Cyber-Resilienz

Schwarze Schwäne im Energiesystem | Das Verteilnetz war lange «blind». Will man die Beobachtbarkeit und Kontrollierbarkeit bis zur Haushaltsebene erhöhen, muss mehr IKT (Mess- und Steuergeräte) eingesetzt werden. Dies erhöht zwar die Flexibilität, Effektivität und Nachhaltigkeit in Verbrauch und Produktion, birgt aber auch gewisse Risiken.

TEXT DAVOOD BABAZADEH, CHRISTOPH MAYER, SEBASTIAN LEHNHOFF

Im klassischen Risikomanagement werden Ereignisse entsprechend ihrer Häufigkeit und Konsequenzen kategorisiert. Ein technisches System wird üblicherweise so entworfen, dass es häufige und mittelhäufige Ereignisse mit geringer Auswirkung tolerieren kann. Meist ist es nicht wirtschaftlich, seltene Ereignisse mit hohem Schaden während der Designphase zu berücksichtigen. **Bild 1** zeigt einige reale Beispiele von Ereignissen in Energiesystemen. So führen z. B. häufig eintretende Überlastungssituationen im indischen System zu schwerwiegenden ökonomischen Schäden durch Blackouts. Reguläre Ereignisse am Markt resultierten in Engpässen bei der Lieferung von Elektrizität in Kalifornien, da Regulierer der Versorgungssicherheit nicht so viel Beachtung geschenkt, sondern sich auf die Profite der Monopolisten konzentriert hatten. Das sehr seltene Ereignis einer Sonnenfinsternis mit enormem Einfluss auf die PV-Einspeisung konnte in Europa ohne Probleme abgefangen werden. Im Allgemeinen ist die Häufigkeit bestimmter Ereignisse und deren Auswirkungen auf das System subjektiv und abhängig von der Situation des Versorgungssystems hinsichtlich geografischer Lage, technologischer Beschaffenheit und wirtschaftlichem Rahmen. Das bedeutet, dass Entscheidungsträger, Systemdesigner oder Stakeholder in der Lage sind, die Ereignis-Ausmass-Abbildung zu ändern – je nachdem, wie «resilient» sie ihr regionales, nationales oder sogar internationales Energiesystem gestalten.

Schwarze Schwäne und Resilienz

Ein System wird als resilient bezeichnet, wenn es fähig ist, nach Störungen rasch zum Normalzustand zurückzukehren, sich zu erholen und dabei den Schaden gering zu halten. Der Resilienzprozess **(Bild 2)** umfasst die geeignete Reaktion auf ein Ereignis (Absorbieren der Störung), das Zurückfallen auf kritische Funktionen und Stabilisierung des Systems (Stabilisierung) und

Bild: BKW

zuletzt das kontrollierte Zurückbringen zum Normalbetrieb des Systems (Wiederherstellung).

Durch die Entwicklung hin zu einem digitalen, komplexen Energiesystem mit dessen unvorhersagbarer und volatiler Natur entsteht ein neuer, riskanter Ausgangspunkt für sogenannte «Schwarzer-Schwan-Ereignisse». Der Schwarze Schwan in Talebs Theorie bezieht sich auf seltene, schwer vorhersagbare und unerwartete, disruptive Ereignisse mit hohem Schadensausmass, die normalerweise als Ausreisser bezeichnet werden.[1]

In Energiesystemen können Schwarzer-Schwan-Ereignisse durch verschiedene Ursachen oder Kombinationen von Ursachen hervorgerufen werden. Beispiele sind natürliche Ereignisse (z. B. Überflutung, Erdbeben, Eisregen und Kombinationen hiervon), physikalische oder Cyber-Angriffe (Terroristen, Hacker) oder schlechtes Marktdesign. Eine Eigenschaft von Schwarzen Schwänen ist, dass sie unbekannt oder schwer vorhersagbar sind. Das ist umso kritischer im modernen durch verteilte Erzeugung dominierten Energiesystem, da die Erfahrung im Betrieb und damit historische Daten zu neuen Technologien limitiert sind.

In Deutschland gibt es bereits umfassende Massnahmen zur IT-Sicherheit sowie Gesetze und Regulierungen für verschiedene neue IKT-Entwicklungen (z. B. BSI-Schutzprofile für das Smart Meter Gateway). Trotzdem kann das System nicht gegen alle Ausfälle gesichert werden. Deshalb sollten die Natur und Dynamiken der störenden Ereignisse, die auf die neue Struktur des Systems zielen, genau verstanden werden, insbesondere deren Einfluss auf die Gesamtperformanz des Systems. Die Wahrscheinlichkeit erfolgreicher, politisch motivierter Hacker-Angriffe kann beispielsweise kaum geschätzt werden. Der Schaden sowie die Wahrscheinlichkeit für ein solches Ereignis sind oft nicht abhängig von früheren Ereignissen.

Wie wirken sich diese Entwicklungen (z. B. vermehrte Cyber-Komponenten) auf den Resilienz-Prozess aus und wie lassen sich Verbesserungen schaffen? Für den Resilienzprozess **(Bild 2)** sind besonders das Lagebild, die Zuverlässigkeit bei der Durchführung der Aktionen und die Beurteilung der Auswirkung der Aktionen von Bedeutung. Das

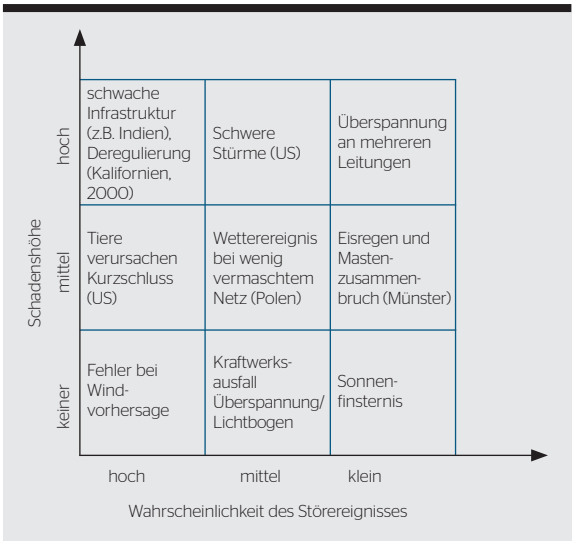

Bild 1 Ereignishäufigkeit und Schaden.

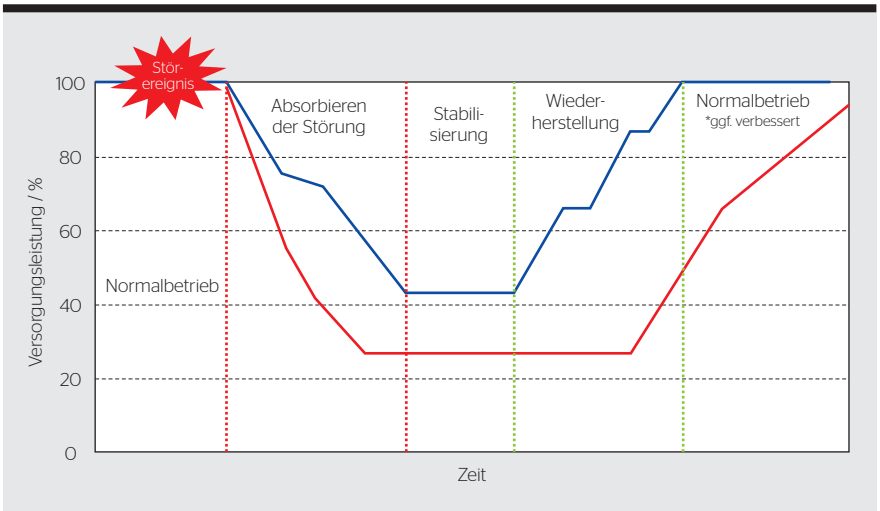

Bild 2 Wiederherstellung der Funktionsfähigkeit eines Systems. Blau: resilientes System, Rot: nicht-resilientes System.

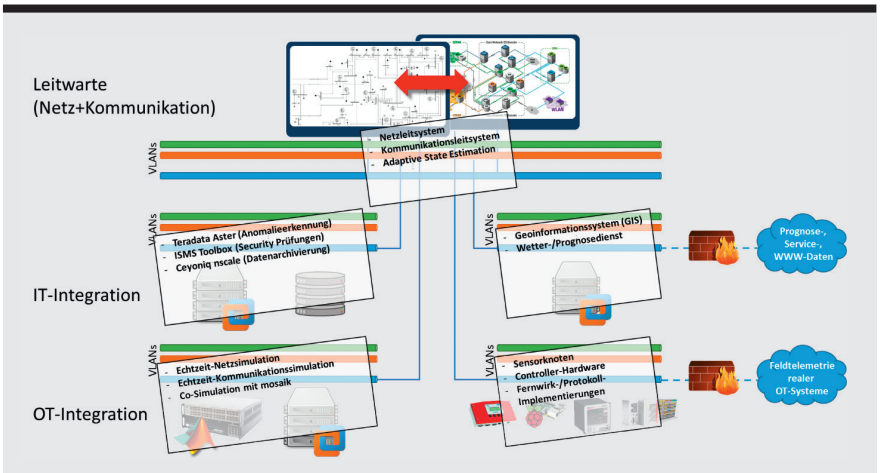

Bild 3 Schematischer Laboraufbau zur Abbildung der unterschiedlichen Schichten eines typischen Energieversorgungssystems.

Bilder: Offis

Lagebild muss auch eine Einschätzung des Zustandes aller IKT-Systeme enthalten, soweit sie für Systembetrieb und -wiederherstellung eine Rolle spielen. Bisher gingen Resilienz-Prozesse häufig davon aus, dass untere Spannungsebenen keine grosse Bedeutung für die Versorgungssicherheit (z. B. Systemdienstleistungen) und den Wiederaufbau haben. Da sich das ändert, benötigen die Netzbetreiber sowohl viel bessere Informationen über die Situation in den Verteilnetzen als auch Berechnungen, wie sich das Verteilnetz unter ungünstigen Voraussetzungen beim Wiederaufbau verhält. So ist etwa heute nicht bekannt, wie sich die PV-Anlagen im Krisenfall verhalten werden. Die Resilienz-Prozesse müssen ausserdem vorher im «Labor» simulativ getestet werden. Mechanismen der Selbstorganisation werden voraussichtlich eine Rolle spielen, die zur Koordination und Kontrolle IKT benötigen. Die IKT muss daher für Resilienzprozesse im neuen Energiesystem eine tragende Rolle übernehmen.

Wie kann Cyber-Resilienz helfen?

Ein System ist dann «cyber-resilient», wenn die IKT-Komponenten und die auf IKT basierenden Prozesse zusammen mit den energietechnischen Komponenten die Resilienz des Gesamtsystems erhöhen. Dazu gehören die Möglichkeiten, ein genaues Lagebild zu erzeugen und die Auswirkungen von Massnahmen besser prognostizieren zu können. Ganz besonders leistet die Cyber-Resilienz auch eine Abschätzung, inwieweit sich Risiken durch ein Ereignis ändern, etwa indem nun andere Ereignisse deutlich wahrscheinlicher (etwa ein Erdschluss, da Leitungen aufgrund hoher Belastung stärker durchhängen) oder deutlich gefährlicher werden (etwa da aufgrund von IKT-Problemen nicht mehr ausreichend reagiert werden kann). Schwarzer-Schwan-Ereignisse besser zu verstehen, erhöht die Vorhersagbarkeit der Ereignisse und deren Konsequenzen. Es ermöglicht eine ähnliche Reaktion wie vorhersagbare Ereignisse.

Labor-Infrastruktur

Um das Konzept der Cyber-Resilienz zu simulieren und zu untersuchen, wird im Offis – Institut für Informatik in Oldenburg eine Testumgebung für Konzepte zur Systemintegration und -führung unter unsicheren Bedingungen in digitalisierten Energieversorgungssystemen aufgebaut. Dieser einmalige Laboraufbau kombiniert Techniken zur Gefährdungserkennung und -analyse von Smart-Grid-Architekturen mit Methoden zur Anomalie-Erkennung in Informationsprozessen auf unterschiedlichen Ebenen (OT/IT) heutiger Energieversorgungssysteme. In der hier aufzubauenden Laborumgebung sollen präventive Sicherheitsmassnahmen, die solchen Angriffen vorbeugen, aber auch reaktive Massnahmen zur schnellen Erkennung und Behandlung von IT-Sicherheitsattacken in Stromversorgungssystemen entwickelt und getestet werden können.

Fazit

Das neue Energiesystem hat viele Vorteile im Hinblick auf Nachhaltigkeit, Effizienz und Flexibilität. Es so resilient und robust wie das konventionelle System zu machen, ist jedoch eine ernstzunehmende Herausforderung, die zu scheitern droht und damit zu einer neuen Bedrohungsquelle für die Gesellschaft werden kann. Entscheidungsträger, Stakeholder und Akteure müssen IKT-Innovationen als ein Mittel zur Sicherung der neuen Struktur des Energiesystems einsetzen, d.h. sich hin zu Cyber-Resilienz bewegen.

Konferenz

Energieinformatik 2018

Die 7. D-A-CH+ Konferenz für Energieinformatik wird vom 11. bis 12. Oktober 2018 in Oldenburg stattfinden.

Ziel der Konferenz ist es, die Forschung, Entwicklung und Implementierung von Informations- und Kommunikationstechnologien im Energiebereich zu fördern und den Austausch zwischen Wissenschaft, Industrie und Dienstleistern zu fördern.

www.offis.de/offis/aktuelles/veranstaltung/energieinformatik-2018.html

Autoren

Dr. **Davood Babazadeh** ist Leiter der F&E-Gruppe «Automation, Communication and Control» und Principal Scientist im Bereich «Energie» am Offis.
→ Offis – Institut für Informatik, DE-26121 Oldenburg
→ davood.babazadeh@offis.de

Dr. **Christoph Mayer** ist Leiter des Bereichs «Energie» am Offis.
→ christoph.mayer@offis.de

Prof. Dr. **Sebastian Lehnhoff** ist Professor für Energieinformatik an der Carl-von-Ossietzky-Universität Oldenburg, Vorstand des Offis und Sprecher des Bereichs «Energie».
→ sebastian.lehnhoff@offis.de

RÉSUMÉ

Cyber-résilience

Des cygnes noirs dans le système énergétique

La gestion du réseau de distribution a longtemps été « aveugle » et « passive ». Augmenter la possibilité de surveillance et de contrôle jusqu'aux bas niveaux de tension implique une utilisation nettement plus intense d'instruments de mesure et de commande communicants. Le nouveau système énergétique numérisé présente de nombreux avantages en termes de durabilité, d'efficacité et de flexibilité. Toutefois, rendre ce système aussi robuste que celui utilisé jusqu'à présent est un sérieux défi qui soulève de nombreuses questions. Des erreurs fondamentales pourraient menacer notre société. Des environnements de développement et d'essai novateurs aideront à mieux comprendre les rapports entre les TIC et la technique de l'énergie et permettront de simuler des scénarios possibles de risques. Ainsi, des connaissances concernant le design et le fonctionnement technique d'un système énergétique cyber-résilient pourront être acquises afin d'aider les acteurs de l'économie énergétique, les législateurs et le service de régulation à prendre les décisions nécessaires pour atteindre cet objectif. NO