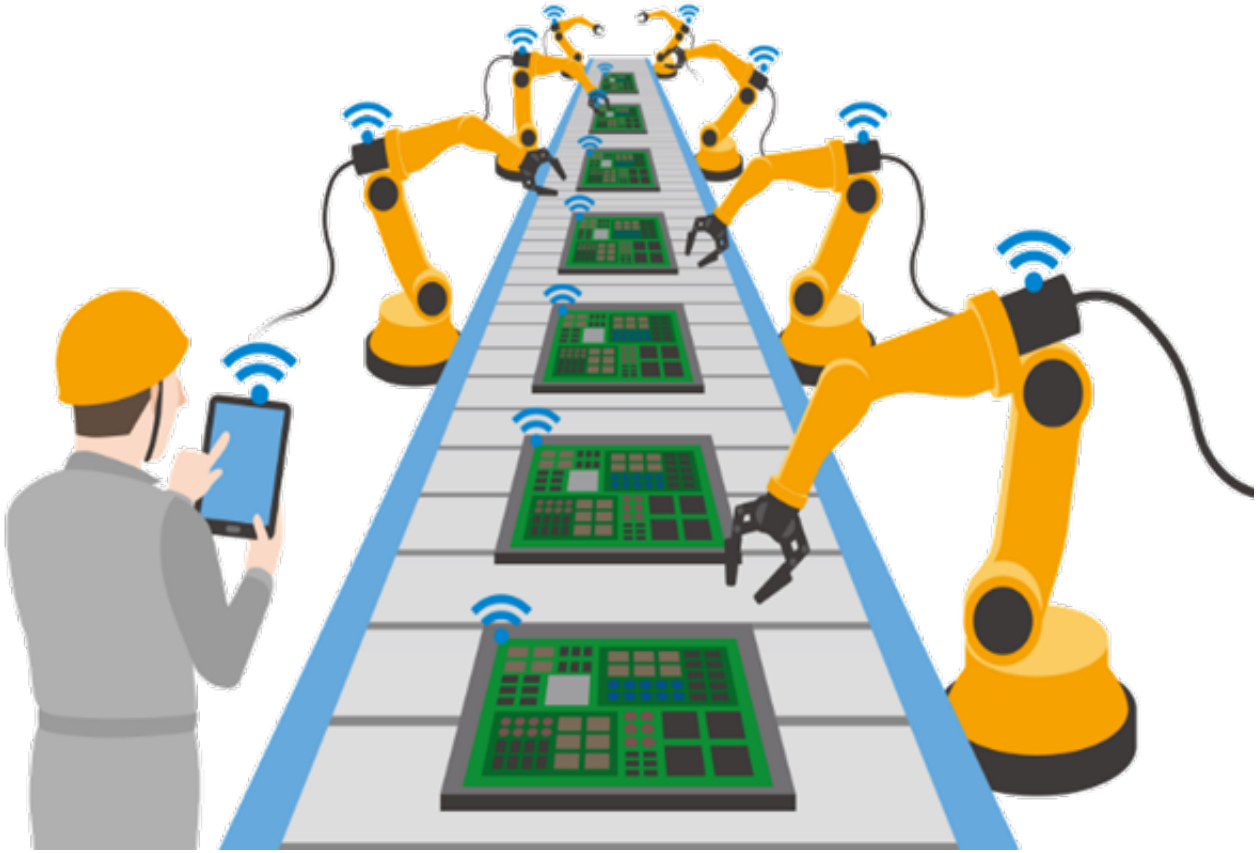
SWS COMPUTERSYSTEME
Member of ACP Group

# IoT Webinar-Reihe

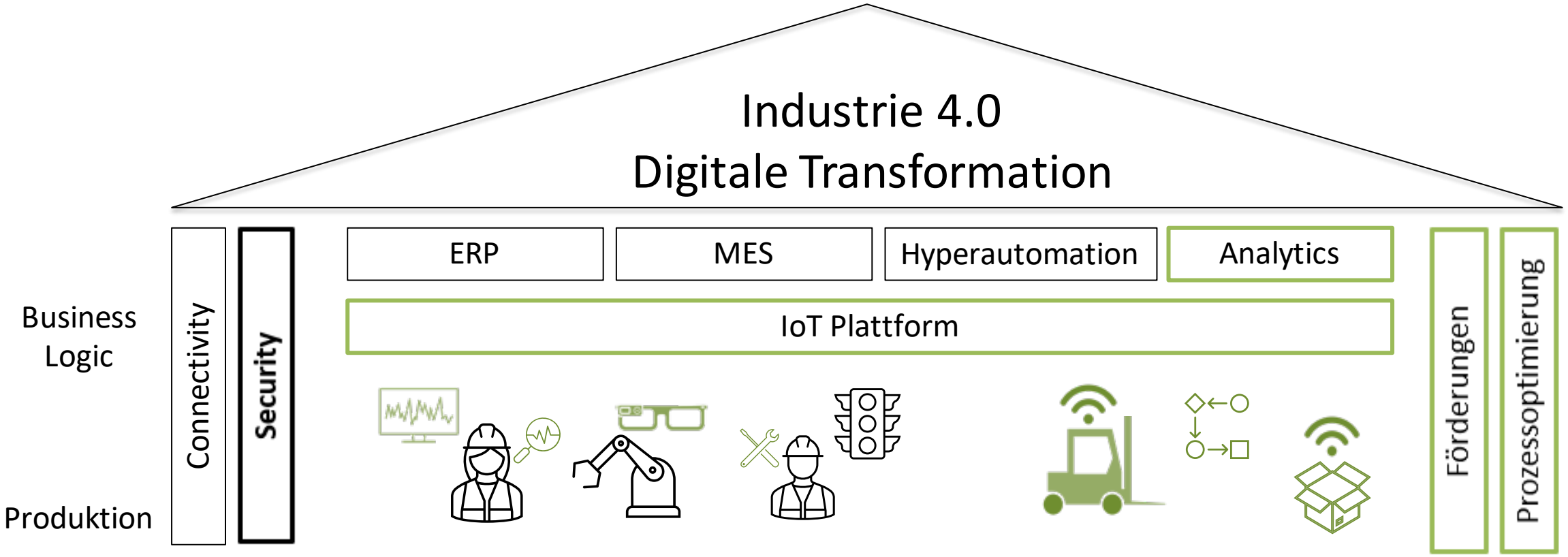
IoT Solutions for innovators.

## Teil 8: Security im OT Bereich



**Johannes Fuchs, M.Sc.**
**Business Development & Consultant IoT**

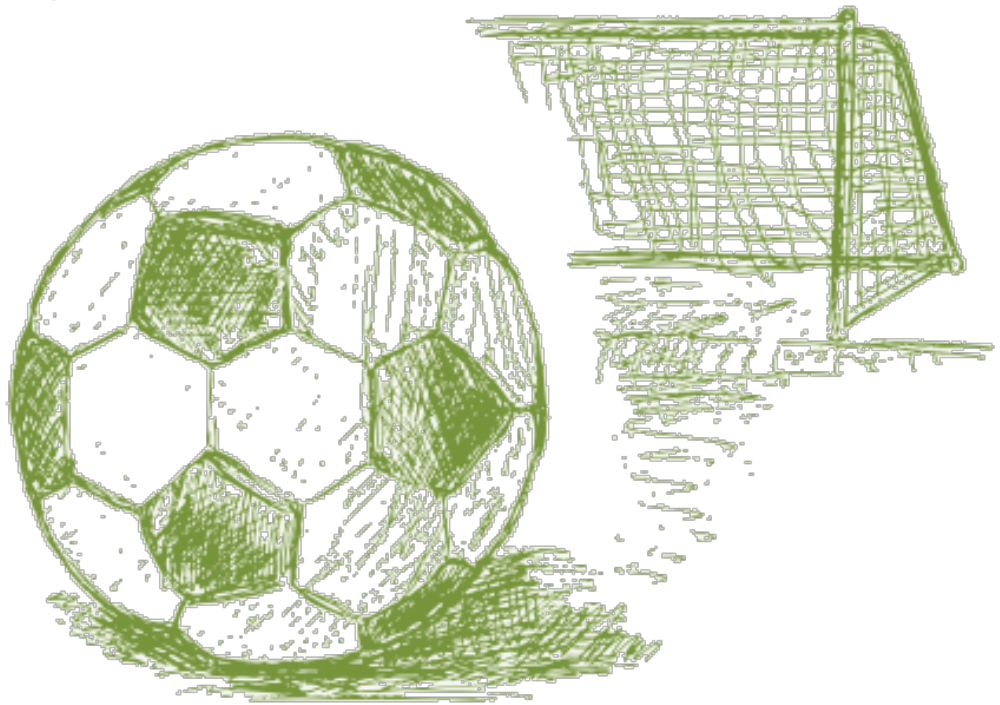
**28. September 2021**


Industrie 4.0
Digitale Transformation
Business Logic
Produktion
Connectivity
Security
ERP
MES
Hyperautomation
Analytics
IoT Plattform
Förderungen
Prozessoptimierung

# Digitalisierung = Mannschaftssport



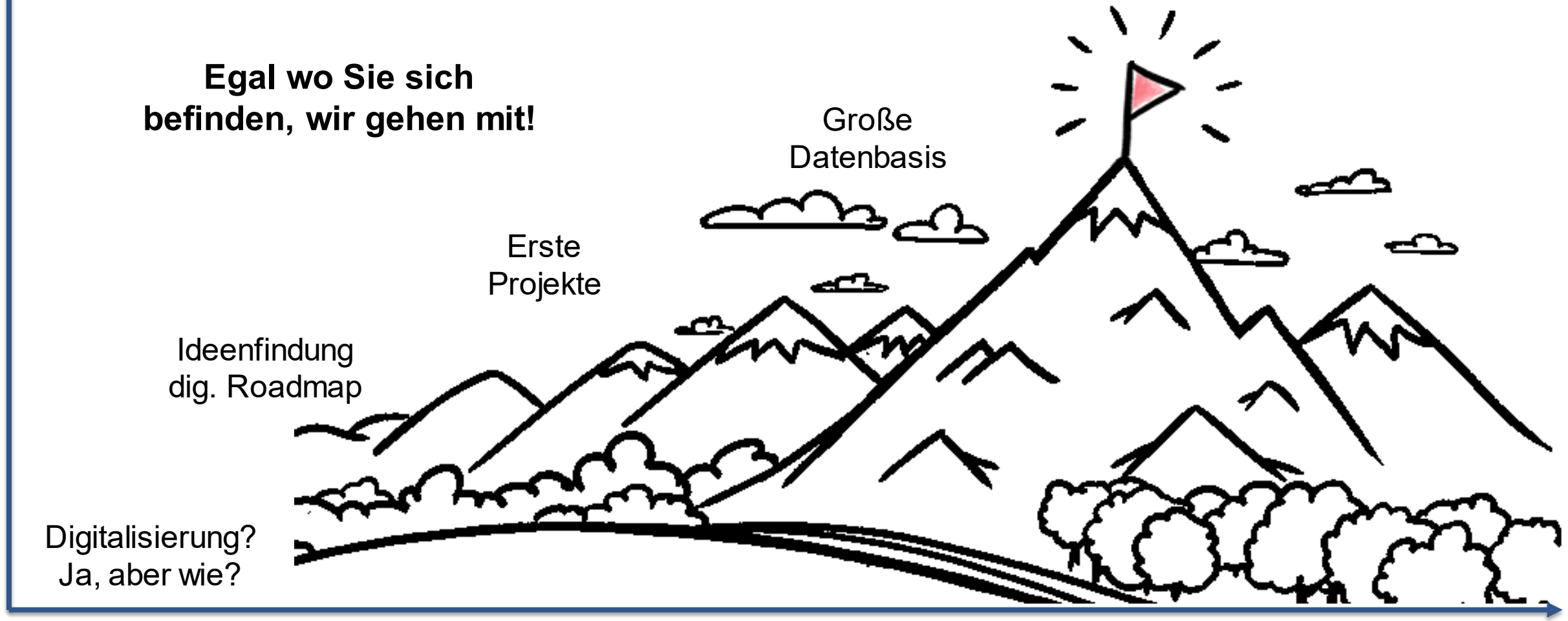
**Spieler, deren Fähigkeiten und das Zusammenspiel müssen aufeinander abgestimmt sein!**



# Strategie und Ideenfindung

Digitalisierungsgrad

**Egal wo Sie sich befinden, wir gehen mit!**




Zeitachse

# SWS IoT ECOsystem

## Beraten

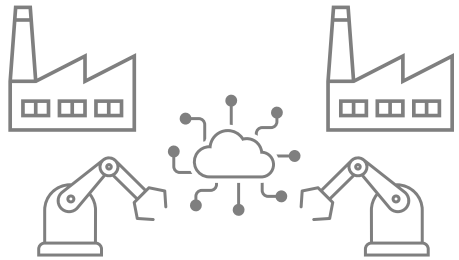
- ✓ Ganzheitliche Strategie
- ✓ Dig. Roadmaps
- ✓ Neue Geschäftsmodelle
- ✓ Techn. Konzepte
- ✓ Prozessoptimierung
- ✓ Menschen & Kultur
- ✓ Förderungen
- ✓ Wissenschaft
- ✓ Technologie
- ✓ Security

## Sammeln

- ✓ IoT Plattform
- ✓ Konnektivität
- ✓ Infrastruktur
- ✓ Datenquellen
- ✓ Schnittstellen
- ✓ Steuerungen
- ✓ Sensoren
- ✓ Bilder / Videos
- ✓ Security

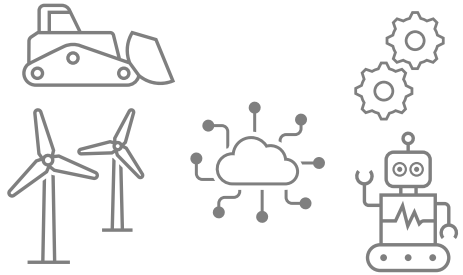
## Auswerten

- ✓ Automation
- ✓ Geschäftslogik
- ✓ Visualisierung
- ✓ Alarmierung
- ✓ Analysen
- ✓ Prognosen
- ✓ Weiterleiten
- ✓ Benutzeroberflächen
- ✓ SW Entwicklung



Smart Connected Production

**USP:**
**Dig. Transformation**
**End 2 End Lösungen**



Smart Connected Products

# Warum OT Security?



## Treiber

- Industrie 4.0
- Digitale Transformation
- Smart Factory
- Smart Warehouse
- Smart Building
- Remote Workforce
- Remote Maintenance
- Predictive Maintenance
- 5G, Wireless

...

## Herausforderungen

- Sichtbarkeit
  - Geräte
  - Applikationen
  - Kommunikation
  - Protokolle
- Integration von Cloud Lösungen
- Segmentierung

…

Wegen Erpressersoftware "Petya"

03.07.2017, 16:53 Uhr

## Milka-Fabrik steht seit einer Woche still

In Deutschland leiden Unternehmen weiter an den Folgen der Cyberattacke mit der Erpressersoftware "Petya". Besonders hart traf es den Lebensmittelkonzern Mondelez. VON OLIVER VOSS


Verschlüsselt. Beim Milka Schokofest in Lörrach hatte Werksleiter Alexandre David noch gut Lachen. Im Beisein von Skisprung Star... FOTO: OBS

Quelle: https://www.tagesspiegel.de/wirtschaft/wegen-erpressersoftware-petya-milka-fabrik-steht-seit-einer-woche-still/20013388.html

Produktion in Süd- und Nordamerika

## Hackerangriff auf Rheinmetall: Fertigung stark beeinträchtigt

Rheinmetall spricht nach einem Hackerangriff von "schweren Beeinträchtigungen der Betriebsabläufe". Wo die Produktion bei dem Rüstungskonzern und Autozulieferer jetzt stockt.

27.09.2019

Quelle: https://www.produktion.de/wirtschaft/hackerangriff-auf-rheinmetall-fertigung-stark-beeintraechtigt-242.html

# Security



22.09.2020

## CYBER-KRIMINELLE LEGEN BETRIEB LAHM
## Hacker-Angriff auf Verpackungsspezialist Optima in Schwäbisch Hall

Quelle: https://www.swr.de/swraktuell/baden-wuerttemberg/heilbronn/hackerangriff-optima-schwaebisch-hall-100.html

# Ablauf einer typischen Cyber-Crime-Attacke

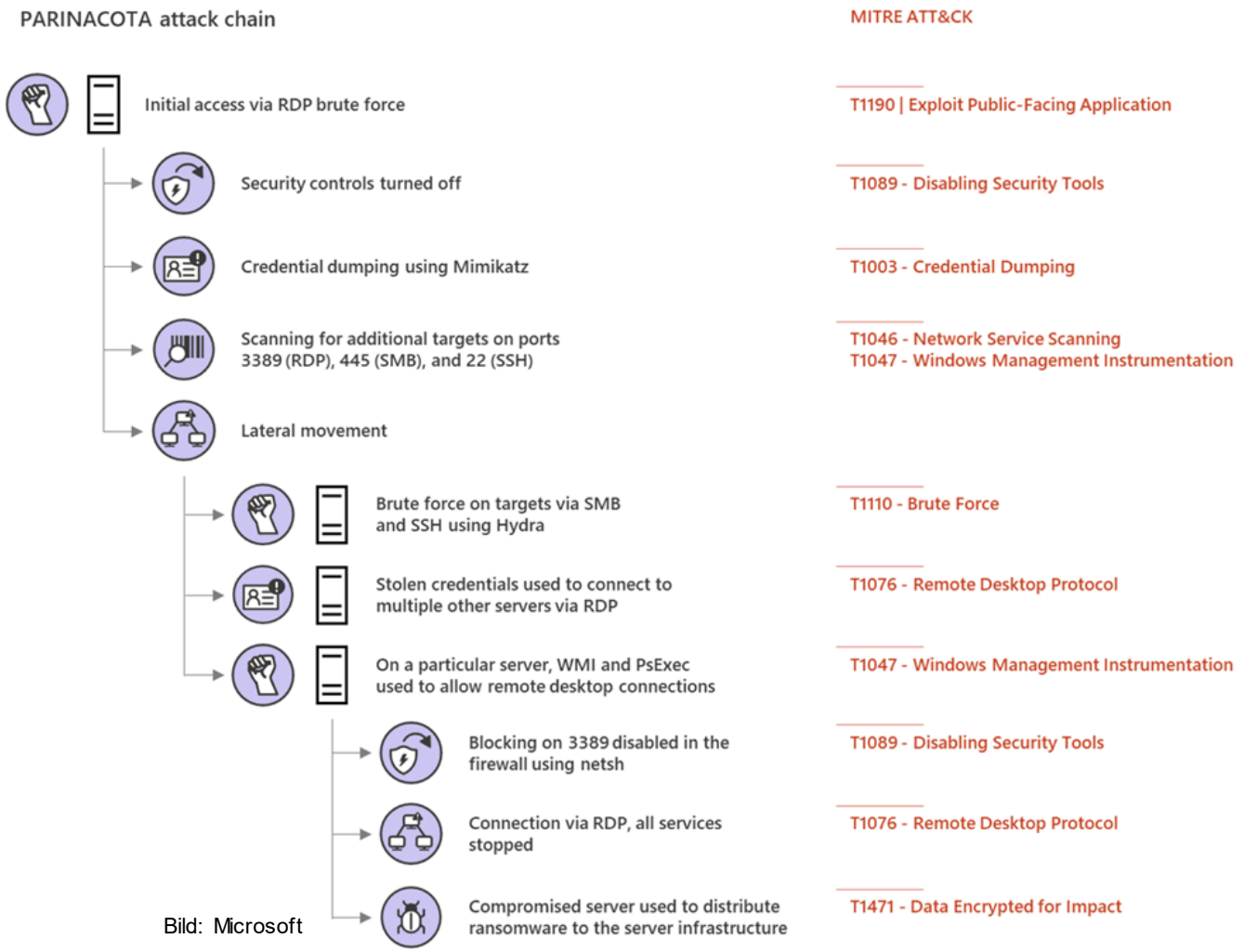



Bild: Microsoft

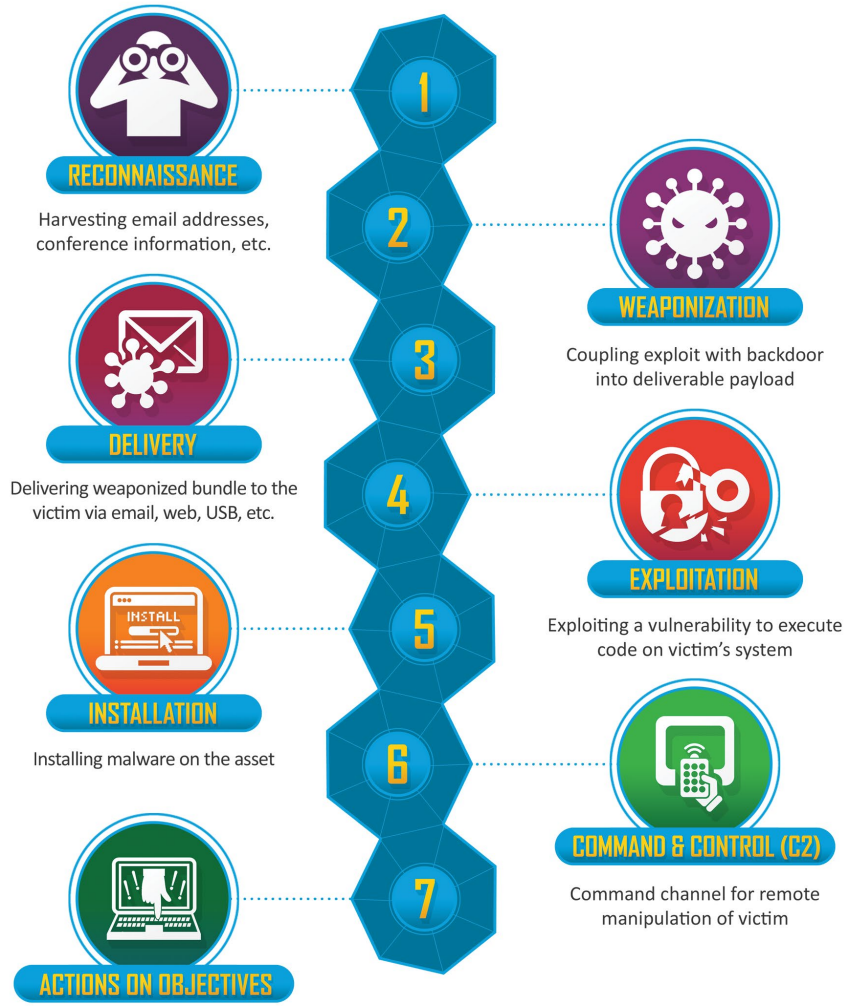



Bild: Lockheed Martin

Quelle: https://www.heise.de/hintergrund/Cybercrime-Erpressung-auf-neuem-Niveau-4867430.html

# Produktionsausfälle



## Fernwartung

Bild: Adobe Stock

Bild: produktion.de

# Produktionsausfälle



## Supply Chain Attacks

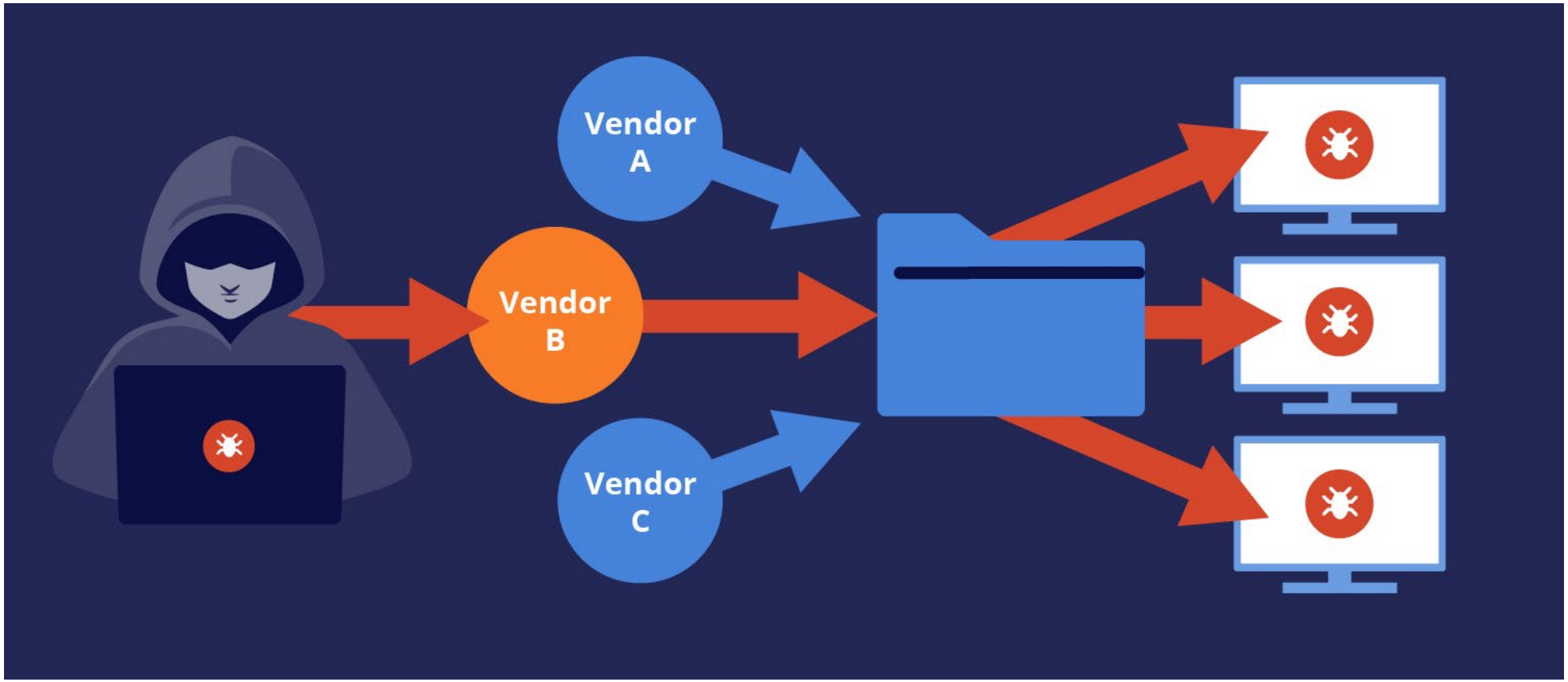
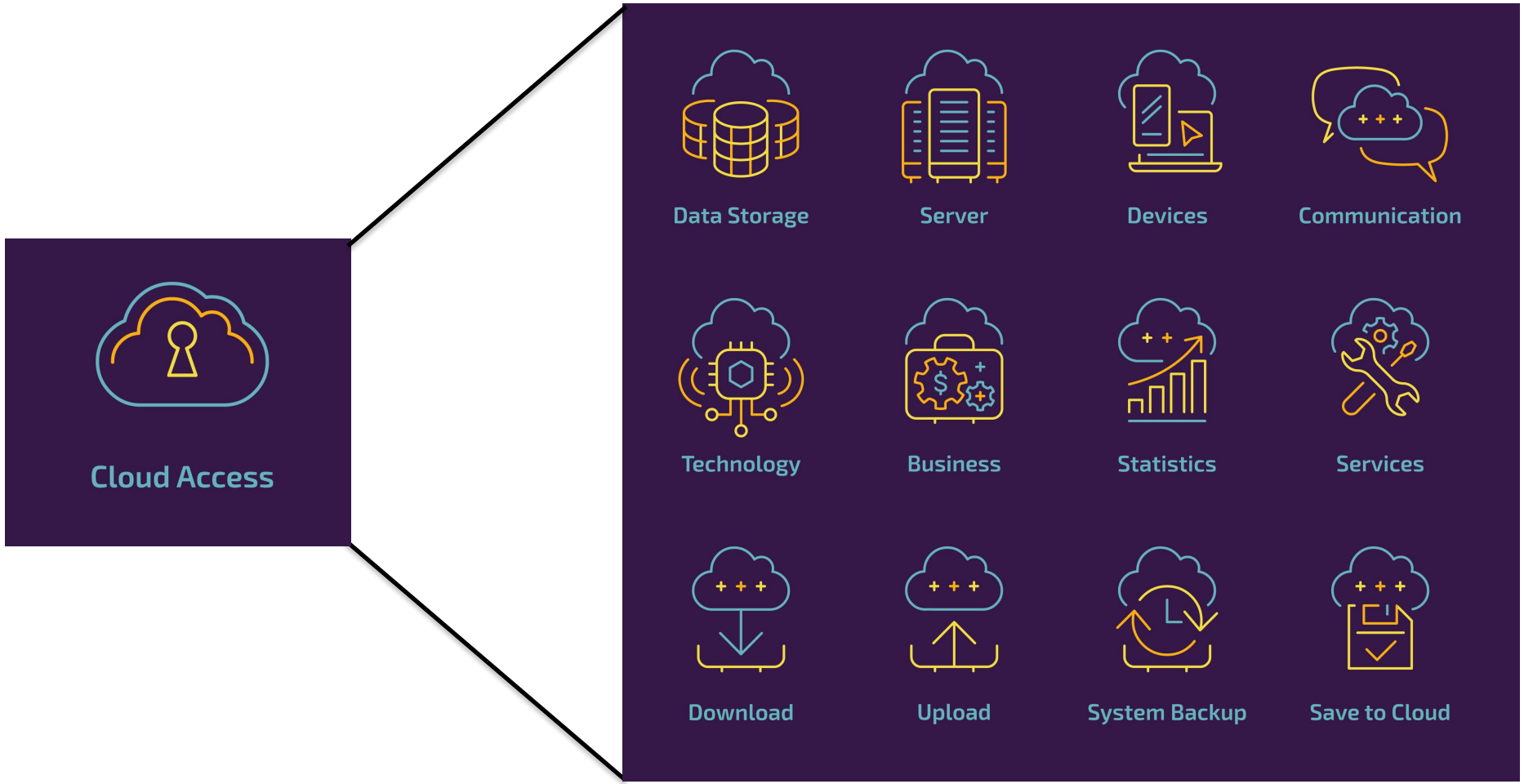



Bild: finitestate.io

# Produktionsausfälle



## Schlechte Absicherung von Cloud Diensten




Bilder: Adobe Stock

# Produktionsausfälle



Durchgriff IT auf OT

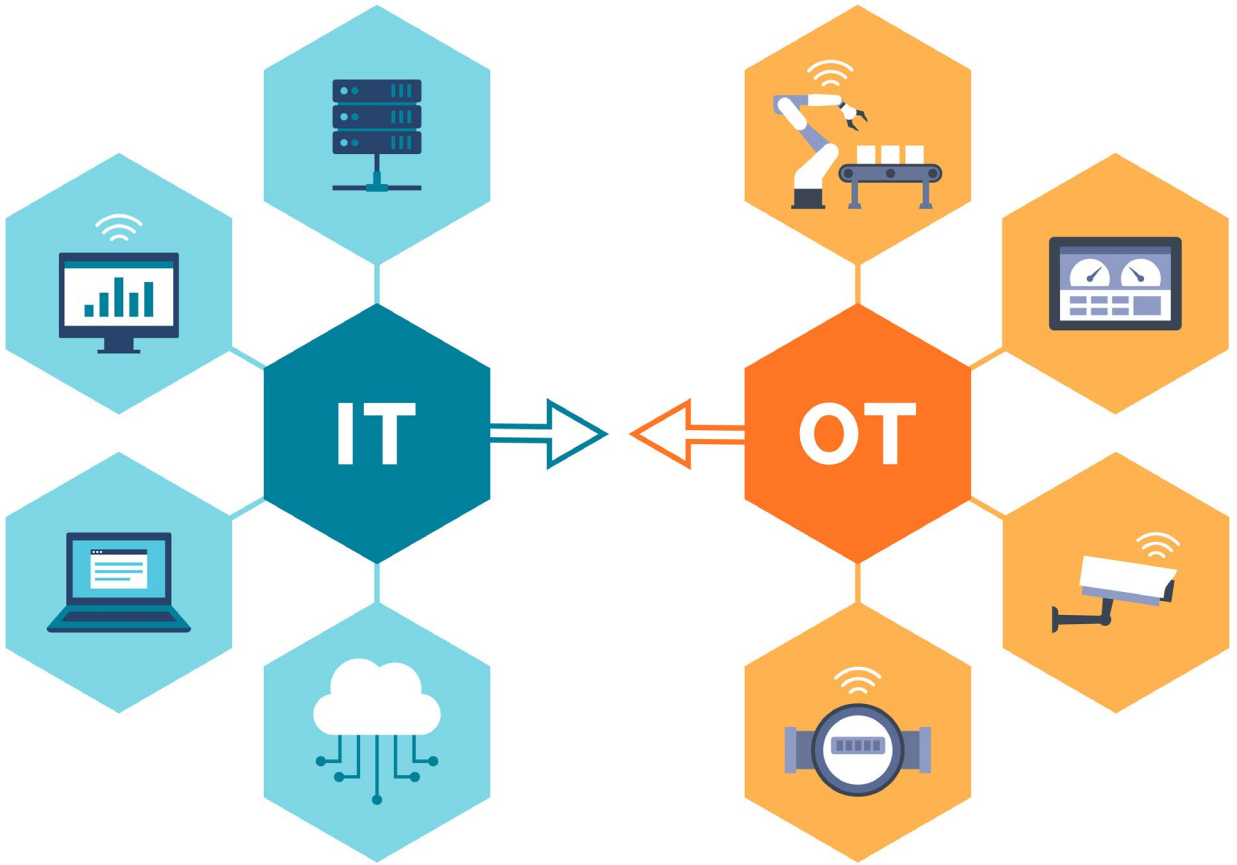



Bild: Adobe Stock

# Top 10 Bedrohungen in der Produktion (BSI)

- Einschleusen von Schadsoftware über externe Geräte ↗
- Infektion mit Schadsoftware über Internet und Intranet ↗
- Menschliches Fehlverhalten und Sabotage ↑
- Kompromittierung von Extranet und Cloud-Komponenten ↑
- Social Engineering und Phishing ↘
- (D)DoS Angriffe ↑
- Internet-verbundene Steuerungskomponenten →
- Einbruch über Fernwartungszugänge →
- Technisches Fehlverhalten und höhere Gewalt ↘
- Kompromittierung von Smartphones im Produktionsumfeld →

Quelle: BSI: „Industrial Control System Security - Top 10 Bedrohungen und Gegenmaßnahmen 2019“

# Abgrenzung IT - OT



| | IT | OT |
|---|---|---|
| **Umfeld** | Büro, PCs, Drucker… | Sensoren, Prozesse, Automaisierung… |
| **Steuerung** | Daten | Physik |
| **Messung** | Bits & Bytes | Temperatur, Druck, Füllstand, Durchfluss… |
| **Lebensdauer** | Lebensdauer des Systems | Lebensdauer der Fertigung |
| **Konsequenzen** | Wettbewerbsnachteil, Reputation, Finanzieller Verlust | Produktschäden, Körperliche Unversehrtheit, Umweltschäden |
| **Prioritäten** | Vertraulichkeit, Integrität, Verfügbarkeit | Sicherheit, Verfügbarkeit, Steuerbarkeit, Zuverlässigkeit |
| **Ausbildungs-Hintergrund** | Informatik, Informationssysteme, Cybersecurity | Berufliche und technische Ausbildung, Elektrotechnik |
| **Meldekette** | ISO, CISO, CIO | Schichtleiter, Werksleiter, leitender Geschäftsführer |
| **Betriebswirtschaftliche Sicht** | Cost Center | Profit Center |
| **Zugangssteuerung** | Netzwerk Authentifizierungs- und Zugangsrichtlinien | Strikter physischer Zugang aber einfaches Netzwerk |
| **Motivation von Cyberkriminellen** | Monetarisierung | Unterbrechung der Produktion |
| **Bedrohungserkennung** | Endpunktschutz, AV-Lösung | Traffic Monitoring, Sensorik |
| **Bedrohungsschutz** | Zugriff abschalten | Isolieren, aber in Betrieb halten |
| **Instandhaltung** | Mehrere Unterstützungsquellen, 3-5 Jahre Lebensdauer, modulare, zugängliche Komponenten, IT-Personal oder Serviceverträge | Unterstützung durch einzelnen Anbieter, 15-20 Jahre Lebensdauer der Komponenten, entfernte Komponenten, verdeckter Zugang, keine IT-Vollzeitmitarbeiter |
| **Aktualisierungen** | häufige Patches und Updates; im Betrieb automatisch bereitgestellt | sorgfältig geplant und getestet; während Downtime vorgesehen oder gar nicht durchgeführt |
| **Hauptakteure** | CIO und IT Personal | Ingenieure, Techniker, Anwender und Manager |

# Abgrenzung IT - OT



| | IT | OT |
|---|---|---|
| **Umfeld** | Büro, PCs, Drucker… | Sensoren, Prozesse, Automaisierung… |
| **Steuerung** | Daten | Physik |
| **Messung** | Bits & Bytes | Temperatur, Druck, Füllstand, Durchfluss… |
| **Lebensdauer** | Lebensdauer des Systems | Lebensdauer der Fertigung |
| **Konsequenzen** | Wettbewerbsnachteil, Reputation, Finanzieller Verlust | Produktschäden, Körperliche Unversehrtheit, Umweltschäden |
| **Prioritäten** | Vertraulichkeit, Integrität, Verfügbarkeit | Sicherheit, Verfügbarkeit, Steuerbarkeit, Zuverlässigkeit |
| **Ausbildungs-Hintergrund** | Informatik, Informationssysteme, Cybersecurity | Berufliche und technische Ausbildung, Elektrotechnik |
| **Meldekette** | ISO, CISO, CIO | Schichtleiter, Werksleiter, leitender Geschäftsführer |
| **Betriebswirtschaftliche Sicht** | Cost Center | Profit Center |
| **Zugangssteuerung** | Netzwerk Authentifizierungs- und Zugangsrichtlinien | Strikter physischer Zugang aber einfaches Netzwerk |
| **Motivation von Cyberkriminellen** | Monetarisierung | Unterbrechung der Produktion |
| **Bedrohungserkennung** | Endpunktschutz, AV-Lösung | Traffic Monitoring, Sensorik |
| **Bedrohungsschutz** | Zugriff abschalten | Isolieren, aber in Betrieb halten |
| **Instandhaltung** | Mehrere Unterstützungsquellen, 3-5 Jahre Lebensdauer, modulare, zugängliche Komponenten, IT-Personal oder Serviceverträge | Unterstützung durch einzelnen Anbieter, 15-20 Jahre Lebensdauer der Komponenten, entfernte Komponenten, verdeckter Zugang, keine IT-Vollzeitmitarbeiter |
| **Aktualisierungen** | häufige Patches und Updates; im Betrieb automatisch bereitgestellt | sorgfältig geplant und getestet; während Downtime vorgesehen oder gar nicht durchgeführt |
| **Hauptakteure** | CIO und IT Personal | Ingenieure, Techniker, Anwender und Manager |

# Historischer Abriss



- Verantwortung für Security oft beim IT-CISO, Zusammenführung der Security von IT und OT

  ⇒ Herausforderung: „Cyber Security Resiliency“

- Problem: kaum Skills, Technologien oder Prozesse im OT Bereich, kein Wissen über Produktionsprozesse und Schutz ohne Prozessbeeinträchtigung in der IT.

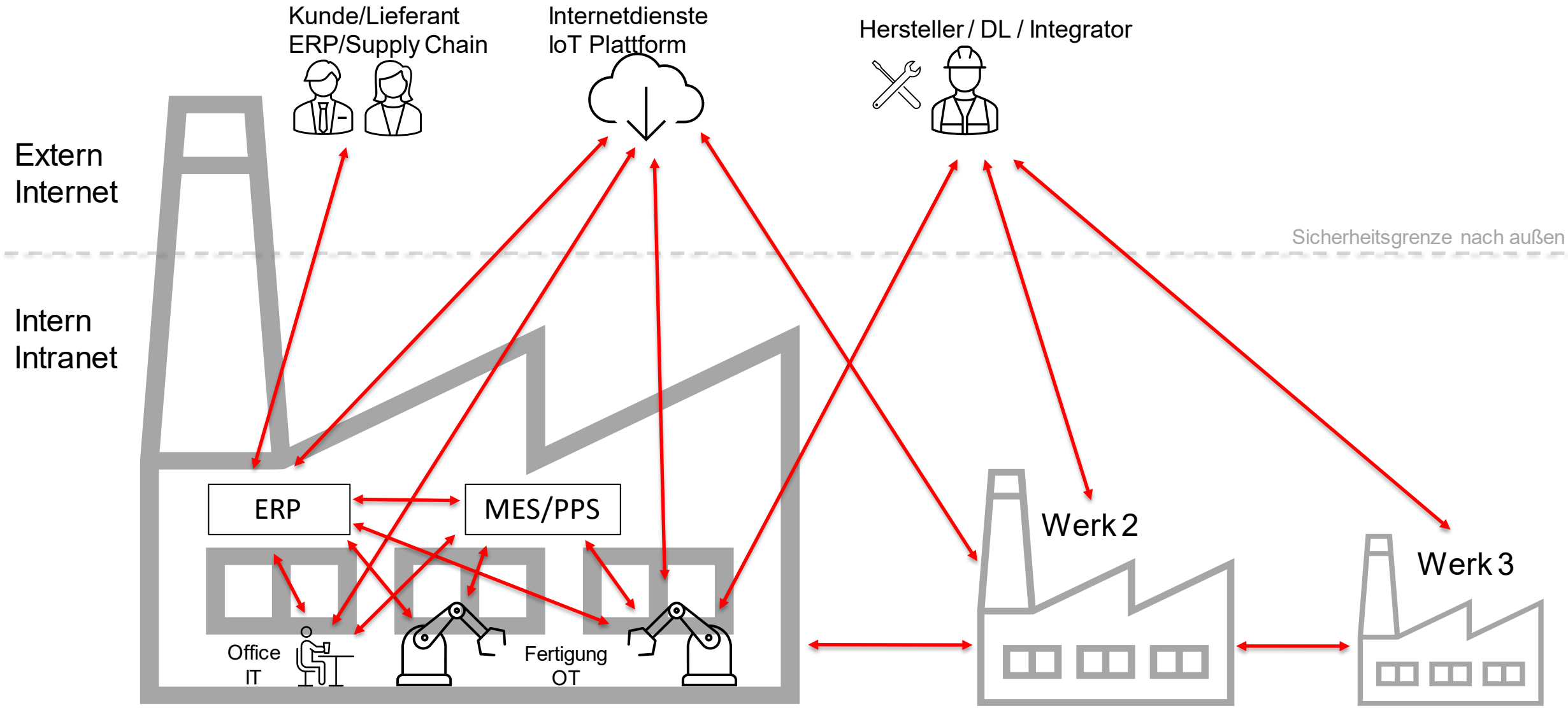
  ⇒ beide Teams müssen zusammenarbeiten.

- Vorgehen zum Schutz ähnlich, aber Ansätze sind unterschiedlich.

- Cyberangriffe kennen keine Grenze zwischen IT und OT

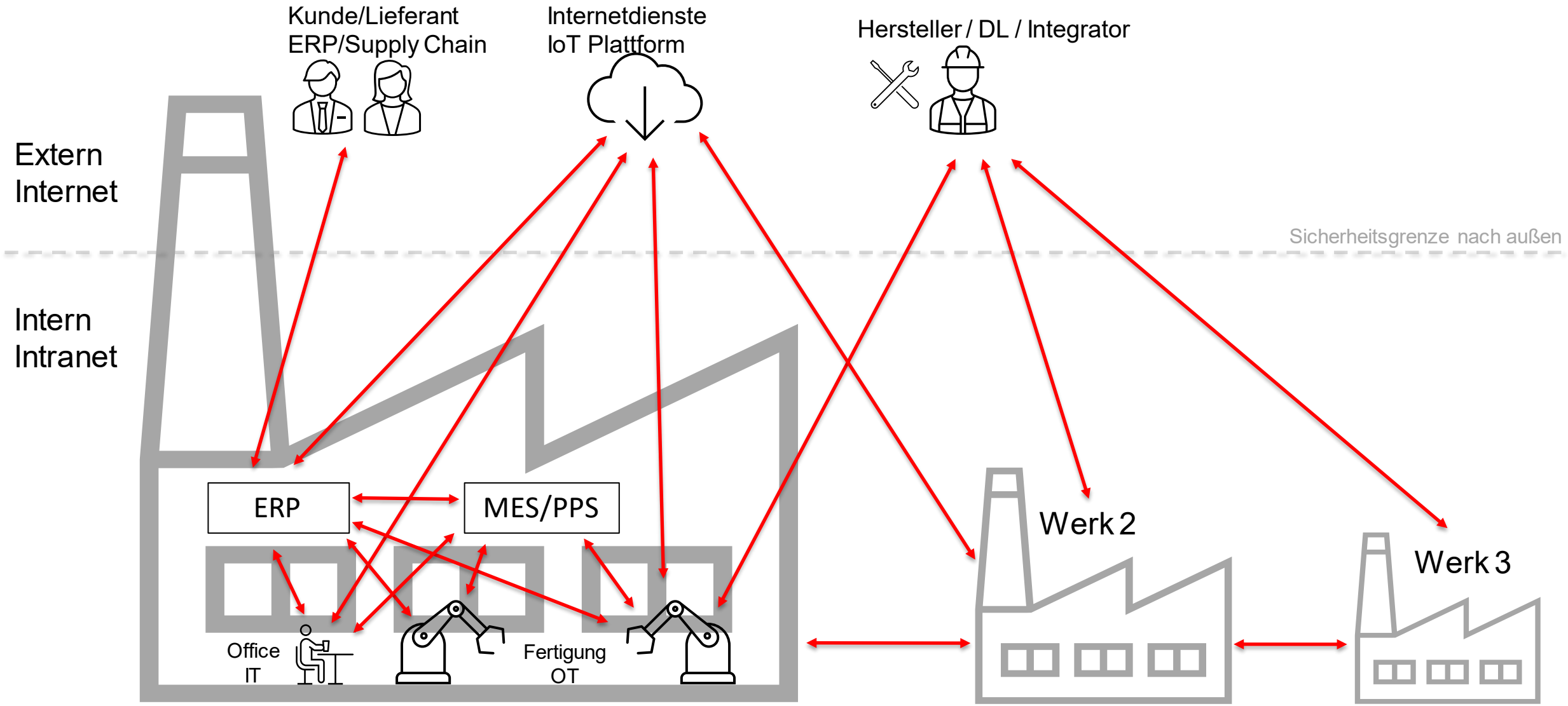
  ⇒ Austausch und Koordination notwendig

# Kommunikationsbeziehungen



# Kommunikationsbeziehungen





# Security?



NERC-CIP

NIST SP800-82

BSI Grundschutz

VDI/VDE 2182

EN/ISO 2700x

WIB M-2784

IEC 62443 | ANSI/ISA 99

IEC 62351

KRITIS

Bild: Adobe Stock

# IEC 62443



„Industrielle Kommunikationsnetze - IT Sicherheit für Netze und Systeme“

- Internationale Normenreihe
- beschreibt technische und prozessbezogene Aspekte der industriellen Cybersicherheit
- Unterscheidet verschiedene Rollen:
  - Betreiber
  - Integratoren (Dienstleister für Integration und Wartung)
  - Hersteller
- Umfassende Leitlinie zur Planungsvorbereitung für OT Security
- Defense in Depth-Ansatz, definiert Zones und Conduits
- enthält Elemente mehrerer Standards
- kompatibel zu EN/ISO 27001

Quelle: Wikipedia

# IEC 62443 – Referenz-Achitektur



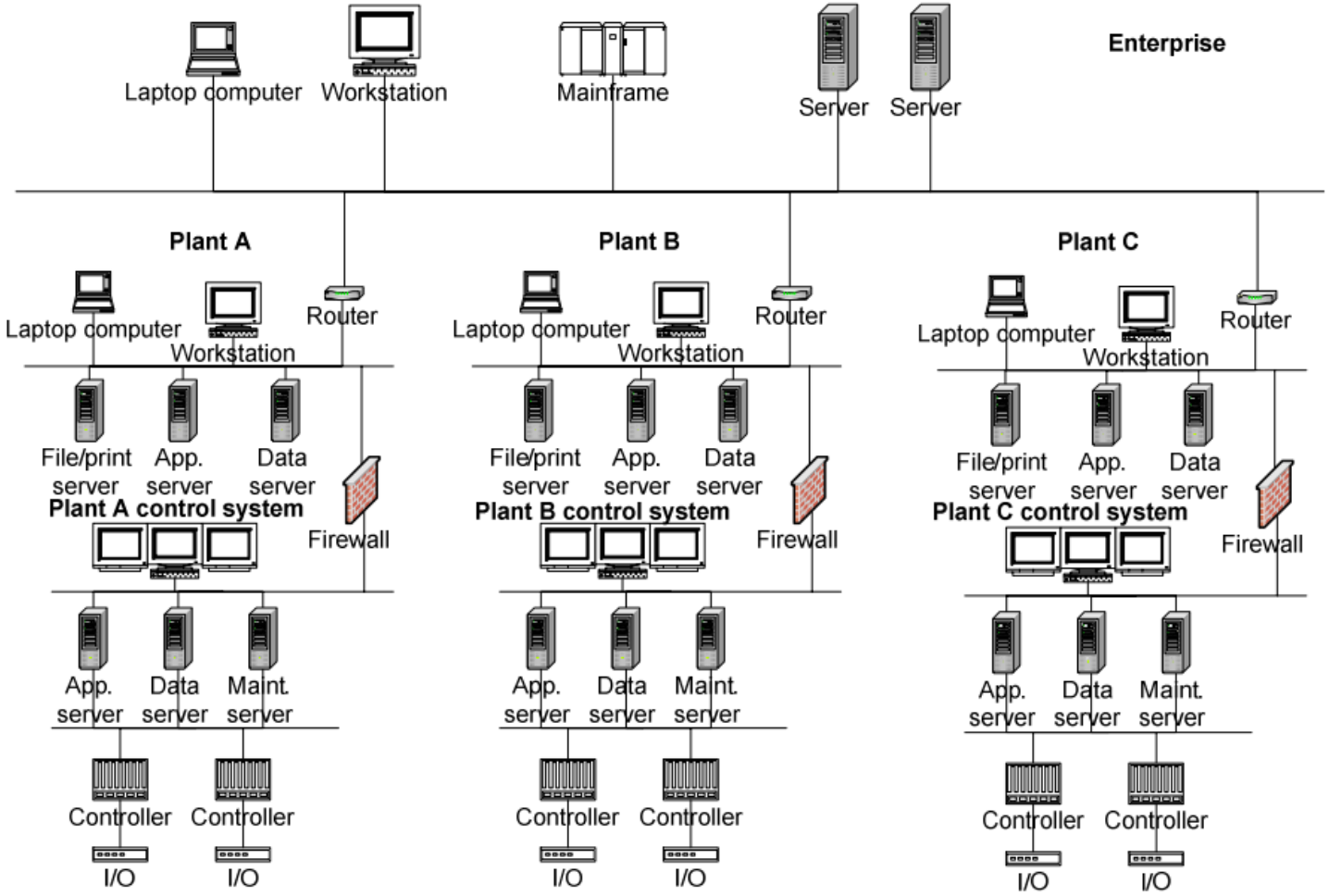



Bild: IEC 62443

# IEC 62443



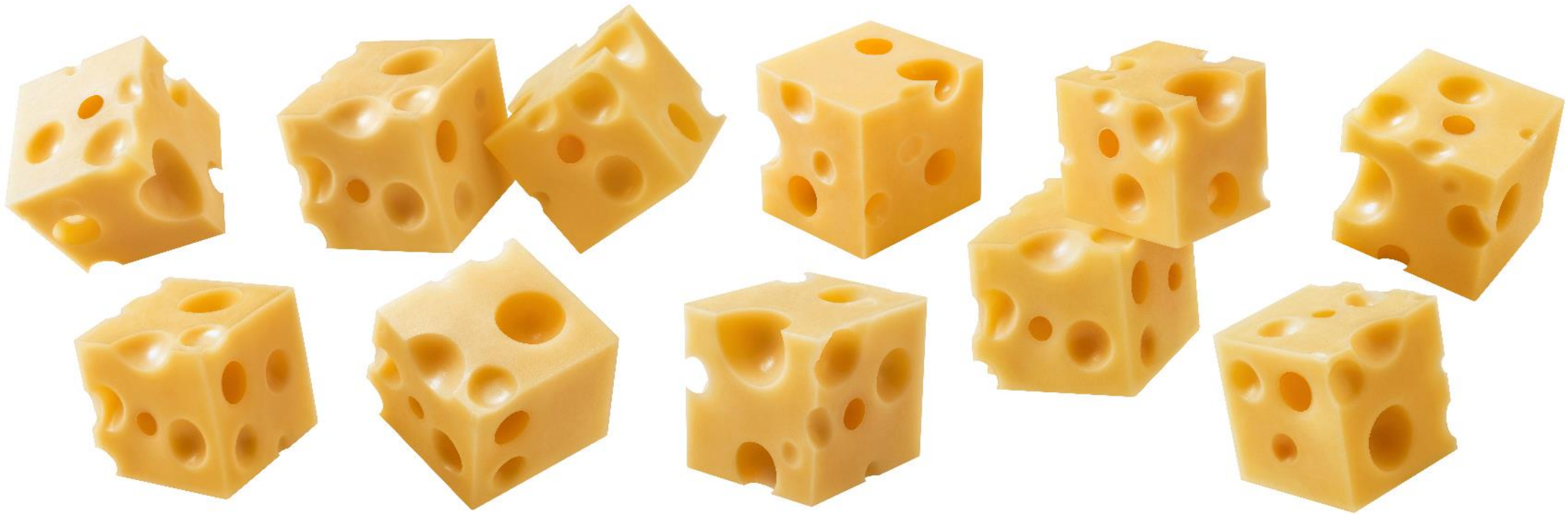


Bild: Adobe Stock

# IEC 62443 - Zonenkonzept



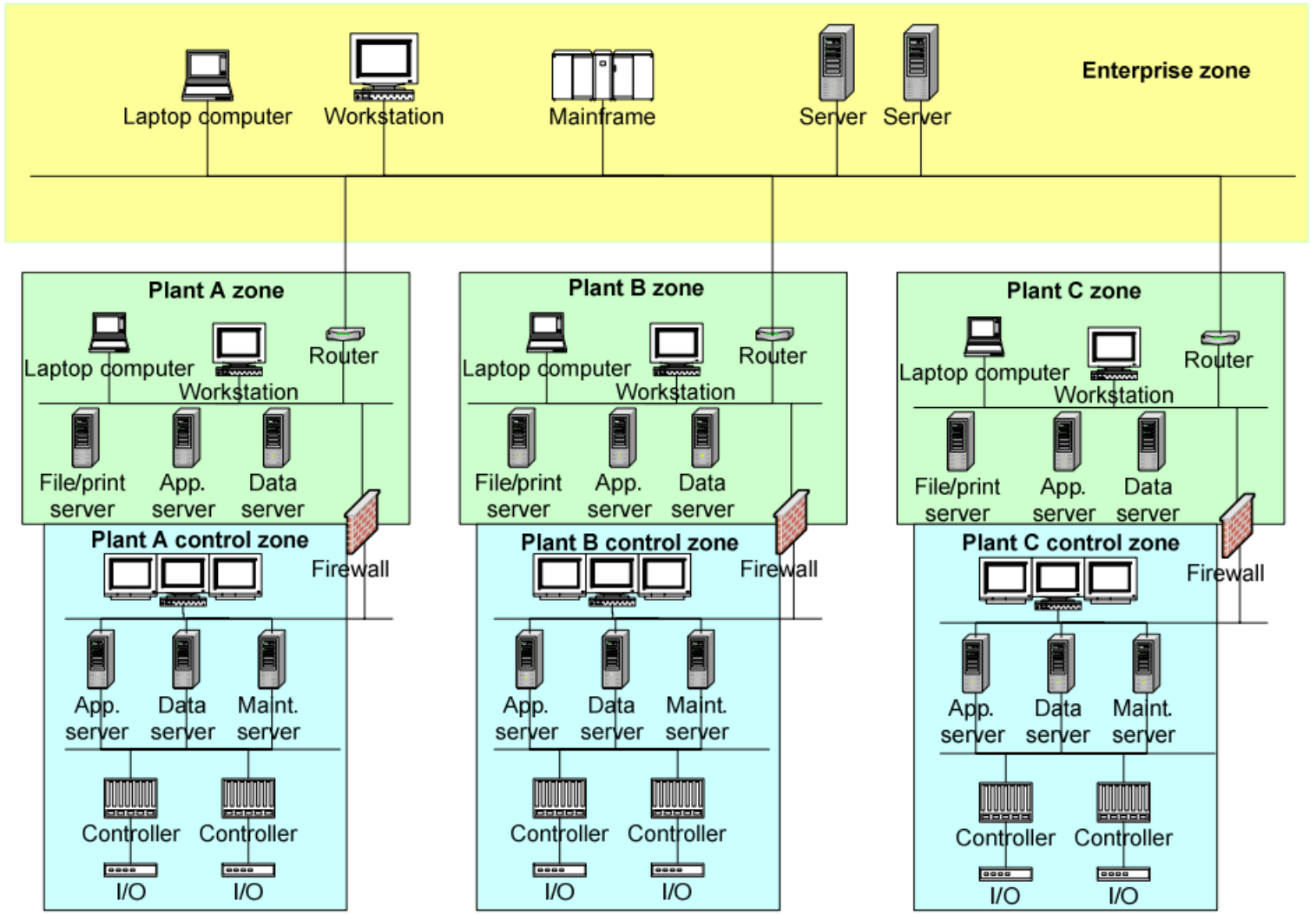



Bild: IEC 62443

# IEC 62443 – Verschachtelte Zonen

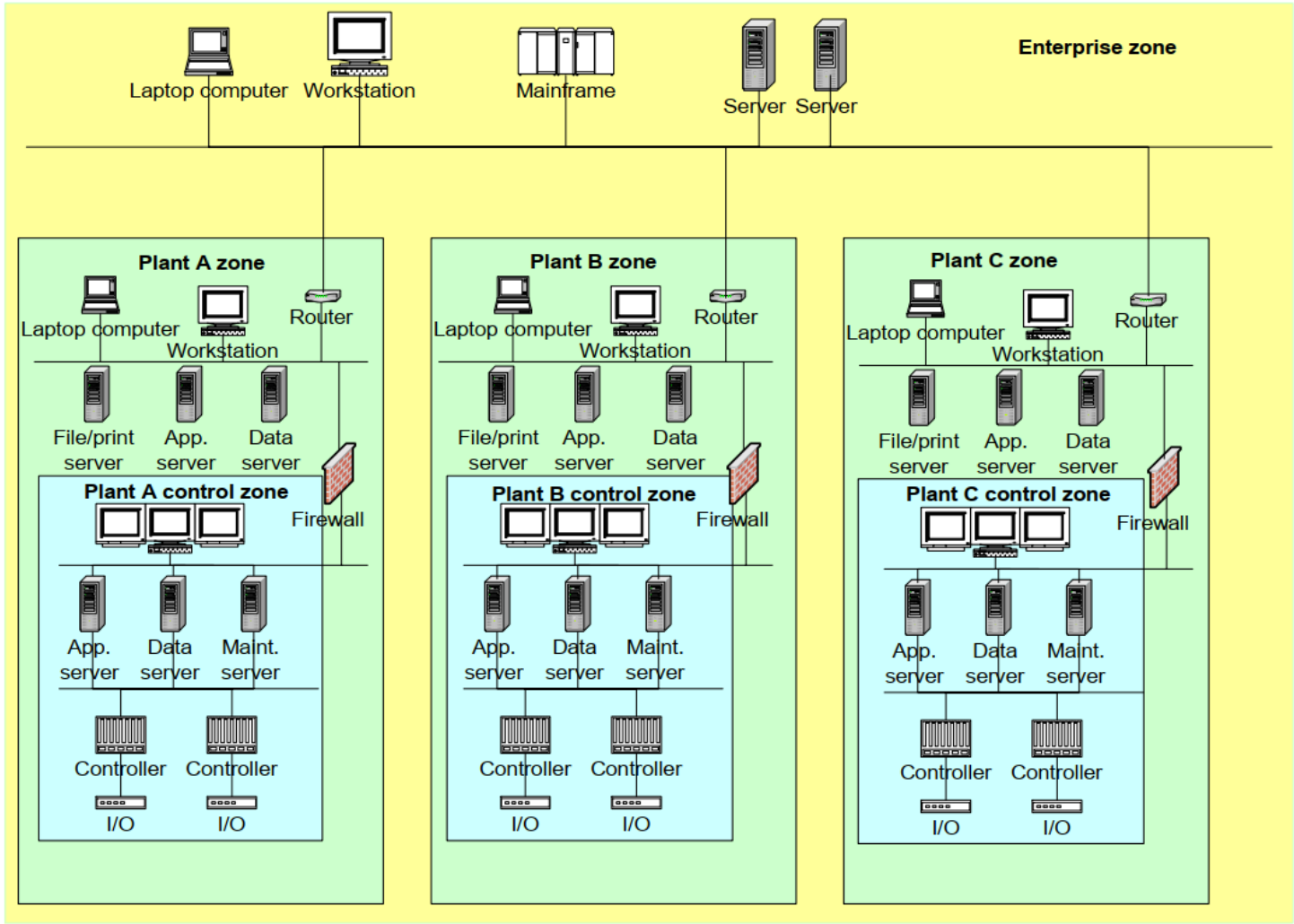



Bild: IEC 62443

# IEC 62443 – SCADA Beispiel

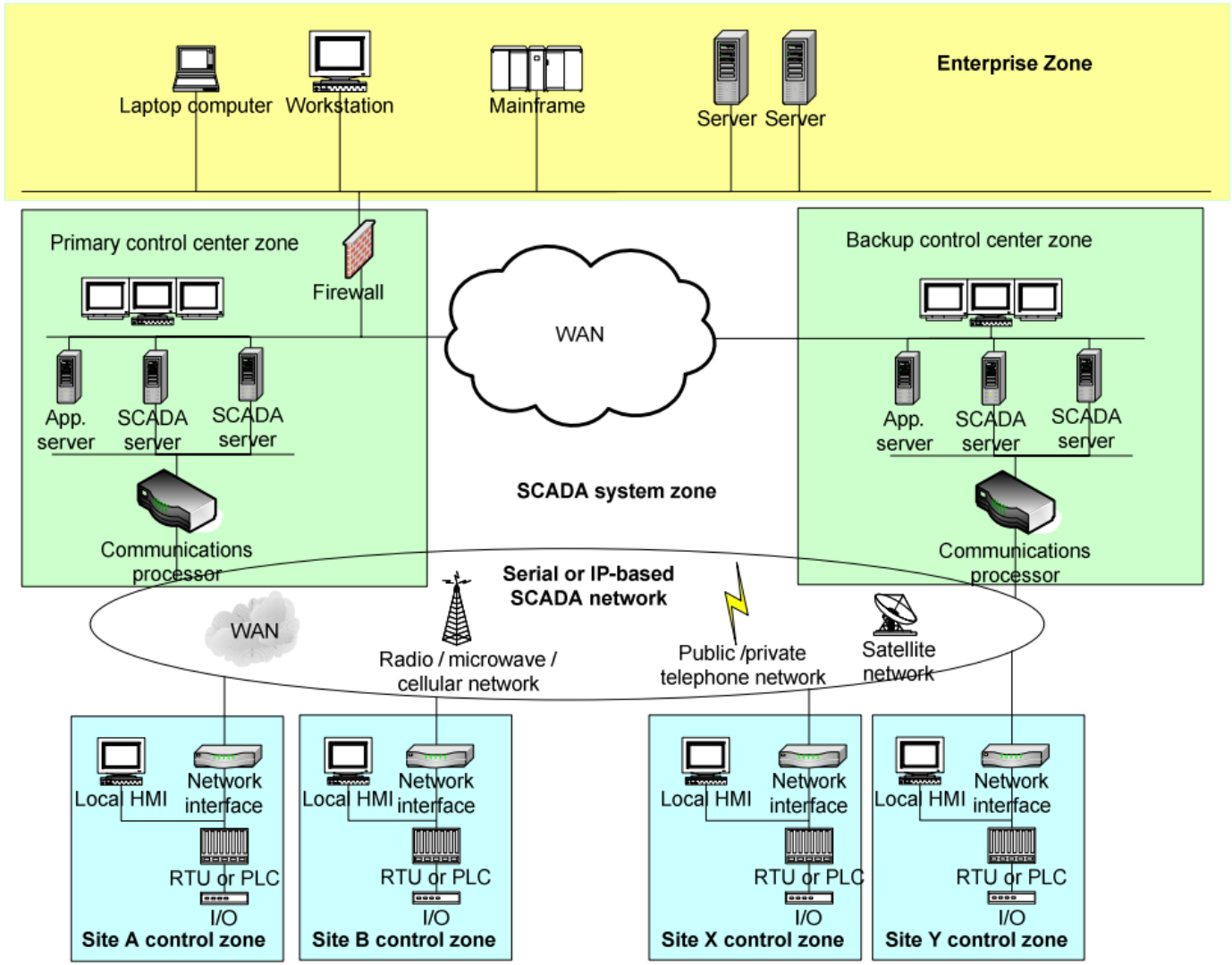



Bild: IEC 62443

# IEC 62443 – Conduits



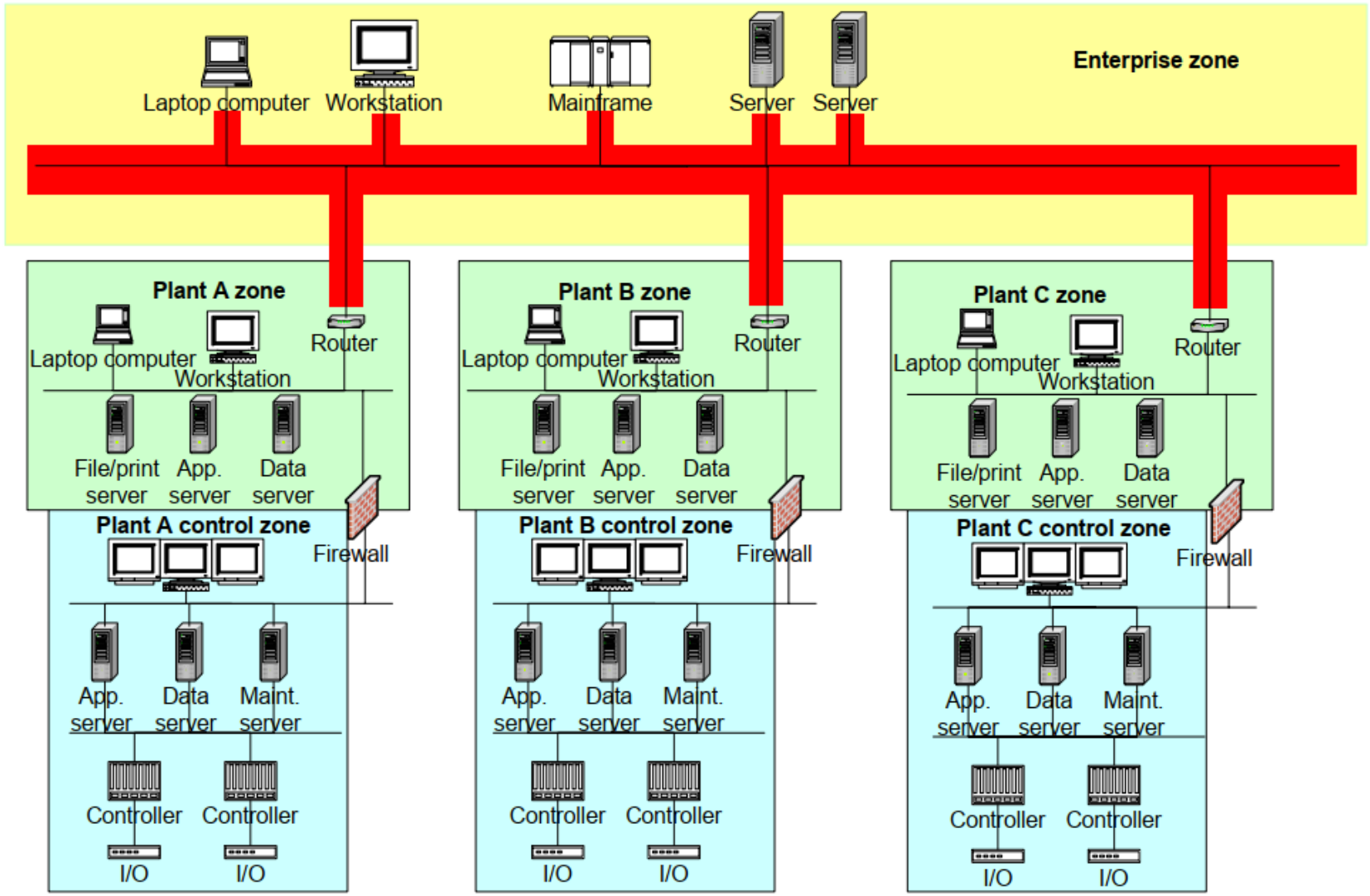



Bild: IEC 62443

# IEC 62443 – SCADA Conduit

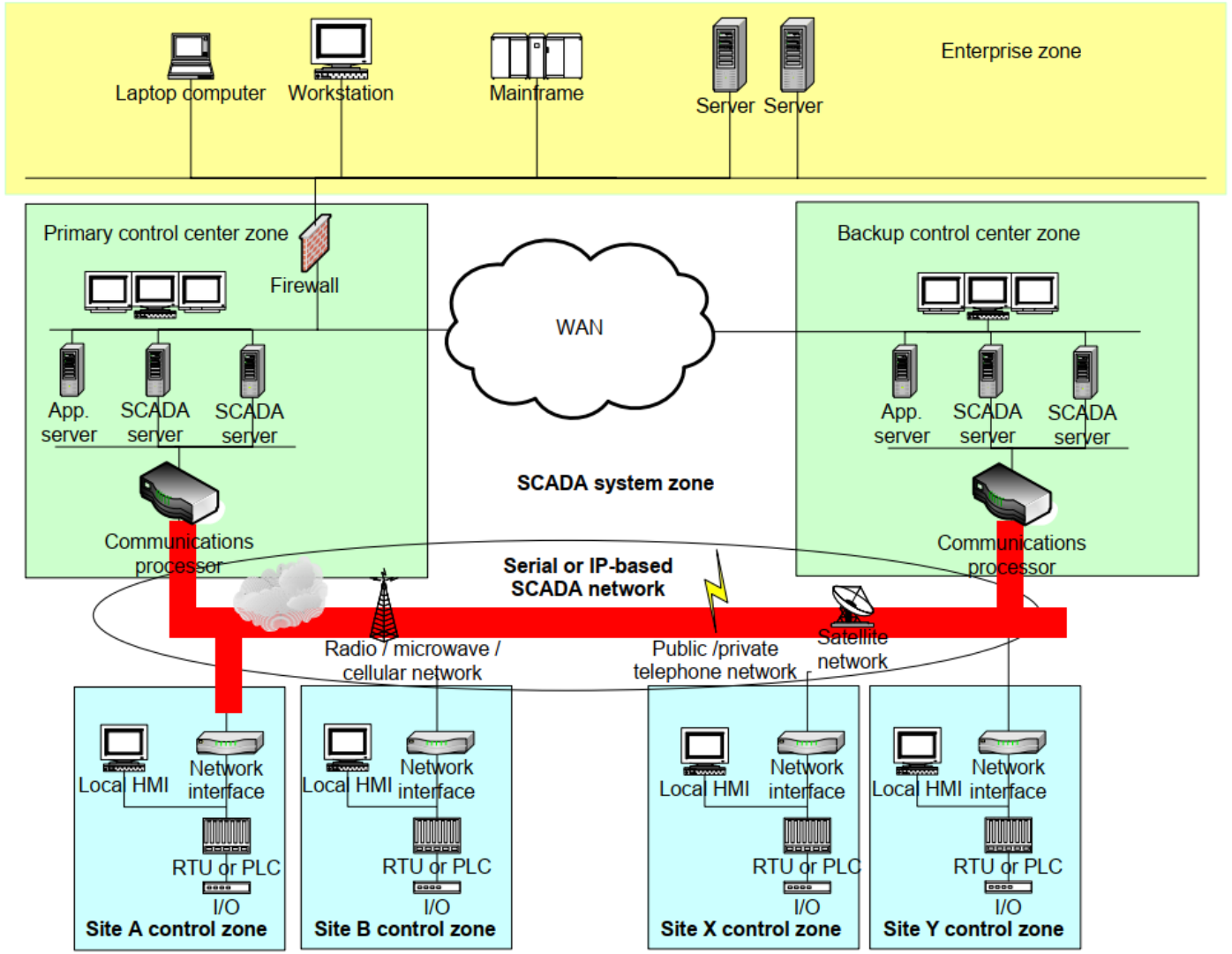



Bild: IEC 62443

# IEC 62443 – Conduits und Channels



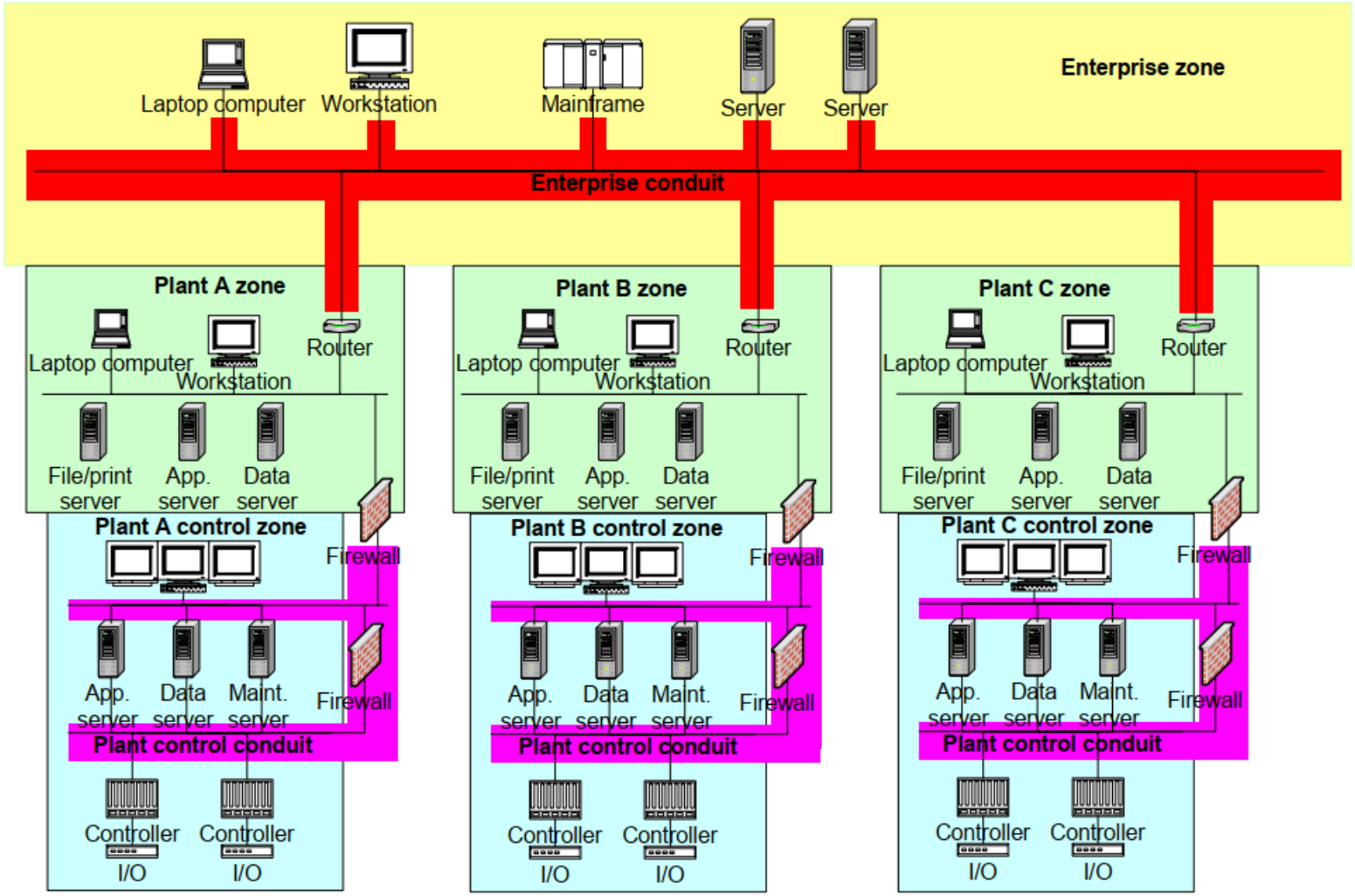



Bild: IEC 62443

# IEC 62443 – Beispiel Fertigung



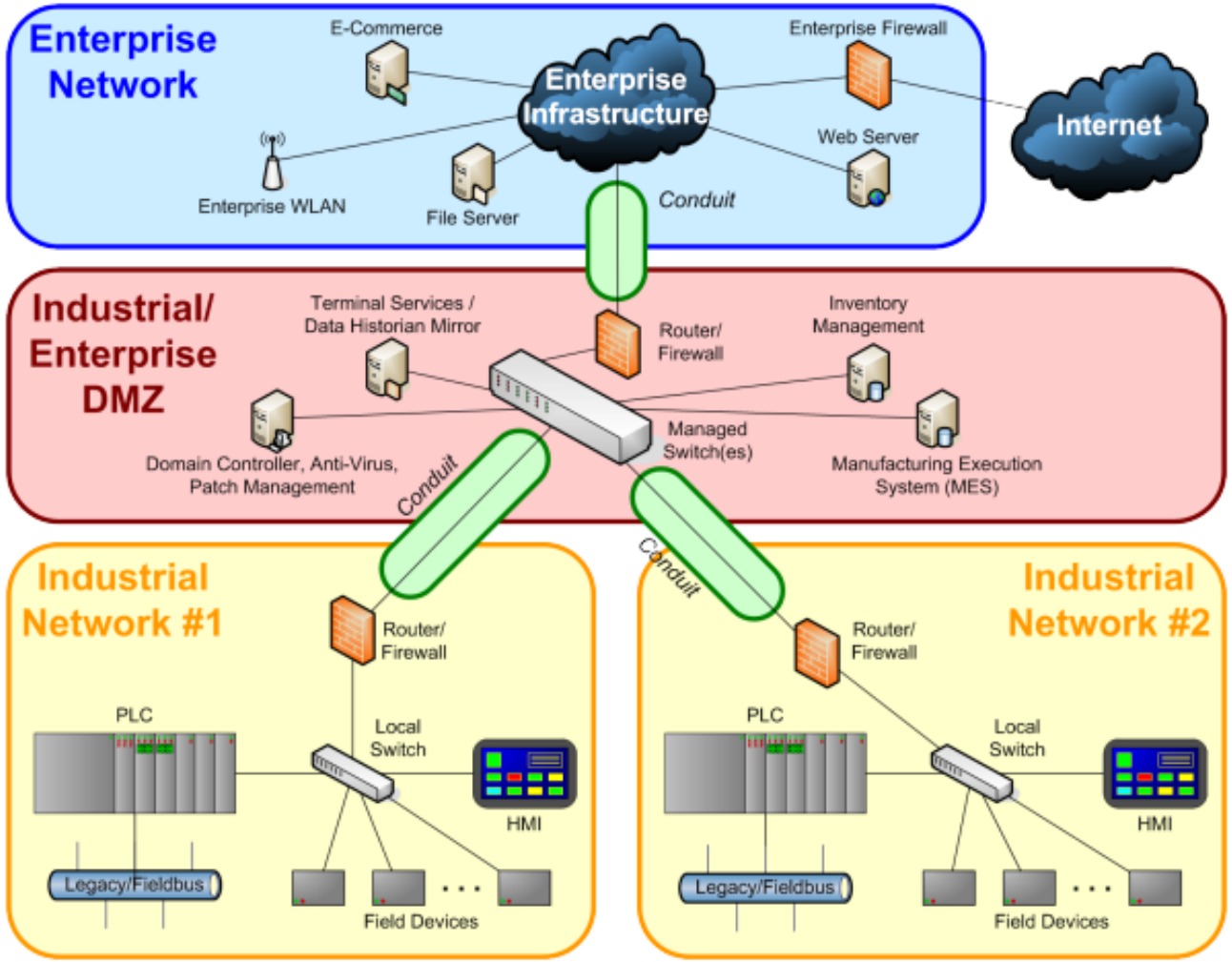



Bild: IEC 62443

# IEC 62443 Beispiel Prozessindustrie



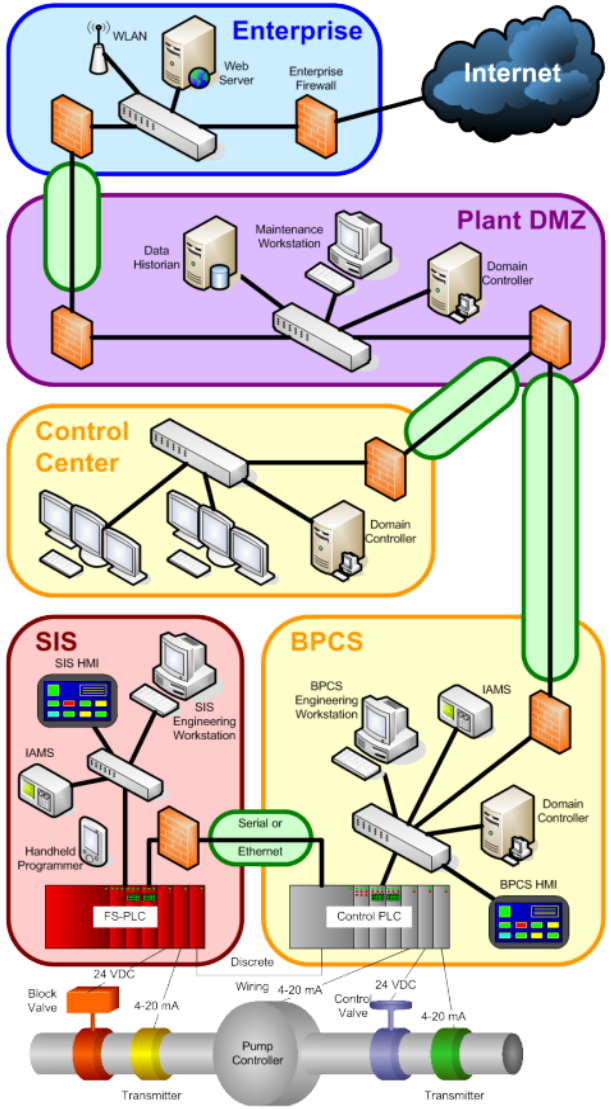



Bild: IEC 62443

# NIST SP800-82



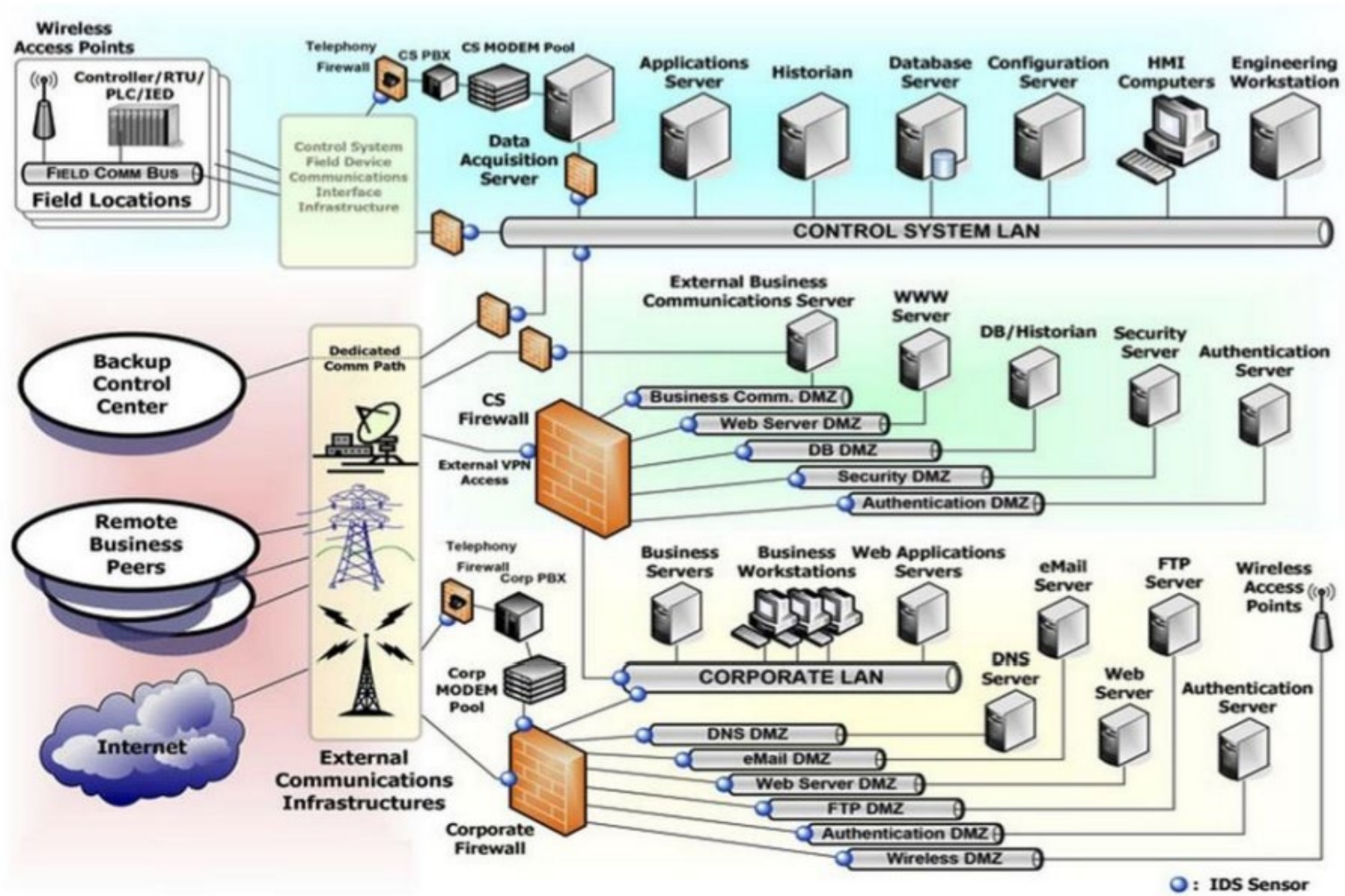



Bild: NIST SP800-82

# Herangehensweise



schrittweises Vorgehen:

- Situationsfeststellung: Identifikation der Assets bzw. der Unternehmenswerte
- Mögliche Bedrohungen analysieren / Schutzbedarfsfeststellung
- Risikobewertung
- Mögliche Schutzmaßnahmen ermitteln und Wirksamkeit bewerten
- Auswahl der geeigneten Maßnahmen
- Umsetzung der Schutzmaßnahmen
- Prozessreview zur Überprüfung der Wirksamkeit

# Herangehensweise



Heute ("Pflicht")

- IT Sicherheitskonzepte adaptieren
- Schwachstellen-Management
- Segmentierung
- Patchen
- Kill Chain unterbrechen
- Supply Chain Hardening
- Prozessreview
- Awareness
- Logmanagement

Morgen ("Kür"):

- Threat Hunting
- Virtualisierung: Verbesserung der RTO
- Anomalieerkennung
- Protokoll-Monitoring
- SIEM / SOAR

**Buchen Sie Ihren IoT Security Check!**

# Kontakt


**Digitalisierung**
**=**
**Mannschaftssport**

**Johannes Fuchs**, M.Sc.
Business Development & Consultant IoT
+49 8586 9604128
+49 151 18068735
johannes.fuchs@sws.de
www.sws.de/iot iot@sws.de

**Hans-Martin Kuhn**
Senior Security Consultant
+49 941 20605 429
+49 151 18069009
hans-martin.kuhn@sws.de
www.sws.de

# Weiter Infos und Verlinkungen

**Melden Sie sich an, bleiben Sie Up 2 Date und erfahren Sie praxisnah, wie unsere Kunden durch Digitalisierung profitieren!**

**IoT Newsletter**

**IoT Webinar-Reihe**

**Termin folgt Teil 9: Microsoft Powerapps**

**IoT Terminbuchung**

**Prüfen Sie kostenlos Ihre individuellen Fördermöglichkeiten!**

**Förderschnellcheck**