Cyberresilienz in der Energieversorgung

Deutsch-Finnisches Businessforum 2023
Rostock, 28.09.2023

Steffen Nicolai, Fraunhofer IOSB-AST

IOSB GESAMT

790 **Mitarbeiterinnen und Mitarbeiter**

- ca. 370 Wissenschaftler*innen
- ca. 200 Studierende
- Hauptsitz: Karlsruhe

65 **Millionen Euro Haushalt**

Betrieb und Investitionen 2020

16 **Wissenschaftliche Abteilungen**

5 **Geschäftsfelder**

6 **Standorte**

Lernlabor Cybersicherheit Energie- und Wasserversorgung

State-of-the-Art Forschung im Bereich der IT-Cybersicherheit für kritische Infrastrukturen. Umfangreiches Schulungsportfolio. Individuelle Kundenberatung vor Ort.

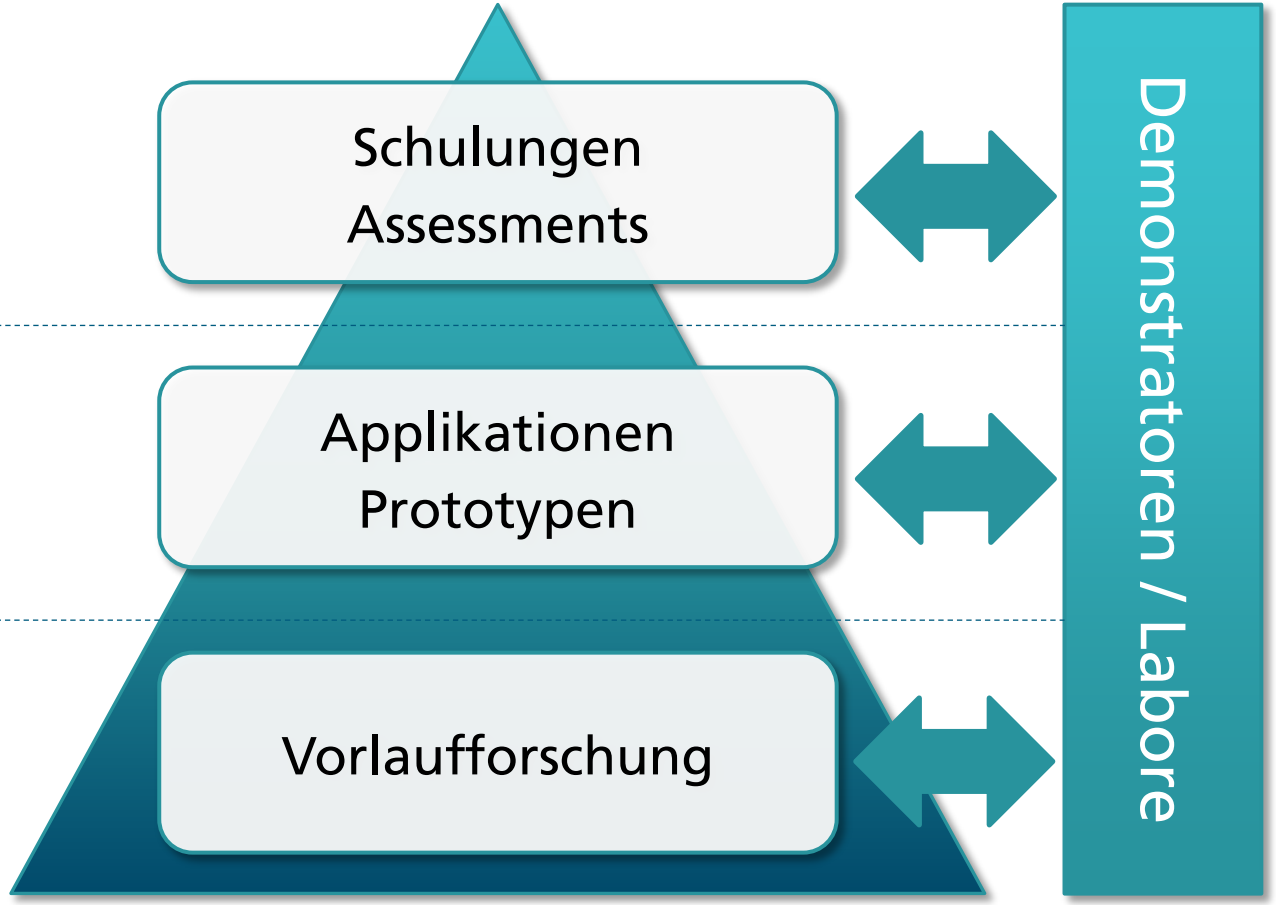
Lernlabor Cybersicherheit „Energie- und Wasserversorgung“

Schwerpunkte

- Awareness, Inhouse-Schulungen, Technische Intensivkurse
- Analysen, Konzepte und Workshops

- Überführung in Hardwareplattform
- Erprobung / Validierung

- Entwicklung neuer Methoden und Verfahren zur Erkennung und Abwehr von Cyber-Angriffen



Cyberresilienz in der Energieversorgung

Cyberresilienz in der Energieversorgung

Herausforderungen

Herausforderungen

- Energieversorgung als Kritische Infrastruktur
- Höchst komplexes gekoppeltes System mit sehr vielen Akteuren
- Fortschreitende Digitalisierung der Energieversorgung bei gleichzeitiger Dezentralisierung der Erzeugung
- Prozess-IT (OT) als heterogenes, stark verteiltes System mit signifikanten Unterschieden zu herkömmlichen IT-Systemen
- Zunehmende Abhängigkeit der Versorgungssicherheit von IT/OT-Infrastrukturen
- Vollständige Absicherung der OT-Infrastrukturen kaum möglich

Cyberresilienz in der Energieversorgung

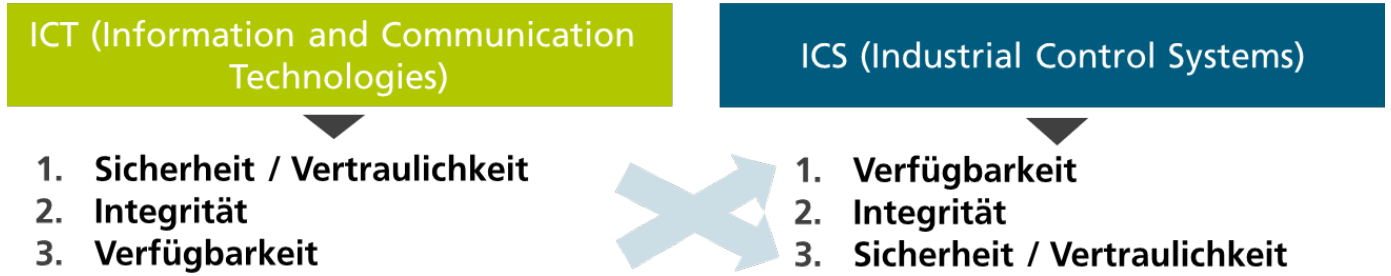
Herausforderungen - Schutzziele

Schutzziele allgemein

- **Vertraulichkeit** - *Schutz vor unbefugter Preisgabe von vertraulichen Informationen*
- **Integrität** - *Korrektheit, Manipulationsfreiheit von IT-Systemen und Informationen*
- **Verfügbarkeit** – *Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems oder Informationen*

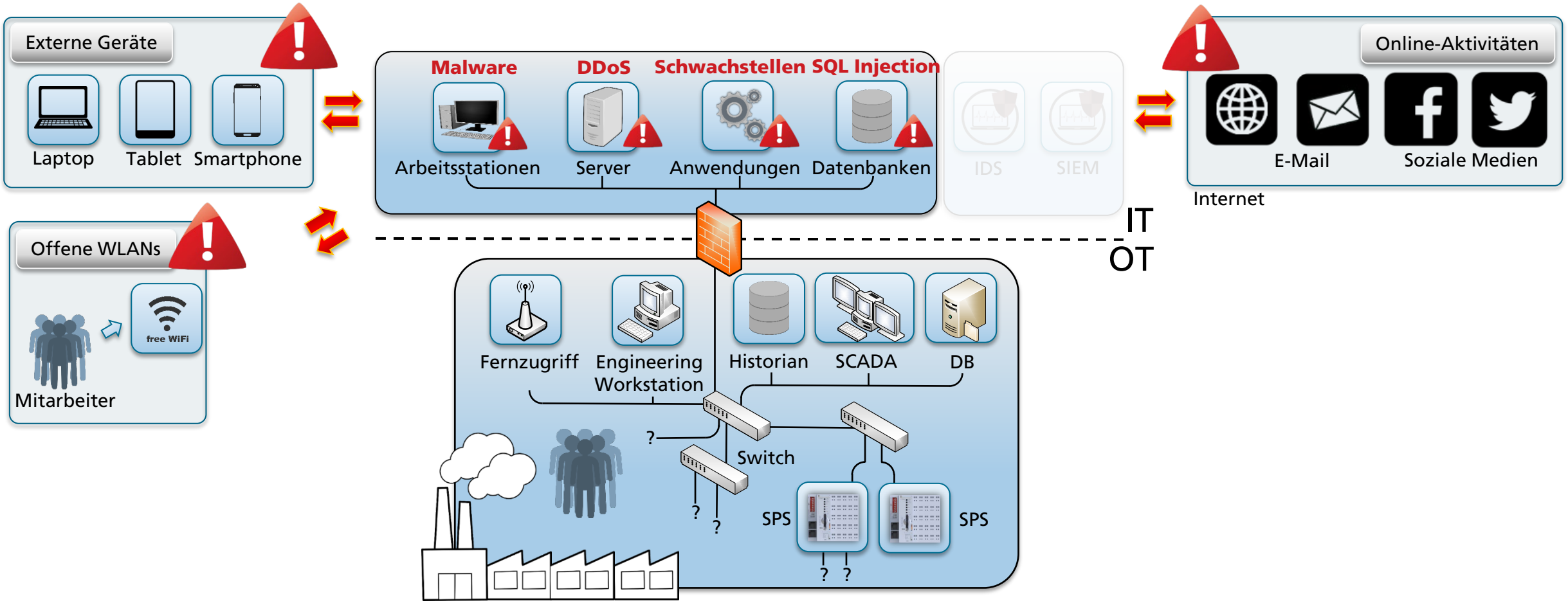
Umkehr Schutzziele in OT-Systemen (ICS)

- Oberste Anforderung im OT-Bereich war bisher Verfügbarkeit
- Sicherheit / Vertraulichkeit bisher strukturell durch isolierte Umgebungen („air gapped“) realisiert
- zunehmende Vernetzung der ICS-Strukturen über TCP/IP basierte Protokolle
- Adaption der Schutzziele notwendig



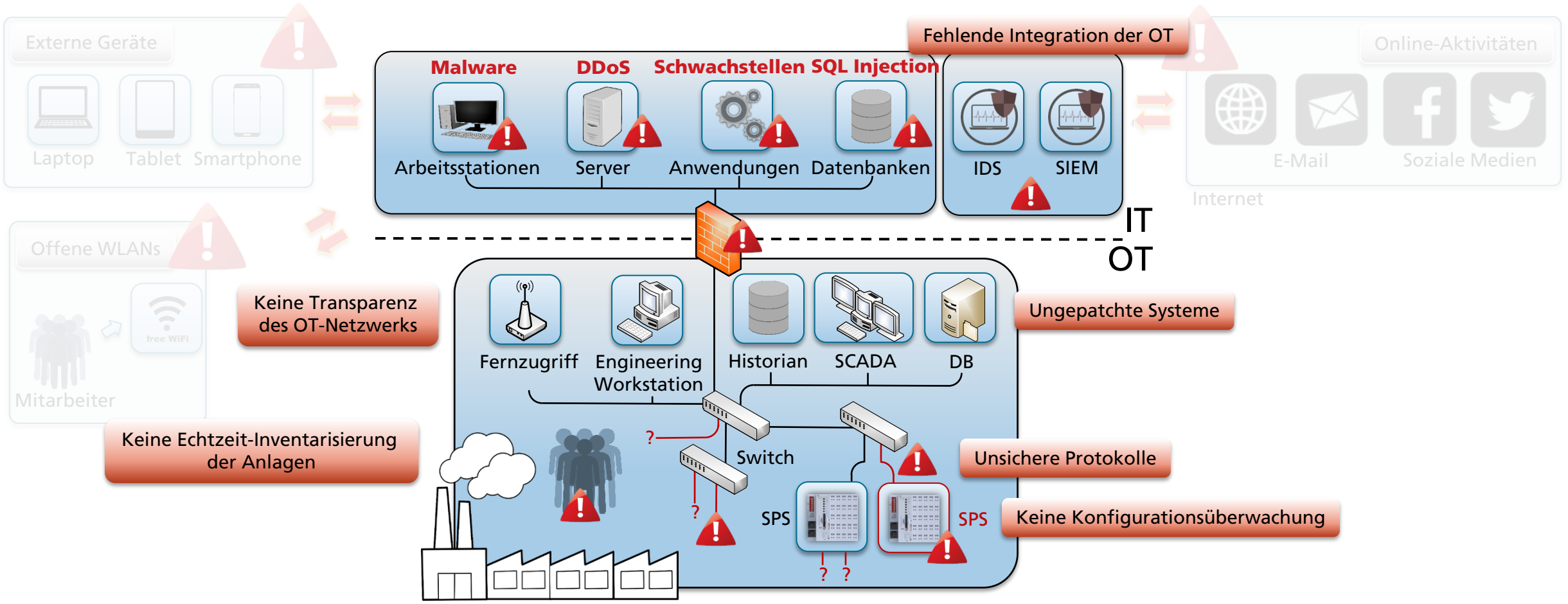
Cyberresilienz in der Energieversorgung

Mögliche Bedrohungen und Schwachstellen – IT-Bereich



Cyberresilienz in der Energieversorgung

Mögliche Bedrohungen und Schwachstellen – OT-Bereich



Cyberresilienz in der Energieversorgung

Cyberresilienz als ganzheitlicher Ansatz der Cybersicherheit

Definition Cyberresilienz (Quelle: nvlpubs.nist.gov/)

The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.
Cyber resiliency is intended to enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment.

Cyberresilienz Framework

- Betrachtung der Cyberresilienz als Phasen
- Zuordnung von Tasks zu den einzelnen Phasen
- Resilienz als fortlaufender Zyklus

Grafik: https://www.infusedinnovations.com/blog/secure-intelligent-workplace/the-fundamentals-of-a-strong-cybersecurity-framework

Cyberresilienz in der Energieversorgung

Resilienz-Phasen und Tasks

Identify

- Security Assessments in OT-Infrastrukturen
- Risiko- / Auswirkungsanalysen Versorgungsprozess
- Assetmanagement

Protect

- Awareness / Schulungen
- Daten-, Gerätesicherheit und sichere OT-Kommunikation

Detect

- Cyber-physische Anomalieerkennung
- Systeme zur Angriffserkennung / Advanced SIEM

Respond

- Incident Management
- N-1-Sicherheit Energie- und IKT-Infrastrukturen

Recover

- Recovery Planung Energieinfrastrukturen
- Resiliente Kommunikationsinfrastrukturen

Cyberresilienz in der Energieversorgung

Cyberresilienz Metriken

Cyberresilienz Metriken

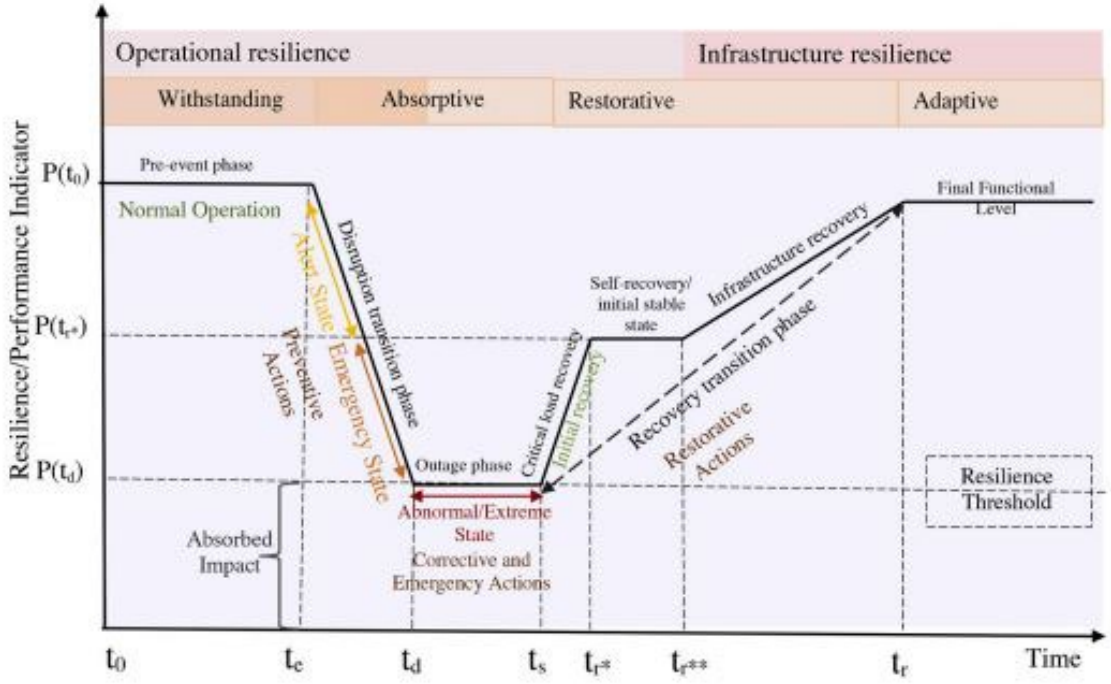
- Bewertung der Resilienzfähigkeit mit messbaren Indikatoren (KPI)
- Resilienzkurve anhand derer die verschiedenen Phasen des Zyklus identifiziert werden können
- KPI-basierte Messung erfordert Resilienzmetriken

Statische Metriken

- Mean-time-to-patch
- Percent of systems without known severe vulnerabilities
- Mean-time-to-repair
- Number of new vulnerabilities discovered

Dynamische Metriken

- Traffic tolerance
- Number of detected attacks
- Mean-down-time
- Percent of improvement in incident response time



Cyberresilienz in der Energieversorgung

Gesetzliche Vorgaben zur Etablierung einer Cyberresilienz

IT-Sicherheitsgesetz 2.0

- Wesentlicher Aspekt sind Systeme zur Angriffserkennung
- Zum 01.05.2023 erste Zertifizierung

Orientierungshilfe für Systeme zur Angriffserkennung (BSI)

- Unterteilung in drei relevante Bereiche mit definierten Anforderungen
  - Protokollierung, Detektion und Reaktion
- Übergeordnet werden allgemeine Anforderungen an das SzA definiert
  - Rahmenbedingungen, Angriffsmuster, Plattform, Signaturen und Konfiguration

Zukünftige Gesetzgebungen

- Verstärkter Fokus auf Resilienz
- Erweiterung des Kreises betroffener Betreiber
- Mehr Verpflichtungen zur systematischen Prävention, Detektion und Reaktion gegenüber Cyber-Angriffen

Cyberresilienz in der Energieversorgung

Forschungsansätze - Simulations-basierte Risiko- und Auswirkungsanalysen

Simulations-basierte Risiko- und Auswirkungsanalysen

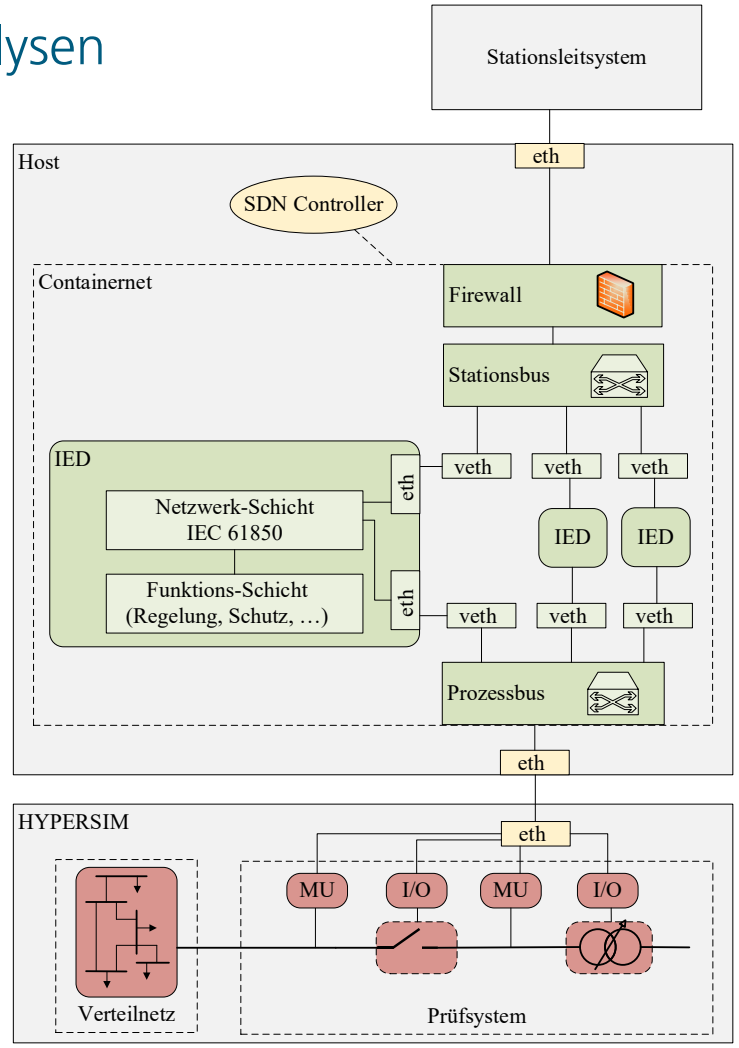
- Abbildung der Abhängigkeiten zwischen Energienetz und Kommunikationsnetz
- Mögliche Anwendungen:
  - Simulation von Cyberangriffen
  - Nutzung als Entwicklung für Erkennungsverfahren

Entwicklung einer Co-Simulation der Stationsautomatisierung

Entwicklung einer virtuellen Digitalen Station

- Abbildung der Komponenten der Stationsautomatisierung als virtuelle Instanzen
  - Nutzung von Container-basierter Virtualisierung als Docker Container
  - Integration von IEC 61850 Netzwerkschicht und Funktionsschicht

Virtuelles Testbed für simulative Analysen



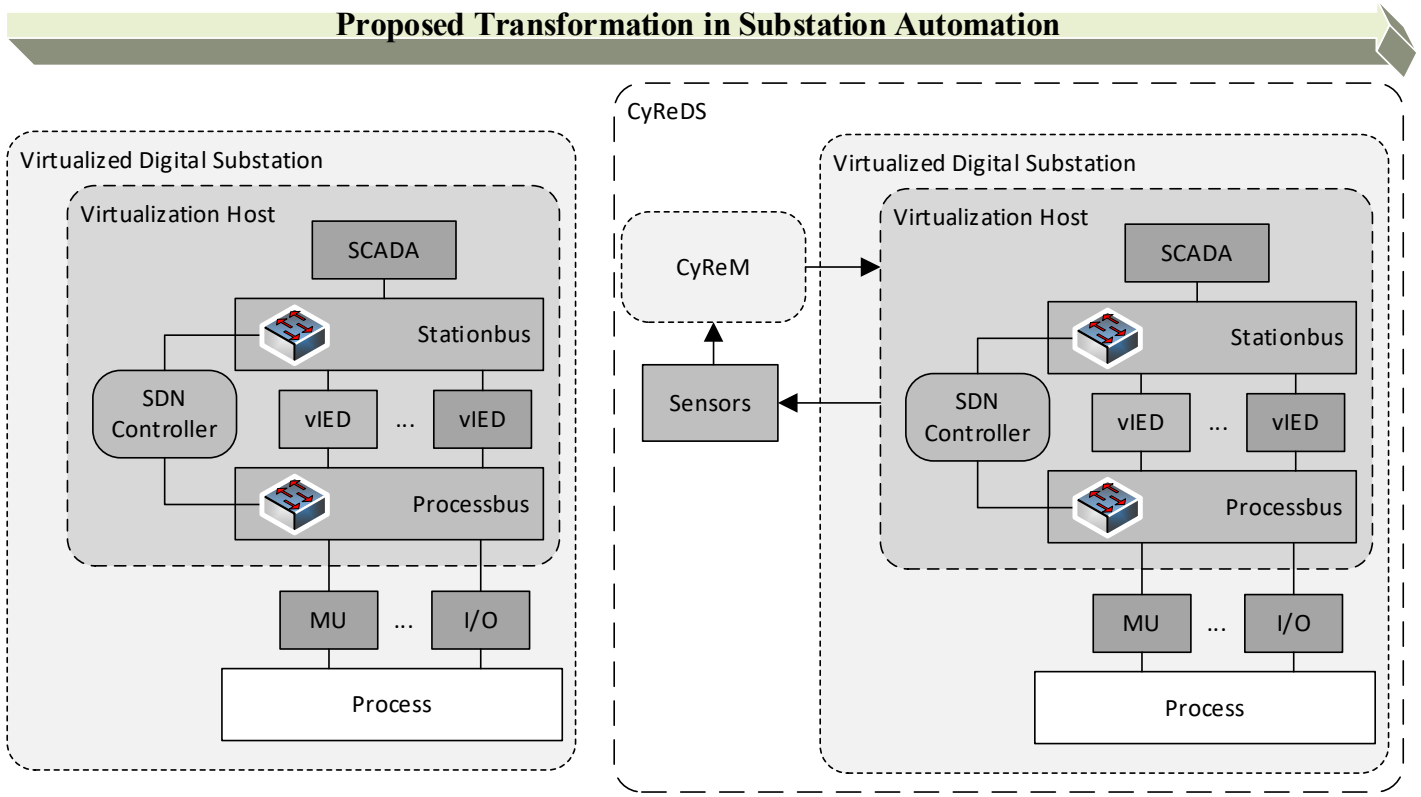
D. Rösch et. al: Combined simulation and virtualization approach for interconnected substation automation. In: 2021 6th International Conference on Smart and Sustainable Technologies (SpliTech), Bol and Split, Croatia, pp. 1–6.

Cyberresilienz in der Energieversorgung

Forschungsansätze - Erhöhung der Cyberresilienz durch Virtualisierung

Resiliente / Virtualisierte Infrastrukturen

- Überführung der physischen Sekundärsysteme in virtuelle Abbildungen für zukünftige Umspannstationen
- Einbinden von Resilienz- und Redundanz-Strategien durch flexibles Design der Virtualisierung
- Baustein für automatisiert verwaltete Stationen (Update- und Patch-Management)
- Integration in Konzepte der Cyber-Resilienten-Digitalen-Stationen



Rösch, Dennis; Bauer, Thomas; Kummerow, André; Kühne, Marcel; Nicolai, Steffen; Bretschneider, Peter (2023): Transformation in substation automation: Cyber-Resilient Digital Substations (CyReDS) in power grids. In: at - Automatisierungstechnik 71 (9), S. 789–801. DOI: 10.1515/auto-2023-0075.

Kontakt:

Dipl.-Ing. Steffen Nicolai
Fraunhofer IOSB-AST
Am Vogelherd 90
98693 Ilmenau
03677 461 112
steffen.nicolai@iosb-ast.fraunhofer.de
www.iosb-ast.fraunhofer.de