



Leopoldina
Nationale Akademie
der Wissenschaften



Resilienz digitalisierter Energiesysteme – Wie können Blackout-Risiken begrenzt werden?

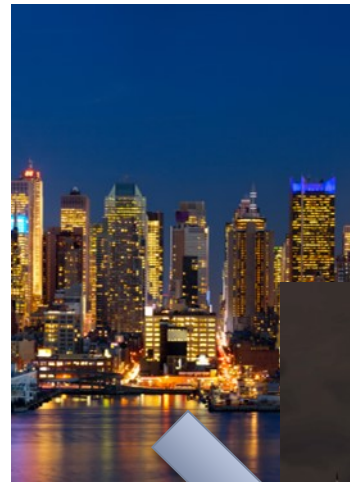
Christoph Mayer (OFFIS), Gert Brunekreeft (Jacobs University Bremen)

05.02.2021 Ergebnispräsentation

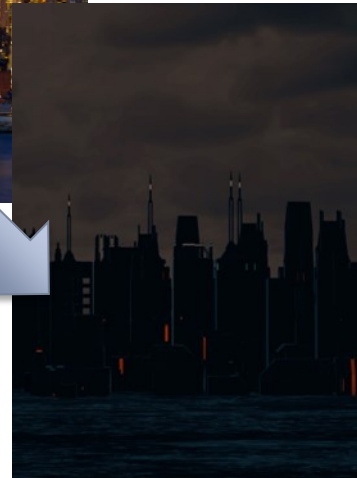
www.energiesysteme-zukunft.de

Wie könnte es zukünftig zu Blackouts kommen?

- Möglicher Verlauf
 - erfolgreicher Cyber-Angriff auf eine Plattform, die eine große Anzahl kleiner Anlagen (z.B. Elektrofahrzeuge) ansteuern können
 - Anlagen werden gezielt gleichzeitig an- und abgeschaltet.
 - Es kommt zum großflächigen Blackout.
- Folgen eines Blackouts:
 - bereits nach Stunden **massive Einschränkungen**
 - nach einigen Tagen **Störungen der öffentlichen Ordnung** und des **Vertrauens in Gesellschaft und Staat**



© AdobeStock/Oleksandr Dibrova



© AdobeStock/Jacqueline Weber

Wie verändern Digitalisierung und Energiewende langfristig* das Risiko für große Blackouts?

- Heute: weltweit eine der **sichersten Stromversorgungen**
- Herausforderungen durch **Wandel der Energieversorgung** und **zunehmende Digitalisierung**, u.a.
 - Erzeugung und Verbrauch mit aktiven dezentralen Komponenten
 - Volatilere Energiemärkte
 - Internet of Things, künstliche Intelligenz
 - Neue Akteure und veränderte Rolle von Privatakteuren
 - politischer Rahmen und Wertewandel

→ **mehr Unsicherheit und unerwartete Ereignisse**

*innerhalb der nächsten zwei Dekaden



Wesentliche Ursachen für mögliche neue Bedrohungen

1. Die Vielzahl an **kleinen, aktiv steuerbaren Erzeugungs- und Verbrauchsanlagen** ist durch die Möglichkeit von simultanem Verhalten, welches durch Digitalisierung induziert wird, systemrelevant.
2. **Fehlverhalten der IKT** kann **massiven Auswirkungen** haben. Softwarefehler, Bedienungsfehler oder Cyberterrorismus stellen ein wachsendes Risiko dar.
3. Die technische **Systemkomplexität** erschwert die **Vorhersage** im operativen Betrieb der Netzbetreiber.
4. Ungewissheiten über **zukünftige Entwicklungen** erschweren ein **optimales Systemdesign**.



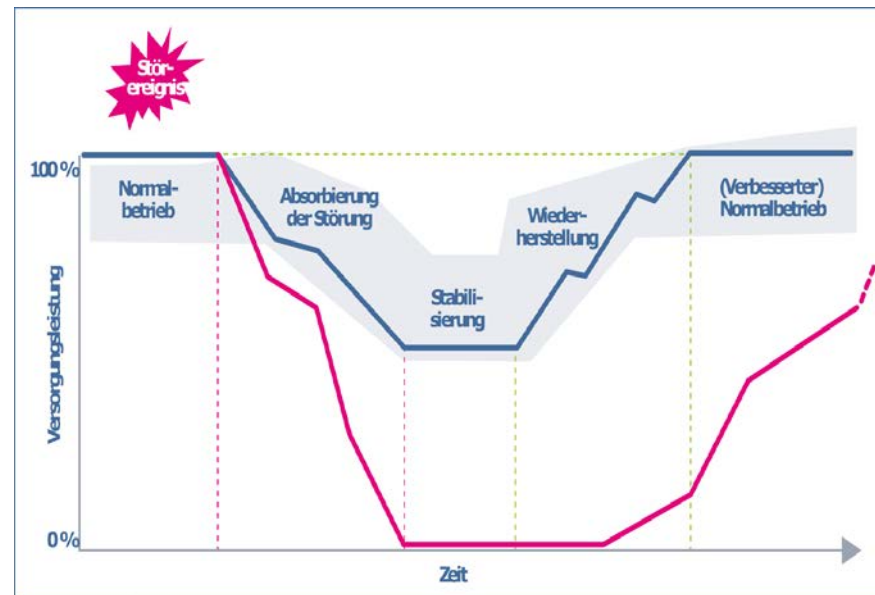
„Resilienz“ zur Absicherung gegen neue Bedrohungen

• Robustheit

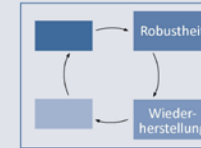
- Risikobetrachtung (Abschätzung der Wahrscheinlichkeit gravierender Störereignisse)
- „Härten“ der Stromversorgung gegen diese Ereignisse

• Resilienz

- Vorbereit sein auf **Unsicherheit und Überraschungen**
- Störereignisse **unbeschadet abfangen** oder
- in kurzer Zeit mit möglichst geringem Schaden und vertretbaren Kosten wieder **in den normalen Betriebszustand zurückkehren**



Handlungsoption 7: Regelwerk für Resilienz durch dezentrale Strukturen erarbeiten lassen



Ergebnis: Einzelne Netzabschnitte sind **inselbetriebsfähig** und können so einen Blackout überbrücken. Kritische Verbraucher werden bevorzugt mit Strom versorgt.



Dringlichkeit: ● ●

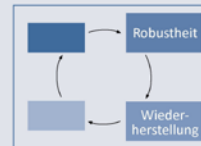
Wirksamkeit: ● ● ●



Was kann man heute tun?

- Forschungs- und Entwicklungsprojekte zur Ausgestaltung und anschließende Feldtests durchführen.

Handlungsoption 8: Standardisierung zur Vermeidung problematischen simultanen Verhaltens initiieren



Ergebnis: Gerätestandards verringern die Wahrscheinlichkeit von stabilitätsgefährdenden Gleichzeitigkeiten und **simultanen Verhaltens**

Dringlichkeit: ● ● ●

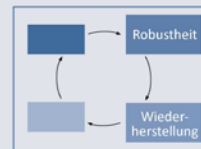
Wirksamkeit: ● ●



Was kann man heute tun?

- Eine Richtlinie für Patchability erarbeiten, verabschieden und einführen.
- Analysen und Forschung für die Plausibilisierung von Schaltbefehlen anhand lokaler physikalischer Größen durchführen.

Handlungsoption 9: Systemstabilisierung durch dezentrale Anlagen ausbauen



Ergebnis: Dezentrale Anlagen leisten einen wesentlichen Beitrag zur Stabilität des elektrischen Energiesystems.

Dringlichkeit: ● ●

Wirksamkeit: ● ● ●



Was kann man heute tun?

- Maßnahmen zur Herstellung der notwendigen kommunikationstechnischen Anbindung erarbeiten und dabei relevante Akteure wie Netzbetreiber, Anlagenbetreiber oder Telekommunikationsunternehmen einbeziehen.
- Zum Einsatz von künstlicher Intelligenz forschen, um auch auf komplexe und unbekannte Störereignisse oder Angriffe angemessen reagieren zu können.

Handlungsoption 10: Eine Resilienzkomponente in die Anreizregulierung integrieren



Ergebnis: Die ARegV enthält Anreize für die Netzbetreiber, effektive resilienzverbessernde Maßnahmen durchzuführen.



Dringlichkeit: ● ●

Wirksamkeit: ● ●



Was kann man heute tun?

- Eine R-Komponente in die ARegV als zusätzliche Regelung zur Verbesserung der Resilienz einführen.

Handlungsoption 11: Resilienzverbessernde Netzentgelte und Anschlussgebühren einführen



Ergebnis: Durch eine Novellierung der StromNEV wird es den Netzbetreibern ermöglicht, Netznutzungsentgelte effektiv resilienzverbessernd anzupassen.



Dringlichkeit: ● ●

Wirksamkeit: ● ●



Was kann man heute tun?

- **Smart Connection Agreements** um eine Resilienzbetrachtung erweitern, sodass resilienzverbessernde Standortentscheidungen und Vermeidung von Gleichzeitigkeiten belohnt werden.

Fazit

- Veränderungen und Unsicherheiten verlangen politisches Handeln, um Blackouts auch in Zukunft zu vermeiden.
- Wesentliche Trends und Risiken stammen nicht aus der Energiewirtschaft.
- Risikobewertungen müssen um Resilienzbewertungen ergänzt werden.
- Ohne massive Digitalisierung sind weder Resilienz noch Effizienz zu erreichen.
- Neue Akteure (auch außerhalb der elektrischen Energieversorgung) müssen in den Blick rücken.





Leopoldina
Nationale Akademie
der Wissenschaften



Kontakt

Koordinierungsstelle Energiesysteme der Zukunft

Dr. Berit Erlach
Wissenschaftliche Referentin

Pariser Platz 4a
10117 Berlin
erlach@acatech.de
www.energiesysteme-zukunft.de



OFFIS - Institut für Informatik

Dr. Christoph Mayer
Bereichsleiter Energie

Escherweg 2
26131 Oldenburg
mayer@offis.de
www.offis.de

Nationale Akademie der Wissenschaften Leopoldina
acatech – Deutsche Akademie der Technikwissenschaften
Union der deutschen Akademien der Wissenschaften