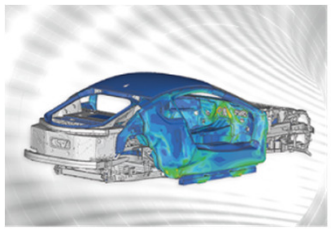

AUTOMOTIVE


INFOKOM


MOBILITÄT, ENERGIE & UMWELT


LUFTFAHRT


RAUMFAHRT


VERTEIDIGUNG & SICHERHEIT

IEC 62443

Die ganzheitliche Betrachtung von Security in der industriellen Fertigung

Industrial Security Forum, Hannovermesse, 03.04.2019

IABG

Inhalt

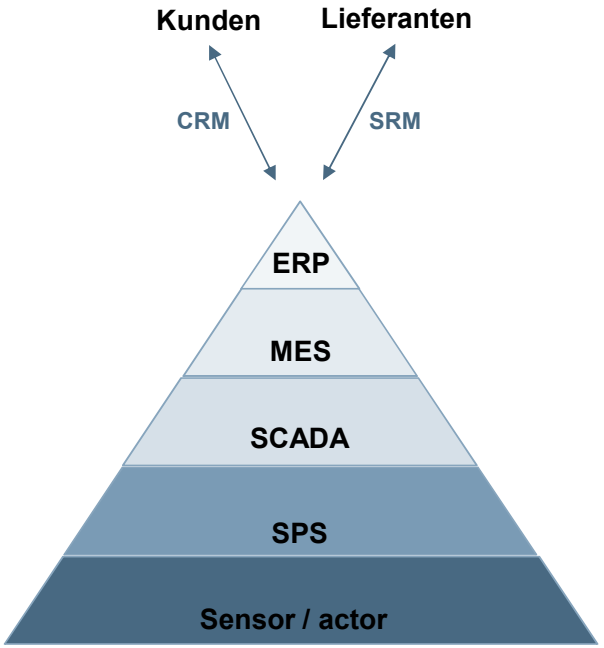
- Notwendigkeit von Industrial Security
- Umsetzung von Industrial Security
- Zusammenfassung

NOTWENDIGKEIT VON INDUSTRIAL SECURITY

Digitalisierung und Vernetzung als Voraussetzung für Industrie 4.0 Services

- **Vernetzung erfolgt**
  - Innerhalb der Operational Technology (OT) Umgebung
  - Zwischen IT und OT Umgebungen
  - Zwischen Geschäftspartnern (OEM, Lieferanten, Vertriebskanäle, Kunden, …)

- **Eine verstärkte Vernetzung schafft neue Security-Herausforderungen, z.B.**
  - Bislang isolierte Bereiche werden vernetzt
  - Erhöhung der Angriffsmöglichkeiten
  - Unterschiedliche Stufen und Ansätze für Security müssen integriert werden



Die Lage der IT-Sicherheit in Deutschland

- **Schadsoftware**
  - Täglich mehr als 390.000 neue Varianten von Schadprogrammen
  - Nach wie vor eine der größten Bedrohungen
- **Ransomware**
  - Nutzerdaten werden verschlüsselt und nur gegen Lösegeld entschlüsselt (z. B. Locky, GandCrab, Petya/NotPetya, WannaCry, …)
  - Seit 2016 starker Anstieg beobachtbar
- **Advanced Persistant Threats (APT)**
  - Gezielter, strategischer und längerfristiger Cyberangriff
  - Werden häufig über (Spear)Phishing Angriffe initiiert, dann weitere Ausbreitung (Lateral Movement)
- **Botnetze**
  - Infizierung zahlreicher Fremdsysteme mit Schadsoftware zum Missbrauch für Angriff, Spam, …
  - Immer mehr IoT werden für Botnetze missbraucht (z. B. Mirai)

Quelle: Bundesamt für Sicherheit in der Informationstechnik

Top 10 Bedrohungen für industrielle Steueranlagen (ICS) 2018

Nr.	Bedrohung
1	Unberechtigte Nutzung von Fernwartungszugängen
2	Online-Angriffe über Büro- / Unternehmensnetzwerke
3	Angriffe auf Standardkomponenten innerhalb des ICS-Netzwerkes
4	(D)Dos Angriffe
5	Menschliches Fehlverhalten und Sabotage
6	Über Wechseldatenträger und externe Hardware eingeschleuste Malware
7	Lesen und Schreiben von Nachrichten/Kommandos im ICS-Netzwerk
8	Unberechtigter Zugriff auf Ressourcen
9	Angriffe auf Netzwerkkomponenten
10	Technisches Fehlverhalten und höhere Gewalt

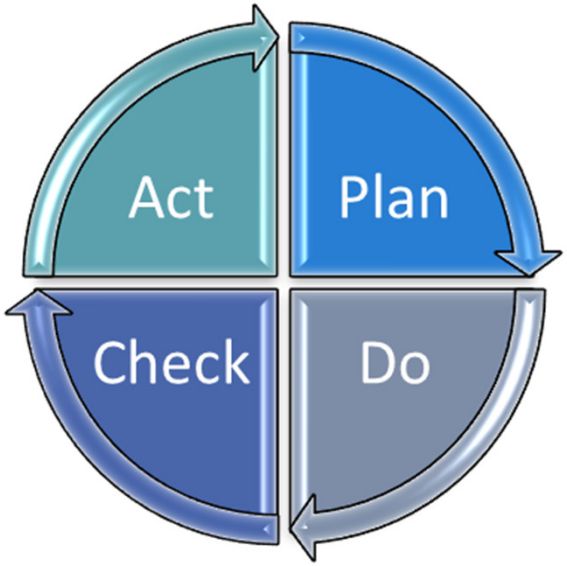
UMSETZUNG VON INDUSTRIAL SECURITY

Informationssicherheitsmanagement nach ISO 27001

Strukturiertes Vorgehen zur Einführung eines Informationssicherheitsmanagements (in Anlehnung an ISO 27001)

Verantwortung für Informationssicherheitsmanagement auf C-Level

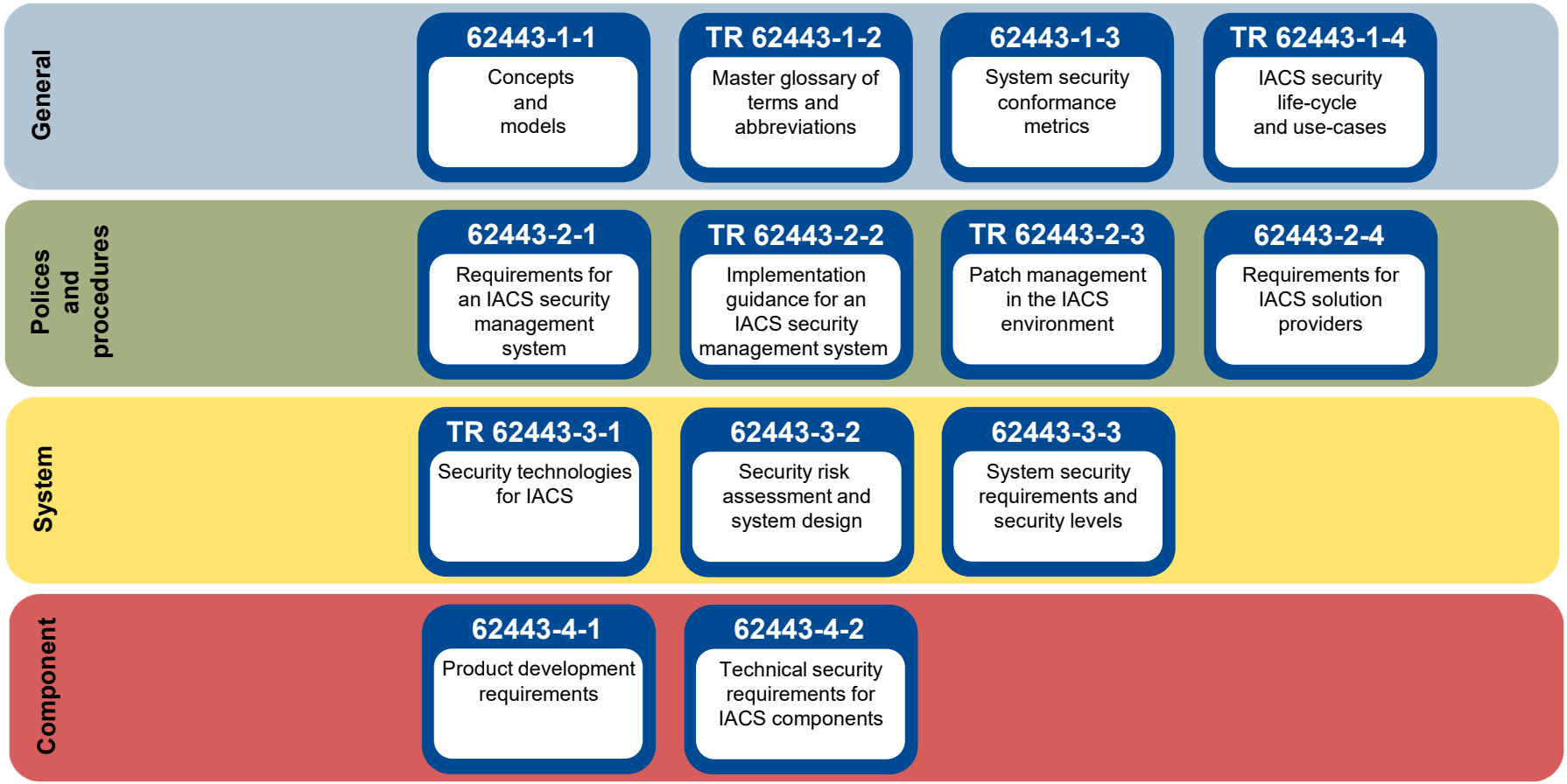
- Spezifikation von Organisation, Rollen und Prozessen
- Identifikation der Werte und Bestimmung des Schutzbedarfs
  - z.B. Verfügbarkeit, Integrität, Vertraulichkeit
- Umsetzung von Securitymaßnahmen
  - Bestimmen/Bewerten/Managen von Risiken
    - Einschließlich Bedrohungs- und Schwachstellenanalyse
  - Auswahl geeigneter Securitymaßnahmen
  - Integration der Securitymaßnahmen
  - Kontrolle der Wirksamkeit der Securitymaßnahmen (KPIs)
- Spezifikation von Vorgaben und Richtlinien
- Durchführung von Maßnahmen für Security Awareness und Training



Wesentliche Unterschiede zwischen IT und OT/ICS in Bezug auf Security

	IT	OT / ICS
Performance	Erledigt Aufgaben meist ohne garantiertes Zeitfenster	Erledigt Aufgaben in garantiertem Zeitfenster (Echtzeit)
Ressourcen	Umfassende Ressourcen wie CPU oder Speicher ermöglichen Installation von Security Software	Limitierte Ressourcen wie CPU oder Speicher erlauben nur bedingt Installation von Security Software
Verfügbarkeit	Wartungsausfall kann kurzfristig geplant werden und verursacht wenig Kosten Reboot der Systeme kein zu großes Problem	Wartungsausfall kann nur langfristig geplant werden und verursacht hohe Kosten Reboot im Produktionsumfeld problematisch
Safety	Spielt wenig Rolle	Spielt oft wichtige Rolle (Patchen mit Software verletzt Safety-Zertifizierungen)
Typische Lebensdauer Komponenten	< 4 Jahre	z.T. 20 – 25 Jahre

IEC 62443: Industrial communication networks – Network and system security



Relevanz der IEC 62443 für die jeweiligen Rollen

- Allgemein
  - IEC 62443-1-1: Konzepte und Modelle
- Betreiber
  - IEC 62443-2-1: Anforderungen an Security Managementsysteme
  - IEC 62443-2-3: Patchmanagement
  - IEC 62443-2-4: Anforderungen an Lösungsanbieter
- Integrator
  - IEC 62443-2-4: Anforderungen an Lösungsanbieter
  - IEC 62443-3-2: Risikobewertung und Secure System Design
  - IEC 62443-3-3: Security Anforderungen auf Systemebene
- Hersteller
  - IEC 62443-3-3: Security Anforderungen auf Systemebene
  - IEC 62443-4-1: Security Anforderungen an die Produktentwicklung
  - IEC 62443-4-2: technische Security Anforderungen an Komponenten

Allgemeine Konzepte gemäß IEC 62443-1-1

- Security objectives (AIC versus CIA)
- 7 Basisanforderungen (Foundational Requirements)
- Defense in depth
- Security context (Assets, Bedrohungen, Risiken, Gegenmaßnahmen)
- Bedrohungs- / Risikoanalyse
- Reifegrad der Security (Konzeptionierung, Analyse, Umsetzung, Betrieb, Ausphasen)
- Richtlinien
- Zonierung
- Security in der Lieferkette
- Security Level

IEC 62443 Security Level

- **Spezifikation des Security Level**
  - Einer „Zone“ zugeordnet
  - Target, Capability, Achieved
  - Qualitativ (später ggf. auch quantitativ)

1	**Casual or coincidental violation**
2	**Intentional violation using simple means with low resources, generic skills and low motivation**
3	**Intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation**
4	**Intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation**

Foundational (FR) and System (SR) Requirements gemäß 62443-3-3

7 Basisanforderungen (FR), welche jeweils weiter durch Systemanforderungen (SR) detailliert werden

- Identification and authentication control
- Use control
- System integrity
- Data confidentiality
- Restricted data flow
  - Network segmentation
  - Zone boundary protection
  - General purpose person-to-person communication restrictions
  - Application partitioning
- Timely response to events
- Resource availabilty

Systemanforderungen (SR) der Basisanforderung (FR) „Restricted data flow“

Security Maßnahme „Zonierung“ gemäß 62443-3-3 (1)

- **Empfehlung der IEC 62443-3-3**
  - Zusammenfassen von Geräten mit ähnlichen Sicherheitsanforderungen (Security Level) in Zonen
  - Beispiel
    - Control Zone (PLCs)
    - SCADA / Supervisory Zone (ICS, HMI)
    - Enterprise Network (ERP)
    - DMZ

- **Jede Zone hat verschiedene Eigenschaften, wie**
  - Inventar der physikalischen (z.B. Gerätschaften) und logischen (z.B. Software) Assets
  - Richtlinien für und Kontrolle des Zugangs
  - Sicherheitsrichtlinien
  - Bewertung der Bedrohungen und Schwachstellen
  - Zugelassene Technologien

Security Maßnahme „Zonierung“ gemäß 62443-3-3 (2)

- **Switches**
  - Port-basierte VLANs (untagged)
  - Tagged VLANs
- **Router**
  - Verschiedene IP Subnetze
- **Firewalls**
  - Paketfilter versus Deep Packet Inspection (z.B. Profinet / Modbus TCP / OPC / …)
  - Netzwerkfirewall versus Host Firewall (z.B. Integrated Firewall auf SCADA)
- **Datendioden**

Gap-Analyse als Startpunkt: Betreiber *(z.B. Anlehnung an IEC 62443-2-1)*

Beispielfragen

Gibt es Prozesse für die Installation von Patches und Upgrades inklusive der Überprüfung der Auswirkungen auf das Target Security Level?	ja	nein	teilweise	unbekannt
Gibt es Prozesse für Backup und Recovery inklusive der kontinuierlichen Überprüfung, dass Backups unbeschädigt sind?	ja	nein	teilweise	unbekannt
Gibt es ein Dokumenten- und Informationsmanagement-system inklusive Policies und Prozesse zur Klassifizierung und Aufbewahrung?	ja	nein	teilweise	unbekannt

Gap-Analyse als Startpunkt: Hersteller *(z.B. Anlehnung an IEC 62443-4-1)*

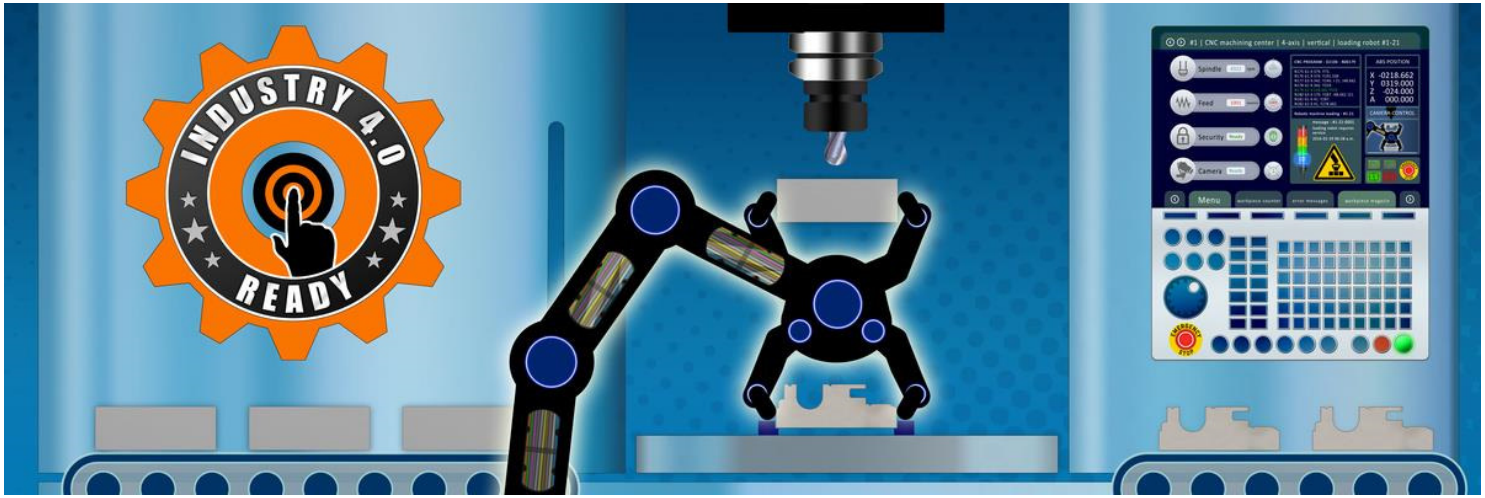
Beispielfragen

Gibt es einen Prozess, der die organisatorischen Rollen und das verantwortliche Personal für die erforderlichen Prozesse einer sicheren Produktentwicklung identifiziert?	ja / nein / teilweise / unbekannt
Gibt es einen Prozess der sicherstellt, dass für jedes Produkt ein Bedrohungsmodell vorhanden ist?	ja / nein / teilweise / unbekannt
Gibt es einen Prozess der sicherstellt, dass für jedes Produkt Sicherheitsanforderungen dokumentiert werden (inkl. Installation, Betrieb, Wartung, Außerbetriebnahme)?	ja / nein / teilweise / unbekannt

ZUSAMMENFASSUNG

Zusammenfassung

- Angriffe auf IoT nehmen auf breiter Basis zu – Notwendigkeit der Betrachtung von Industrial Security
- Ganzheitliche Umsetzung eines Informationssicherheitsmanagements – ISO 27001 und IEC 62443 als Leitfäden
  - Start mit Gap-Analyse
- Herkömmliche „Prevention“ Maßnahmen sind Pflicht, Detection & Response sind die Kür
- Immer mehr Sicherheitsprodukte sind angepasst auf die Charakteristik von Industrienetzen



Ihr Ansprechpartner

IABG mbH
Wolfgang Fritsche
Leiter Competence Center
Einsteinstrasse 20
85521 Ottobrunn
Telefon +49 89 6088-2897
fritsche@iabg.de
www.iabg.de

Besuchen Sie uns in Halle 6, Stand D08