WKO - SAFETY DAY

Keine Safety ohne Security

Maschinensicherheit in der Operational Technology (OT)

14.10.2024

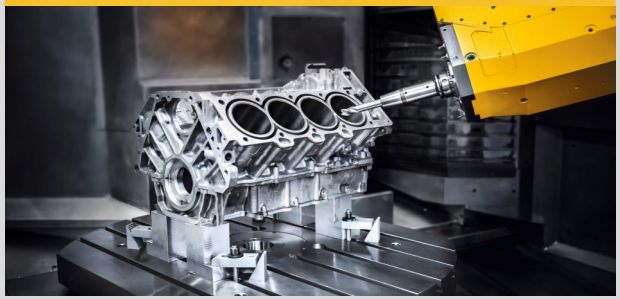
PILZ
THE SPIRIT OF SAFETY

Unsere Mission

Ganzheitliche Lösungen in allen Branchen

Verpackungstechnik

Maschinenbau und Robotik



Nahrungsmittelindustrie

Automobilindustrie

Brennertechnologie

Fördertechnik und Logistik

Ganzheitliche Lösungen in allen Branchen

Amusement

Chemie- und Pharmaindustrie

Prozessindustrie

Seilbahntechnik

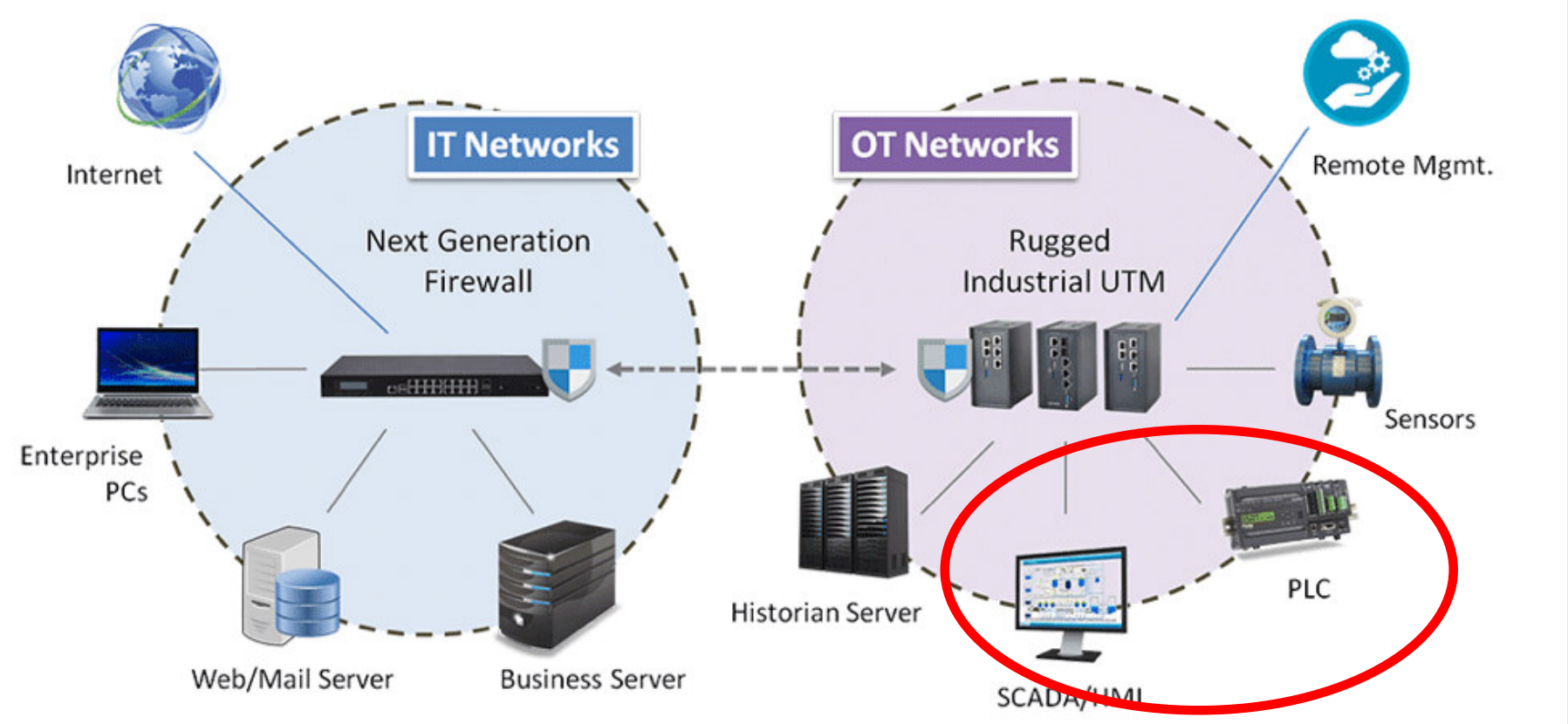
Holz und Papierindustrie

Transportwesen

Portfolio

Sonntag, 13. Oktober 2019 – 13:00

Einfallstor im Juni (!!) 2019 ….



01

Keine Safety ohne Security

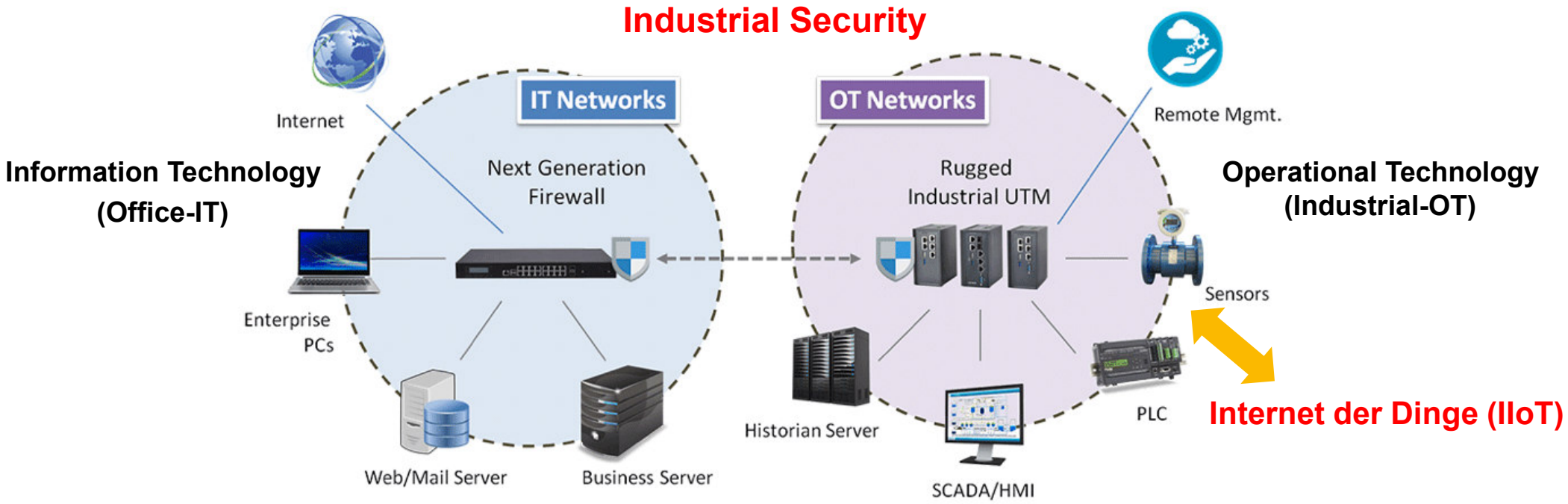
Maschinensicherheit in der Operational Technology (OT)

Cyber Security → Industrial Security

IT und OT Network Security

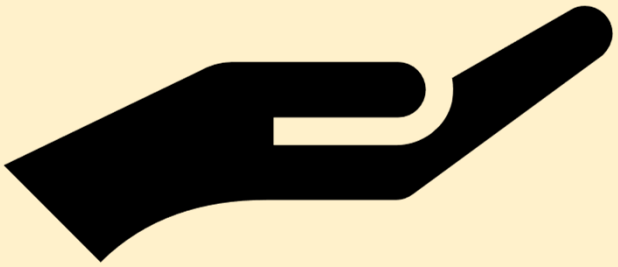
Industrie 4.0 ist gekennzeichnet von einer **zunehmenden Vernetzung** von Anlagen und der umfassenden Analyse und Auswertung der gesammelten Datenmengen.

… **bisher getrennte Welten beginnen zu verwachsen**



Erreichen der Sicherheitsziele ist oberste Priorität

Vertraulichkeit (Confidentiality)

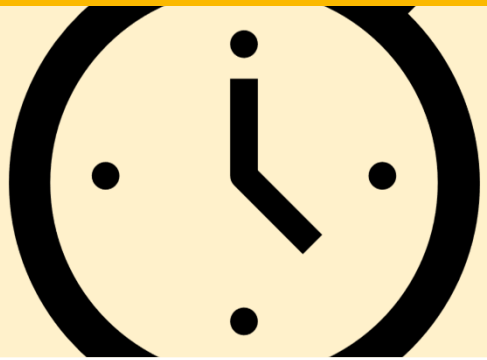


Daten dürfen nur von **autorisierten Benutzern** gelesen oder geändert werden. Dies gilt sowohl für den Zugriff auf gespeicherte Daten als auch während der Datenübertragung.

Integrität (Integrity)

Daten dürfen nicht unwissentlich verändert werden. Alle Änderungen müssen nachvollziehbar sein.

Verfügbarkeit (Availability)



Verhinderung v. Systemausfällen. Der Zugriff auf die Daten muss innerhalb eines vereinbarten Zeitraums gewährleistet sein.

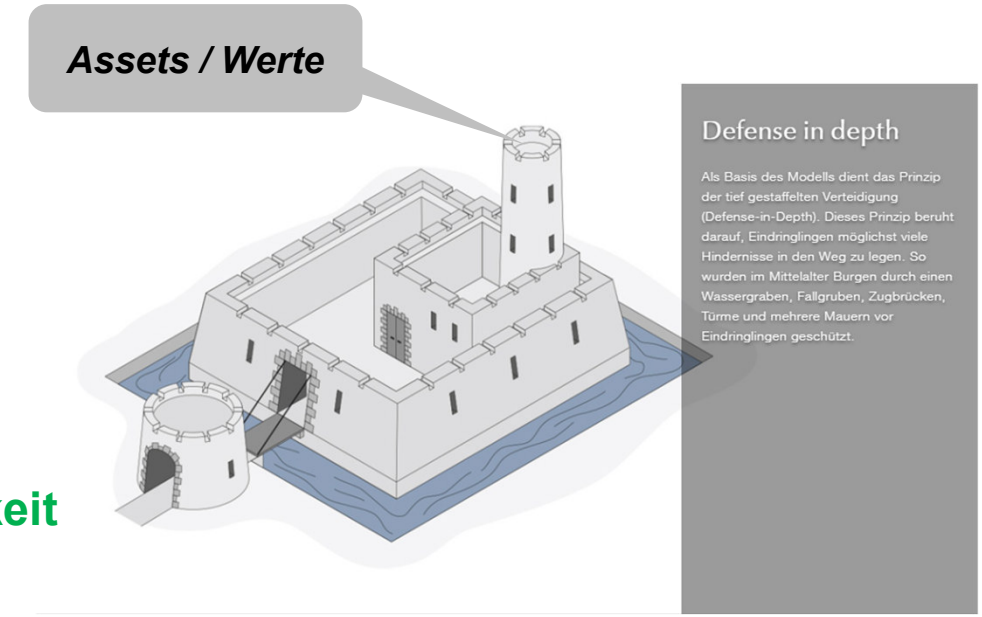
IT

OT

Grundlegende Anforderungen an Industrial Security

→ technische und organisatorische Maßnahmen

- **Grundsatz der**
  Vertraulichkeit
- **Grundsatz der**
  Integrität
- **Grundsatz der**
  Verfügbarkeit und Belastbarkeit
- **Grundsatz der**
  regelmäßigen Überprüfung, Bewertung und Evaluierung



IEC 62443 - Security-Risk Management

1. **Assets/Werte** identifizieren
2. **Threats/Bedrohungen** analysieren
3. Relevante **Schutzziele** ermitteln
4. **Risiken** analysieren und bewerten
5. **Schutzmaßnahmen** wählen und umsetzen
6. **Resilienzmanagement**

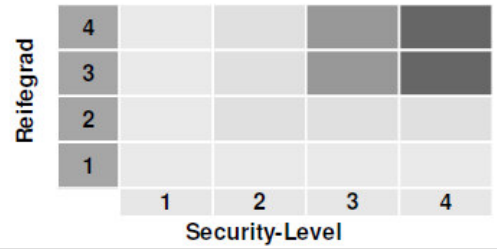
Normen für eine holistische Security

Schutzlevel = funktionale + organisatorische Maßnahmen

Bewertung der umgesetzten funktionalen Maßnahmen	
SL 1	Fähigkeit zum Schutz gegen ungewollten, zufälligen Missbrauch
SL 2	Fähigkeit zum Schutz gegen gewollten Missbrauch unter Verwendung von einfachen Mitteln, mit niedrigem Aufwand, allgemeinen Kompetenzen und niedriger Motivation
SL 3	Fähigkeit zum Schutz gegen gewollten Missbrauch unter Verwendung von technisch ausgefeilten Mitteln, mit moderatem Aufwand, automatisierungs-technisch spezifischen Kompetenzen und moderater Motivation
SL 4	Fähigkeit zum Schutz gegen gewollten Missbrauch unter Verwendung von technisch ausgefeilten Mitteln, mit erheblichem Aufwand, automatisierungstechnisch spezifischen Kompetenzen und hoher Motivation

Bewertung der Umsetzung der organisatorischen Maßnahmen	
ML 1	Initial – Die Prozesse sind ad-hoc, schwach kontrolliert und nicht voraussagbar.
ML 2	Managed – Es werden Prozesse reaktiv gelebt.
ML 3	Defined – Die Prozesse sind beschrieben und werden proaktiv umgesetzt.
ML 4	Optimized – Die Prozesse werden bewertet, kontrolliert und kontinuierlich verbessert.

Schutz-Levels



PL 1	Schutz gegen ungewollten, zufälligen Missbrauch
PL 2	Schutz gegen gewollten Missbrauch unter Verwendung von einfachen Mitteln, mit niedrigem Aufwand, allgemeinen Kompetenzen und niedriger Motivation
PL 3	Schutz gegen gewollten Missbrauch unter Verwendung von technisch ausgefeilten Mitteln, mit moderatem Aufwand, automatisierungstechnisch spezifischen Kompetenzen und moderater Motivation
PL 4	Schutz gegen gewollten Missbrauch unter Verwendung von technisch ausgefeilten Mitteln, mit erheblichem Aufwand, automatisierungstechnisch spezifischen Kompetenzen und hoher Motivation

PL → **Security Program Rating** (**SPR**) in neuen Auflagen

Segmentierung der Netzstruktur - IEC 62443

Netzwerke nach dem „Zones und Conduits“-Modell unterteilen.

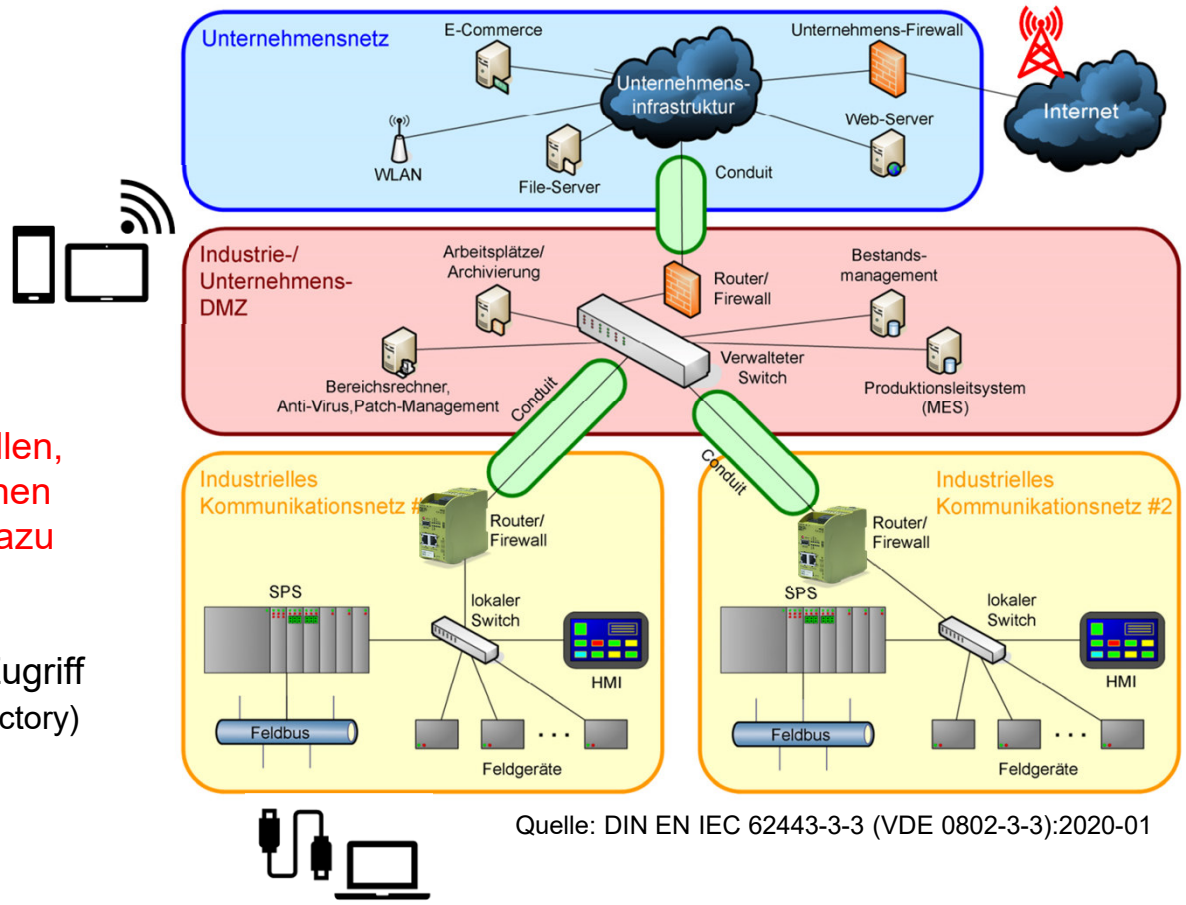
Verwaltungsnetzwerk (Office-IT) und
Produktionsnetzwerk (Industrial OT) segmentieren
… bis hin zu einzelnen Fertigungszellen

Zonen identifizieren, in denen Geräte ähnliche (Security-) Anforderungen haben

Firewalls oder sichere Router setzen und sicherstellen, dass über die Leitungen (Conduits) zwischen den Zonen nur die Geräte senden und empfangen können, die dazu berechtigt sind

DMZ mit VPN-Einwahlfunktionalität für den Remote-Zugriff
(z.B. Remote Access, File Exchange, Active Directory)
„**Zero-Trust-Concept**“

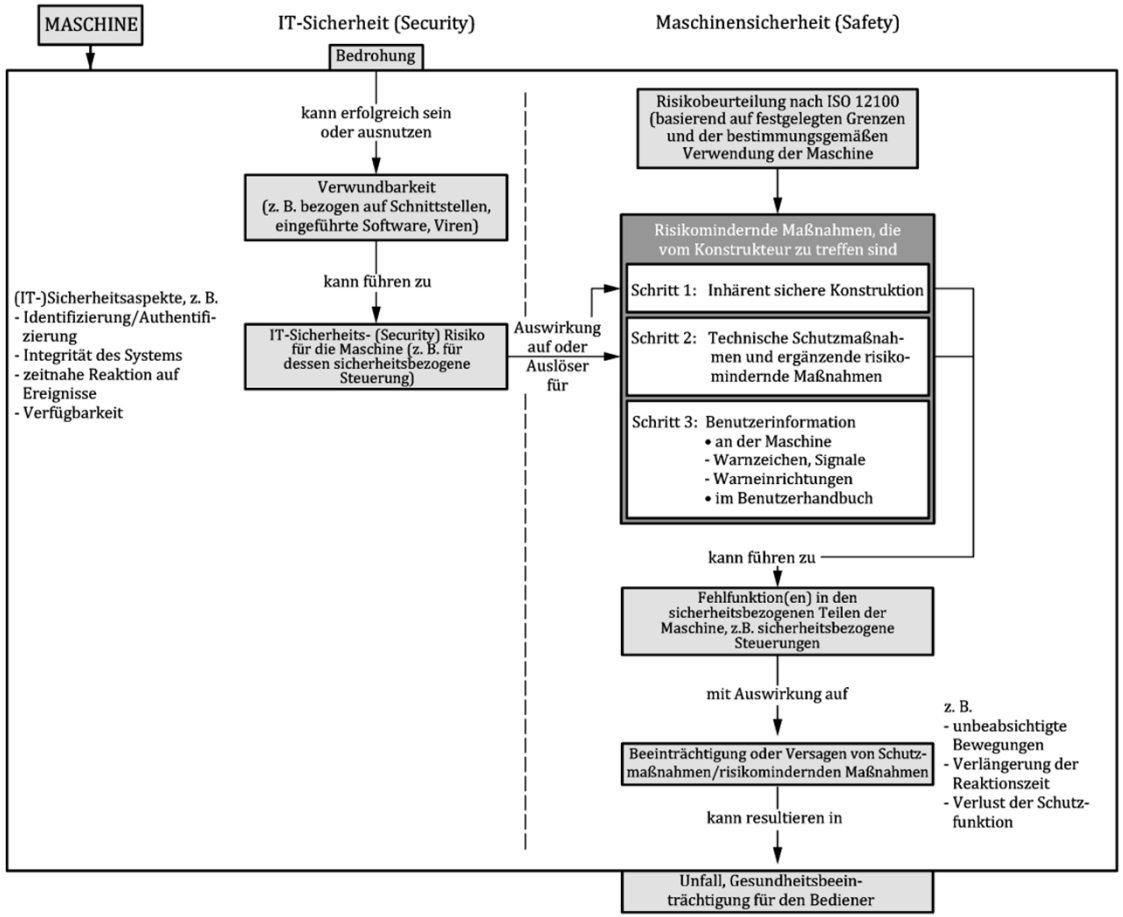
DMZ: De-MilitarizedZone



Quelle: DIN EN IEC 62443-3-3 (VDE 0802-3-3):2020-01

EN ISO 22100-4

Zusammenhang mit ISO 12100 - Teil 4: Leitlinien für Maschinenhersteller zur Berücksichtigung der damit verbundenen IT-Sicherheits- (Cybersicherheits-) Aspekte



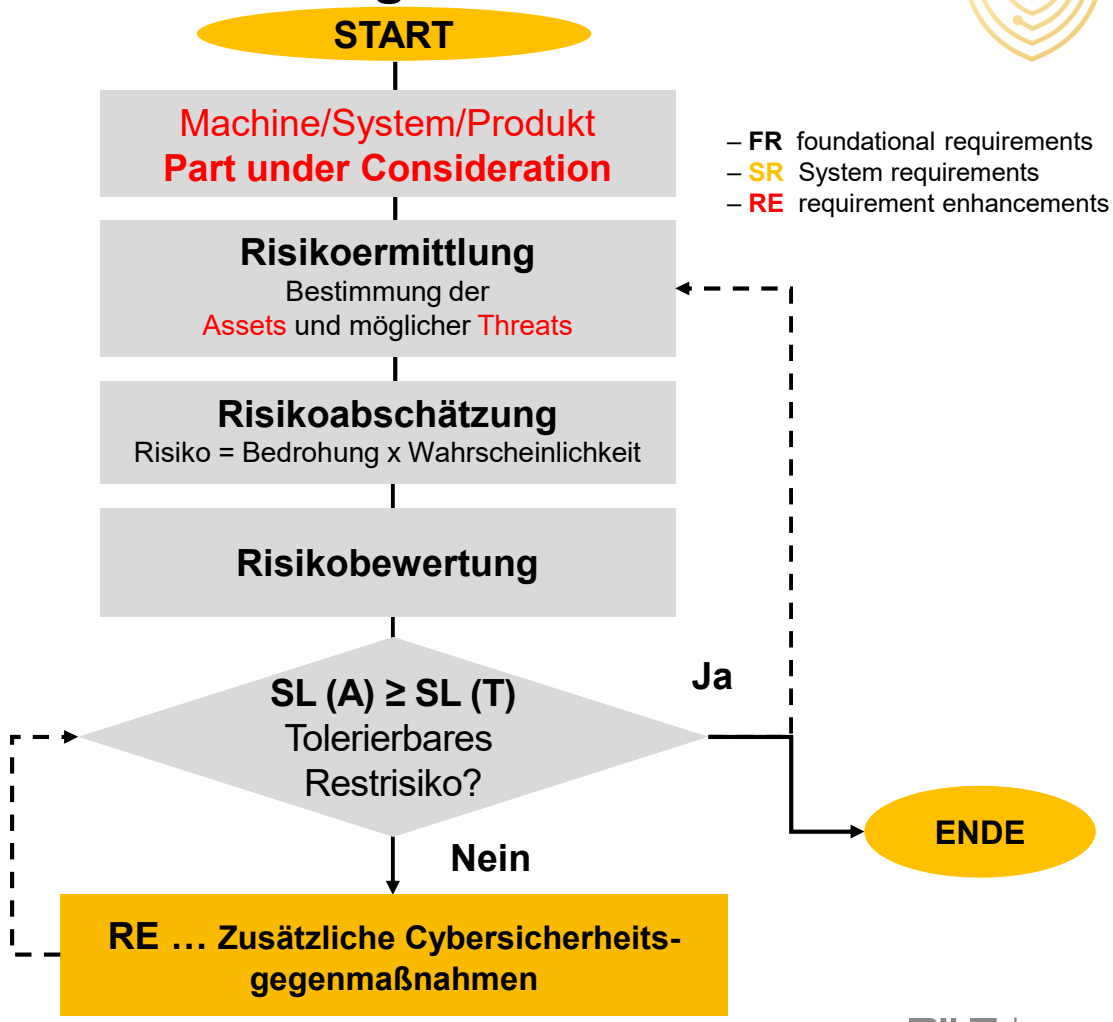
IEC 62443-3-3 - Cybersicherheitsrisikobeurteilung

M-VO Anhang III - 1.1.9. Schutz gegen Korrumpierung

- physischer Zugang
- Organisation
- **FR 1** - Identifizierung und Authentifizierung
- **FR 2** - Nutzungskontrolle
- **FR 3** - Systemintegrität
- **FR 4** - Vertraulichkeit der Daten
- **FR 5 - eingeschränkter Datenfluss**
- **FR 6** - rechtzeitige Reaktion auf Ereignisse
- **FR 7** - Ressourcenverfügbarkeit

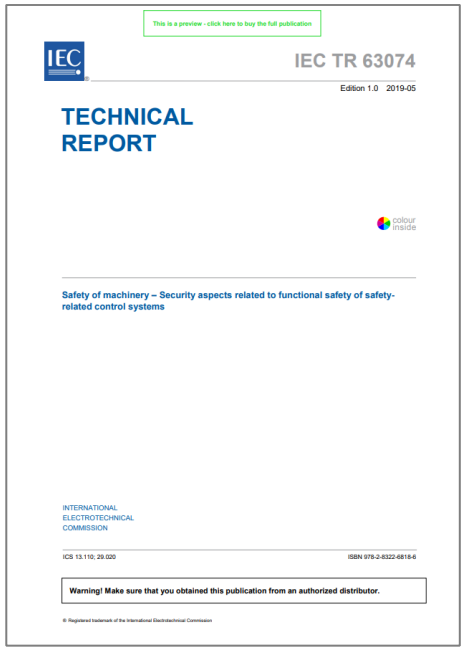
FR **SL** **SR & RE**

Foundational Requirement (FR)	Security Level	Security Requirements
FR 1 – Identification and authentication control (IAC)	SL2	SR1.1
FR 2 – Use control (UC)	SL2	SR2.1, SR2.8, SR2.9
FR 3 – System integrity (SI)	SL2	SR3.1, SR3.4, SR3.5, SR3.6
FR 4 – Data confidentiality	None	None
FR 5 – Restricted data flow (RDF)	SL1	SR5.1
FR 6 – Timely response to events (TRE)	SL1	SR6.1
FR 7 – Resource availability (RA)	SL2	SR7.1, SR7.2



IEC 62061 → IEC TR 63074

Aspekte zur **Cybersicherheit** in Verbindung mit der
funktionalen Sicherheit von sicherheitsrelevanten Steuerungssystemen



IEC 62061 - 6.8 Securityaspekte

Security umfasst **vorsätzliche Angriffe** auf die Hardware, Anwendungsprogramme und zugehörige Software, **sowie unbeabsichtigte Ereignisse**, die auf menschliches Versagen zurückzuführen sind.

.. Zustand der Systemressourcen, **frei von** unbefugtem Zugriff und unbefugter oder versehentlicher Änderung, Zerstörung oder Verlust

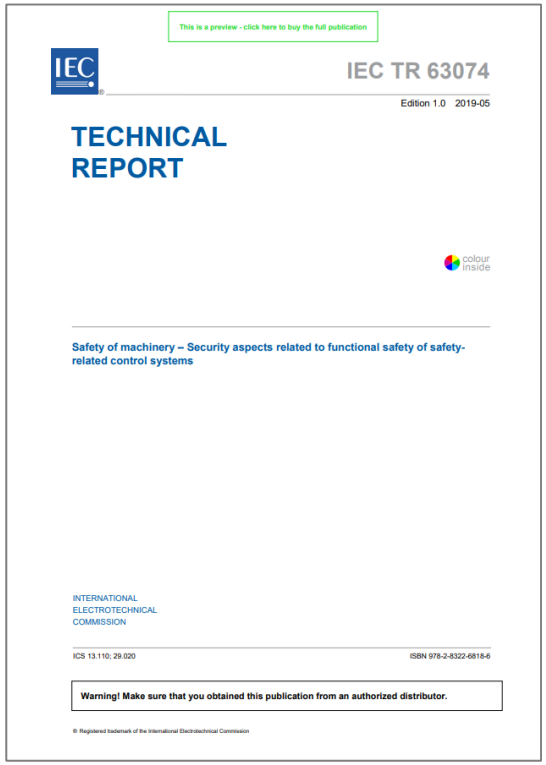
.. **unbefugte Personen und Systeme dürfen** weder die Software und ihre Daten verändern, noch Zugriff auf die Systemfunktionen erlangen können, und
→ **autorisierten Personen und Systemen** ist dies jedoch nicht zu verweigert

IEC TR 63074

gibt eine **Anleitung zur Anwendung von IEC 62443** (alle Teile) in Bezug auf Sicherheitsbedrohungen durch **sicherheitsbezogene Steuerungssysteme (SCS)**

IEC TR 63074

Aspekte zur Cybersicherheit in Verbindung mit der
funktionalen Sicherheit von sicherheitsrelevanten Steuerungssystemen



Cybersicherheitsziele:

- Integrität gegen Manipulation
- Vertraulichkeit durch anerkannte Verfahren
- Verfügbarkeit der Maschine / Sicherheitsfunktion

→ **Cybersicherheitsrisikobeurteilung**
→ **Cybersicherheitsrisikoreaktionsstrategie**

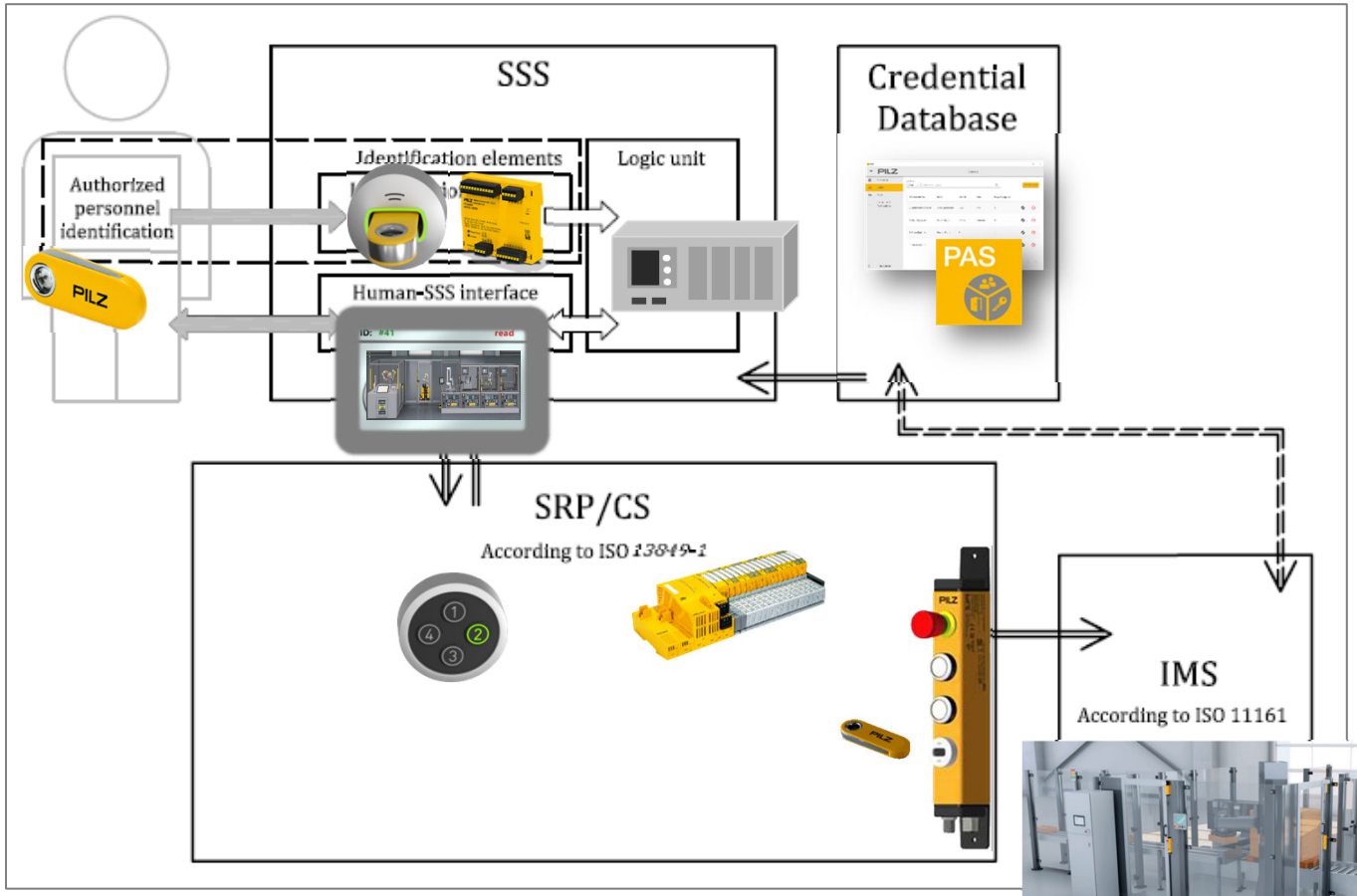
Gegenmaßnahmen der Cybersicherheit

→ **Netzwerkarchitektur;**
a) Netzwerkentwurf (z.B. das Zonen- und Conduit-Modell);
b) Firewall-Konfiguration;
c) Benutzerautorisierung und -authentifizierung;
d) Verbindungen zwischen verschiedenen Prozesssteuerungsnetzwerken;
e) Kabellose Kommunikation;
f) Zugang zu externen Netzwerken (d. h. das Internet).

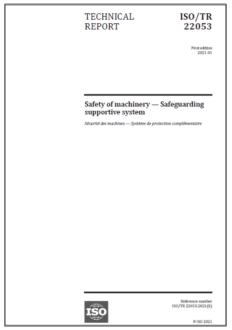
→ **tragbare, schnurlose Geräte und Messfühler**
→ **Fernzugang;**
→ **Schnittstellen zu anderen Systemen / Mensch-Maschine-Schnittstellen**

ISO TR 22053 Safety of machinery — Safeguarding supportive system

Identifikation und Authentifikation – Aufzeichnung- & Nachweisverpflichtung



Identification & Access Management (IAM)



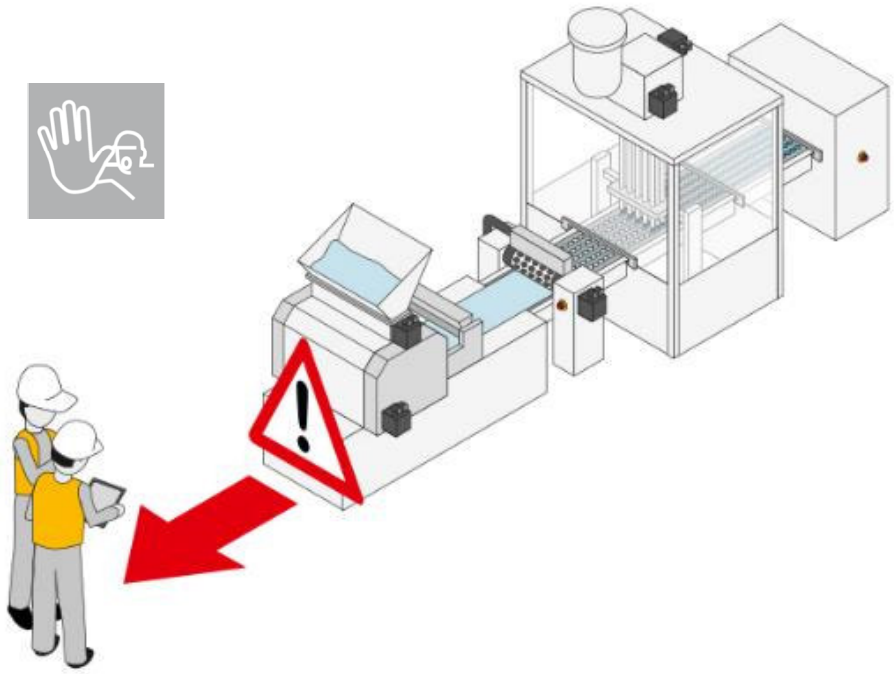
a) **Identifizieren**
b) **Berechtigen**
c) **Informieren**
d) **Freigeben** der **Betriebsart**
e) **Freigeben** der **Zonen**

IMS … Integriertes Fertigungssystem
… *SI - Zoneneinteilung*

Safety & Security-Maßnahmen für eine Automatisierungsanlage

Interaktion Mensch & Maschine

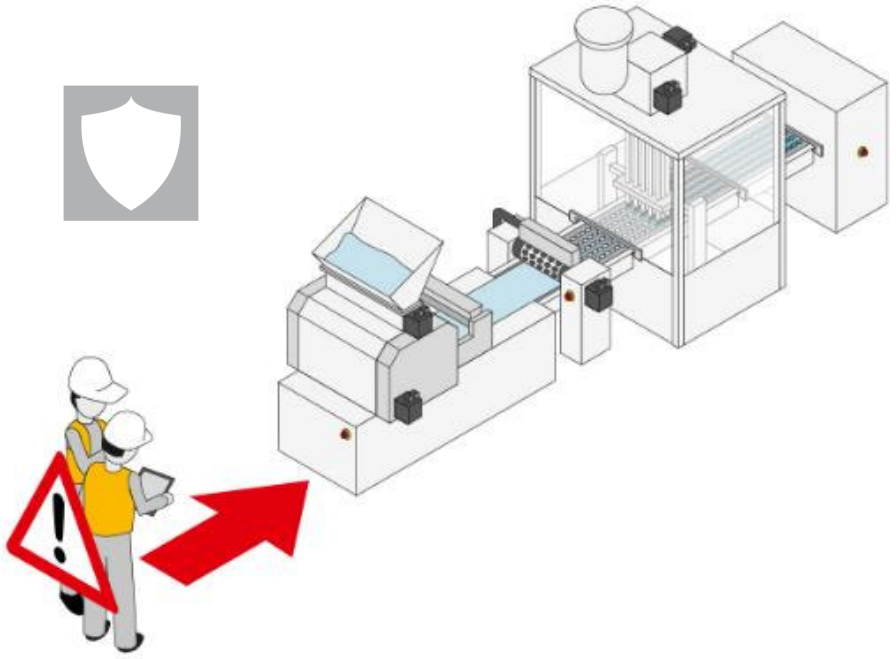
Funktionale Sicherheit



Schutz des **Menschen** vor Gefahren der Maschine

z.B. Schutz vor Gefährdung durch bewegliche Maschinenteile

Industrial Security



Schutz der **Maschine** vor dem Menschen.

z.B. Schutz vor unautorisierten Zugriffen und Fehlbedienungen

.. stay **safe & secure** !!

PILZ

THE SPIRIT OF SAFETY

Gerhard Stockhammer

Pilz Ges.m.b.H, Wagramer Strasse 19, 1220 Wien

+43 1 798 6263-0, pilz@pilz.at, www.pilz.com

www.pilz.com