Cybersecurity for Industry Operational Guidelines

Version 2.2

SIEMENS

Operational Guidelines

Ziel der Operational Guidelines ist es, Empfehlungen zu grundsätzlichen Security-Maßnahmen für einen gesicherten Maschinen- und Anlagenbetrieb im industriellen Umfeld zu geben.

Darauf basierend können Maschinen- und Anlagenbauer ihre Systeme entsprechend bewerten und bei Bedarf anpassen.

SIEMENS

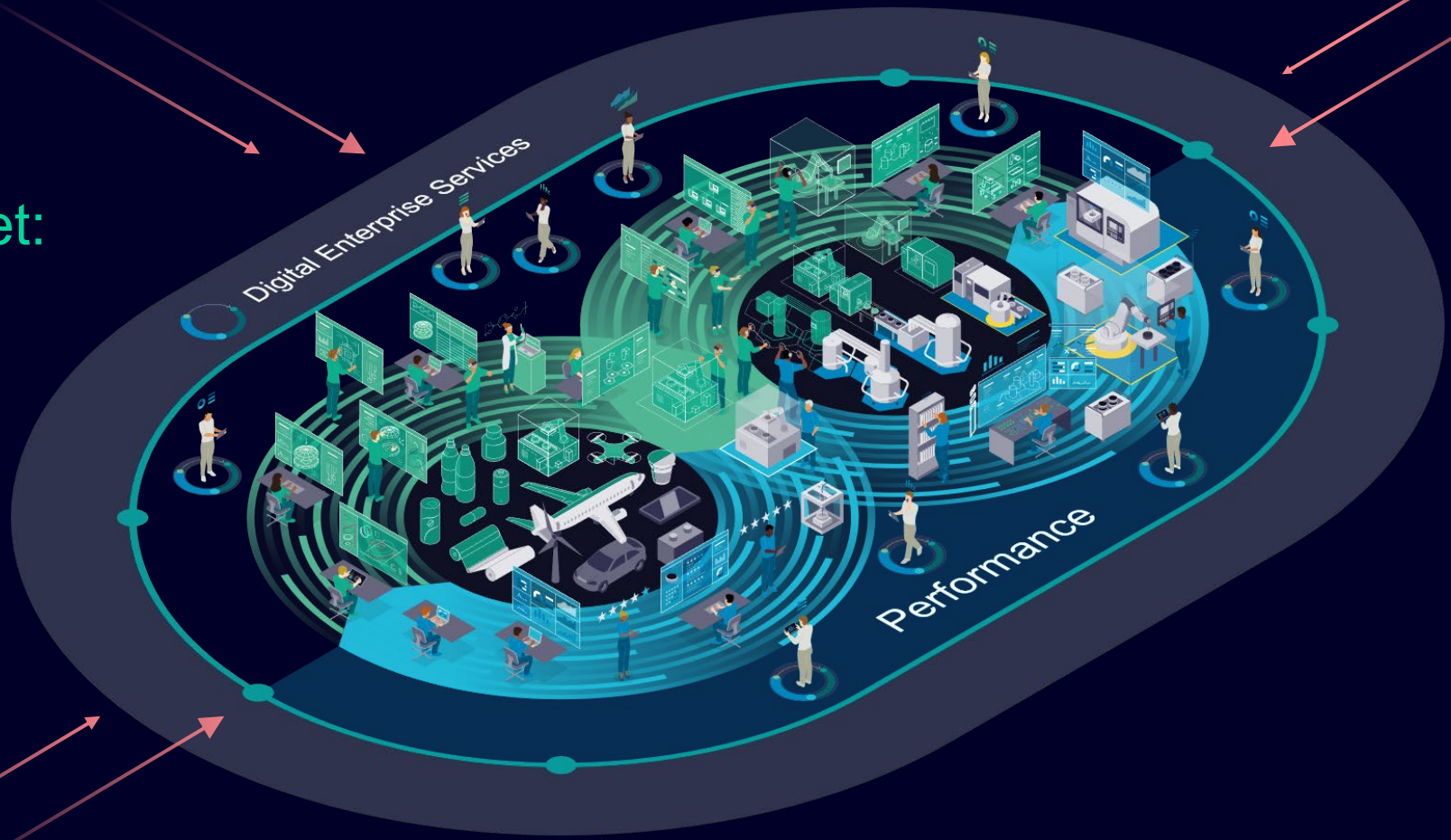
Übersicht

SIEMENS

Maschinen & Automatisierungssysteme sind Teil des IoT
Das bedeutet OT / IT Integration in allen Ebenen

OT / IT Konvergenz bedeutet:

- **Mehr Vernetzung**
- **Mehr Daten**
- **Neue Cyber-Risiken!**



SIEMENS

Cyber-Risiken in der Industrie-Automatisierung

Informationstechnologien kommen in der Industrie-Automatisierung zum Einsatz

- Horizontale und vertikale Integration

- Offene Standards
- PC-basierte Systeme

Dringender Handlungsbedarf durch wachsende Sicherheitsbedrohung

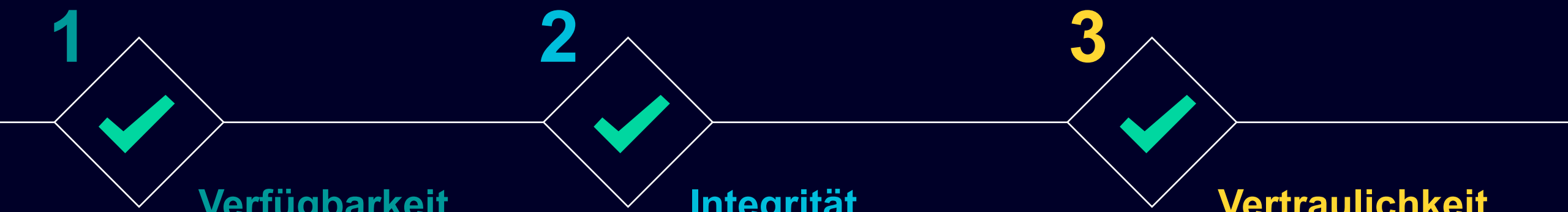
- Verlust geistigen Eigentums, von Rezepturen, etc.
- Anlagenstillstand, z. B. durch Viren oder Malware
- Sabotage in der Produktionsanlage
- Manipulation von Daten oder Anwendungssoftware
- Unbefugte Nutzung von Systemfunktionen
- Verbindliche Einhaltung von Standards und Vorschriften

➔ **Etablierung von Security-Maßnahmen erforderlich – angepasst an das jeweilige Risiko**

SIEMENS

Schutzziele und Mehrwertaspekte

Produktivität umfassend schützen



Verfügbarkeit

Erhöhte Anlagenverfügbarkeit durch Reduzierung von Beeinträchtigungen, die durch Angriffe oder Malware verursacht werden.

Integrität

Erhöhter Schutz der System- und Datenintegrität zur Vermeidung von Fehlfunktionen oder Produktionsfehlern.

Vertraulichkeit

Erhöhter Schutz vertraulicher Daten und Informationen sowie des geistigen Eigentums.

Verfügbarkeit, Integrität und Vertraulichkeit absichern – auf vertretbares Risiko.

SIEMENS

Industrial Cybersecurity nur im Zusammenspiel von Anlagenbetreibern, Systemintegratoren und Produktherstellern

IEC 62443 – Standard für Industrial Cybersecurity

Rollen

Produkthersteller:
Produkte (Komponenten, Systeme) mit integrierten und konfigurierbaren Security-Features

Systemintegrator:
Sichere Konfiguration und Einbindung des Produkts in das Gesamtsystem

Anlagenbetreiber:
Security-Management, inkl. Pflege und Anpassung der Security-Funktionen entsprechend veränderter Rahmenbedingungen
(z. B. neu erkannte Schwachstellen, Änderungen von Netztopologie)

SIEMENS

Nur ein ganzheitliches Sicherheitskonzept kann effektiven Schutz vor Cyber-Bedrohungen bieten

Sicherheitsrisiken zwingen zum Handeln

Anlagensicherheit

- Physischer Zugangsschutz
- Security Richtlinien
- Security Monitoring

Netzwerksicherheit

- Zellenschutz, Perimeter Netzwerk und vertrauenswürdige Zonen
- Firewalls und VPN

Systemintegrität

- Systemhärtung
- Patch-Management
- Authentifizierung und Zugriffsschutz

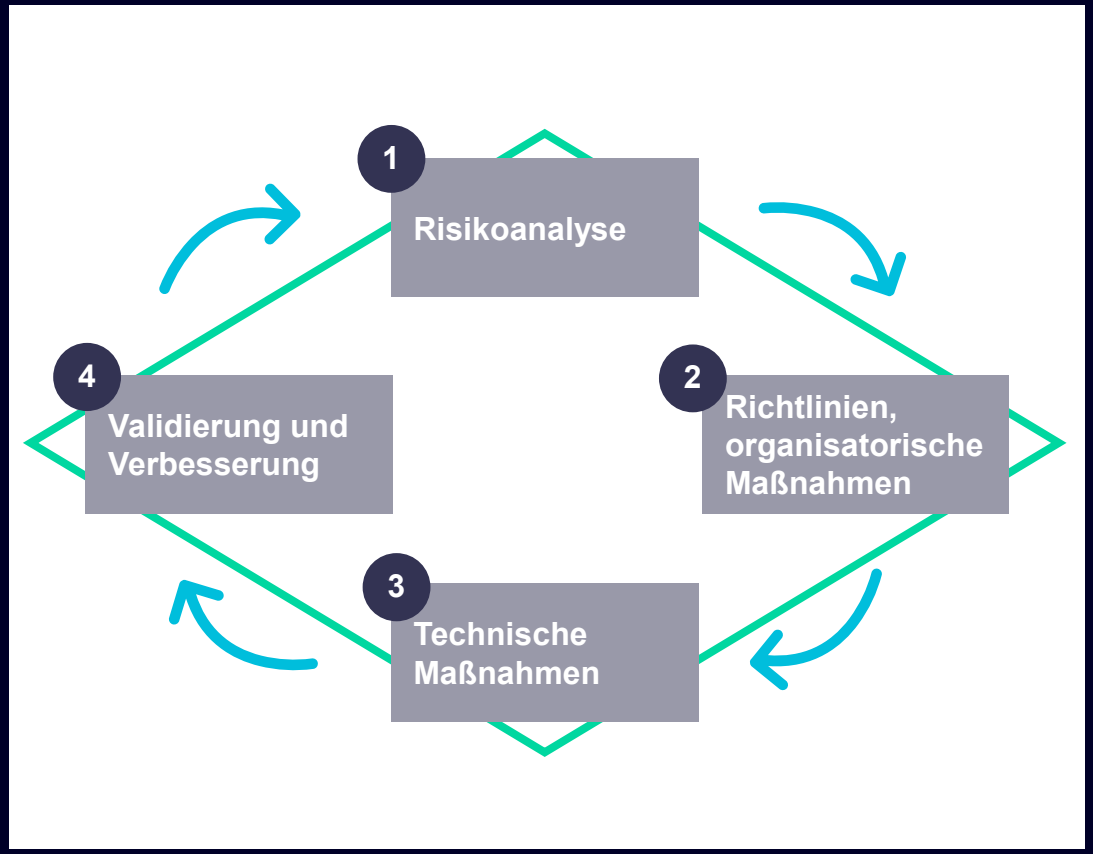
Durch den Einsatz mehrerer Security Layer, die die gesamte Anlage, das Netzwerk und die Automatisierungssysteme schützen.

SIEMENS

Security-Maßnahmen müssen auf die individuelle Anlage ausgerichtet und kontinuierlich überprüft werden

Security-Management-Prozess

- Security-Management bildet einen **wesentlichen Bestandteil jedes Industrial Security-Konzeptes**.
- Definition der Security-Maßnahmen **passend zur individuellen Anlage** in Abhängigkeit von identifizierten Gefahren und Risiken.
- Erreichen und Beibehalten des notwendigen Security-Levels erfordert einen **kontinuierlichen Security-Managementprozess**:
  - Risikoanalyse mit Bewertung aktueller Bedrohungen und Definition von Gegenmaßnahmen zur Reduktion des Risikos auf akzeptables Maß
  - Abgestimmte organisatorische / technische Maßnahmen
  - Regelmäßige / ereignisgesteuerte Wiederholung.
- Produkte, Anlagen und Prozesse müssen geltenden Sorgfaltsmaßstäben entsprechen, basierend auf Gesetzen, Standards, internen Richtlinien und dem Stand der Technik.



SIEMENS

Übersicht

SIEMENS

Risikoanalyse ist der erste Schritt zur Bestimmung der Security-Maßnahmen

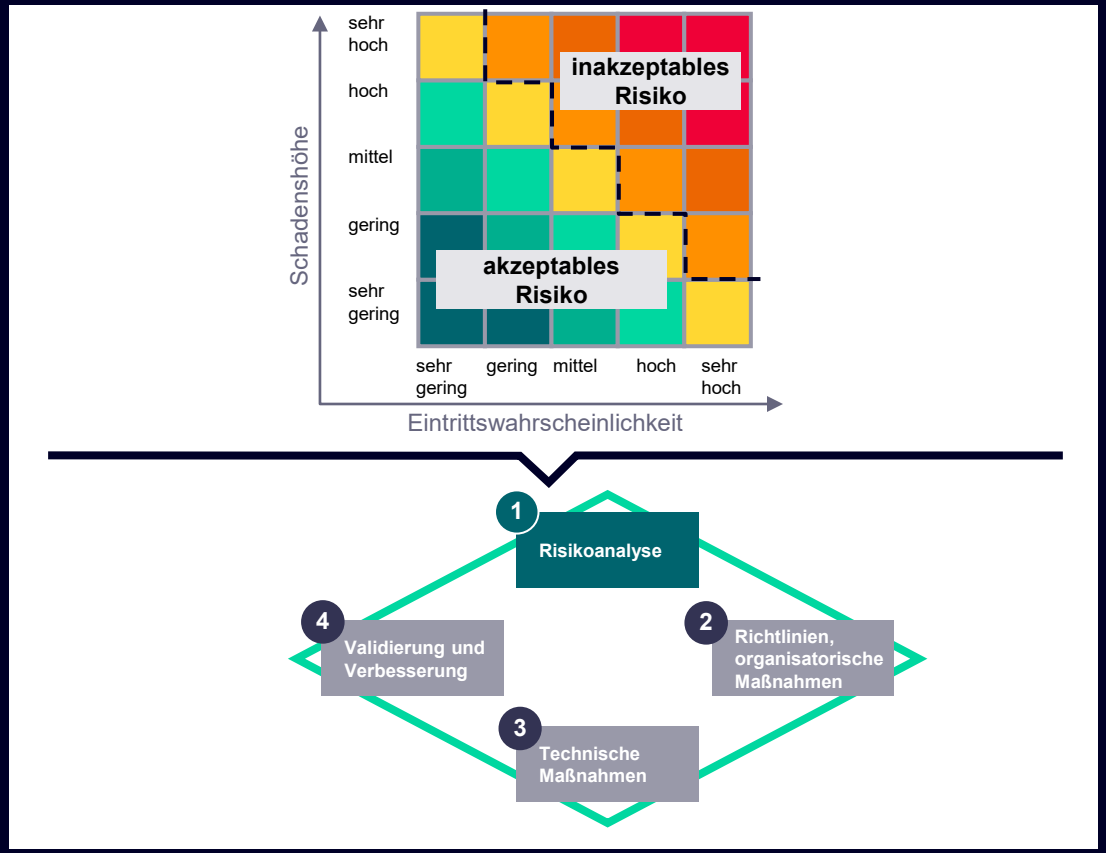
Die Risikoanalyse ist eine wichtige Voraussetzung für das Security-Management einer Anlage oder Maschine zur Identifizierung und Bewertung individueller Gefahren und Risiken.

Typische Inhalte einer Risiko-Analyse

- Identifikation bedrohter Objekte und deren Schutzziele
- Analyse von Wert und Schadenspotential
- Bedrohungs- und Schwachstellenanalyse
- Identifikation bestehender Sicherheitsmaßnahmen
- Risikobewertung

Die identifizierten und nicht akzeptablen Risiken müssen durch geeignete Maßnahmen ausgeschlossen bzw. typischerweise reduziert werden.

Welche Risiken letztendlich akzeptabel sind, kann nur individuell für die jeweilige Anwendung festgelegt werden.



Eine absolute Sicherheit kann jedoch prinzipbedingt weder durch eine Einzelmaßnahme noch durch eine Kombination mehrerer Maßnahmen gewährleistet werden.

SIEMENS

Übersicht

SIEMENS

Nur ein ganzheitliches Sicherheitskonzept kann effektiven Schutz vor Cyber-Bedrohungen bieten

Sicherheitsrisiken zwingen zum Handeln

Anlagensicherheit

- Physischer Zugangsschutz
- Security Richtlinien
- Security Monitoring

Netzwerksicherheit

- Zellenschutz, Perimeter Netzwerk und vertrauenswürdige Zonen
- Firewalls und VPN

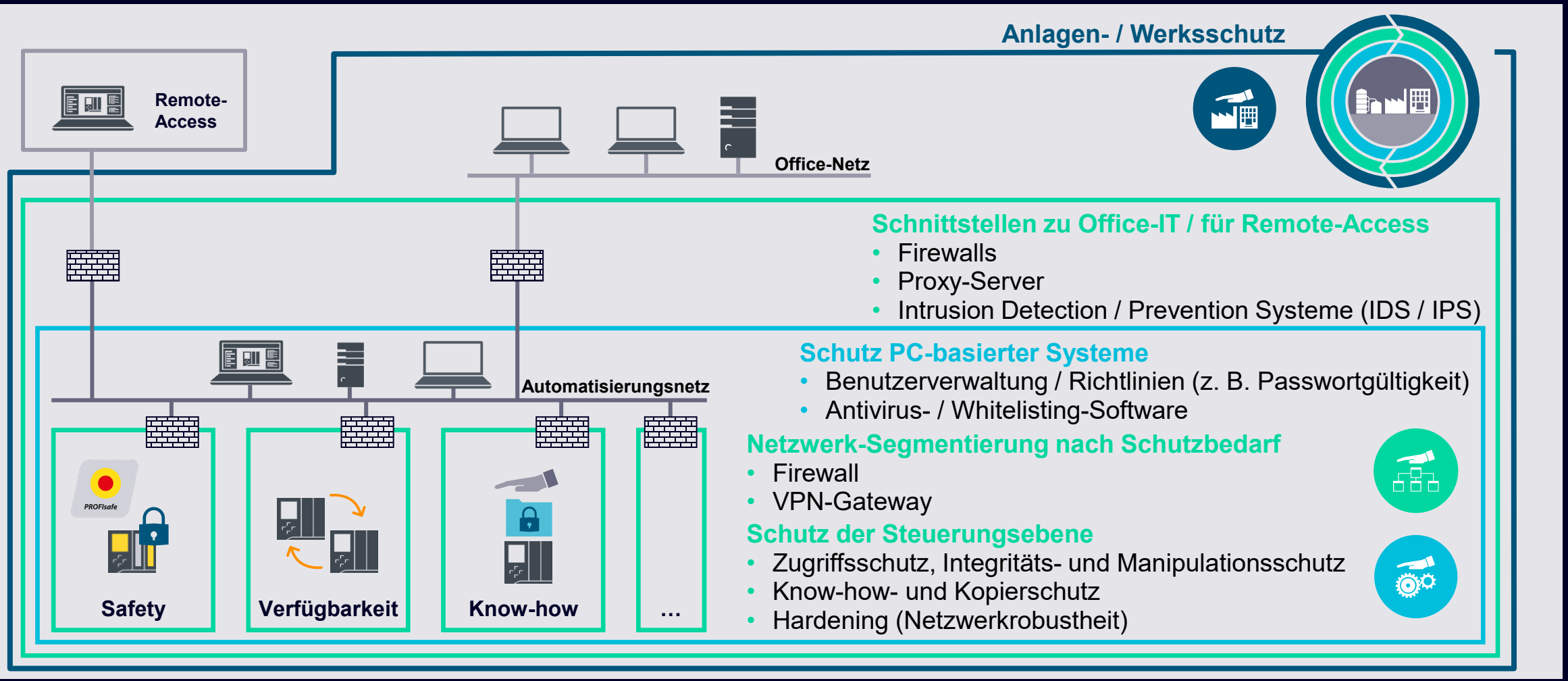
Systemintegrität

- Systemhärtung
- Patch-Management
- Authentifizierung und Zugriffsschutz

Durch den Einsatz mehrerer Security Layer, die die gesamte Anlage, das Netzwerk und die Automatisierungssysteme schützen.

SIEMENS

Abgestufte Security-Architektur zum Schutz von Automatisierungsanlagen (Defense-in-Depth-Architektur)



SIEMENS

Übersicht

SIEMENS

Anlagensicherheit
Etablierung von Security in der Organisation

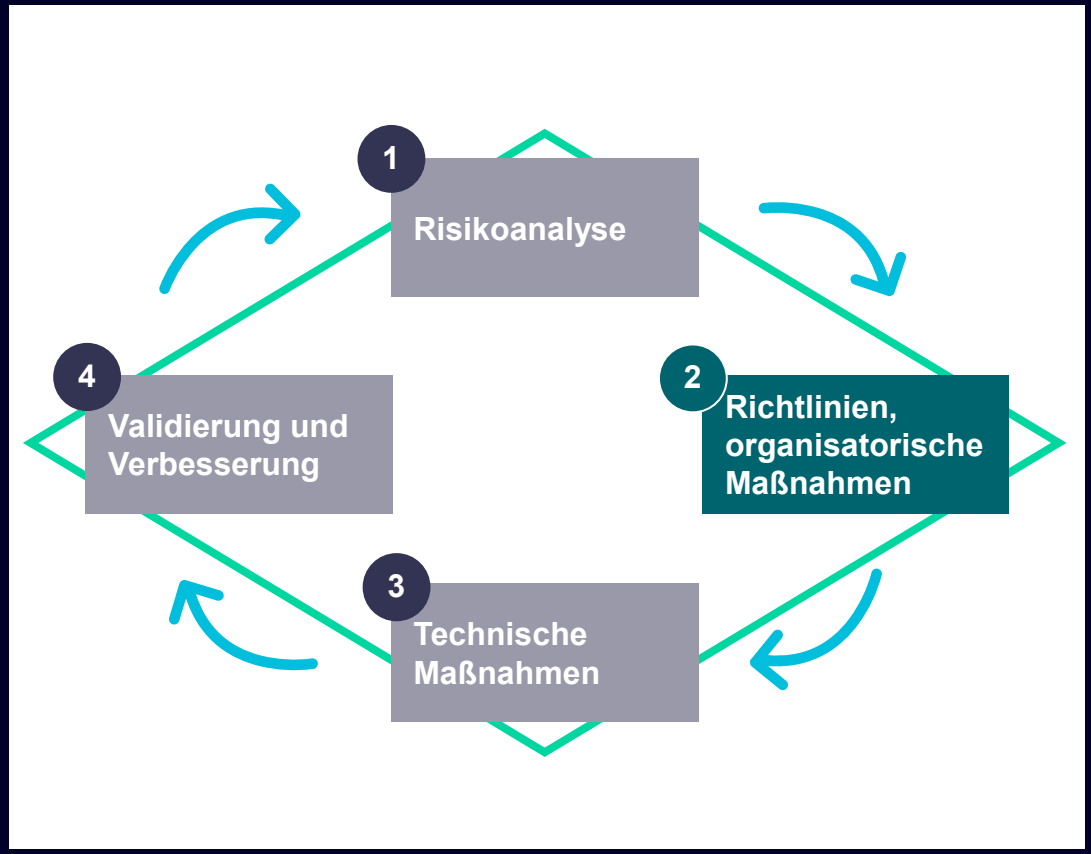
Industrial Security kann nicht alleine mit technischen Maßnahmen realisiert werden, sondern muss auch in allen relevanten Unternehmensbereichen im Sinne eines kontinuierlichen Prozesses gelebt werden.

Industrial Security als Managementaufgabe

- Unterstützung für Industrial Security durch die Geschäftsleitung
- Klar definierte und abgestimmte Verantwortlichkeiten für Industrial Security, IT-Security sowie physikalische Sicherheit des Unternehmens
- Etablieren einer fachgebietsübergreifenden Organisation / eines Netzwerkes mit Zuständigkeit für alle Industrial Security-Angelegenheiten

Sicherstellung des notwendigen Security-Bewusstseins

- Entwicklung und regelmäßige Durchführung von Trainingsprogrammen für produktionsbezogene Security-Themen
- Durchführung von Security-Assessments auch mit „Social Engineering“-Aspekten



SIEMENS

Anlagensicherheit
Richtlinien und Prozesse

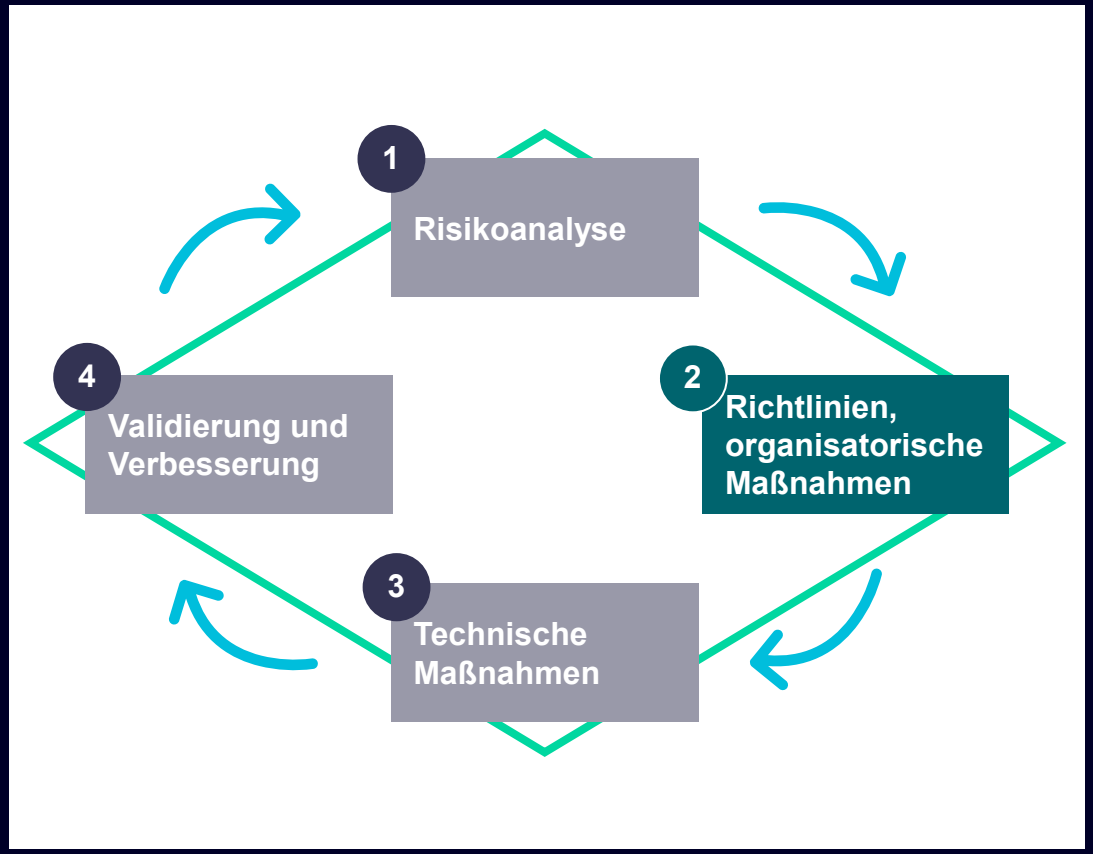
Definition von Richtlinien und Prozessen, um ein einheitliches Vorgehen zu erzielen sowie die Einhaltung des definierten Industrial Security-Konzepts zu unterstützen.

Beispiele für Security-relevante Richtlinien

- Einheitliche Vorgaben für akzeptable Security-Risiken
- Reporting-Mechanismen über ungewöhnliche Aktivitäten und Ereignisse
- Kommunikation und Dokumentation von Security-Vorfällen
- Sicherer Umgang mit mobilen PCs, Smartphones und Datenträgern im Produktionsbereich (z. B. keine Nutzung außerhalb dieses Bereiches / des Produktionsnetzes erlauben)
- Richtlinien für Lieferanten von Produkten, Lösungen oder Dienstleistungen

Beispiele für Security-relevante Prozesse

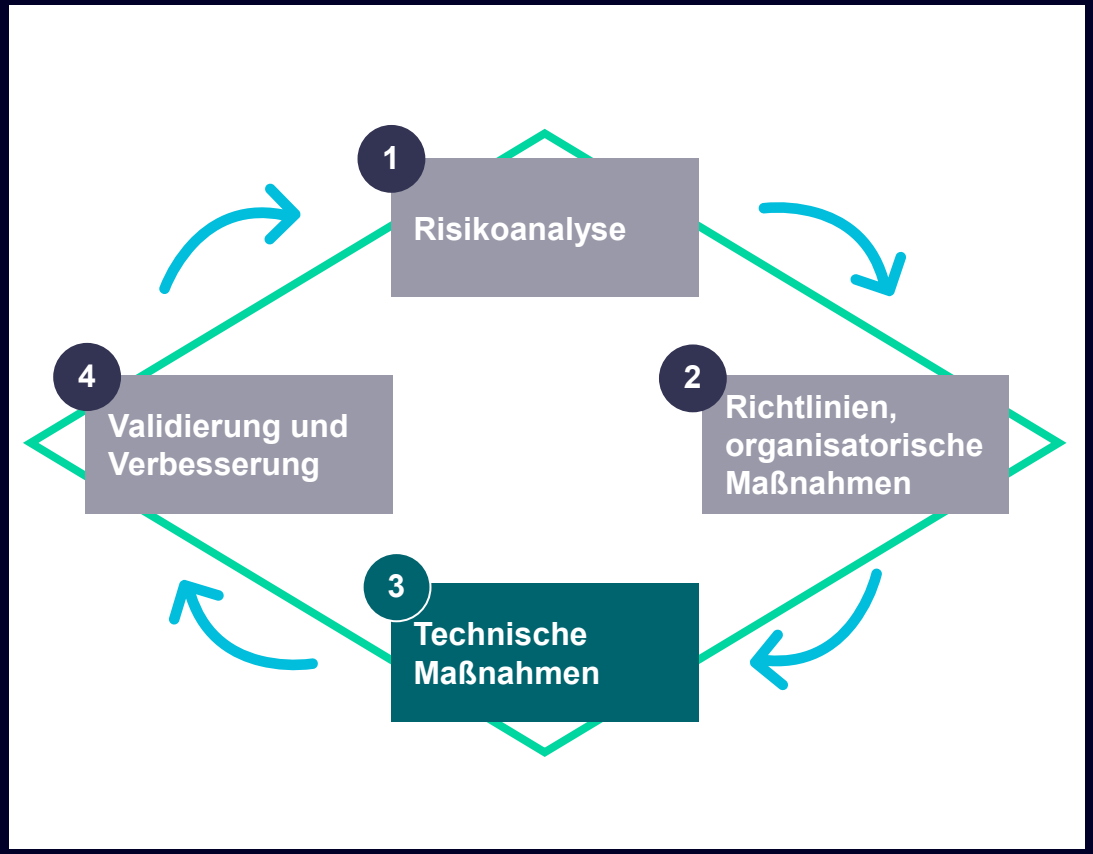
- Umgang mit bekannten / korrigierten Schwachstellen bei eingesetzten Komponenten
- Vorgehen bei Security-Vorfällen („Incident Response Plan“)
- Vorgehen zur Wiederherstellung der Produktionssysteme nach Security-Vorfällen
- Protokollierung und Auswertung von Security-Ereignissen und Konfigurationsänderungen
- Prüfverfahren externer Datenträger vor Verwendung im Produktionsbereich



SIEMENS

Anlagensicherheit
Schutz gegen physikalischen Zugriff auf Produktionsbereiche erforderlich

- Maßnahmen und Prozesse, die den Zugang nicht autorisierter Personen zur Anlage verhindern
- Physikalische Trennung unterschiedlicher Produktionsbereiche mit differenzierten Zugangsberechtigungen
- Physikalischer Zugangsschutz für kritische Automatisierungs-komponenten (z. B. sicher verschlossene Schaltschränke)
- Abgestimmte Richtlinien für physikalische Security und Anlagen-IT-Security erforderlich



SIEMENS

Anlagensicherheit
Physikalischer Schutz kritischer Produktionsbereiche

Risiken

- Betreten des Produktionsgeländes / -gebäudes durch Unbefugte
- Physikalische Beschädigung oder Veränderung von Produktionseinrichtungen
- Verlust vertraulicher Informationen durch Beobachtungen Betriebsfremder

Maßnahmen

Unternehmenssicherheit

- Abgesperrtes und überwachtes Unternehmensgelände
- Einlasskontrolle inkl. Protokollierung, Schlösser / Kartenleser und/oder Pförtner
- Begleitung betriebsfremder Personen durch Unternehmensangehörige

Physikalische Produktionssicherheit

- Abgesperrte Produktionsbereiche mit eingeschränkten Zutrittsberechtigungen
- Einbau kritischer Komponenten in sicher abschließbare Schaltschränke / Schalträume inkl. Überwachungs- und Alarmierungs-möglichkeiten

SIEMENS

Übersicht

SIEMENS

Netzwerksicherheit

Schutz der Automatisierung durch sicheres Netzwerkdesign

Durchgängige Kommunikation von der Leit- bis zur Feldebene ist vor dem Hintergrund aktueller Trends wie dem digitalen Zwilling oder dem Industrial IoT heute wichtiger denn je. Vollständige Konnektivität birgt jedoch auch erhöhte Risiken, die durch Security-Maßnahmen adressiert werden müssen:

Trennung zwischen Produktions- und Office-Netzwerken

- Gesicherter Zugriff über demilitarisierte Zone

Anwendung des Zellenschutzkonzeptes

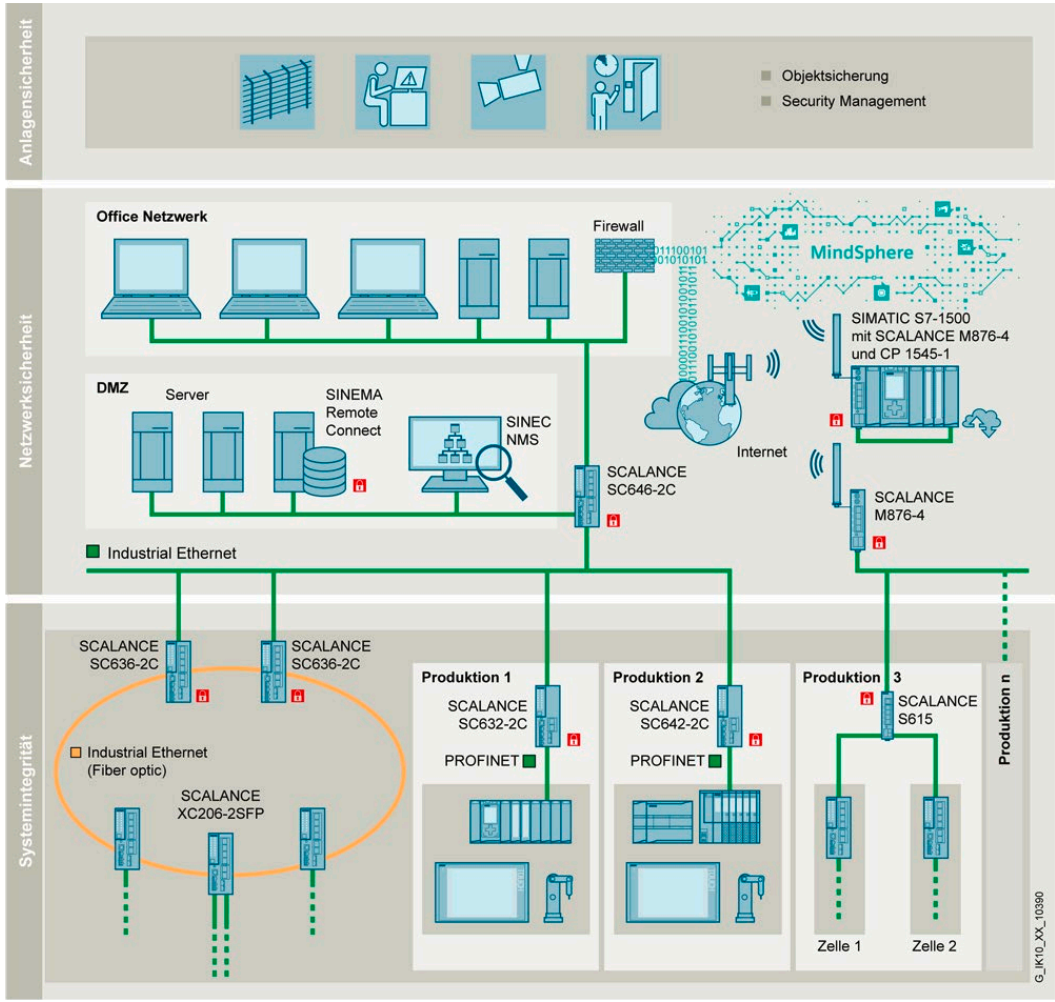
- Unterteilung der Produktion in geschützte Zellen

Sicherer Fernzugriff für Service und Wartung

- Authentifizierte und autorisierte Zugriffe

Sicher mit der Cloud verbinden

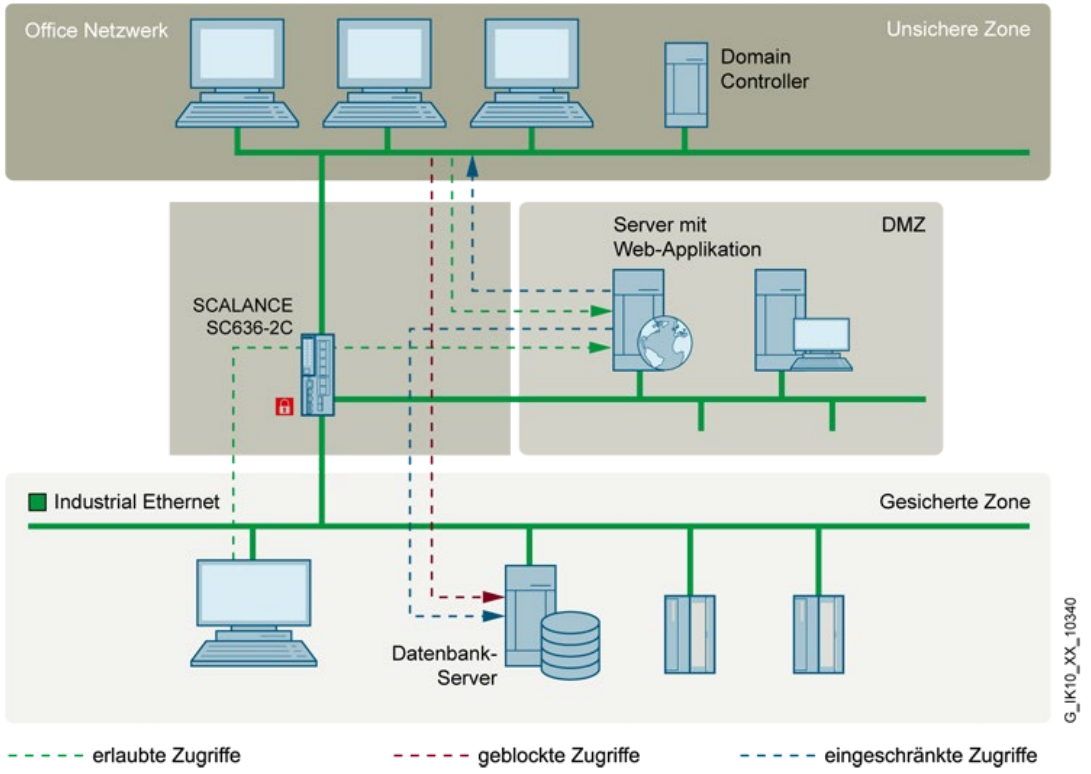
- Zugriffsschutz und sichere Datenübertragung



SIEMENS

Netzwerksicherheit
Trennung zwischen Produktions- und Office-Netzwerken

- Der erste Schritt der Netzwerksegmentierung besteht in der strikten Trennung zwischen Produktionsnetzwerken und den übrigen Unternehmensnetzwerken.
- Im einfachsten Fall erfolgt die Trennung über ein einzelnes Firewall-System, das die Kommunikation zwischen den Netzwerken kontrolliert und reglementiert.
- Bei der sichereren Variante erfolgt die Kopplung über ein separates Netzwerk – der sogenannten demilitarisierten Zone (DMZ), auch Perimeter-Netzwerk genannt.
- Direkte Kommunikation zwischen Produktions- und Unternehmensnetzwerk wird dabei durch Firewalls komplett unterbunden – sie erfolgt ausschließlich indirekt über Serverabfragen in der DMZ.



Netzwerksicherheit
Anwendung des Zellenschutzkonzepts

Segmentierung des Produktionsnetzwerkes in mehrere gesicherte Automatisierungszellen zum Schutz der Komponenten gegen unberechtigte Zugriffe, Netzwerküberlast und weitere Bedrohungen:

Zielsetzung

1. Eine “Zelle” ist ein sicherheitstechnisch abgeschottetes Netzwerksegment
2. Zugriffskontrolle am “Zelleneingang” mit Security-Netzwerkkomponenten
3. Echtzeitkommunikation bleibt unbeeinflusst innerhalb einer Zelle
4. Kommunikation zwischen den Zellen über sichere verschlüsselte Kanäle.

Lösung

Industrial Security Appliance Firewall / VPN

Vorteile

- Schützt Geräte und Kommunikationsprotokolle ohne eigene Mechanismen innerhalb einer Zelle.
- Bietet auch Schutz für Safety-Applikationen innerhalb der Zelle.
- Schützt die Zelle durch Bandbreitenbegrenzung vor externer Netzwerküberlast und hält Datenverkehr innerhalb der Zelle ungestört aufrecht.

SIEMENS

Netzwerksicherheit
Kriterien für Netzwerksegmentierung

- Beim Zellenschutzkonzept wird ein Netzwerksegment von außen gegen unbefugte Zugriffe **geschützt**.
- Der Datenverkehr **innerhalb der Zelle** wird durch die Security Appliance **nicht kontrolliert** und muss daher als sicher angenommen oder durch Schutzmaßnahmen innerhalb der Zelle ergänzt werden.
- Eine Zelle enthält nur Komponenten mit **demselben Schutzbedarf**.
- Die Netzwerkstruktur sollte **ausgehend vom Produktionsablauf** geplant werden. Dies erlaubt die Definition von Zellen mit geringer Kommunikation über Zellengrenzen hinweg und mit minimalen Firewall-Freigaben.

Empfehlungen für Netzwerkgröße und Netzwerksegmentierung

- Alle Geräte eines PROFINET-Systems gehören zu einer Zelle.
- Geräte zwischen denen hohe Kommunikation besteht, sollten in einer gemeinsamen Zelle zusammengefasst werden.
- Geräte, die nur mit Geräten einer Zelle kommunizieren, sollten bei identischem Schutzbedarf in diese Zelle integriert werden.
- Lassen Sie nur die Kommunikation zu, die auch tatsächlich benötigt wird
  → **„Need-to-connect“ Prinzip**

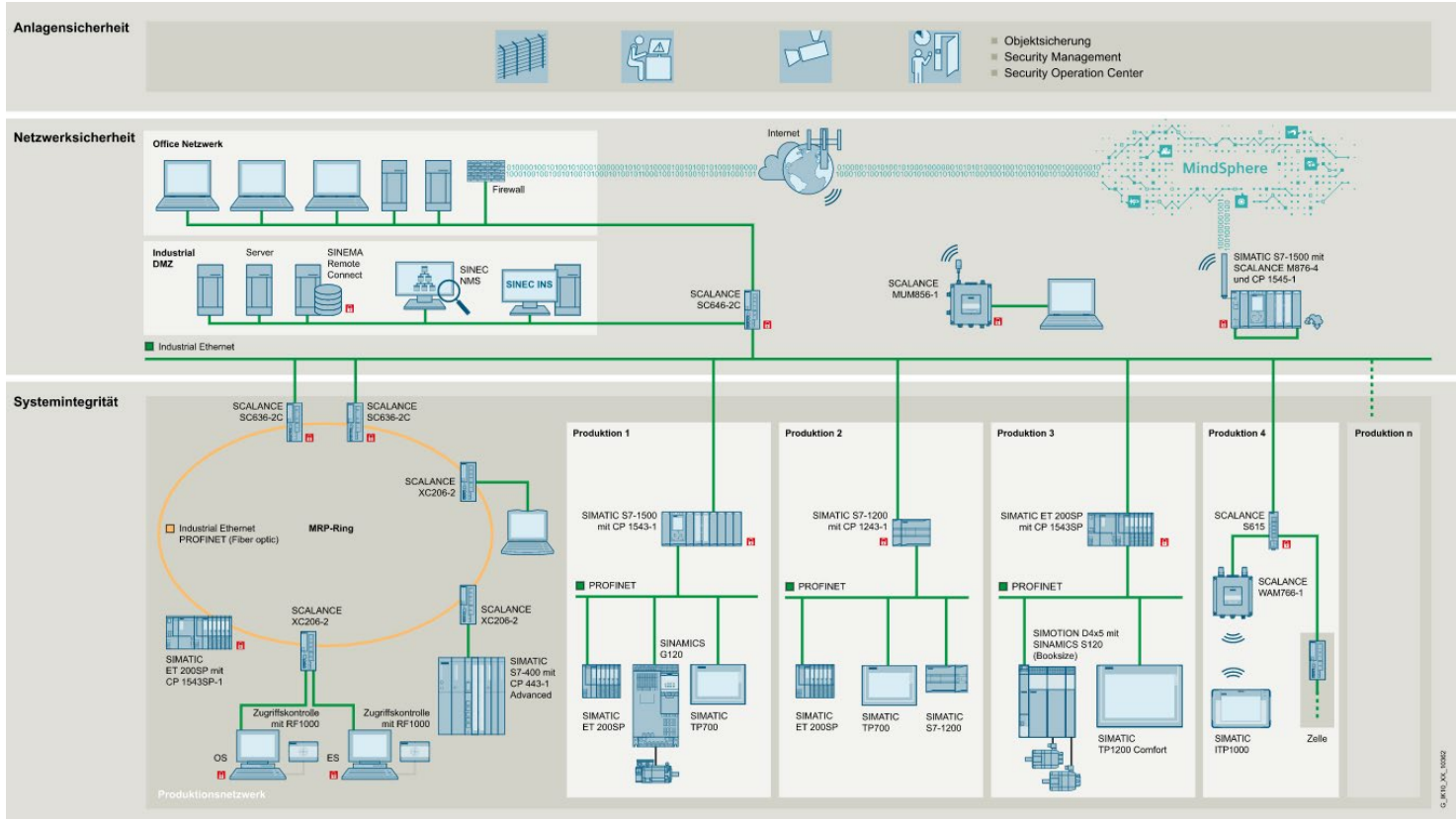
SIEMENS

Netzwerksicherheit
Beispiel: Netzwerksegmen-tierung mit Security Appliances

Alternativ oder ergänzend zu Industrial Security Appliances können auch SIMATIC S7- und PC-Kommunikations-prozessoren (CP) mit **"Security Integrated“** Funktionalität (Firewall und VPN) für den Schutz von Automatisierungs-geräten und -zellen eingesetzt werden.

Die S7-Kommunikationsprozessoren schützen durch die **integrierte Firewall** die unterlagerten Netzwerke.

Zusätzlich können damit **verschlüsselte VPN-Verbindungen** direkt bis zur SIMATIC S7-1200, S7-1500 oder Distributed Controller ET 200SP aufgebaut werden.

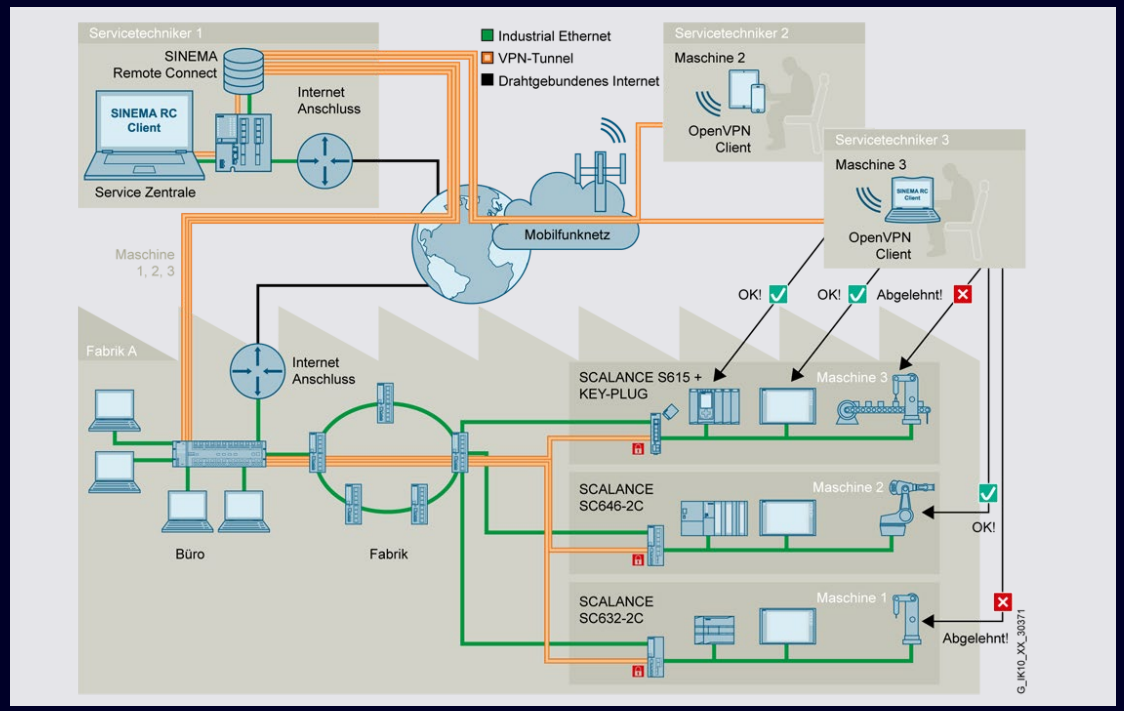


SIEMENS

Netzwerksicherheit
Sicherer Fernzugriff für Service und Wartung

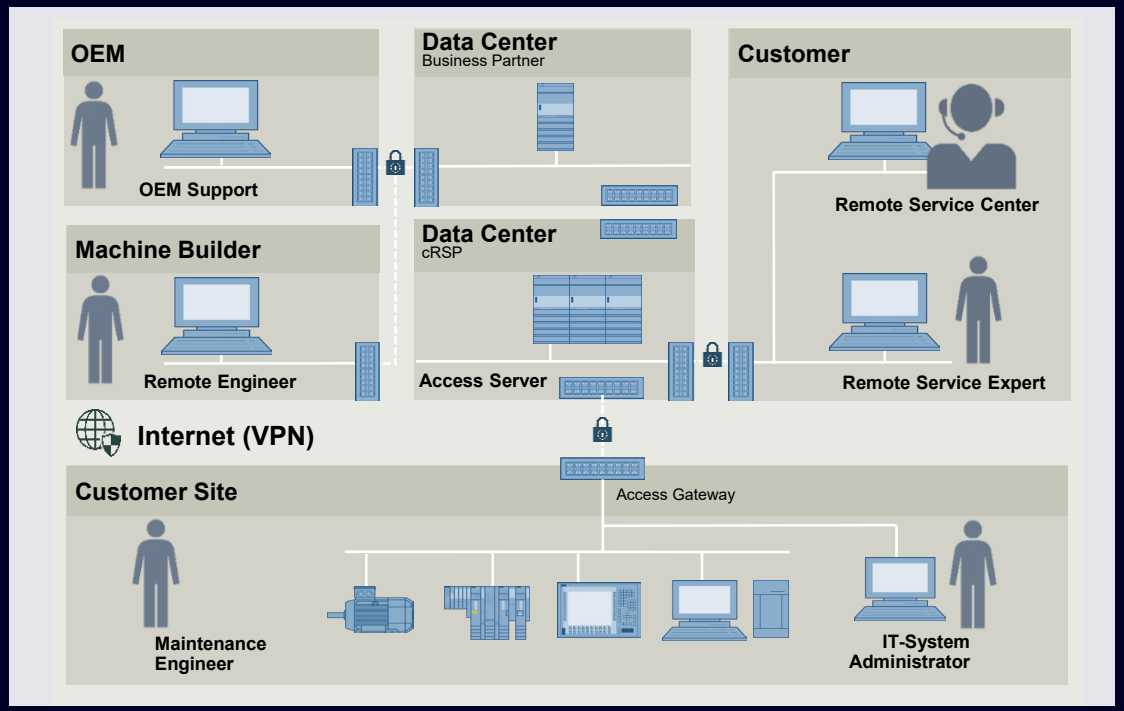
SINEMA Remote Connect

- Betrieb und Verwaltung eines firmeneigenen **Rendezvous-Servers** für sichere Fernzugriffe
- **Geräteabhängige Zugriffskontrolle** über granulare Benutzer- und Gruppenverwaltung



Siemens common Remote Service Platform – cRSP

- Durch **SIEMENS** gemanagte **Cloud Plattform** für sichere Fernzugriffe
- Fein-granulare Benutzerrechte und durchgängige Auditfähigkeit und **Zertifizierung gemäß ISO 27001**



SIEMENS

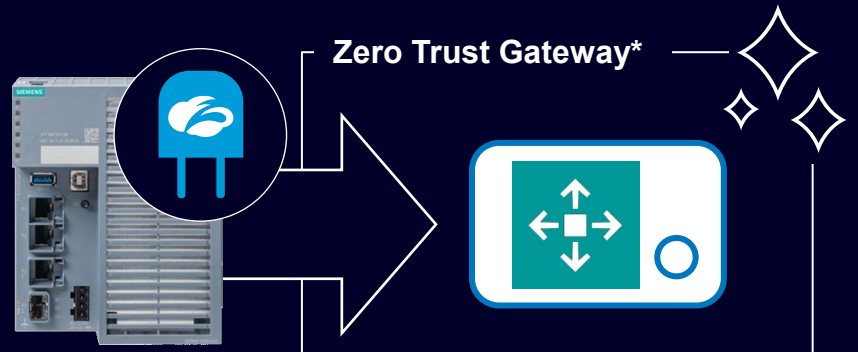
Netzwerksicherheit

Sicherer Zugriff auf den OT-Bereich basierend auf das Zero-Trust-Konzepts

siemens.de/zero-trust

OT / IT-Kollaboration

- Sicherer Zugang mit **einer einheitlichen Lösung** für die Zusammenarbeit zwischen OT und IT, die zentral betrieben und verwaltet wird
- Robuste Lösung basierend auf **Zero-Trust**-Prinzipien
- Anwendungsbasierter, gerätespezifischer Zugriff in Abhängigkeit von zugewiesenen Benutzerrechten für einen **sicheren und transparenten Zugriff auf den OT-Bereich**
- **Flexible und skalierbare** Cloud-basierte Lösung, die in **bestehende Netzwerke eingefügt** werden kann, ohne dass dazu Komponenten ausgetauscht werden müssen
- Höhere Mitarbeiterzufriedenheit durch **ortsunabhängiges mobiles Arbeiten**
- Kostenoptimierung durch Zugriff vom Büro zum Shopfloor mittels **zentralem und ganzheitlichem Zugriffsrichtlinien-Management für OT / IT**



SCALANCE LPE +
Zscaler App Connector

SIEMENS

Netzwerksicherheit

Vorteile von Zero Trust durch SCALANCE LPE mit Zscaler Private Access

Herausforderung

Sicheren Zugriff auf OT-Bereiche – auch eingeschränkte – auf die Maschinenebene von innerhalb oder außerhalb des Kundennetzwerks ermöglichen, ohne die aktuelle Netzwerkinfrastruktur zu verändern. Dabei Einhaltung der IT-Regeln in Bezug auf Zero Trust Exchange.

Lösung

- SCALANCE LPE inklusive Zscaler-Anwendung als Lösung für OT in industriellen Umgebungsbedingungen
- Einfache Firewall-Konfiguration – ausschließlich über ausgehende Verbindungen
- Anwendungsbasierter und gerätespezifischer Zugriff in Abhängigkeit von zugewiesenen Benutzerrechten
- Fernzugriff auf Shopfloor ohne VPN-Tunnelmechanismen oder Jump-Host-Server für eine hohe Transparenz und ein reduziertes Risiko von z. B. Lateral Movement

Vorteile auf einen Blick

Hoher Datenschutz aufgrund der Ende-zu-Ende-Verschlüsselung und des kundeneigenen Identity Providers

Sofortiger Zugriff auf die OT-Umgebung

Cloud-basierte Wartung von Sicherheits- und Zugriffsrichtlinien sowie skalierbarer Konnektivität

SIEMENS

Netzwerksicherheit
Gesicherte Cloud-Anbindung

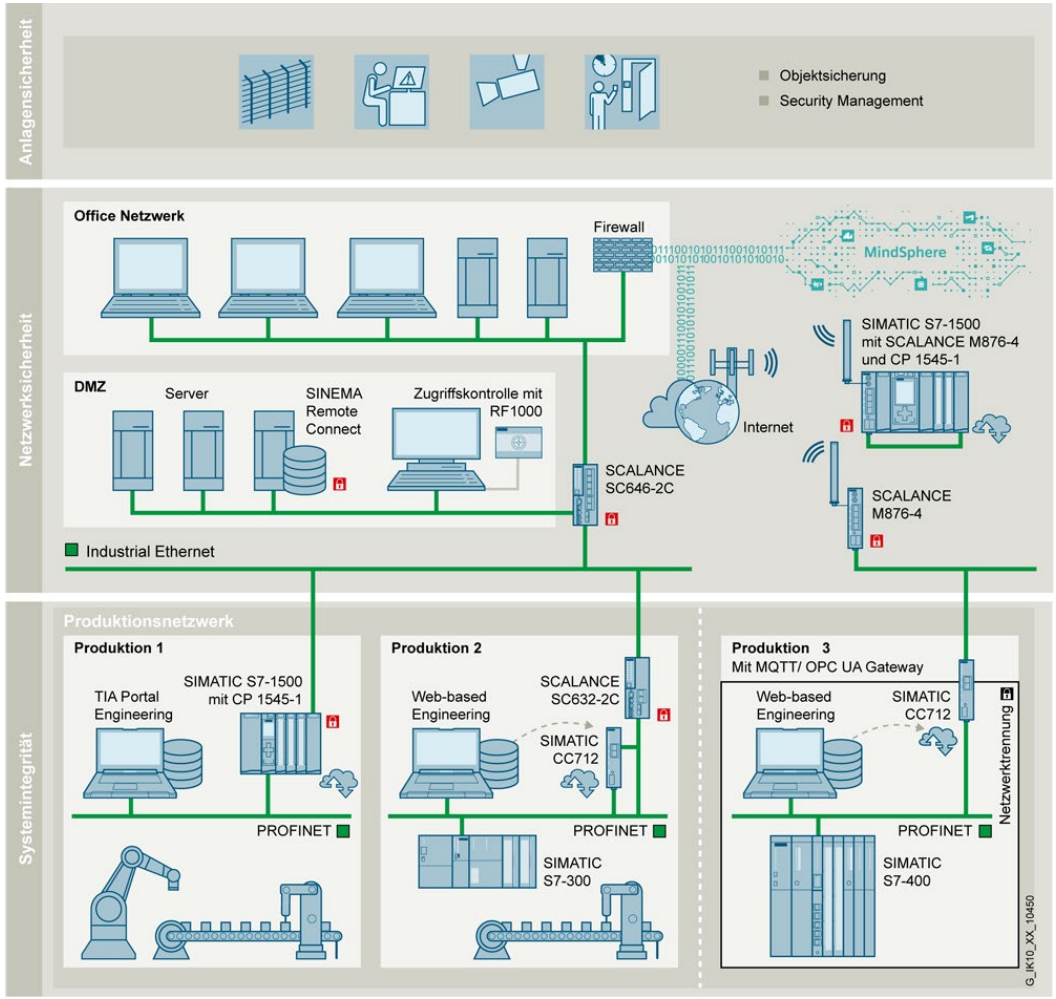
- Es sollten nur **TLS-basierte Kommunikations-protokolle** wie z. B. HTTPS, MQTT inkl. TLS für Gerätezugriffe und Datenübertragungen verwendet werden.

- Anstelle anonymer Zugriffe sollten ausschließlich **authentifizierte Geräte- und Datenzugriffe** z. B. mittels individueller Kennwörter oder Zertifikate konfiguriert werden.

- Bestehende **Netzwerksegmentierungen** und **Zellenschutzkonzepte** durch z. B. Firewalls oder Netzwerktrennungen sollten aufrechterhalten werden.

- Anbindung von Bestandsanlagen über geeignete Gateways wie z. B. **SIMATIC CloudConnect 7**

Weitere Informationen: MindSphere Security Whitepaper



SIEMENS

Netzwerksicherheit
Mögliche Risiken und empfohlene Maßnahmen

Risiken

- Unberechtigter Zugriff auf Automatisierungsgeräte ohne eigene Security-Mechanismen
- Beeinträchtigung der Geräteverfügbarkeit durch Netzwerküberlast
- Spionage / Manipulation der Datenübertragung in oder zwischen Automatisierungs-systemen

Maßnahmen

- Aufteilung des Automatisierungsnetzes in sinnvolle Netzwerksegmente und Kontrolle des ein- und ausgehenden Datenverkehrs durch eine Firewall (Perimeterschutz). Kritische Netzwerkprotokolle können damit beispielsweise gesperrt werden.
- Einsatz der Bandbreitenbegrenzung, beispielsweise in der Zellen-Firewall oder in Switches. Eine Netzwerküberlast von außerhalb der Zelle kann die innen liegenden Komponenten dadurch nicht beeinträchtigen.
- Datenübertragungen über unsichere Netze beispielsweise zwischen Zellen oder von Clients zu Zellen können mit der Security- bzw. VPN-Appliance, die den Zugang zur Zelle schützt verschlüsselt und authentifiziert werden.
- Sicherer und bedarfsgerechter Zugriff auf OT-Anwendungen und -Systeme mit einer durchgängigen Zero Trust-Lösung für die OT / IT-Zusammenarbeit im Produktions- und Büronetzwerk.

SIEMENS

Übersicht

SIEMENS

Sichere PG/HMI Kommunikation mit TIA Portal V17

TLS*-basierter Schutz der Kommunikation zwischen S7-Controller und Engineering Stationen mit TIA Portal oder HMI-Stationen

Verschlüsselt die Kommunikation mittels individueller Zertifikate

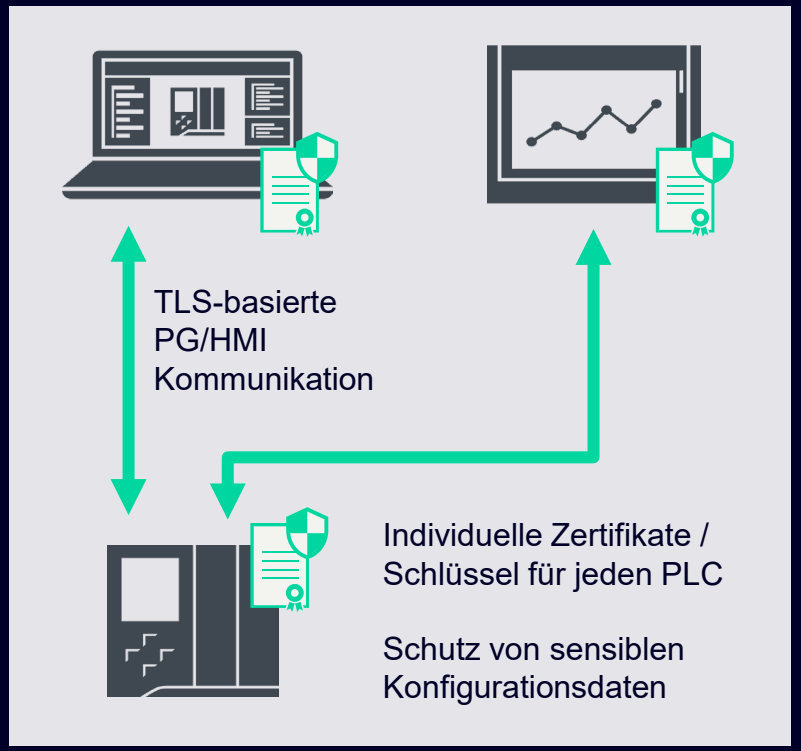
*) TLS - Transport Layer Security

SIEMENS

Sichere SIMATIC PG/HMI Kommunikation
Erhöhte Kommunikationssicherheit

Sicherheitsverbesserungen für die PG/HMI Kommunikation zwischen TIA Portal V17, HMIs und S7-1200/1500 CPUs

- Der Kommunikationsschutz basiert auf dem Internet-Standard **TLS***
- Unterstützt die individuelle Identifikation jeder PLC auf Basis von **individuellen Zertifikaten** (z. B. erstellt über TIA Portal)
- Kompatibilitätsmodus für bisherige und neue TLS-basierte Kommunikation gleichzeitig aktivierbar
- Bietet zusätzlichen Schutz der Vertraulichkeit durch verschlüsselte Kommunikation
- Ermöglicht den Schutz sensibler Konfigurationsdaten im TIA Portal und in den Steuerungen über benutzerdefinierte Passwörter (optional)



* TLS - Transport Layer Security

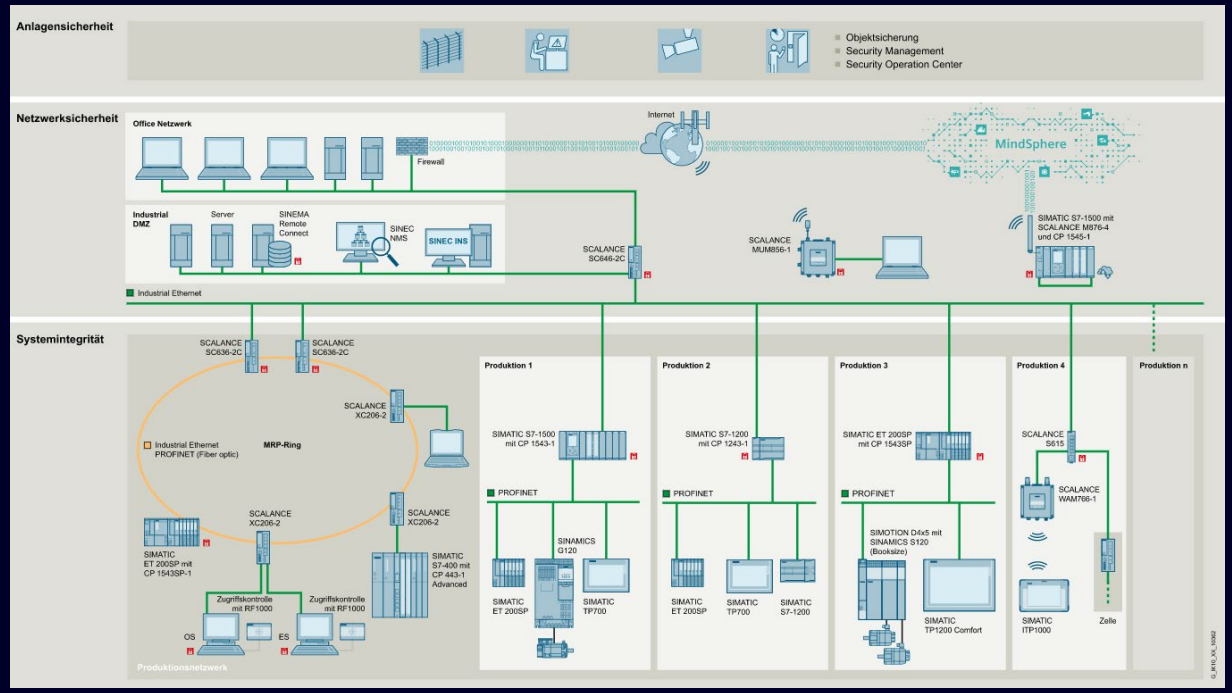
Vorteile

- Ermöglicht die individuelle Identifizierung jeder PLC auf Basis von individuellen Zertifikaten
- Bietet zusätzlichen Schutz der Vertraulichkeit durch verschlüsselte Kommunikation
- Konfigurationsdatenschutz basierend auf individuellen Passwörtern

SIEMENS

Systemintegrität
Zugriffsschutz zur Konfiguration von Automatisierungssystemen

Zur Vermeidung unerlaubter Konfigurationsänderungen an Automatisierungskomponenten wird dringend empfohlen, **die integrierten Zugriffschutzmechanismen** zu nutzen.



Dazu zählen beispielsweise:

- Firewalls (User-Authentifizierung)
- WLAN Access Points (User-Authentifizierung)
- Managed Switches (User-Authentifizierung)
- HMI-Panels (Zugriffsschutz für Geräteeinstellungen)
- PLCs (Schutzstufen für Projektierung und HMI-Zugriff)
- Antriebe (Know-how-Schutz).

Einsatz von Komponenten mit integrierten Security-Funktionalitäten wie beispielsweise die S7-1500 Controller, SINUMERIK ONE

Verwendung jeweils unterschiedlicher und möglichst sichererer Passworte (wenn möglich mind. 12 Zeichen mit Groß- / Kleinbuchstaben, Zahlen und ggf. Sonderzeichen)

Zur einfacheren Hantierung der Passwörter empfiehlt sich der Einsatz eines allgemeinen Passwort-Managers. Bei mehreren Personen sollte dieser dann zentral auf einem Netzlaufwerk inkl. Zugriffsrechten abgelegt werden.

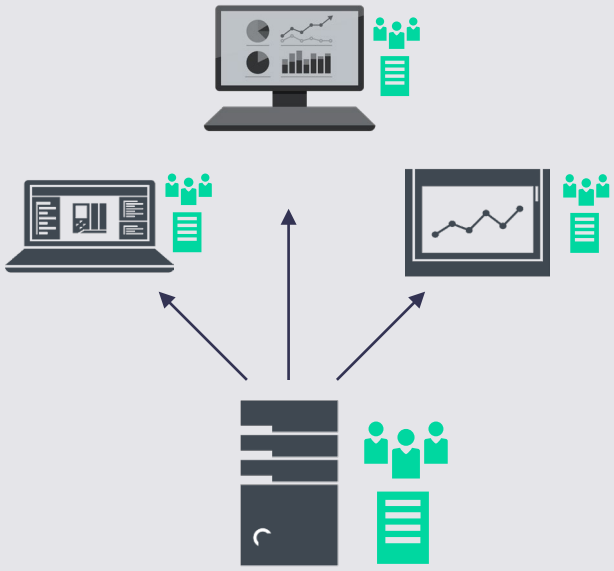
SIEMENS

Systemintegrität
Zugriffsschutz für Bedienoperationen (Runtime)

- Da die Bedienung von Maschinen / Anlagen typischerweise durch unterschiedliche Personen erfolgt, empfiehlt sich der Einsatz einer zentralen Benutzerverwaltung.
- Diese basiert typischerweise auf Benutzer-Accounts eines Windows Active Directory. Die Anbindung der SIMATIC (HMI) Runtime-Applikationen erfolgt in diesem Fall über SIMATIC Logon oder UMC.
- Damit erfolgt eine implizite Festlegung / Durchsetzung von Security-Richtlinien (z. B. Passwortgültigkeit, Überwachung fehlerhafter Anmeldevorgänge, etc.).
- Zentrale Benutzer-Verwaltung vereinfacht regelmäßiges Review von Zugriffsberechtigungen (z. B. Erkennen ungenutzter Accounts).
- Abhängig vom Security-Bedarf können auch für unterschiedliche Netzwerk-zellen / -zonen getrennte Windows-Domänen zum Einsatz kommen.
- Abhängig von den erforderlichen Rollen (Bediener, Administrator, etc.) sollten den Benutzer-Accounts nur die jeweils erforderlichen Bedienberechtigungen zuweisen werden.

Zentrale Verwaltung von

- Benutzer-Accounts / -Gruppen
- Policies



SIEMENS

Systemintegrität
Zugriffsschutz für Netzwerkkomponenten (Netzwerk)

Zugriffsschutz für Netzwerke durch

- Port-Security bei Switch-Ports: MAC- oder IP-Accesslisten beschränken den Zugriff,
- Port-Security mit zentraler Geräteverwaltung und RADIUS-Authentifizierung (802.1X),
- Perimeterschutz eines Netzwerkes zu anderen Netzwerken (z. B. Internet) mit Firewalls.

WLAN-Security

- Schutz der Datenübertragung mit min. WPA2
- Verwendung des Advanced Encryption Standards (AES) zur Datenverschlüsselung
- Authentifizierung mit zentraler Geräteverwaltung durch RADIUS-Authentifizierung (nach 802.1X)
- Gesicherte Projektierzugriffe auf Webinterface mittels HTTPS und sicheres Einloggen via SSH

Systemintegrität
Systemhärtung zur Reduktion von Angriffspunkten

Netzwerkdienste

- Aktive Netzwerkdienste stellen grundsätzlich ein potentielles Sicherheitsrisiko dar.
- Zur Risikominimierung sollten bei allen Automatisierungskomponenten nur die benötigten Dienste aktiviert sein.
- Alle aktivierten Dienste (insb. Webserver, FTP, Remote Desktop, etc.) sollten im Security-Konzept berücksichtigt sein.
- Hardening-Maßnahmen (Netzwerkrobustheit und Security-by-Default Einstellungen) in unseren Automatisierungs- und Antriebs-produkten erhöhen die Security ohne separate Anwenderkonfiguration.

HW- & System-Schnittstellen

- Hardware-Schnittstellen stellen ein Risiko dar, wenn darüber unerlaubter Zugriff auf Geräte oder das System möglich ist und sollen daher deaktiviert werden:
  - USB, Ethernet / PROFINET-Ports
  - WLAN, Bluetooth, Mobilfunk.
- Schutz durch Abschalten oder zumindest mechanisches Blockieren.
- Booten und Autostart-Mechanismen von externen Medien deaktivieren.
- Zugriffsschutz auf BIOS- bzw. UEFI-Einstellungen aktivieren.
- Remote-Management (z. B. AMT) nur gesichert betreiben.

Benutzer-Accounts

- Jeder aktive Benutzer-Account ermöglicht einen Zugriff auf das System und ist damit ein potentielles Risiko.
- Reduktion konfigurierter / aktivierter Benutzer-Accounts auf das wirklich benötigte Minimum.
- Verwendung sicherer Zugangsdaten für die vorhandenen Accounts.
- Regelmäßige Prüfung insbesondere der lokal konfigurierten Benutzer-Accounts.

Wichtig:
Ändern Sie die ggf. systemseitig voreingestellten Standard-Passwörter bei der Inbetriebnahme!

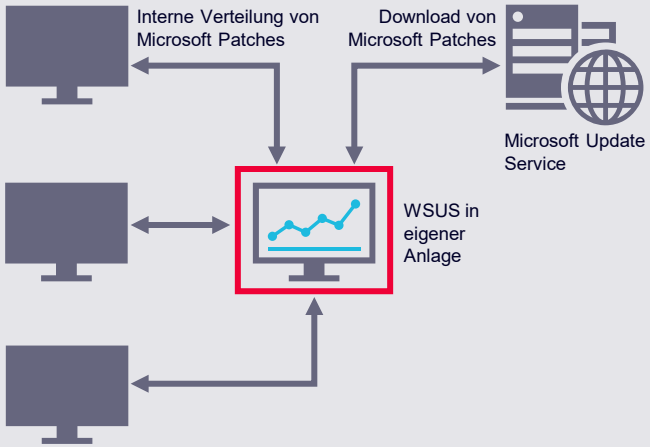
SIEMENS

Systemintegrität
Patch-Management schließt Sicherheitslücken in Betriebssystem und Applikationen

Viele Security-Angriffe erfolgen heute über Schwachstellen, für die es bereits Patches seitens der Hersteller gibt. Nur in seltenen Fällen kommen Zero-day-Exploits zum Einsatz, bei denen die Schwachstelle noch nicht offiziell bekannt ist bzw. es noch keine Updates gibt.

- Einspielen von Patches bzw. Updates ist eine wichtige Maßnahmen zur Erhöhung der Security.
- Siemens unterstützt durch Verträglichkeitstests mit Microsoft Security Patches:
  - SIMATIC PCS 7: http://support.automation.siemens.com/WW/view/de/22754447
  - SIMATIC WinCC: http://support.automation.siemens.com/WW/view/de/18752994
- Durchführung eigener anlagenspezifischer Verträglichkeitstests empfohlen.
- Zentrale Verteilung der Patches über einen Update-Server in der DMZ und Windows Server Update Services (WSUS).

  Industrial Security Services
- Die Einrichtung von Update-Gruppen und Prozesse für Online-Updates erleichtert die Verteilung der Patches (z. B. bei redundanten Systemen).



SIEMENS

Systemintegrität
Software-Updates für mehr Sicherheit von Automatisierungskomponenten

- Auch bei Automatisierungskomponenten, die kein Standard-PC-Betriebssystem nutzen, kann es erforderlich sein, Security-relevante Schwachstellen durch ein Software-Update zu beheben.
- Informationen dazu erhalten Sie über die Siemens Industrial Security Webseite (http://www.siemens.com/industrialsecurity) sowie unsere Newsletter bzw. RSS-Feed.

- Sobald Informationen über eine Schwachstelle verfügbar sind, sollte diese zunächst auf Relevanz für die eigene Anwendung bewertet werden.
- Davon abhängig kann dann entschieden werden, ob weitere Maßnahmen zu treffen sind:
  - Keine Aktion, da vorhandene Maßnahmen ausreichenden Schutz bieten
  - Zusätzliche externe Maßnahmen, um Security-Niveau weiterhin zu gewährleisten
  - Installation des aktualisierten Software-Updates, um Schwachstelle zu beheben.
- Der Vorgang ist vergleichbar mit einer Risikoanalyse wie zu Beginn, aber mit eingeschränktem Fokus.

Tipp: Werkzeuge wie das SIMATIC Automation Tool oder SINEC NMS unterstützen auch bei der Software-Aktualisierung von Automatisierungs- bzw. Netzwerkkomponenten.

SIEMENS

Systemintegrität
Schadsoftware erkennen / verhindern durch Virenscanner

Zur Erkennung von Schadsoftware und zur Verhinderung weiterer Ausbreitung sollte eine passende Antivirus-Software eingesetzt werden.

Je nach Anwendungsfall sind jedoch besondere Aspekte zu berücksichtigen:

- Performance-Verluste durch Scan-Vorgang; Alternativ z. B. nur automatischer Scan des eingehenden Datentransfers und manueller Scan während Wartungspausen.
- Regelmäßiges Update der Virensignaturen – ggf. über zentralen Server.
- Verfügbarkeit muss in der Regel auch bei Infektion mit Schadsoftware gewährleistet werden.
  Das bedeutet, der Virenscanner darf unter keinen Umständen:
  - Dateien entfernen, den Zugriff darauf blockieren oder in Quarantäne verschieben,
  - Kommunikation blockieren,
  - Systeme herunterfahren.

Siemens unterstützt durch Verträglichkeitstest *) mit Lösungen von

- McAfee

  Industrial Security Services
- Symantec
- Trend Micro

Weitere Informationen finden Sie im Kompatibilitäts-Tool:
http://www.siemens.de/kompatool

*) **Bitte beachten Sie:** Die Verträglichkeit muss für jede spezielle Konfiguration überprüft werden.

SIEMENS

Systemintegrität
Schadsoftware erkennen / verhindern durch Virenscanner

Grundprinzip

- Whitelisting-Mechanismen bieten zusätzlichen Schutz gegen unerwünschte Applikationen bzw. Schadsoftware sowie unerlaubte Änderungen an installierten Applikationen.
- Whitelisting-Software erstellt oder beinhaltet eine Liste von Programmen und Applikationen, die auf dem PC ausgeführt werden dürfen.
- Software, die nicht Teil dieser „Whitelist“ ist, wird die Ausführung verwehrt.

Vorteile

- Keine regelmäßigen bzw. zeitlich verzögerte Pattern-Updates
- Zusätzlicher Schutzmechanismus
- Höherer Schutz gegen bestimmte Arten von Schadsoftware

Siemens unterstützt durch Verträglichkeitstest mit *)

- McAfee Application Control

Industrial Security Services

Weitere Informationen finden Sie im Kompatibilitäts-Tool:
http://www.siemens.de/kompatool

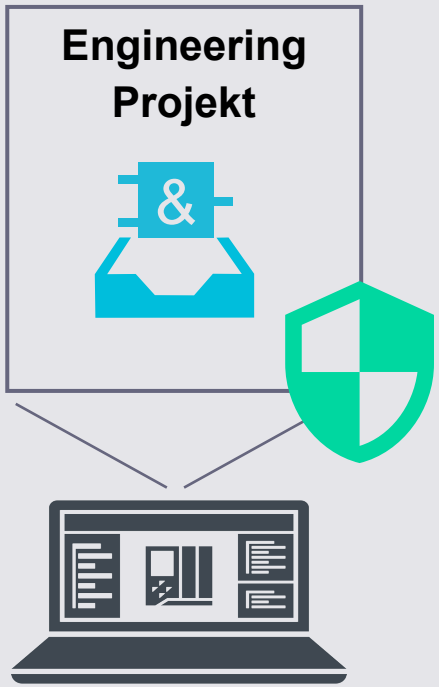
*) **Bitte beachten Sie:** Die Verträglichkeit muss für jede spezielle Konfiguration überprüft werden.

SIEMENS

Systemintegrität
Zugriffsschutz für industrielle Projektierungsdaten

Projektierungsdaten für industrielle Automatisierungslösungen (z. B. Engineering Projekte) enthalten häufig internes Know-how, das nicht in fremde Hände gelangen sollte. Beachten Sie daher folgende Hinweise:

- Schützen Sie ihre Projektierungsdaten grundsätzlich vor unberechtigtem Zugriff.
- Schützen Sie gespeicherte Projektierungsdaten z. B. mittels Zugriffsschutz der Dateisystemrechte oder Speicherung in einem verschlüsselten Laufwerkscontainer.
- Verschlüsseln Sie vertrauliche Projektierungsdaten, wenn sie diese transportieren (z. B. via verschlüsselter E-Mail oder verschlüsselten ZIP Archiven).
- Wenden Sie konsequent das „Need to know“-Prinzip an.
- Konfigurieren Sie Security-Mechanismen, die Online-Dienste nutzen, um auf schadhafte Daten zu prüfen, so dass Projektdateien nicht unbeabsichtigt hochgeladen werden. Dies betrifft beispielsweise 3rd-party E-Mail-Gateways, Endpoint Protection Systeme, DLPs oder IDSs.



SIEMENS

Systemintegrität
Mögliche Risiken und empfohlene Maßnahmen

Risiken

- Manipulation / Spionage durch unberechtigten Zugriff auf Geräteprojektierungen
- Unberechtigte Durchführung von Bedienoperationen
- Beeinträchtigung der Geräteverfügbarkeit durch Installation und Weiterverbreitung von Schadsoftware
- Unberechtigter / öffentlicher Zugriff auf Projektierungsdateien

Maßnahmen

- Verwendung der Zugriffschutzmechanismen in den Automatisierungskomponenten, um nur berechtigten Personen Zugriff auf Konfigurationsdaten und -einstellungen zu gewähren.
- Durchführung individueller Härtungsmaßnahmen für die einzelnen Automatisierungskomponenten zur Reduktion von Angriffsflächen.
- Installation von bereitgestellten Updates bei Behebung Security-relevanter Schwachstellen oder Etablierung alternativer Schutzmaßnahmen.
- Nutzung von Antivirus- und Whitelisting-Mechanismen zum Schutz gegen Schadsoftware.
- Einsatz von Schutzmechanismen für Projektierungsdateien über den gesamten Lebenszyklus (verschlüsseltes Speichern / Transferieren; Zugriffsschutz; Hochladen zu Online-Scannern unterbinden; Sicheres Löschen alter Daten).

Übersicht

SIEMENS

Überprüfung der Maßnahmen

Überprüfung und Verbesserungen

Nach Umsetzung aller geplanten Maßnahmen erfolgt ein Security-Audit um sicherzustellen, dass

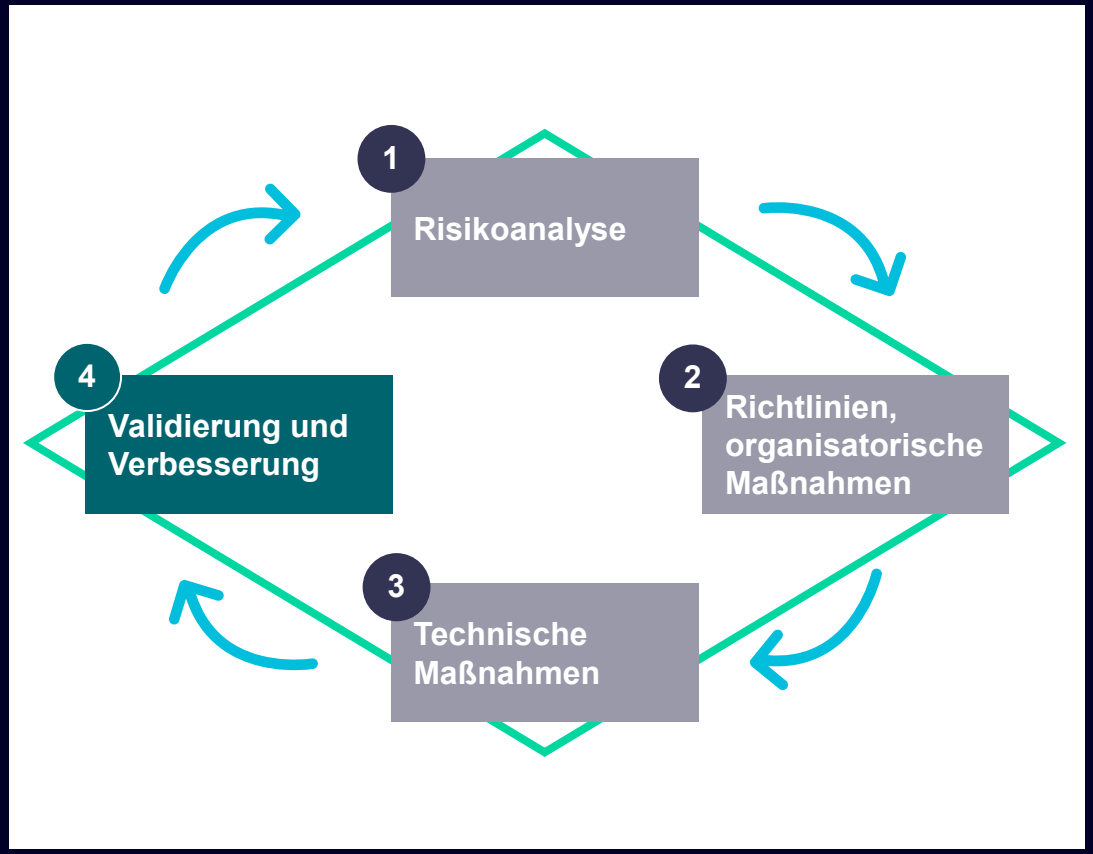
- die Maßnahmen wie geplant umgesetzt wurden,
- diese Maßnahmen die identifizierten Risiken wie erwartet reduzieren.

Je nach Ergebnis können hier noch Maßnahmen geändert / ergänzt werden um den erforderlichen Schutz zu erreichen.

Wiederholung der Risikoanalyse

Aufgrund sich ändernder Security-Bedrohungen ist eine regelmäßige Wiederholung der Risikoanalyse erforderlich, um die Sicherheit einer Maschine / Anlage zu gewährleisten.

- Aufgrund bestimmter Ereignisse (bei Erweiterungen oder Änderungen der Maschine / Anlage, signifikante Änderungen der Security-Bedrohungen, etc.)
- Jährliche Überprüfung, ob erneute Risikoanalyse erforderlich ist.



SIEMENS

Industrial Security
Siemens ProductCERT

ProductCERT ist ein spezialisiertes Team von anerkannten Security-Experten zur Untersuchung, internen Koordination und Veröffentlichung von Sicherheitsproblemen mit Bezug zu Siemens Produkten, Lösungen oder Services.

https://www.siemens.com/cert

ProductCERT

- unterhält starke und verlässliche Beziehungen zu Partnern und Security Researchern weltweit,
- ist die zentrale Anlaufstelle, um potentielle Sicherheitsschwachstellen in Siemens Produkten zu melden,
- koordiniert und unterhält die Kommunikation mit involvierten internen als auch externen Parteien, um identifizierte Sicherheitsprobleme angemessen zu adressieren,
- veröffentlicht Security Advisories, welche den Kunden
- über die betroffenen Produkte informieren,
- eine genaue Schwachstellenbeschreibung enthalten (CVE),
- ermöglichen, die Relevanz für eigene Lösungen zu ermitteln, z. B. anhand der CVSS-Bewertung,
- über notwendige Schritte für einen geschützten Betrieb seiner Anlage informieren.

SIEMENS

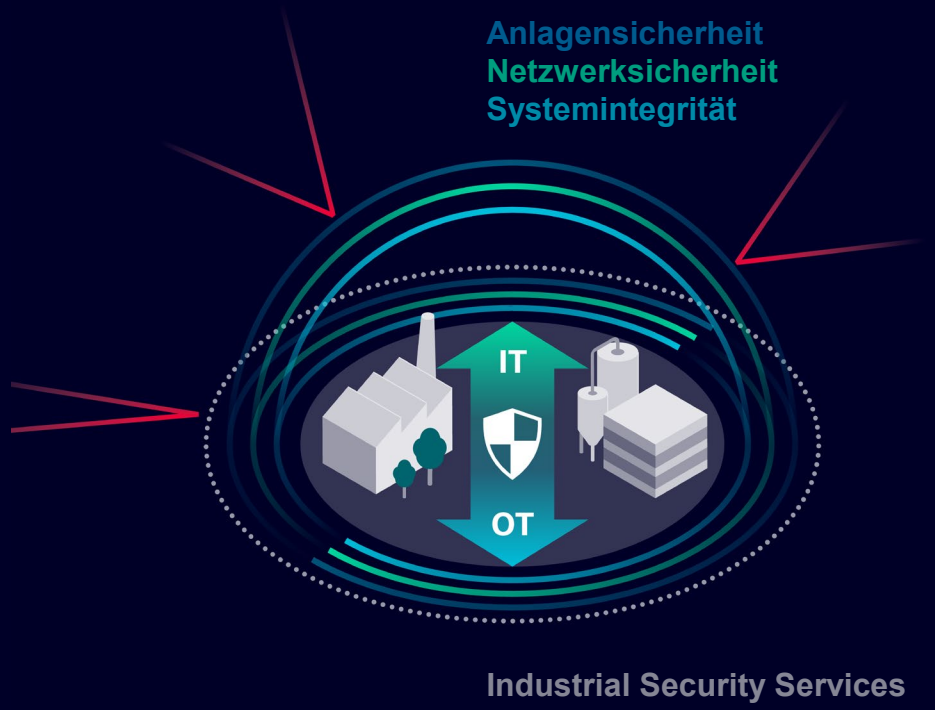
Übersicht

SIEMENS

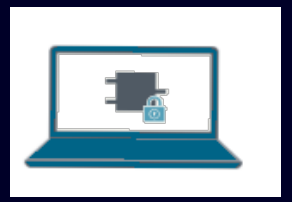
Unser Angebot für Industrial Cybersecurity

Defense in Depth

basierend auf IEC 62443

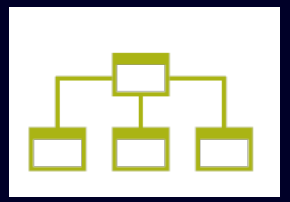


Siemens Produkte und Systeme mit integrierter Security



Know-how und Kopierschutz

Authentifizierung und Nutzerverwaltung



Firewall und VPN

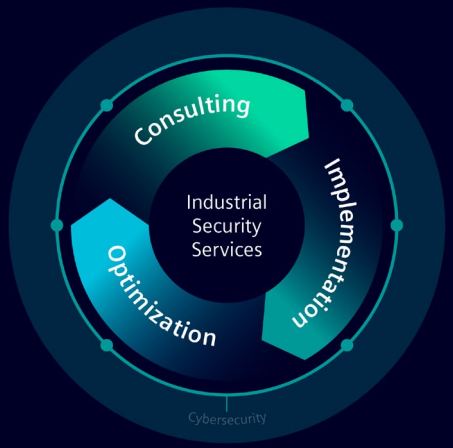
System-Härtung und kontinuierliche Überwachung mit Anomalie Erkennung

Siemens Industrial Security Services

Transparenz über den aktuellen Security-Status

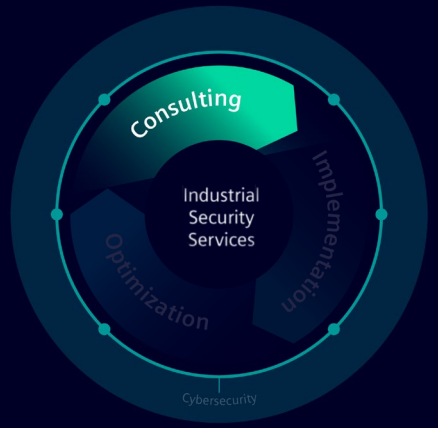
Erhöhtes Security-Level durch das Schließen von Sicherheitslücken

Langfristiger Schutz durch kontinuierliches Security-Management



V2.1
SIEMENS

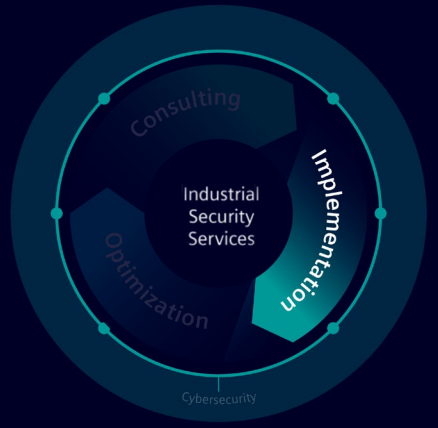
Industrial Cybersecurity Services
Ein ganzheitlicher Ansatz



Security Consulting

Evaluierung des aktuellen Security-Status in industriellen Anlagen

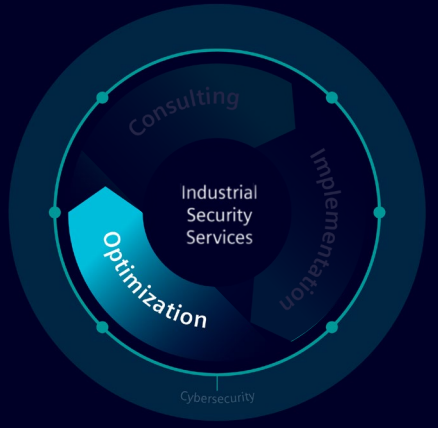
- Security Assessments
- Scanning Services
- Industrial Security Consulting



Security Implementation

Risikominderung durch die Implementierung von Security-Maßnahmen

- Security Awareness Training
- Automation Firewall
- Endpoint Protection z. B. Hardening-Maßnahmen (Netzwerkrobustheit)



Security Optimization

Höherer Schutz durch Managed Services

- Industrial Anomaly Detection
- Industrial Security Monitoring
- Remote Incident Handling
- Industrial Vulnerability Manager
- Patch Management
- SIMATIC Security Service Packages

https://support.industry.siemens.com/cs/de/de/sc/4973

SIEMENS

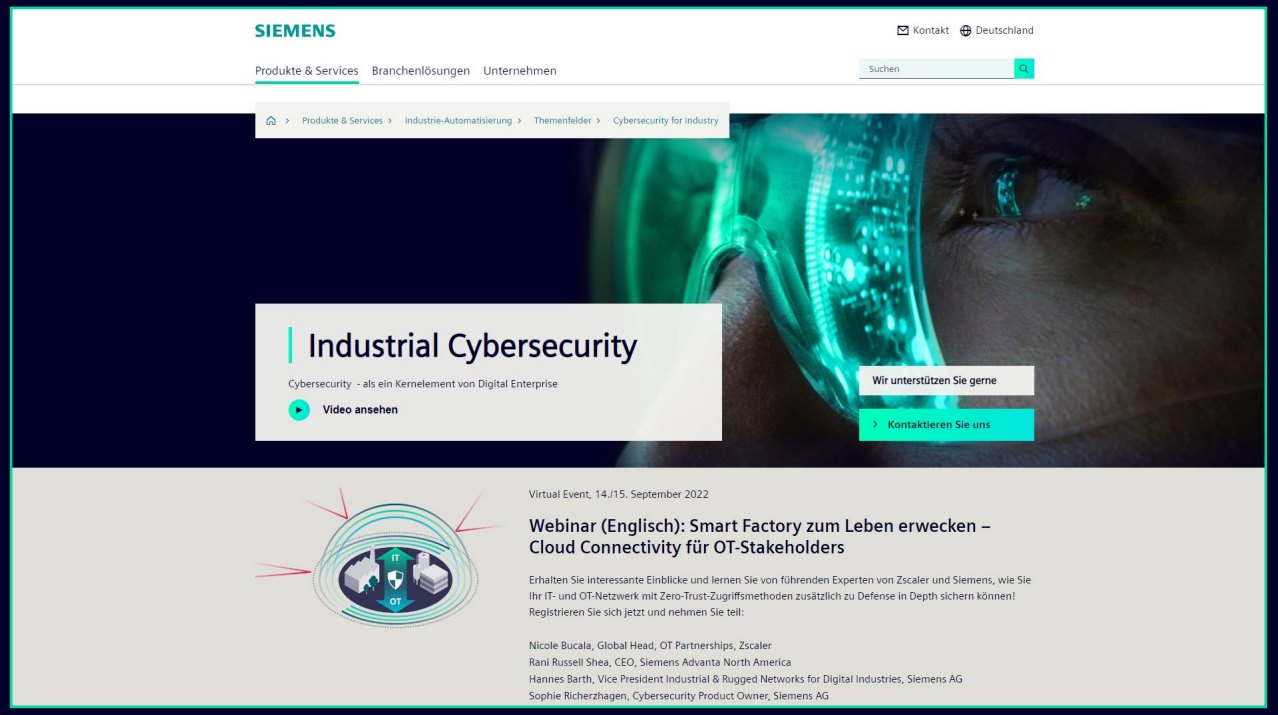
Zusammenfassung

Industrial Cybersecurity

- Industrial Cybersecurity ist nicht nur ein technisches Thema, sondern muss als Prozess gelebt und als Management-Aufgabe verstanden werden.
- Abhängig von den Risiken der Automatisierungsanwendung sind sinnvolle organisatorische und technische Maßnahmen zu ergreifen und regelmäßig zu prüfen.
- Nur im engen Zusammenspiel aller Beteiligten entsteht maximaler Schutz.
- Siemens Digital Industries bietet Produkte und Systeme als auch Security Services an, um umfassende Industrial Security Lösungen für unsere Kunden sicherzustellen.

SIEMENS

Industrial Security –
… entdecken Sie mehr – Konzepte, Produkte und News!



Weitere Informationen auf unserer Industrial Cybersecurity Homepage:
siemens.de/industrialsecurity

Siemens ProductCERT – Contact for Products, Solutions and Services

PGP Public Key and Fingerprint: 7F04 6EDA 338E 6D94 A3AA 4974 BB67 95EA 8E55 D52E

Email: productcert@siemens.com

Siemens CERT – Contact for Infrastructure

PGP Public Key and Fingerprint: A3D1 8E40 D104 DEAD A112 3FF6 B485 0E2E 1AA2 2CD8

Email: cert@siemens.com

SIEMENS

Weiterführende Security Guidelines

Security Leitfaden für SIMATIC HMI Bediengeräte
https://support.industry.siemens.com/cs/ww/de/view/109481300

Empfohlene Sicherheitseinstellungen für IPCs im Industrieumfeld
https://support.industry.siemens.com/cs/ww/de/view/109475014

Security bei SIMATIC Controllern
https://support.industry.siemens.com/cs/ww/de/view/90885010

SIMATIC Process Control System PCS 7 Security Concept PCS 7 & WinCC (Basic)
https://support.industry.siemens.com/cs/ww/de/view/60119725

SIMATIC Process Control System PCS 7 Compendium Part F - Industrial Security
https://support.industry.siemens.com/cs/ww/de/view/109756871

SINUMERIK / SIMOTION / SINAMICS Industrial Security
https://support.industry.siemens.com/cs/ww/de/view/108862708

SIEMENS

Security-Hinweise

Siemens bietet Produkte und Lösungen mit Industrial Security-Funktionen an, die den sicheren Betrieb von Anlagen, Systemen, Maschinen und Netzwerken unterstützen. Um Anlagen, Systeme, Maschinen und Netzwerke gegen Cyber-Bedrohungen zu sichern, ist es erforderlich, ein ganzheitliches Industrial Security-Konzept zu implementieren (und kontinuierlich aufrechtzuerhalten), das dem aktuellen Stand der Technik entspricht. Die Produkte und Lösungen von Siemens formen einen Bestandteil eines solchen Konzepts.

Die Kunden sind dafür verantwortlich, unbefugten Zugriff auf ihre Anlagen, Systeme, Maschinen und Netzwerke zu verhindern. Diese Systeme, Maschinen und Komponenten sollten nur mit dem Unternehmensnetzwerk oder dem Internet verbunden werden, wenn und soweit dies notwendig ist und nur wenn entsprechende Schutzmaßnahmen (z. B. Firewalls und/oder Netzwerksegmentierung) ergriffen wurden.

Weiterführende Informationen zu möglichen Schutzmaßnahmen im Bereich Industrial Security finden Sie unter https://www.siemens.com/industrialsecurity.

Die Produkte und Lösungen von Siemens werden ständig weiterentwickelt, um sie noch sicherer zu machen. Siemens empfiehlt ausdrücklich, Produkt-Updates anzuwenden, sobald sie zur Verfügung stehen und immer nur die aktuellen Produktversionen zu verwenden. Die Verwendung veralteter oder nicht mehr unterstützter Versionen kann das Risiko von Cyber-Bedrohungen erhöhen.

Um stets über Produkt-Updates informiert zu sein, abonnieren Sie den Siemens Industrial Security RSS Feed unter https://www.siemens.com/industrialsecurity.

Disclaimer

Änderungen und Irrtümer vorbehalten. Die Informationen in diesem Dokument enthalten lediglich allgemeine Beschreibungen bzw. Leistungsmerkmale, welche im konkreten Anwendungsfall nicht immer in der beschriebenen Form zutreffen bzw. welche sich durch Weiterentwicklung der Produkte ändern können. Die gewünschten Leistungsmerkmale sind nur dann verbindlich, wenn sie bei Vertragsschluss ausdrücklich vereinbart werden.

Alle Produktbezeichnungen können Marken oder sonstige Rechte der Siemens AG, ihrer verbundenen Unternehmen oder dritter Gesellschaften sein, deren Benutzung durch Dritte für ihre eigenen Zwecke die Rechte der jeweiligen Inhaber verletzen kann.

SIEMENS