Öffentlich (IV)

100 Jahre Leidenschaft für Technologie und Innovation

Willkommen

Industrial Cyber Security: Herausforderungen und Lösungen der neuen MVO

PHOENIX CONTACT

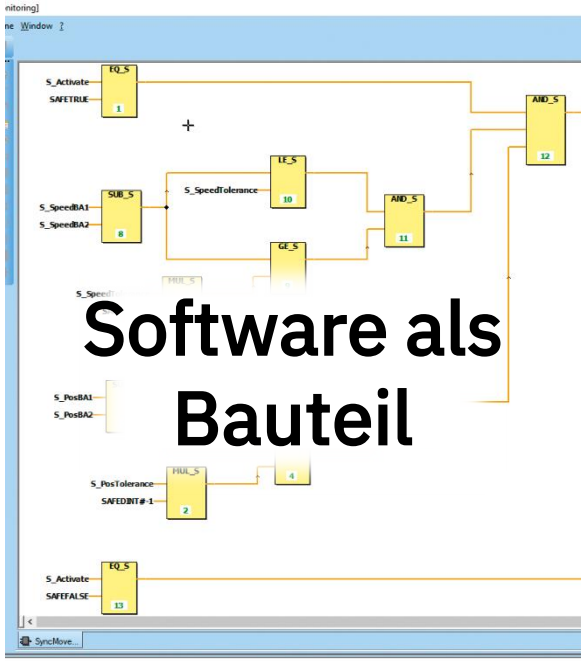
Agenda

- Motivation – Die neue MVO
- Begriffe, Maßnahmen und Konzepte
- Sicheres Anlagendesign
  - Risikomanagement

Motivation

MVO

Die bisherige MRL ist aus 2006, bzw. 2009
→ Neue Herausforderungen nicht betrachtet



Motivation

MVO

- Besonderer Bezug auf Security-Themen im Abschnitt „Schutz gegen Verfälschungen“ (Anh. III, 1.1.9)
  - Kontrolle von lokalen und entfernten Schnittstellen
  - Verwendete Hardware-Komponenten müssen gehärtet sein
  - Sicherheitskritische Software muss dokumentiert sein
  - Sicherheitskritische Software muss geschützt werden
  - Zugriffsprotokollierung

Motivation

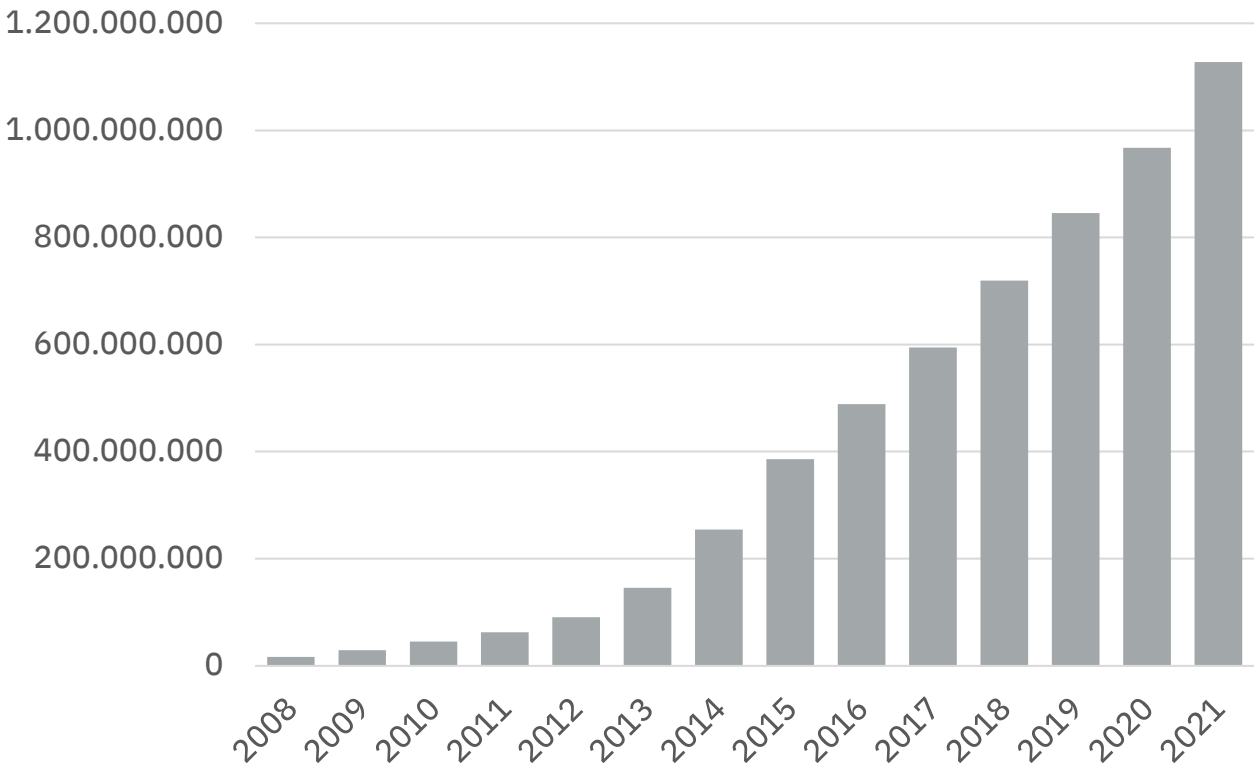
MVO

- Besonderer Bezug auf Security-Themen im Abschnitt „Schutz gegen Verfälschungen“ (Anh. III, 1.1.9)
  - Kontrolle von lokalen und entfernten Schnittstellen
    - → *Bedrohungsanalyse und Netzwerkdesign*
  - Verwendete Hardware-Komponenten müssen gehärtet sein
    - → *technische Maßnahmen*
  - Sicherheitskritische Software muss dokumentiert sein
    - → *Asset-Erfassung*
  - Sicherheitskritische Software muss geschützt werden
    - → *Schutzbedarfsanalyse*
  - Zugriffsprotokollierung
    - → *technische und organisatorische Maßnahmen*

Motivation

Bedrohungslage

Neun von zehn Unternehmen (88 Prozent) waren 2020/2021 von Angriffen betroffen.



TOP 3 Bedrohungen im OT-Umfeld:

1. Einschleusen von Schadsoftware über Wechseldatenträger und mobile Systeme
2. Infektion mit Schadsoftware über Internet und Intranet
3. Menschliches Fehlverhalten und Sabotage

Quellen: bitkom, AV-Atlas, BSI

Motivation

Bedrohungslage

*„Vor allem kleine und mittlere Anlagen sind **schlecht** geschützt“*

*„In nur **wenigen Minuten** konnte zahlreiche unverschlüsselte Login-Seiten gefunden werden.“*

*„Für den Login auf die Steuerung genügte das **Standard-Passwort**..“*

*„Die Anlage könnte **mit einem Klick** heruntergefahren werden.“*

*„Fälle von gezielten Angriffen können schnell zu **Problemen für die Energieversorgung** in Deutschland führen.“*

Schutzziele

Availability (Verfügbarkeit)
Informationen bzw. Systeme müssen abrufbar sein

Integrity (Integrität)
Information dürfen nicht verfälscht werden

Confidentiality (Vertraulichkeit)
Informationen dürfen nur von berechtigten Personen eingesehen werden

Begriffe, Maßnahmen und Konzepte

Unterschiede IT- und OT-Security

Information Technology

Vertraulichkeit

Integrität

Verfügbarkeit

≠

Operation Technology

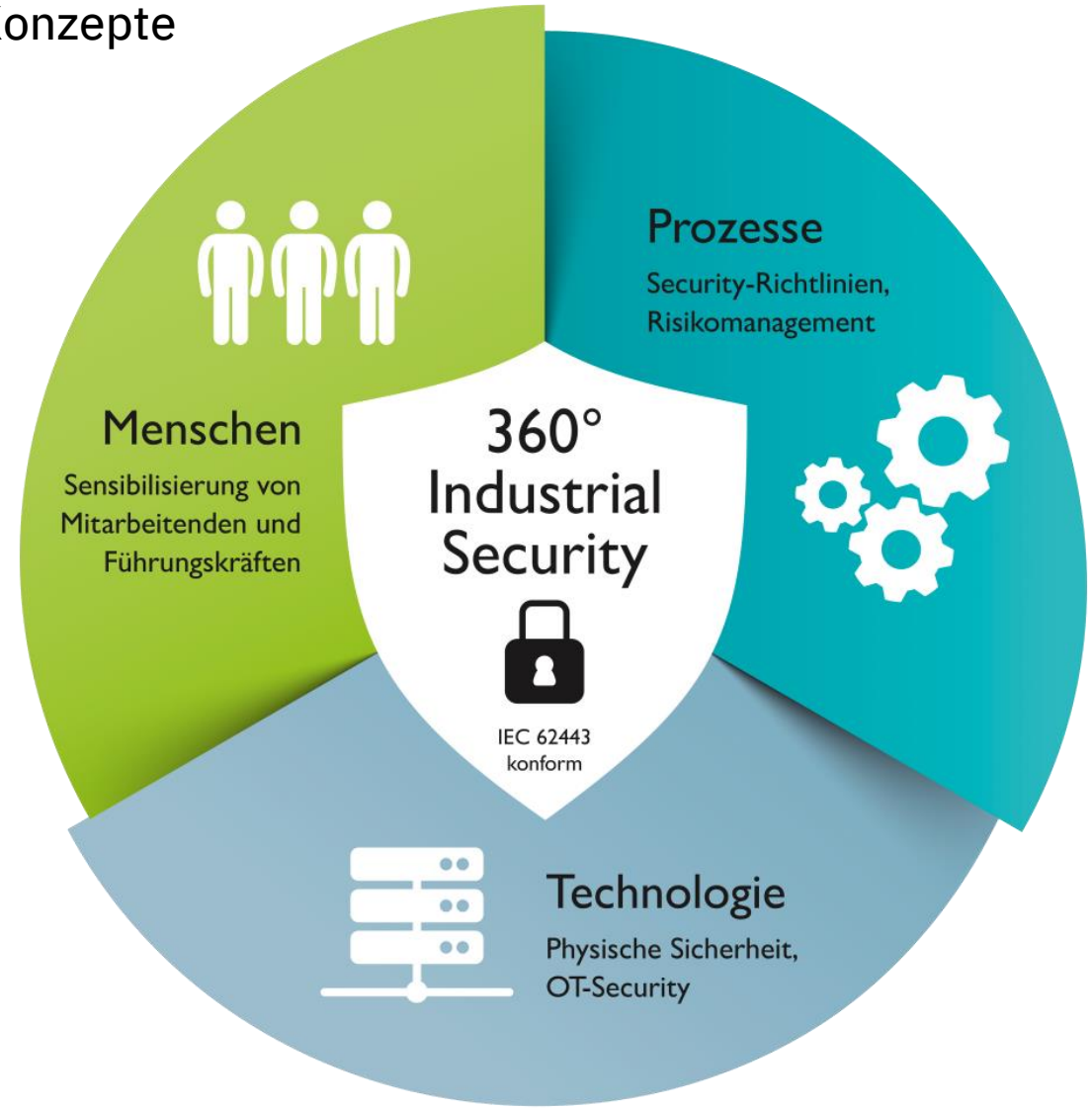
Verfügbarkeit

Integrität

Vertraulichkeit

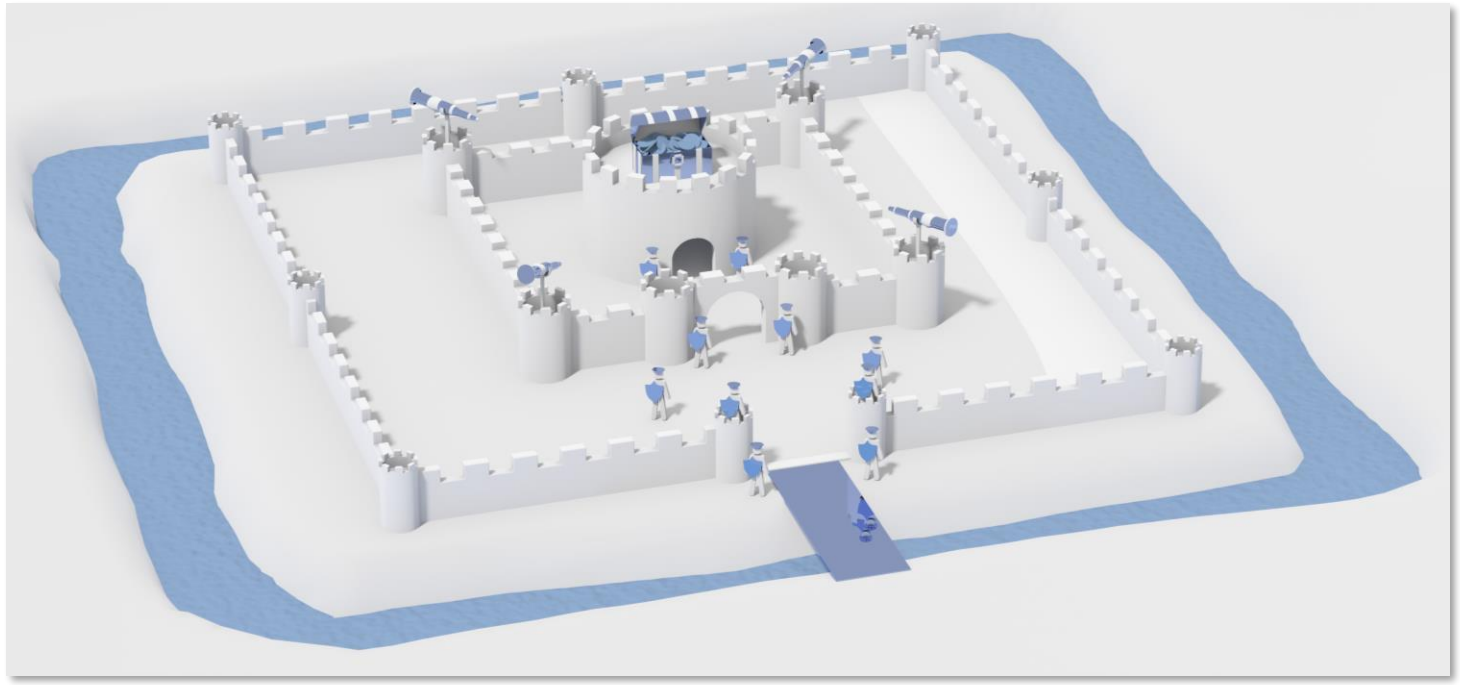
Begriffe, Maßnahmen und Konzepte

Maßnahmen



Begriffe, Maßnahmen und Konzepte

Defense in Depth



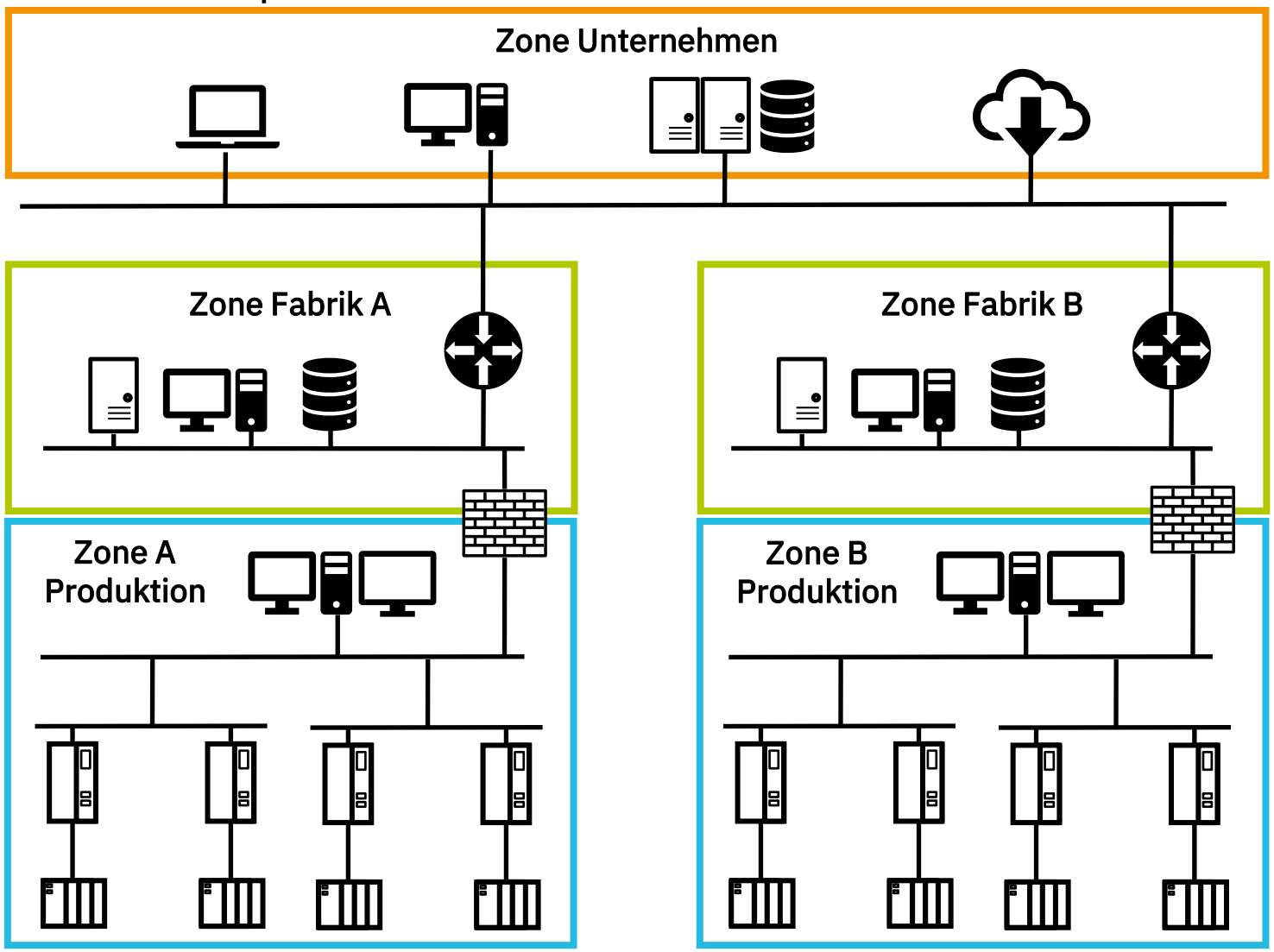
Anlagensicherheit:
Technische und organisatorische Maßnahmen
- Prozesse
- Schulung
- Berechtigungskonzept
- Erkennung von Angriffen

Netzwerksicherheit:
Absicherung/ Kontrolle von Zutritt, Zugang, Zugriff
- Zellenschutz
- Zonen, Conduits
- Firewalls und VPN

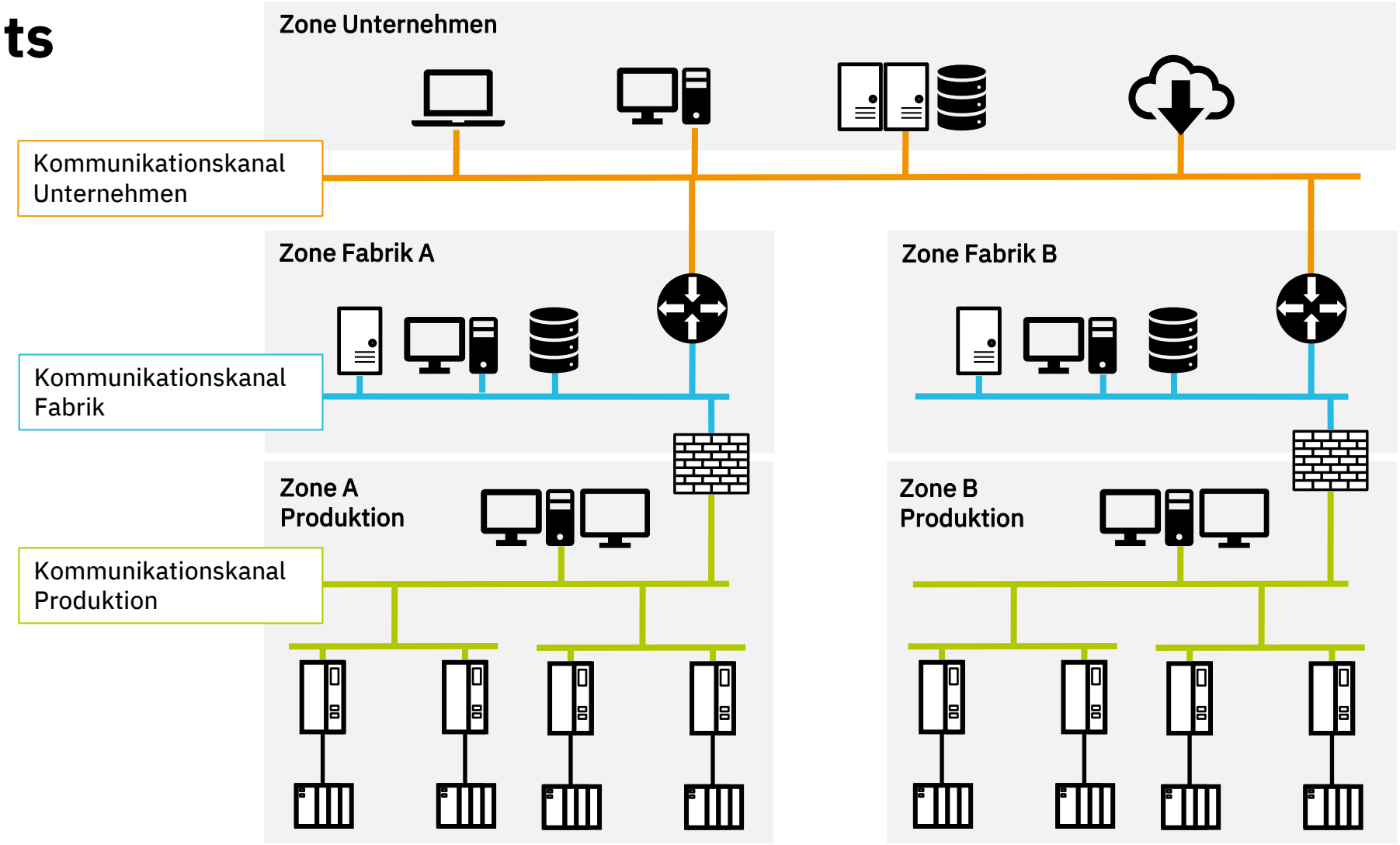
Systemintegrität:
Schutz der Lösung
- Systemhärtung
- Authentifizierung/ Benutzerverwaltung
- Patch Management

Implementierung gestaffelter, auf mehreren Ebenen ansetzende und sich ergänzende Sicherheitsmaßnahmen.

Zones


Zone Unternehmen
Zone Fabrik A
Zone Fabrik B
Zone A
Produktion
Zone B
Produktion

Conduits

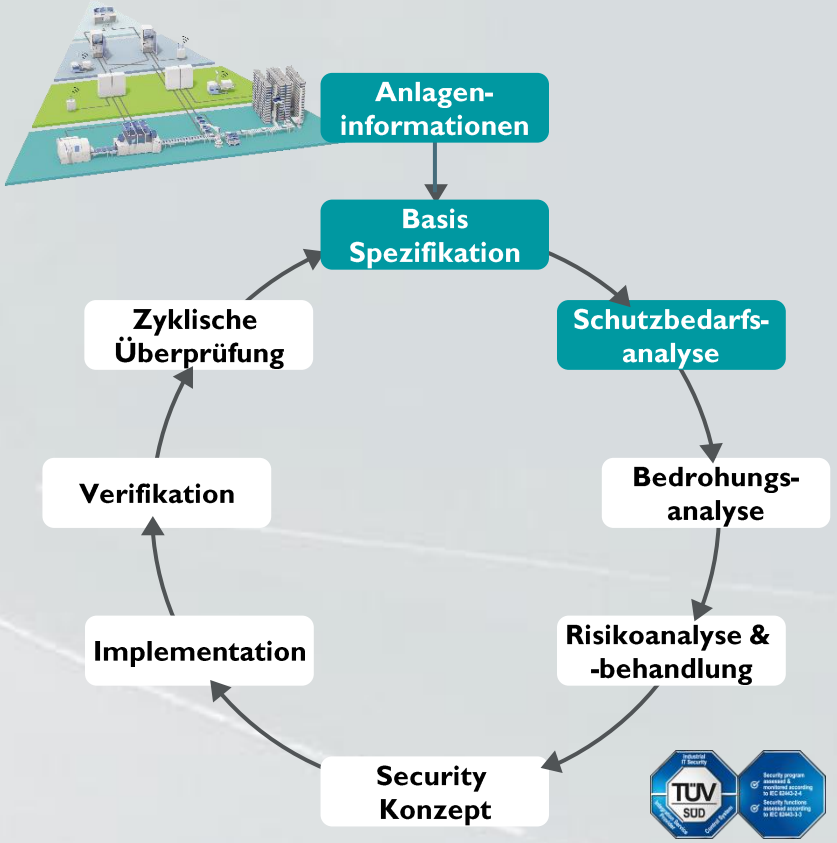

Zone Unternehmen
Kommunikationskanal Unternehmen
Zone Fabrik A
Zone Fabrik B
Kommunikationskanal Fabrik
Zone A Produktion
Zone B Produktion
Kommunikationskanal Produktion

Sicheres Anlagendesign

Beispielhafte Vorgehensweise

Aktivitäten (auszugsweise)

- Sammeln von Informationen zu Assets und Anlagenumfeld
- Bestimmung besonders schützenswerter Informationen und Assets
- Erstellen einer Basisspezfikation unter Beachtung notwendiger Themengebiete
- Schutzbedarf und Schutzziele der schützenswerten Assets definieren
- Zonen und Conduits festlegen



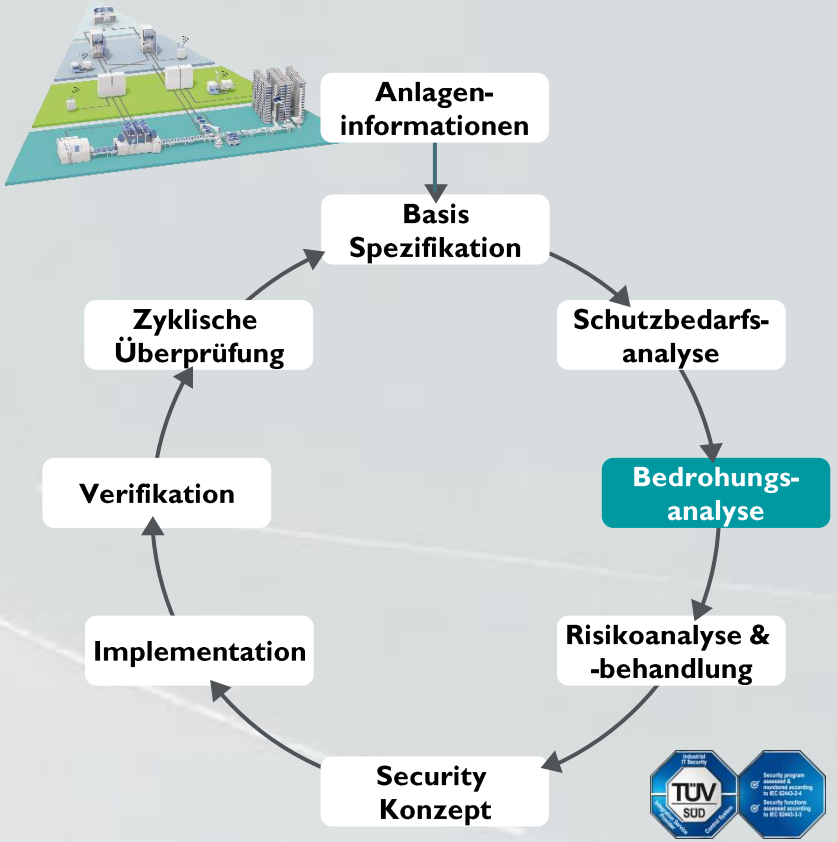
Sicheres Anlagendesign

Beispielhafte Vorgehensweise

Aktivitäten

Identifizierung relevanter Bedrohungen für die Automatisierungslösung

- Abstimmung und ggf. Erweiterung des Bedrohungskatalogs mit dem Betreiber
- Bewertung der Bedrohungen bezüglich der Relevanz für die Automatisierungslösung



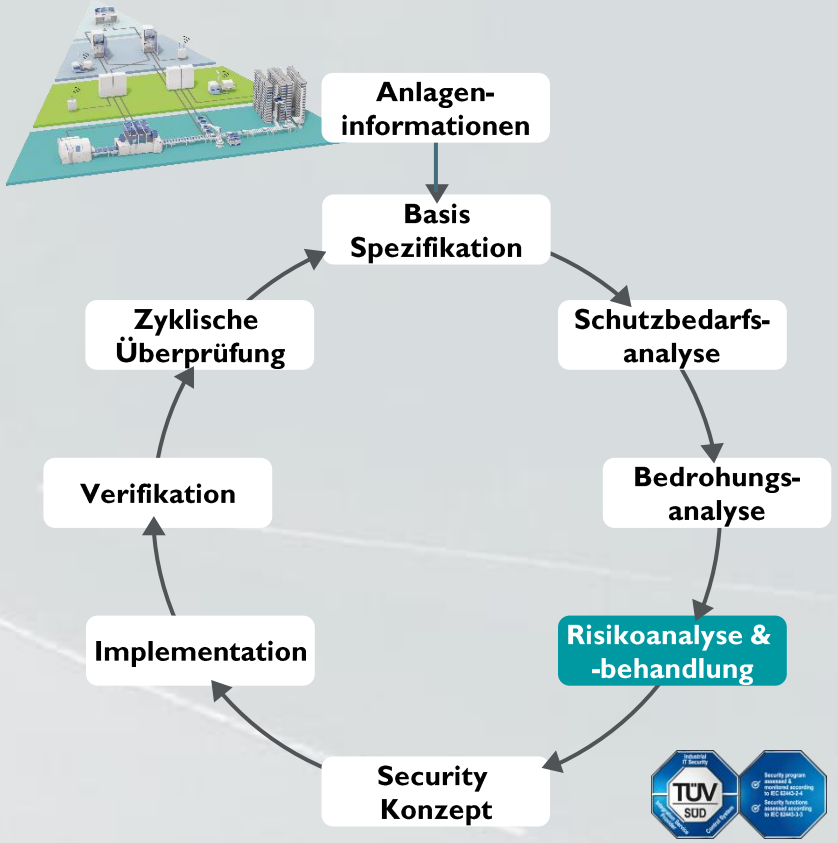
Sicheres Anlagendesign

Beispielhafte Vorgehensweise

Aktivitäten

Erstellung eines Risk Assessments in dem folgenden Punkte erfasst sind:

- Ermittlung der Risikotoleranz des Betreibers
- Bewertung der erkannten Bedrohungen auf Basis der Security Spezifikation
- Maßnahmenvorschläge zur Risikominimierung

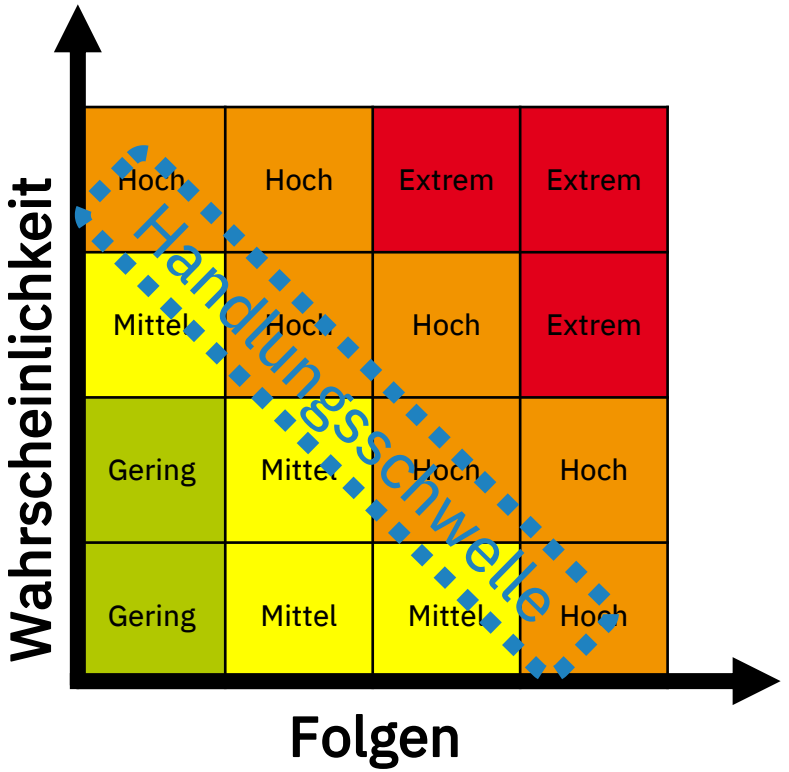


Risikomanagement

Risikoanalyse

Risikobewertung:

- Schwachstellen
- Bedrohung
- Folgen/Schaden



Risiko = Bedrohung x Schwachstelle x Folgen

Wahrscheinlichkeit

Risikomanagement

TID	Bedrohung - Szenario	Risiko ohne Maßnahmen	Risiko mit Maßnahmen	Maßnahmen	Kosten Schätzung	Risk Owner	Status	Frist zur Umsetzung
1	<Hier werden die Bedrohungen aus der Bedrohungsanlayse eingefügt>	Hoch	Gering	<Maßnahmen zur Risikominderung definieren>	<Kostensc hätzung>	<Verantwortlic hen einfügen>	Umgesetzt	Offen
2	<Hier werden die Bedrohungen aus der Bedrohungsanlayse eingefügt>	Hoch	Mittel	<Maßnahmen zur Risikominderung definieren>	<Kostensc hätzung>	<Verantwortlic hen einfügen>	Risiko akzeptiert	Offen

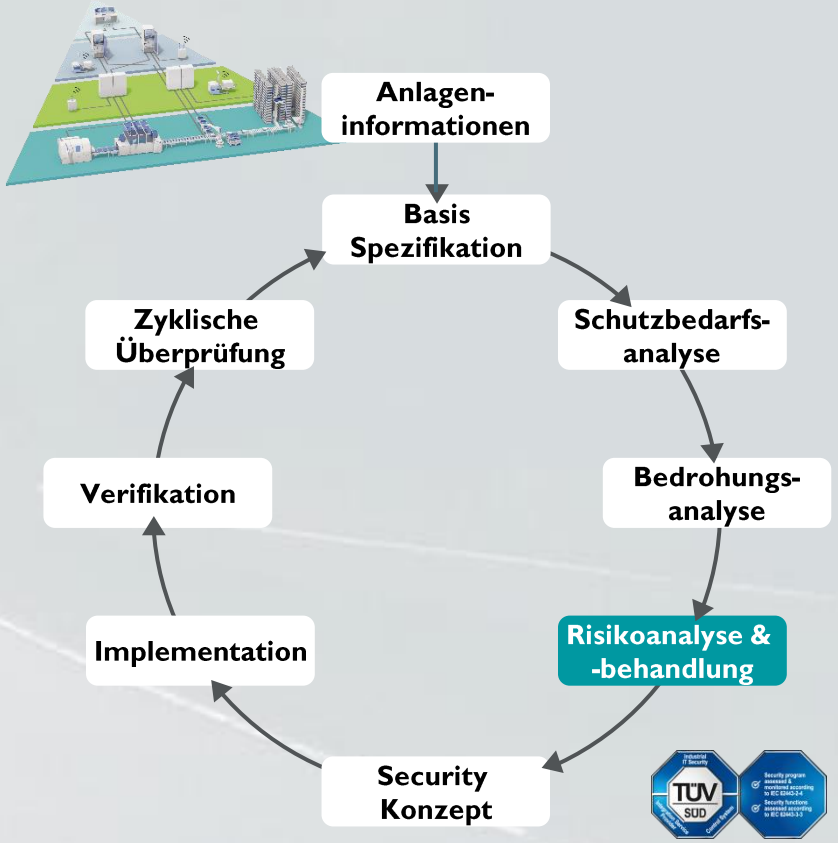
Sicheres Anlagendesign

Beispielhafte Vorgehensweise

Aktivitäten

Erstellung eines Risk Assessments in dem folgenden Punkte erfasst sind:

- Ermittlung der Risikotoleranz des Betreibers
- Bewertung der erkannten Bedrohungen auf Basis der Security Spezifikation
- Maßnahmenvorschläge zur Risikominimierung

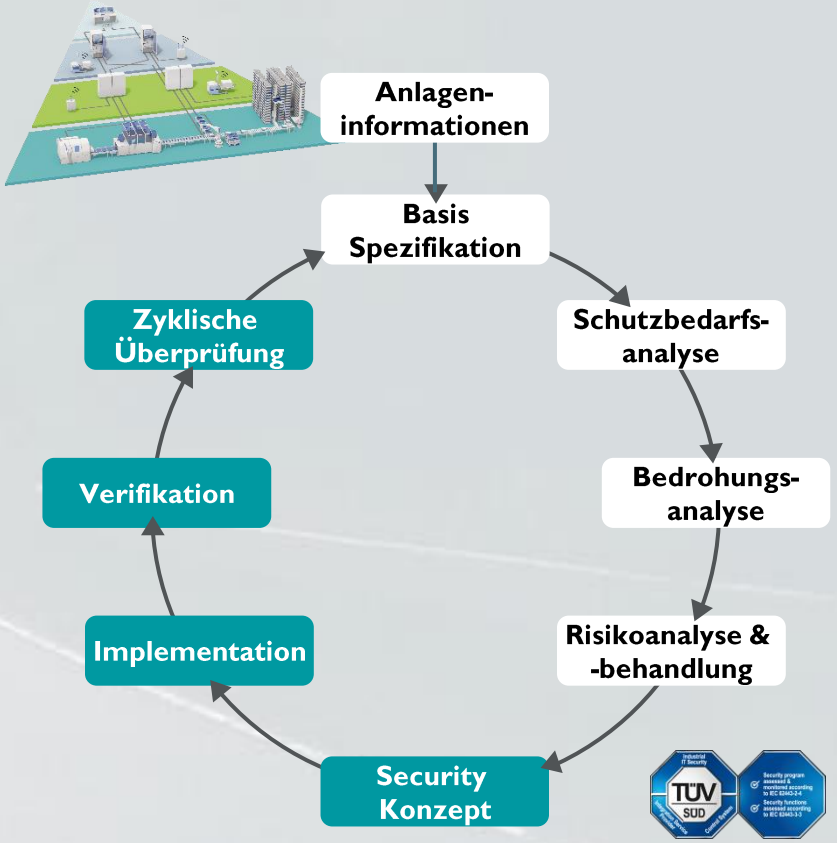


Sicheres Anlagendesign

Beispielhafte Vorgehensweise

Aktivitäten (auszugsweise)

- Security Konzept: Basis wird durch risikomindernde Maßnahmen ergänzt
- Zyklische Überprüfung: In regelmäßigen Abständen wird auf neue Bedrohungen und die Wirksamkeit des bestehenden Konzepts geprüft



Mathis Mohr
Industrial Security Consultant

PHOENIX CONTACT
Deutschland GmbH

Tel.: +49 5281 946-2155
E-Mail: mathis.mohr@phoenixcontact.de

100 Jahre Leidenschaft für Technologie und Innovation

Danke

Industrial Cyber Security: Herausforderungen und Lösungen der neuen MVO