Whitepaper

Fernzugriff auf industrielle Automatisierungssysteme

Best-Practice-Empfehlungen

Erfahren Sie mehr über folgende Themen

- Übersicht zum Thema Fernzugriff
- Häufige Security-Fallstricke
- Praktische Herausforderungen
- Best-Practice-Empfehlungen
- Wesentliche Vorteile
- Fernzugriff und Cyber-Security-Lösungen

PHOENIX CONTACT

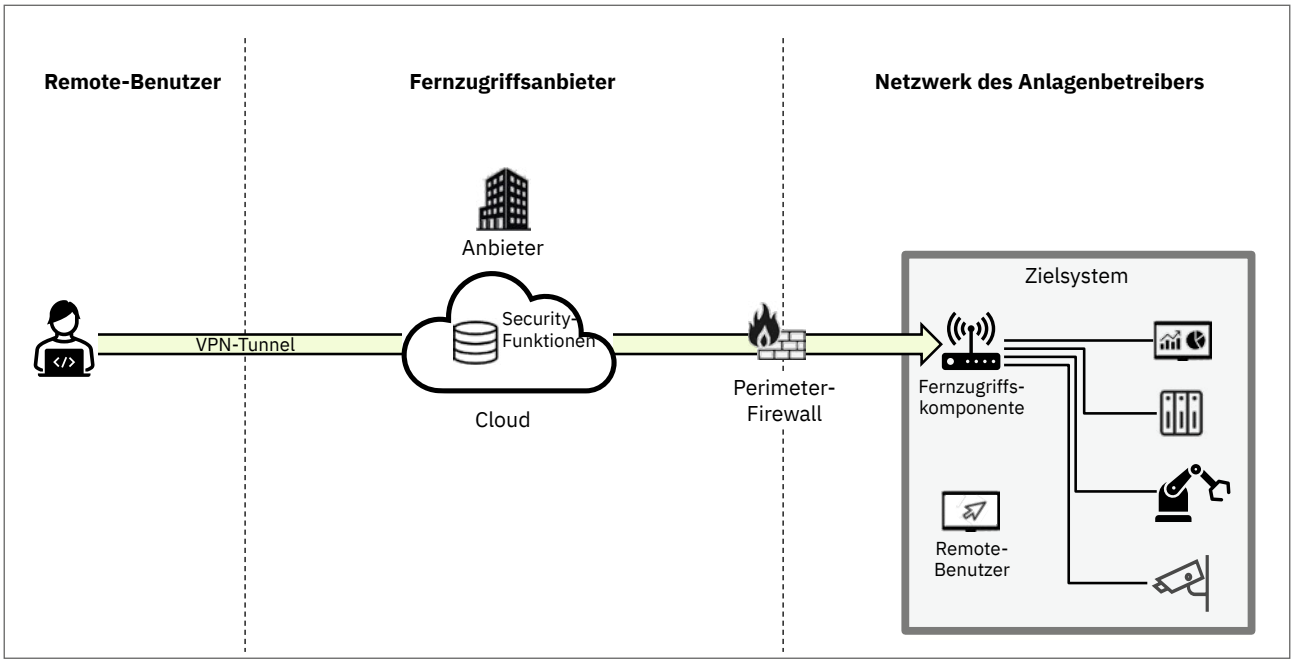
Einführung

Fernzugriff ist ein zentraler Bestandteil industrieller Automatisierungssysteme (ICS). Er ermöglicht Bedienenden, Ingenieurinnen, Ingenieuren, Technikerinnen und Technikern die Überwachung, Fehlerbehebung und Verwaltung von Systemen aus der Ferne. Während der Fernzugriff Komfort bietet und von Anlagenbetreibern, Maschinenbauern und Dienstleistern flächendeckend eingeführt wurde, muss er ordnungsgemäß integriert und gesichert sein, um unautorisierten Zugriff und Cyber-Bedrohungen zu verhindern. Dieses Whitepaper beleuchtet gängige Security-Fallstricke und praktische Herausforderungen. Gleichzeitig gibt es Best-Practice-Empfehlungen, um die **Security**, **Flexibilität**, **Konsistenz** und **Verfügbarkeit** des Fernzugriffs in ICS-Umgebungen zu verbessern.

Übersicht zum Thema Fernzugriff

Der Fernzugriff erfolgt typischerweise per VPN-Technologie (oder ähnliche Methoden), um einen sicheren Tunnel zwischen einem entfernten Benutzer und einem Zielsystem zu erstellen, der die Kommunikation so ermöglicht, als wären beide im selben Netzwerk. Der Aufbau der Verbindung erfolgt über eine Fernzugriffskomponente – entweder als Hardware (z. B. IoT-Gateway oder Firewall) oder als Software auf einer Steuerung, einem Edge-Computer, einer Workstation oder einem HMI. Ein gängiger Ansatz ist der Remote-Desktop. Er ermöglicht Remote-Benutzern, mit dem System zu interagieren, als säßen sie direkt davor.

Fernzugriffstunnel können mit einer anbieterseitig verwalteten Cloud oder ohne sie aufgebaut werden. Cloudbasierte Lösungen sind inzwischen Mainstream, da sie komplexe IT-Konfigurationen vereinfachen und zusätzliche Security-Funktionen bieten. Die Cloud-Nutzung bringt jedoch besondere Security-Aspekte mit sich, die berücksichtigt werden müssen.



Häufige Security-Risiken

1. **Fehlende Segmentierung**
   Ein häufiger Fehler besteht darin, Fernzugriffskomponenten direkt mit dem ICS zu verbinden, ohne sie ausreichend zu isolieren. Diese Komponenten kommunizieren im Hintergrund mit externen Anbietern oder dem Internet, was die Anfälligkeit für Cyber-Bedrohungen erhöht, wenn keine ordnungsgemäße Segmentierung erfolgt.

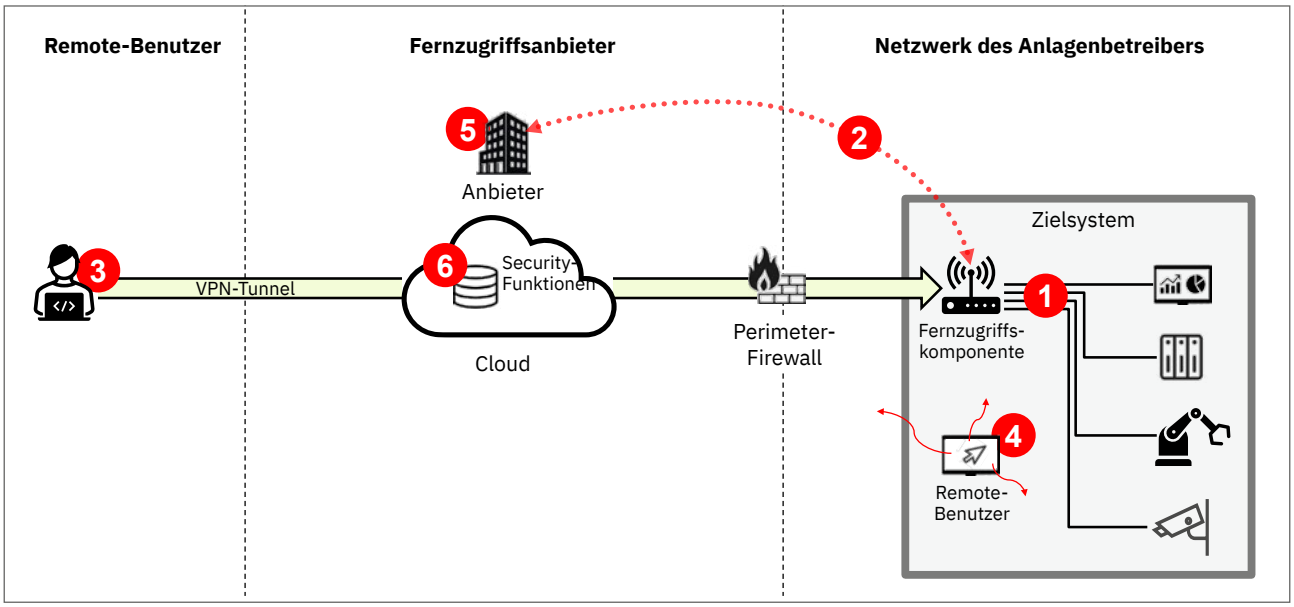
2. **Ungesicherte Backdoors**
   Fernzugriffskomponenten mit direkter Internetverbindung – insbesondere über Mobilfunknetze – können Perimeter-Firewalls umgehen und versteckte Einstiegspunkte schaffen. In einer Anlage können mehrere solcher Backdoors existieren, wenn Maschinenbauer eigene Fernzugriffslösungen einbauen.

3. **Trust-by-default**
   Beim Aufbau von Fernzugriffstunneln sind ein Remote-Benutzer und das Zielsystem in dasselbe Netzwerk eingebunden und vertrauen sich standardmäßig. Das System gewährt oft weitreichenden, uneingeschränkten Zugang und erlaubt den Remote-Benutzern die Navigation im System mit wenigen oder keinen Einschränkungen.

4. **Übermäßiger Zugang**
   Mangels einer granularen Zugriffskontrolle erhalten Remote-Benutzer häufig mehr Rechte als nötig. Insbesondere kann eine Remote-Desktop-Sitzung unbeabsichtigt den Zugriff auf größere Teile des Netzwerks oder sogar das Internet ermöglichen.

5. **Übermäßiges Vertrauen in Cloud-Security**
   Obwohl cloudbasierte Fernzugriffslösungen integrierte Security-Funktionen bieten, liegt die Kontrolle über die Sicherheit beim Anbieter. Dies macht das System anfällig für cloudspezifische Bedrohungen und Angriffe auf die Lieferkette.

6. **Generische statt maßgeschneiderte Security**
   Ein weiterer Nachteil der cloudbasierten Security ist die mangelnde Anpassungsfähigkeit an unterschiedliche Systeme mit individuellen Anforderungen. Oftmals sind die in der Cloud konfigurierten Security-Regeln generisch und nicht auf das Zielsystem abgestimmt.



Praktische Herausforderungen

ICS-Umgebungen zeichnen sich durch lange Lebenszyklen und viele Beteiligte aus – darunter Anlagenbetreiber (Asset Owner), Maschinenbauer, Dienstleister und weitere. Neben technischen Aspekten gibt es reale Herausforderungen:

Diversität
Ein Anlagenbetreiber hat womöglich mehrere Werke, jeweils mit unterschiedlichen Maschinen verschiedener Lieferanten. Ebenso produzieren Maschinenbauer eine Reihe von Maschinentypen mit unterschiedlichen Konfigurationen. Das Security-Management über diese Vielfalt hinweg ist komplex.

Flexibilität
Fernzugriff ist ein integraler Bestandteil von ICS und unterliegt Veränderungen. Maschinenbauunternehmen bevorzugen möglicherweise eine Plattform, während Anlagenbetreiber eine andere fordern. Technologische Veränderungen, Budgetrestriktionen oder Lieferantenwechsel können ebenfalls zu Änderungen führen. Häufig sind die Nutzenden jedoch an die Cloud-Plattformen ihrer Anbieter gebunden, was den Wechsel zwischen den Plattformen erschwert.

Konsistenz
Security-Regeln und -richtlinien konsistent zu halten und dabei Vielfalt und Flexibilität zu ermöglichen, ist eine Herausforderung. Wie können z. B. Maschinenbauunternehmen dieselben Zugriffskontrollrichtlinien, dieselbe Benutzerkontenverwaltung und dieselbe Rechtekontrolle einsetzen – unabhängig davon, welche Fernzugriffslösung Anlagenbetreiber verlangen?

Verfügbarkeit
Von ICS-Systemen wird erwartet, dass sie über längere Zeiträume laufen. Ausfälle von Fernzugriffs-Cloud-Diensten, Cyber-Angriffe oder Anbieterabkündigungen verursachen Stillstandszeiten und haben erhebliche Auswirkungen auf das Geschäft. Die Sicherstellung der Widerstandsfähigkeit der Systeme ist sowohl aus technischer als auch aus betrieblicher Sicht geboten.

Best-Practice-Empfehlungen

1. **Segmentieren Sie Ihr System in Zonen**
   Folgen Sie dem Purdue-Modell und der Norm IEC 62443 und segmentieren Sie Ihr System in Zonen und Conduits. Dieser Ansatz begrenzt die Datenströme, unterbindet laterale Datenbewegungen und schafft die Basis für sicheren Fernzugriff.

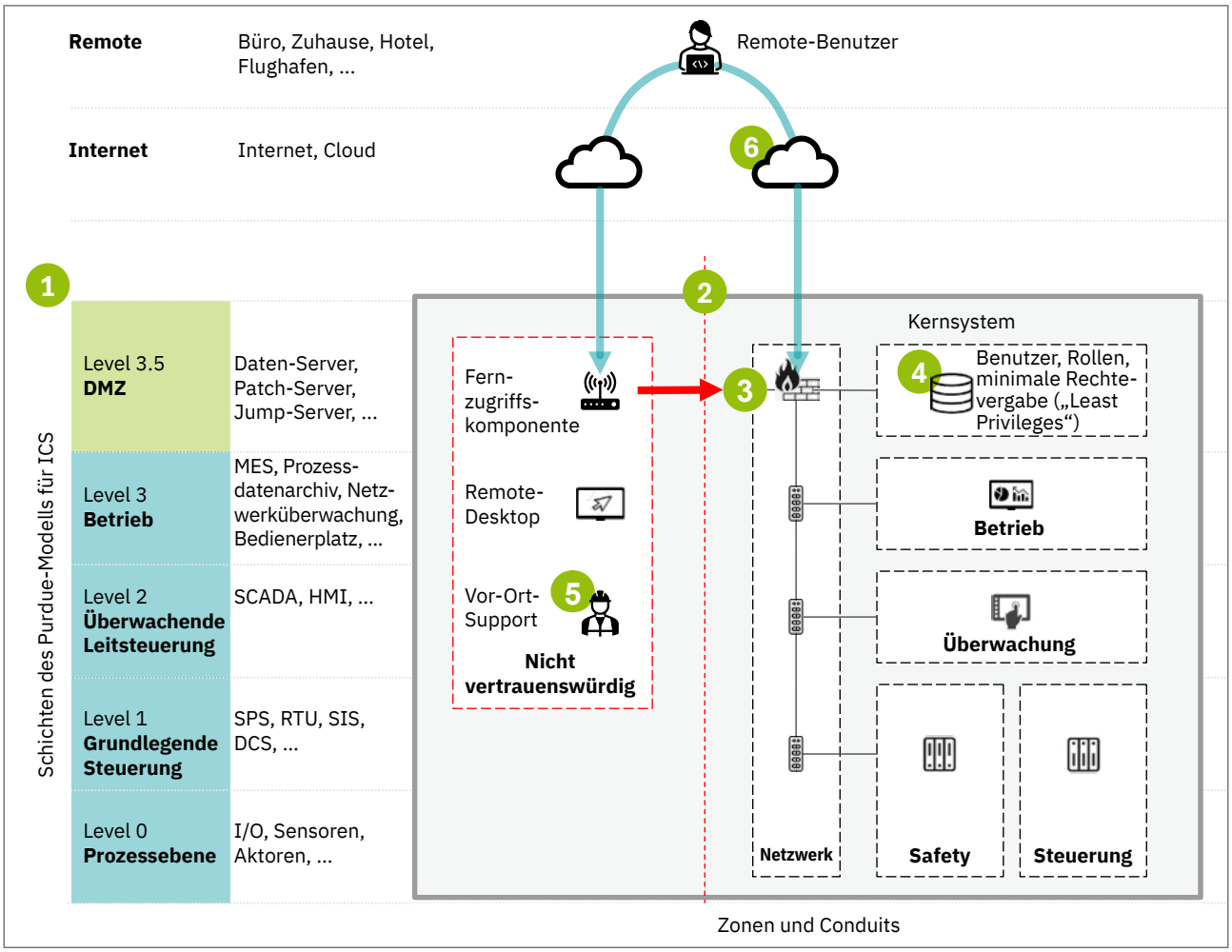
2. **Trennen Sie den Fernzugriff von Ihrem System**
   Fernzugriffskomponenten übertragen sowohl Nutzerdaten als auch Hintergrundverkehr an den Anbieter und ins Internet. Entscheidend ist, sie als nicht vertrauenswürdig zu behandeln und vom Kernsystem zu trennen. Die Isolation reduziert die Angriffsfläche gegenüber externen Bedrohungen.

3. **Minimieren Sie die Angriffsfläche für den Fernzugriff**
   Wenden Sie das Prinzip der minimalen Angriffsfläche an. Begrenzen Sie den Fernzugriff. Idealerweise sollte der Fernzugriff durch einen einzigen, ausgewiesenen Port gelenkt werden. Dies vereinfacht die Security-Zugriffskontrolle, reduziert die Komplexität und verbessert die Abwehr von Bedrohungen.

4. **Implementieren Sie systembasierte Security**
   Statt sich ausschließlich auf cloudbasierte Security-Funktionen zu verlassen, sollte die Zugriffskontrolle direkt im System am definierten Port integriert werden. So wird eine durchgängige Security über verschiedene Einsatzszenarien hinweg gewährleistet – unabhängig von der Fernzugriffsplattform. Realisieren Sie Prinzipien wie „deny-by-default, allow by exception“, „rollenbasierte Zugriffskontrolle“ und „Least Privilege“. Ein verbundener Remote-Benutzer sollte blockiert bleiben, bis er gemäß systemeigener Regeln authentifiziert und autorisiert wurde – nicht nach generischen Cloud-Regeln.

5. **Vereinheitlichen Sie die Oberfläche für Remote- und Vor-Ort-Zugriff**
   Remote- und lokale Benutzer übernehmen oft ähnliche Funktionen wie Überwachung und Wartung. Vereinheitlichen Sie die Zugriffspunkte und Security-Regeln für beide. Reduzieren Sie dadurch die Komplexität und interne Bedrohungsvektoren.

6. **Integrieren Sie Redundanz durch eine zweite Quelle**
   Integrieren Sie eine sekundäre Fernzugriffslösung von einem alternativen Anbieter, um die Verfügbarkeit bei Störungen des Diensts aufrechtzuerhalten. Um doppelten Aufwand oder eine inkonsistente Konfiguration zu vermeiden, wenden Sie die gleichen Security-Regeln sowohl für die primären als auch für sekundäre Pfade an.



Wesentliche Vorteile

Security

- Orientiert sich am Purdue-Modell und an den Gestaltungsprinzipien der Norm IEC 62443
- Erzeugt sichere Zonen und Conduits, um seitliche Bewegungen zu verhindern
- Trennt nicht vertrauenswürdigen Fernzugriff von Kernsystemen
- Minimiert die Angriffsfläche für Fernzugriffe
- Ermöglicht systembasierte Security, statt cloudbasierte Security
- Ermöglicht an das System angepasste Security anstatt generischer Security in der Cloud
- Setzt ein Zero-Trust-Konzept um, bei dem standardmäßig verweigert und nur per Ausnahme zugelassen wird
- Integriert rollenbasierte Zugriffskontrolle und „Least Privileges“-Prinzipien

Flexibilität

- Vermeidet Anbieterabhängigkeit, da keine Bindung an einen bestimmten Anbieter von Fernzugriffsdiensten besteht
- Passt sich an jede Fernzugriffsplattform an
- Vereinfacht den Wechsel zwischen Plattformen und Anbietern

Konsistenz

- Gewährleistet durchgängige Security-Regeln unabhängig davon, welche Fernzugriffsplattform genutzt wird
- Standardisierte Security-Regeln für Remote- und Vor-Ort-Benutzer
- Einheitliche Zugriffsregeln für primäre und redundante Fernzugriffspfade

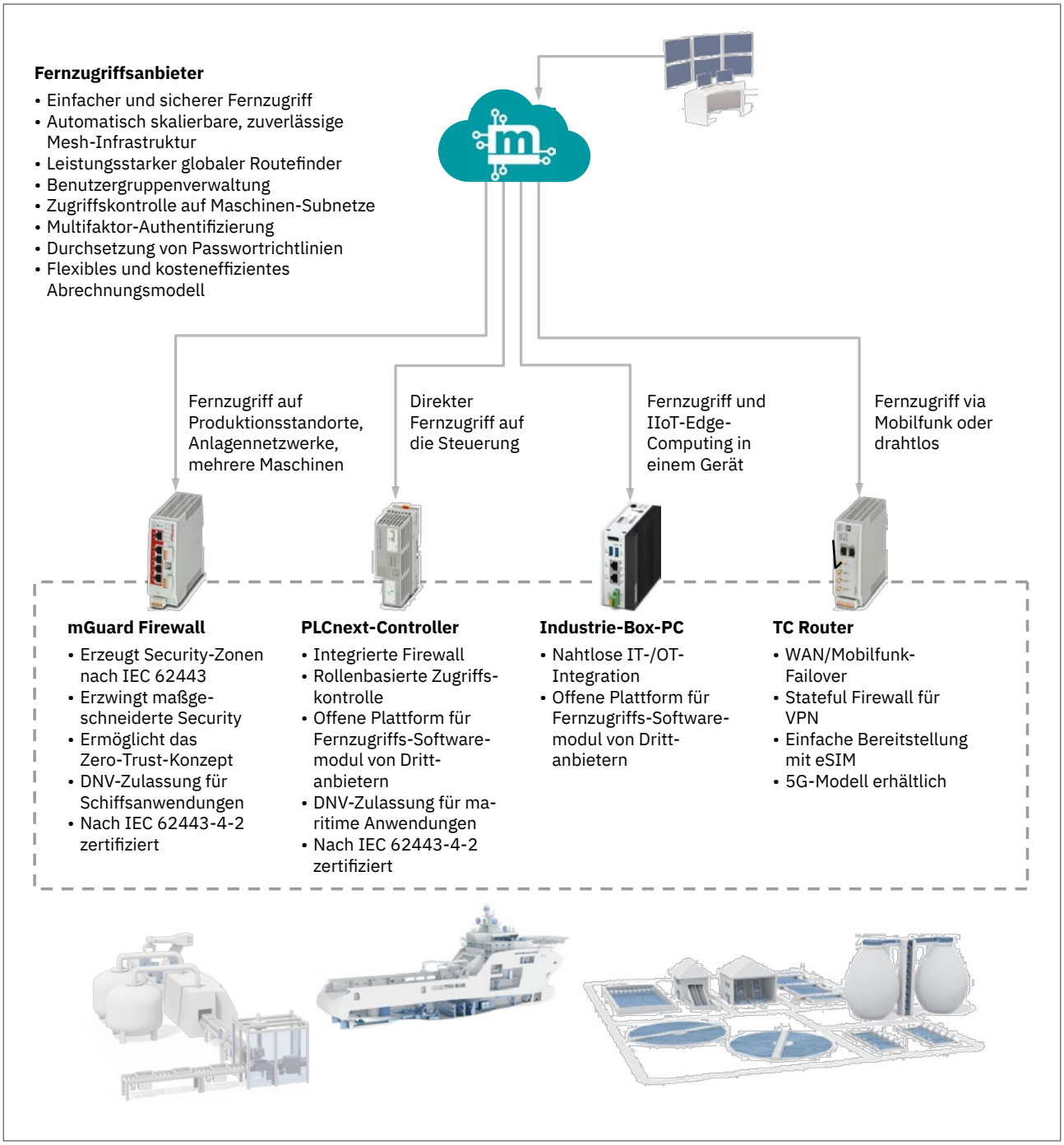
Verfügbarkeit

- Erhöht die Resilienz des Systems durch einen redundanten Fernzugriff
- Mindert Risiken durch Cloud-Ausfälle und Anbieterabkündigungen

Fernzugriffs- und Cyber-Security-Lösungen von Phoenix Contact

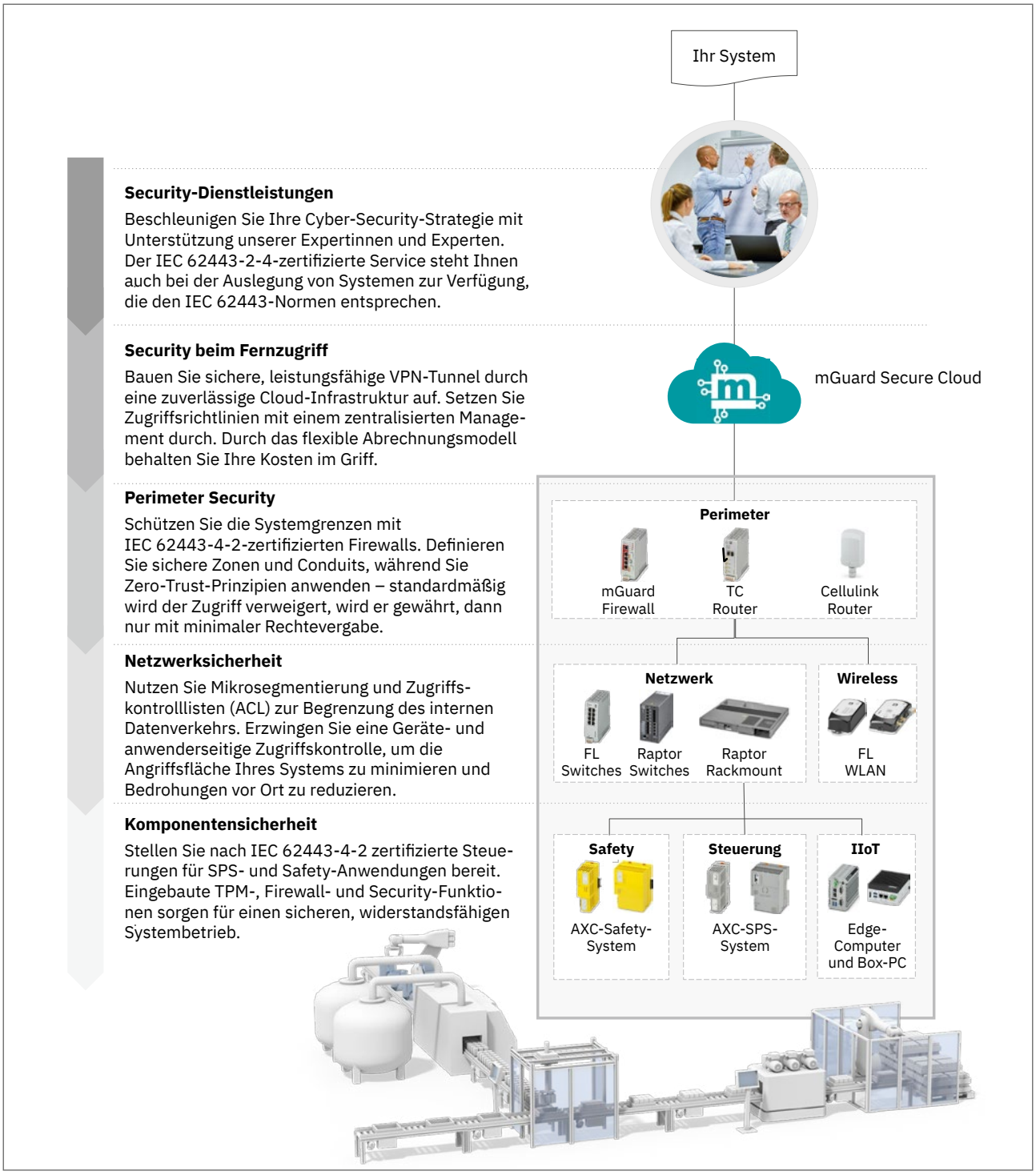
mGuard Secure Cloud

Der Cloud-Service von Phoenix Contact ermöglicht einen einfachen und sicheren Fernzugriff – von einem einfachen VPN-Client bis hin zu umfangreichen Systemnetzwerken.



Defense-in-Depth für Remote Access Systeme

Phoenix Contact setzt seit 2017 die IEC 62443-Standards um und bietet Cyber-Security-Dienstleistungen, Lösungen und Produkte, um ein mehrschichtiges Security-Konzept („Defense-in-Depth“) zu realisieren – vom Fernzugriff über den Perimeter-Schutz bis hin zur Netzwerk- und Komponentensicherheit. Damit soll der sichere und robuste Betrieb Ihrer industriellen Steuerungssysteme sichergestellt werden.



Kontakt

Wir empfehlen, mit unserer Cyber-Security-Einschätzung und Beratungsdienstleistung zu beginnen. Bewerten Sie mit unserem Spezialistenteam für Netzwerk- und Cyber Security das Risikoprofil Ihres Systems. Erhalten Sie kompetente Beratung zu IEC 62443, Netzwerksegmentierung, modularen Architekturen und mehrschichtiger Bedrohungsabwehr sowie sicherem Fernzugriff.

Sprechen Sie uns hierzu gern an.

JJ Sun

Spezialist für Netzwerk- und Cyber Security

Im Rahmen des Cyber-Security-Schulungsprogramms des TÜV Rheinland zertifizierter Spezialist mit 20 Jahren Erfahrung mit industriellen Netzwerken.

jsun@phoenixcontact.com

Warum Phoenix Contact

Cyber Security ist ein Prozess und Phoenix Contact ist Ihr vertrauenswürdiger Partner mit konsequenter Umsetzung von NIS2, CRA, IEC 62443. Wir entwickeln Technologien und fertigen Security-Komponenten. Mit diesen schützen wir unsere weltweiten Produktionsstandorte – und auf Wunsch auch Ihre.

Ihr Nutzen

Cyber Security erfordert einen ganzheitlichen Ansatz. Unsere 360°-Security reicht vom Produkt über Lösungen bis hin zu Dienstleistungen und bietet eine effiziente Möglichkeit, Ihr System in den Bereichen Netzwerk, Safety, Automatisierung und IIoT zu schützen – alles aus einer Hand.

phoenixcontact.com

15.08.2025/00

3012721056