Leopoldina
Nationale Akademie
der Wissenschaften

acatech
DEUTSCHE AKADEMIE DER
TECHNIKWISSENSCHAFTEN

UNION
DER DEUTSCHEN AKADEMIEN
DER WISSENSCHAFTEN

Februar 2021
Kurzfassung der Stellungnahme

Resilienz digitalisierter Energiesysteme

Wie können Blackout-Risiken begrenzt werden?

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

Durch die Energiewende und die zunehmende Digitalisierung werden in den nächsten zwei Jahrzehnten neue Risiken für die Stromversorgung entstehen. Um diese Risiken beherrschbar zu machen und Blackouts mitsamt ihren Folgeschäden für die Gesellschaft zuverlässig zu verhindern, ist eine Resilienzstrategie erforderlich. Die Arbeitsgruppe „Resilienz digitalisierter Energiesysteme“ des Akademienprojekts „Energiesysteme der Zukunft“ identifiziert dafür folgende Eckpfeiler:

- Die **Digitalisierung** bietet die Chance, dezentrale Erzeugungsstrukturen, Elektromobilität und neu auftretende Marktakteure effizient und sicher ins Energiesystem zu integrieren. Sie muss daher **aktiv gestaltet** und gefördert werden.
- **Kleine Akteure** der Energieversorgung, **Akteure außerhalb der Stromversorgung** (Gerätehersteller, Plattformbetreiber, Betreiber von öffentlichen Kommunikationsnetzen) und **Haushalte** haben zunehmend Einfluss auf die Sicherheit der Stromversorgung. Sie müssen daher stärker in die Resilienzsicherung einbezogen werden.
- Neue Angriffsflächen für Cyberkriminelle und Abhängigkeiten zwischen Strom- und IKT-System können zu **unvorhergesehenen oder sogar unvorhersehbaren Ereignissen** mit großem Bedrohungspotenzial führen. Die Netzbetreiber müssen mit diesen Risiken umgehen können.
- Die Politik sollte versuchen, zukünftige Entwicklungen rechtzeitig zu antizipieren und die hier geforderte Resilienzstrategie fortlaufend anpassen. Dafür ist ein **konsequentes Monitoring** erforderlich.

Digitalisierung und wachsende Komplexität führen zu neuen Bedrohungen

Eine zuverlässige Stromversorgung ist für eine moderne Industriegesellschaft unverzichtbar. Große Blackouts **– lang anhaltende und flächendeckende Stromausfälle** – würden in kürzester Zeit andere kritische Infrastrukturen wie Transportsysteme, Wasserversorgung und -entsorgung, Gesundheitswesen oder Informations- und Kommunikationssysteme empfindlich stören oder gar zusammenbrechen lassen.

Durch die Energiewende wird das Energiesystem komplexer: Immer mehr elektrische Energie wird wetter-, jahres- und tageszeitabhängig von Windenergie- und Solaranlagen bereitgestellt. Strom wird zunehmend auch für Elektrofahrzeuge und Wärmepumpen benötigt. Privatpersonen erzeugen Strom mit der eigenen Solaranlage, und neue Marktakteure mit neuen Geschäftsmodellen treten neben die klassischen Energieversorger. Großkraftwerke, die bisher für die Stabilisierung der Stromversorgung zuständig waren, gehen außer Betrieb.

Parallel dazu schreitet die **Digitalisierung** rasant voran. Es kommt zu einer starken Vernetzung, einer zunehmenden Automatisierung und dem Einsatz digitaler Technologien – nicht nur im Strombereich. Über das sogenannte **Internet der Dinge** werden viele Milliarden Geräte vernetzt – von Beleuchtung über Kühlschränke bis hin zu Industrieanlagen. Da diese Geräte auch an das Stromnetz angeschlossen sind, können sie in ihrer Summe die Stabilität der Stromversorgung beeinflussen.

Die **zunehmende Verknüpfung zwischen Stromversorgung und IKT** ist notwendiger Bestandteil einer sowohl zuverlässigen als auch ökonomisch effizienten Energieversorgung: **ohne Digitalisierung keine Energiewende**. Andererseits entstehen durch die zunehmende Komplexität in der Stromversorgung **neue Blackout-Risiken:**

1. Werden **viele kleine Erzeugungs- und Verbrauchsanlagen** gewollt oder zufällig gleichzeitig an- oder abgeschaltet, kann dies die Stromversorgung destabilisieren.
2. Die Stromversorgung wird anfälliger für **Fehlverhalten der IKT.** Besonders problematisch ist dabei, dass ein Teil der eingesetzten IKT im Fehlerfall nicht abgeschaltet werden kann, ohne die Stromversorgung empfindlich zu gefährden.
3. Die komplexen Abhängigkeiten zwischen dezentraler Erzeugung, Marktgeschehen und Änderungen im Verbrauch machen das Systemverhalten **schwerer vorhersehbar** und können zu **neuartigen komplexen Störfallabläufen** führen.
4. **Ungewissheit über zukünftige Entwicklungen erschwert ein optimales Systemdesign.** Eine zusätzliche Herausforderung stellt dabei die hohe Innovationsgeschwindigkeit im IKT-Bereich dar, die sich mit jahrzehntelangen Investitionszyklen in der Stromversorgung nur schwer verträgt.

Unvorhergesehene und unvorhersehbare Risiken erfordern eine Resilienzstrategie

Durch die Veränderungen im Energiesystem und den stärkeren Einfluss der Digitalisierung steigt die Unsicherheit über zukünftige Entwicklungen. Damit sind Wahrscheinlichkeiten für bekannte oder erwartete Ereignisse (wie zum Beispiel Hacker-Angriffe) nicht mehr einfach bestimmbar. Die klassische Risikoanalyse, die auf diesem Prinzip beruht und auf deren Basis das System robust gestaltet wird, ist nicht mehr ausreichend. Zudem müssen sich die für die Systemsicherheit verantwortlichen Netzbetreiber zukünftig auf deutlich mehr Unsicherheit und Überraschungen einstellen. Daher wird es zunehmend wichtig, dass sie auch **auf unvorhergesehene und sogar unvorhersehbare Ereignisse reagieren,** diese beherrschen und auch im Falle eines Blackouts schnell wieder zum Normalbetrieb des Systems zurückkehren. Für solche Situationen hat sich das **Konzept der Resilienz** bewährt. Resilienz bedeutet, die Auswirkungen eines Störereignisses abzufangen – im schlimmsten Fall je nach Konstellation auch mit kurzzeitig abnehmender Versorgungsqualität –, ohne dass das System kollabiert, um anschließend zügig wieder in den normalen Betriebszustand zurückzukehren (siehe Abbildung 1).

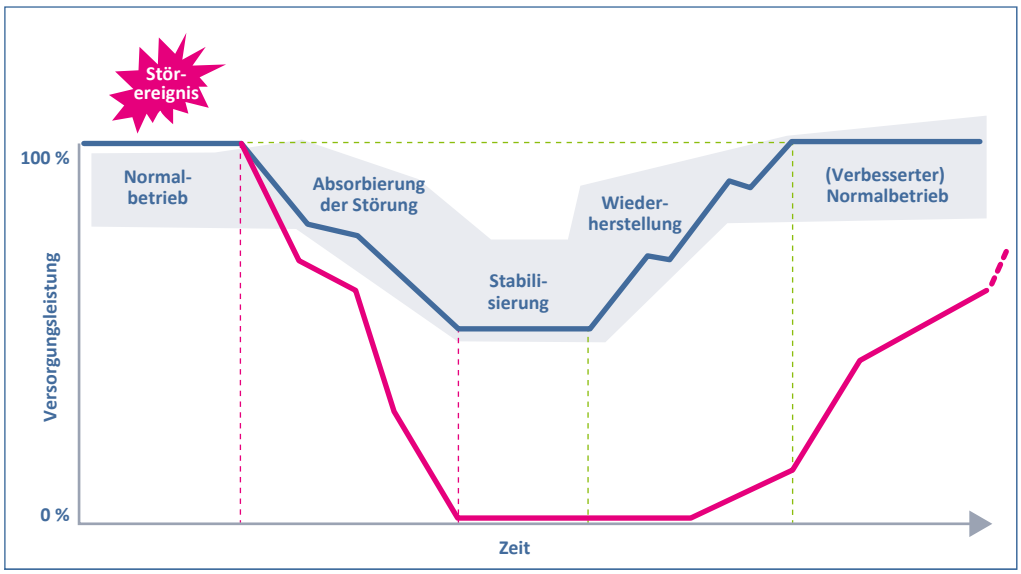

Abbildung 1: Wiederherstellung der Funktionsfähigkeit eines Systems: „die geeignete Reaktion auf ein Ereignis (Absorbieren der Störung), das Zurückfallen auf kritische Funktionen und Stabilisierung des Systems (Stabilisierung) und zuletzt das kontrollierte Zurückbringen zum Normalbetrieb des Systems (Wiederherstellung)."[1]

Eine **Resilienzstrategie** erfordert ein Portfolio an Maßnahmen – von der möglichst weitgehenden Identifikation von Schwachstellen und Risiken über Maßnahmen zur Unterstützung der Robustheit und Widerstands- und Anpassungsfähigkeit bis hin zu lernenden und das System verbessernden Maßnahmen einschließlich einer kosteneffizienten Notfallplanung.

Die Arbeitsgruppe hat **15 Handlungsoptionen** identifiziert (siehe nächste Seite), die als Bausteine einer Resilienzstrategie gegen große Blackouts dienen können. Diese Handlungsoptionen wurden so gewählt, dass sie den bereits **heute gegebenen Handlungsbedarf** adressieren, um die neu entstehenden Risiken **in einem langfristigen Zeithorizont bis 2040** abzufangen. Nur wenn die Resilienzstrategie mit der rasant voranschreitenden Energiewende und der Digitalisierung Schritt hält, können die Potenziale für eine effiziente, sichere und nachhaltige Energieversorgung bestmöglich genutzt und die Blackout-Risiken in einer digitalisierten Welt beherrscht werden.

1 Babazadeh, D./Mayer, C./Lehnhoff, S.: „Cyber-Resilienz". In: *bulletin.ch*, 5, 2018, S. 32–34.

Wie können Blackout-Risiken begrenzt werden?

Als Bausteine einer umfassenden Resilienzstrategie für das digitalisierte Energiesystem bieten sich die folgenden Maßnahmen an:

Handlungsfeld:
Wechselwirkung IKT und Energie verstehen und lenken

Die elektrische Energieversorgung wird zukünftig stärker von IKT-Systemen abhängig sein.
Die Gefahr, dass Störungen der IKT-Systeme zu Blackouts führen, ist zu vermeiden.

- **HO 1. Abhängigkeiten zwischen Stromversorgung und Kommunikationsnetzen analysieren lassen,** um das Risiko kaskadierender Ausfälle zu minimieren.
- **HO 2. Regeln für resiliente Kommunikationsnetze schaffen,** durch Vorgaben zu größerer Redundanz und Schwarzfallfestigkeit.
- **HO 3. Akteure zu einer integrierten Betriebsführung der IKT-Systeme und elektrischen Netze hinleiten** mit dem Ziel der Integration der IKT-Überwachung in die Netzleittechnik und der Erstellung eines integrierten Lagebilds.

Handlungsfeld:
Cyber-Sicherheit systemisch entwickeln

Die Anforderungen an die Cyber-Sicherheit müssen bei allen Akteuren auf ein ausreichend hohes Niveau gebracht werden. Dies erfordert sowohl technisch als auch organisatorisch
neue Lösungen.

- **HO 4. Cyber-Sicherheitsstandards für alle Blackout-relevanten Akteure einführen,** unter anderem für kleine Netzbetreiber, branchenfremde Akteure und Geräte „hinter dem Zähler".
- **HO 5. Maßnahmen zum Umgang mit Sicherheitslücken definieren,** um Vulnerabilitäten aufgrund menschlichen Versagens im Sicherheitsmanagement, aufgrund von Softwarefehlern oder staatlich gewollten Hintertüren zu begegnen.

Handlungsfeld:
Technische Resilienz durch Netzbetreiber und Netznutzer stärken

Insbesondere in den Verteilnetzen wird die Netzführung zukünftig anspruchsvoller. Sowohl kleine Netzbetreiber als auch Betreiber kleiner Erzeugungsanlagen müssen deutlich mehr als heute üblich zur Resilienz beitragen.

- **HO 6. Digitalisierung der Stromnetze voranbringen,** durch entsprechende technische Ausstattung auch kleiner Netzbetreiber.
- **HO 7. Regelwerk für Resilienz durch dezentrale Strukturen erarbeiten lassen.** Sind einzelne Netzabschnitte inselbetriebsfähig, können sie im Falle eines Blackouts temporär die lokale Versorgung aufrechterhalten und beim Wiederaufbau der Versorgung helfen.

Handlungsfeld: **IKT-Integration kleiner Anlagen netzdienlich gestalten** 
Der Großteil der Anlagen und Kleingeräte wird zukünftig mit dem Internet verbunden sein und sich darüber digital steuern lassen. Unerwünschtes simultanes Verhalten – etwa hohe Leistungsspitzen durch Gleichzeitigkeiten – kann die Stabilität des elektrischen Energiesystems gefährden und muss vermieden werden. Auf der anderen Seite können diese Anlagen auch genutzt werden, um das Energiesystem aktiv zu stabilisieren. • **HO 8. Standardisierung zur Vermeidung problematischen simultanen Verhaltens initiieren,** zum Beispiel durch Mindeststandards zur „Patchability" von Erzeugungsanlagen und Geräten. So kann die Software von Geräten im laufenden Betrieb an neue Anforderungen angepasst werden. • **HO 9. Systemstabilisierung durch dezentrale Anlagen ausbauen** und die dafür erforderliche kommunikationstechnische Anbindung voranbringen.
Handlungsfeld: **Anreize für Netzbetreiber zur Steigerung der Resilienz stärken** 
Es fehlen weitgehend effektive und effiziente Anreize für die Netzbetreiber und Marktparteien, sich resilienzverbessernd zu verhalten. Dazu sollten marktliche Anreize geschaffen werden. • **HO 10. Eine Resilienzkomponente in die Anreizregulierung integrieren,** damit Netzbetreiber in Resilienzmaßnahmen investieren. • **HO 11. Resilienzverbessernde Netzentgelte und Anschlussgebühren einführen,** um die Standortwahl und die Betriebsweise für Erneuerbare-Energie-Anlagen zu beeinflussen.
Handlungsfeld: **Beteiligung von Privatakteuren bei der Gestaltung und Umsetzung von Resilienz sicherstellen** 
Zur Systemstützung kann auch die Steuerung von Anlagen aufseiten privater Akteure notwendig werden. Zur Ausgestaltung sollte ein Stakeholder-Gremium geschaffen werden, das Lösungen entwickelt, die für verschiedene Nutzergruppen wählbar sind und Fragen der Akzeptabilität berücksichtigen. • **HO 12. Ein Stakeholder-Gremium zur Berücksichtigung der Belange von Privatakteuren entwickeln** und alle relevanten Akteure in die Entscheidungsfindung für neue Regelungen einbeziehen. • **HO 13. Bewusstsein für den Einfluss privater Akteure schaffen,** durch Informations- und Bildungskampagnen.
Handlungsfeld: **Langfristige Risiko- und Resilienzbewertung institutionalisieren** 
Es wird zukünftig unvorhersehbare Trends geben, die etwa aus der Digitalisierung und der Energiewende entstehen und die Gefahr von Blackouts erhöhen könnten. Es sollte ein geeigneter Organisationsrahmen geschaffen werden, der es ermöglicht, flexibel auf solche Trends zu reagieren und mit ihnen umzugehen. • **HO 14. Organisationsrahmen für die Meldung von Störfällen und die Resilienzbewertung schaffen** und geeignete Kenngrößen für Resilienz entwickeln. • **HO 15. Einen übergeordneten Begleitprozess ins Leben rufen,** um die Resilienzstrategie regelmäßig zu evaluieren.

Tabelle 1: Übersicht über Handlungsfelder und Handlungsoptionen (HO)

Nur wenn zukünftig alle relevanten Akteure ihren Teil zur Resilienz beitragen, wird es gelingen, die gewohnt hohe Zuverlässigkeit der Stromversorgung aufrechtzuerhalten. Durch eine geeignete Resilienzstrategie kann die Politik hierfür den Rahmen setzen.

Das Akademienprojekt „Energiesysteme der Zukunft“

Die Stellungnahme „Resilienz digitalisierter Energiesysteme. Wie können Blackout-Risiken begrenzt werden? “ ist im Rahmen des Akademienprojekts „Energiesysteme der Zukunft“ entstanden. In interdisziplinären Arbeitsgruppen erarbeiten rund 100 Expertinnen und Experten Handlungsoptionen für den Weg zu einer umweltverträglichen, sicheren und bezahlbaren Energieversorgung.

Mitglieder der Arbeitsgruppe „Resilienz digitalisierter Energiesysteme“

Mitglieder: Dr. Christoph Mayer (AG-Leiter, OFFIS), Prof. Dr. Gert Brunekreeft (AG-Leiter, Jacobs University Bremen), Dr. Marius Buchmann (Jacobs University), Mathias Dalheimer Fraunhofer ITWM, Dr. Volker Distelrath (Siemens AG), Prof. Dr. Bernd Hirschl (IÖW/ BTU), Prof. Dr. Jochen Kreusel (Hitachi ABB Power Grids), Prof. Dr. Wolfgang Kröger (ETH Zürich), Prof. Dr. Sebastian Lehnhoff (OFFIS), Dr. Till Luhmann (BTC AG), Prof. Dr. Jannika Mattes (Universität Oldenburg), Prof. Dr. Ellen Matthies (Universität Magdeburg), Dr. Philipp Werdelmann (Westnetz GmbH), Prof. Dr.-Ing. Christof Wittwer (Fraunhofer ISE)
Wissenschaftliche Referentinnen und Referenten: Dr. Achim Eberspächer (acatech), Dr. Berit Erlach (acatech), Katharina Bähr (acatech), Dr. Marita Blank-Babazadeh (OFFIS), Sanja Stark (OFFIS)

Kontakt:

Dr. Ulrich Glotzbach
Leiter der Koordinierungsstelle „Energiesysteme der Zukunft“
Pariser Platz 4a, 10117 Berlin
Tel.: +49 30 206 30 96 - 0 I E-Mail: glotzbach@acatech.de

Die Nationale Akademie der Wissenschaften Leopoldina, acatech – Deutsche Akademie der Technikwissenschaften und die Union der deutschen Akademien der Wissenschaften unterstützen Politik und Gesellschaft unabhängig und wissenschaftsbasiert bei der Beantwortung von Zukunftsfragen zu aktuellen Themen. Die Akademiemitglieder und weitere Experten sind hervorragende Wissenschaftlerinnen und Wissenschaftler aus dem In- und Ausland. In interdisziplinären Arbeitsgruppen erarbeiten sie Stellungnahmen, die nach externer Begutachtung vom Ständigen Ausschuss der Nationalen Akademie der Wissenschaften Leopoldina verabschiedet und anschließend in der *Schriftenreihe zur wissenschaftsbasierten Politikberatung* veröffentlicht werden.

Deutsche Akademie der Naturforscher Leopoldina e. V.
Nationale Akademie der Wissenschaften
Jägerberg 1
06108 Halle (Saale)
Tel.: 0345 47239-867
Fax: 0345 47239-839
E-Mail: politikberatung@leopoldina.org

Berliner Büro:
Reinhardtstraße 14
10117 Berlin

acatech – Deutsche Akademie der Technikwissenschaften e. V.
Geschäftsstelle München:
Karolinenplatz 4
80333 München
Tel.: 089 520309-0
Fax: 089 520309-9
E-Mail: info@acatech.de

Hauptstadtbüro:
Pariser Platz 4a
10117 Berlin

Union der deutschen Akademien der Wissenschaften e. V.
Geschwister-Scholl-Straße 2
55131 Mainz
Tel.: 06131 218528-10
Fax: 06131 218528-11
E-Mail: info@akademienunion.de

Berliner Büro:
Jägerstraße 22/23
10117 Berlin