Strength Networks / IT Security

Pharma Forum 2022

Warum ist Industrielle CyberSecurity so wichtig?

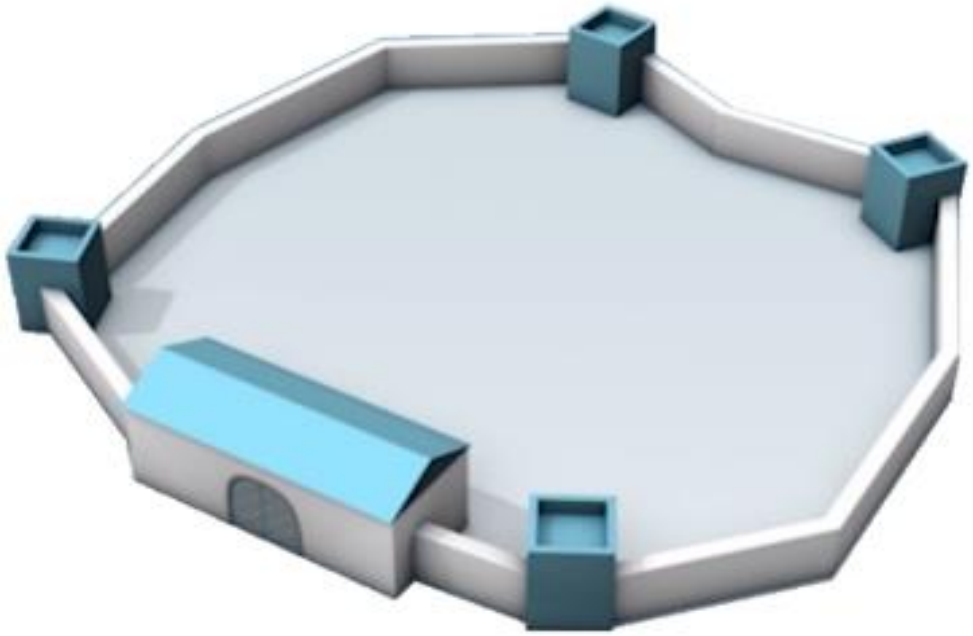
Cyberkriminalität ist weit verbreitet und kostet der Weltwirtschaft US$ 6000 Milliarden jährlich.
Cyber Angriffe betreffen Firmen aller Größen, in allen Märkten.
Beispiel: Colonial Pipeline Inc.

Schutz der Produktivität – aber wie?

Das Defense-in-Depth-Konzept 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.

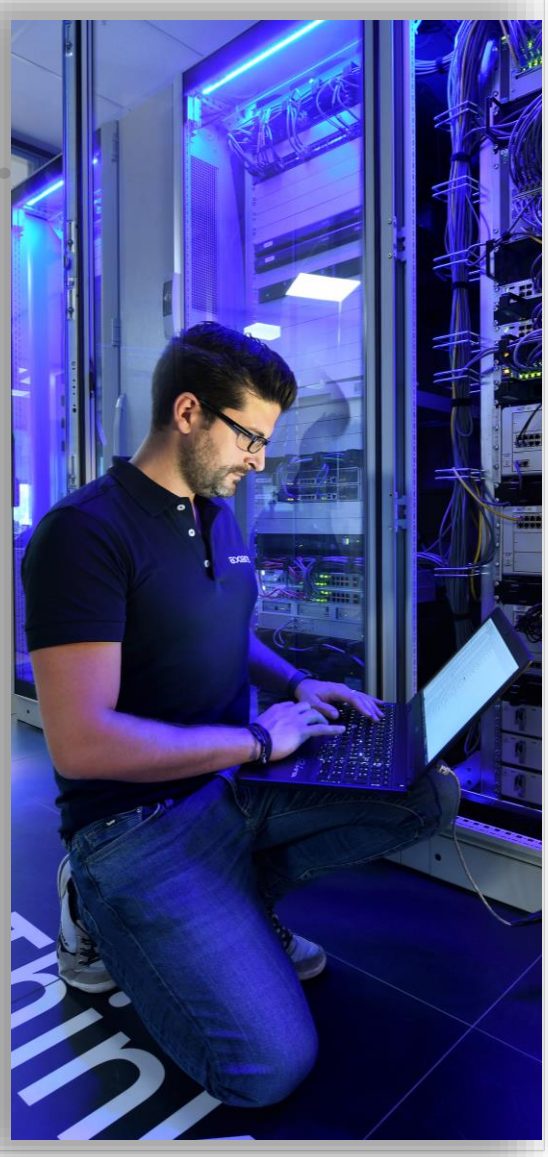
IT/OT Unterschiede

OT

- Interoperabilität
- Alternder Maschinenpark
- Vorausschauende (Predictive) Wartung
- Operative Exzellenz

IT

- Datenverfügbarkeit und -integrität
- Verwaltung von Geschäftsinformationen
- Vernetzte Nutzer und Anlagen
- Globale Sicherheit



Actemium + Axians:
Kombination von OT und IT zur Förderung der Smart und Secure Industry

ACTEMIUM axians

Industrial performance – Powered by IT

Kompetenzen und strategischen Partnerschaften

OT

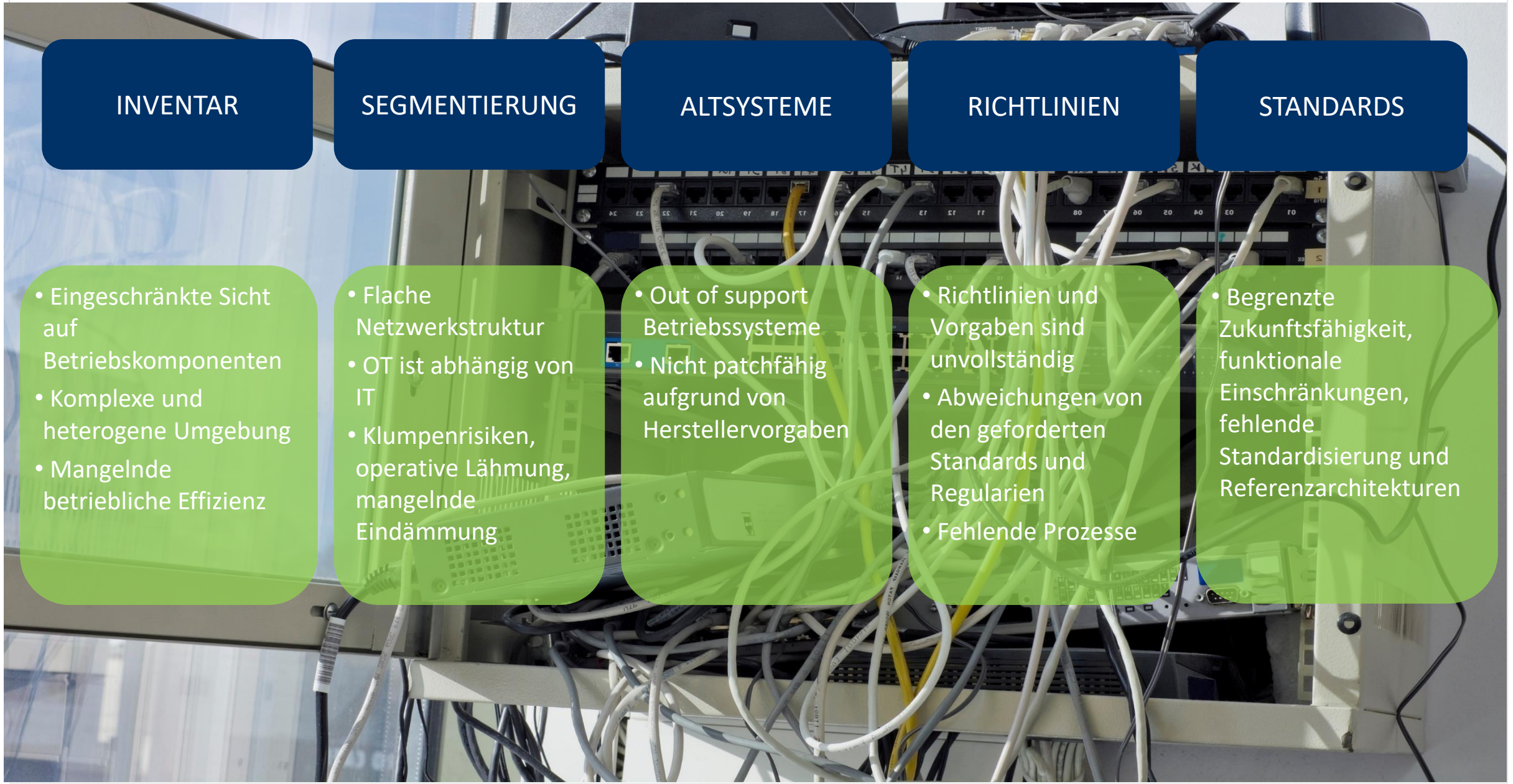
- ✓Siemens Solution Partner
  - Pharma/Chemie/Food
  - Simatic IT – PCS 7
  - Industrial Strength Networks
- ✓ABB Value Provider
- ✓Schneider
- ✓OSISoft

ACTEMIUM

IT

- ✓CISCO
- ✓Microsoft
- ✓VMWare
- ✓Fortinet
- ✓Nozomi Networks
- ✓Qualys
- ✓Pentera

axians



INVENTAR	SEGMENTIERUNG	ALTSYSTEME	RICHTLINIEN	STANDARDS
• Eingeschränkte Sicht auf Betriebskomponenten • Komplexe und heterogene Umgebung • Mangelnde betriebliche Effizienz	• Flache Netzwerkstruktur • OT ist abhängig von IT • Klumpenrisiken, operative Lähmung, mangelnde Eindämmung	• Out of support Betriebssysteme • Nicht patchfähig aufgrund von Herstellervorgaben	• Richtlinien und Vorgaben sind unvollständig • Abweichungen von den geforderten Standards und Regularien • Fehlende Prozesse	• Begrenzte Zukunftsfähigkeit, funktionale Einschränkungen, fehlende Standardisierung und Referenzarchitekturen

Mehrwert einer IT/OT-Allianz

Challenge

Ersetzen und Upgrade der bestehende Infrastruktur

Antwort

- Nutzung einer Virtualisierungslösung welche von "IT" gehostet und zur Verfügung gestellt wird.
- Nutzung der DataCenter Location von IT (Ideale Umgebungsbedigungen, Monitoring, Sicherheit..)
- Virtualisierung aller Physischen Komponenten
- Vertikale wie auch Horizontale Netzwerk-Segmentierung für Package Units
- Virtuelle Lösung für Windows 10 Rechner
- Monitoring und Alerting in der Infrastruktur um frühzeitig Ausfälle zu merken

Manufacturing Cybersecurity Remediation Program

Challenge

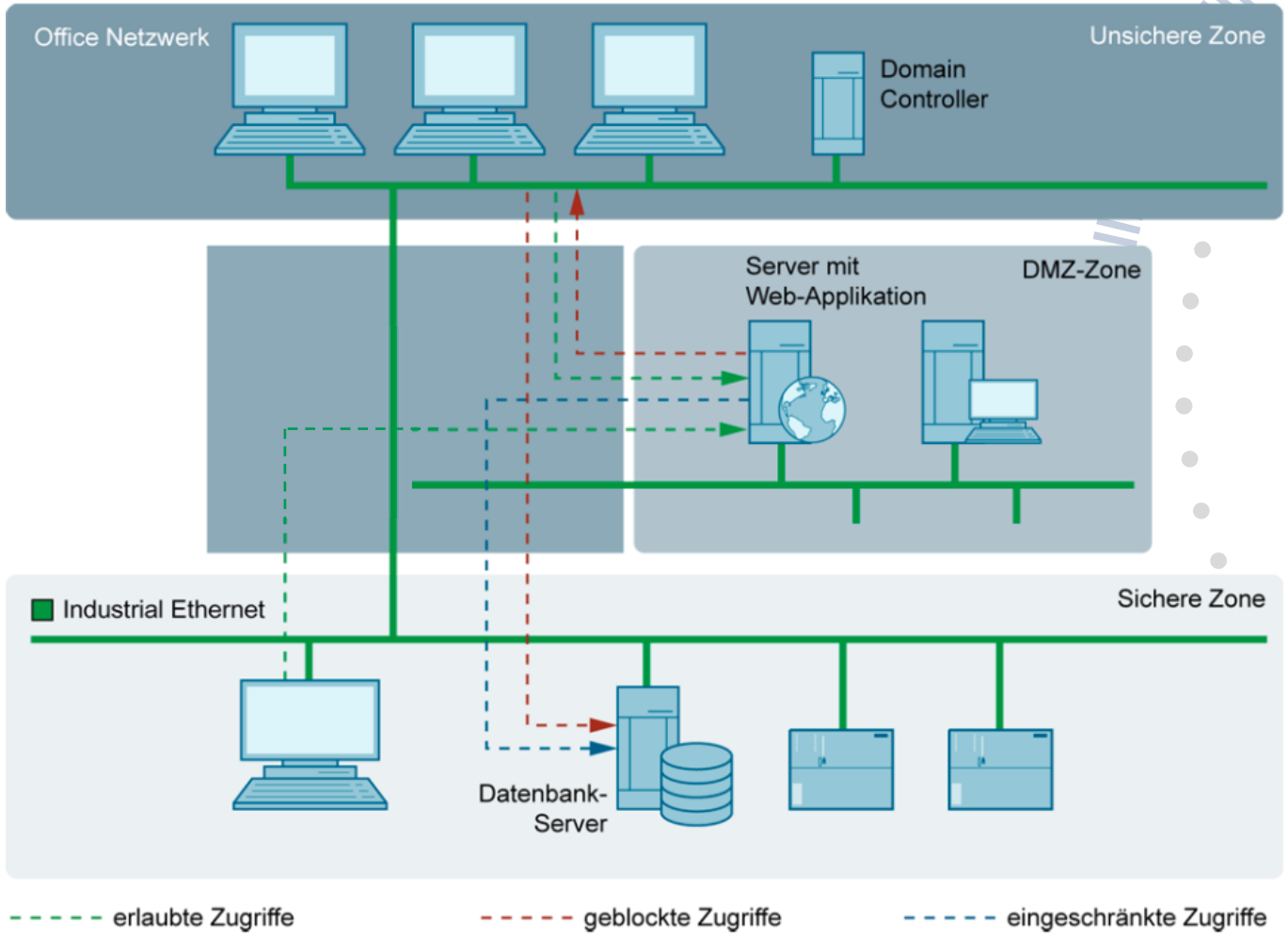
Industrial Cybersecurity in bestehender Infrastruktur und Netzwerke einarbeiten.

Antwort

- Erstellen und implementieren von Cybersecurity Policies und Abläufe
- Erstellen eines OT Asset Inventory und implementieren von Security Monitoring in Manufacturing Netzwerke
- Definieren und implementieren von Netzwerk-Trennung und Segmentierung
- Implementieren von üblichen Security Dienste (Access Management, Malwareschutz…)

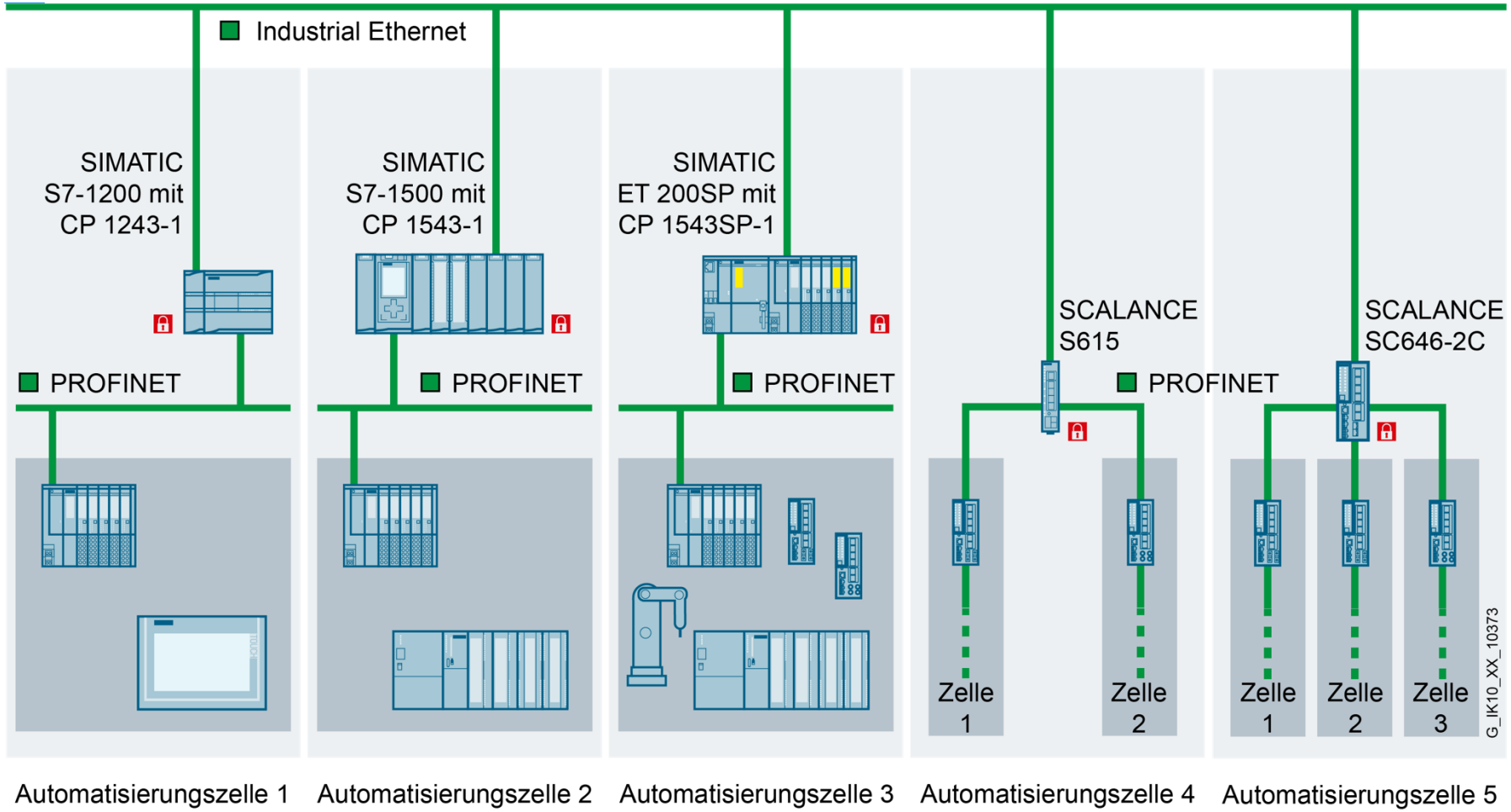
Unterschiedliche Anwendungszwecke

Vertikale Segmentierung für zentrales Prozessleitsystem



Unterschiedliche Anwendungszwecke

Horizontale Zellen-Segmentierung für Produktionsanlagen oder Package Units



Product Lifecycle und Herstellerabhängigkeit

Defense in Depth

basierend auf IEC 62443

Siemens Produkte und Systeme mit integrierter Security

Know-how and copy protection

Authentication and user management

Firewall and VPN

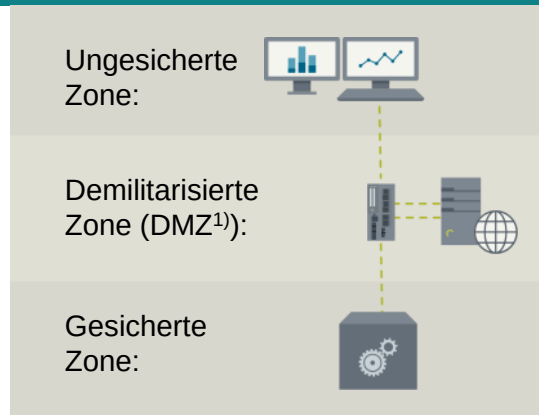
System hardening, continuous monitoring and anomaly detection

Anwendungsfälle Netzwerksicherheit

DMZ

Schutz durch Datenaustausch über eine DMZ[1)] und Vermeidung eines direkten Zugriffs auf das Automatisierungsnetzwerk.

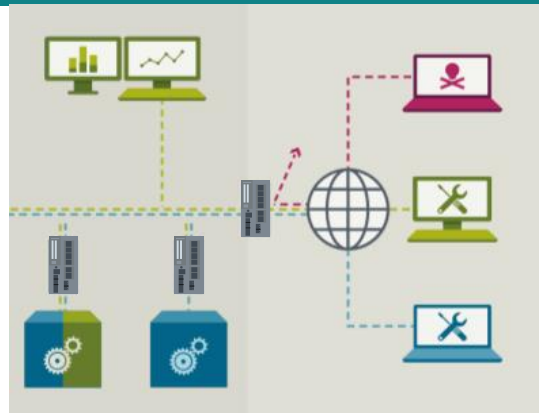
➔ Eine Firewall kontrolliert den Datenverkehr zwischen den Netzwerken und der DMZ[1)].



Fernzugriff

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

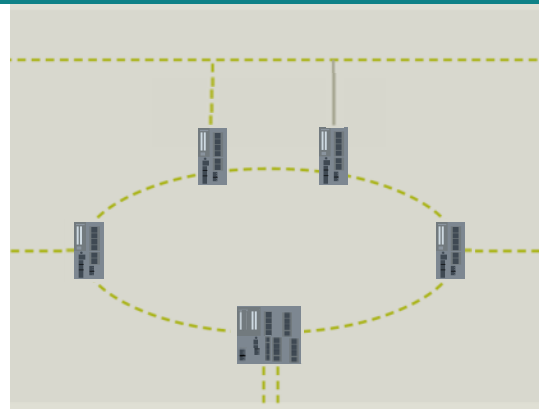
➔ Verschlüsselung der Daten-übertragung und Zugriffskontrolle auf dedizierte Endgeräte



Redundanz

Erhöhte Zuverlässigkeit und Verfügbarkeit segmentierter Netzwerke durch redundante Anbindung.

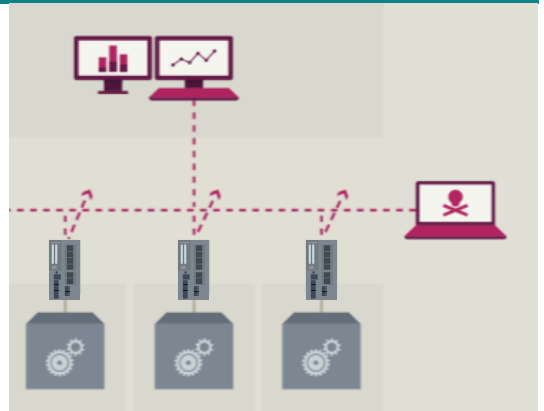
➔ Industrial Security Appliances SCALANCE S zur redundanten Anbindung von Ring-Topologien



Zellenschutz

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

➔ Zugriff auf Automatisierungszelle wird über Firewall-Mechanismen abgesichert.



Empfehlungen

KURZFRISTIG

- Schaffung von Bewusstsein und Verantwortung
- Neuausrichtung der Zusammenarbeit von OT und IT
- Bestandsaufnahmen, Technik und Compliance

MITTELFRISTIG

- Planung und Neugestaltung von OT/IT Architekturen
- Festlegung minimaler Cyber Security Standards für Neubeschaffungen und Altsysteme

LANGFRISTIG

- Migration von Produktionssystemen auf gesicherte Infrastrukturen
- Ersatz und Modernisierung von Altsystemen

Gemeinsame OT Cyber Security Journey

FOKUS AUF DAS KERNGESCHÄFT

- SOC Services
- Managed Services

PROZESSE

- Identity & Access Management
- Vulnerability Management

TECHNISCHE MAßNAHMEN

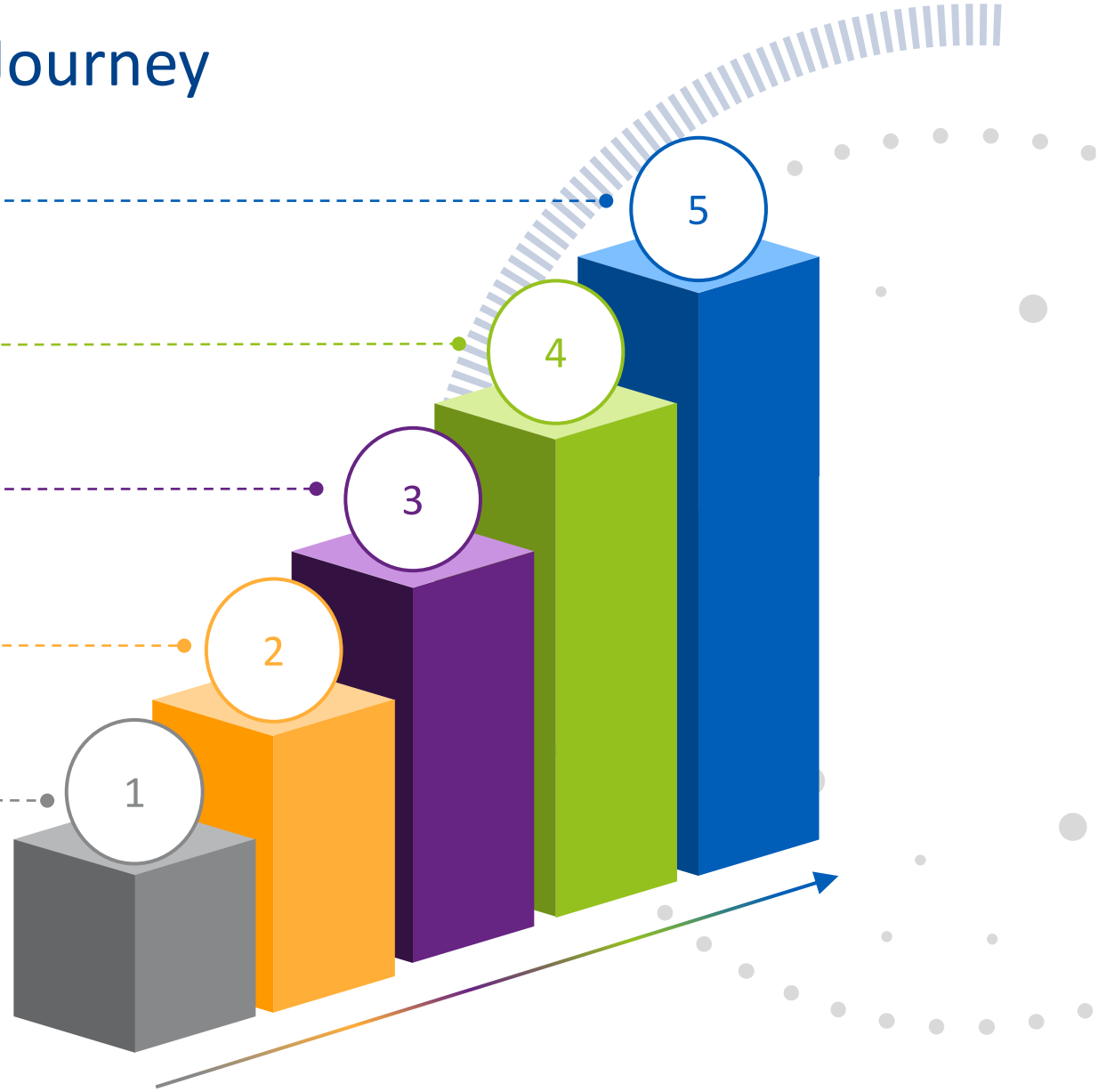
- Secure OT/IT Network
- Secure Legacy Systems
- Secure OT/IT Platform
- Secure Communication

BESTANDSAUFNAHME

- Asset Inventory
- Guidelines & Policies
- Network Visibility

STANDORTBESTIMMUNG

- Security Assessment
- Compliance Check
- Security Awareness



Industrial Security
Vom Risiko zur Ausfallsicherheit

Ungeschütztes Business

- Personen und Vermögenswerte, die einem Risiko ausgesetzt sind
- Störungen, Sabotage und Diebstahl
- Kosten und Haftung
- Reputationsschaden

Geschütztes Business

- Sichere und widerstandsfähigere Umgebungen
- Nachhaltigere Geschäftstätigkeit, schnellere Wiederaufnahme des Betriebs
- Verbesserte Anlagenverfügbarkeit und Rentabilität
- Vertrauen zu Kunden und Aktionären

VIELEN DANK

PharmaForum 2022
26.04.2022
Marc Reymann