Ausgestaltung des Stromversorgungssystems

Fundamentale Resilienzstrategien für die Stromversorgung erforderlich

Durch den verstärkten Einsatz von Informations- und Kommunikationstechnik im Bereich der Energieversorgung wird diese verwundbarer gegenüber Ausfällen und Störungen. Um dies zu verhindern, sind Veränderungen notwendig, die fundamentale Aspekte der Systemarchitektur betreffen. Von Astrid Aretz, Mark Bost, Bernd Hirschl, Mariela Tapia, Max Spengler und Stefan Gößling-Reisemann

Die Transformation des Stromsystems hin zu erneuerbaren Energien erfolgt heute parallel mit seiner Digitalisierung. Die Digitalisierung bietet eine Vielfalt an Vorteilen für die Einbindung dezentraler fluktuierender erneuerbarer Energien durch die Entwicklung von neuen Überwachungs-, Steuerungs- und Betriebsstrategien sowie viele neue Geschäftsmodelle.

Hinsichtlich der Versorgungssicherheit mit elektrischer Energie wird jedoch eine neue kritische Dimension eingeführt, denn durch den zunehmenden Einsatz von Informations- und Kommunikationstechnik (IKT) im Bereich der Energieversorgung wird diese komplexer und verwundbarer gegenüber Ausfällen. Mit dem fundamentalen Umbruch des Energiesystems bieten sich aber auch neue Gestaltungsmöglichkeiten, insbesondere in Bezug auf die Umsetzung von Resilienzstrategien in der Systemarchitektur. In dem Vorhaben „Strom-Resilienz“ wurde in den letzten zwei Jahre untersucht, durch welche Gestaltungsoptionen die Resilienz der Stromversorgung erhöht werden kann [1].

Entwicklungsoptionen für das Energiesystem

Die immer noch stark zentral ausgelegte Struktur des Energiesystems wird durch die zunehmende Zahl an dezentralen und erneuerbaren Erzeugungsanlagen (EE) deutlich verändert. Durch den Vorrang der EE-Anlagen, der ihnen durch das Erneuerbare-Energien-Gesetz eingeräumt wurde, muss eine Vielzahl an kleinen Anlagen mit fluktuierender Einspeisung integriert werden, wodurch sich die Leistungsflüsse in den Netzen zum Teil deutlich verändern. Ein Teil der fundamentalen Neuausrichtung des Energiesystems wurde bereits vollbracht, aber angesichts des Ziels, von derzeit 33 % EE-Strom im Jahr 2035 55 bis 60 % zu erzeugen, wird die Notwendigkeit einer Fortsetzung der Umgestaltung des Energiesystems deutlich. Hierfür stehen grundsätzlich verschiedene Pfade zur Verfügung. Eine Ausprägung der Systemcharakteristika, die im Rahmen des Projektes „Strom-Resilienz“ näher untersucht wurde, ist die Granularität des Systems. Damit ist die Größe des kleinsten zu stabilisierenden Netzelements beim Wiederaufbau der Stromversorgung gemeint. Extrembeispiele, welche den Begriff der Granularität gut veranschaulichen, sind in diesem Zusammenhang auf der einen Seite ein Stromversorgungssystem, das auf sehr kleinzelligen autarken Einheiten basiert (bis hinunter zu autarken Gebäuden oder industriellen Einheiten), und auf der anderen Seite ein stark zentral ausgerichtetes Stromsystem, welches mithilfe von zentralen Steuerungseinheiten und verbleibenden Großkraftwerken eine flächendeckende Versorgung gewährleistet, die auf der Stabilität weniger großer Zellen basiert. Wie die technische Umsetzung eines feingranularen Systems möglich sein kann, war beispielsweise Gegenstand der Studie „Der zelluläre Ansatz“ (VDE 2015).

Die Granularität des Energiesystems hat, so eine zentrale These des Vorhabens, große Auswirkungen auf die Verwundbarkeit und muss im Rahmen von entsprechenden Resilienzstrategien und somit durch politische Rahmensetzungen adressiert werden. Gleiches gilt für die zunehmende Durchdringung und Nutzung von IKT im Energiesystem. Die Notwendigkeit dieser Nutzung wird angesichts der zunehmenden Komplexität, Fluktuation sowie des steten Ausgleichsbedarfs des Stromsystems nicht infrage gestellt, jedoch zeigt sich auch hier die Dringlichkeit resilienzfördernder Gestaltungsoptionen.

Die Diskussion über Verwundbarkeiten und folglich die Resilienz einer digitalen Stromversorgung bekommt derzeit in der politischen und fachlichen Debatte noch nicht den Stellenwert eingeräumt, der angesichts der Relevanz des Stromnetzes für alle Infrastrukturen und damit letztlich für alle Wirtschafts- und Lebensbereiche notwendig ist.

Verwundbarkeit des Stromnetzes

Um die kritischen Bedingungen, welche ein System verwundbar machen, zu analysieren, wurde im Rahmen des Projekts eine Vulnerabilitätsanalyse durchgeführt. Die Methode verfolgt einen praxisnahen, interdisziplinären Ansatz, bei dem Expert/innen aus dem Energie- und IT-Sektor zu den, für die Systemverwundbarkeit kritischen Eigenschaften, Strukturen und Elementen in Workshops und in vertieften Einzelinterviews befragt wurden. Ziel war es dabei, Hypothesen über die Hauptbedrohungen eines cyber-physikalischen Energiesystems zu entwickeln.

*Ökologisches*Wirtschaften 4.2017 (32) | DOI 10.14512/OEW320422
© 2017 A. Aretz, M. Bost, B. Hirschl, M. Tapia, M. Spengler, S. Gößling-Reisemann; licensee IÖW and oekom verlag. This is an article distributed under the terms of the Creative Commons Attribution Non-Commercial No Derivates License (http://creativecommons.org/licenses/by-nc-nd/4.0/deed.de), which permits copying and redistributing the material in any medium or format, provided the original work is properly cited, it is not used for commercial purposes and it is not remixed, transformed or built upon. The access to the digital version of this article is reserved to subscribers of *Ökologisches*Wirtschaften until two years after the date of publication; after two years it is available to all readers.

Die Ergebnisse der Analyse zeigen eine große Spannbreite an Bedingungen auf, welche zu Angriffen auf die Stromversorgung und damit zu negativen Auswirkungen auf die Systemleistung führen können, bis hin zum weitreichenden Blackout. Diese Bedingungen beziehen sich dabei auf Technologien, Regulierungen und Standards, politische Rahmenbedingungen und den Faktor „Mensch". Die von den Experten als am relevantesten beschriebenen Bedingungen und daraus resultierende Gefahren werden im Folgenden beschrieben.

So kann der Mangel an effektiven Trainingsprogrammen bezüglich Sicherheit und Sicherheitsbewusstsein zu einem in Cyber-Sicherheitsfragen unzureichend geschulten und unaufmerksamen Personal führen. Experten gaben an, dass „social engineering" eines der am schnellsten wachsenden Sicherheitsprobleme ist, welches es den Angreifer/innen ermöglicht, eine Schwäche aller Organisationen auszunutzen: die Mitarbeiterinnen und Mitarbeiter.

Andererseits sind sich die interviewten Expert/innen einig, dass ein System auch dann verwundbar ist, wenn es stark dezentral organisiert und nah am Konsumierenden angelegt ist, wenn die bei den Verbrauchenden installierten und verwendeten Geräte (Heimautomatisierungssystem, Internet of Things-Geräte, Mobilfunkgeräte, Laptops) mit schlechten Sicherheitsfunktionen ausgestattet sind und nicht über Cyber-Sicherheitsaspekte verfügen, so wie es derzeit noch die Regel ist. Weiterhin bedrohen die fehlende Aufmerksamkeit und mangelndes Verständnis um die Konsequenzen der Sicherheitslücken auf Seite der Konsumierenden ein Energiesystem, in dem die Verbraucher/innen mit weitreichenden Steuerungsmöglichkeiten ausgestattet sind.

Ein weiteres Problem können *Prosumer* darstellen. Dies sind Endverbraucher/innen, die eine Stromerzeugungsanlage betreiben, den Strom bei Bedarf selbst verbrauchen und überschüssigen Strom einspeisen. Durch die Verbindung von dezentralen Energieanlagen mit dem Stromnetz wird der „Air-Gap", welcher bisher ein gewisses Maß an Cyber-Sicherheit bot, überbrückt. Probleme entstehen, wenn diese dezentralen Systeme mit unsicheren Netzwerken oder dem Internet verbunden sind, wovon derzeit ausgegangen werden muss. Weiter erwähnten Experten, dass allein die Vielzahl dezentraler Kleinanlagen und Geräte Probleme hinsichtlich der Sicherung von Endpunkten bereitet, auch wenn durch Standardisierung und Regulierungsauflagen diese Gefahr vermindert werden könnte.

Obwohl es bereits Adaptions- und Schadensminderungsmechanismen gibt, verhindern mangelnde Durchsetzung von Sicherheitsbestimmungen in der Breite und eine häufig fehlende Bereitschaft von Akteure/innen eine Implementierung erforderlicher Sicherheitsmaßnahmen. Gründe sind oft die fehlende Priorisierung oder Kostenargumente. Allerdings gibt es, wie die befragten Expert/innen betonten, keine vollkommene Sicherheitslösung. Die Herausforderung liegt hier darin, eine angemessene Regulierungslandschaft zu kreieren, die nicht nur komplexe Prozeduren hinzufügt, welche die Sicherheit nicht zwingendermaßen erhöhen. Dabei ist die Überwachung der Implementation von Bestimmungen, die ja teilweise schon existieren, eine der großen Herausforderungen.

„Die Verwundbarkeiten der digitalen Stromversorgung werden in der politischen Debatte nicht ausreichend thematisiert."

Resilienzstrategien

Die cyber-physische Resilienz eines Energiesystems kann interpretiert werden als die Kapazität eines Systems, sich bei gleichbleibender Systemleistung und ohne die genaue Kenntnis von Ereignissen und Stressoren auf cyber-physische Störeinflüsse vorzubereiten, mit ihnen umzugehen und sich davon zu erholen (Gößling-Reisemann 2016).

Die Resilienz von sozio-technischen Systemen, zu denen auch cyber-physikalische Energiesysteme gehören, wird beeinflusst durch strukturelle Eigenschaften (wie Redundanzen, Puffer und Speicher, lose Kopplungen [Gößling-Reisemann 2016]) und einen Managementprozess, der generell in vier Phasen eingeteilt werden kann (Gößling-Reisemann 2016; Acatech et al. 2017): Vorbereitung und Prävention, Implementation von robustem und vorsorglichem Design, Umgang und Erholung von Krisen sowie Lernen für die Zukunft. Aus den Interviews und Workshops in *Strom-Resilienz* sowie aus der Diskussion in der Literatur lassen sich einige Hypothesen ableiten, wie ein cyber-physikalisches Energiesystem resilienter gemacht werden kann.

Bezüglich der Struktur gilt es zunächst, zwischen einer zentralen und einer dezentralen Struktur zu unterscheiden. Auf Basis der ausgewerteten Interviews lässt sich ableiten, dass eine stark zentral ausgerichtete Struktur mit Großkraftwerken, zentralen Steuerungseinheiten und zentralisierter Datenverarbeitung als wenig resilient gesehen wird, da hier nur ein einzelner Zugriffspunkt nötig ist, um einen großen Stromausfall herbeizuführen. Ebenso ist aber auch eine stark dezentralisierte Struktur wenig resilient, insbesondere da hier eine adäquate Pflege von Sicherheitsstandards und die Koordination von stabilisierenden Eingriffen in die Stromversorgung als Engpass gesehen werden. Mehr Aussicht auf erhöhte Resilienz wird stattdessen einer zellulären Struktur eingeräumt, bei der Erzeugung und Verbrauch zunächst innerhalb einer angemessenen Zellgröße ausbalanciert werden, bevor ein weiterer Ausgleich mit Nachbarzellen stattfindet. Dies schließt auch die Erfassung und Verarbeitung von Daten ein. Die angemessene Zellgröße zu finden, ist Teil von aktuellen Forschungsprojekten, diskutiert werden vor allem die Quartiersebene, Städte

oder größere Liegenschaften. Als ein weiteres strukturbezogenes Strategieelement wurden dezentrale physikalische Backupsysteme diskutiert, die auch bei Ausfall von zentralen IT- und Kommunikationssystemen eine stabile Mindestversorgung in dezentralen Strukturen aufrechterhalten können. Diese sollen in der Lage sein, nur auf der Basis von physikalischen Netzparametern entsprechende Lastfluss-, Frequenz- und Blindleistungsanpassungen durchführen zu können.

Weitere im Projekt diskutierte Maßnahmen lassen sich in die oben genannten vier Managementphasen einordnen. Während der ersten Phase müssen Schwachpunkte des Systems identifiziert und entsprechende Sicherheitsmaßnahmen sowie Richtlinien entworfen werden (Acatech et al. 2017). Zudem sind für die Prävention Verschlüsselungsmethoden nötig, um die Integrität der Daten für Kommunikationsprotokolle zu gewährleisten. Endpunkte der Kommunikation könnten trotz sicherer Kommunikationskanäle kompromittiert werden. Um die mit end-to-end Sicherheit verbundenen Herausforderungen zu adressieren, muss daher eine schnelle Identifikation der Sicherheitslücke möglich sein. Eine weitere notwendige Voraussetzung für die Prävention sind Authentifizierungs- und Autorisierungsmechanismen in Endusergeräten sowie in dezentralen Steuerungsgeräten. Ferner wird empfohlen, Testverfahren in das Patch-Management zu integrieren, um fehlerhafter Soft- und Hardware durch manipulierte Updates entgegenzuwirken.

Die zweite Phase umfasst die Implementierung von robustem und vorsorglichem Design. Anhaltspunkte für ein resilientes Design sind beispielsweise: Diversität der IT-Komponenten in Bezug auf Hersteller, Betriebssysteme und Kommunikationsprotokolle sowie Redundanzen in Kommunikationskanälen und Anlagen. Adaptionsmechanismen, welche Echtzeitüberwachung sowie Angriffserkennungs- und Anomalieerkennungssysteme in Kommunikationskanälen beinhalten, ermöglichen es, Prozessstörungen zu entdecken und sie von Cyberangriffen unterscheiden zu können.

In Phase drei des Resilienzmanagements sollte es im Falle eines erfolgreichen cyber-physischen Störfalles in Subsystemen möglich sein, die Systemleistung so schnell wie möglich wiederherzustellen. Dazu sollten Geschäftskontinuitätspläne, Notfallpläne sowie entsprechende Maßnahmen auf regionaler und lokaler Ebene implementiert werden. Mittels des Konzepts der multiagentenbasierten Steuerung mit dezentralisiertem Steuerungskonsens könnte die Stabilität und Sicherheit in Krisenfällen verbessert werden (Lehnhoff et al. 2013).

Vergangene Katastrophen und vermiedene Ernstfälle sollten in Phase vier genutzt werden, um aus ihnen zu lernen und somit die Anpassungsfähigkeit des Systems zu verbessern. Hierzu zählt, dass Krisen und Ereignisse dokumentiert sowie analysiert werden, um Schwachstellen zu identifizieren. In diesem Sinne würde die digitale Forensik es erlauben, Vorfälle sowie Beinahe-Ausfälle eingehend zu untersuchen und Lektionen daraus zu ziehen. Umgekehrt können die identifizierten Stärken, die zur Vermeidung oder Wiederherstellung beitragen, als Basis für die Planung weiterer Strategien und Notfallszenarien verwendet werden (Gößling-Reisemann 2016, acatech et al. 2017).

Anmerkung

[1] Weitere Informationen zu dem im Rahmen des Förderschwerpunkts „Innovations- und Technikanalyse“ (ITA) vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Projekts: www.stromresilienz.de

Literatur

Deutsche Akademie der Technikwissenschaften e. V. (acatech)/Deutsche Akademie der Naturforscher Leopoldina e. V./Union der deutschen Akademien der Wissenschaften e. V. (Hrsg.) (2017): Das Energiesystem resilient gestalten. Maßnahmen für eine gesicherte Versorgung. Berlin, Königsdruck.

Gößling-Reisemann, S. (2016): Resilience – Preparing Energy Systems for the Unexpected: In: IRGC Resource Guide on Resilience. In: Resource Guide on Resilience (IRGC). Lausanne: EPFL International Risk Governance Center. Version 29. 07. 2016.

Lehnhoff, S./Krause, O. (2013): Agentenbasierte Verteilnetzautomatisierung. In: Göhner, Peter (Hrsg.): Agentensysteme in der Automatisierungstechnik. Heidelberg, Springer. 207–223.

Verband der Elektrotechnik, Elektronik, Informationstechnik e. V. (VDE) (2015): Der Zellulare Ansatz: Grundlage einer erfolgreichen, regionenübergreifenden Energiewende. Frankfurt, Energietechnische Gesellschaft.

AUTOR/INNEN + KONTAKT

Dr. Astrid Aretz und ***Mark Bost*** sind Wissenschaftler/innen und ***Prof. Dr. Bernd Hirschl*** Leiter des Forschungsfelds „Nachhaltige Energiewirtschaft und Klimaschutz“ am Institut für ökologische Wirtschaftsforschung (IÖW).

Institut für ökologische Wirtschaftsforschung (IÖW) GmbH, Potsdamer Str. 105, 10785 Berlin. E-Mail: astrid.aretz@ioew.de, mark.bost@ioew.de, bernd.hirschl@ioew.de, Website: www.ioew.de

Prof. Dr. Bernd Hirschl ist außerdem Stiftungsprofessor an der Brandenburgischen Technischen Universität (b tu) Cottbus-Senftenberg.

Brandenburgische Technische Universität Cottbus-Senftenberg, Großenhainer Straße 57, 01968 Senftenberg. Website: www.b-tu.de/fg-energieversorgungsstrukturen/

Mariela Tapia ist wissenschaftliche Mitarbeiterin, ***Max Spengler*** ist studentischer Mitarbeiter und ***Prof. Dr. Stefan Gößling-Reisemann*** Leiter des Fachgebiets „Resiliente Energiesysteme“ am Fachbereich Produktionstechnik der Universität Bremen.

Universität Bremen, Enrique-Schmidt-Str. 7, 28359 Bremen. E-Mail: mariela.tapia@uni-bremen.de, spengler@uni-bremen.de, sgr@uni-bremen.de, Website: www.res.uni-bremen.de