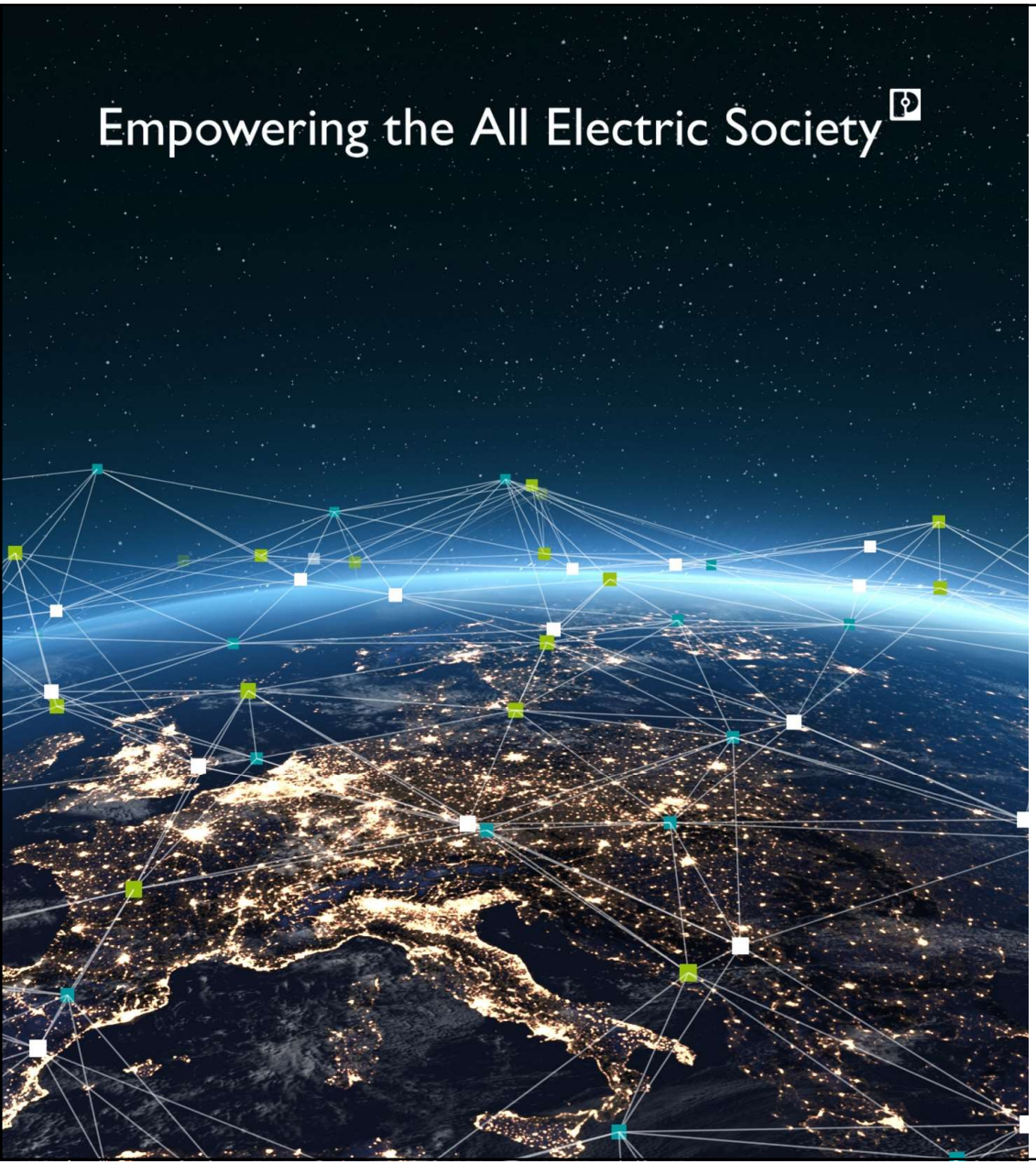
Hinweis: Urheberrechtsschutz und Disclaimer

Die Informationen und Beispiele dieser Präsentation dienen als Hilfestellung zur Umsetzung der Richtlinien und Normen. Sie erheben keinerlei Anspruch auf Rechtsverbindlichkeit und Vollständigkeit. PHOENIX CONTACT übernehmen keinerlei Haftung für etwaige Fehler, die in den Seminaren mündlich oder schriftlich übermittelt werden oder in den Unterlagen enthalten sind.



100 Jahre Leidenschaft für Technologie und Innovation

Willkommen

Ganzheitliche OT-Security-Betrachtung für Hersteller und Betreiber

PHOENIX CONTACT

Wer bin ich?

Hauke Kästing

PHOENIX CONTACT Deutschland GmbH

Industry Management and Automation

Competence Center Services

Industrial Security & Netzwerk

Dringenauer Str. 30

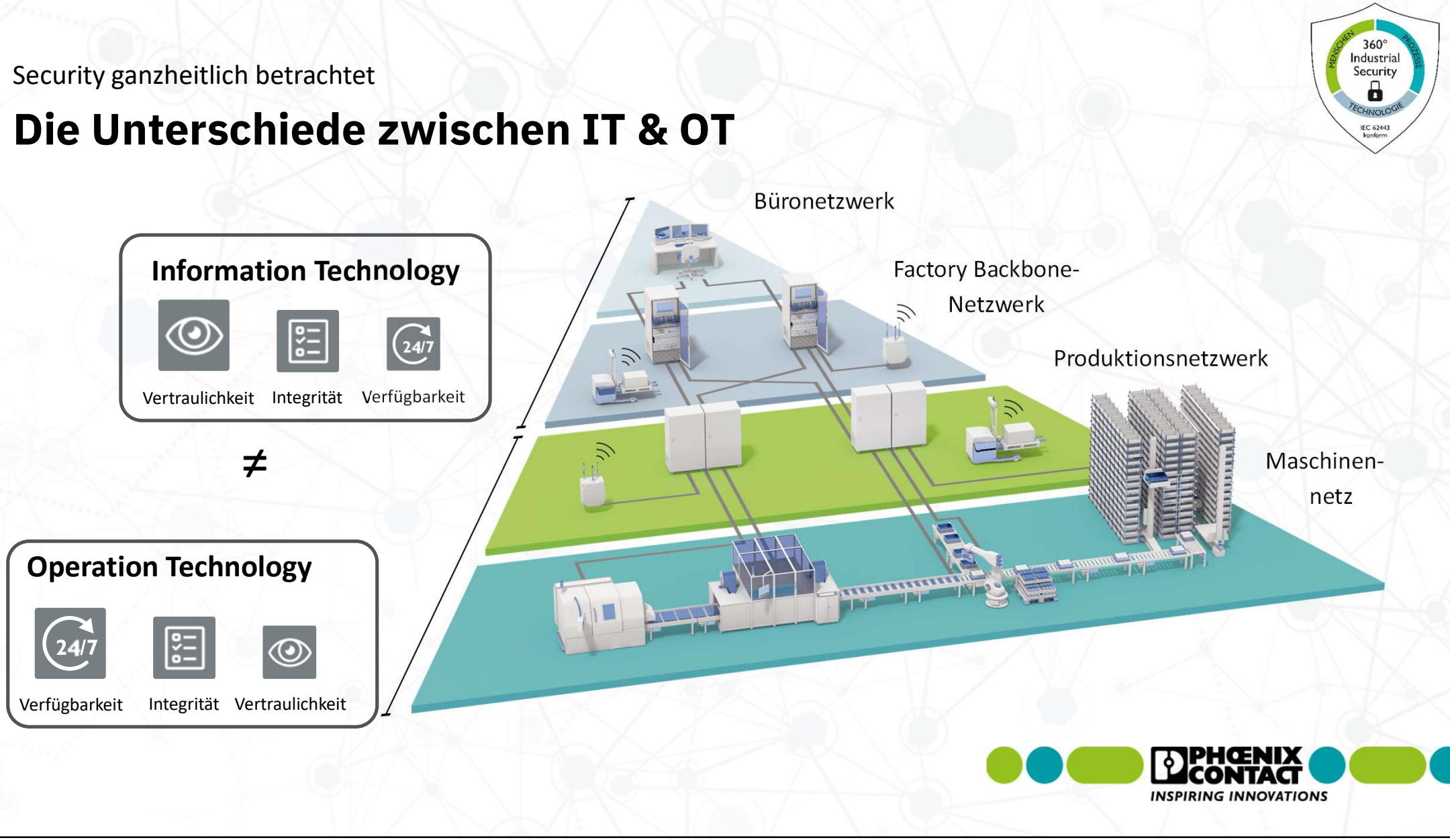
31812 Bad Pyrmont

Fon: +49 5281 946- 2113

Email: hauke.kaesting@phoenixcontact.de

Security ganzheitlich betrachtet

Die Unterschiede zwischen IT & OT



Security ganzheitlich betrachtet

OT-Security vs. IT Security

Unterschiedliche Prioritäten der Schutzziele

OT-Security	Eigenschaft	IT-Security
Verfügbarkeit Integrität Vertraulichkeit		Vertraulichkeit Integrität Verfügbarkeit
Ausfall nicht tolerierbar	Verfügbarkeit	Kurzer Ausfall tolerierbar
Schwierig	Neustart	Möglich
Große Herausforderung	Patch Management	Automatisiert möglich
7-20 Jahre	Lebenszeit HW	3-5 Jahre
Verteilt	Know How	Zentralisiert
Ja	Echtzeit	Nein
In der Regel nicht vorhanden	Risk Owner	In der Regel vorhanden
In der Regel nicht vorhanden	Asset Management	Vorhanden

Komplettübersicht IEC 62443

IEC 62443: Aufbau

Allgemein	Richtlinien und Verfahren	System	Komponente
1-1 Technologie, Konzepte und Modelle	2-1 Anforderungen an ein IACS-Sicherheitsmanagementsystem	3-1 Sicherheitstechnologien für IACS (TR)	4-1 Sicherer Lebenszyklus der Produktentwicklung
1-2 Master-Glossar der Begriffe und Abkürzungen	2-2 Sicherheitsschutzbewertung	3-2 Sicherheitsrisikobewertung und Systemdesign	4-2 Technische Sicherheitsanforderungen für IACS-Produkte
1-3 Kennzahlen zur Einhaltung der Systemsicherheit	2-3 Patch-Management im IACS-Umfeld (TR)	3-3 Systemsicherheits-anforderungen und Sicherheitsstufen	
1-4 Systemsicherheitslebenszyklus und Einsatzgebiet	2-4 Anforderungen an IACS-Lösungsanbieter		
	2-5 Implementierungsanleitung für IACS Asset Owner		
Definitionen Metriken	Sicherheitsanforderungen an Anlagenbesitzer und Lieferanten	Sicherheitsanforderungen an ein sicheres System	Sicherheitsanforderungen für sichere Komponenten

Funktionale Anforderungen

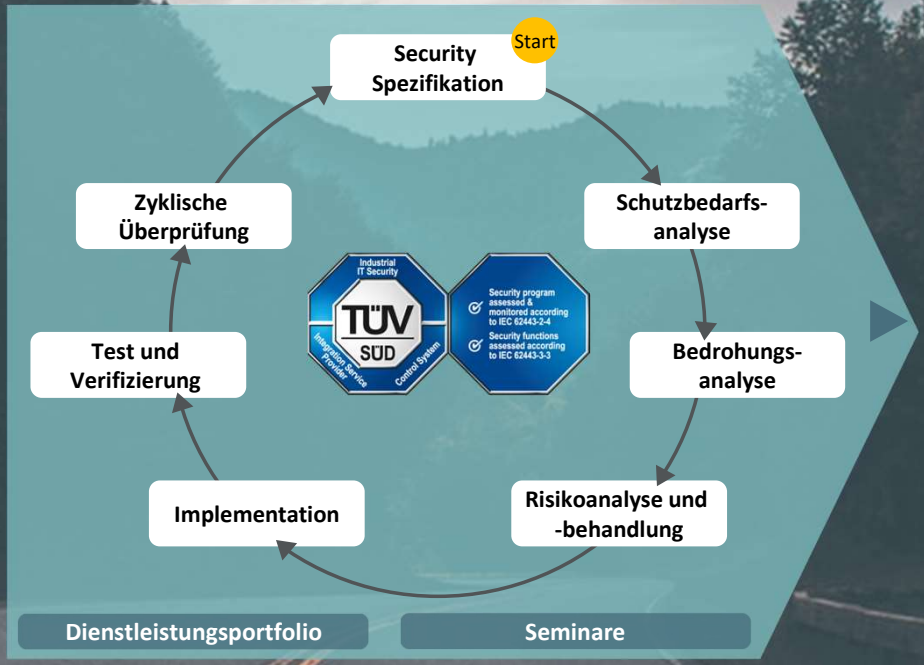
Prozessanforderungen

PHOENIX CONTACT
INSPIRING INNOVATIONS

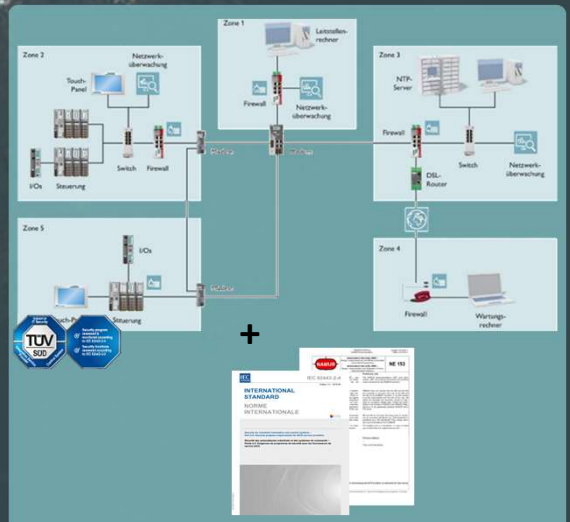
Möglichkeiten der Umsetzung

Ausgangsbasis:
Kundenanlageninformation

Vorgehensweise:
Security Design einer Automatisierungslösung



Ergebnis:
Blueprint & Dokumentation



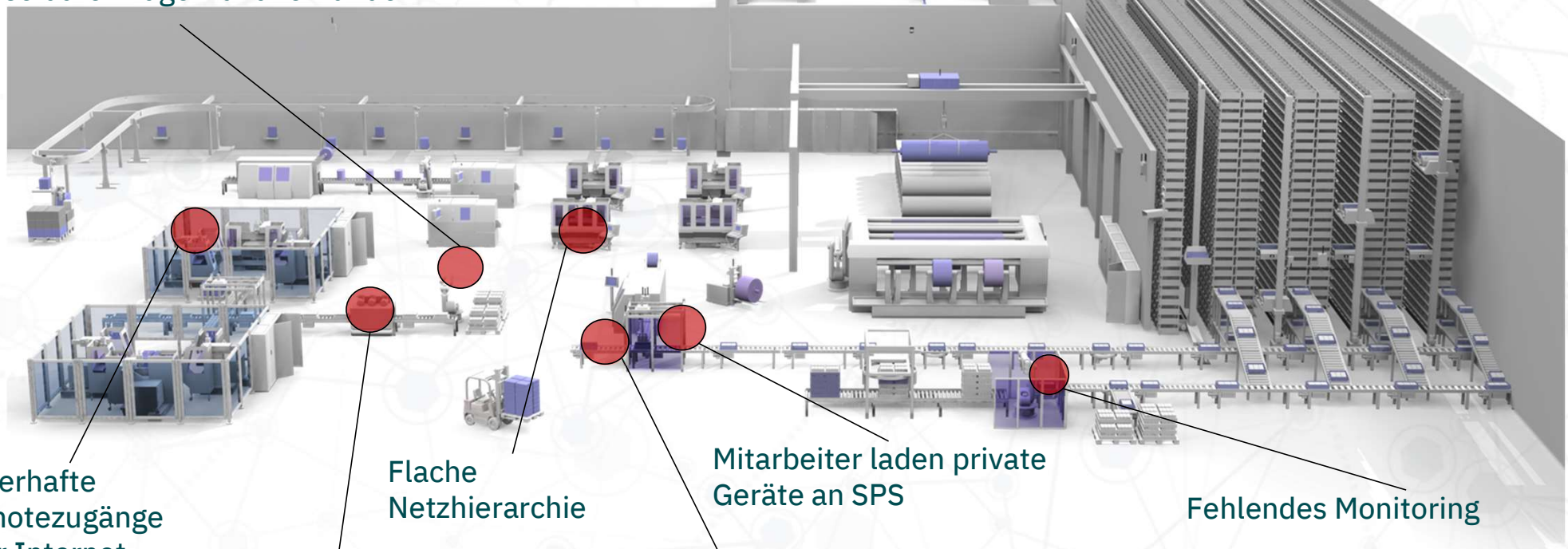
Security Design mit entsprechender Dokumentation der einzelnen Prozessschritte gemäß IEC 62443

Sicherstellung der Anlagenverfügbarkeit

Minimierung der Cyber-Sicherheitsrisiken durch individuelle Absicherungsstrategie

Kosteneffizienz durch Blueprint Ansatz

Bedrohungs- & Schwachstellenanalyse



Einkauf von Komponenten nur aufgrund funktional notwendiger Features

Dienstleister verwenden gleichen Wechseldatenträger für alle Kunden

Dauerhafte Remotezugänge über Internet

„Kernjuwelen“-Komponenten nicht redundant vorhanden

Flache Netzhierarchie

Sensible Informationen werden unverschlüsselt übertragen

Mitarbeiter laden private Geräte an SPS

Fehlendes Monitoring

Komplettübersicht IEC 62443

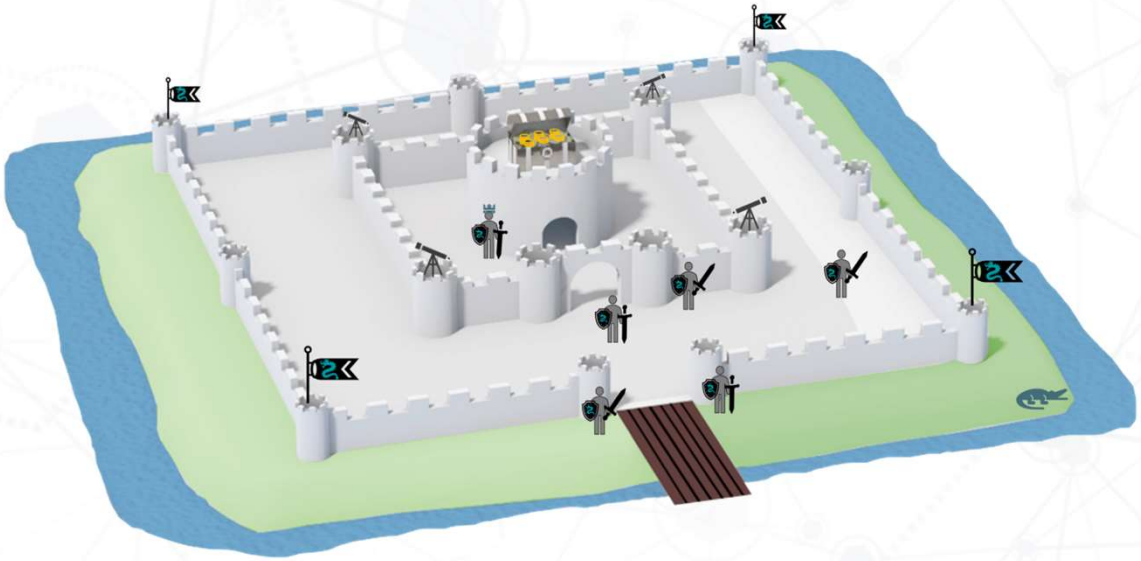
Anforderungen der IEC 62443-2-4

Wert	SP-Anford.-ID	Beschreibung
Mitarbeiter	SP.01.XX	Anforderungen an die Zuweisung von Personal durch den Dienstleister für Tätigkeiten in Zusammenhang mit der „Automatisierungslösung“
Zusicherung	SP.02.XX	Anforderungen an das Vertrauen, dass die IT-Sicherheitsleitlinien für die „Automatisierungslösung“ durchgesetzt werden
Systemaufbau	SP.03.XX	Anforderungen an die Auslegung der „Automatisierungslösung“
Drahtlose Verbindung (drahtlos)	SP.04.XX	Anforderungen an die Verwendung von Drahtlose Verbindungen in der „Automatisierungslösung“
SIS	SP.05.XX	Anforderungen an die Integration von PLT-Sicherheitseinrichtungen in die „Automatisierungslösung“
Konfigurationsverwaltung	SP.06.XX	Anforderungen an die Konfigurationssteuerung der „Automatisierungslösung“
Fernzugriff	SP.07.XX	Anforderungen an den Fernzugriff auf die „Automatisierungslösung“
Behandlung von Ereignissen	SP.08.XX	Anforderungen an die Behandlung von Ereignissen in der „Automatisierungslösung“
Verwaltung von Nutzerkonten	SP.09.XX	Anforderungen an die Verwaltung von Nutzerkonten in der „Automatisierungslösung“
Schutz gegen Schadsoftware	SP.10.XX	Anforderungen an den Einsatz von Anti-Malware in der „Automatisierungslösung“
Patch-Management	SP.11.XX	Anforderungen an die IT-Sicherheitsaspekte der Genehmigung und Installation von Softwarepatches
Datensicherung/ -wiederherstellung	SP.12.XX	Anforderungen an die IT-Sicherheitsaspekte der Datensicherung und Wiederherstellung

- Anforderungen an den Personaleinsatz
  - Kompetenz
  - Rollen/Verantwortung
  - Prozesse
  - Leitlinien
- Anforderungen an die Automatisierungslösung
  - Prozesse
  - Funktionen
  - Dokumentation

Security ganzheitlich betrachtet

Das „Defense in Depth“ Konzept

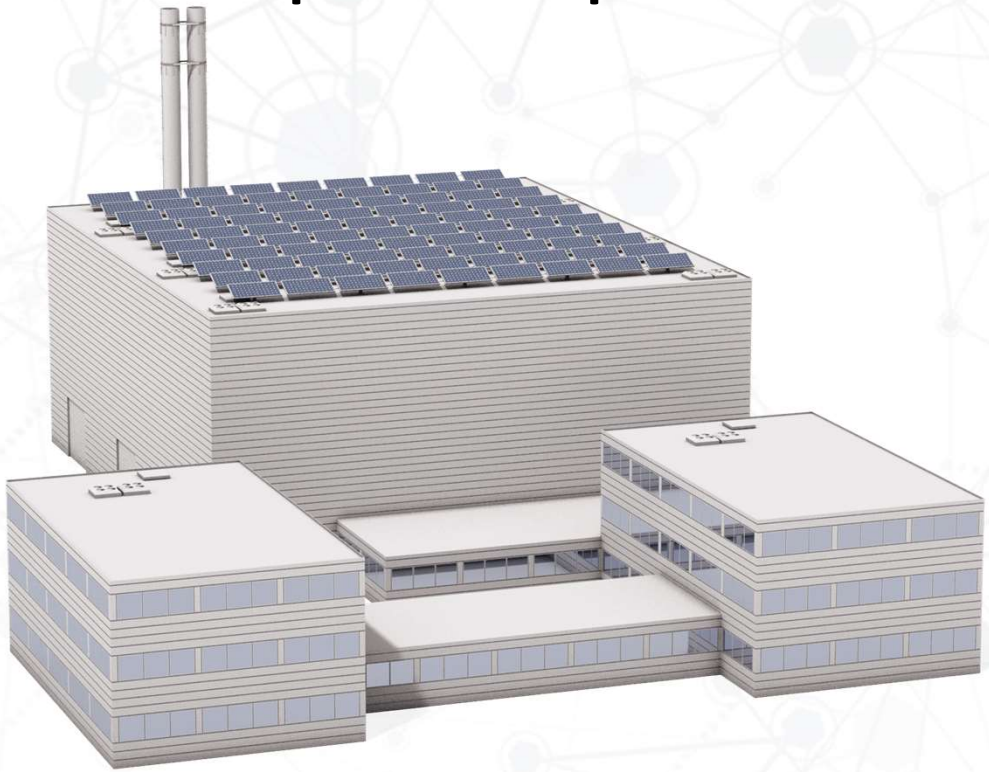


Mehrere Verteidigungslinien

- Wassergraben
- Mauern
- Wachtürme
- Bewaffnete Ritter
- Zugbrücke

Security ganzheitlich betrachtet

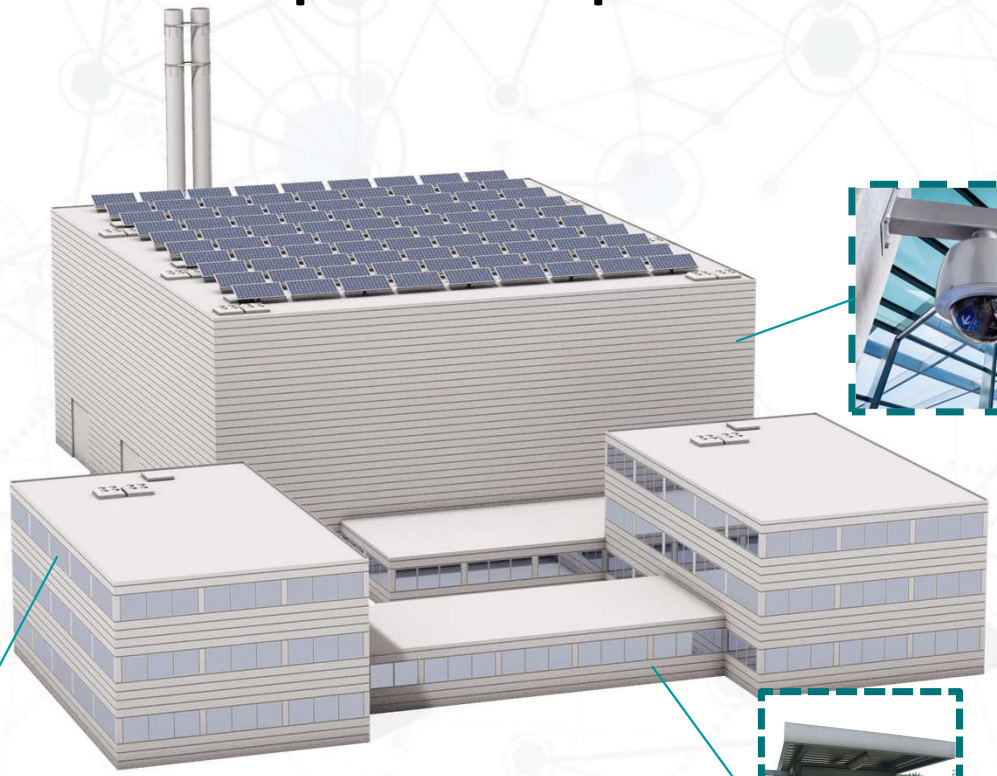
Das „Defense in Depth“ Konzept



- Unternehmensebene
- Netzwerkebene
- Produktebene

Security ganzheitlich betrachtet

Das „Defense in Depth“ Konzept



Unternehmensebene

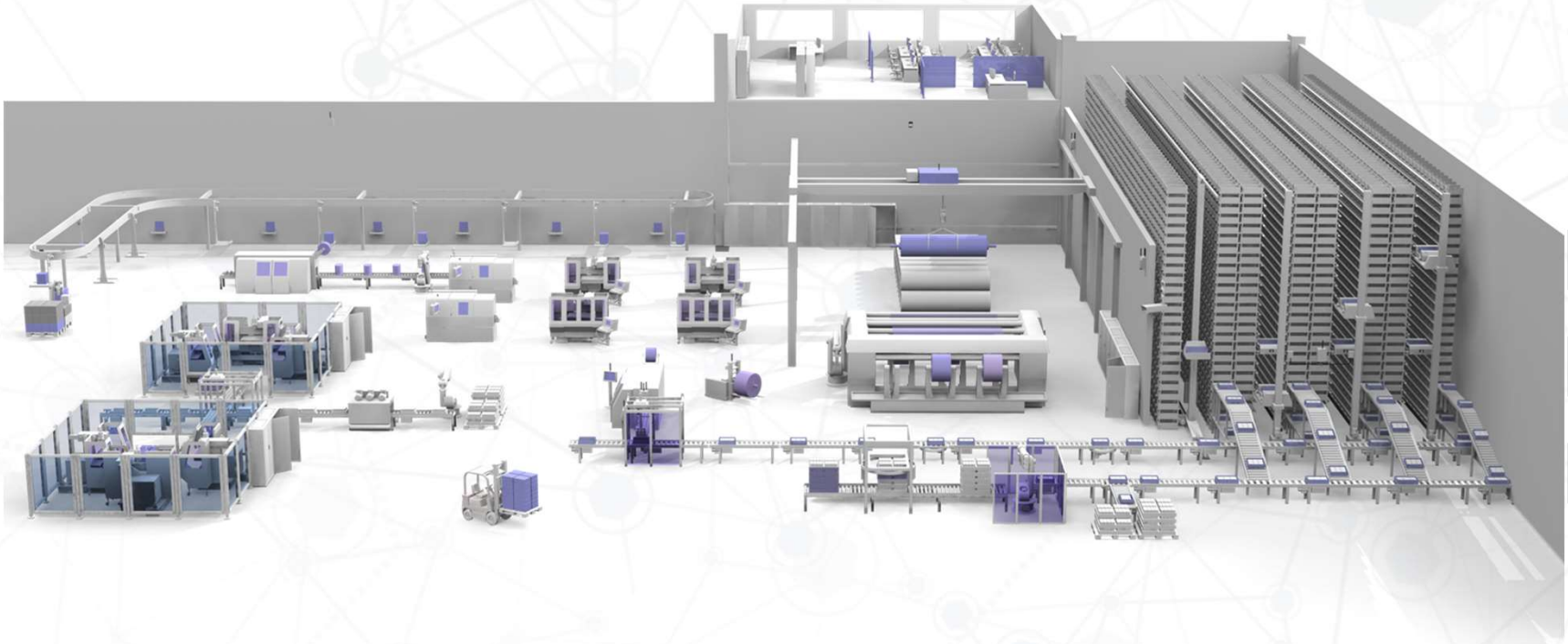
- Physische Maßnahmen
- Berechtigungskonzept
  - Zutritt
  - Zugang
  - Zugriff
- Awareness Schulungen
- ISMS – Prozesse
- …

Netzwerkebene

Produktebene

Security ganzheitlich betrachtet

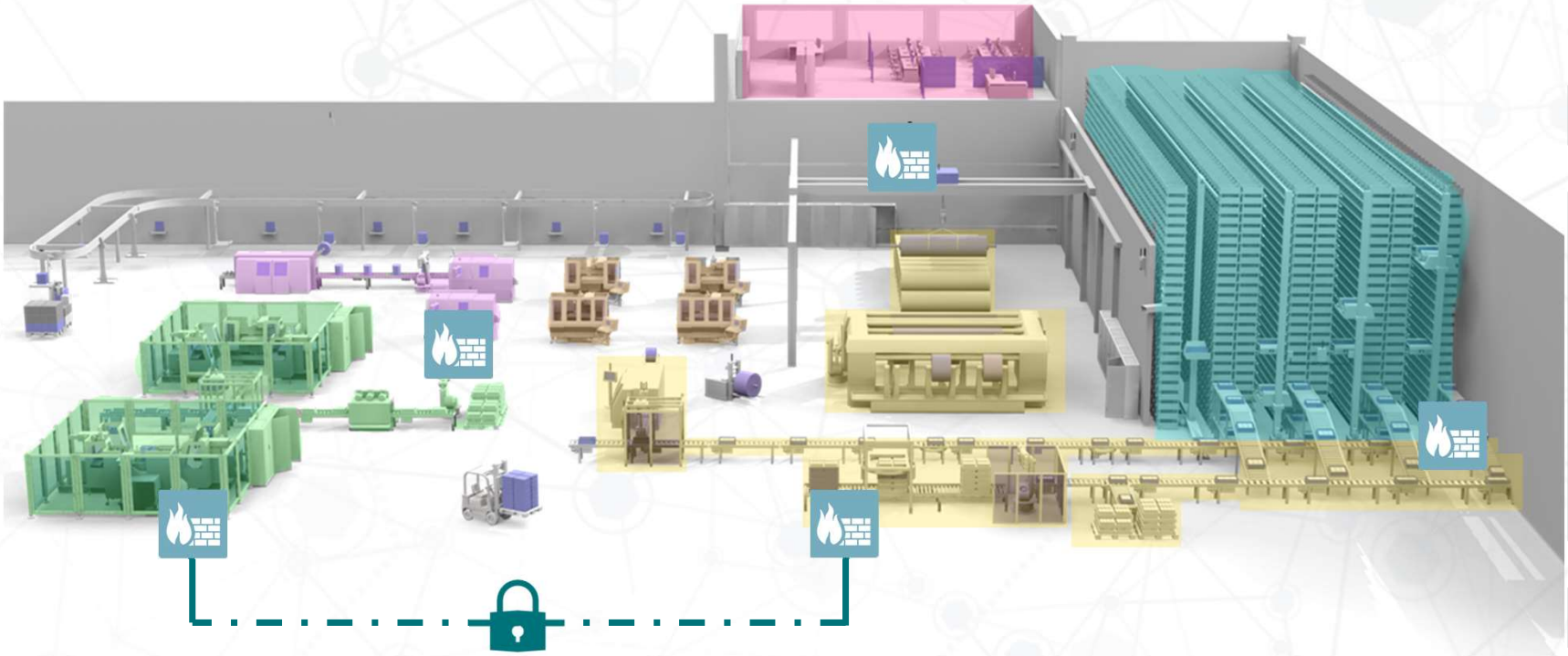
Das „Defense in Depth“ Konzept



- Unternehmensebene
- Netzwerkebene
- Produktebene

Security ganzheitlich betrachtet

Das „Defense in Depth“ Konzept



Unternehmensebene

Netzwerkebene

- Netzsegmentierung
  - Zonen
  - Conduits
- VPN
- Verschlüsselung
- Firewalls
- …

Produktebene

Security ganzheitlich betrachtet

Schnittstellen Schutz

Kontrolle von lokalen und entfernten Schnittstellen

Netzwerkmonitoring

Firewalls

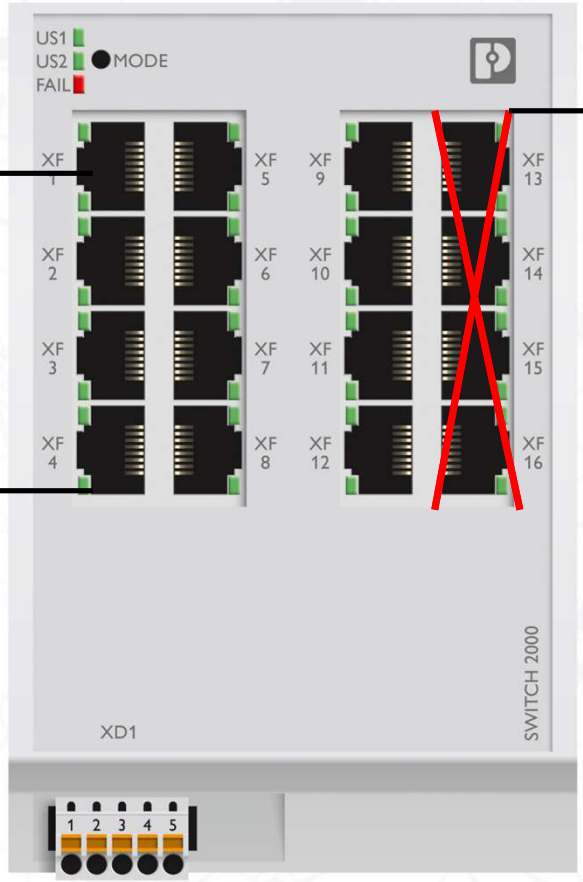
Abschalten von physischen und virtuellen Schnittstellen

Security ganzheitlich betrachtet

Härtung

Deaktivierung ungenutzter Software/Dienste

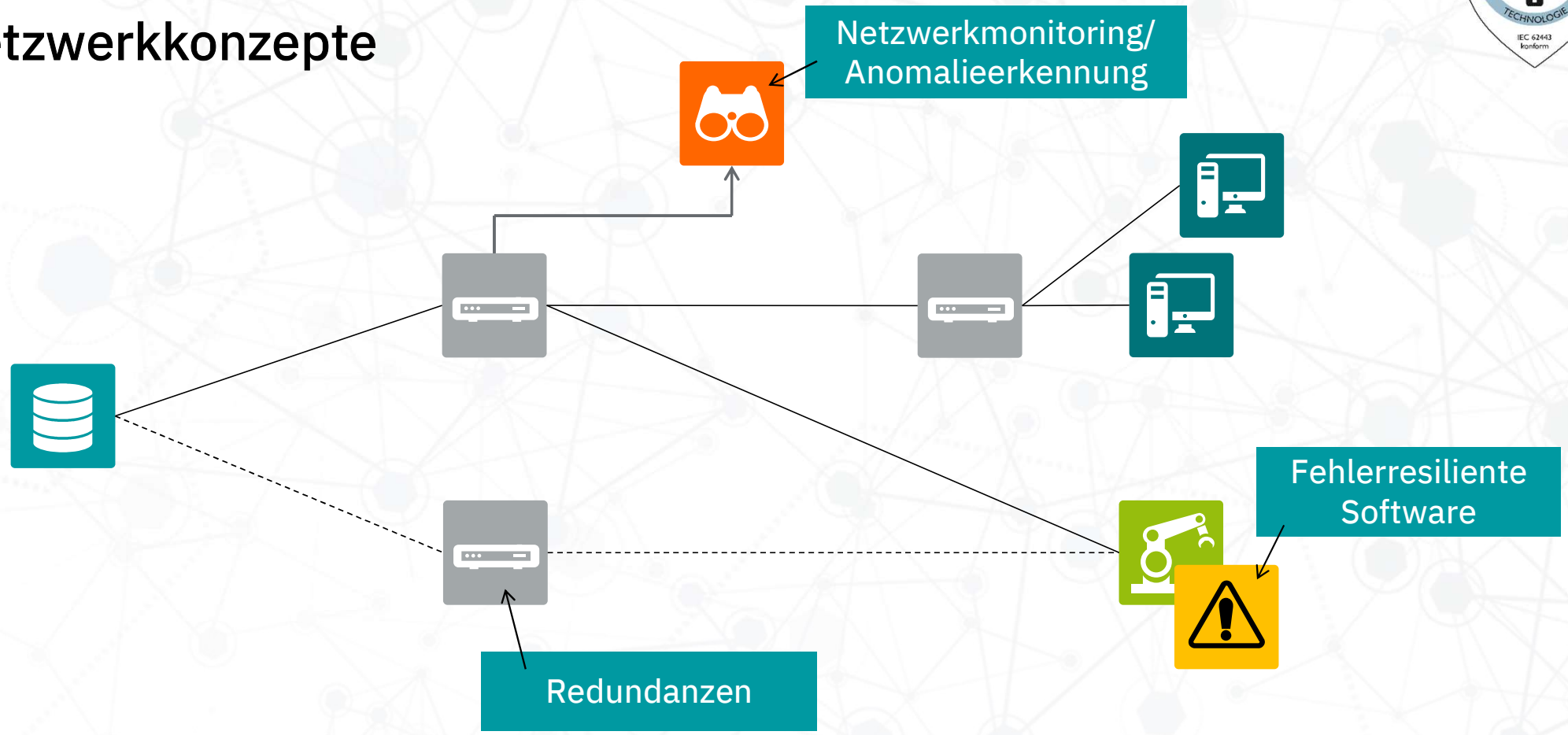
Einschränkung von Benutzerrechten



Abschaltung von ungenutzten Schnittstellen

Security ganzheitlich betrachtet

Netzwerkkonzepte



Security ganzheitlich betrachtet

Zugriffsprotokollierung

Wer hat wann worauf zugegriffen?

- Nachverfolgbarkeit von Fehlern und Änderungen
- Identifikation von ungewöhnlichem Verhalten

Lorem ipsum dolor sit amet, consectetuer adipiscing elit.
Maecenas porttitor congue massa.
Fusce posuere, magna sed pulvinar ultricies

Purus lectus malesuada libero, sit amet commodo magna eros quis urna.
Nunc viverra imperdiet enim. Fusce est. Vivamus a tellus.
Pellentesque habitant morbi tristique senectus et netus et malesuada.

Security ganzheitlich betrachtet

Das „Defense in Depth“ Konzept

- Unternehmensebene
- Netzwerkebene
- Produktebene

Security ganzheitlich betrachtet

Das „Defense in Depth“ Konzept

Unternehmensebene

Netzwerkebene

Produktebene

- Security Features
- Systemhärtung
- „Security by Design“ Komponenten
- …

Security ganzheitlich betrachtet

Resiliente Software

Software hat einen entscheidenden Einfluss auf die Funktionalität von Anlagen

Gefährdungen können nicht nur aus technischen Fehlern entstehen, sondern auch aus einprogrammiertem Fehlverhalten

Security ganzheitlich betrachtet

Resiliente Software

Wassertemperatur: 1999 °C

Fehlbedienung und Fehlerhafte Eingaben erkennen und verhindern

01010101010101000000001 10101010

Fehler in verarbeiteten Daten (z.B. Von Sensoren) erkennen und korrekt behandeln

Sonderfälle wie Grenzwerte, Manuelle Unterbrechungen, maximale Auslastung etc. korrekt behandeln

Security ganzheitlich betrachtet

Festlegung von Zielen

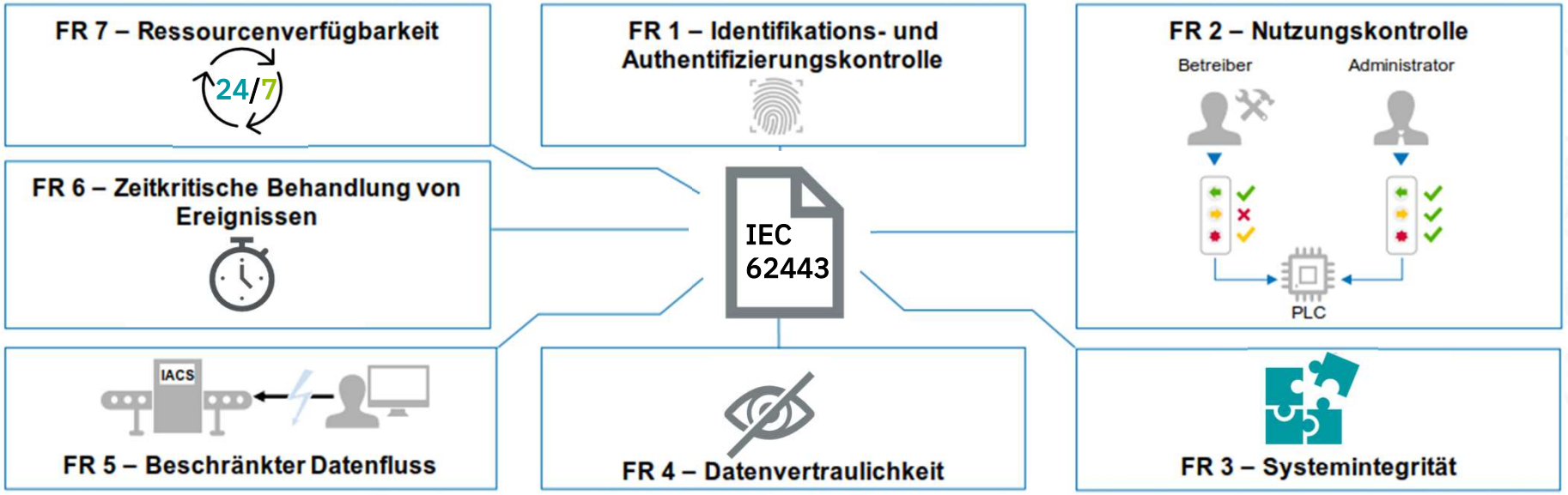
Schutz vor:	
SL-0	Kein Schutz
SL-1	Durchschnittlichen Internet-Nutzern
SL-2	Interessierten Einzelpersonen und Firmen mit allgemeinen Security-Kenntnissen
SL-3	Experten und Firmen, die mit klaren Zielen effektive, jedoch kostenorientierte Angriffsszenarien entwickeln und einsetzen
SL-4	Staatlichen Organisationen, bei denen die Erreichung des spezifisch ausgewählten Angriffsziels um fast jeden Preis im Vordergrund steht

Security ganzheitlich betrachtet

Anforderungen Systeme und Komponenten IEC 62443-4-2/3-3

7 Foundational Requirements / 56 Requirements

Bewertung nach grundlegenden Sicherheitskategorien:



Security ganzheitlich betrachtet

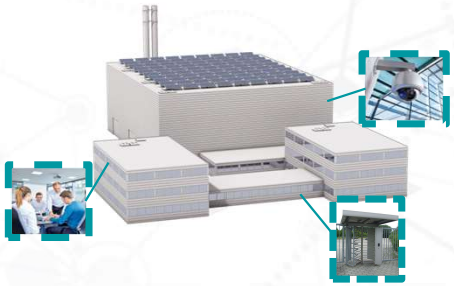
Festlegung von Zielen

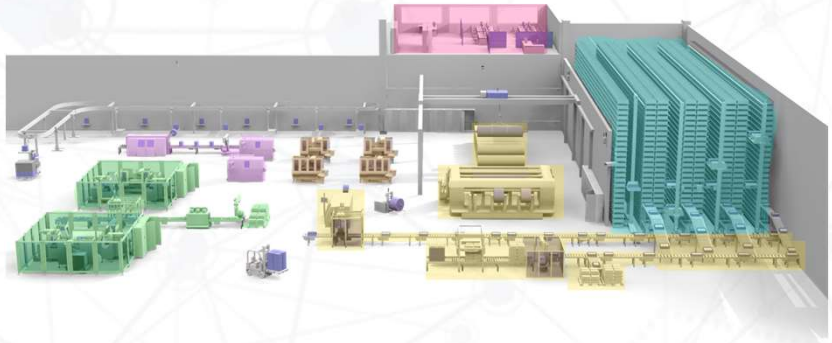
SRs und REs	SL-1	SL-2	SL-3	SL-4
SR 1.1 Identifizierung und Authentifizierung von menschlichen Nutzern	✓	✓	✓	✓
RE (1) Eindeutige Identifizierung und Authentifizierung		✓	✓	✓
RE (2) Multifaktor-Authentifizierung über nicht vertrauenswürdige Netze			✓	✓
RE (3) Multifaktor-Authentifizierung über alle Netze				✓

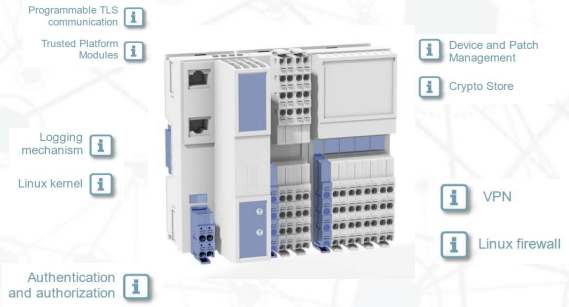
SR: System Requirement RE: Requirement Enhancements

Security ganzheitlich betrachtet

Das „Defense in Depth“ Konzept







Implementierung gestaffelter und sich ergänzender Sicherheitsmaßnahmen auf mehreren Ebenen.

Security ganzheitlich betrachtet

Unabdingbar: Ein 360° Industrial Security-Ansatz

Competence Center Services

Ihr Partner für Produktunabhängige Dienstleistungen

OT-Security Service Provider nach IEC 62443

CERT@VDE

LinkedIn Industrial Services - Security | Safety | CE

www.phoenixcontact.de/services

Danke

für Ihr Interesse!

Fragen?

Hauke Kästing

Email: hauke.kaesting@phoenixcontact.de
Telefon: 0171 / 97 838 47

PHOENIX CONTACT
INSPIRING INNOVATIONS