Leopoldina
Nationale Akademie
der Wissenschaften

acatech
DEUTSCHE AKADEMIE DER
TECHNIKWISSENSCHAFTEN

UNION
DER DEUTSCHEN AKADEMIEN
DER WISSENSCHAFTEN

Januar 2023
Impuls

Sind Blackouts in Deutschland wahrscheinlich?

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

Impuls

Deutschland hat aktuell eine der sichersten Stromversorgungen weltweit. Größere Stromausfälle bis hin zu Blackouts sind unwahrscheinlich. Um das im Wandel begriffene Energiesystem auch in Zukunft mindestens so sicher wie heute gestalten zu können, gilt es jetzt zukunftsgerichtete Maßnahmen zu treffen. Dabei betonen Fachleute folgende Punkte:

- Nur die wenigsten Stromausfälle sind Blackouts. Hier genau zu differenzieren, ist wichtig, um eine realistische Einschätzung von Ereignissen und deren Folgen vornehmen zu können.
- Aktuell ist kein Blackout durch eine Energie-Unterversorgung zu befürchten, weil es starke und ausgereifte Sicherungsmechanismen gibt.
- Diese Mechanismen können zwar temporäre Unterbrechungen der Stromversorgung bedeuteten, betreffen jedoch zumeist nur industrielle Großverbraucher und bleiben daher ohne die bisweilen befürchteten katastrophalen Folgen für die Gesellschaft.
- Mit dem Fortschreiten der Energiewende wird die Energieversorgung dezentraler und zunehmend digitalisiert. Das bietet Chancen für die Sicherheit der Energieversorgung.
- Es können sich aber auch neue Risiken ergeben. Diese bereits jetzt anzugehen, ist notwendig für die zukünftige Versorgungssicherheit.

Inhalt

Sind Blackouts in Deutschland wahrscheinlich?

Kein Blackout sind …

- Stromausfälle, die nur ein kleines Gebiet betreffen oder von kürzerer Dauer sind (zum Beispiel durch Baustellen ausgelöst),
- kontrollierte Situationen, bei denen das Netz stabilisiert wird, indem gezielt einzelne Verbraucher oder Gebiete vorübergehend nicht mit Strom beliefert werden („rollierende Abschaltungen“ oder „kontrollierte Brownouts“)
- In diesen Situationen drohen nicht annähernd die gleichen gravierenden Folgen wie bei einem Blackout.

Eine Unterversorgung mit Energie stellt aktuell kein Blackout-Risiko dar. Die Netzbetreiber erkennen eine potenzielle Unterversorgung rechtzeitig und behalten mit verschiedenen Maßnahmen die Kontrolle über das Netz – im Extremfall über Abschaltungen einzelner industrieller Großverbraucher oder rollierende Abschaltungen.

Ein Blackout ist ein großer Stromausfall, bei dem …

- das Gebiet so lange ohne Strom und so groß ist, dass die Versorgung mit Basisdiensten wie Rettungskräften und Polizei nicht über die umliegenden Gebiete geschehen kann,
- die Einschränkungen so massiv sind, dass gravierende gesellschaftliche und ökonomische Folgen drohen,
- der Netzbetreiber temporär die Kontrolle über das Netz verliert.

Mögliche Ursachen für Blackouts können unter anderem Naturkatastrophen, menschliches Versagen oder Terrorismus sein. Deutschland hat Notfallpläne, um im Falles eines Blackouts die Grundversorgung aufrechtzuerhalten. Das Risiko für katastrophale Blackouts mit drastischen Folgen schätzen Fachleute als sehr gering ein.

Welche Blackout-Risiken können in Zukunft entstehen?

Das Energiesystem wird digitaler und muss eine große Anzahl dezentraler Erneuerbarer Energien-Anlagen und Speicher koordinieren. Hinzu kommen neue, über das Internet gesteuerte Verbraucher wie E-Autos und Smart-Home-Systeme. Einerseits entstehen dadurch neue Möglichkeiten zur Sicherung des elektrischen Energiesystems, andererseits ändern sich die Risiken.

Mögliche Risiken

1. Viele ans Stromnetz angeschlossene Anlagen und Verbraucher (Wind- und PV-Anlagen, E-Fahrzeuge, Wärmepumpen) können über das Internet gesteuert werden. Werden z. B. viele dezentrale Anlagen ungewollt oder gewollt („Hacker“) gleichzeitig abgeschaltet, kann das Netz destabilisieren.
2. Die genutzte Software kann sowohl durch Fehler („Bugs“) als auch durch Cyberangriffe ungewünschtes Verhalten von Anlagen verursachen und so zu Problemen in der Stromversorgung führen.
3. Die erhöhte Komplexität des Systems erschwert die Analyse des Netzgeschehens. Es kann zu unvorhersehbarem Verhalten kommen („emergentes Verhalten“).
4. Für einige der zukünftigen Entwicklungen lassen sich keine der für das klassische Risikomanagement notwendigen Wahrscheinlichkeiten ermitteln.

Was müssen wir tun?

Wir müssen ein Energiesystem gestalten, dass neben den bekannten auch unvorhergesehene, neuartige Störereignisse mit möglichst geringem Schaden überstehen und zu vertretbaren Kosten wieder in den normalen Betriebszustand zurückkehren kann („Resilienz“). Hierfür braucht es Maßnahmen insbesondere in den folgenden Bereichen.

1. **Dezentralität nutzen:**
   Mit kleinen Erzeugungsanlagen, Speichern und flexiblen Verbrauchern gezielt die Versorgungssicherheit erhöhen.
2. **Sichere und sichernde Digitalisierung gestalten:**
   Hohe Cybersicherheitsstandards auch für Akteure außerhalb der klassischen Stromversorgung sicherstellen – etwa für Prosumer, Gerätehersteller und Plattformbetreiber.
3. **Die Öffentlichkeit einbinden:**
   Risiken transparent und faktenbasiert kommunizieren und gesellschaftlich Regeln verhandeln, wie Verbraucher und Prosumer zukünftig zur Resilienz der Stromversorgung beitragen sollen.
4. **Resilienzstrategie mit Monitoring institutionalisieren:**
   Eine nationale Resilienzstrategie erarbeiten und regelmäßig evaluieren. Dafür sind zunächst Kenngrößen zu definieren, um Resilienz zu bemessen.

1 Blackouts – eine reale Gefahr?

Deutschland hat eines der weltweit sichersten elektrischen Energiesysteme. Selbst kleinere Stromunterbrechungen sind im Alltag eher ungewohnt. Im Jahr 2021 betrug die durchschnittliche Ausfallzeit in Deutschland gerade einmal 12 Minuten und 45 Sekunden. Auch im gesamten europäischen Verbundnetz ist die Qualität der Stromversorgung hoch. Dennoch bestehen derzeit Ängste vor einem Blackout, die teilweise medial und politisch geschürt werden. Auslöser für diese Sorgen sind insbesondere die durch den Angriffskrieg Russlands gegen die Ukraine ausgelöste Gasknappheit und die aktuell hohen Ausfallraten der Atomkraftwerke in Frankreich. Das hohe Interesse an dem Thema Blackouts zeigte sich unter anderem in einer Debatte im Bundestag, Medienberichten und Talkshows.

Dabei ist zunächst einmal wichtig, den schillernden Begriff „Blackout“ einzuordnen. Er erinnert an ein Katastrophenszenario, wie der Autor Marc Elsberg es in seinem gleichnamigen Roman von 2013 beschreibt: Durch einen mehrwöchigen europaweiten Stromausfall bricht darin die öffentliche Ordnung weitestgehend zusammen. Vor dem Hintergrund der allgemeinen Verunsicherung, die der Krieg in Europa und die Energiekrise auslösen, erscheint ein solches Szenario einigen Menschen weniger weit weg als vorher.

Doch eine Einordnung von Fachleuten zeigt:

- Nicht jeder Stromausfall ist ein Blackout. Diese Feststellung – und sprachliche Präzision – ist wesentlich, denn nicht jede Unterbrechung der Stromversorgung ist mit den harschen Konsequenzen verbunden, wie sie Blackouts zugewiesen werden. Und selbst wenn es zu einem Blackout käme, würde damit nicht gleich ganz Europa „lahmgelegt“ werden. Damit sich ein Blackout zu dem von Marc Elsberg beschriebenen Katastrophenszenario ausweitet, müssten viele unglückliche Umstände und Fehler zusammentreffen. Fachleute schätzen das Risiko für einen derart katastrophalen Blackout als sehr gering ein, selbst für kürzere und regional begrenzte Blackouts – und zwar auch unter den verschärften Rahmenbedingungen der derzeitigen Energiekrise. Ein katastrophaler Blackout ist, so lässt sich heute sagen, extrem unwahrscheinlich.

- Deutschland begegnet potenziellen Blackout-Ereignissen zudem nicht unvorbereitet. Um im Falle eines Blackouts eine Grundversorgung der Bevölkerung aufrechtzuerhalten, gibt es konkrete Notfallpläne. Kritische Infrastrukturen wie beispielsweise Krankenhäuser verfügen über eine Notstromversorgung. Die Empfehlungen des Katastrophenschutzes, für den Fall eines längeren Stromausfalls unter anderem Trinkwasser, eine Taschenlampe, Batterien und ein batteriebetriebenes Radio im Haus zu haben, gab es auch schon vor der aktuellen Krise – sie wurden nur weniger diskutiert und beachtet.

- Der Umbau des Energiesystems ist nicht nur wichtig für den Klimaschutz, sondern eröffnet auch eine Chance für die Erhöhung der Versorgungssicherheit: Der Ausbau der erneuerbaren Energien reduziert die Abhängigkeit von Importen fossiler Energieträger und damit verletztlicher Lieferketten. Die Dezentralisierung der Energieversorgung verteilt externe Ausfallrisiken auf eine große Anzahl von Anlagen, macht damit die Versorgung weniger physisch angreifbar und verringert die potenziellen Folgen von Angriffen oder Sabotageakten auf beispielsweise Großkraftwerke oder Pipelines. Über den gezielten Einsatz von Digitalisierung ist es zudem möglich, genaue Informationen zum Zustand des Energiesystems zu erheben und in kritischen Situationen schneller und besser zu reagieren.

Ausgehend von dieser ersten Einordnung liefert dieses Papier zunächst eine wissenschaftsbasierte Einschätzung für das Risiko eines Blackouts in der derzeitigen Situation. Es erklärt, wie sich ein Blackout von einem kleineren Stromausfall und einem Brownout unterscheidet, was ihn verursacht und welche Folgen er hat. Im Anschluss wird erläutert, welche Risikoursachen für einen Blackout in Zukunft einflussreicher werden, und es werden Handlungsoptionen aufgezeigt, wie mit Dezentralisierung und Digitalisierung die Versorgungssicherheit nicht nur erhalten, sondern sogar erhöht werden kann.

2 Was ist ein Blackout und welche Folgen hat er?

Ein Blackout ist ein großer Stromausfall. Es gibt keine einheitliche Definition dafür, ab welcher räumlichen Ausdehnung und Dauer man von einem Blackout spricht, es müssen aber die folgenden drei Merkmale gleichzeitig erfüllt sein:

- Der Stromausfall ist so großflächig, dass das betroffene Gebiet nicht mehr ausreichend durch die nicht betroffenen angrenzenden Gebiete versorgt werden kann.
- Der Stromausfall dauert so lang, dass gravierende gesellschaftliche und ökonomische Folgen verursacht werden.
- Der Stromausfall ist ungeplant. Die für die sichere Stromversorgung zuständigen Netzbetreiber verlieren zumindest eine Zeitlang die Kontrolle über das Geschehen im Stromnetz.

Einen Blackout in diesem Sinne hat es in Nachkriegsdeutschland bisher nicht gegeben. Sollte jedoch ein Blackout eintreten, hätte er – abhängig von seiner Dauer und räumlichen Ausdehnung – mitunter gravierende Folgen für die Gesellschaft: Bereits nach einigen Stunden können erhöhte Todes- und Verletztenzahlen auftreten, weil Rettungsdienste oder die Polizei aufgrund entladener Mobilfunkgeräte nicht gerufen werden können. Nahrungsmittel für Kleinkinder können nur noch eingeschränkt bereitgestellt werden. Auch beträchtliche ökonomische Verluste (z.B. durch Produktionsausfälle) können bereits nach einigen Stunden auftreten. Krankenhäuser verfügen über eine Notstromversorgung mit Batterien und/oder Dieselgeneratoren, die für eine begrenzte Dauer einen Stromausfall überbrücken können. Nach mehr als 24 Stunden wären die meisten Krankenhäuser jedoch nur noch bedingt handlungsfähig und Patient*innen müssten in Krankenhäuser verlegt werden, die die Notstromversorgung länger aufrechterhalten können.

Auch die Lebensmittelversorgung wäre nach mehr als 24 Stunden merklich eingeschränkt. Bei einem mehrtägigen Stromausfall käme es zu gehäuften Todesfällen in Pflegeheimen – unter anderem weil Pflegekräfte nicht mehr zur Arbeit kommen können, wenn die öffentliche Verkehrsinfrastruktur und Tankstellen nicht mehr betrieben werden können, die Versorgung mit Medikamenten eingeschränkt ist und Bewohner*innen unterkühlt sind. In landwirtschaftlichen Betrieben würde ein Massensterben von Nutztieren beginnen. Auch die ökonomischen Schäden wären enorm: Ein deutschlandweiter Stromausfall würde Schätzungen zufolge einen Schaden von 0,6–1,3 Mrd. Euro pro Stunde verursachen. Selbst wenn die Stromversorgung nach einigen Tagen wieder funktionieren würde, könnten gravierende Folgen für die Gesellschaft auch lange nach der Störung bestehen bleiben, weil die Schäden des Blackouts nicht sofort behoben werden könnten.

Aber: Die hier skizzierten Folgen treten nicht bei **kurzen und räumlich begrenzten Stromausfällen** auf, deshalb gilt es sorgfältig zu unterscheiden. Mehrstündige Stromausfälle, die auf ein kleines Gebiet, zum Beispiel wenige Straßenzüge, beschränkt sind, treten in Deutschland fast täglich auf. Sie treffen den

Einzelnen aber selten und bleiben meist vom nicht betroffenen Teil der Bevölkerung unbemerkt. Häufig ist die Ursache, dass bei Bauarbeiten ein Stromkabel beschädigt wird. Zwar verursachen auch solche kleineren Stromausfälle Komforteinbußen und in gewissem Umfang auch wirtschaftliche Verluste, ihre Folgen sind aber überschaubar und nicht mit denen eines Blackouts vergleichbar. Angrenzende Gebiete können die Versorgung mit Gütern und Leistungen wie Gesundheitsversorgung ohne besondere Schwierigkeiten leisten.

Von einem Blackout zu unterscheiden ist auch eine kontrollierte Abschaltung eines Teils der Verbraucher. Dieser sogenannte **kontrollierte Brownout** kann notwendig werden, wenn zu einem Zeitpunkt die Stromnachfrage nicht gedeckt werden kann, etwa weil ein großer Teil der Kraftwerke gleichzeitig nicht mit Brennstoff versorgt werden kann oder sich in Wartung befindet wie derzeit die AKW in Frankreich. In einem solchen Fall, der in Deutschland bisher nicht aufgetreten ist, muss der Netzbetreiber Verbraucher vom Netz trennen, um die Stabilität der Stromversorgung zu sichern. Vorzugsweise nimmt er zunächst einzelne Großverbraucher regional und zeitlich begrenzt vom Netz. Eine große Zahl von Industrieunternehmen hat solche Abschaltmöglichkeiten in ihren Stromlieferverträgen festgeschrieben. Reicht dies nicht, werden durch eine **rollierende Abschaltung**, also eine abwechselnde, zeitlich vorab klar begrenzte Abschaltung, mehrere Gebiete vom Netz getrennt. Je nach Ursache können die betroffenen Verbraucher vorgewarnt werden und sich somit vorbereiten. In solchen Fällen behält der Netzbetreiber durchgehend die Kontrolle über das Geschehen im Netz und kann die Versorgung auch problemlos wieder aufnehmen. Eine Unterversorgung mit wichtigen Gütern oder Dienstleistungen ist in solchen Fällen nicht zu befürchten.

3 Welche Ursachen für Blackouts und andere Stromausfälle bestehen?

Gleichzeitiges technisches Versagen einer Vielzahl von Betriebsmitteln der Stromversorgung (Leitungen, Transformatoren, Schaltanlagen. Kraftwerke), Naturereignisse in Form von Wetterextremen, hohe Krankenstände aufgrund einer Pandemie, menschliches Versagen und bösartige Aktivitäten wie Sabotage, Terrorismus oder Kriege können zu größeren Stromausfällen oder, im schlimmsten Fall, zu einem Blackout führen. So gab es im europäischen Verbundnetz unter anderem 2003 und 2006 gravierende Stromausfälle. Im Jahr 2003 waren sogar 95 Prozent Italiens mehrere Stunden ohne Strom. In beiden Fällen spielte menschliches Versagen eine wesentliche Rolle. In Deutschland konnten im Jahr 2005 Strommasten in Münster den Schnee auf den Leitungen nicht mehr tragen – die Menschen in der Region waren zum Teil mehrere Tage ohne Strom. In der Ukraine führte im Jahr 2015 ein Cyber-Angriff zu einem mehrstündigen Stromausfall, von dem mehrere hunderttausend Menschen betroffen waren. Doch in all diesen Fällen kam es aufgrund der kürzeren Dauer (z.B. Europa 2006, Ukraine 2015 jeweils wenige Stunden) oder der begrenzten Region (Münster 2005) nicht zu den oben beschriebenen extremen Folgen.

Im Falle eines Stromausfalls versuchen die Netzbetreiber, die Destabilisierung weiterer Teile des Netzes zu verhindern und die Versorgung im betroffenen Gebiet schnellstmöglich wiederherzustellen. Die notwendigen Maßnahmen sind in **Netzwiederaufbauplänen** festgelegt und werden durch regelmäßige **Übungen** trainiert, in denen verschiedene Störungsszenarien simuliert werden. Bei den oben genannten Ursachen (abgesehen von Krieg) würde sich ein Stromausfall nur dann zu einem mehrtägigen überregionalen Blackout ausweiten, wenn noch weitere unglückliche Umstände oder Fehler hinzukommen und die Stabilisierung des restlichen Netzes und den Netzwiederaufbau verhindern.

Eine mögliche Ursache für einen Tage oder gar Wochen andauernden Stromausfall in großen Teilen Europas wäre ein starker Sonnensturm. Simulationen zeigen, dass dieser Schäden an Großkomponenten wie Transformatoren verursachen und dadurch einen großen Blackout herbeiführen könnte. Mit den möglichen

Folgewirkungen solcher Extremereignisse, deren Eintrittswahrscheinlichkeit sehr gering ist, beschäftigen sich unter anderem die europäischen Übertragungsnetzbetreiber und der Katastrophenschutz.

4 Ist ein Blackout aufgrund der Energiekrise zu befürchten?

Wie sieht die Situation derzeit aus? Aktuell ist in Deutschland das Risiko eines Blackouts aufgrund einer **Unterversorgung mit Energie** gering. In der öffentlichen Diskussion formulierte Befürchtungen bestätigen sich nicht. Selbst im Worst Case, also wenn der Leistungsbedarf die verfügbare Kraftwerksleistung im Inland tatsächlich übersteigen würde und das Defizit auch nicht durch Importe aus den Nachbarländern gedeckt werden könnte, würde dies nicht zu einem Blackout führen. Die Netzbetreiber, denen diese Mangellage aufgrund von Prognosen und der europäischen Abstimmungsprozesse im Regelfall spätestens 24 Stunden vorher bekannt wäre, würden dann vorausschauend geplant zunächst wenige **industrielle Großverbraucher** abschalten. Wenn dies nicht ausreichen würde, würden sie durch rollierende Abschaltungen von Netzgebieten Blackouts vermeiden. Aber auch solche geplanten Abschaltungen sind hochgradig unerwünscht und sollten nur eine Notlösung sein. Ziel der Energiepolitik muss es vielmehr sein, dass Haushalte, Gewerbe und Industrie auch zukünftig mindestens so gut und sicher mit Strom versorgt werden können wie heute.

5 Welche Blackout-Risiken bestehen in Zukunft?

Im Zuge der Energiewende wird und muss sich die Stromversorgung zügig ändern – um die Energieversorgung zu dekarbonisieren, aber auch um die Abhängigkeit von Energieimporten wie etwa Erdgas zu verringern: Eine große Anzahl an Windenergie- und Photovoltaikanlagen liefert dann den Großteil der Energie und ersetzt die fossilen und nuklearen Großkraftwerke. Dass dies keineswegs zwangsläufig zu Einbußen bei der Versorgungaqualität führt, zeigen die vergangenen 30 Jahre: Im Zuge des Ausbaus der erneuerbaren Energien auf 45 Prozent der Nettostromerzeugung hat sich die Versorgungsqualität nicht verringert.

Während das Gleichgewicht von Stromeinspeisung, Transportverlusten im Netz und Stromverbrauch im europäischen Verbundnetz auf technischer Ebene heute erreicht wird, indem die Stromerzeugung flexibel dem gewünschten Verbrauch angepasst wird (**Lastfolge**), muss zukünftig die Entnahme von elektrischer Energie stärker an die fluktuierende Stromeinspeisung der erneuerbaren Energien angepasst werden (**Erzeugungsfolge**). Dazu müssen finanzielle Anreize für die technische Verbrauchsflexibilisierung geschaffen werden (insbesondere Lastverschiebung bei industriellen Verbrauchern, aber auch z.B. gesteuertes Laden von Elektrofahrzeugen). Neben dem verstärkten Einsatz von Batteriespeichern muss zudem grüner Wasserstoff oder daraus hergestelltes synthetisches Methan (SNG) für die Stromerzeugung in Gaskraftwerken vorgehalten werden, um eine Dunkelflaute, also einige Wochen fehlender Einspeisung aus Wind- und Photovoltaik-Anlagen, klimaneutral überbrücken zu können, wenn Erdgas nicht mehr verbrannt werden darf.

Im Unterschied zu heute wird zukünftig eine große Anzahl von kleinen, dezentralen Anlagen im Zusammenspiel eine zuverlässige Stromversorgung sicherstellen. Zudem kommt eine **Vielzahl an Akteuren** hinzu: Heute wirken vor allem die Erzeuger großer Leistungsmengen (Betreiber von Großkraftwerken oder einer großen Anzahl von erneuerbaren Anlagen), Netzbetreiber und Betreiber großer Energiebörsen auf die Stabilität des Energiesystems ein. In Zukunft werden auch andere Akteure eine Rolle spielen, zum Beispiel Betreiber von Ladeinfrastrukturen, Prosumer, Unternehmen, die sich auf die Bündelung und Vermarktung von Flexibilitäten als Dienstleistung fokussiert haben (sogenannte Aggregatoren), oder Betreiber von

Anlagen und Betreiber ist nur mittels Automatisierung und Digitalisierung möglich. Zudem steht eine größere Zahl kleiner Stromerzeuger und Speicher zur Verfügung, um als „Schwarm“ das elektrische Energiesystem zu stützen (siehe 6.1 Dezentralität nutzen).

Klar ist: Die geschilderte **Dezentralisierung und die zunehmende Digitalisierung** des Energiesystems wirken sich auch auf das Risiko eines Blackouts aus. Einige Risiken werden durch den Umbau des Energiesystems verringert. So reduziert der Ausbau der erneuerbaren Energien die Abhängigkeit von Importen fossiler Energieträger und trägt maßgeblich zur Erhöhung der Versorgungssicherheit bei. Und die dezentralere Stuktur des zukünftigen Energiesystems reduziert die Abhängigkeit von Großanlagen, die Ziel eines physischen Angriffs oder Sabotageakts werden können. Digitalisierung trägt dazu bei, das Zusammenspiel der verschiedenen Anlagen und Betreiber zu optimieren. Sie ermöglicht es, umfangreiche Daten zum Zustand des Energiesystems zu erheben, auszuwerten und mit anderen relevanten Akteuren zu teilen und erleichtert dadurch ein abgestimmtes, schnelles und zielführendes Vorgehen im Falle einer Störung.

Es gibt aber auch Risiken, die im zukünftigen System relevanter werden. Die heutigen Gesetze und Verordnungen zur Sicherung der Stromverordnung gehen auf diese Veränderungen noch nicht ausreichend ein. Mögliche neue oder unter diesen Bedingungen verschärfte Risikoursachen für einen Blackout sind besonders die folgenden:

1. Kleine, aktiv steuerbare Erzeugungs- und Speicheranlagen sowie elektrische Geräte werden zukünftig systemrelevant für die Energieversorgung: Werden sie mittels IKT (Informations- und Kommunikationstechnologien) zeitgleich angesteuert und zum Beispiel an- oder abgeschaltet, können Spannung oder Frequenz, die beiden wichtigsten Größen für die Stabilität des Stromnetzes, wesentlich beeinflusst werden. Dies kann zur Stabilisierung des Netzes beitragen, bei bösartiger Absicht oder im Fehlerfall aber auch zur Destabilisierung führen. Gleiches gilt für elektrische Verbraucher, vom Fahrzeug über die Wärmepumpe bis zum Kühlschrank, die zunehmend durch das Internet ansprechbar werden.

2. Fehlfunktionen in den Systemen der IKT können zu massiven Bedrohungen führen. Dies gilt nicht nur für Ereignisse wie den Cyber-Angriff auf die Kontrollzentren (Leitstände) in der Ukraine 2015. Zukünftig könnten noch weit komplexere Angriffe geplant werden. Mögliche Ziele wären Hersteller von Wechselrichtern für Erneuerbare Energie-Anlagen (EE-Anlagen), um über die ans Internet angeschlossenen Wechselrichter Zugriff auf die EE-Anlagen zu erlangen. Auch Angriffe auf Betreiber von IT-Plattformen, auf denen eine ausreichend große Leistungsmenge kommunikationstechnisch angesteuert werden kann, oder eine Attacke, die sich direkt auf eine sehr große Anzahl dezentraler Anlagen richtet, wären denkbar. So könnten Attacken auf die Stromversorgung koordiniert werden, die sich von bekannten Störungen stark unterscheiden. Ein weltweiter „Markt“ für Software und Informationen, die solchen Angriffen dienen können, steigert dieses Risiko noch. Auf diesem kaufen auch Staaten ein („Staatstrojaner“). Ein Blackout-verursachender Angriff auf IKT-Systeme würde erhebliche finanzielle und personelle Ressourcen erfordern. Diese dürften vor allem staatlich unterstützten Akteuren zur Verfügung stehen.

3. Die erhöhte Komplexität des künftigen Energiesystems wird es schwieriger machen, das Netzgeschehen zu analysieren. Das hat auch Folgen für den operativen Netzbetrieb. Werden in Zukunft Anlagen und Geräte mehr und mehr digital angebunden und durch Algorithmen gesteuert, häufig unter Nutzung Künstlicher Intelligenz (KI), könnten Verhaltensmuster gebildet werden, die nicht vorhersehbar sind, etwa ein synchronisiertes An- oder Abschalten von Geräten (sogenanntes „emergentes Verhalten“).

4. Neue Ungewissheiten erschweren es, ein zukunftssicheres elektrisches Energieversorgungssystem optimal zu planen und umzusetzen: Technischer Aufbau, Prozesse, Richtlinien, Standards und Regulierung werden immer auf Grundlage von expliziten und impliziten Annahmen über die Zukunft erschaffen oder angepasst – auch die europäische Energiezukunft birgt einige Ungewissheiten. Denkbar wären zudem (geo-)politische und gesellschaftliche Entwicklungen, die die Gefahr krimineller oder terroristischer Angriffe erhöhen. Auch hybride Kriege mit Cyber-Angriffen auf die Energieversorgung wären möglich. Einige der Unsicherheiten könnten sich als problematisch erweisen. Dies gilt insbesondere, wenn bei der Weiterentwicklung des Energiesystems sogenannte Pfadabhängigkeiten geschaffen werden, also durch einmal getroffene Entscheidungen Hürden aufgebaut werden, die den späteren Umstieg auf eine andere Option erschweren oder verhindern. Diese könnten eine spätere Anpassung an überraschende Entwicklungen erschweren, weil zum Beispiel langwierige Umrüstungsprozesse notwendig wären.

Um das zukünftige klimafreundliche, dezentralisierte und digitalisierte Energiesystem möglichst widerstandsfähig und versorgungssicher zu gestalten, gilt es, den oben genannten **Risikoursachen aktiv zu begegnen** und nicht abzuwarten, bis der Fall der Fälle eingetreten ist. Dennoch bleibt das Restrisiko eines mehrtägigen großflächigen Blackouts auch in einem widerstandsfähigen Energiesystem immer bestehen. Umfangreiche Sicherheitsmaßnahmen müssen daher auch außerhalb des Energiesystems getroffen werden, unter anderem im Katastrophenschutz und in der Katastrophenvorsorge. Mit dieser Aufgabe befasst sich etwa das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.

6 Was tun?

Das heute Energiesystem ist deshalb so sicher und zuverlässig, weil umfangreiche Risikoanalysen, **Erfahrungswissen** und Lehren aus der Vergangenheit genutzt wurden, um Schwachstellen zu beseitigen. Der wichtigste Baustein ist dabei **Redundanz**: Es bestehen erhebliche Überkapazitäten bei den Kraftwerken, die Übertragungsnetze sind nach dem „n-1“-Prinzip ausgelegt – es gibt also immer eine Leitung mehr, als im ungestörten System gebraucht wird. Zusätzlich sind Betriebsmittel so dimensioniert, dass sie im Normalbetrieb deutlich unter dem erlaubten Maximum ausgelastet werden. Ein weiterer wichtiger Baustein sind die **Reserveleistungen**, die teilweise europaweit und teilweise national organisiert sind. So kann der gleichzeitige Ausfall von zwei der größten betriebenen Kraftwerksblöcke kompensiert werden, ohne dass die Stromverbraucher davon etwas merken. Teile der Reserveleistung werden dabei bewusst auch ohne digitale Kommunikation bereitgestellt. Zudem sind die nationalen Verteilnetze größtenteils unterirdisch verlegt, was teuer ist, aber zum Beispiel in einer wesentlich höheren **Robustheit** gegenüber Extremwetter führt, als dies etwa aus den USA bekannt ist.

Jedoch müssen die bisherigen Ansätze nun ergänzt werden, um auch die zukünftigen Blackout-Risiken meistern zu können. In solchen Situationen hat sich das Konzept der **Resilienz** bewährt: Ziel dieses Konzepts ist es, auch solche Störereignisse mit möglichst geringem Schaden zu überstehen, deren verlustfreie Abwehr nicht vorab geplant und im Systemdesign berücksichtigt werden kann. Eine resiliente Stromversorgung besitzt die Fähigkeit, ein Störereignis unbeschadet abzufangen oder zumindest in kurzer Zeit mit möglichst geringem Schaden und zu vertretbaren Kosten wieder in den normalen Betriebszustand zurückzukehren – sogar wenn das Ereignis überraschend oder neuartig ist. Weiterhin sollte ein resilientes Energiesystem hinreichend wirksam und in gutem Aufwand-Nutzen-Verhältnis auf unerwartete Entwicklungen reagieren können. Gerade die Digitalisierung kann hier unterstützen, da die kurzen Innovationszyklen der Digitalwirtschaft eine große Flexibilität ermöglichen.

Neben der digitalen Kommunikation verfügt das Stromsystem über die physikalischen Führungsgrößen Spannung und Frequenz. Erzeugungs- und Verbrauchsanlagen reagieren teils automatisch auf Abweichungen von den Sollwerten und tragen so zur Stabilität der Stromversorgung bei. Ein wirtschaftlich oder technisch optimaler Betrieb kann alleine durch diese Mechanismen allerdings nicht erreicht werden, sondern erfordert ein Zusammenspiel dieser physikalischen Regelungsmechanismen mit digital gesteuerten Prozessen.

7 Handlungsfelder

Die genannten Risikoursachen spielen heute noch eine geringe Rolle, werden in Zukunft aber deutlich zunehmen. Deshalb gilt es, potenziellen Risiken durch wirksame Maßnahmen bereits jetzt zu begegnen und vorzusorgen. Aktivitäten in den folgenden **vier Handlungsfeldern** können dazu beitragen:

7.1 Dezentralität nutzen

Eine dezentrale digitalisierte Energieversorgung bietet neue Möglichkeiten, das Energiesystem resilient zu gestalten. Diese Chance gilt es nun zu nutzen. Dezentrale Anlagen (Windenergie, Photovoltaik, Batteriespeicher usw.) können dazu beitragen, dass Störereignisse keine oder deutlich weniger gravierende Auswirkungen haben. Im Falle eines größeren Stromausfalls können sie im Notbetrieb eine regionale Versorgung innerhalb eines Netzgebietes im sogenannten **„Inselbetrieb“** sicherstellen – unabhängig vom Zustand des europäischen Verbundnetzes und in der Regel ohne große industrielle Verbraucher. Es könnten zum Beispiel insbesondere Teile kritischer Infrastrukturen wie Krankenhäuser oder Rettungsdienste bevorzugt mit Strom versorgt werden, bis die allgemeine Stromversorgung wieder hergestellt ist.

Um diesen **systemdienlichen Einsatz dezentraler Anlagen** zu ermöglichen, sind sowohl Forschung und Entwicklung als auch neue gesetzliche Regelungen, technische Prozesse und Standards erforderlich. Die Vielzahl technischer Optionen für dezentrale Anlagen nicht einzuschränken, wird wesentlich sein, um auf unbekannte Herausforderungen flexibel reagieren zu können. Ermöglicht wird dies unter anderem, wenn sich die Software der dezentralen Anlagen durch **automatische Updates** anpassen lässt. So können Lernerfahrungen, die aufgrund von äußeren Ereignissen oder durch die Software selbst gemacht wurden, auch nachträglich in die Anlagen eingespeist werden. Ist die Steuerung hingegen teilweise in Hardware oder elektrotechnischen Komponenten implementiert, kann dies später dazu führen, dass eine große Anzahl dezentraler Anlagen an ihrem jeweiligen Standort nachgerüstet werden muss. Dies ist nicht nur viel teuer als Softwareupdates, sondern bedeutet auch einen erheblich größeren Zeitaufwand von vielen Jahren.

Künstliche Intelligenz (KI) kann weitere Potenziale zur **Systemstabilisierung** erschließen. Einige neuartige Angriffe auf die Stromversorgung lassen sich voraussichtlich sogar nur abwehren, wenn KI in die dezentralen Anlagen integriert wird. Für all das ist insbesondere die **Digitalisierung der Verteilnetze** notwendig, da der weit überwiegende Teil der erneuerbaren Erzeugung an die Verteilnetze angeschlossen ist. Außerdem muss zukünftig in großem Maßstab Lastbeeinflussung („**Demand Side Management**“) in den Verteilnetzen stattfinden, um wetter-, tages- und jahreszeitabhängig schwankende Stromerzeugung auszugleichen. Lokal sollte das Versorgungssystem in die Lage versetzt werden, ohne zentrale Steuereinheit auszukommen und durch Selbstorganisation und Kommunikation von Netzknoten zu Netzknoten betriebsbereit zu bleiben, ähnlich dem Betrieb des Internets. Sinnvoll wäre eine solche Organisation etwa, wenn die Leitstelle des zuständigen Netzbetreibers durch einen Cyber-Angriff nicht mehr funktional wäre.

Auch in Zukunft müssen Netzbetreiber die Verantwortung für die Sicherheit des Elektrizitätsversorgungssystems wahrnehmen. Hierfür müssen sie die Möglichkeit erhalten, das Potenzial der kommunikationstechnisch angeschlossenen dezentralen Anlagen zu nutzen. Das erfordert Ergänzungen in der Ausbildung des Betriebspersonals, das unter anderem den **Umgang mit ganz neuen und überraschenden Störereignissen** erlernen muss. Nicht zuletzt sind Verordnungen anzupassen, um die Finanzierung dieser Maßnahmen zu sichern.

7.2 Sichere und sichernde Digitalisierung gestalten

Während politischer Wille – nicht zuletzt, um ein sicheres Elektrizitätsversorgungssystem beizubehalten – und Marktkräfte die notwendige Digitalisierung der Stromversorgung vorantreiben, muss man nun auf die damit verbundenen Risiken reagieren. Auf europäischer und nationaler Ebene gibt es bereits umfangreiche Maßnahmen zur Erhöhung der IT-Sicherheit – teilweise auch **„Cyberresilience“** genannt. Diese sollten auf ihre Effizienz und Effektivität bezüglich der Resilienz des Energiesystems geprüft und durch weitere Maßnahmen ergänzt werden, falls sie bestimmte Risiken nicht abdecken. Als gute technische Basis ließe sich die geplante Smart-Meter-Infrastruktur nutzen.

Gesetze sollten auch Akteure umfassen, die nicht der eigentlichen Energieversorgung zuzurechnen sind, aber einen großen Einfluss auf die Sicherheit der Stromversorgung haben könnten. Dies sind beispielsweise Hersteller von Produkten mit digitalen Komponenten, zu denen bereits EU-Verordnungen in Vorbereitung sind. Für Betreiber von Plattformen, etwa Hersteller von E-Fahrzeugen oder Wechselrichtern sowie Anbieter von Smart-Home-Systemengibt es jedoch noch keine entsprechenden umfassenden Gesetzgebungsvorhaben. Entsprechende technische Standards für intelligentes (bi-)direktionales Laden liegen hingegen bereits vor.

Vor allem sind noch lange nicht alle Abhängigkeiten bekannt, die sich zwischen der Stromversorgung und Entwicklungen außerhalb der Stromversorgung ergeben. Diese Wissenslücken müssen geschlossen werden, um die Blackout-Risiken schließlich mit Gesetzen und Verordnungen zu begrenzen.

Doch auch vom Staat selbst gehen Bedrohungen aus: Staaten und ihre Sicherheitsbehörden haben Interesse daran, dass Lücken in der IT-Sicherheit verbleiben. Dahinter steht die Annahme, dass auf diese Weise kriminelle Aktivitäten wirksamer ausgespäht oder nachgewiesen werden könnten. Auch werden digitale Angriffswerkzeuge entwickelt („Staatstrojaner“). Wenn sich ein Staat dazu entscheidet, durch diese hochumstrittenen Maßnahmen die IT-Sicherheit vieler Systeme zu verringern und damit auch das Blackout-Risiko zu erhöhen, sollte eine (inbesondere von mit polizeilichen oder nachrichtendienstlichen Aufgaben befassten Einrichtungen) unabhängige Stelle transparent evaluieren, welcher Nutzen in der Kriminalitätsbekämpfung welchen Gefahren für die europäische Energieversorgung gegenübersteht.

Es wird voraussichtlich nicht möglich sein, alle Sicherheitslücken im digitalisierten Energiesystem zu schließen. Deshalb werden vordringlich Mechanismen und Vorgaben benötigt, um auch mit korrumpierten („gehackten“) IKT-Systemen die Stromversorgung aufrechtzuerhalten.

7.3 Die Öffentlichkeit einbinden

Die aktuelle Energiekrise löst Ängste aus. Gerade deshalb sollte die **öffentliche Diskussion** über vorhandene oder auch nicht vorhandene Risiken unbedingt faktenbasiert geführt werden. So wird etwa der Begriff „Blackout“ in den Medien und in der Politik teilweise unpräzise verwendet und kann – oder soll sogar – Ängste schüren. Um dem entgegenzuwirken, braucht es **Informationen**, unter anderem zur Unterscheidung von geplanten rollierenden Abschaltungen, kleineren, lokalen Stromausfällen und einem großen Blackout.

Diese sollten an die Informationsbedürfnisse der Zielgruppen angepasst sein und die jeweiligen möglichen Ursachen und Folgen für die Bürger*innen klar benennen.

Es sollte auch kommuniziert werden, dass Maßnahmen, die Privatverbraucher*innen in Sorge vor einer mangelhaften Wärmeversorgung treffen, problematisch sein können: Nutzen sehr viele Haushalte in einem kleinen Gebiet gleichzeitig elektrische Heizlüfter, kann dies zu Schutzabschaltungen im Niederspannungsbereich und damit zu einem lokal begrenzten Stromausfall führen. Es ist daher, etwa durch Umfragen, zu prüfen, ob die Appelle von Verbänden, Verbraucherschutzzentralen und Politik, auf die Nutzung solcher Geräte möglichst zu verzichten, bei den Verbraucher*innen angekommen sind.

Doch auch unabhängig von der aktuellen Situation ist es wichtig, die Öffentlichkeit einzubinden. Im zukünftigen Energiesystem werden Privatakteur*innen eine viel aktivere Rolle einnehmen. Als sogenannte „Prosumer“ können sie ihren Verbrauch und gegebenenfalls die Einspeisung ins Netz mittels eigener Erneuerbare-Energie-Anlage aktiv managen und so zur Steigerung der Resilienz beitragen. Dafür ist gesellschaftlich zu verhandeln, inwieweit beispielsweise Netzbetreiber zur Stabilisierung der Versorgung auf Prosumer-Anlagen zugreifen dürfen, und welche Daten in Haushalten erhoben werden sollten, um Verbrauchsprognosen zu verbessern. Regeln und Anreize hierfür sollten in transparenten Verfahren mit Beteiligungsmöglichkeiten für Bürger*innen erarbeitet werden.

7.4 Resilienzstrategie mit Monitoring institutionalisieren

Werden diese und weitere Maßnahmen in eine nationale Resilienzstrategie für die Energieversorgung integriert, sollte ein **institutionalisiertes, unabhängiges Monitoring** etabiliert werden. Dieses sollte regelmäßig evaluieren, ob sich die verfolgte Strategie als effektiv, effizient und weiterhin adäquat erweist, und ob während der Umsetzung unerwünschte Pfadabhängigkeiten oder unerwünschte Nebeneffekte entstanden sind. Basierend auf den Evaluationsergebnissen können dann die politischen Entscheidungsgremien diskutieren und entscheiden, inwieweit Maßnahmen ergänzt, hinzugefügt oder abgeschafft werden. Als notwendige Voraussetzung braucht es hierfür einen – möglichst europäisch abgestimmten – Ordnungsrahmen, der es erlaubt, Resilienz zu quantifizieren: Zukünftig wird es nicht ausreichen, Erfahrungsgrößen aus der Vergangenheit wie etwa die Häufigkeit von Stromausfällen und deren Ursachen zu betrachten, um die Gefahr zukünftiger Blackouts abschätzen zu können. Dies gilt besonders dann, wenn es sich um neue und bisher beispiellose Störereignisse handelt, wie etwa gravierende Cyber-Vorfälle.

8 Fazit

Wenngleich es äußerst unwahrscheinlich ist, dass die derzeitige Energiekrise zu größeren Stromausfällen führt, gibt es Blackout-Risiken. Diese waren allerdings vor der Krise bereits in ähnlicher Größenordnung vorhanden und wurden lediglich von der breiten Öffentlichkeit weniger beachtet und von Politik und Medien weniger kommuniziert. Um die Stromversorgung auch zukünftig auf gewohnt hohem Niveau halten zu können, gilt es aber, die Entwicklung verschiedener Risikoursachen sorgfältig im Blick zu behalten. Denn die Ursachen für einige der Risiken wiegen sogar von Jahr zu Jahr schwerer und neue mögliche Ursachen kommen hinzu. So ist insbesondere das Ineinandergreifen von Dezentralisierung durch die Energiewende und Digitalisierung eine Weiterentwicklung des Energiesystems, die es gut zu begleiten gilt. Richtig gemacht, werden eine aktiv gestaltete Digitalisierung und dezentrale erneuerbare Energien die Resilienz des Systems sogar erhöhen – etwa durch die Möglichkeit von Inselnetzbildung – und somit die Blackout-Gefährdung verringern. Es ist zu hoffen, dass die derzeitige Aufmerksamkeit für das Thema die Politik zu einer raschen Umsetzung wirksamer Maßnahmen bewegt.

Quellenverzeichnis

Mehr zum Thema

Dieser Impuls beruft sich im Wesentlichen auf die Ergebnisse der Stellungnahme

„Resilienz digitalisierter Energiesysteme. Wie können Blackout-Risiken begrenzt werden?“
https://energiesysteme-zukunft.de/digitalisierung

acatech/Leopoldina/Akademienunion (Hrsg.): Resilienz digitalisierter Energiesysteme. Wie können Blackout-Risiken begrenzt werden? (Schriftenreihe zur wissenschaftsbasierten Politikberatung), 2021. ISBN: 978-3-8047-4224-6

1 Blackouts – eine reale Gefahr?

„Dennoch bestehen derzeit Ängste vor einem Blackout, die teilweise medial und politisch geschürt werden. Das hohe Interesse an dem Thema Blackouts zeigt sich unter anderem in Debatten im Bundestag, Medienberichten und Talkshows.“

Debatte im Bundestag zu Blackouts am 28.09.2022:

https://www.bundestag.de/dokumente/textarchiv/2022/kw39-de-aktuelle-stunde-blackout-912734

Thema Blackout in Talkshows, z.B. am 23.09.22 bei Markus Lanz:

https://www.rnd.de/politik/markus-lanz-im-zdf-bauingenieurin-warnt-vor-blackouts-3QLJLVWY5BCWJCFHYCFVVMB4EU.html

...*und am 29.11. bei Sandra Maischberger:*

*https://www.*ardmediathek*.de/video/maischberger/der-chef-der-bundesnetzagentur-klaus-mueller-ueber-die-wahrscheinlichkeit-von-blackouts/das-erste/Y3JpZDovL2Rhc2Vyc3RlLmRlL21lbnNjaGVulGJlaSBtYWlzY2hiZXJnZXIvNWJiYmUxO-TAtYjVhZi00MDkxLTgzMmItZDliNjgzZjBlOTU1*

„Deutschland hat eines der weltweit sichersten elektrischen Energiesysteme. Selbst kleinere Stromunterbrechungen sind ungewohnt.“

Bundesnetzagentur: Kennzahlen der Versorgungsunterbrechungen Strom, 2022.
URL: https://www.bundesnetzagentur.de/DE/Fachthemen/ElektrizitaetundGas/Versorgungssicherheit/Versorgungsunterbrechungen/Auswertung_Strom/start.html// [Stand 08.12.2022].

CEER Benchmarking Report 6.1 on the Continuity of Electricity and Gas Supply Data update 2015/2016
URL: https://www.ceer.eu/documents/104400/-/-/963153e6-2f42-78eb-22a4-06f1552dd34c

Zum Vergleich: In den USA betragen die durchschnittlichen Versorgungsunterbrechungen jährlich mehrere Stunden:
Eia U.S. Energy Information Administration: U.S. customers experienced an average of neyrly six hours of power interruptions in 2018, 2020. URL: https://www.eia.gov/todayinenergy/detail.php?id=43915 [Stand 15.12.2022].

„Im Jahr 2021 betrug die durchschnittliche Ausfallzeit in Deutschland gerade einmal 12 Minuten und 45 Sekunden."

Die durchschnittliche Versorgungsunterbrechung wird mithilfe der Kenngröße $SAIDI_{EnWG}$ (System Average Interruption Duration Index) bemessen. Sie gibt die durchschnittliche Versorgungsunterbrechung je angeschlossenem Letztverbraucher innerhalb eines Kalenderjahres an.
URL: https://www.bundesnetzagentur.de/DE/Fachthemen/ElektrizitaetundGas/Versorgungssicherheit/Versorgungsunterbrechungen/Auswertung_Strom/start.html// [Stand 08.12.2022].

2 Was ist ein Blackout und welche Folgen hat er?

Beispiele für Definitionen von Blackouts:

Einer der größten regionalen Energieversorger, die EWE, beschreibt einen Blackout als „einen plötzlichen und sehr umfassenden Stromausfall, von dem sehr viele Menschen über einen längeren Zeitraum betroffen sind."
EWE*: Versorgungslage in schweren Zeiten. Wir ordnen die Geschehnisse aus der Energiewelt ein*, 2022.
ULR: https://www.ewe.com/de/media-center/neuigkeiten/stuermische-zeiten-in-der-energiewelt [Stand 08.12.2022].

Das Bundesamt für Sicherheit in der Informationstechnik geht davon aus, dass Ausfälle, die über 500.000 Personen betreffen, „mit den vorhandenen Notfallkapazitäten nicht mehr ausreichend kompensiert werden" können. Diese Zahl ist als untere Grenze zu verstehen und liegt daher auch der ESYS Stellungnahme zugrunde.

Bundesamt für Sicherheit in der Informationstechnik (BSI): *Fragen und Antworten zur BSI-Kritisverordnung.* ULR: https://www.bsi.bund.*de*/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/KRITIS-FAQ/FAQ-BSI-KritisV/faq_kritisv_node.html [Stand 08.12.2022].

Die Bundesnetzagentur legt einen strengeren Maßstab an: „Ein Blackout ist ein unkontrollierter und unvorhergesehener Ausfall, bei dem mindestens größere Teile des europäischen Stromnetzes ausfallen."

Bundesnetzagentur: *Stromnetz, 2022*. ULR: https://www.bundesnetzagentur.de/DE/Fachthemen/ElektrizitaetundGas/Versorgungssicherheit/Stromnetz/start.html [Stand 08.12.2022].

Der Verband der europäischen Übetragungsnetzbetreiber sieht allgemein den „Blackout State" als gegeben, wenn ein Übertragungsnetzbetreiber in einem Teil seines schwarz gefallenen Netzes keine Kontrolle mehr hat.

Verband Europäischer Übertragungsnetzbetreiber (entsoe): *Policy 5: Emergency Operations*, 2015.
ULR: https://eepublicdownloads.entsoe.eu/clean-documents/Publications/SOC/Continental_Europe/oh/20150916_Policy_5_Approved_by_ENTSO-E_RG_CE_Plenary.pdf [Stand 08.12.2022].

Folgen eines Blackouts

Petermann, T./Bradke, H./Lüllman, A./Poetzsch, M./ Riehm, U.: Was bei einem Blackout geschieht: Folgen eines langandauernden und großräumigen Stromausfalls (Studien des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag – 33), Berlin: edition sigma 2011.

„Ein deutschlandweiter Blackout würde Schätzungen zufolge einen Schaden von 0,6 – 1,3 Mrd. Euro pro Stunde verursachen."

Petermann, T./Bradke, H./Lüllman, A./Poetzsch, M./ Riehm, U.: Was bei einem Blackout geschieht: Folgen eines langandauernden und großräumigen Stromausfalls (Studien des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag – 33), Berlin: edition sigma 2011.; S. 67.

„In landwirtschaftlichen Betrieben beginnt ein Massensterben"

Reichenbach, G./Göbel, R./Wolff, H./von Neuforn, S.: Risiken und Herausforderungen für die Öffentliche Sicherheit in Deutschland. Szenarien und Leitfragen. Grünbuch des Zukunftsforums Öffentliche Sicherheit, Berlin, 2008.

„Nahrungsmittel für Kleinkinder können nur noch eingeschränkt bereitgestellt werden"

Menski, U./Gardemann,J.: Auswirkungen des Ausfalls Kritischer Infrastrukturen auf den Ernährungssektor am Beispiel des Stromausfalls im Münsterland im Herbst 2005, 2008.

Krankenhausversorgung bei Stromausfall

Laut einer Umfrage des deutschen Krankenhausinstituts sind 14% der Krankenhäuser bei einem mehrtägigen Stromausfall noch zu einer vollen Versorgung ihrer Patienten in der Lage.

DKI Deutsches Krankenhaus Institut: DKI Krankenhaus-Pool, 2022. URL: https://www.bdpk.de/fileadmin/user_upload/BDPK/Service/Studien/2022/2022_10_13_Krankenhaus-Pool_Moegliche_Ausfaelle_der_Energieversorgung_und_Notfallplaene.pdf Stand 15.12.2022].

Höhne, C./Lenz, K.: Was tun bei einem Stromausfall im Krankenhaus. In: Deutsches Ärzteblatt, Jg. 116, Heft 44, 1. November 2019.

„Mehrstündige Stromausfälle, die auf ein kleines Gebiet, zum Beispiel wenige Straßenzüge, beschränkt sind, treten in Deutschland fast täglich auf."

Bundesnetzagentur: Kennzahlen der Versorgungsunterbrechungen Strom, 2022. ULR: https://www.bundesnetzagentur.de/DE/Fachthemen/ElektrizitaetundGas/Versorgungssicherheit/Versorgungsunterbrechungen/Auswertung_Strom/start.html,2021. [Stand 08.12.2022].

Informationen zu rollierenden Abschaltungen / kontrollierten Brownouts

Kontrollierte Abschaltungen sind geregelt in der Verordnung zur Sicherung der Elektrizitätsversorgung in einer Versorgungskrise (Elektrizitätssicherungsverordnung - EltSV).

3 Welche Ursachen für Blackouts und andere Stromausfälle bestehen?

Risiken durch Naturereignisse wie Wetterextreme

Panteli/Mancarella weisen darauf hin, dass Extremwetterereignisse einen signifikanten Einfluss auf die kritische Infrastruktur der Stromversorgung haben, und dass es mit der durch den Klimawandel zunehmenden Häufigkeit, Schwere und Dauer solcher Ereignisse wichtiger wird, die Resilienz des Stromnetzes zu erhöhen:

Panteli, M./Mancarella, P.: *Influence of extreme weather and climate change on the resilience of power systems: Impacts and possible mitigation strategies*. Electric Power Systems Research, Volume 127, 2015, pp. 259 – 270.

Im Falle eines Stromausfalls versuchen die Netzbetreiber, die Destabilisierung weiterer Teile des Netzes zu verhindern und die Versorgung (…)

50Hertz Transmission GmbH, Amprion GmbH, Tennet TSO GmbH, TransnetBW GmbH (Hrsg.): *Netzwiederaufbaukonzepte vor dem Hintergrund der Energiewende, 2020.*

2003 waren sogar 95% Italiens mehrere Stunden ohne Strom

Union for the Co-ordination of the Transmission of Electricity (UCTE, Hrsg.): *Final Report of the Investi-gation Committee on the 28 September 2003 Blackout in Italy*, 2004. ULR: https://eepublicdownloads.entsoe.eu/clean-documents/pre2015/publications/ce/otherreports/20040427_UCTE_IC_Final_report.pdf [Stand 08.12.2022].

UCTE 2006 Union for the Co-ordination of the Transmission of Electricity (UCTE, Hrsg.): *Final Report – System Disturbance on 4 November 2006*, 2006.

Bundesnetzagentur: *Bericht über die Systemstörung im deutschen und europäischen Verbundsystem am 4. November 2006*, 2007. ULR: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/Netzreserve/Bericht_9.pdf [Stand 08.12.2022].

„In Deutschland konnten im Jahr 2005 Strommasten in Münster den Schnee auf den Leitungen nicht mehr tragen – die Menschen in der Region waren zum Teil mehrere Tage ohne Strom."

Menski, U./Gardemann, J.: *Schneechaos und Stromausfall im Münsterland vom November und Dezember 2005: Auswirkungen auf den Ernährungs- und Gesundheitssektor sowie die private Katastrophenvorsorge und Bevorratung*. In: Das Gesundheitswesen 2009, 71(06), S. 349 – 350.

„In der Ukraine führte im Jahr 2015 ein Cyber-Angriff zu einem mehrstündigen Stromausfall, von dem mehrere hunderttausend Menschen betroffen waren"

Whitehead et al. 2017 Whitehead, D./Owens, K./Gammel, D./Smith, J.: *Ukraine Cyber-Induced Power Outage:* Analysis *and Practical Mitigation Strategies*. In: 70th Annual Conference for Protective Relay Engineers (CPRE), 2017.

Folgen einen Sonnensturms

Eastwood, J.P., Biffis, E., Hapgood, M.A., Green, L., Bisi, M.M., Bentley, R.D., Wicks, R., McKinnell, L.-A., Gibbs, M. and Burnett, C.: *The Economic Impact of Space Weather: Where Do We Stand? Risk Analysis*, 2017, 37: 206-218. ULR: https://doi.org/10.1111/risa.12765.

„In der aktuellen Situation ist in Deutschland das Risiko eines Blackouts aufgrund einer Unterversorgung mit Energie gering“

Bundesnetzagentur: *Stromnetz*, 2022. ULR: https://www.bundesnetzagentur.de/DE/Fachthemen/ElektrizitaetundGas/Versorgungssicherheit/Stromnetz/start.html [Stand 08.12.2022].

„Im Falle eines Stromausfalls versuchen die Netzbetreiber, die Destabilisierung weiterer Teile des Netzes zu verhindern und die Versorgung im betroffenen Gebiet schnellst möglich wieder herzustellen. Die notwendigen Maßnahmen sind in Netzwiederaufbauplänen festgelegt und werden durch regelmäßige Trainings, in denen verschiedene Störungsszenarien simuliert werden, eingeübt.“

Consentec: *Bericht für die deutschen Übertragungsnetzbetreiber*, 2020. URL: https://www.netztransparenz.de/portals/1/Content/Weitere%20Ver%C3%B6ffentlichungen/Consentec_%C3%9CNB_NWA_Abschlussb_20200707.pdf [Stand 15.12.2022].

Hintergrundinformationen zum europaweiten Day-Ahead-Stromhandel:

Verband Europäischer Übertragungsnetzbetreiber (entsoe): *Single Day-ahead Coupling (SDAC)*, 2022. ULR: https://www.entsoe.eu/network_codes/cacm/implementation/sdac/ [Stand 08.12.2022].

4 Ist ein Blackout aufgrund der Energiekrise zu befürchten?

„In der aktuellen Situation ist in Deutschland das Risiko eines Blackouts aufgrund einer Unterversorgung mit Energie gering.“

Einschätzung der Bundesnetzagentur:

„Ein großflächiger Blackout ist äußerst unwahrscheinlich. Das elektrische Energieversorgungssystem ist mehrfach redundant ausgelegt und verfügt über zahlreiche Sicherungsmechanismen, die selbst bei größeren Störungsereignissen einen völligen Zusammenbruch des Übertragungsnetzes verhindern sollen. Die Sicherungsmechanismen werden kontinuierlich auf ihre Eignung geprüft und bei Bedarf angepasst.“

Bundesnetzagentur: *Stromnetz*, 2022. ULR: https://www.bundesnetzagentur.de/DE/Fachthemen/ElektrizitaetundGas/Versorgungssicherheit/Stromnetz/start.html [Stand 08.12.2022].

5 Welche Blackout-Risiken bestehen in Zukunft?

Die mögliche Ausgestaltung der zukünftigen klimaneutralen Energieversorgung wird in verschiedenen Energieszenarien untersucht, zum Beispiel:

Ausfelder et al.: *Sektorkopplung« – Untersuchungen und Überlegungen zur Entwicklung eines integrierten Energiesystems,* Schriftenreihe Energiesysteme der Zukunft, München 2017.

„Während des Ausbaus der erneuerbaren Energien auf 45% der Nettostromerzeugung hat sich die Versorgungsqualität nicht verringert."

Bundesnetzagentur, Bundeskartellamt: *Monitoringbericht 2022*, 2022, S. 160. ULR: https://www.bundesnetzagentur.de/SharedDocs/Mediathek/Monitoringberichte/MonitoringberichtEnergie2022.pdf?__blob=publicationFile&v=3 [Stand 15.12.2022].

Folgende Definition für „Digitalisierung der Stromversorgung" liegt den Untersuchungen zugrunde:

"Digitalisierung beschreibt das anhaltende Fortschreiten der auf Informations- und Kommunikationstechnologien (IKT) beruhenden Vernetzung von Anwendungen, Prozessen, Akteuren und von mit Sensorik und Aktorik versehenen Geräten oder Objekten der physikalischen Welt. Darüber hinaus beinhaltet Digitalisierung das Erfassen, Verarbeiten, Austauschen und Analysieren von Informationen und Daten in allen Wertschöpfungsstufen und über verschiedene Wertschöpfungsstufen der Stromversorgung hinweg."

Mayer, C./Brunekreeft, G. (Hrsg.): *Resilienz digitalisierter Energiesysteme. Blackout-Risiken verstehen, Stromversorgung sicher gestalten* (Schriftenreihe Energiesysteme der Zukunft), 2020, S. 22.

Die verschiedenen Entwicklungen und Trends der Digitalisierung (beispielsweise Künstliche Intelligenz, digitale Plattformen, Cloud Computing, Big Data, Internet der Dinge, Distributed Ledger Technology) und deren Bedeutung für das Energiesystem werden detailliert beschrieben in Mayer/Brunekreeft 2020, S. 52-72.

„Die geschilderte Dezentralisierung und die zunehmende Digitalisierung des Energiesystems wirken sich auch auf das Risiko eines Blackouts aus"

Die Risikoursachen für Blackouts im digitalisierten Energiesystem werden in der Stellungnahme und Analyse der ESYS-Arbeitsgruppe „Resilienz digitalisierter Energiesysteme" detailliert beschrieben:

acatech – Deutsche Akademie der Technikwissenschaften, Nationale Akademie der Wissenschaften Leopoldina, Union der deutschen Akademien der Wissenschaften (Hrsg.): *Resilienz digitalisierter Energiesysteme. Wie können Blackout-Risiken begrenzt werden?* (Schriftenreihe zur wissenschaftsbasierten Politikberatung), 2021. S. 21 -24.

Mayer, C./Brunekreeft, G. (Hrsg.): *Resilienz digitalisierter Energiesysteme. Blackout-Risiken verstehen, Stromversorgung sicher gestalten* (Schriftenreihe Energiesysteme der Zukunft), 2021, S. 84-91.

„Elektrische Verbraucher, vom Fahrzeug über die Wärmepumpe bis zum Kühlschrank, die zunehmend durch das Internet ansprechbar sind"

Man bezeichnet dies als Internet of Things

Vermesan, O./Bacquet, J. (Hrsg.): Next Generation Internet of Things, Distributed Intelligence at the Edge and Human Machine-to-Machine Cooperation, River Publishers 2018.

Staatstrojaner

The Economist: *Offering software for snooping to governments is a booming business*, 2019. URL: https://www.economist.com/business/2019/12/12/offering-software-for-snooping-to-governments-is-a-booming-business [Stand: 26.06.2020].

„Ein Blackout-verursachender Angriff auf IKT-Systeme erfordert erhebliche finanzielle und personelle Ressourcen."

World Energy Council: *Perspectives – The road to resilience,* 2016. ULR: https://www.worldenergy.org/assets/downloads/20160926_Resilience_Cyber_Full_Report_WEB-1.pdf [Stand 15.12.2022].

Hybride Kriege mit Cyber-Angriffen auf die Energieversorgung:

McGraw, G.: *Cyber War is Inevitable (Unless We Build Security In)*. In: Journal of Strategic Studies, 36: 1; 2013, S. 109 - 119.

6 Was tun?

„Es bestehen erhebliche Überkapazitäten bei den Kraftwerken“

Zwar ist Deutschland seit einigen Jahren in einigen Stunden des Jahres auf Importe angewiesen - doch ist dies im Wesentlichen, um die Lastdeckung marktbasiert zu erreichen. Reservekraftwerke stehen zusätzlich zur Verfügung. Der Jahreshöchstlast in Deutschland von 81,4 GW in 2021 stand eine Kraftwerksleistung von 238,4 GW gegenüber, davon über 100 GW gesicherte Leistung.

Bundesnetzagentur/Bundeskartellamt 2022: *Monitoringbericht 2022*. URL: https://www.bundesnetzagentur.de/SharedDocs/Mediathek/Monitoringberichte/MonitoringberichtEnergie2022.pdf [Stand 15.12.2022].

„Teile der Reserveleistung werden dabei bewusst auch ohne digitale Kommunikation bereitgestellt.“

Reserveleistung auch ohne Kommunikationsanbindung gilt besonders für die Primärregelung (FCR): Die Bereitsteller von FCR können in kürzester Zeit auf größere Abweichungen der Stromfrequenz reagieren auch ohne dass eine Anforderung durch den Übertragungsnetzbetreiber erfolgt.

Informationen zu den Mindestanforderungen an die Kommunikationsanbindung für Anbieter von Regelenergie:

Verband Europäischer Übertragungsnetzbetreiber: *IT-Mindestandforderungen des Reserveanbieters zur Erbringung von Regelreserve*, 2022. https://www.regelleistung.net/ext/download/minAnforderungInformationstechnikSrl [Stand 16.12.2022].

Informationen zu Maßnahmen der Netzbetreiber zur Sicherung der hohen Versorgungsqualität:

Verband Europäischer Übertragungsnetzbetreiber (entsoe): *System Operations Reports*. ULR: https://www.entsoe.eu/publications/system-operations-reports [Stand 08.12.2022].

Konzept der Resilienz

Kröger, W.: *Achieving Resilience of Large-Scale Engineered Infrastructure Systems*. In: Noroozinejad Farsangi, E./Takewaki I./Yang T./Astaneh-Asl A./Gardoni P. (Hrsg.): Resilient Structures and Infrastructure, Singapore: Springer 2019, S. 289–313.

7 Handlungsfelder

„Im Falle eines größeren Stromausfalls können dezentrale Anlagen im Notbetrieb eine regionale Versorgung innerhalb eines Netzgebietes im sogenannten „Inselbetrieb“.“

M. Braun, C. Hachmann and J. Haack: *Blackouts, Restoration, and Islanding: A System Resilience Perspective*. In *IEEE Power and Energy Magazine*, vol. 18, no. 4, pp. 54-63, July-Aug. 2020, doi: 10.1109/MPE.2020.2986659.

„Lokal sollte das Versorgungssystem in die Lage versetzt werden, ohne zentrale Steuereinheit auszukommen und durch Selbstorganisation ähnlich dem Betrieb des Internets durch Kommunikation von Knoten zu Knoten betriebsbereit zu bleiben.“

Einen Überblick über solche Konzepte gibt:

T. Strasser et al., „A Review of Architectures and Concepts for Intelligence in Future Electric Energy Systems,“ in IEEE Transactions on Industrial Electronics, vol. 62, no. 4, pp. 2424-2438, April 2015, doi: 10.1109/TIE.2014.2361486.

„Ist die Steuerung hingegen teilweise in Hardware oder elektrotechnischen Komponenten implementiert, kann dies später dazu führen, dass eine große Anzahl dezentraler Anlagen an ihrem jeweiligen Standort nachgerüstet werden müssen.“

Ein Beispiel dafür ist das sogenannte 50,2-Hertz-Problem: In der Annahme, dass es zukünftig immer bei einem nur geringen Photovoltaik-Ausbau bleiben würde, verabschiedete der verantwortliche Verband der Netzbetreiber (VDN)2005/2006 eine Regel, der zufolge sich Photovoltaik-Anlagen bei einem Überangebot an Strom (gemessen an einem Frequenzanstieg über 50,2 Hertz) spontan abschalten müssen. Alle Photovoltaik-Anlagen hatten dieses Verhalten fest implementiert. Schalten sich dabei jedoch viele Anlagen ab, führt dies zu einem Leistungsverlust, der die zu hohe Einspeisung massiv überkompensiert. Als Reaktion darauf wurde 2012 mit der Systemstabilitätsverordnung vorgeschrieben, dass die Photovoltaik-Anlagen umgerüstet werden müssen. Dies erforderte einen jahrelangen Prozess. Zudem gab es in diesem Zeitraum das Risiko, dass die Photovoltaik-Anlagen das System in speziellen Situationen destabilisieren.

Siehe dazu

Bdew: *50,2-Hertz-Problem: Allgemeine Informationen*, 2012. URL: https://www.bdew.de/energie/systemstabilitaetsverordnung/502-hertz-problem/ [Stand 16.12.2022].

„Dies sind beispielsweise Hersteller von Produkten mit digitalen Komponenten, zu denen bereits EU-Verordnungen in Vorbereitung sind.“

EU-Verodnung EG Nr. 0359/2020 des Europäischen Parlaments und des Rates vom 16. Dezember.2020 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148.

EU-Verodnung EG Nr. 0272/2022 des Europäischen Parlaments und des Rates vom 15. September 2022 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020.

„Einige neuartige Angriffe auf die Stromversorgung lassen sich voraussichtlich sogar nur abwehren, wenn KI in die dezentralen Anlagen integriert wird."

Eric MSP Veith, Lars Fischer, Martin Tröschel, and Astrid Nieße: Analyzing Cyber-Physical Systems from the Perspective of Artificial Intelligence, 2020, S. 91f. In Proceedings of the 2019 International Conference on Artificial Intelligence, Robotics and Control (AIRC '19). Association for Computing Machinery, New York, NY, USA, pp. 85–95. https://doi.org/10.1145/3388218.3388222.

Ein Teil des Einsatzes von KI unmittelbar in der Energieversorgung wird europäisch reguliert werden:

EU-Verordnung EG Nr. 0106/2021 des Europäischen Parlaments und des Rates vom 21.04.2021 zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union.

„Auf europäischer und nationaler Ebene gibt es bereits umfangreiche Maßnahmen zur Erhöhung der IT-Sicherheit"

Bundesgesetz Nr. 2034 des Bundestages vom 26. August 2016 zur Digitalisierung der Energiewende, Bundesgesetzblatt Jahrgang 2016 Teil I Nr. 43 vom 1.09.2016.

EU-Verordnung EG Nr. 943/2019 des Europäischen Parlaments und des Rates vom 05. Juni 2019 über den Elektrizitätsbinnenmarkt, Amtsblatt der Europäischen Union (ABl.) Nr. L 158/54 vom 14.06.2019.

Unternehmen im besonderen öffentlichen Interesse (UBI) sind ab dem 01. Mai 2023 verpflichtet eine Selbsterklärung zur IT-Sicherheit vorzulegen und mindestens alle zwei Jahre zu erneuern. Welche Unternehmen als UBI gelten, ist im Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) geregelt.
https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Weitere_regulierte_Unternehmen/UBI/ubi_node.html

EU-Verordnungen in Vorbereitung

Die Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, auch als Network and Information Security (NIS 2) -Richtlinie bezeichnet, wurde am 27. Dezember 2022 im EU-Amtsblatt veröffentlicht und wird am 16. Januar 2023 in Kraft treten. Ab diesem Zeitpunkt haben die Mitgliedstaaten 21 Monate Zeit, um die Richtlinie in nationales Recht überzuführen.
https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555&from=EN#d1e40-80-1.

Die Richtlinie über die Resilienz kritischer Einrichtungen wurde ebenfalls am 27.12. im EU-Amtsblatt veröffentlicht. Auch für diese Richtlinie besteht eine Umsetzungspflicht innerhalb von 21 Monaten für die Mitgliedstaaten.
https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2557&from=DE

Ebenfalls relevant für IKT-Produkte ist die derzeit im Verabschiedungsprozess stehende Verordnung über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen (auch als Cyber Resilience Act bezeichnet):
https://eur-lex.europa.eu/procedure/EN/2022_272

„Staaten und ihre Sicherheitsbehörden haben Interesse daran, dass Lücken in der IT-Sicherheit verbleiben. Dahinter steht die Annahme, dass auf diese Weise kriminelle Aktivitäten wirksamer ausgespäht oder nachgewiesen werden könnten."

siehe z.B.

Bundeskriminalamt (BKA): *Quellen-TKÜ und Online-Durchsuchung,* 2022. URL: https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung_node.html [Stand 08.12.2022].

„Nutzen sehr viele Haushalte in einem kleinen Gebiet gleichzeitig elektrische Heizlüfter, kann dies zu Schutzabschaltungen im Niederspannungsbereich und damit zu einem lokal begrenzten Stromausfall führen.":

BDEW Bundesverband der Energie- und Wasserwirtschaft e.V.: *Fakten und Argumente Heizlüfter, Strom-Radiatoren und Co.*, 2022. URL: https://www.swa-netze.de/fileadmin/Downloadfiles/Sonstig/bdew/BDEW_Fakten_Argumente_Heizluefter-Heizungsalternativen_2-8-2022.pdf [Stand 15.12.2022].

Tagesspiegel: *Blackout-Gefahr: Netzagentur warnt vor Einsatz von Heizlüftern*, 2022. URL: https://www.tagesspiegel.de/politik/blackout-gefahr-netzagentur-warnt-vor-einsatz-von-heizluftern-8630299.html [Stand 08.12.2022].

Empfohlene Zitierweise

acatech/Leopoldina/Akademienunion (Hrsg.): *„Sind Blackouts in Deutschland wahrscheinlich?* (Impuls)“, Akademienprojekt „Energiesysteme der Zukunft” (ESYS), 2023, https://doi.org/10.48669/ESYS_2023-1

Die Publikation basiert auf der Stellungnahme *„Resilienz digitalisierter Energiesysteme. Wie können Blackout-Risiken begrenzt werden*“ (https://energiesysteme-zukunft.de/digitalisierung)

Kernteam

Dr. Christoph Mayer (OFFIS – Institut für Informatik), Dr. Berit Erlach (ESYS Koordinierungsstelle | acatech), Prof. Dr.-Ing. Manfred Fischedick (Wuppertal Institut für Klima, Umwelt, Energie GmbH), Prof. Dr. Hans-Martin Henning (Fraunhofer-Institut für Solare Energiesysteme ISE), Prof. Dr. Ellen Matthies (Otto-von-Guericke-Universität Magdeburg), Prof. Dr. Karen Pittel (ifo Institut), Prof. Dr. Jürgen Renn (Max-Planck-Institut für Wissenschaftsgeschichte), Prof. Dr. Dirk Uwe Sauer (RWTH Aachen), Prof. Dr. Indra Spiecker genannt Döhmann (Goethe-Universität Frankfurt am Main), Dr. Cyril Stephanos (ESYS Koordinierungsstelle | acatech)

Weitere Mitwirkende

Christiane Abele (ESYS Koordinierungsstelle | acatech), Benedikte Eiden (ESYS Koordinierungsstelle | acatech), Anja Lapac (ESYS Koordinierungsstelle | acatech), Annika Seiler (ESYS Koordinierungsstelle | acatech)

Reihenherausgeber

acatech – Deutsche Akademie der Technikwissenschaften e. V. (Federführung)
Koordinierungsstelle München, Karolinenplatz 4, 80333 München | www.acatech.de

Deutsche Akademie der Naturforscher Leopoldina e. V.
– Nationale Akademie der Wissenschaften –
Jägerberg 1, 06108 Halle (Saale) | www.leopoldina.org

Union der deutschen Akademien der Wissenschaften e. V.
Geschwister-Scholl-Straße 2, 55131 Mainz | www.akademienunion.de

DOI

https://doi.org/10.48669/esys_2023-1

Projektlaufzeit

03/2016 bis 12/2023

Finanzierung

Das Projekt wird vom Bundesministerium für Bildung und Forschung (Förderkennzeichen 03EDZ2016) gefördert.

Die Akademien danken allen Mitwirkenden für ihre Beiträge. Die Inhalte des Impulses liegen in alleiniger Verantwortung der Akademien.

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

Das Akademienprojekt „Energiesysteme der Zukunft“

Mit der Initiative „Energiesysteme der Zukunft“ (ESYS) geben acatech – Deutsche Akademie der Technikwissenschaften, die Nationale Akademie der Wissenschaften Leopoldina und die Union der deutschen Akademien der Wissenschaften Impulse für die Debatte über Herausforderungen und Chancen der Energiewende in Deutschland. Im Akademienprojekt erarbeiten mehr als 100 Fachleute aus Wissenschaft und Forschung in interdisziplinären Arbeitsgruppen Handlungsoptionen zur Umsetzung einer sicheren, bezahlbaren und nachhaltigen Energieversorgung.

Kontakt:

Dr. Cyril Stephanos
Leiter der Koordinierungsstelle „Energiesysteme der Zukunft“
Pariser Platz 4a, 10117 Berlin
Tel.: +49 30 206 30 96 - 0
E-Mail: stephanos@acatech.de
web: energiesysteme-zukunft.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