikat zum „CESA – Certified Expert for Security in Automation“ zum Nachweis Ihrer Qualifikation.

CESA – Certified Expert for Security in Automation

Details zur Schulung	Dauer 2 Tage Inhalte ▶ Einleitung - Einführung in Industrial Security ▶ Gesetzgebung - Überblick über internationale Rechtsvorschriften - EU-Maschinenverordnung - Cyber Resilience Act (CRA) - NIS-2-Richtlinie ▶ Normen - Überblick über internationale Normen zu Industrial Security - Grundlagen der IEC 62443 als zentrales Rahmenwerk für Industrial Security (IACS-Lebenszyklus, Verantwortlichkeiten/Konformität) ▶ Rollen und Verantwortlichkeiten von Betreibern, Integratoren und Hersteller im Kontext der IEC 62443 und gesetzlicher Anforderungen - Betreiberbezogene Normen für das OT-Security-Management, Steuerung und kontinuierliches Risikomanagement: - ISO 27000 - IEC 62443-2-1, -2-2 - Herstellerbezogene Normen für Produktentwicklung gemäß Industrial Security, technische Security-Anforderungen und Schutz vor Manipulation: - IEC 62443-3-3, -4-1, -4-2 - EN 50742 - Integratorbezogene Normen: Security-Programm-Anforderungen und Methodik für Dienstleister: - IEC 62443-2-4, -6-1 ▶ Risikobeurteilung (detaillierte Überprüfung) - Anforderungen an die Security-Risikobeurteilung gemäß den gesetzlichen Vorschriften (NIS 2, CRA, Maschinenverordnung) - Verschiedene Arten von Security-Risikobeurteilungen gemäß den Normen - Security-Risikobeurteilung auf der Grundlage von IEC 62443-3-2
Zielgruppen	Die Qualifizierung zum CESA richtet sich insbesondere an Hersteller, Integratoren und Anwender industrieller Automatisierungssysteme sowie an: ▶ Anlageningenieure ▶ Maschinenbauingenieure ▶ Konstrukteure ▶ Projekt ingenieure ▶ Systemintegratoren ▶ Produktionsleiter/Produktionsverantwortliche ▶ Verantwortliche für die Modernisierung und Wartung von Anlagen und Maschinen ▶ Entwicklungsleiter ▶ Chief Information Security Officers (CISO)

Melden Sie sich jetzt an und werden Sie zum Certified Expert for Security in Automation!



Online-Info unter www.pilz.com/cesa



Ihr besonderer Vorteil: CESA wurde in Zusammenarbeit mit dem TÜV NORD konzipiert

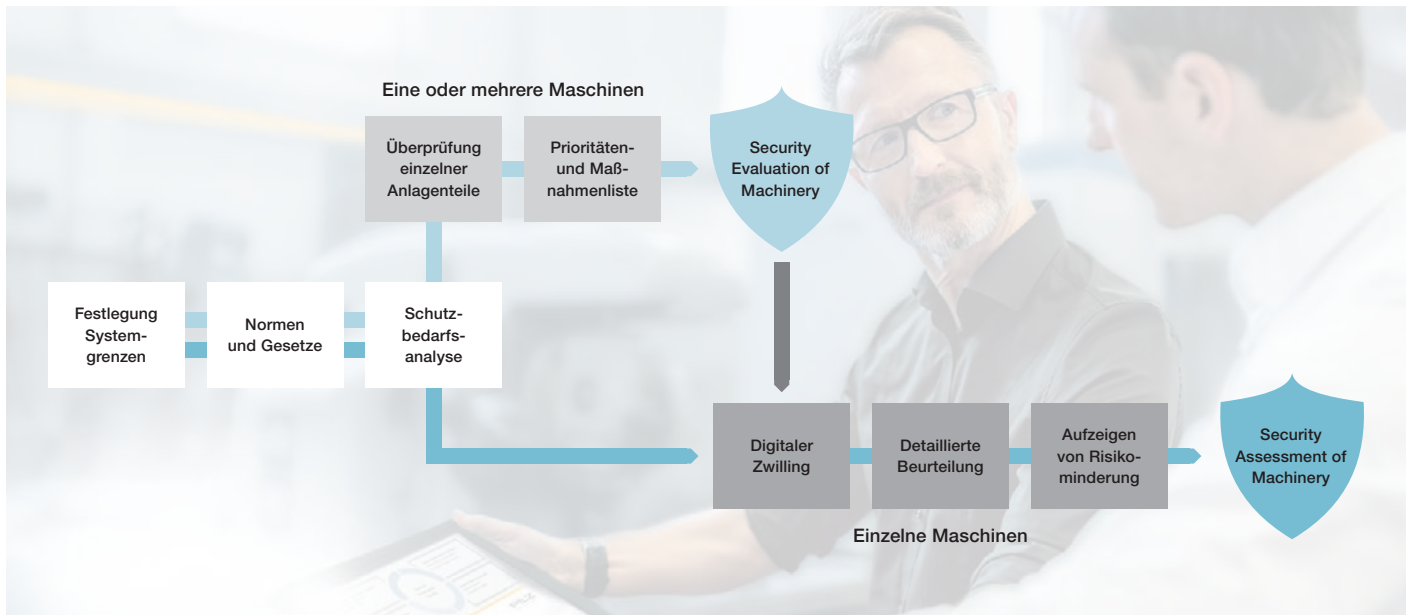
Nach dem erfolgreichen Abschluss der Prüfung erhalten Sie das weltweit anerkannte Zertifikat, das vom TÜV NORD als Nachweis Ihrer persönlichen Zertifizierung ausgestellt wird.

- ▶ Die Gültigkeit des Zertifikats ist auf vier Jahre befristet und kann durch die Teilnahme an einer Rezertifizierungsschulung um weitere vier Jahre verlängert werden.
- ▶ Die Zertifizierung erlaubt es Ihnen, den Titel „CESA – Certified Expert for Security in Automation“ zu führen.

► Industrial Security Services

Risiken kennen. Security stärken. Schützen, was wichtig ist.

Ihre Maschinen. Unsere Kompetenz. Ihr Weg zu Industrial Security an Maschinen.



Pilz bietet spezielle Dienstleistungen zu Industrial Security in verschiedenen technischen Stufen an, die Herstellern und Endanwendern helfen, Bedrohungen und Schwachstellen zu erkennen, zu priorisieren und zu bewerten – von einzelnen Maschinen bis zur gesamten Produktionsanlage. Hauptziel ist es, die Maschinensicherheit zu schützen und alle relevanten Vorschriften zu Industrial Security zuverlässig einzuhalten.

Jetzt mehr erfahren!



Online-Info unter
www.pilz.com/iscs

Ihre Vorteile auf einen Blick

- Schutz der Maschinensicherheit vor Korruption und Manipulation
- höhere Effizienz durch besseren Schutz vor Cyberangriffen und produktionsunterbrechenden Vorfällen
- Wahrung der Integrität des Produktes und der Vertraulichkeit von Daten
- Erfüllung von gesetzlichen und normativen Industrial-Security-Anforderungen
- Unterstützung für die verpflichtende Einhaltung der EU-Konformitätserklärung

► Security Evaluation of Machinery und Security Assessment of Machinery

Zwei Dienstleistungen. Einzelne oder als leistungsstarkes Duo.



Security Evaluation of Machinery

Typische Anwendungsszenarien:

Übersicht über den Security-Status bestehender Maschinen oder beim Kauf neuer Maschinen

- Bewertung des Sicherheitsstatus der Maschine(n) und Identifikation bestehender Schwachstellen
- Ermittlung kritischer Komponenten und Bewertung des damit verbundenen Sicherheitsrisikos basierend auf Auswirkung und Eintrittswahrscheinlichkeit
- Aufzeigen wesentlicher Sicherheitslücken inklusive empfohlener Maßnahmen zur Risikominderung
- kompakter, umsetzbarer Bericht zum aktuellen Security-Status
- Einschätzung des Handlungsbedarfs: Reichen erste Maßnahmen aus oder ist eine vertiefte Security-Risikobeurteilung notwendig?

Security Assessment of Machinery

Typische Anwendungsszenarien:

Stark vernetzte Maschinen mit entscheidenden Auswirkungen auf Sicherheit und Geschäftsfähigkeit

- tiefgehende, strukturierte Security-Analyse nach IEC 62443
- effizienter Prozess durch Nutzung vorhandener Evaluationsdaten (sofern vorhanden)
- detaillierte Untersuchung der Maschine zur Identifikation von Schwachstellen und Bewertung ihrer Auswirkungen
- präzise Ableitung gezielter Maßnahmen zur Risikominderung durch detaillierte Aufschlüsselung
- Bereitstellung konkreter Strategien zur Risikominderung, um Maschinen vor Cybermanipulation zu schützen und die Industrial Security zu stärken

► Pilz Sicherheitslösungen

Entwickeln Sie passende Sicherheitsstrategien für Ihre Maschinen mit Pilz. Unsere erfahrenen Sicherheitsexperten unterstützen Sie dabei, die Sicherheit Ihrer Maschinen zu optimieren und die Verfügbarkeit Ihrer Anlagen zu erhöhen.



Sicherheit für jede Phase des Maschinenlebenszyklus

- Consulting- und Engineering-Dienstleistungen für Design, Betrieb und Optimierung von Maschinen
- Sensorik und Steuerungstechnik – die sichere Komplettlösung für Ihre Maschinen
- Pilz Trainings für Know-how in Ihrem Unternehmen
- MYZEL Lifecycle Platform für das Management Ihrer Personen- und Maschinendaten



Sprechen Sie noch heute
mit Ihrem Pilz Sicherheitsexperten!

www.pilz.com/safety-security

► Identification and Access Management – I.A.M.

Von der Authentisierung des Anwenders über die Auswahl des Betriebsmodus bis hin zu Daten- und Netzwerksicherheit sowie Zugriffsverwaltung. Wir bieten Safety und Security in einem System.



Unsere Safety- und Security-Produktlösungen

Entdecken Sie unsere integrierten Safety- und Security-Lösungen aus dem Portfolio Identification and Access Management – I.A.M.! Mit maßgeschneiderten Angeboten für Mitarbeiterschutz, Haftungsschutz, maximale Produktivität und den Schutz Ihrer Daten.

Erfahre mehr zu I.A.M.



Online-Info unter www.pilz.com/iam

