NIDS und 62443
mehr gemeinsam als man denkt

Ein Gedankenanstoß

C0 - Public

$ whoami

- OT-Security Consultant
  - What I am good at:
    - IT/OT- Netzwerksecurity
    - (Alarm) Analyse
    - Projektplanung und Durchführung im Bereich Networksecurity
      - Erfahrung mit allen gängigen OT-IDS Plattformen
  - What I am bad at:
    - Foliendesign

Simon Rommer

simon.rommer@omicronenergy.com
0043 59 495

OMICRON

OMICRON ist Weltmarktführer

35 Jahre
im elektrischen Energiemarkt

10 Jahre
im Sektor
Cyber Security

24/7 Support
von Techniker:innen

> 1.000
Mitarbeiter:innen

Prüftechnik in der elektrischen Energieversorgung

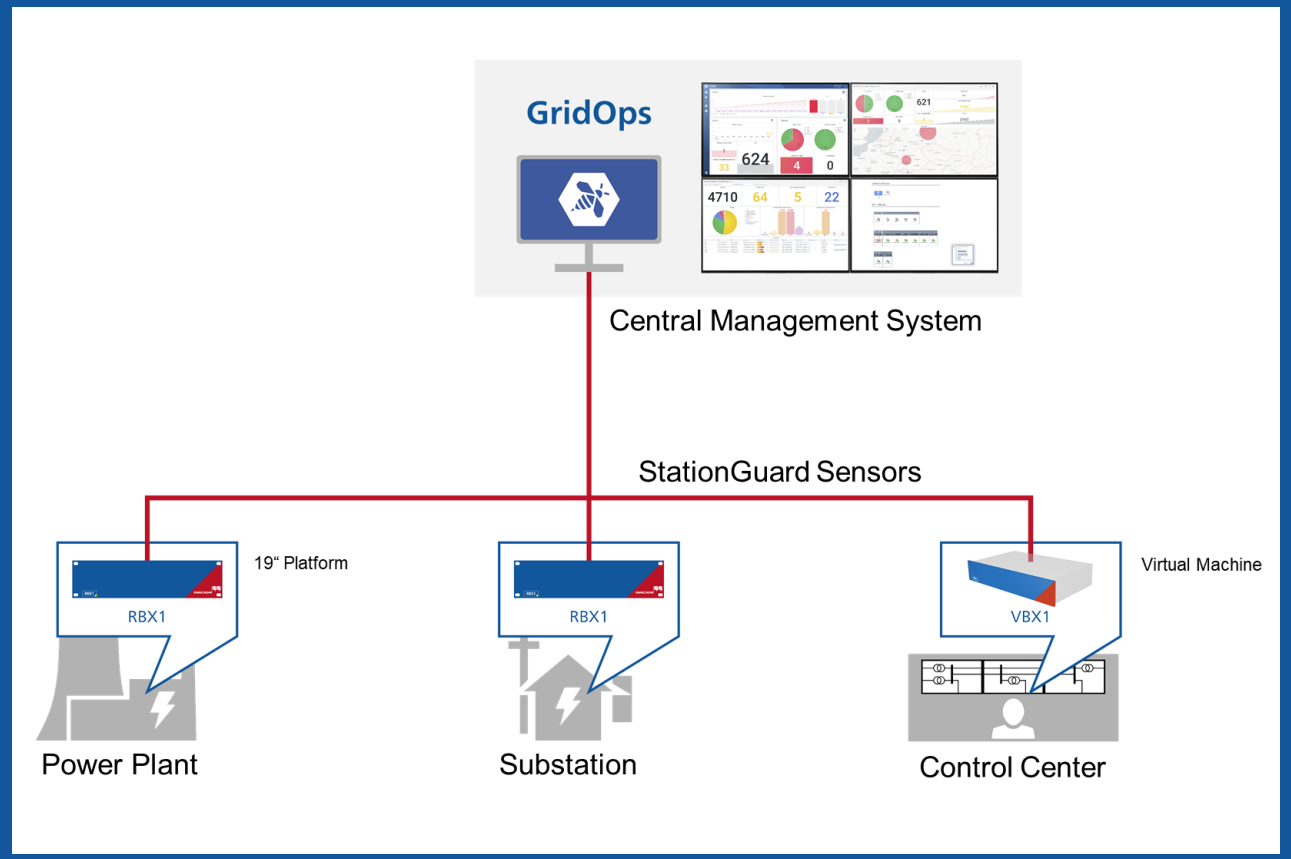
>40.000
Energieunternehmer-Kund:innen

in über 170 Ländern

Die größten Schwierigkeiten beim Assessment...

sind unvollständige / fehlerhafte Dokumentation.

C0 - Public



Wo hilft mir hier das NIDS?

Hilfestellung während ersten Schritte

- Erstellen eines Netzwerkdiagramms und einer Assetliste

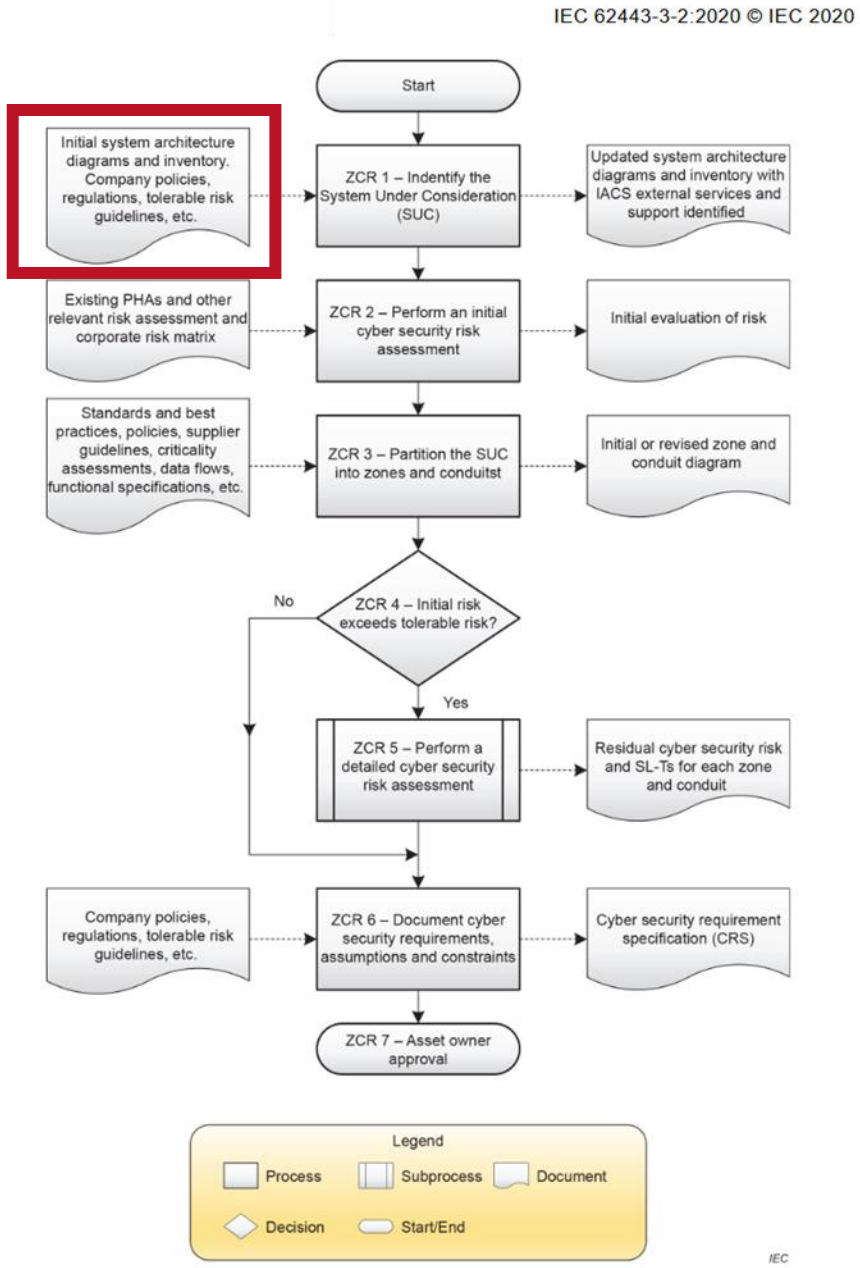
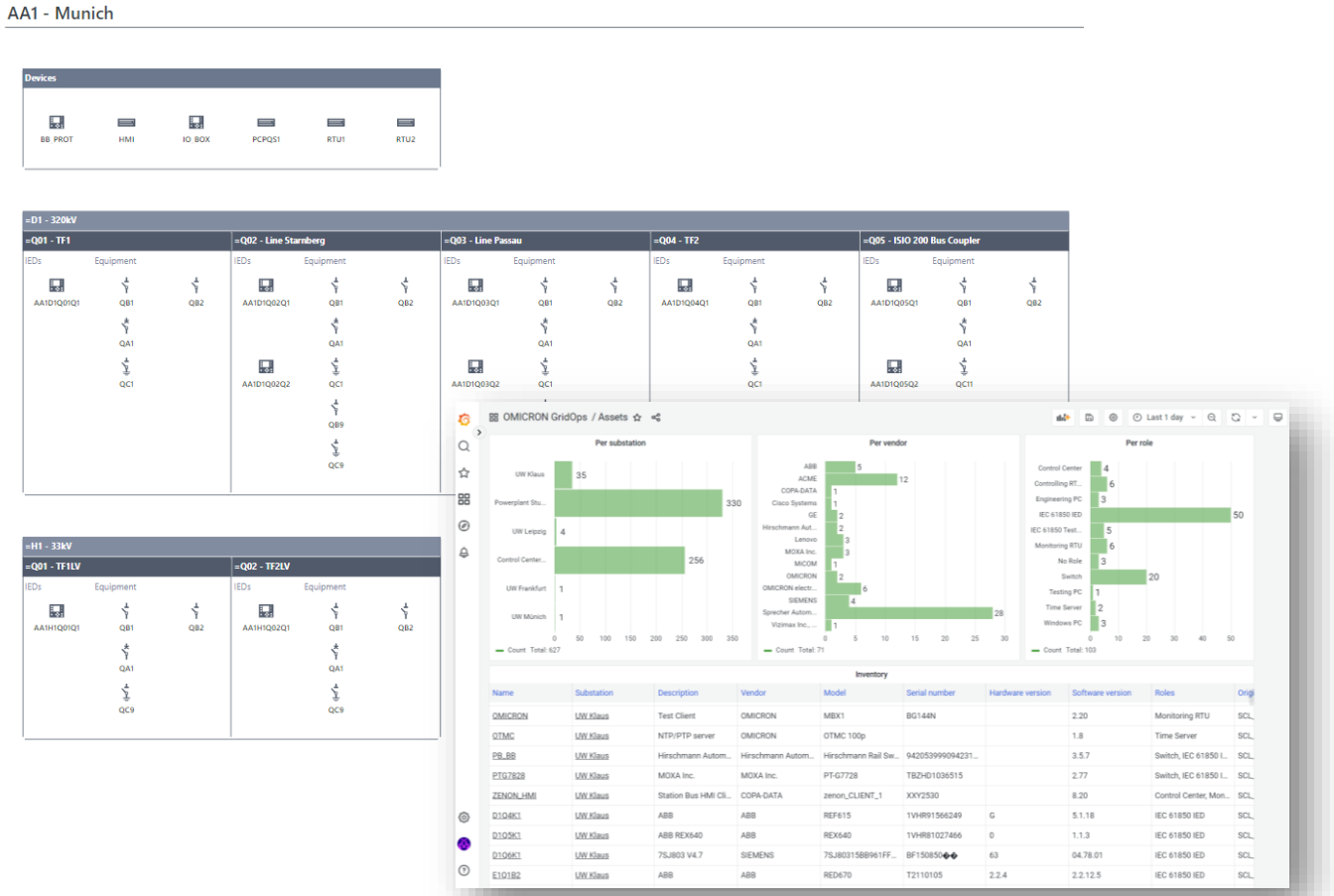


Figure 1 – Workflow diagram outlining the primary steps required to establish zones and conduits, as well as to assess risk



Hilfestellung während ersten Schritte

- Erstellen eines Netzwerkdiagramms und einer Assetliste

- Vulnerability Informationen
  - Auch für IEC62443-2-3 Patch Management

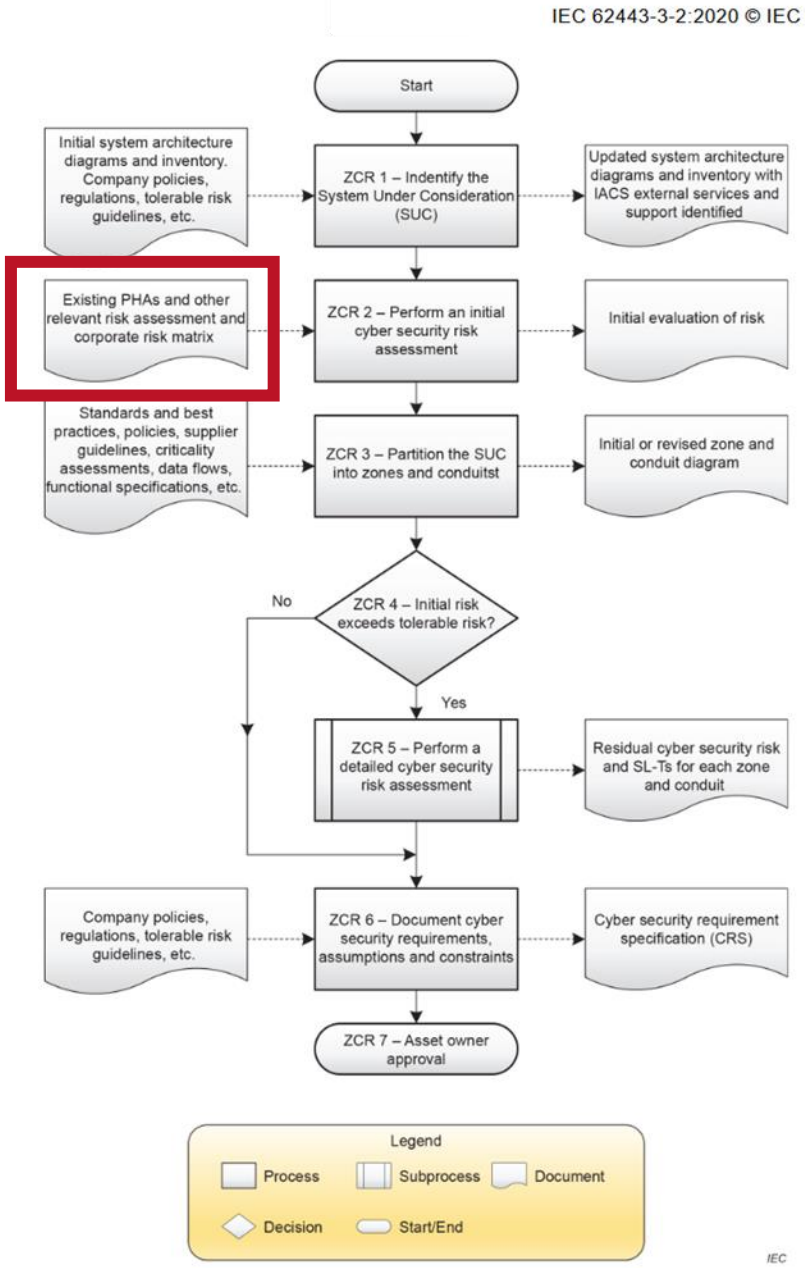
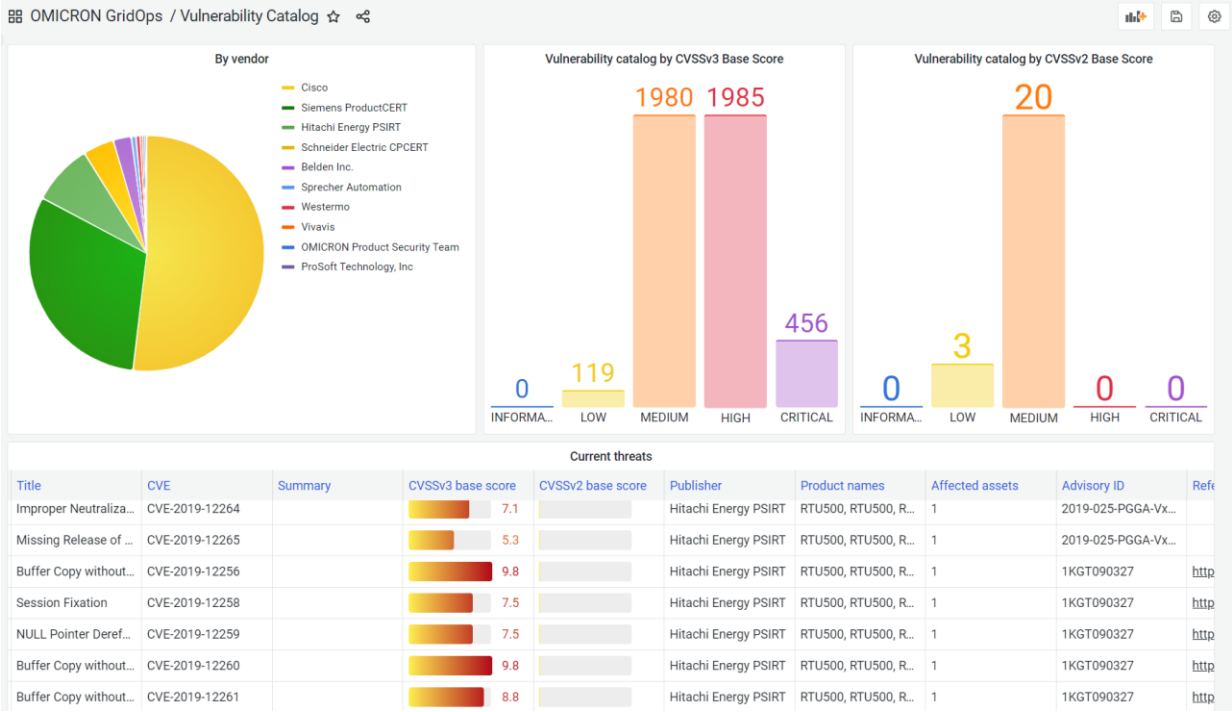


Figure 1 – Workflow diagram outlining the primary steps required to establish zones and conduits, as well as to assess risk



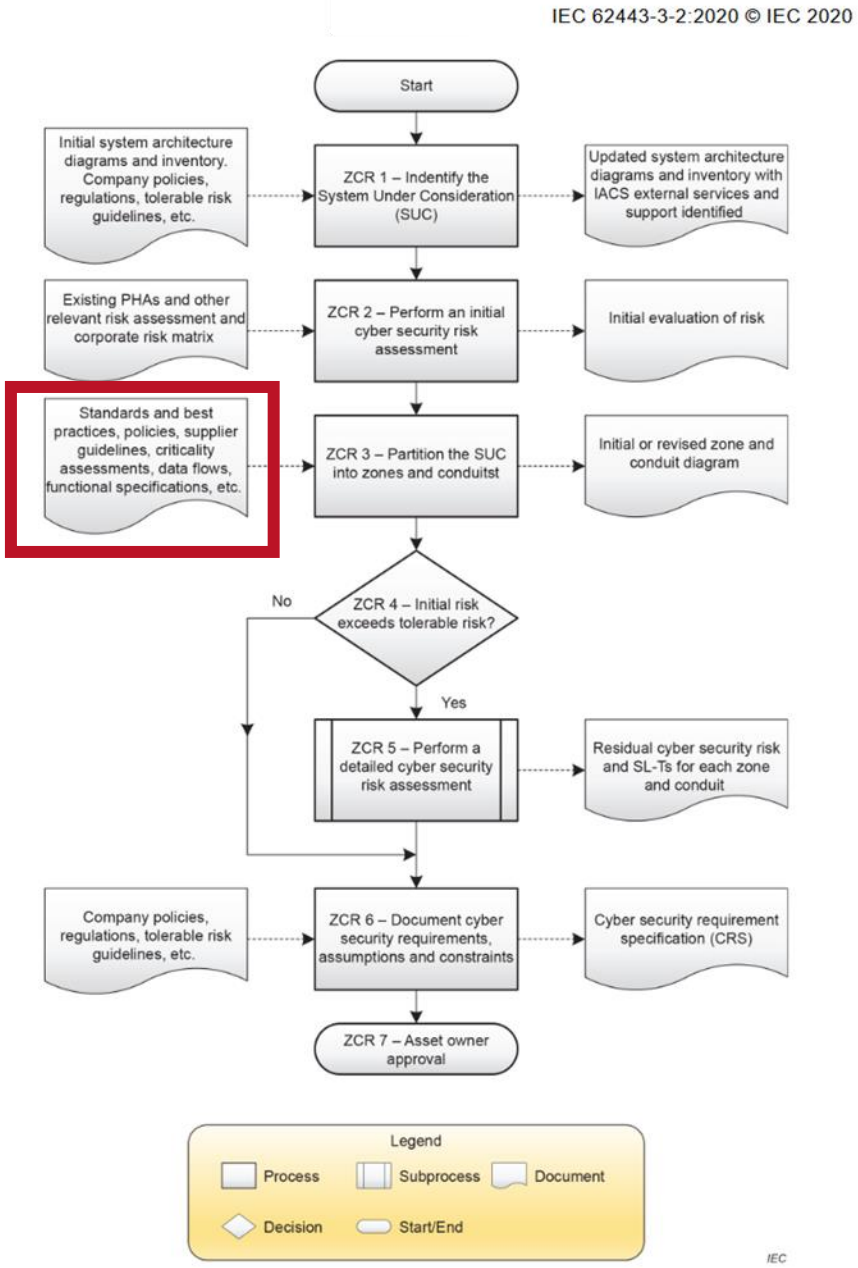
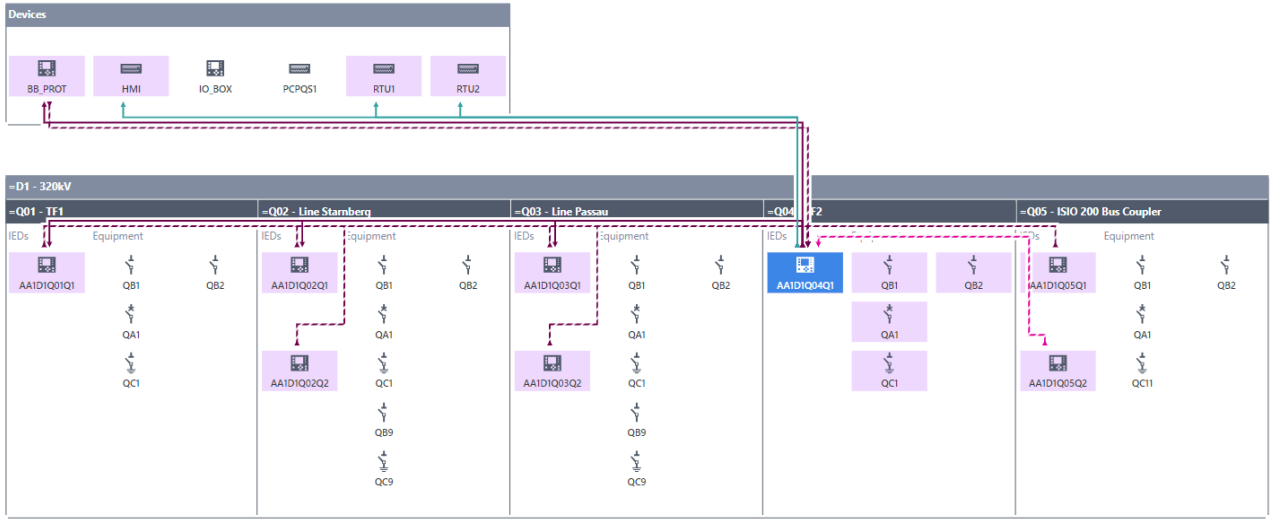


Figure 1 – Workflow diagram outlining the primary steps required to establish zones and conduits, as well as to assess risk

Hilfestellung während ersten Schritte

- Erstellen eines Netzwerkdiagramms und einer Assetliste
- Vulnerability Informationen
- Visualisieren von Data Flows
  - in speziellen Fällen auch mit Operational Functions



Validieren der Maßnahmen im nachgang

- Prüfen ob die Zones und Conduits eingehalten werden

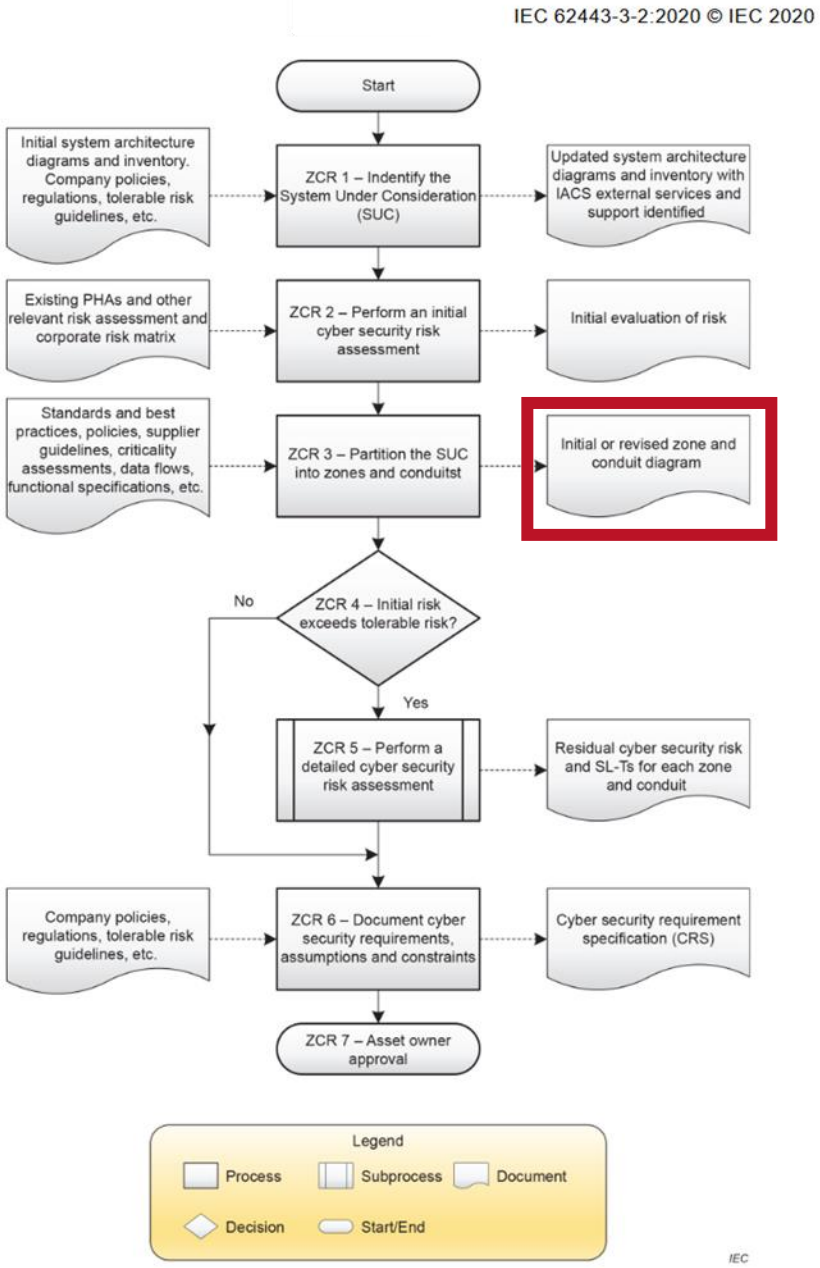
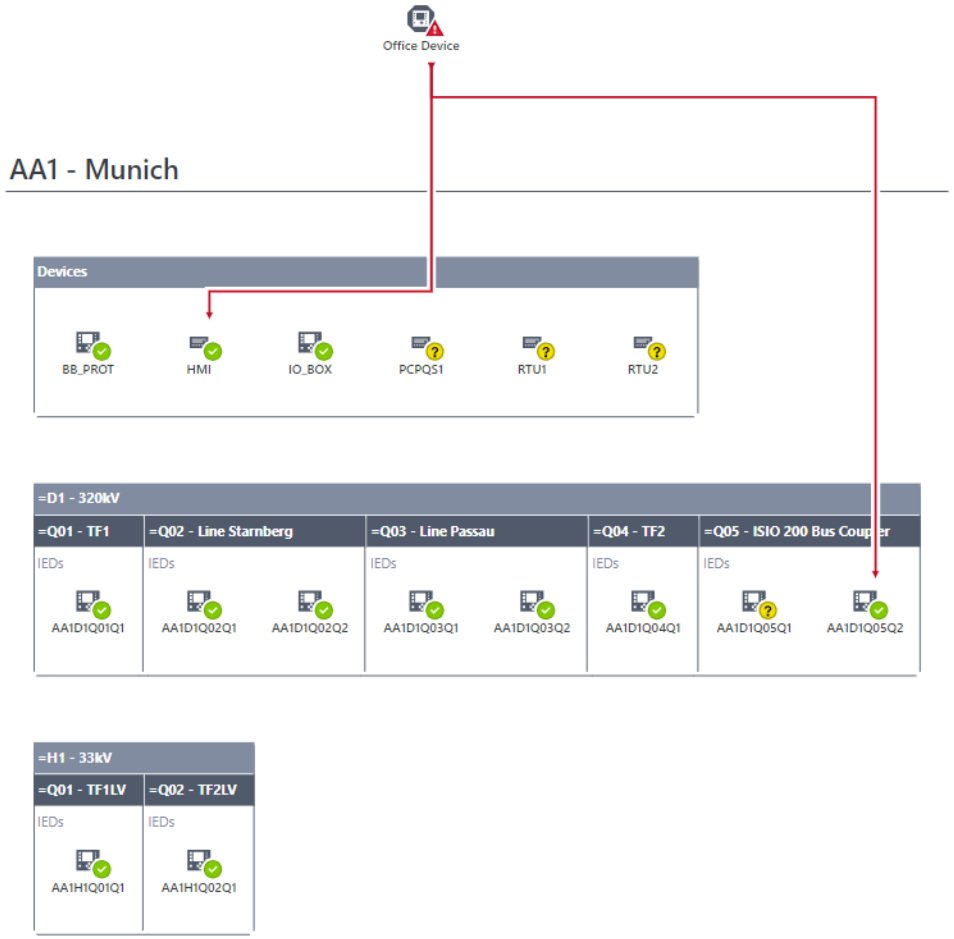
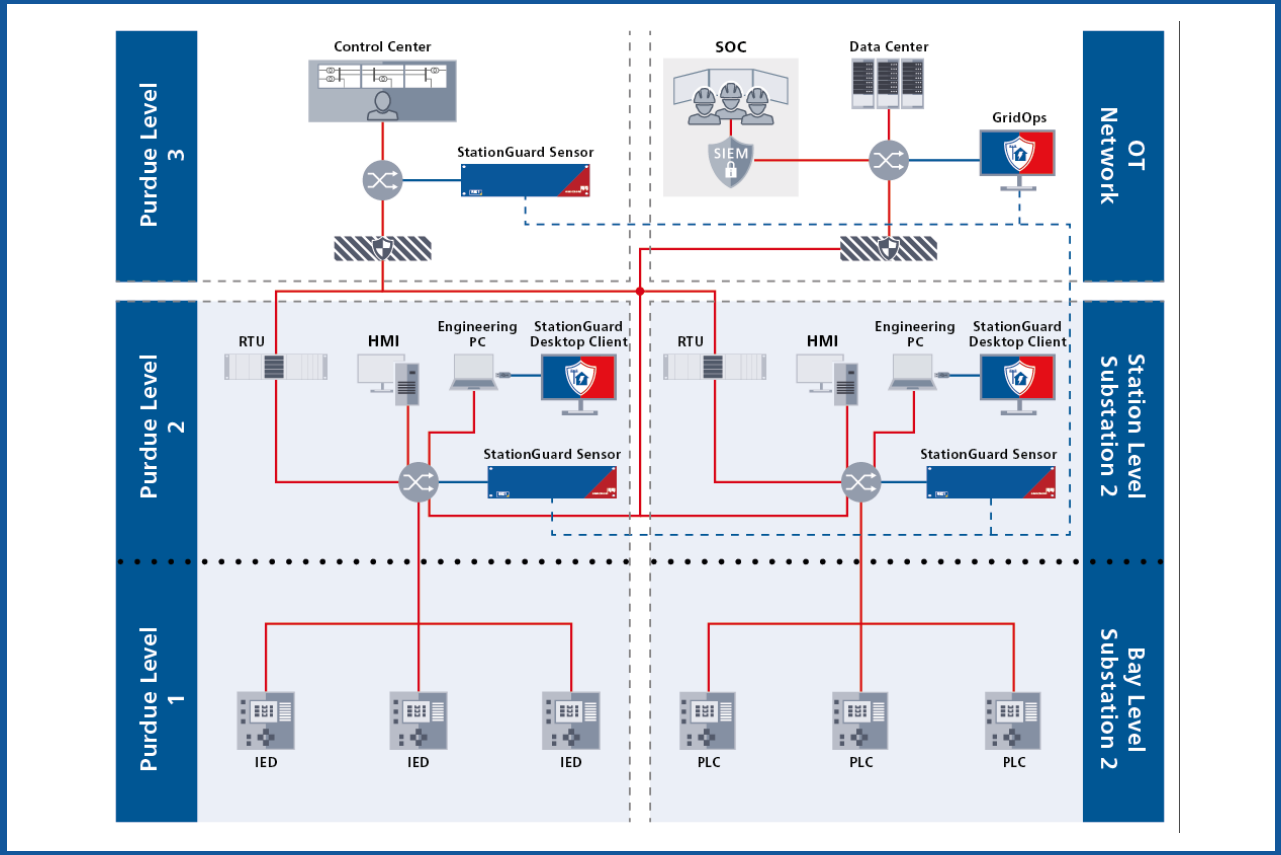


Figure 1 – Workflow diagram outlining the primary steps required to establish zones and conduits, as well as to assess risk



OMICRON



Was bewirkt das NIDS?

Beispiele aus IEC62443-3-3

FR 1 – Identification and authentication control (IAC)

- SR 1.11 – **Unsuccessful login attempts** The control system shall provide the capability to enforce a limit of a configurable number of consecutive invalid access attempts by any user (human, software process or device) during a configurable time period. The control system shall provide the capability to deny access for a specified period of time or until unlocked by an administrator when this limit has been exceeded. For system accounts on behalf of which critical services or servers are run, the control system shall provide the capability to disallow interactive logons.

- SR 1.12 – **System use notification** The control system shall provide the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorized personnel.

OMICRON

FR 2 – Use control (UC)

- SR 2.2 RE 1 – **Identify and report unauthorized wireless devices** The control system shall provide the capability to identify and report unauthorized wireless devices transmitting within the control system physical environment.

- SR 2.8 – **Auditable events** The control system shall provide the capability to generate audit records relevant to security for the following categories: access control, request errors, operating system events, control system events, backup and restore events, configuration changes, potential reconnaissance activity and audit log events. Individual audit records shall include the timestamp, source (originating device, software process or human user account), category, type, event ID and event result.

OMICRON

FR 3 – System integrity (SI)

- SR 3.1 – **Communication integrity** The control system shall provide the capability to protect the integrity of transmitted information.

- SR 3.2 – **Malicious code protection** The control system shall provide the capability to employ protection mechanisms to prevent, detect, report and mitigate the effects of malicious code or unauthorized software. The control system shall provide the capability to update the protection mechanisms.

OMICRON

FR 5 – Restricted data flow (RDF)

- SR 5.1 – **Network segmentation** The control system shall provide the capability to logically segment control system networks from non-control system networks and to logically segment critical control system networks from other control system networks.

- SR 5.2 – **Zone boundary protection** The control system shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk-based zones and conduits model.

Viele (Security) Lösungen haben „zusätzliche Features“

last uns diese auch nutzen.

C0 - Public

Danke für Ihre Aufmerksamkeit

C0 - Public