

secunet



encrypt. protect. trust.

04.10.2018, Workshop "Industrial Security in der Automatisierungspraxis"

Safety und IT-Security

Agenda

1. **Safety und IT-Security im Zeitalter der Vernetzung und Synergie-Gewinnung**
2. **Unterschied zwischen Safety und Security**
3. **Herangehensweisen und Charakteristiken der Risikoanalysen**
4. **Fazit**

Information Technology - Operational Technology - Safety Technology

Inhaltliche
Abgrenzung

IT-Sicherheit ist durch zunehmende Vernetzung nicht nur bei IT ein wesentlicher zu betrachtender Faktor

IT

Informations- und
Datenverarbeitung auf Basis dafür
bereitgestellter technischer Services
und Funktionen

OT

Hardware und Software, die eine
Änderung durch die direkte
Überwachung und/oder Kontrolle von
physikalischen Geräten, Prozessen
und Ereignissen im Unternehmen
erkennen oder verursachen.

Safety

Teil der Sicherheit einer Anlage, der
von der korrekten Funktion des
sicherheitsbezogenen Systems und
anderer risikomindernder
Maßnahmen abhängt.

Vorfälle mit IT-Bezug im Umfeld Safety

Angriff auf Heizungen

Hacker lassen Finnen frieren

09.11.2016, 09:09 Uhr | mak, Spiegel Online



DDoS-Angriffe

Werk Baunatal

VW-Roboter tötet Arbeiter

Eigentlich sollte er nur den neuen Fertigungsroboter einrichten. Doch dann ging irgendetwas schief – ein junger Mitarbeiter im VW-Werk Baunatal wurde von einem Roboter gegen eine Wand gequetscht und starb. Der Staatsanwalt ermittelt.



Quelle: Stern

Angriff auf Irans Atomprogramm

Stuxnet-Virus könnte tausend Uran-Zentrifugen zerstört haben

Neue Erkenntnisse über den hinterhältigen Stuxnet-Wurm: Möglicherweise hat die Schad-Software in der iranischen Anreicherungsanlage Natans größere Schäden angerichtet, als das Regime in Teheran eingestehen will. Bis zu tausend Uran-Zentrifugen hat der Virus womöglich auf dem Gewissen.

Von Christian Stöcker



Quelle: Spiegel

Robotik außer Kontrolle

VDMA-Studie

Security-Vorfälle bedrohen zunehmend Produktion

© 12. Dezember 2017



Quelle: Industrieanzeiger

Die Bahn plant digitales Netz quer durch Deutschland



Die Bahn treibt ein Milliardenprojekt voran: Um Züge enger takteten zu können, sollen sie künftig überall automatisch fahren – so wie schon jetzt auf der ICE-Strecke München-Berlin. Wenn sich denn das Geld auftreiben lässt.

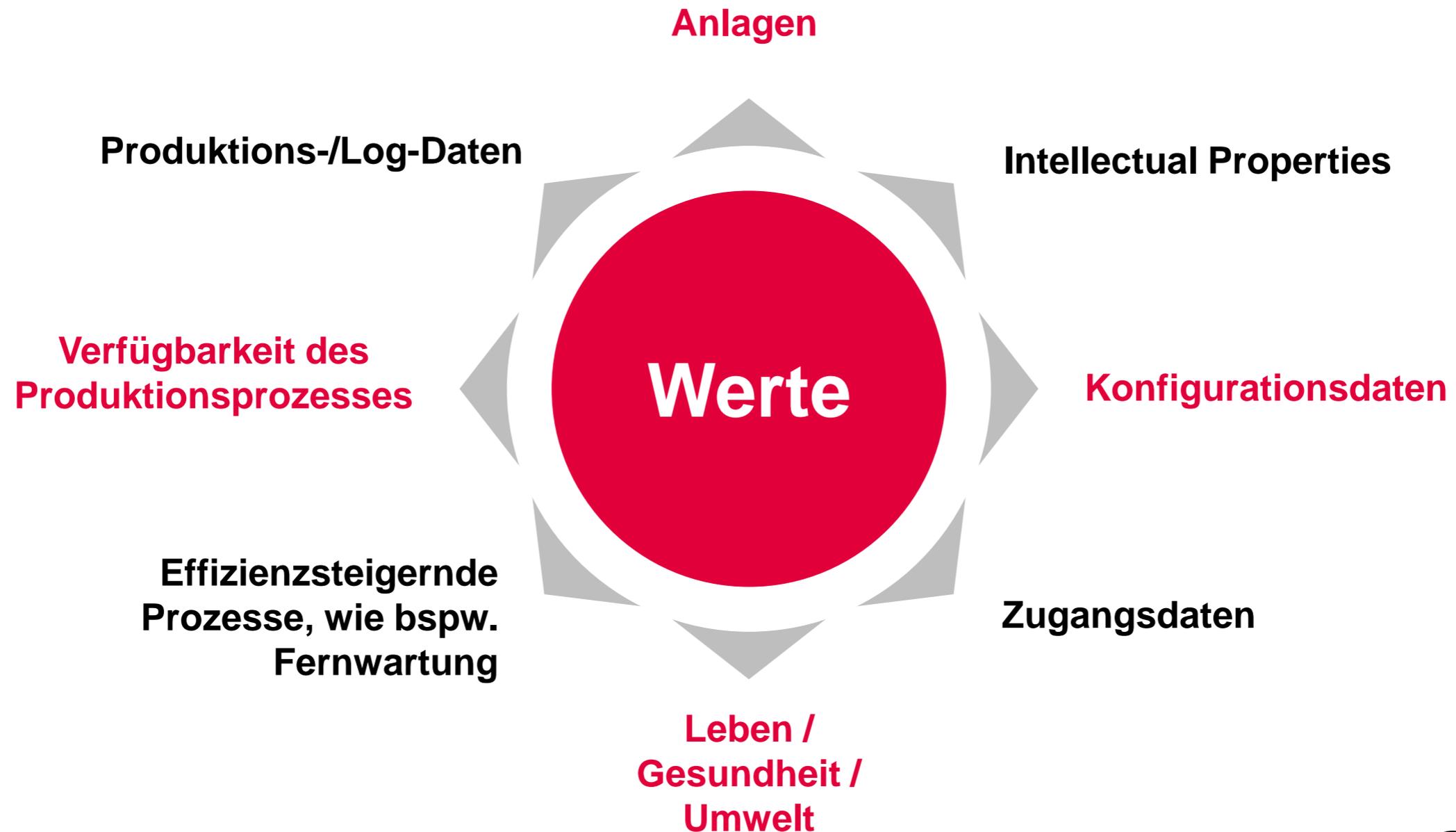
Von Markus Balseer, Berlin

Bis zum 10. Dezember konnte sicher kaum ein deutscher Bahnkunde mit dem Kürzel ETCS etwas anfangen. Dann aber begann eine steile wie unrühmliche Karriere: Die digitale Zugsteuerung European Train Control System war für die peinliche Pannenserie zum Start der neuen Schnelltrasse München-Berlin verantwortlich. Fehler im System bremsen nicht nur den Premierenzug aus, sondern auch noch Dutzende Folgezüge. Wo auf dem Milliardenprojekt liegen blieb, dem raunt das Zuggespersonal meist nur vier Buchstaben zu: ETCS.

Quelle: SZ

Störung der Verfügbarkeit

Welche Assets (Werte) sind zu schützen ...



Klassische Trennung von Safety und IT-Security ist nicht mehr gegeben

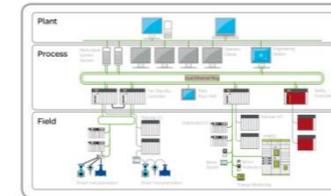
- Informationstechnik wird auch im Safety-Bereich eingesetzt.



- Nutzen gleicher Hardware für funktions- und sicherheitsgerichtete Anwendungen.



- Durch zunehmende Vernetzung werden Infrastrukturen sicherer / unsicherer.



- Ein Inseldenkens hinsichtlich Sicherheit übersieht Risiken.



- Ein übergreifendes Sicherheitsmanagement gewinnt an Bedeutung.



- Stärkung der Widerstandskraft (Resilienz) statt Abschottung (periphere Sicherheit) als einzige Maßnahme.



- Kontinuierlicher Prozess erforderlich, da sich die Bedrohungen ändern können bzw. neue Angriffsszenarien möglich sind.

Genereller Unterschied zwischen Safety und IT-Security

Safety

- Das System soll die Umgebung nicht schädigen -

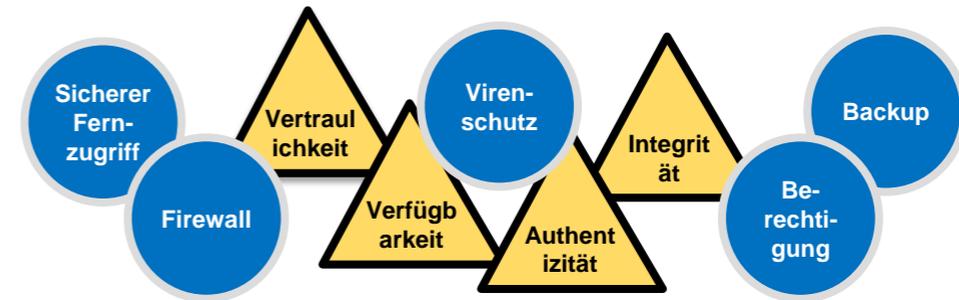
- Fokus: Unversehrtheit von Umwelt und Mensch
- Hauptziel: Schutz der Umgebung vor dem Fehlverhalten des Systems



IT-Security

- Die Umgebung soll das System nicht schädigen -

- Fokus: technische Verarbeitung, Speicherung und Übertragung von Informationen
- Hauptziel: Schutz der IKT-Systeme und der gespeicherten Daten vor unerwünschten Einwirkungen aus deren Umgebung



Unterschiedliche Standards

Safety (Beispiele)

- DIN EN ISO 13849 mit Gestaltungsleitsätzen zu sicherheitsbezogenen Teilen von Steuerungen
- IEC 61508 (VDE 0803) - funktionale Sicherheit von elektrischen, elektronischen sowie programmierbaren elektronischen Systemen anwendungsunabhängig als Sicherheitsgrundnorm
 - » Beispiele für anwendungsspezifische Ausprägungen
 - » ISO 26262 für Fahrzeugelektronik
 - » IEC 62061 für Maschinensteuerungen
- IEC EN 62061 für elektrisch programmierbare, sicherheitsrelevante Funktionen (SIL)
- IEC EN 61800: Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl

Es fehlen beispielsweise:
Kryptographische Lösungen für
Authentisierung und
Verschlüsselung

IT-Security (Beispiele)

- ISO 27XXX Normen
- Neuer BSI IT-Grundschutz (inkl. ICS)
- COBIT (Framework zur IT-Governance)
- ISO /IEC 15408 (Common Criteria) zur Evaluierung und Zertifizierung von IT-Sicherheitsprodukten
- (ITIL - Information Technology Infrastructure Library)

Es fehlen beispielsweise:
Reduktion von Abhängigkeiten,
um kaskadierende Fehlereffekte
zu unterbinden
Vollständig definierte
Schnittstellen

ISO 31000 (Risikomanagement)

IEC 62443: Spezifikation der IT-Sicherheit in industriellen Automatisierungssystemen – betrachten auch IT-Security im Safety-Umfeld

Security-Konzepte für diesen klassischen Safety-Kontext sind u. a. Sicherheitszonen und -kanäle zur Strukturierung von mehrfachen Verteidigungslinien und zur sicheren Kommunikation, Sicherheits-Level, die Bewertung der Reife von IT-Sicherheitsprogrammen sowie IT-Sicherheitsleitlinien.

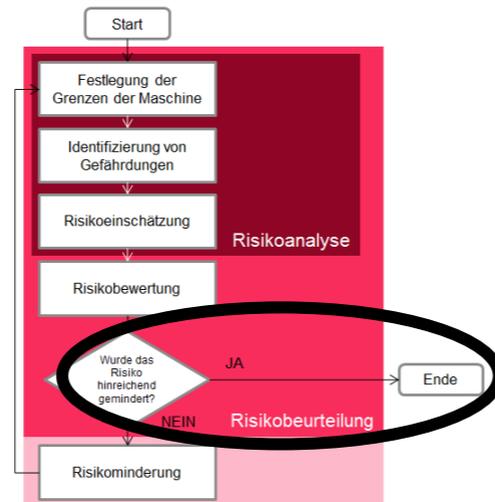
Risikomanagement – Wesentliche Unterschiede

Safety

■ Einmaliger Prozess (vor dem Betrieb)

- Risikobewertung läuft so lange, bis das Risiko ausreichend gemindert ist und Restrisiken beschrieben wurden

Anpassungen der Bewertungen mittlerweile teilweise auch während der Lebensdauer (z.B. Arbeitsschutz)



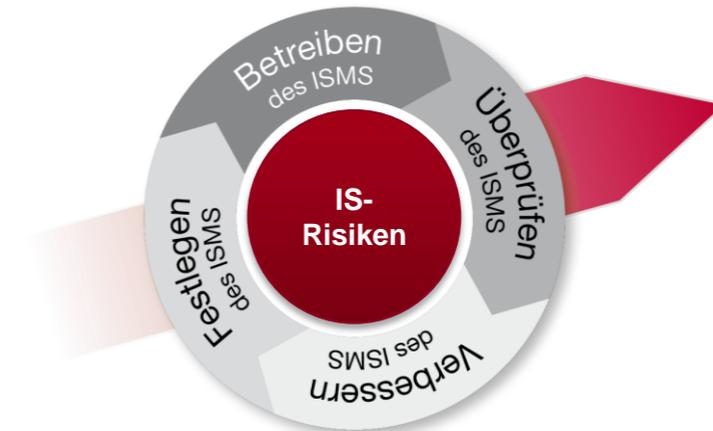
■ Klare Vorgaben für die Bewertung von Risiken

- z.B. Ausfallraten, Schwere der Verletzung, Häufigkeit der Gefährdungsexposition

IT-Security

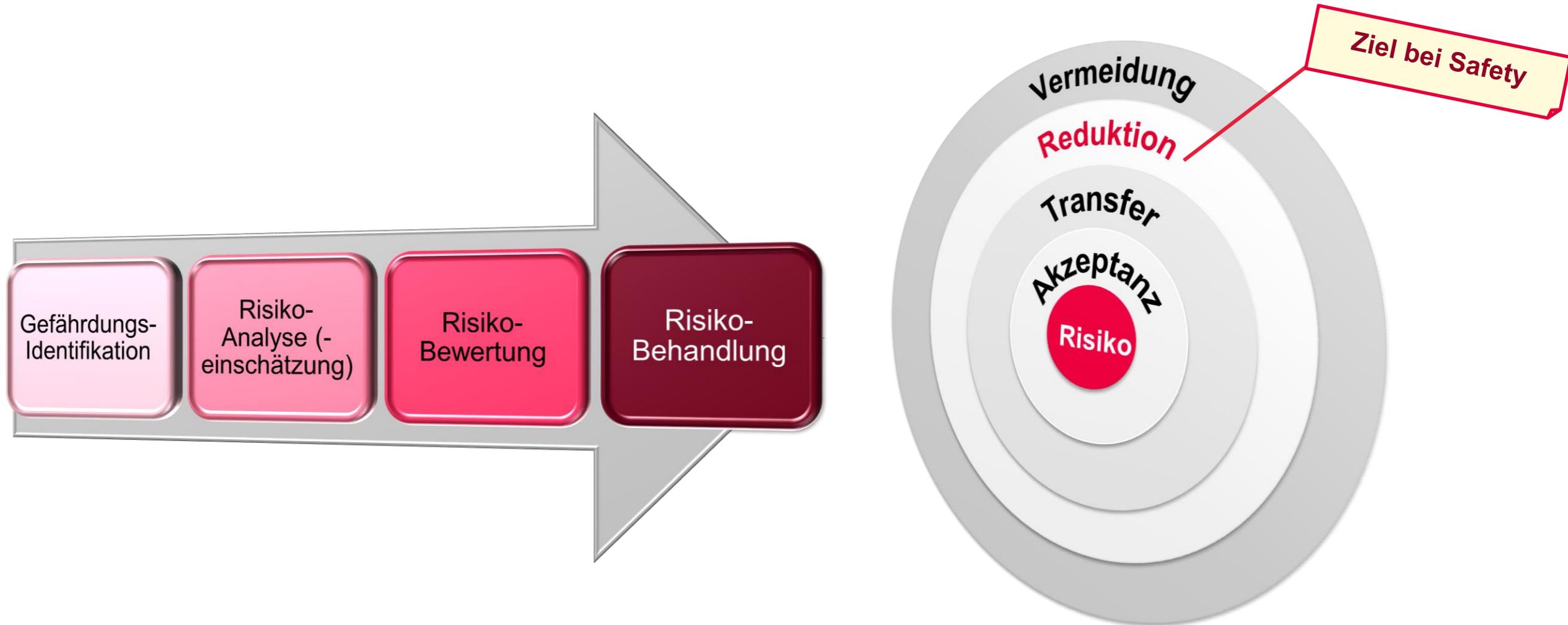
■ Kontinuierlicher Prozess (vor & während des Betriebs)

- Regelmäßige wiederholende Zyklen (angestoßen durch Vorfälle, Bekanntwerden von Schwachstellen, definierte zeitliche Zyklen – z.B. einmal jährlich)



■ Keine übergreifend einheitlichen Vorgaben zur Bewertung von Risiken

Identischer Prozess des Risikomanagements für Safety und IT-Security



Risikobehandlungs-Alternativen

■ Risikoreduktion

- >> durch Implementierung von (zusätzlichen) Sicherheitsmaßnahmen oder deren Verbesserung

■ Risikoakzeptanz

- >> Risikoübernahme ohne Umsetzung weiterer technischer und organisatorischer Maßnahmen

■ Risikotransfer

- >> überträgt das Risiko an Vertragspartner wie Dienstleister oder Versicherungen

■ Risikovermeidung

- >> indem die geschäftlichen, organisatorischen oder technischen Gegebenheiten so verändert werden, dass das Risiko in der Form nicht mehr besteht

■ Maßnahmen (entfallen bei Risikoakzeptanz)

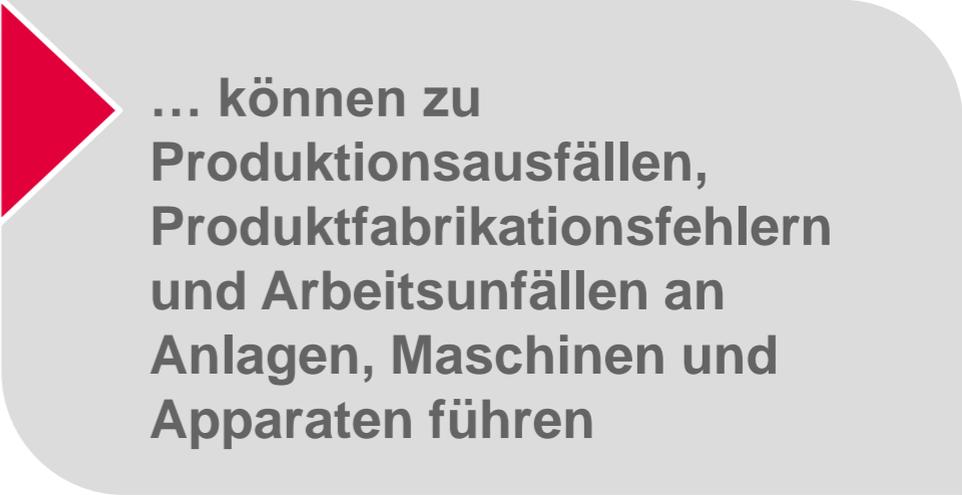
- >> Festlegen - Umsetzen - Prüfen



Top 10 IT-Bedrohungen für Industrial Control Systems

Ermittelt durch Bundesministerium für Sicherheit in der Informationstechnik (BSI) in Zusammenarbeit mit der Industrie:

1. Infektion mit Schadsoftware über Internet und Intranet
2. Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware
3. Social Engineering
4. Menschliches Fehlverhalten und Sabotage
5. Einbruch über Fernwartungszugänge
6. Internet-verbundene Steuerungskomponenten
7. Technisches Fehlverhalten und höhere Gewalt
8. Kompromittierung von Smartphones im Produktionsumfeld
9. Kompromittierung von Extranet und Cloud-Komponenten
10. (D)DoS Angriffe



... können zu
**Produktionsausfällen,
Produktfabrikationsfehlern
und Arbeitsunfällen an
Anlagen, Maschinen und
Apparaten führen**

Wesentliche IT-Schutzziele

(1.) Verfügbarkeit



Die Verfügbarkeit von Diensten, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese den Benutzern stets uneingeschränkt zur Verfügung stehen.

(2.) Integrität



Die Integrität bezeichnet die Sicherstellung der Korrektheit von Daten und Informationen sowie die Gewährleistung der korrekten Funktionsweise von Systemen.

(3.) Vertraulichkeit



Die Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.

IT-Gefährdungen auch innerhalb der Safety-Risikoanalyse berücksichtigen!

Beispiel zu einer Gefährdung

Risikoidentifizierung		Risikoanalyse (Brutto-Eintrittswahrscheinlichkeit)								
Lfd. Nr.	Bezugsobjekt (Informationswert)	Risiko	Eintrittswahrscheinlichkeit	Schutzbedarf (Vertraulichkeit)	Risikokennzahl (Vertraulichkeit)	Schutzbedarf (Integrität)	Risikokennzahl (Integrität)	Schutzbedarf (Verfügbarkeit)	Risikokennzahl (Verfügbarkeit)	Risikokennzahl
13	Remote Access	Externe Angreifer (Hacker, Cracker, Terroristen, Nation, State)	3	4	12	4	12	4	12	12

1. Risikoidentifizierung - Brutto

Risikoanalyse			Risikobewertung (Netto-Eintrittswahrscheinlichkeit)		Netto-Eintrittswahrscheinlichkeit							
Lfd. Nr.	Bezugsobjekt (Informationswert)	Eintrittswahrscheinlichkeit (Brutto)	Risiko	Umgesetzte Maßnahmen	Eintrittswahrscheinlichkeit	Schadensausmaß (Vertraulichkeit)	Risikokennzahl (Vertraulichkeit)	Schadensausmaß (Integrität)	Risikokennzahl (Integrität)	Schadensausmaß (Verfügbarkeit)	Risikokennzahl (Verfügbarkeit)	Erwartetes Restrisiko (Risikokennzahl gesamt)
13	Remote Access	3	Externe Angreifer (Hacker, Cracker, Terroristen, Nation, State)	Berechtigungskonzept, Zutrittsregelungen, DMZ- und Firewallschutz, IDS System, DLP, Sichere Mail-Gateways, 2 Faktor-Authentifizierung	2	3	6	3	6	3	6	6

2. Risikoanalyse - Netto

Bezugsobjekt (Informationswert)	Lfd. Nr.	Risiko (Kurzbeschreibung)	Risiko (Detailbeschreibung)	Maßnahme (Kurztitel)	Vorschlag Maßnahme (Beschreibung)	Empfehlung zur Risikobehandlung	Kosten-schätzung	Aufwands-schätzung	Umsetzungs-verantwortlicher	Umsetzungs-frist	Status	Eintrittswahrscheinlichkeit	Schadensausmaß (Vertraulichkeit)	Schadensausmaß (Integrität)	Schadensausmaß (Verfügbarkeit)
Remote Access	13	Externe Angreifer (Hacker, Cracker, Terroristen, Nation, State)	politisch motivierte Angriffe auf die Informationssysteme und Steuerungsanlagen. Diese können rein auf Informationsabfluss aber auch auf Datenmanipulation bis zur Abschaltung / Zerstörung von Systemen reichen.	Umsetzung der OT-Sicherheitsarchitektur (Projekt)	Das Projekt hat zum Ziel, externe Angriffe über einen gesamtheitlichen Ansatz zu behandeln (u.a. sicherer Remotezugang, physikalische und logische Netztrennung (OT/IT-Netze), Schutz vor Schadsoftware, Härtung von IT-Systemkomponenten, Ergänzung des Monitorings hinsichtlich OT-Netze und OT-Systeme,...).	Reduktion	hoch	hoch	Hr. Meyer	Q2 2019	In Arbeit	1	3	3	3

3. Risikobehandlung

Beispiele für technische IT-Schutzmaßnahmen ...



Fazit: Safety und IT-Security müssen gemeinsam betrachtet werden

■ Warum ?

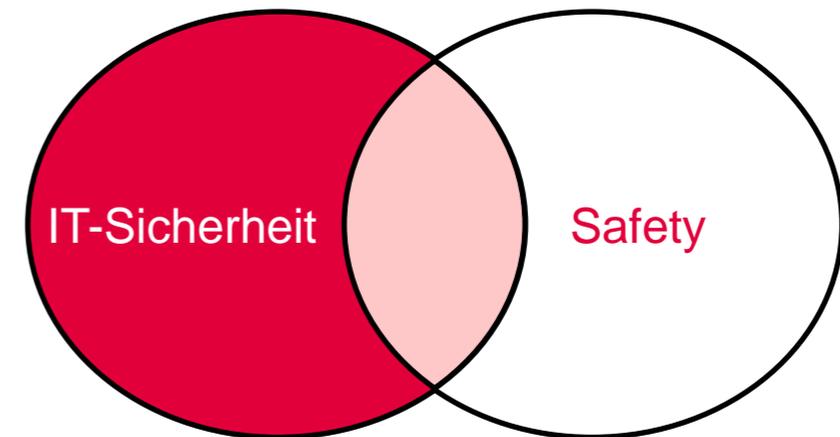
- IT auch im Safety-Bereich
- stärkere Vernetzung aller Systeme – einschließlich der Safety-Systeme
- Nutzung von Hardware-Synergien für Funktion und sicherheitsgerichtete Funktion

- IT-Security-Gefährdungen können Einfluss auf die Safety haben

■ Vorgehensweise

- Einbindung IT-Sicherheit in die Safety-Risikoanalyse
- Berücksichtigung des ständigen Verbesserungsprozesses (Anpassungsbedarf)

IT-Sicherheit und Safety: Entwicklung einer gemeinsamen Sicht



The logo for secunet, featuring the word "secunet" in a bold, sans-serif font. The letters "secunet" are black, and the letters "net" are red. The background of the slide is white with a large, curved red shape on the left side that tapers towards the top right.

Steffen Heyde

Principal

secunet Security Networks AG

Alt-Moabit 96

10559 Berlin

Telefon +49 201 5454-2025

steffen.heyde@secunet.com