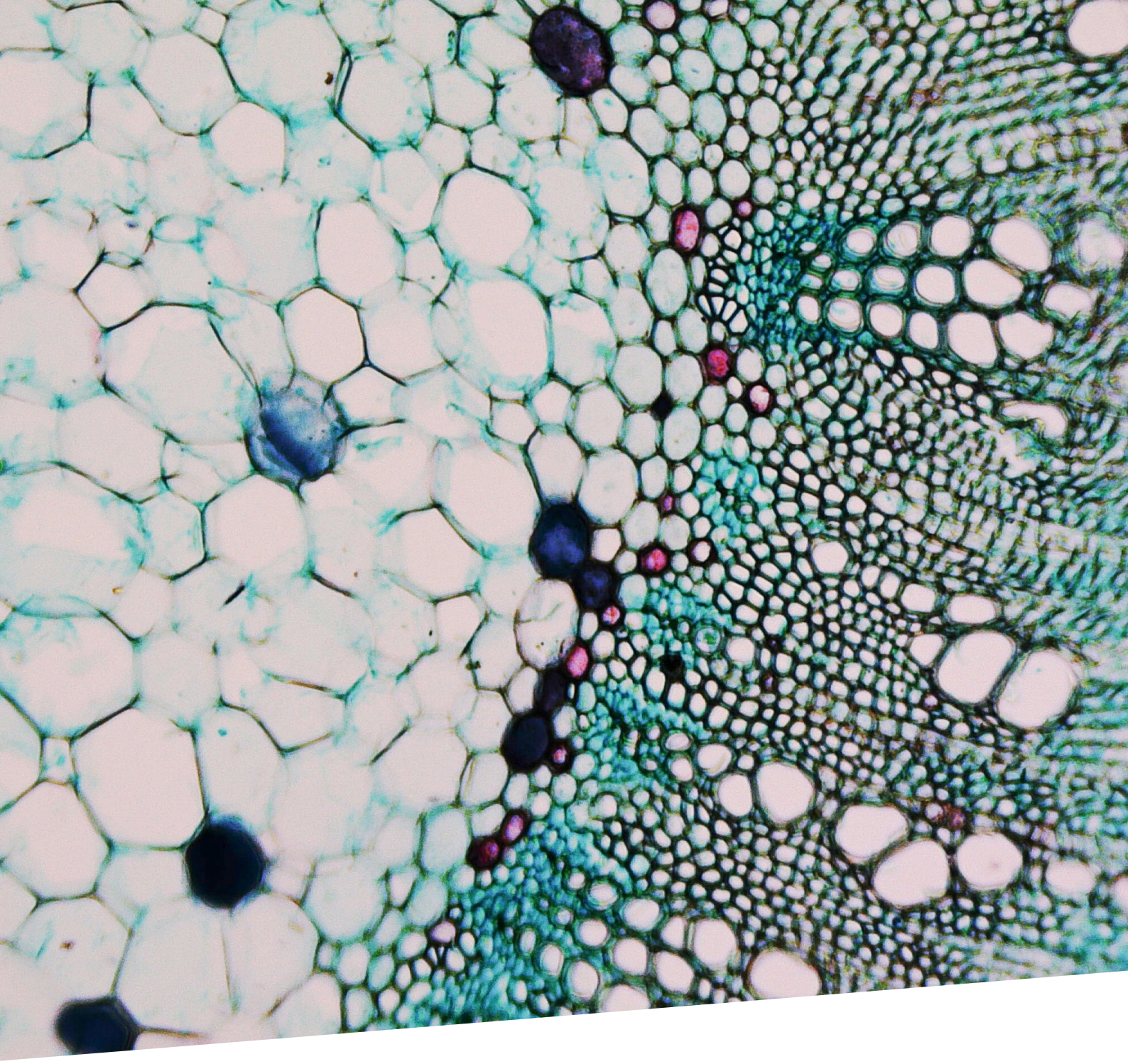

Ausfallsicherheit des Energieversorgungssystems – Von der Robustheit zur Resilienz

Diskussionspapier

www.bitkom.org

bitkom

Herausgeber

Bitkom
Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e. V.
Albrechtstraße 10 | 10117 Berlin
T 030 27576-0
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner

Robert Spanheimer | Bitkom e. V.
T 030 27576-204 | r.spanheimer@bitkom.org

Satz & Layout

Kea Schwandt | Bitkom e. V.

Titelbild

© Claudio Divizia – fotolia.de

Inhaltsverzeichnis

1 Zusammenfassung für Entscheidungsträger

Das Energieversorgungssystem ist von fundamentaler Bedeutung für die Gesellschaft und damit ohne Frage eine kritische Infrastruktur: Ein Ausfall oder eine bloße Beeinträchtigung der Energieversorgung führen zu nachhaltig wirkenden Versorgungsengpässen und erheblichen Störungen der öffentlichen Ordnung und Sicherheit. Im Folgenden steht der Energiesektor, speziell die Stromversorgung im Fokus, weil Störungen sich schnell und überregional ausbreiten. Ferner ist Elektrizität schlecht substituierbar, insbesondere auch in anderen Netzinfrastrukturen, so ist zum Beispiel Telekommunikation ohne Versorgung mit Strom nicht uneingeschränkt funktionsfähig.

Die wichtigste Anforderung an eine kritische Infrastruktur ist ihre Ausfallsicherheit. In der bisherigen Energiewelt wurde dies erreicht, indem das Stromversorgungssystem robust ausgelegt wurde. Man bezeichnet ein technisches System als robust, wenn es die meisten voraussehbaren Störereignisse bewältigt, ohne dass seine Funktionsfähigkeit wesentlich beeinträchtigt wird. Das Stromversorgungssystem leistet dies unter anderem durch das sogenannte N-1-Prinzip: Jedes wesentliche elektrizitätstechnische Element im System gibt es einmal mehr als für die Höchstlast im Normalbetrieb nötig wäre. Wenn ein Stromerzeuger, eine Leitung oder ein Transformator ausfällt, übernimmt ein anderes Element die relevante Funktion, ohne dass es zu großen Beeinträchtigungen kommt. Das deutsche Stromsystem hat in der Vergangenheit seine Robustheit immer wieder eindrucksvoll bewiesen. Gemessen am internationalen Index für die durchschnittliche Ausfalldauer, ist die deutsche Stromversorgung eine der zuverlässigsten der Welt. Sie steht nun allerdings vor neuen Herausforderungen.

Aus drei Gründen lässt sich das bisherige Redundanzprinzip der bisherigen Energiewelt schon heute nicht mehr immer durchgehend einhalten:

1. Die Energiewende: Sonne und Wind entwickeln sich mehr und mehr zum Rückgrat der Stromerzeugung. Damit einher geht die Vervielfachung der dezentralen Erzeugungsanlagen, was dazu führen wird, dass nicht alle Erzeugungsanlagen redundant angebunden werden können.

2. Die Sektorenkopplung bedeutet eine Vielzahl neuer Verbraucher im Wärme- und Verkehrssektor.

3. Die Digitalisierung von Netz, Vertrieb und bei Endverbrauchern ist notwendig, um die beiden vorhergehenden Herausforderungen zu bewältigen. Es wird zum Beispiel nur durch Digitalisierung möglich sein, die künftige Vielzahl von Erzeugungsanlagen zeitnah zu prognostizieren und zu steuern. Dezentrale Intelligenz ist eine Antwort auf zunehmende Komplexität. Der Umbau der Energiewirtschaft und die Digitalisierung der Netze bedingen einander daher. Verzögerungen bei der Bereitstellung sicherer IT-Systeme verschärfen eine potenzielle Cyberbedrohung und verlangsamen schlussendlich die Energiewende.

Im zukünftigen Stromversorgungssystem ist deshalb Resilienz der effektivste Weg um Ausfallsicherheit zu erreichen, denn die bisherige Robustheit lässt sich aufgrund der veränderten Struktur nicht eins zu eins fortführen. Resilienz ist daher die beste Versicherung für die Energieversorgung der Zukunft gegenüber Belastungen mit potenziell großen Schäden, die sich sowohl schlecht quantifizieren und prognostizieren lassen und überraschend eintreffen.

Resilienz ist dabei definiert als die Fähigkeit eines Systems, seine Funktionsfähigkeit unter Belastungen aufrechtzuerhalten beziehungsweise kurzfristig wiederherzustellen.

Resilienz geht über die Eigenschaft der Robustheit hinaus. Man bezeichnet ein System als resilient, wenn seine Funktionsfähigkeit bei Störungen nur wenig beeinträchtigt wird, es zu keinen größeren Schäden kommt und nach der Störung so schnell wie möglich wieder die volle Leistung zur Verfügung steht.

Es sind erhebliche Anstrengungen erforderlich, um angesichts dieser Herausforderungen der Energiewende und Sektorenkopplung auch weiterhin Stabilität und Qualität der Stromversorgung gewährleisten zu können. Hierbei kommt der Cyber-Resilienz (»safe-to-fail«) eine Schlüsselrolle zu, da die in der Vergangenheit bewährten, auf Robustheit setzenden Konzepte (»fail-safe«) zusehends an ihre Grenzen stoßen. Das Energiesystem sollte befähigt werden, auf unvorhergesehene Störungen derart zu reagieren, dass es dennoch seine grundlegende Funktionsfähigkeit erhalten oder sie zumindest eigenständig wiedererlangen kann, so dass sich die Folgen etwaiger Störungen auf ein Minimum begrenzen. Für diese Selbstorganisation ist es unumgänglich, die Informations- und Kommunikationstechnologie als integralen Bestandteil des Stromsystems zu begreifen und das Potential der Digitalisierung für die Erhöhung seiner Resilienz voll auszuschöpfen. Dank Informations- und Kommunikationstechnologie kann das Stromsystem den drei skizzierten Herausforderungen von Energiewende, Sektorenkopplung und Cyber-Bedrohung Stand halten, seiner Bedeutung als kritischer Infrastruktur gerecht werden und somit auch in Zukunft zu den zuverlässigsten Stromsystemen der Welt gehören.

2 Chancen und Risiken der Digitalisierung von Energienetzen

Für die Herausforderungen, die direkten Bezug zur Digitalisierung der kritischen Infrastruktur Energie haben, sind drei Entwicklungen maßgeblich:

1. Der Umbau des Energiesystems

Die Energieversorgung der Zukunft basiert vor allem auf Wind und Sonne und damit auf Millionen von Erzeugungsanlagen statt nur einiger weniger hundert größerer Kraftwerke. Hinzu kommt, dass die Erzeugung wetterbedingt schwankt und sowohl dezentral verteilt wie bei Photovoltaik-Dachanlagen oder räumlich stark konzentriert wie bei der Offshore-Windenergie auftreten kann. Wenn zukünftig ein hoher Anteil der Stromerzeugung dezentral im Nieder- und Mittelspannungsnetz aus schwankendem Quellen erfolgt, können hochgerechnet aus historischen Wetterdaten extreme Schwankungen bei der Erzeugungsleistung auftreten. Die daraus erwachsenden starken Veränderungen der Leistung in der Zeit müssen geregelt werden können. Das bedeutet sowohl hohe benötigte Regelgeschwindigkeit (hohe zeitliche Auflösung) als auch hohe örtliche Auflösung (um Spannungsgradienten innerhalb eines Verteilnetzstrangs auszuregeln). Dies gelingt nur mit weitgehender, dezentraler Automatisierung und einer Kommunikationsinfrastruktur, die noch »schneller« (geringstmögliche Latenz) sein muss als der zu fahrende Gradient. Dabei muss darauf geachtet werden, dass Automatisierung nicht selbst durch aufschwingende Eigenschaften zum Problem wird. Ein Beispiel ist das 50,2 Hertz-Problem: Viele Photovoltaikanlagen waren in der Vergangenheit so ausgelegt, dass sie sich alle bei einer Abweichung der Netzfrequenz selbst abschalteten. Durch die gleichzeitige Abschaltung gefährden sie damit als »Schwarm« selbst die Systemstabilität.

2. Sektorenkopplung

Unter Sektorenkopplung versteht man die Ausweitung der Energiewende, die bisher im Wesentlichen eine »Stromwende« ist, auf die Sektoren Wärme und Verkehr, mit dem Ziel in diesen Sektoren konventionelle, CO2-lastige Energieverbräuche durch CO2-arm erzeugten Strom oder dessen Derivate (Windgas) zu ersetzen. Auf der Nachfrageseite entsteht mit dieser Sektorkopplung eine Herausforderung für die Verteilnetze: Aktuell wird in der Elektromobilität mit Ladeleistungen zwischen 3,6 und 22 kW im Privatbereich, mit 50 kW an den meisten öffentlichen Ladepunkten und mit 100 – 150 kW an Schnellladestationen gerechnet. Durch das gleichzeitige Laden vieler Fahrzeuge in einem räumlich engen Gebiet (zum Beispiel ein städtisches Quartier oder eine Großveranstaltung) können extreme Lastspitzen entstehen. Ähnliche Lastspitzen können und werden auftreten, wenn zunehmend fossile Heizungen durch elektrische Heizungen, wie beispielsweise Wärmepumpen, die ebenfalls als Schwarm steuerbar gemacht werden können, ersetzt wird.

Sektorenkopplung verlangt die integrierte Regelung der Energiesysteme – dies kann nur digital erfolgen. Dadurch erhöht sich der Vernetzungsgrad innerhalb und zwischen den Energienetzen. Sektorenkopplung erfolgt meist lokal, bedingt also dezentrale Strukturen mit hoher örtlicher Auflösung (sensorisch und aktorisch). Hierfür müssen geeignete informationstechnische Archi-

tekturen, Geschäftsmodelle und auch Regularien entwickelt werden. Der aktuelle Trend »Big Data« führt zu Datenübermittlungen, deren Notwendigkeit und Risiken insbesondere im Kontext Energiesystem bedacht werden müssen. Aus Gründen der Systemsicherheit sind unbedingt modulare, klar strukturierte Systemarchitekturen zu entwickeln

3. Digitalisierung

Im Stromversorgungssystem wächst der Druck die Nachfrage zu flexibilisieren und Kommunikationsmöglichkeiten zwischen den Akteuren des Stromangebots und -nachfrage aufzubauen. Mit dem Fortschreiten der Digitalisierung der Energienetze steigen nicht nur die Möglichkeiten zur effizienteren Netzbetriebsweise, sondern erhöhen sich auch die Sorgen vor Cyber-Angriffen und Störungen erheblich. Das gilt auch für kritische Infrastrukturen allgemein.

Die Digitalisierung der Stromnetze, insbesondere der Verteilnetze, weist derzeit eine sehr hohe Schwankungsbreite auf. Insbesondere die unteren Netzebenen (Niederspannung und Teile der Mittelspannung) sind zu großen Teilen noch nicht digitalisiert und dementsprechend einer Beobachtbarkeit weitgehend entzogen. Im Gegensatz hierzu sind Hoch- und Höchstspannungsnetze mit umfassender IT-gestützter Sensorik und Aktorik ausgestattet, um eine effiziente Netzführung zu ermöglichen.

Um Kosten zu reduzieren wurde im Koalitionsvertrag 2018 festgehalten, dass intelligente Steuerung gegenüber dem klassischen Netzausbau gestärkt werden soll. Durch die Nutzung von Flexibilitäten lässt sich teurer Netzausbau vermeiden. Hierbei besteht die Herausforderung darin, für die Netzbetreiber in einer solchen »intelligenten Welt« die richtigen Anreize zu setzen. Regulierte Unternehmen unterliegen dem sogenannten Averch-Johnson-Effekt, der in der Regel dazu führt, dass kapitalintensive (und damit qualitätsstützende) Lösungen bevorzugt werden. Diesen Effekt gilt es im Blick zu behalten und die heutigen Relationen zwischen operativen Kosten und Kapitalkosten in geeigneter Weise anzupassen. Sollen die Netzbetreiber künftig stärker auf Lösungen setzen, die mit erhöhten operativen Kosten einhergehen, muss die Regulierung hierfür Anreize schaffen.

In der Summe ergeben diese Entwicklungen eine höhere Komplexität, die nur durch Informations- und Kommunikationstechnologien beherrschbar ist. Daraus ergibt sich wie in anderen Branchen eine Tendenz zur Konvergenz von Informationstechnologie mit der klassischen (Stromnetz-)Technik. Das ist aus Sicht der Resilienz Chance wie Herausforderung.

2.1 Chancen der Digitalisierung

Die Qualität der Energieversorgung verbessert sich nicht durch Digitalisierung – die Chance liegt in digitalen Zusatzdiensten. Eine zunehmende Digitalisierung erzeugt Wissen, Flexibilität und Geschwindigkeit.

Mit Hilfe von Informations- und Kommunikationstechnologie kann das Energieversorgungssystem resilient gestaltet werden. Dazu muss zum einen die Informations- und Kommunikations-

technologie selbst durch organisatorische, personelle und technische Maßnahmen gegenüber Attacken robuster gemacht werden. Zum anderen kann sie aber vor allem zur Resilienz im eigentlichen Sinne beitragen, indem Störungen frühzeitig erkannt, Gegenmaßnahmen automatisiert eingeleitet und Systemdienstleistungen übernommen werden. In der acatech Studie Future Energy Grid wurde 2012 ein übergreifendes Szenario entwickelt, das unter anderem eine durchgehende Digitalisierung, Nachfragesteuerung, Sektorenkoppelung, europaweite Vernetzung (digital, physikalisch und regulatorisch), Systemdienstleistungen durch erneuerbare Erzeugungsanlagen, und Märkte für Kleinsttransaktionen vorsieht.

Zu den Systemdienstleistungen gehört zum Beispiel die Schwarzstartfähigkeit, also die Fähigkeit des Energiesystems nach einem kompletten Stromausfall die Versorgung wieder herzustellen. Dieser Fall zeigt exemplarisch die wechselseitige Abhängigkeit, weil über die Telekommunikationsinfrastruktur das Wiederhochfahren nach einem kompletten Ausfall koordiniert werden muss. Die Mobilfunkinfrastruktur ist auch heute schon in Teilen über Batteriespeicher an den Basisstationen schwarzfallfest. Wenn allerdings künftig die Telekommunikationsinfrastruktur unabdingbare Voraussetzung für einen Schwarzstart wird, muss deren Funktionsfähigkeit durch größere Speicher für noch längere Zeiträume erhalten werden können. Zudem wird sich mit dem bevorstehenden Rollout der 5G-Technologie die Zahl der Funkstandorte deutlich (Faktor drei bis fünf) erhöhen, sodass zusätzliche Anstrengungen erforderlich werden, sofern auch die neue Technologie geeignet abgesichert werden soll. Ein Finanzierungsrahmen für diese neue gesamtgesellschaftliche Aufgabe und eine Marktorganisation fehlen bisher.

Beispiel für Möglichkeiten der Digitalisierung in den Energienetzen:

Die Digitalisierung wirkt in den Energienetzen in unterschiedlichen Dimensionen, die sich vor allem danach unterscheiden lassen, wie zeitkritisch die Übermittlung der Daten für den betroffenen Prozess ist. Eine verbesserte Datenlage wirkt zunächst in der Planung der Netze. Hier wird es möglich, nicht nach Heuristiken zu entscheiden, sondern auf Basis tatsächlicher Belastungsdaten über Ausbaunotwendigkeiten zu befinden. Der Prozess ist aber offensichtlich nicht zeitkritisch. Ein zweiter relevanter Anwendungsfall liegt in der dem Betrieb vorlaufenden Prognose. Hier erlauben Messdaten im Verein mit anderen Werten wie etwa Wetterprognosen eine deutlich verbesserte Voraussicht und damit Sicherheit im folgenden Betrieb. Zwar müssen die Daten hier zeitnäher zur Verfügung stehen, aber auch dieser Prozess ist nicht wirklich zeitkritisch in Bezug auf die Übermittlung entsprechender Daten. Zusätzliche und verbesserte Daten, die auf Basis digitalisierter Lösungen extrem zeitnah zur Verfügung stehen wirken aber auch während des Betriebs selbst. Sie erlauben es, auf Abweichungen von der Prognose zu reagieren und so zahlreiche dargebotsgetriebene Erzeuger in die Netze einzubinden. Schließlich folgen dem Betrieb ex-post-Analysen, welche wiederum nicht zeitkritisch sind. Hier liegt der Schwerpunkt weniger auf der Aktualität, sondern auf der Detailgenauigkeit für Auswertungen. Alle vier zuvor beschriebenen Anwendungsfälle benötigen aber gegenbenenfalls den gleichen Datensatz beispielsweise einen Viertelstundenlastgang[1]. Dieser muss im Fall kritischer Betriebsmittel oder

1 Im Anwendungsfall Betrieb ist allerdings davon auszugehen, dass die Granularität der benötigten Daten auch deutlich kleiner sein kann als das hier verwandte Beispiel eines Viertelstundenlastgangs.

besonders relevanter Erzeuger aber laufend zur Verfügung stehen, während in den anderen Fällen eine tägliche Übermittlung und ggf. Archivierung des Datensatzes ausreichend sein dürfte. Zudem sind beispielsweise für die Planung gegebenenfalls Extremwerte im Lastgang viel entscheidender als dessen vollständiger Verlauf.

Neben dieser eher anwendungsfallorientieren Betrachtungsweise lässt sich die Wirkungsweise der Digitalisierung aber auch nach Technologien und technischen Lösungen differenzieren und beschreiben:

Sensorik / Aktorik

Sensoren helfen, das Verhalten der Netze zu analysieren. Ableitungen aus Messwerten unterstützen dabei Prognosen zu erzeugen und damit die Planbarkeit zu verbessern. Aktoren wiederum ermöglichen Flexibilitäten, zum Besipiel durch Abschaltung überschüssiger Energie / überschüssigem Verbrauch. Der Einsatz von Sensorik und Aktorik ermöglicht also eine flexible Optimierung von Versorgungs- und Verteilnetzen. Intelligente, fernsteuerbare Leitungsschutz-, Leistungs- und Kuppelschalter lösen mehr und mehr klassische Sicherungen ab. Durch Einsatz dieser Schalter wird es nicht nur ermöglicht, Wiederinbetriebsetzungszeiten zu reduzieren, sondern auch eine regelmäßige Überwachung / Steuerung aus der Ferne zu ermöglichen. Netztopologien können flexibel an die aktuellen Erzeugungs- und Verbrauchssituationen sowie Netzzustände angepasst werden.

Prosumer

Prosumer spielen in intelligenten Energienetzen eine große Rolle. Sie können Erzeugungsspitzen aus erneuerbaren Energien durch den Einsatz von Speichern oder gezielter Ladung von Elektrofahrzeugen aufnehmen. Aber auch bei fehlender Erzeugungsenergie können sie ihre Verbrauchsleistung durch Lastverschiebung reduzieren oder durch Speicherentladung die Erzeugung erhöhen. Durch einen Schwarmansatz können sich nicht nur einzelne Prosumer an der Resilienz beteiligen, sondern ganze Verbünde von Prosumern.

Micro Grids / Micro Smart Grids

Micro Grids und Micro Smart Grids reduzieren die Abhängigkeit von den großen Kraftwerken im Störfall. Bei Ausfällen im vorgelagerten Netz können diese zum Teil ihr eigenes kleines Netz erhalten. Bestes Beispiel hierfür sind die Sicherheitsstromversorgung im Krankenhaus oder für Rechenzentren. Damit wird Autarkie für einen kurzen Zeitraum ermöglicht.

Zukünftig könnten solche »Inselstrukturen« auch in größerem Maßstab genutzt werden und zur Resilienz beizutragen. Wesentliches Problem solcher »Inselstrukturen« ist aktuell aber das Problem a) im Fehlerfall zu erkennen, welche Bereiche noch mit Elektrizität versorgt werden und b) die jeweiligen Inseln wieder zu einem frequenzgleichen Netz zusammenzuschalten und so eine Wiederversorgung weiterer Bereiche nach einem Brown-out/Black-out zu ermöglichen.

Beide Probleme lassen sich durch den verstärkten Einsatz entsprechender Informations- und Kommunikationstechnologie mindern. Hier besteht großer Forschungsbedarf. Ferner sind auch technische Standards und Grid Codes noch auf europäischer Ebene zu definieren.

Übergreifende Sektoren / Sparten

Klassische Stadtwerke haben schon lange den Blick nicht nur auf Strom, sondern auch auf andere Sektoren wie Wasser, Gas und Wärme gerichtet. Der Einsatz von Informations- und Kommunikationstechnologie ermöglicht eine Kopplung der Sektoren. Power-to-Heat, Power-to-Gas oder Power-to-Cool sind Bereiche, die hier in den Vordergrund rücken. Gerade bei der Dezentralisierung ist ein Verbund aus unterschiedlichen Sektoren hilfreich, um Abhängigkeiten zu reduzieren, Flexibilitäten zu erhöhen und auch Speicherkapazitäten bereitzustellen. Nur die intelligente Steuerung und Regelung der Sektoren macht es möglich, die Potenziale daraus in Gänze auszuschöpfen.

Intelligente Ortsnetzstationen

Durch Einsatz intelligenter Ortsnetzstationen kann das Spannungsniveau an die aktuellen Netzsituationen angepasst werden und die Aufnahmekapazität für Erneuerbare Energien durch zeitweise Mehrbelastung der Betriebsmittel erweitert werden. Damit kann zudem der Netzausbau nicht vermieden, aber zumindest unterstützt beziehungsweise zeitlich verzögert werden.

Predictive Maintenance

Durch Predictive Maintenance, unter Berücksichtigung der möglichen Sensorwerte, kann eine zeitnahe Wartungs- und damit Kostenplanung und -ermittlung für den Betrieb abgeleitet werden (ex-ante statt ex-post), wie es oben bereits dargelegt wurde. Zum Beispiel kann durch Integration von Sensoren verteilt über alle Netzebenen hinweg, mittels modernster Big Data Technologien und Analytics Methoden eine Störungshistorie ausgewertet werden. Basis hierfür können sowohl relevante Netzdaten als auch externe Einflüsse (zum Beispiel Wetter, Jahreszeit, ...) sein. Strukturschwächen und deren Ursachen können identifiziert, geografische Aspekte betrachtet und damit verbundene Optimierungspotenziale, etwa die Verkürzung der Wiederinbetriebsetzungszeiten durch eine Veränderung der Allokation von notwendigen Betriebsmitteln, abgeleitet und transparent dargestellt werden.

2.2 Herausforderungen der Digitalisierung

Im Zuge der Energiewende wird das Stromversorgungssystem zum Leitsystem der gesamten Energieversorgung. Im Unterschied zu anderen Energiesystemen (Gas, Wärme) hat das elektrische Netz aber keine puffernde Funktion, ist also instantan und muss daher ständig in Echtzeit geregelt werden. Neben Stromspeichern (Batterien, Wasserkraft, Schwungmasse) versucht man mit Sektorenkopplung Flexibilitäten anderer Sektoren, die sich dort aus Lastverschiebung und Pufferung ergeben, zur Erleichterung der Regelung in der Stromversorgung zu nutzen.

Dieser Trend bedingt, dass die gemeinsame Systemverantwortung von Übertragungsnetzen und Verteilnetzen (one-system approach) sich zunehmend verändert. Den Verteilnetzbetreibern erwächst hierdurch zunehmend eine erweiterte Verantwortung für den Systembetrieb insgesamt. Die heutige Fahrplansteuerung, die sich im Wesentlichen auf große Erzeuger beschränkt, kommt daher an ihre Grenzen und muss dringend in das Verteilnetz ausgedehnt werden und mittelfristig durch flexible, realzeitfähige Mechanismen ergänzt werden. Die Kontrahierung sollte, wo immer möglich, über Märkte erfolgen. Die Aufgaben der Verteilnetzbetreiber verändern sich grundlegend. Diese Herausforderung haben die deutschen VNB im Rahmen der DSO 2.0 Initiative bereits aktiv aufgegriffen und beteiligen sich mit innovativen Konzepten an der Diskussion (Flexrouter-Konzept).

Schlagworte wie Internet of Things and Services, Cloud-Lösungen, künstliche Intelligenz, Ambient Intelligence und Blockchain dominieren auch die Debatte um die Entwicklung der Energiewirtschaft. Wie in anderen Branchen sind disruptive Veränderungen wahrscheinlich, weitere zusätzliche Komplexität sicher. Der direkte Stromtausch-/handel in Quartieren ist ein Beispiel. »Hinter dem Zähler« eröffnet sich eine Vielfalt von neuen Möglichkeiten, aber auch Angriffswegen. Auch die Auswirkungen auf das etablierte Bilanzierungssystem sind noch unklar. Der regulatorische Rahmen muss an die neuen Marktbedingungen angepasst werden.

Der zunehmende Einsatz vernetzter Geräte bei den Endverbrauchern bedeutet gleichzeitig auch einen Zuwachs an Angriffsvektoren - also, an Pfaden, die ein Eindringling nutzen kann, um ein fremdes System zu hacken. Digitalisierung und Cybersecurity müssen Hand in Hand gehen: Wenn Prozesse digitalisiert, vernetzte Geräte eingesetzt und Energieressourcen dezentral gesteuert werden, so müssen fachgerechte Maßnahmen der IT-Sicherheit nach Stand der Technik getroffen werden.

Der Schutz vor Cyberangriffen kann mit technischen Mitteln, wie Datenverschlüsselung, Firewalls und Virenscannern, nicht mehr allein gewährleistet werden. Vielmehr spielen organisatorische Maßnahmen, wie Zutrittskontrolle, das Gefahrenbewusstsein der Mitarbeiter und Berechtigungsstufen eine zunehmend wichtige Rolle. Die Bundesnetzagentur hat gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) einen Anforderungskatalog an IT-Sicherheitsmaßnahmen für Strom- und Gasnetze[2] erstellt. Dabei stellt die Einführung eines Informationssicherheits-Managementsystems (ISMS) nach ISO/IEC 27001 und 27019 und dessen Zertifizierung durch eine unabhängige Instanz eine Kernforderung dar. Ein ISMS begreift die IT-Sicherheit als einen Prozess, der alle Bereiche durchdringt: technische Maßnahmen und organisatorische Verfahren werden festgelegt und umgesetzt, praktische Erfahrungen werden gesammelt und kritisch bewertet, gegebenenfalls Korrekturmaßnahmen eingeleitet.

Die Technik entwickelt sich immer weiter. Deshalb müssen die IT-Sicherheitsmaßnahmen, die im Rahmen eines ISMS implementiert werden, kontinuierlich geprüft und aktualisiert werden. Dies

2 ↗https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheitskatalog_08-2015.pdf?__blob=publicationFile&v=2

dient nicht nur dazu, Sicherheitsdefizite zu beheben, sondern auch das Potenzial neuer technologischer Entwicklungen zu erschließen. So bietet zum Beispiel die automatische Erkennung von Anomalien in Netzwerkdaten mithilfe des maschinellen Lernens neue Möglichkeiten der Gefahrenabwehr im Cyberraum.

Neue Angriffsszenarien / Bedrohungslage

Das Zeitalter des »Internet der Dinge« bricht an. Der Digitalisierungstrend durchdringt alle Lebensbereiche. Im Smart Home-Bereich werden Geräte mit dem Internet vernetzt. In der Industrie 4.0 wird die Fabrik digitalisiert. Im Bereich der E-Mobility kommunizieren Autos miteinander oder mit ihren jeweiligen Flottenkoordinatoren. Geräte und Anlagen, die als Teil des Energiesystems betrachtet werden, sind bereits heute und in Zukunft noch viel stärker über das Internet erreichbar. Auch die Systeme, die eigentlich »hinter« einem Smart Meter Gateway (SMGW) liegen sollten (Smart Home Devices, Consumer Electronics) werden mit eigenem Internetzugang ausgeliefert und ignorieren insofern weitgehend die bisherigen Arbeiten des BSI und der Branche an einer sicheren Kommunikation mit Hilfe der Smart Meter Gateways. Dadurch unterliegen sie steuernden Einflüssen des Nutzers oder dritter Vertragspartner, die sich allein an bestimmten Preissignalen (etwa dem Börsenpreis) orientieren und dabei etwaige externe Effekte zu Lasten des Energiesystems insgesamt (beispielsweise einen entstehenden Netzengpass) ignorieren.

Da die hundertprozentige Absicherung jedes angeschlossenen Gerätes und jeder Anlage nicht möglich ist, muss das System als Ganzes über wirksame Erkennungs- und Abschottungsmechanismen für Angriffe und Ausfälle verfügen. Dies gilt insbesondere für Geräte im unteren Preissegment. Manchmal werden selbst einfache Sicherheitsmaßnahmen bei der Entwicklung vernachlässigt. Dabei entstehen Sicherheitslücken. Diese ermöglichen Angreifern auf eine einfache Art und Weise sich in vernetzte Geräte zu hacken und sie bei einem Massenangriff auf die Netzinfrastrukturen zu mobilisieren.

Jede Netzwerkressource (zum Beispiel ein Server) kann nur eine bestimmte Anzahl an Anfragen gleichzeitig bearbeiten. Wird die Kapazitätsgrenze überschritten, fällt das überlastete Netzwerk aus. Cyber-Attacken, die dieses Prinzip ausnutzen, bezeichnet man als DDoS-Angriffe, also als Distributed-Denial-of-Service-Angriffe. Generell gilt: je mehr Geräte ein Cyberkrimineller für seine DDoS-Kampagne rekrutieren kann, desto schlagkräftiger wird die Attacke sein. Ungesicherte IoT-Geräte lassen sich ohne viel Aufwand als »virtuelle Söldner« anwerben. Damit stellen sie eine Gefahr dar – nicht nur für ihre Inhaber, sondern auch für die kritische Infrastruktur[3].

Hinzu kommt die zunehmende Professionalisierung der Angreifer, die in einer Art Industrialisierung Wertschöpfungsnetzwerke bilden und Marketing betreiben (Stichwort Darknet). Die Hacker-Gemeinschaft investiert kollektiv in die Entwicklung raffinierter Methoden der Cyberkri-

3 Im Herbst 2016 wurden Plattformen wie Twitter, Netflix und Spotify durch einen derartigen DDoS-Angriff lahmgelegt, siehe ↗https://www.nytimes.com/2016/10/22/business/internet-problems-attack.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=first-column-region&region=top-news&WT.nav=top-news&_r=0

minalität. Ransomware entwickelt sich zum Beispiel zu einem lukrativen Geschäft. Energieunternehmen sind aufgrund ihrer Kritikalität ein besonders beliebtes Ziel. Die Frage, wie im Falle einer Übernahme eines Energiesystems durch eine Hackergruppe vorzugehen ist, muss prinzipiell beantwortet werden.

Leider gibt es keine einfachen Antworten auf die hier skizzierten Bedrohungen. Die Herausforderungen der IT-Sicherheit lassen sich nur dann bewältigen, wenn Gesellschaft, Wirtschaft und Staat ihre Hausaufgaben machen. Auf gesellschaftlicher Ebene brauchen wir mehr Bewusstsein für die Gefahren im Cyberspace: Nutzer müssen Vorsicht bei dubiosen Mails walten lassen, komplexe Passwörter verwenden und Sicherheitsupdates zeitnah installieren. Staat und Wirtschaft müssen bekannte Sicherheitslücken so schnell wie möglich schließen.

Die IT-Sicherheit ist nicht die einzige Herausforderung, mit der die Energiewirtschaft im digitalen Bereich zurechtkommen muss. Auch Softwarefehler können zu Gefahren führen. Dies war 2013 der Fall beim »Kreisläuferproblem«: Mehrere Tage waren die Leitsysteme von Verteilnetz-, Übertragungsnetz- und Kraftwerksbetreibern gestört. Durch einen Fehler wurden Zählerabfragen ausgelöst, die den Kommunikationsweg überlasteten. Eine Störung im physikalischen System, etwa durch einen Betriebsmittelausfall, hätte zu gravierenden Blackouts führen können, da die Leitsysteme zeitweilig handlungsunfähig waren. Die Schlussfolgerung aus der Analyse der Störung: Weder Normierung noch Gerätezertifizierung alleine können sicherstellen, dass ein beliebig komplexes System, das über Jahre hinaus durch die Beteiligung vieler immer weiter gewachsen ist, auch weiterhin im Betrieb fehlerfrei arbeitet.

Zusammenfassend lässt sich feststellen: Mit der zunehmenden Vernetzung wachsen die Netzinfrastrukturen, insbesondere Telekommunikation und Elektrizitätsversorgung zusammen und werden dadurch wechselseitig voneinander abhängig. Sicherheit und Widerstandsfähigkeit gegen Angriffe sind möglich, wenn jetzt die Weichen richtig gestellt werden. Das Energiesystem hat enge Beziehungen zu anderen Bereichen wie Smart Home, Industrie 4.0, Verkehr – gemeinsame standardisierte Referenzmodelle helfen hier über das Energiesystem hinaus. Das Smart Grid Architekturmodell (SGAM) wurde auf die Industrie 4.0 (RAMI), Automobilindustrie (RAMA), den Maritimen Sektor (MAF) und den Gesundheitssektor (HBAM) übertragen.

3 Handlungsempfehlungen

Energiewende, Sektorenkopplung und Digitalisierung stellen die Stabilität unseres Energiesystems auf die Probe: Während die Energieeinspeisung durch die Erneuerbaren immer stärker schwankt, die Zahl der Energieerzeuger mittlerweile in die Millionen geht und die Elektromobilität zu massiven (lokalen wie zeitlichen) Nachfragespitzen führen kann, wachsen mit der zunehmenden Vernetzung von Dingen und Geräten die potenziellen Angriffspunkte gleichzeitig enorm. Dabei steht die Energiewirtschaft vor der besonderen Herausforderung, dass sich Strom heute noch nicht in großen Mengen speichern lässt, so dass ein Netzausfall mangels entsprechender Puffer zum sofortigen Stromausfall führt – mit gravierenden Folgen für den Wirtschafts- und Industriestandort Deutschland. Derzeit genügen die in der Vergangenheit bewährten Vorkehrungen und Mechanismen (Robustheit) den neuen, permanent steigenden Anforderungen zwar noch – dank Redundanz (N-1-Prinzip) zählt das deutsche Energiesystem zu einem der zuverlässigsten der Welt – angesichts immer höheren Komplexität stoßen diese Vorkehrungen aber mehr und mehr an ihre Grenzen.

Für die Versorgungssicherheit kommt der Resilienz, das heißt der Fähigkeit eines Systems, trotz erheblicher Belastungen oder Störungen die Funktionsfähigkeit aufrechtzuerhalten beziehungsweise sich nach einem Ausfall von selbst wiederherzustellen, daher strategische Bedeutung zu. Auf diesem Weg vom »fail-safe«- zum »safe-to-fail«-System spielt die Informations- und Kommunikationstechnologie eine Schlüsselrolle.

Drei Aspekte stechen hierbei hervor:

Erstens ist es dank der fortlaufenden dezentralen und automatisierten Analyse aller verfügbaren Daten des Energiesystems möglich, sich im Falle einer Störung ein ebenso umfassendes wie detailliertes Bild der aktuellen Lage zu machen und mit diesem Wissen die richtigen Entscheidungen zur Stabilisierung beziehungweise Wiederherstellung einzuleiten. Dabei können die Effekte der geplanten Maßnahmen mittels datenbasierter Simulationsverfahren nicht nur vorhergesagt, sondern durch die informationstechnische Einbindung aller relevanten Akteure auch in ihrer Wirkung maximiert werden. So lassen sich klare Prioritäten setzen, kontraproduktive Einzelmaßnahmen vermeiden und durch den Informationsaustausch in Echtzeit über alle Ebenen des Energiesystems hinweg die erforderlichen Absprachen erheblich beschleunigen – gegebenenfalls sogar (teil-)automatisieren – so dass schneller reagiert werden kann und die unvermeidlichen Schäden der Störungen sich auf ein Minimum beschränken. Auf lange Sicht ist es dabei so denkbar, dass sich das Energiesystem bei kleineren lokalen oder regionalen Störungen ohne menschlichen Zutun autonom stabilisiert, indem die hierzu nötigen Schritte selbstständig von Algorithmen initiiert werden (Selbstorganisation).

Zweitens lassen sich durch die permanente Analyse der Datenströme in Echtzeit entstehende Störungen im Energiesystem – zum Beispiel verursacht durch Cyberangriffe – über die Identifikation verräterischer oder normabweichender Muster in den Daten des Energiesystems bereits erkennen, während sie sich noch anbahnen. Dies ermöglicht es, proaktiv zu reagieren, d.h. die Störungen zu antizipieren und sie durch geeignete Gegenmaßnahmen zu verhindern oder

zumindest so klein wie möglich zu halten. Hier besteht perspektivisch die Möglichkeit, dass zumindest bei geringfügigen Störungen die proaktiven Gegenmaßnahmen automatisch von Algorithmen durchgeführt werden.

Drittens bieten sich wie oben ausgeführt wurde, zahlreiche datenorientierte Anwendungsfälle, die wie etwa Datenanalyse von Störungshistorien die Möglichkeit, etwaige Strukturschwächen in den Netzen zu identifizieren, entsprechende Optimierungspotenziale aus ihnen abzuleiten und durch strukturelle und/oder organisatorische Anpassungen die Belastbarkeit des Energiesystems zu erhöhen. Der Einsatz Künstlicher Intelligenz erlaubt es, das Verständnis für die komplexen Zusammenhänge und Wechselspiele zwischen den verschiedenen Ebenen des Energiesystems zu vertiefen und so neue Einblicke zu gewinnen.

Bereits diese drei Punkte zeigen stellvertretend das enorme Potenzial auf, das die Informations- und Kommunikationstechnologie für die Resilienz der Energieversorgung bietet. Um es zu heben, muss sie allerdings als integraler Bestandteil des Energiesystems verstanden und dieses im Sinne eines Cyberphysischen Systems interpretiert werden. Darüber hinaus muss den Verteilnetzbetreiber der regulatorische Rahmen so gesetzt werden, dass die entsprechenden Kosten über kapitalmarktadäquate Erlöse zurück verdient werden können. Allerdings steht die Energieforschung hier noch ganz am Anfang. Auf viele offene Fragen gibt es derzeit weder konzeptionelle noch technische Antworten. So stellt sich zum Beispiel das grundlegende Problem, dass die Informations- und Kommunikationstechnologie auf Energie angewiesen ist und im Falle eines Stromausfalls daher nur bedingt einsatzfähig wäre. Darüber hinaus fehlt ein umfassendes Verständnis darüber, welche Implikationen sich für das Energiesystem konkret aus den neuen Herausforderungen ergeben. Die möglichen Störereignisse müssen daher noch besser verstanden werden, etwa die Auswirkungen auf das Gesamtsystem oder die Kombinationen von Störungen der Informations- und Kommunikationstechnologien mit anderen Ereignissen. Die Wahrscheinlichkeit von erfolgreichen politisch motivierten Hackerangriffen lässt sich zum Beispiel aktuell kaum einschätzen.

Um hier größere Klarheit zu schaffen, bedarf es gemeinsamer Forschungsanstrengungen von Wissenschaft, Energiewirtschaft und Digitalbranche. Im Rahmen des 7. Energieforschungsprogramms sollte daher ein strategisches Leitprojekt zum Thema Resilienz der digitalisierten Energieversorgung initiiert werden. Dabei muss das Rad nicht neu erfunden werden. In einem explorativen Leuchtturmprojekt soll eruiert werden, welche besonderen Anforderungen sich in der Energiewirtschaft grundsätzlich stellen, wie bereits im Einsatz befindliche Technologien anderer digitalisierter Branchen angepasst werden können und welche ganz neuen Ansätze notwendig sind, um auch zukünftig Resilienz zu sichern. Dazu sind Cyber-Resilienzlabore sowohl als Reallabore als auch als Experimentierlabore aufzubauen, da sich der Test von Störereignissen in der Realität in vielen Fällen verbietet. Neben der technischen Betrachtung müssen auch Anforderungen an die Gesetzgebung und Regulierung erforscht werden. Sowohl die ITK-Branche als auch die Hersteller der Energiesystemtechnik sind exportorientiert. Daher sind Innovationen zu erforschen, die nicht nur den deutschen Markt bedienen, sondern international zum Gelingen einer resilienten Energiewende betragen können.

Bitkom vertritt mehr als 2.500 Unternehmen der digitalen Wirtschaft, davon 1.700 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen 1.000 Mittelständler, mehr als 400 Start-ups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
F 030 27576-400
bitkom@bitkom.org
www.bitkom.org

bitkom