Effiziente Cyber-Resilienz

Forschung für ein resilientes Energiesystem in Zeiten globaler Krisen
FVEE-Tagung 10. / 11. Oktober 2023

Autoren:

Dr. Kaibin Bao, Dr. Ghada Elbez (KIT)
Dr. Marco Selig, Kerstin Wurdinger (DBFZ)
Stefan Siegl (Fraunhofer IEE)

Warum ist die Widerstandsfähigkeit des deutschen Energiesystems gegenüber Cyberangriffe gerade jetzt ein Thema?

Entwicklung von hierarchischer zur dezentralen/zellularen Netzinfrastruktur der Energiesysteme

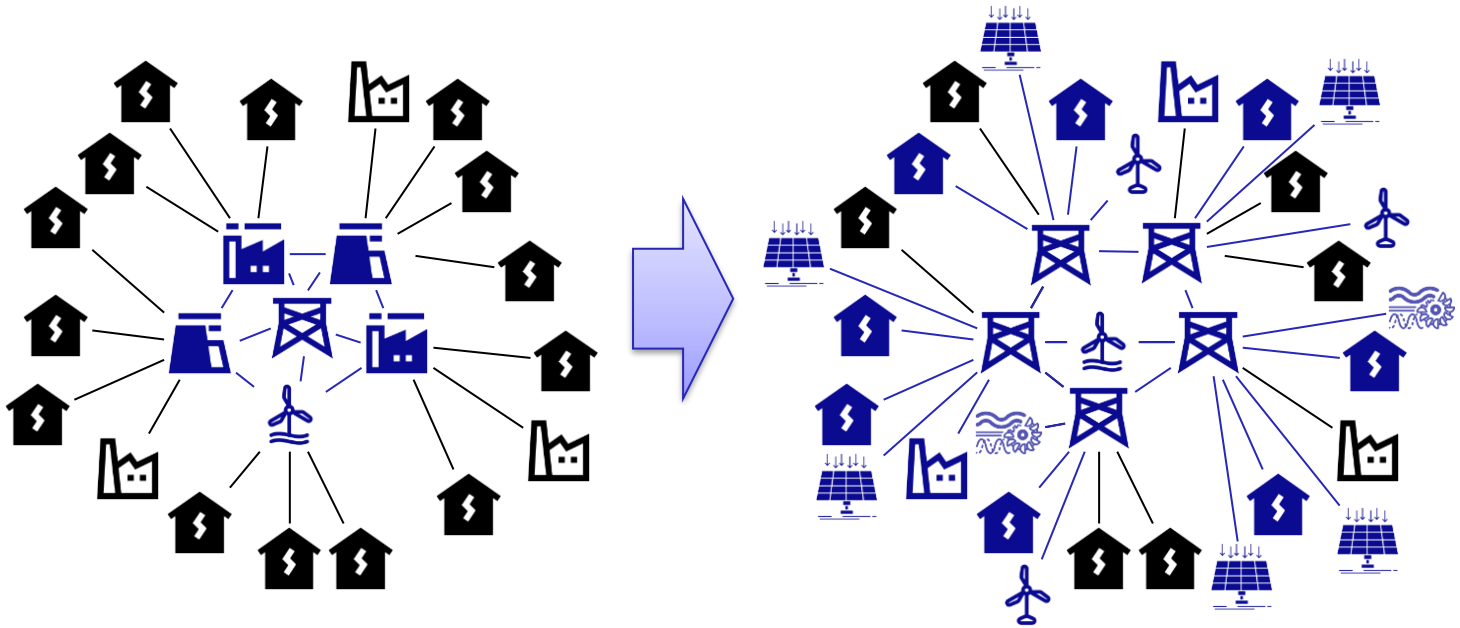
→ Höhere Komplexität

→ Umfassenderes Management (Monitoring, Reglung, Zugangsprüfung, …) der Primärtechnik

→ Mehr Sekundärtechnik (digitale Komponenten) für sicheren Betrieb notwendig

- **Fernwartung**
- **Fernüberwachung**
- **Fernwirktechnik**

→ Vergrößerte Angriffsflächen gegenüber Cyber-Angriffen



Cyber-Resilienz eng verwandt zu Cyber-Sicherheit

„The first questions to ask are:
‚Secure from whom?‘ and ‚Secure against what?‘
[…] Like any adjective, ‚secure‘ is meaningless out of context.“

Bruce Schneier (2000): Secrets & Lies

Verlauf eines Cyberangriffs auf Energiesysteme am Beispiel Industroyer

		MITRE ATT&CK Taktik
	Informationen über Angriffsziel erlangen	Reconnaissance
	Entwicklung der Malware Industroyer	Resource Development
Januar 2016	Phishing Kampagne	Initial Access
	Nutzung von gültigen Zugangsdaten	
	Weitere Zugangsdaten stehlen	Credential Access
	MS-SQL-Konto um Zugriff weitere Daten erweitern	Persistence
	Ersetzen des Texteditors mit einer Hintertür	Persistence
	Durchsuchen des Active Directory / des Netzwerks	Discovery
	Windows Management Instrumentation für Fernzugriff	Execution
Dezember 2016	Zugang zum Automationsnetzwerk erlangt	Lateral Movement
	Anlagen von lokalen Konten	Persistence
	Ziel-spezifische Module übertragen (IEC 104, 61850, OPC)	Lateral Movement
	Löschen von Projektdateien für die Schutztechnik	Inhibit Response
	Auslösen der Leistungstrennschalter im Umschaltwerk	Impact

[MITRE]

Was ist Cyber-Resilienz?

Cyber-Resilienz ist die Fähigkeit einer Organisation, den operativen Betrieb trotz Cyberbedrohungen aufrechtzuerhalten und sich von diesen Bedrohungen zu erholen.

Die Ziele von Cyber-Resilienz [NIST SP 800-160]

Bereitschaft	Widerstehen	Wiederherstellung	Anpassung
Informierte Bereitschaft für Umstände, die es Angreifern (Advanced Persistent Threat, APT) ermöglicht, Sicherheitsvorfälle auszulösen.	Fortführung wesentlicher Aufgaben oder Geschäftsfunktionen trotz Sicherheitsvorfälle.	Wiederherstellung von Einsatz- oder Geschäftsfunktionen während und nach Sicherheitsvorfällen.	Änderung der Aufgaben- oder Geschäftsfunktionen als Reaktion auf vorhergesagte Veränderungen im technischen Umfeld, Betriebsumfeld oder Bedrohungslage.

Rahmen und Grundlagen für Betreiber sog. „Kritischer Infrastrukturen“*)

- BSI IT-Sicherheitsgesetz 1.0 / 2.0
- BSI-Sicherheitsgesetz
- BSI-KritisVerordnung
- EU-Sicherheitsrichtlinie NIS und NIS 2 (Network and Information Security 2)
- EU RCE – CER-Richtlinie (Critical Entities Resilience)
- Übersicht: www.openkritis.de

Anforderungen zum Management von Cyber-Risiken*)

Technische, sicherheitsbezogene und organisatorische Maßnahmen (Management-System, Regelwerk/Richtlinien, Audits, Personalsicherheit, Lieferanten, Meldepflichten, …)

- Mindeststandards für Betreiber
- Verpflichtende Risikobewertungen
- Zentrale Sicherheitsüberwachung

Relevante Normen*)

- ISO 27001 – Management-System für Informationssicherheit (ISMS)
- IEC 62443 – Cybersicherheit für Automationssysteme
- IEC 62351 – Cybersicherheit für digitale Energiesystemkomponenten
- ISO 22301 – Management-System für betriebliche Kontinuität (BCMS)

*) Auswahl

Bausteine für Cyber-Resilienz

Sicherheitsüberwachung

- Security Information and Event Management (SIEM)
- Security Orchestration, Automation and Response (SOAR)
- Extended Detection and Response (XDR)
- Network Security Monitoring (NSM)

Netzwerksegmentierung

- Aufteilung der Systeme an fachlichen und technischen Grenzen
- Zero Trust Model

Notfallpläne

- Entwicklung von Plänen für eine schnelle Reaktion auf Sicherheitsvorfälle
- Meldepflicht

Prävention

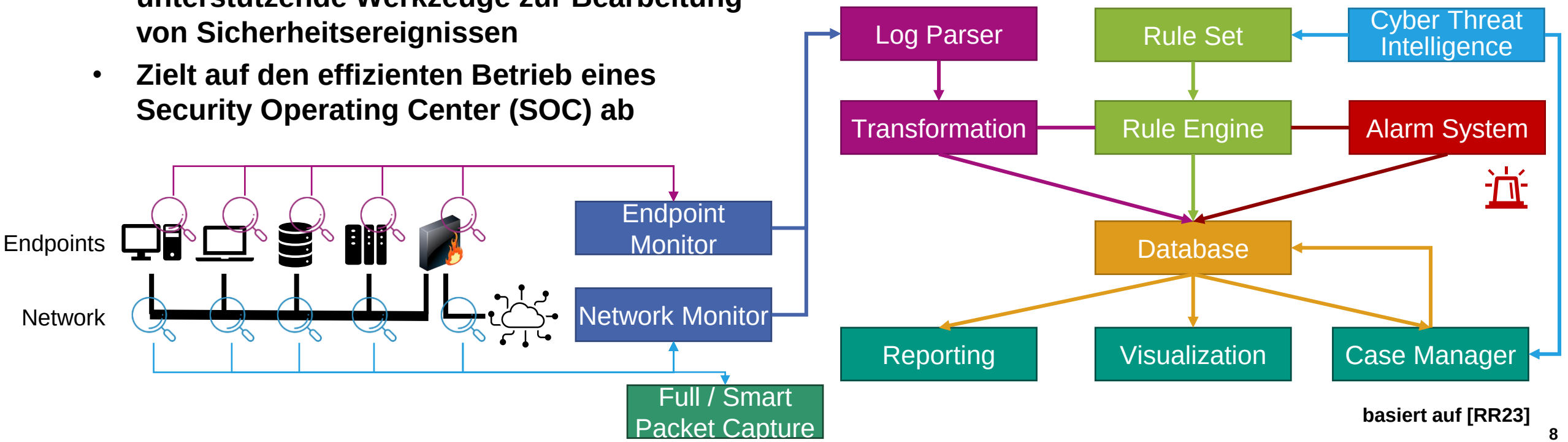
- Cyber Threat Intelligence (CTI)
- Mitarbeiterschulungen
- Schwachstellen-Management
- Risikobewertung

Wiederherstellung

- Effektives Backup- und Wiederherstellungs-Management

Moderne Sicherheitsüberwachungssysteme: Extended Detection and Response (XDR)

- **XDR oder SIEM sammeln Informationen und sicherheitsrelevante Ereignisse im gesamten Cyberphysikalischen System**
- **Moderne XDR-Frameworks enthalten unterstützende Werkzeuge zur Bearbeitung von Sicherheitsereignissen**
- **Zielt auf den effizienten Betrieb eines Security Operating Center (SOC) ab**



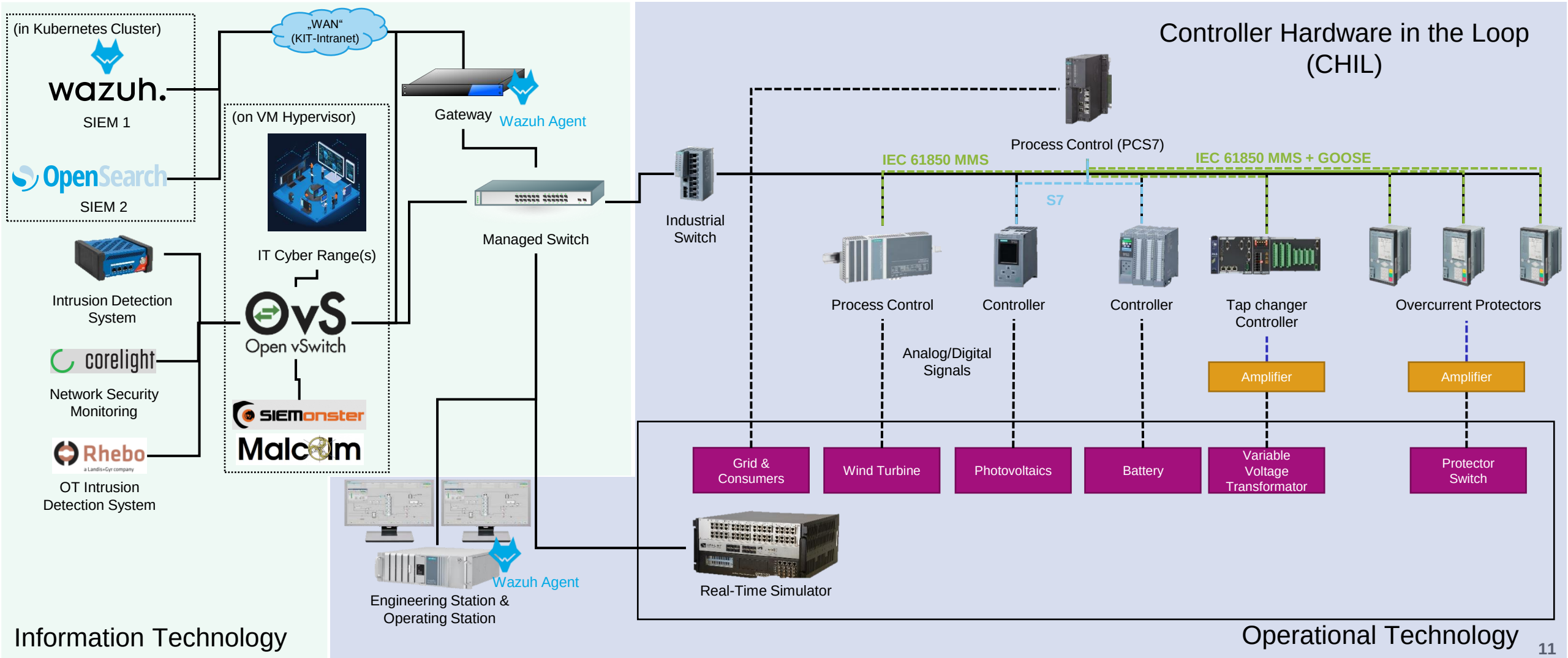
basiert auf [RR23]

Herausforderungen

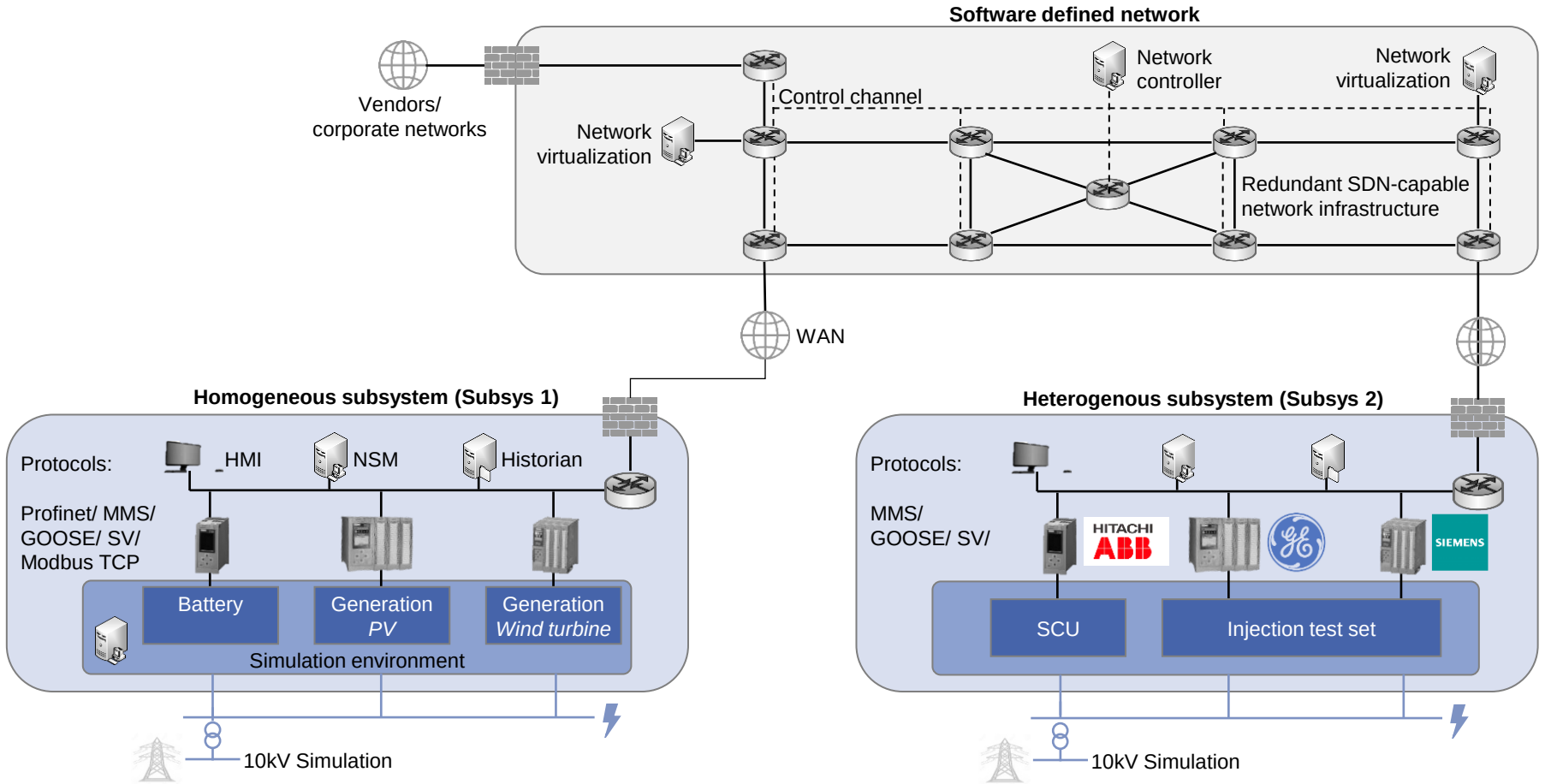
- **Ressourcen**
  - Kann Cyber-Resilienz effizient sein?
    - Zusätzlicher Aufwand/Kosten vs. Risiko/Schadenspotential
- **Sichtbarkeit**
  - Eingeschränkte Quellen für die Sammlung der relevanten Ereignisse zur Erkennung / Nachvollziehung von Cyberangriffen
- **Bandbreite**
  - Kommunikationsgeschwindigkeit in hochverteilten Systemen erlaubt keine feingranulare Aufzeichnung aller Netzwerkdaten bzw. Systemereignisse
- **Aufbau und Betrieb**
  - Security by Design!
  - Aufbau erfordert Anpassung an spezifische IT und OT-Systeme
- **Adaption auf unbekannte Angriffe**
- **Faktor Mensch**
  - „Social Engineering“
  - Bewusstsein der Unternehmensmitarbeiter für Sicherheit und Sicherheitsrisiken

Forschungsprojekte

Forschungsanlagen zur Emulation von Cyberangriffsketten
Security Lab Energy im Energy Lab 2.0

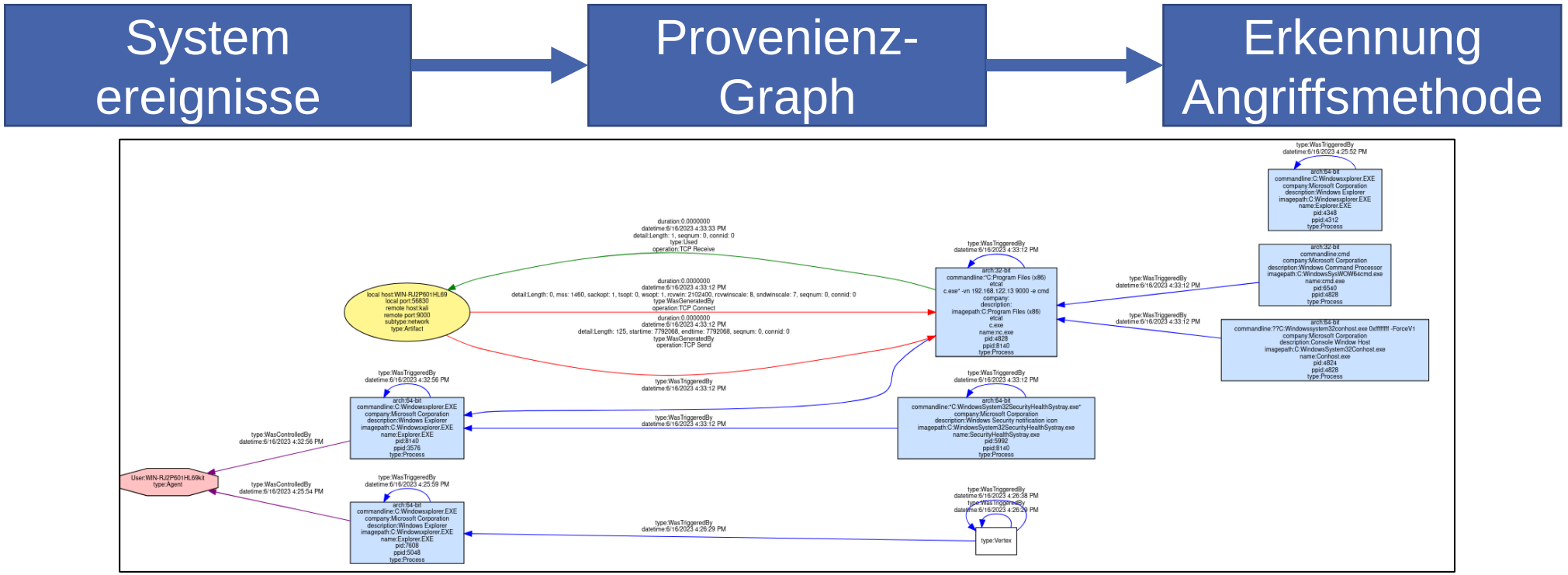


Forschungsanlagen zur Emulation von Cyberangriffsketten
KASTEL Security Lab Energy



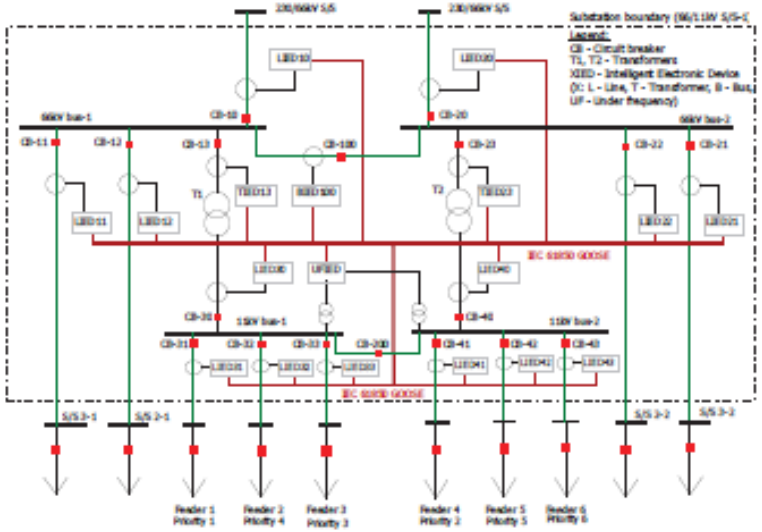
Erkennung von Angriffsschritte aus Provenienz von Systemereignissen

- **Einzelne Systemereignisse haben begrenzte Aussagekraft bzgl. Angriffsvorgehen und Methoden**
- **Nur im Kontext der Systemereignisse (Provenienz) sind Rückschlüsse auf Kritikalität und Angriffskette möglich**



Beispiel eines Provenienzgraphen bestehend aus Systemereignissen

Anomaliebasierte Angriffserkennung



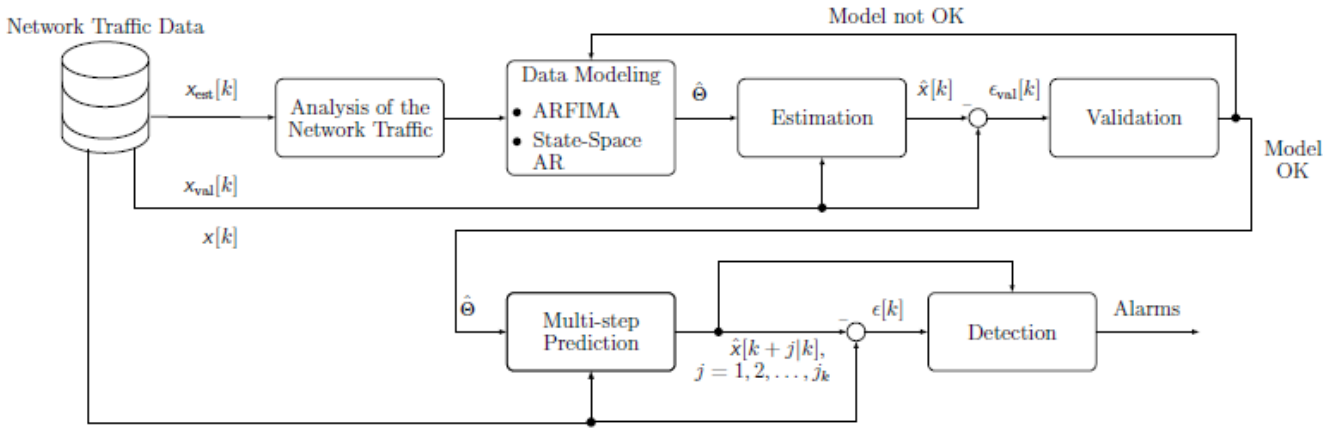
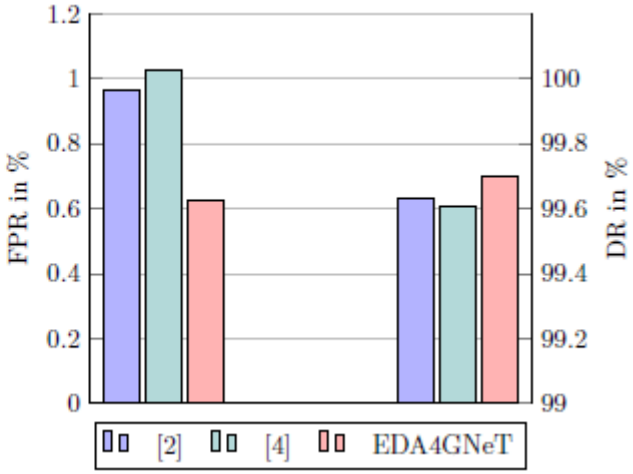


Fig 11. The single-line diagram of a 66/11 kV substation [10]

Change	Earliness of Detection*			Basic					
				FPR [%]			FNR [%]		
	[2]	[4]	EDA4GNeT	[2]	[4]	EDA4GNeT	[2]	[4]	EDA4GNeT
1	–	–	−29.51	0.7810	2.4796	0.4430	0.2983	0.9471	0.1692
2	–	–	−30.24	1.3017	1.5143	1.0970	0.4972	0.5784	0.4190
3	–	–	−30.88	1.5130	1.9984	0.9752	0.5779	0.7633	0.3725
4	–	–	−30.52	0.7917	0.7029	0.7072	0.3024	0.2685	0.2701
5	–	–	−30.43	0.9635	1.0282	0.6253	0.3680	0.3927	0.2389
6	–	–	−29.97	0.9886	0.7047	0.4576	0.3776	0.2692	0.1748

Comparison of the detection results of EDA4GNeT with available methods



[Elbez23]

Forschungsbedarf

- **Labore für die Emulation von Cyberangriffen sowie deren Verteidigung**
- **Datensätze für realistische, mehrschrittige Angriffsketten über komplexe Netzwerke und mehreren Endpunkten**
- **Schließen der Lücke zwischen Wissenschaft und Praxis**
  - Kommerzielle Angriffserkennungssysteme vs. Forschungslösungen
- **Verständnis Use Cases / Anwendungsdomänen vs. Verständnis Informationstechnologie**
  → interdisziplinärer Wissenstransfer

Zusammenfassung

- **Energiewende und Digitalisierung des Energienetzes erfordert Cyber-Resilienz**
- **Cyber-Resilienz ist der Umgang mit unvermeidlichen Lücken im System**
- **Ein Cyberphysikalisches System besteht aus technischen, organisatorischen und menschlichen Elementen**
- **Nachbildung dieses komplexen Systems für die Wissenschaft ist eine Herausforderung**
- **Schließung der Lücke zwischen Wissenschaft und Praxis ist nur so möglich**
- **Erforderlichkeit von interdisziplinärer Forschung**

Referenzen

Paper & Internet-Quellen

[Elbez23] Elbez, Ghada, Klara Nahrstedt, and Veit Hagenmeyer. "Early Attack Detection for Securing GOOSE Network Traffic." IEEE Transactions on Smart Grid (2023). https://doi.org/10.1109/TSG.2023.3272749

[GM23] Google, & Mandiant. (2023). *Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape*. https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf

[EX22] Exabeam. SIEM Architecture: Technology, Process and Data. https://www.exabeam.com/explainers/siem/siem-architecture/. Stand 2022-05-23

[RR23] Richard Rudolph. *Cyber Incident Detection and Response*. Februar 2023.

[MITRE] MITRE ATT&CK Framework. https://attack.mitre.org

Gesetze

[BSI KritisV] Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV) https://www.gesetze-im-internet.de/bsi-kritisv/index.html

[BSI IT-SIG 2.0] Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0) https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s1122.pdf

[EU NIS] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016L1148

[EU NIS2] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (Text von Bedeutung für den EWR) https://eur-lex.europa.eu/eli/dir/2022/2555

[EU RCE] Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates (Text von Bedeutung für den EWR) https://eur-lex.europa.eu/eli/dir/2022/2557/oj

Normen

[NIST SP 800-160] National Institute of Standards and Technology (2021), Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, NIST Special Publication 800-160, Volume 2, Revision 1, https://doi.org/10.6028/NIST.SP.800-160v2r1

[ISO 27001] ISO/IEC 27001: Information security management systems. International Organization for Standardization, Geneva, Switzerland. https://www.iso.org/standard/27001

[IEC 62443] IEC 62443: Industrial communication networks - Network and system security. International Electrotechnical Commission, Geneva, Switzerland. https://webstore.iec.ch/searchform&q=IEC%2062443

[IEC 62351] IEC 62351: Power systems management and associated information exchange - Data and communications security. International Electrotechnical Commission, Geneva, Switzerland. https://webstore.iec.ch/publication/6912

[ISO 22301] ISO/IEC 22391: Security and resilience — Business continuity management systems. International Organization for Standardization, Geneva, Switzerland. https://www.iso.org/standard/75106.html