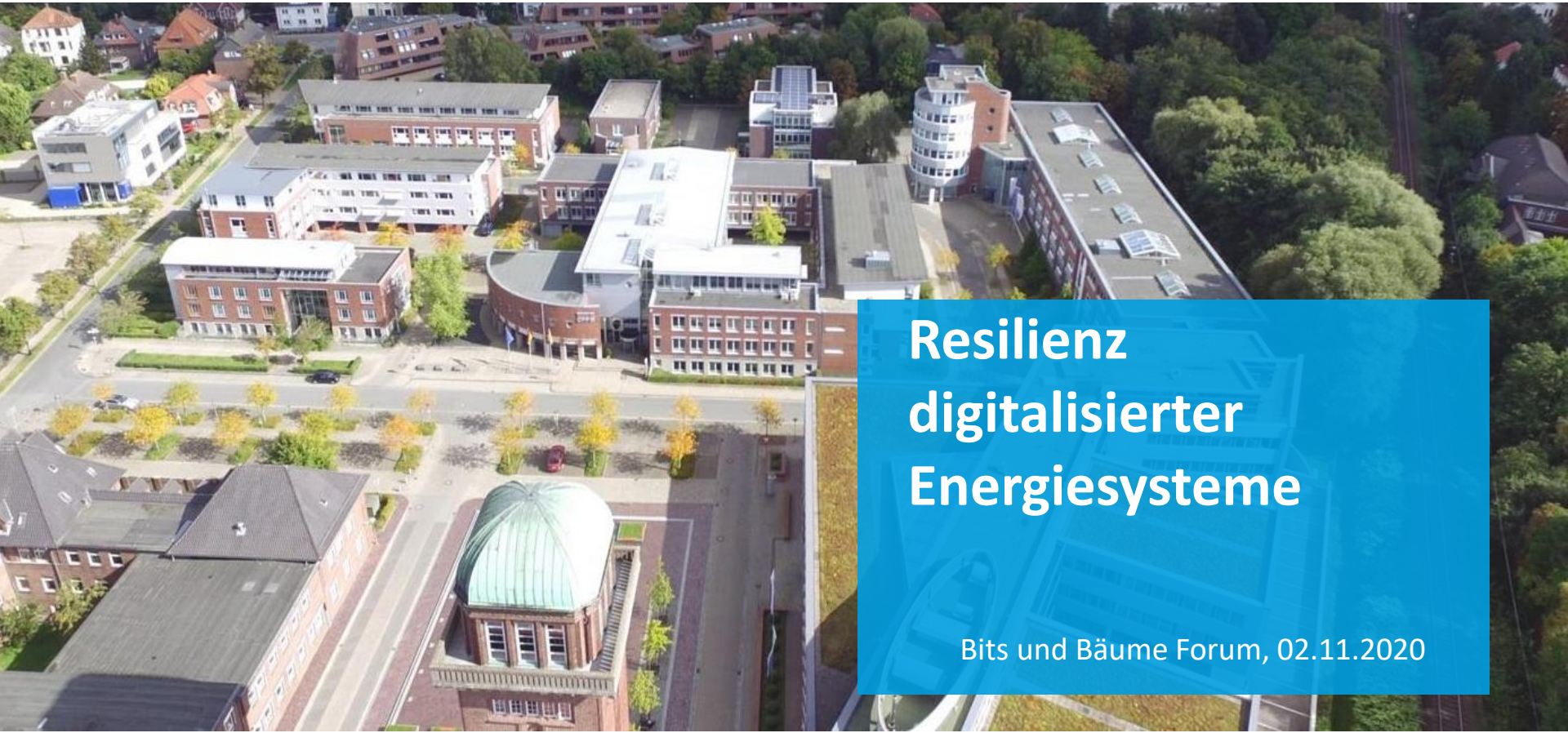


Resilienz digitalisierter Energiesysteme

Bits und Bäume Forum, 02.11.2020

Eine neue Risikostruktur in der Energieversorgung…

- führt zu anderen Vulnerabilitäten

Änderungen in Erzeugung und Verbrauch, z.B.

- deutlich mehr Leistungseinheiten jenseits der Versorger
- neue Akteure (z.B. Aggregatoren)

IKT-basierte Bedrohungen

- ausgereifte Wertschöpfungsketten für Cyber-Kriminalität
- staatlich organisierte und bezahlte Hacker (z.B. „Staatstrojaner

Digitalisierung der Lebenswelten

- Soziale Netzwerke
- Internet of Things
- Künstliche Intelligenz
- Konvergenz von Prozess-IKT und übriger (Internet-verbundener) IKT

Neue Ungewissheiten

- Politik-bedingte Entwicklungspfade und Pfadänderungen
- Unklare Ursache-Wirkung-Zusammenhänge im Netzbetrieb

Frage an Sie:

Wird die Energieversorgung durch die Digitalisierung sicherer? Oder unsicherer?

Wenn Sie an die Versorgungssicherheit denken:

Überwiegen die positiven Aspekte der Digitalisierung oder die negativen?

Bitte in den Chat schreiben

Folgen von großen Stromausfällen (Blackouts)

In den ersten Stunden

- Ausfall der Mobilfunkverbindung
- Verkehrsunfälle

Nach einem Tag

- massive Einschränkung der medizinischen Versorgung
- lokale Ernährungsengpässe
- Tiersterben in der Landwirtschaft

Nach einigen Tagen

- Störungen der öffentlichen Ordnung, Unruhen
- Große Einschränkungen medizinischer Versorgung
- Zunahme der Kriminalität
- nachhaltige Störung des Vertrauens der Gesellschaft in den Staat und sich selbst als soziale Gemeinschaft

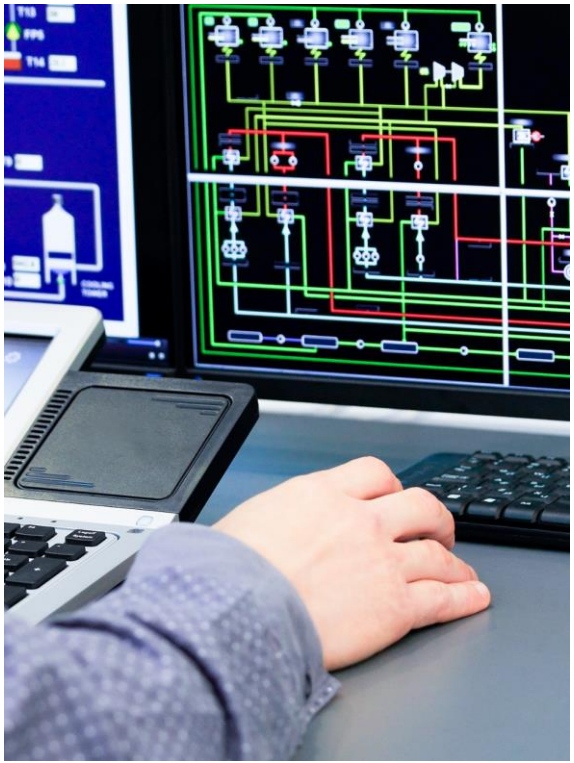
Risikobasierte Absicherung und Resilienz

Heute: Schwerpunkt auf Robustheit

- Aufgabe der Systemsicherung: Schutz gegen Ausfall großer Komponenten („N-1 Sicherheit“
- basiert auf theorie-und erfahrungsbasierter Risikoabschätzung (Abschätzung der Wahrscheinlichkeit gravierender Störereignisse)
- Ziel: auch gravierende Ereignisse verursachen keinen Blackout
- Mechanismen: Zentralisierung, strikte Regeln, Kontrolle

Morgen: Ergänzung um Resilienz

- teilweise große Ungewissheiten und unbekannte Wahrscheinlichkeit
- Ziel: Störereignisse unbeschadet abzufangen **oder zumindest** in kurzer Zeit mit möglichst geringem Schaden und vertretbaren Kosten wieder in den normalen Betriebszustand zurückzukehren
- Mechanismen: dezentrale Selbstorganisation, (trainierte) Spontaneität, Adaptivität



Mögliche Maßnahmen

Beispiele

Verankern von Abwehrmaßnahmen auf dezentraler Ebene

- Security-by-Design aus Systemsicht
- intelligente und lernende Algorithmen in vernetzten energietechnischen Komponenten reagieren autonom auf bedrohliche „Anomalien“

Ermöglichen dezentralen Inselbetriebs bei Blackouts

- technische Voraussetzungen schaffen
  - Digitalisierung
  - Erzeugungsstruktur
- regulatorisch gestalten
  - Anreize
  - Normen und Standards
- Akzeptabilität sichern
  - priorisierte Verbraucher
  - Teilnahme