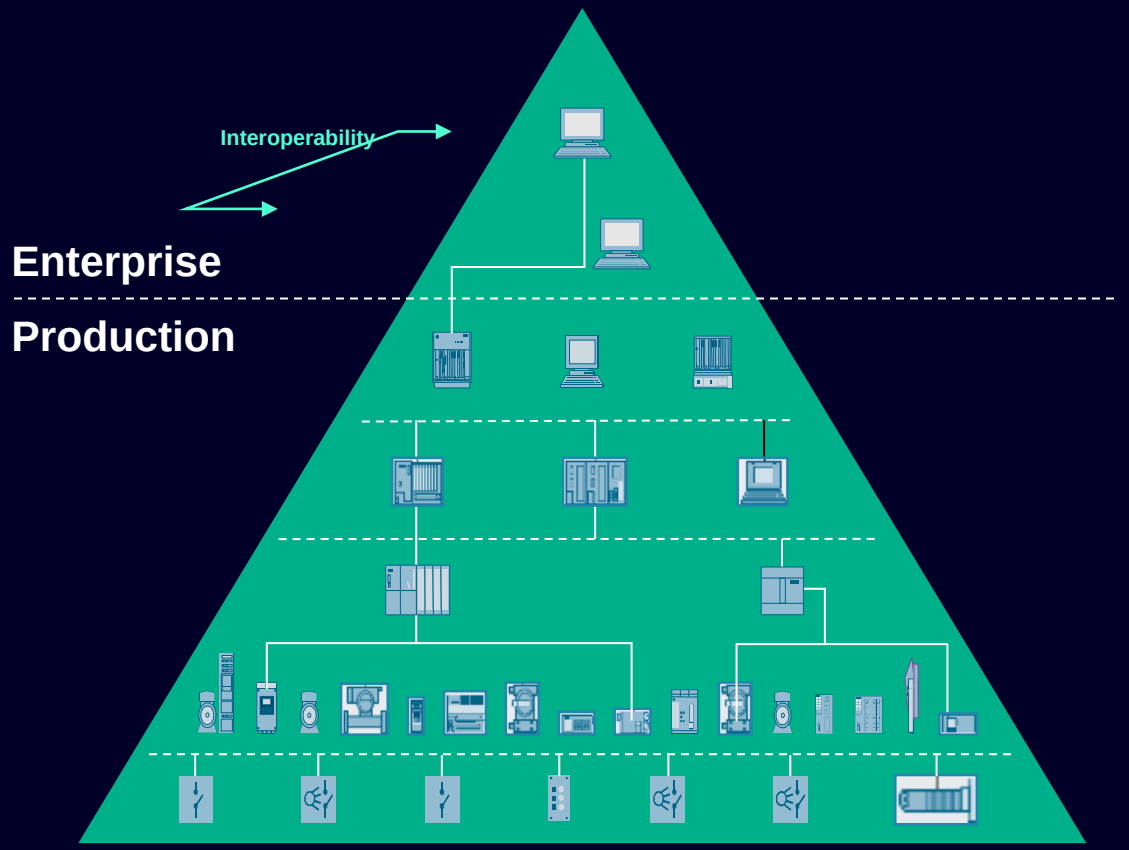
Defense-in-Depth

Industrial Security Tag, 30.11.2022

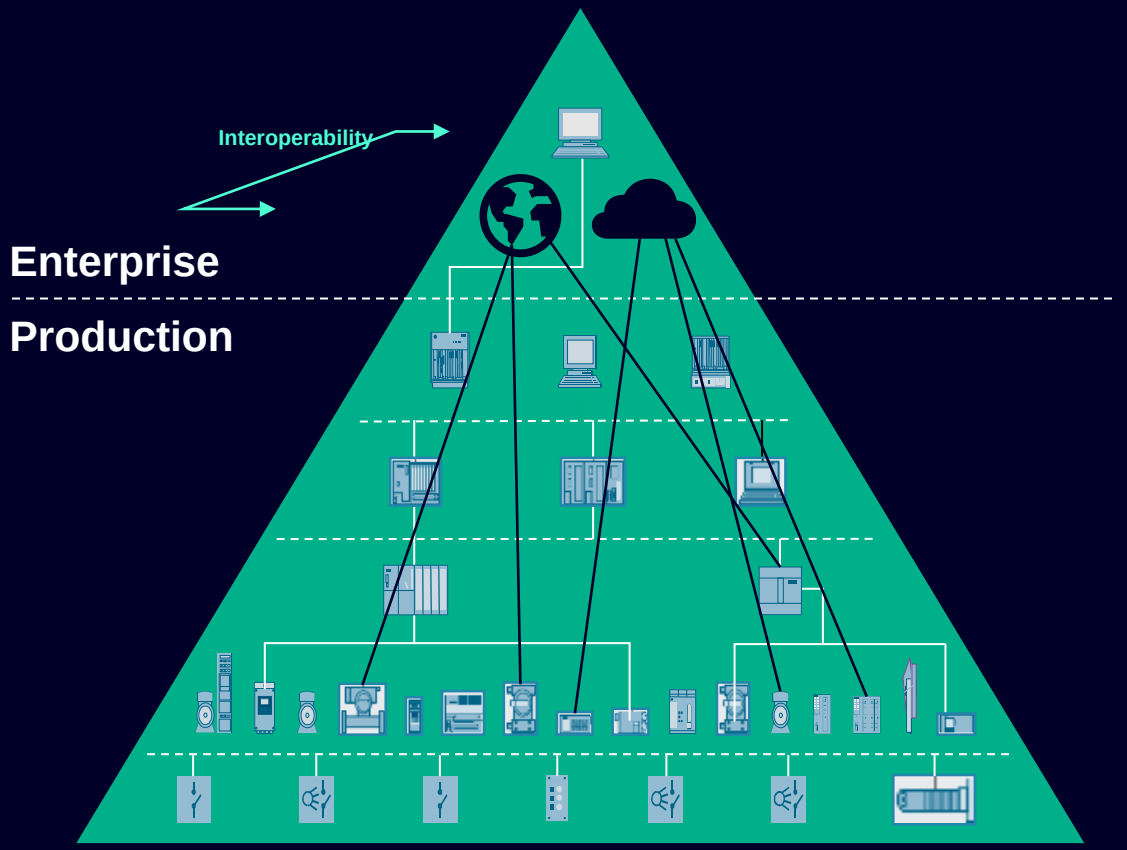
SIEMENS

Gestern: klare getrennte Strukturen



SIEMENS

Heute: Vermischung zwischen IT und OT



SIEMENS

Morgen: Connectivity vom Shopfloor zum Topfloor
Cybersicherheit ist ein Muss für IT **und** OT!

Information Technology (IT)

Operational Technology **(OT)**

Cloud

Software für vertikale Integration

Edge

Controller-/Automatisierungsplattformen

Feldgeräte

Entwicklung von Low-Code-Apps

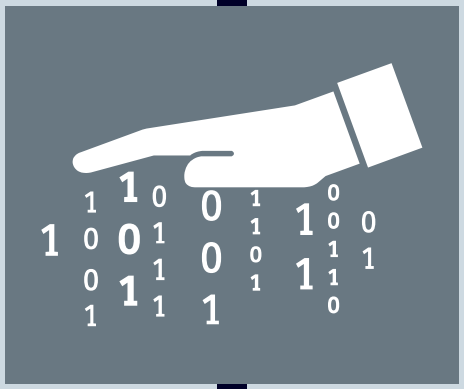
Kommunikations-plattformen

Cybersicherheit

SIEMENS

IT und OT im Vergleich

Büro-Netzwerke	IT	OT	Industrielle Netze, Bussysteme
Vertraulichkeit			**Verfügbarkeit**
Integrität			Integrität
Verfügbarkeit			Vertraulichkeit



Abgrenzung und Definition
Verantwortung
Topologie und Dateninhalte
Verfügbarkeit, Standort und Robustheit der Komponenten
Deterministik und Echtzeitanforderungen
Produktlebenszyklus / Updates

SIEMENS

Industrial Security

BSI[1]: Top 10 Bedrohungen bei ICS-Systemen[2]

- Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware
- Menschliches Fehlverhalten und Sabotage
- Social Engineering und Phishing
- Internet-verbundene Steuerungskomponenten
- Technisches Fehlverhalten und höhere Gewalt

- Infektion mit Schadsoftware über Internet und Intranet
- Kompromittierung von Extranet und Cloud-Komponenten
- (Distributed) Denial of Service Angriffe
- Einbruch über Fernwartungszugänge
- Soft- und Hardwareschwachstellen in der Lieferkette

1) Bundesamt für Sicherheit in der Informationstechnik
2) Systeme zur Fertigungs- und Prozessautomatisierung
Quelle: BSI-Veröffentlichung zur Cyber-Sicherheit 2019

SIEMENS

Industrial Security
BSI[1]: Top 10 Bedrohungen bei ICS-Systemen[2]

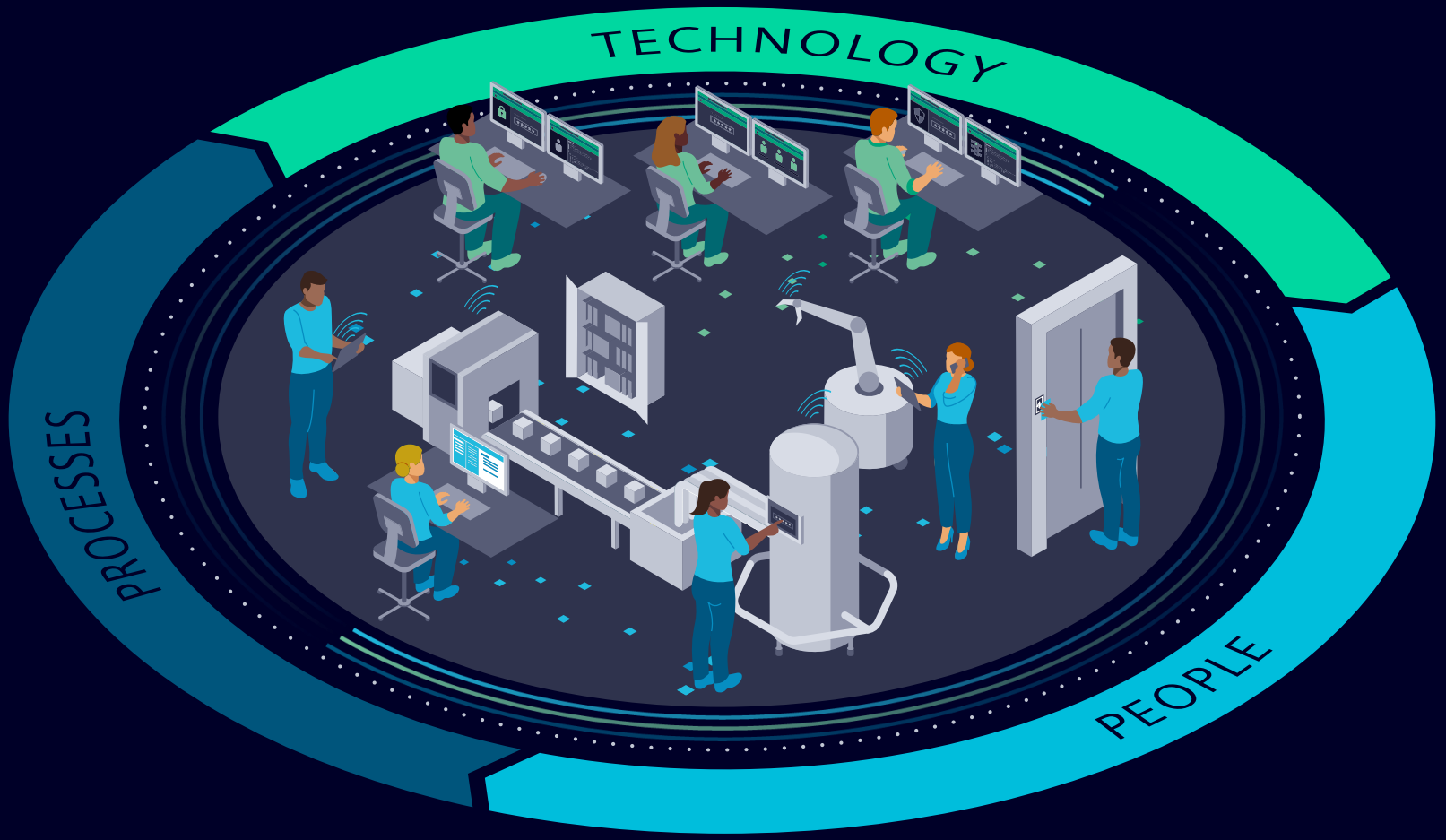
- **Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware**
- **Menschliches Fehlverhalten und Sabotage**
- **Social Engineering und Phishing**
- Internet-verbundene Steuerungskomponenten
- **Technisches Fehlverhalten und höhere Gewalt**

- Infektion mit Schadsoftware über Internet und Intranet
- Kompromittierung von Extranet und Cloud-Komponenten
- (Distributed) Denial of Service Angriffe
- Einbruch über Fernwartungszugänge
- **Soft- und Hardwareschwachstellen in der Lieferkette**

1) Bundesamt für Sicherheit in der Informationstechnik
2) Systeme zur Fertigungs- und Prozessautomatisierung
Quelle: BSI-Veröffentlichung zur Cyber-Sicherheit 2019

SIEMENS

Ein ganzheitlicher Cybersecurity-Ansatz wird von drei Hauptsäulen geleitet:
Menschen, Technologien und Prozesse



Richtlinien und Prozesse

Funktionale Cybersecurity-Maßnahmen

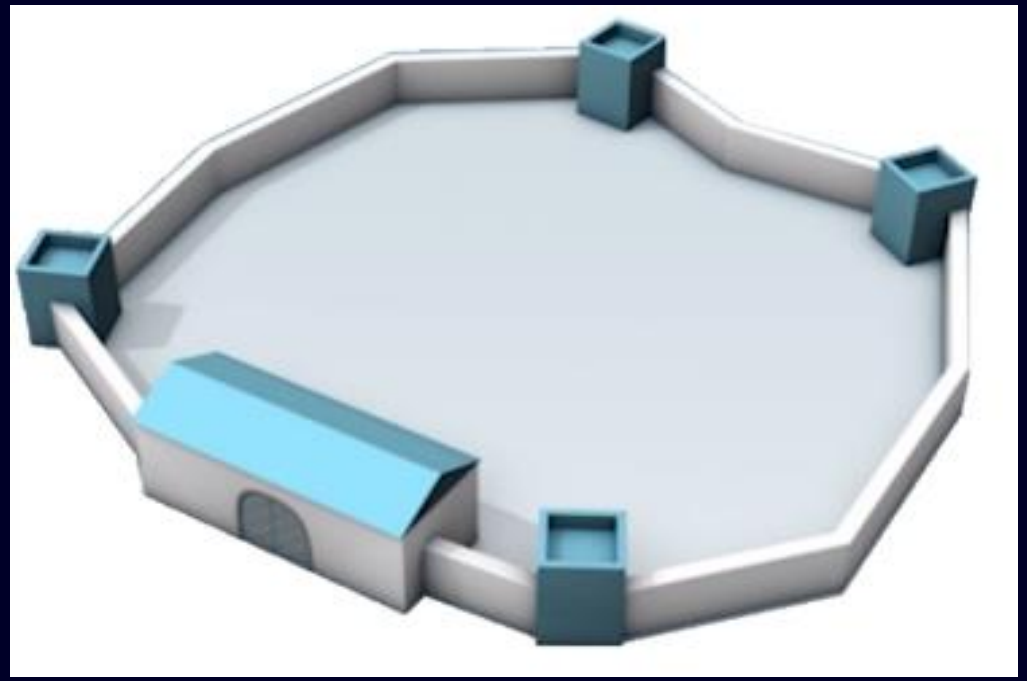
Kompetenz, Akzeptanz

SIEMENS

Schutz der Produktivität – aber wie? Das Defense-in-Depth-Konzept von Siemens bietet mehrschichtigen Schutz

Von der „Großen Mauer“

- Undurchdringliche Mauer
- Einschichtiger Schutz
- Ein Angriffspunkt

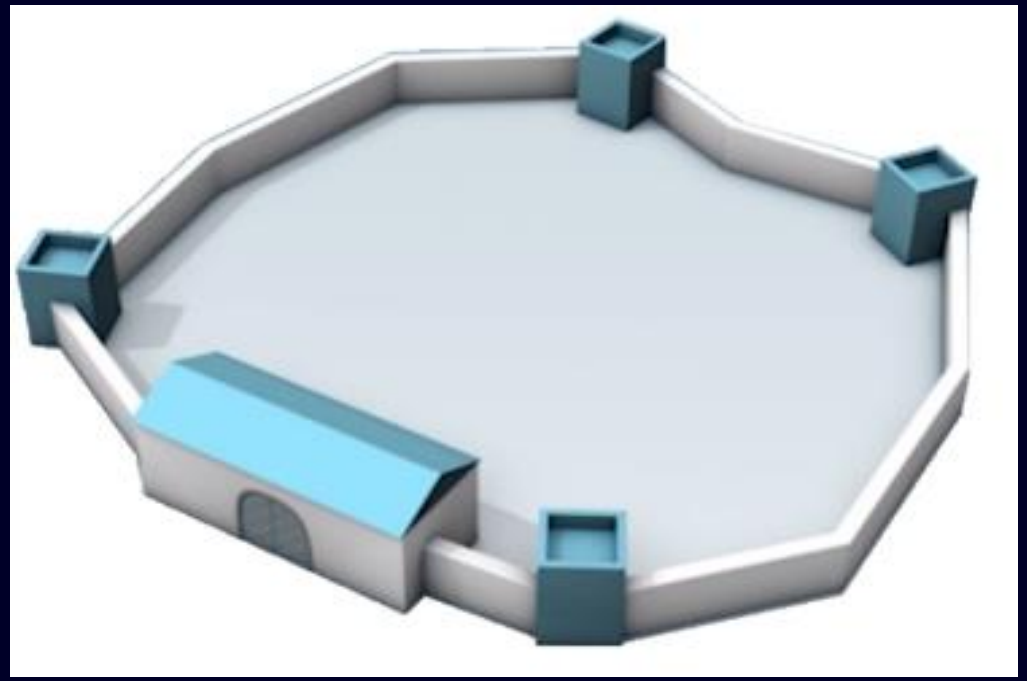


SIEMENS

Schutz der Produktivität – aber wie? Das Defense-in-Depth-Konzept von Siemens bietet mehrschichtigen Schutz

Von der „Großen Mauer“

- Undurchdringliche Mauer
- Einschichtiger Schutz
- Ein Angriffspunkt



zu „Defense in Depth“

- **Mehrschichtiger** Schutz
- Jede Schicht schützt die anderen Schichten
- Ein Angreifer benötigt an jedem Übergang Zeit und Aufwand.

SIEMENS

Only a holistic Industrial Security concept can be effective against cyber-threats

Security threats demand action

Anlagensicherheit

- Physischer Zugangsschutz
- Security Richtlinien
- Security Monitoring

Netzwerksicherheit

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

Systemintegrität

- Systemhärtung
- Patch-Management
- Authentifizierung und Zugriffsschutz

SIEMENS

Netzwerksicherheit

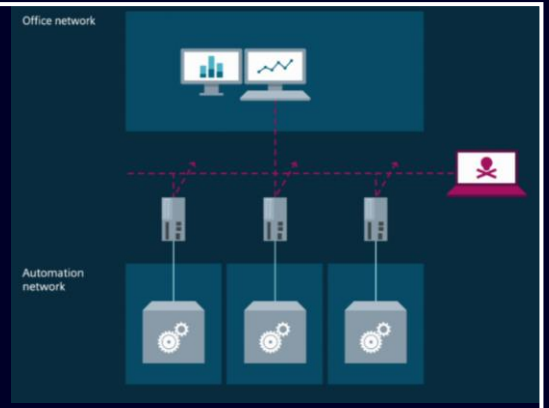
SIEMENS

Anwendungsfälle Netzwerksicherheit

Zellenschutz

Schutz von Geräten ohne eigene Netzwerksicherheits-Mechanismen innerhalb einer Automatisierungs-zelle.

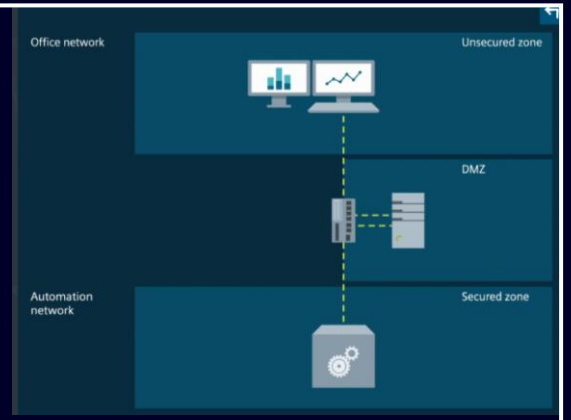
➔ Zugriff auf Automatisierungszelle wird über Firewall-Mechanismen abgesichert.



Demilitarisierte Zone (DMZ)

Schutz durch Datenaustausch über eine DMZ und Vermeidung eines direkten Zugriffs auf das Automatisierungsnetzwerk.

➔ Eine Firewall kontrolliert den Datenverkehr zwischen den Netzwerken und der DMZ.



Bedarfsgerechter Zugriff auf OT-Netzwerke

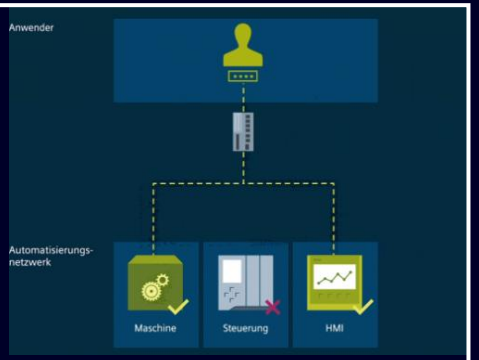
Sicherer und bedarfsgerechter Zugriff auf OT-Anwendungen und mit Zero Trust-Prinzipien.

➔ Teilnehmer müssen identifiziert und autorisiert werden, bevor sie Zugriff auf Systeme des Produktionsnetzwerks erhalten.

Benutzerspezifische (dynamische) Firewall

Zugriff auf Netzwerkbereiche und Endgeräte werden personen- und rollenabhängig eingeschränkt.

➔ Benutzerspezifische Firewall-Regeln werden mit den Industrial Security Appliances SCALANCE S temporär angelegt.



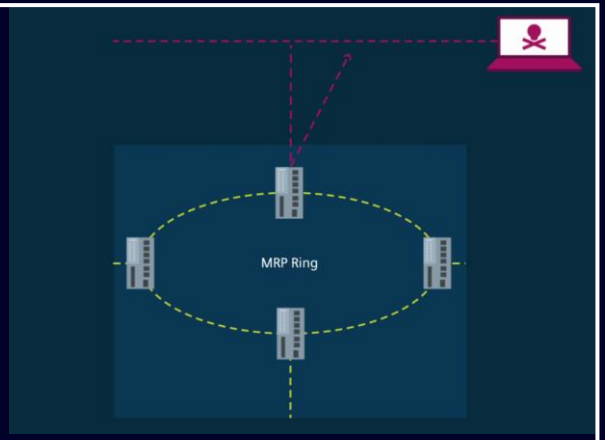
SIEMENS

Anwendungsfälle Netzwerksicherheit

Redundanz

Erhöhte Zuverlässigkeit und Verfügbarkeit segmentierter Netzwerke durch redundante Anbindung.

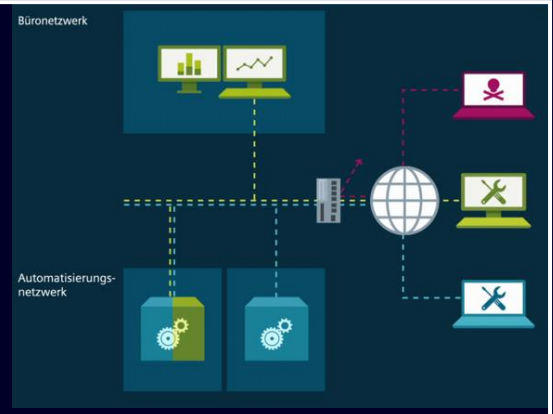
➔ Industrial Security Appliances SCALANCE S zur redundanten Anbindung von Ring-Topologien.



Fernzugriff

Abgesicherter Fernzugriff über Internet oder mobile Netzwerke zur Vermeidung von Spionage und Sabotage.

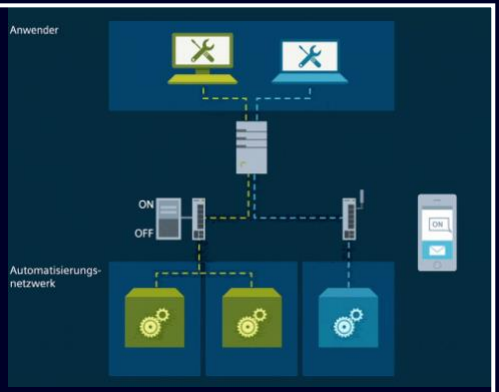
➔ Verschlüsselung der Daten-übertragung und Zugriffskontrolle auf dedizierte Endgeräte.



Fernzugriffsmanagement

Einfacher und gesicherter Fernzugriff für Teleservice und Fernwartung

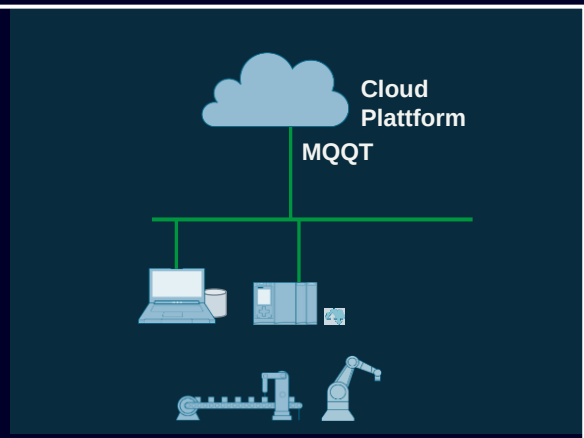
➔ Gesicherte VPN-Tunnel-Verbindung mit SINEMA Remote Connect via digitalem Eingang oder SMS aktivierbar.



Sichere Cloud-Anbindung

Vom Sensor in die Cloud - sichere und einfache Anbindung an Cloud-Plattformen

➔ Sichere Security Konzepte mit CloudConnect für Bestands- und Neuanlagen.



SIEMENS

Systemintegrität

Anlagensicherheit

Netzwerksicherheit

System-integrität

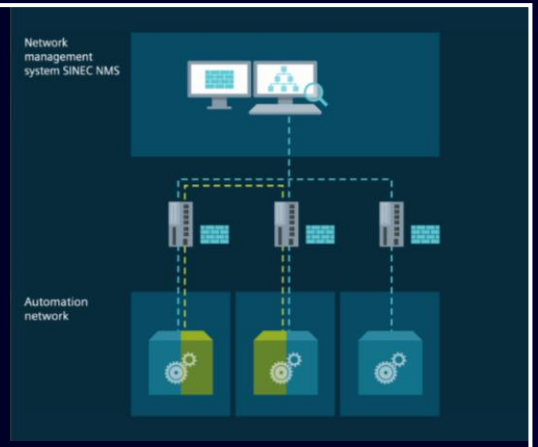
SIEMENS

Anwendungsfälle Systemintegrität

Zentrales Firewall-Management

Zentrale Konfiguration und Verwaltung der Regelsätze dezentraler Zellenfirewalls.

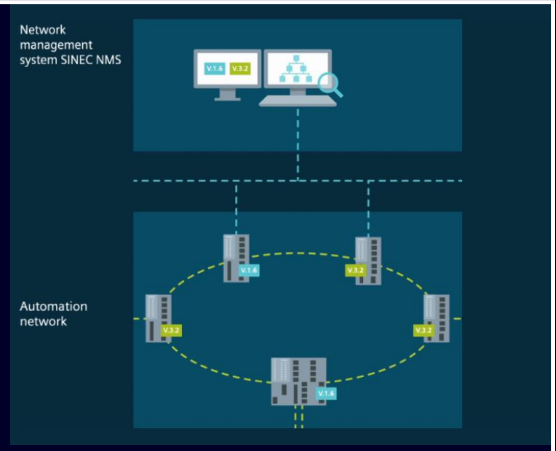
➔ Grafische und regelbasierte Konfiguration aller zulässigen Kommunikationsbeziehungen an Zonenübergängen



Zentrale Firmwareupdates

Geräteunabhängige und gleichzeitige Verteilung aktueller Firmwareupdates.

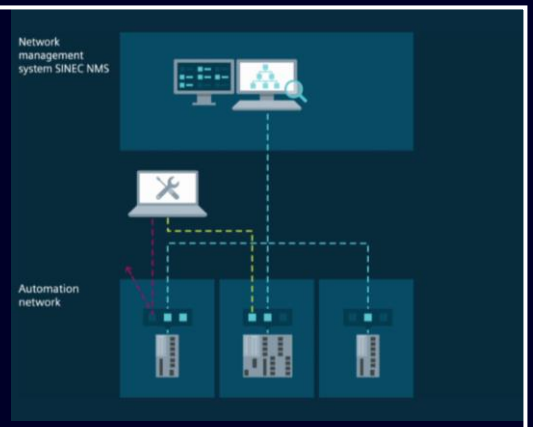
➔ Beseitigung von Software-Schwachstellen durch regelmäßige Firmware-aktualisierung



Gerätehärtung

Regelbasierte Gerätehärtung durch Deaktivieren nicht benötigter Dienste und Ports

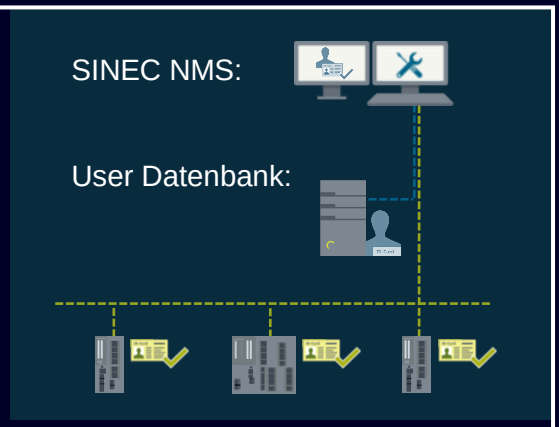
➔ Reduzierung der Angriffs-oberfläche überwachter Netzwerkkomponenten



Zentrale Benutzerverwaltung

Kontrollierter und nachvollziehbarer Gerätezugriff mit zentralisierter Benutzer-verwaltung

➔ Integration bestehender Benutzerdatenbanken, wie Active Directory



SIEMENS

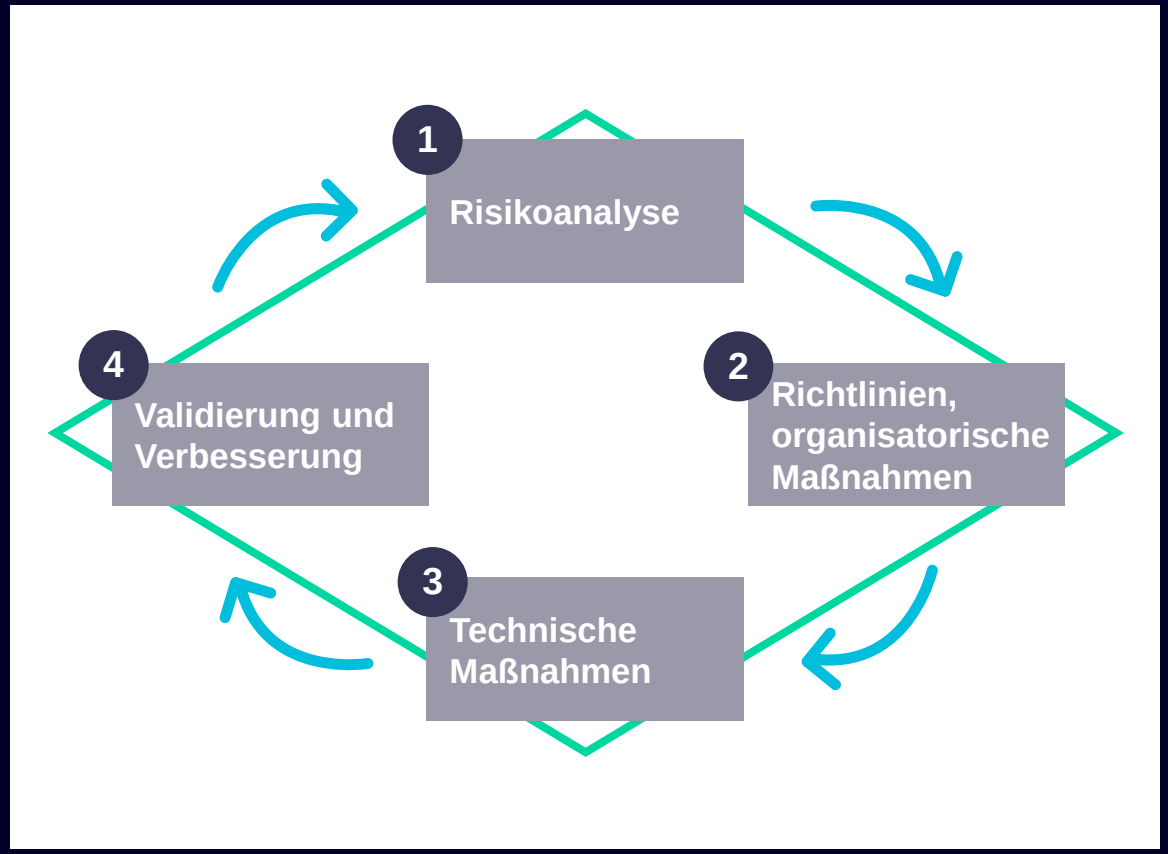
Anlagensicherheit

SIEMENS

Industrial Security
Security-Management

Security-Management-Prozess

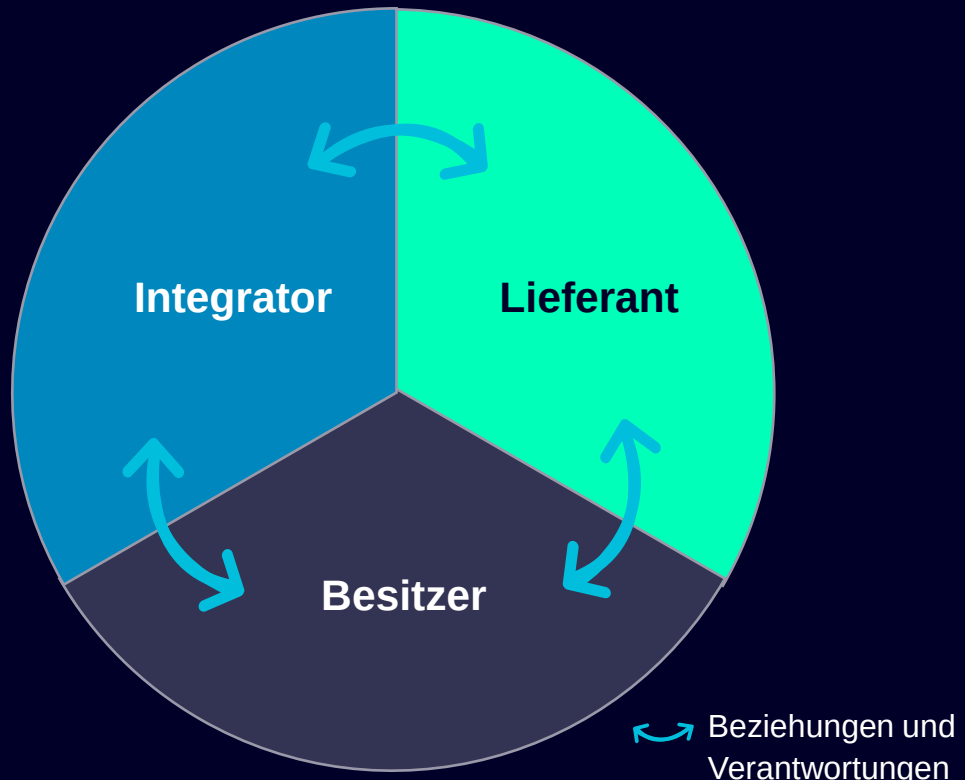
- Risikoanalyse mit Definition von Risikominderungsmaßnahmen
- Festlegung von Richtlinien und Koordinierung organisatorischer Maßnahmen
- Koordination technischer Maßnahmen
- Regelmäßige/ereignisabhängige Wiederholung der Risikoanalyse



Security-Management ist unverzichtbar für ein durchdachtes Sicherheitskonzept

SIEMENS

Akteure gemäß IEC 62443



SIEMENS

Security ist nicht nur eine Firewall!

SIEMENS

Kontakt

Benjamin Schrunner
Head of Digital Connectivity and Power Products CEE
RC-AT DI PA PR DCP
Siemensstraße 90
1210 Wien
Österreich

Mobil +43 664 80117 15362

E-Mail industrial.communication.at@siemens.com

SIEMENS

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.