CyberSecurity

Securing Critical Business

Asset Management in der ICS Security

9. Oktober 2019

Matthias Glawe, Security Engineer ICS

AIRBUS

Agenda

CyberSecurity

Agenda

AIRBUS

Assets

- Assets sind materielle und immaterielle Werte, die bedroht sein können und schützenswert sind.
  [VDI 2182][BSI ICS Security Kompendium]

- Die Bezeichnung Assets bezieht sich auf alle zu schützenden Unternehmenswerte, sie umfasst also sowohl physische Gegenstände als auch geistiges Eigentum wie geheime Rezepturen oder Kenntnisse über bestimmte Produktionsverfahren und deren Parameter.
  [Plattform Industrie 4.0 – IT-Security in der Industrie 4.0]

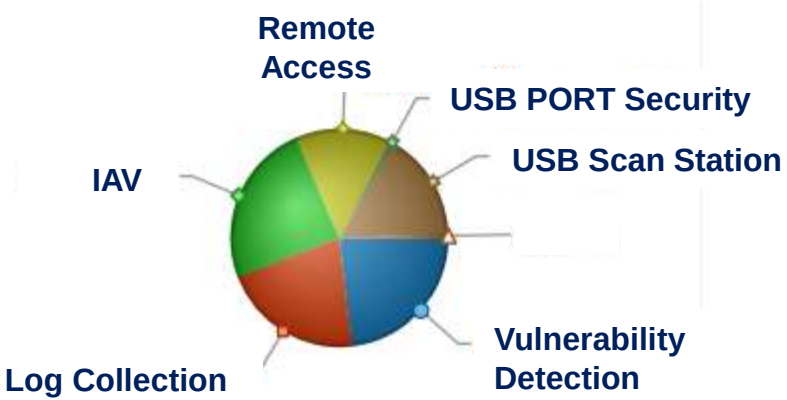
- In der Praxis zeigt sich, dass die wichtigste Grundlage eine vollständige Dokumentation darstellt. Das betrifft auch die Altsysteme.
  [Kuschmitz – IT-Sicherheit und Automation]

Asset Inventory

Basis für:

- Risikobewertung
- Planung von Security Maßnahmen
- Überwachung von Security Maßnahmen
- Bewertung von Incidents
- Incident Response

Endpoint – SECURITY DEPLOYMENTS

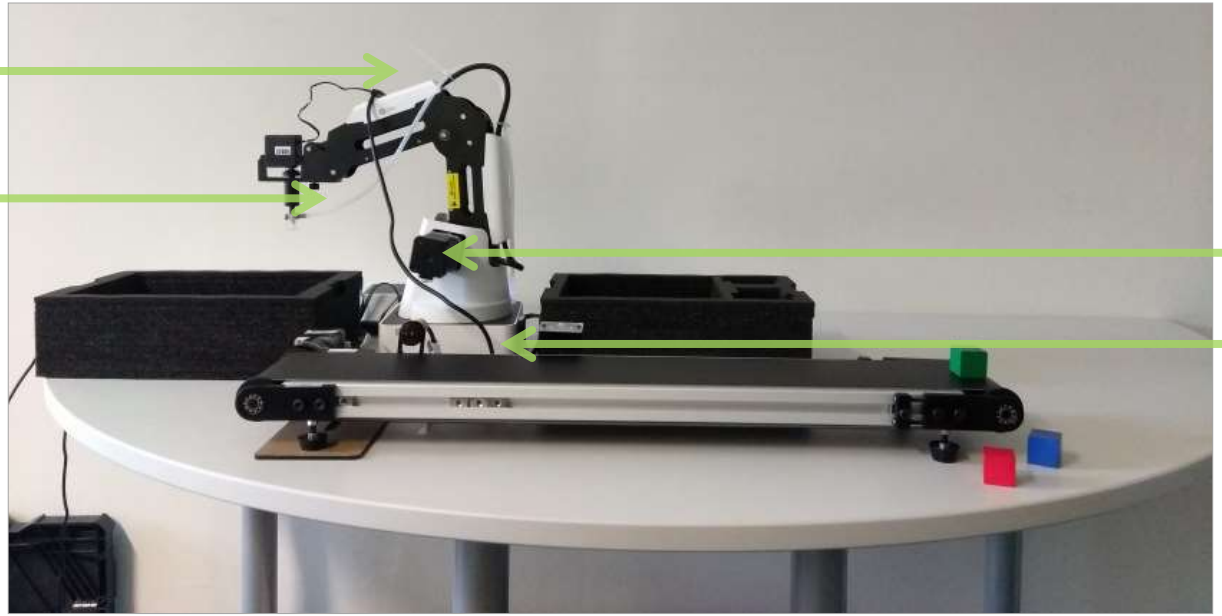


Agenda

Informationsbedarf

Komponenten

Software/Firmware Versionen



Vernetzung

Schnittstellen

Informationsbedarf

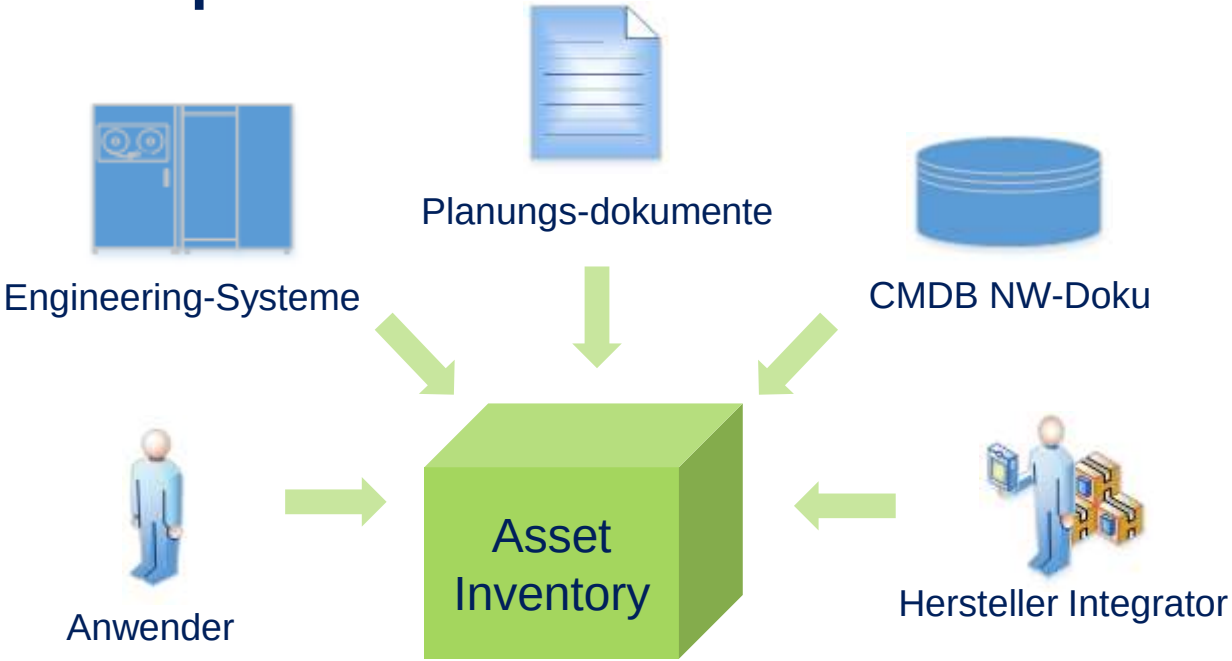
Kontext

Produktlinie/ Prozess

Kommunikationsbeziehungen

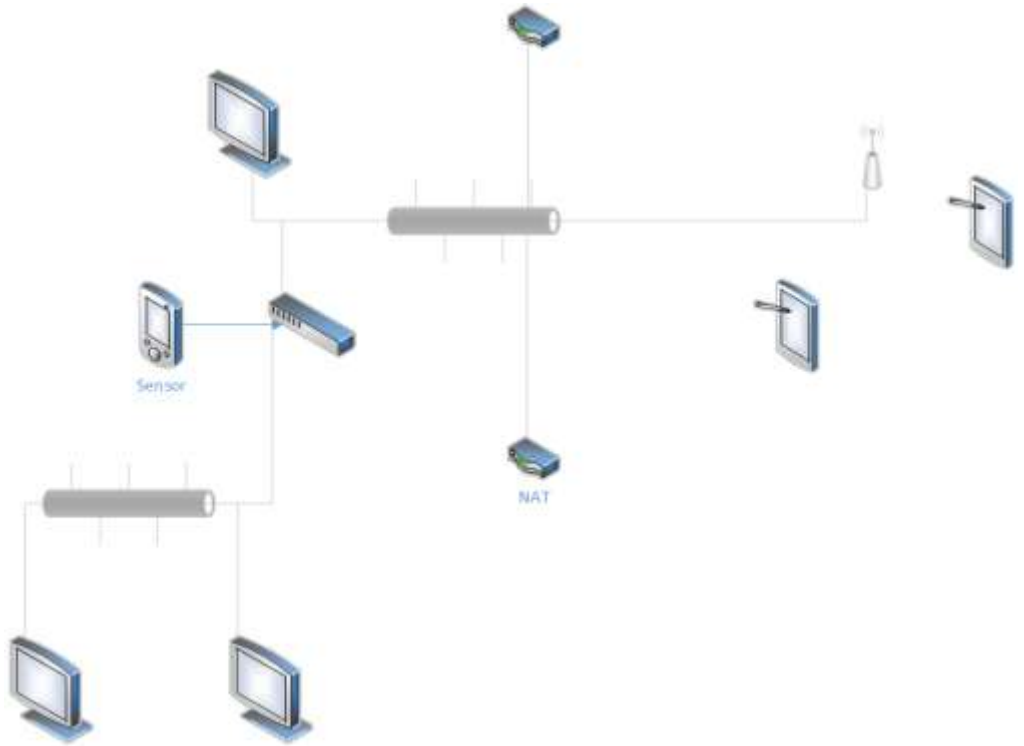
Ansprechstellen Anwender

Informationsquellen



Automatisches Asset Discovery

- Sensor im Netzwerk erkennt automatisch Vorhandene Assets
- Aufbereitung der Informations-austausche
- Auflistung der Assets



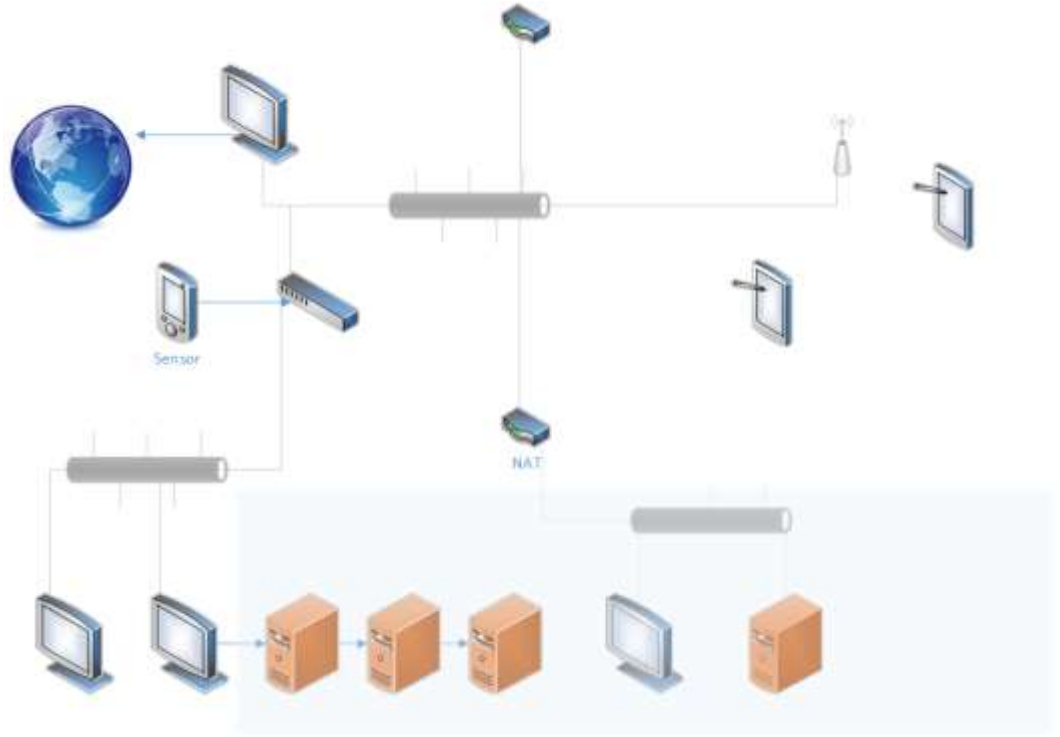
CyberSecurity

Automatisches Asset Discovery

Problemfelder:

- Direkte Internetverbindung
- Proprietäre bzw. nicht IP-basierte Bus-Systeme
- NAT-Router

- Konfigurationen
- Kontext/Prozess



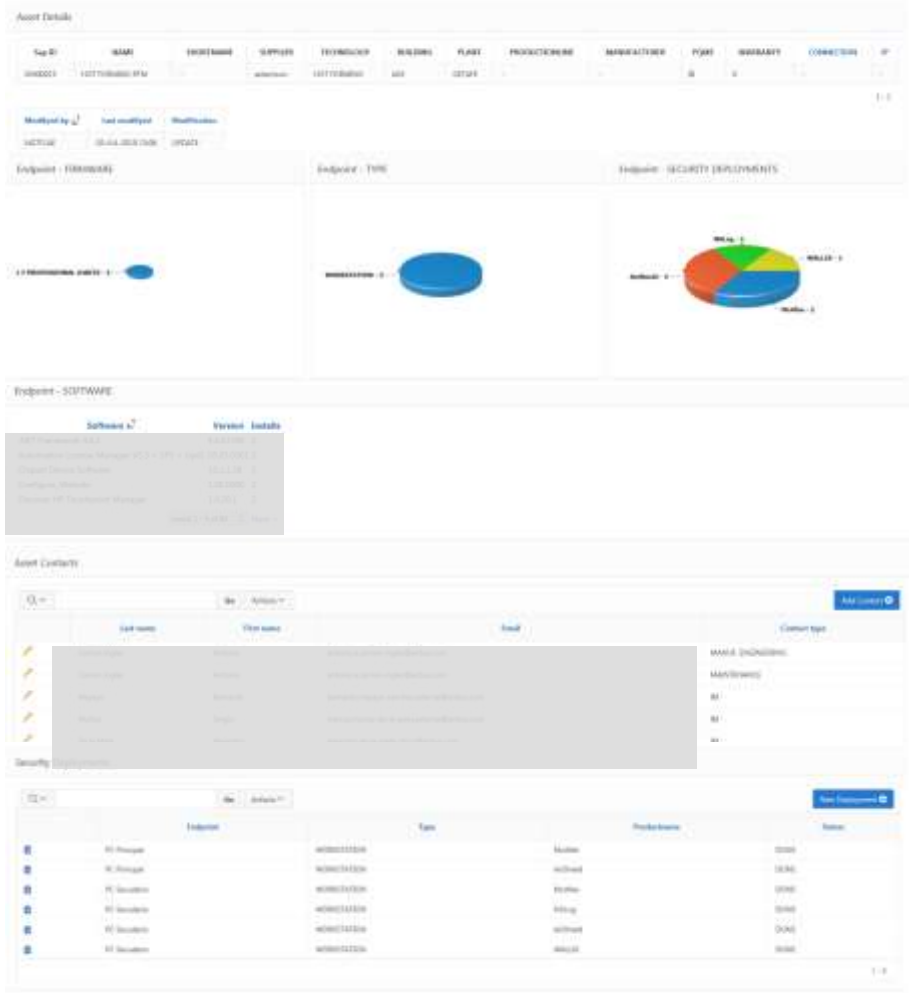
CyberSecurity

ICS Asset Inventory

- Zentralisiert, Geeignete Abbildungsform

- Erreichbar für alle Interessengruppen
  - Anwender,
  - Verantwortliche und
  - Auswerter
- Abbildung Heterogener Komponentenstruktur

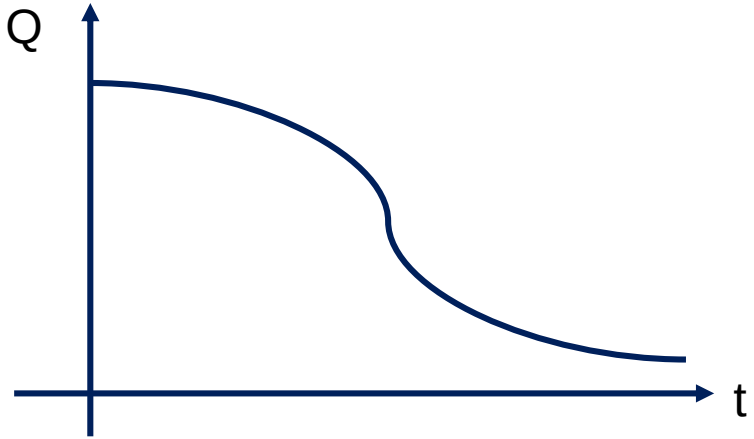
- Einbindung in Security Management System



Inventory Quality

Inventory accuracy is a key factor in meeting the security goals set forth in the security policy. *[IEC62443-1-1]*

Systeme sind bestmöglich zu dokumentieren und diese Dokumentation ist zu pflegen. *[VDMA]*



- Maintained Asset Inventory
  - ICS Lifecycle
- Prozesse
- Verantwortlichkeiten
- Kontrolle / Steuerung

Agenda

Verwendung Asset Informationen

- Kontextinformationen zur Bewertung
- Identifizierung von Ansprechstellen
- Eindämmung

- Kritischer Assets
- Risikobewertung
- Schwachstellenidentifikation

- Überwachung von Security Maßnahmen
- Zusammenhänge erkennen
- Abgleich mit automatischen Discovery Lösungen

- Zielgerichtete Planung von Security Maßnahmen
- Zonierungskonzept
- Update/ Patchplanung

Agenda

AIRBUS

CyberResilience for Tomorrow

Our approach

Assess

Gain visibility of your critical assets and receive recommendations to mitigate the identified risks

Protect

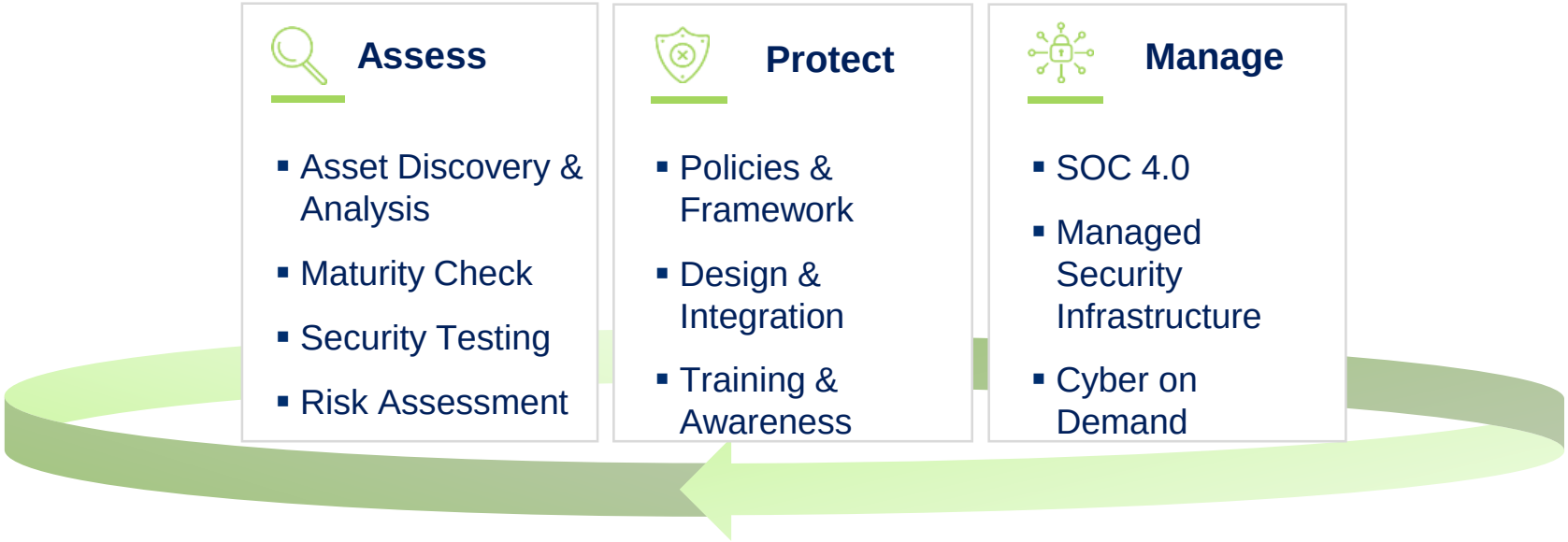
Improve your OT security controls with tailored consulting, training and design & integration services

Manage

Protective monitoring and continuous improvements of your security controls with tailored managed security services

CyberResilience for Tomorrow

Our OT Security Service & Solution Offerings




it sa 2019
Die IT-Security Messe und Kongress
8. - 10. Oktober 2019
Nürnberg
Halle 10.1
Stand 428
CyberSecurity
AIRB