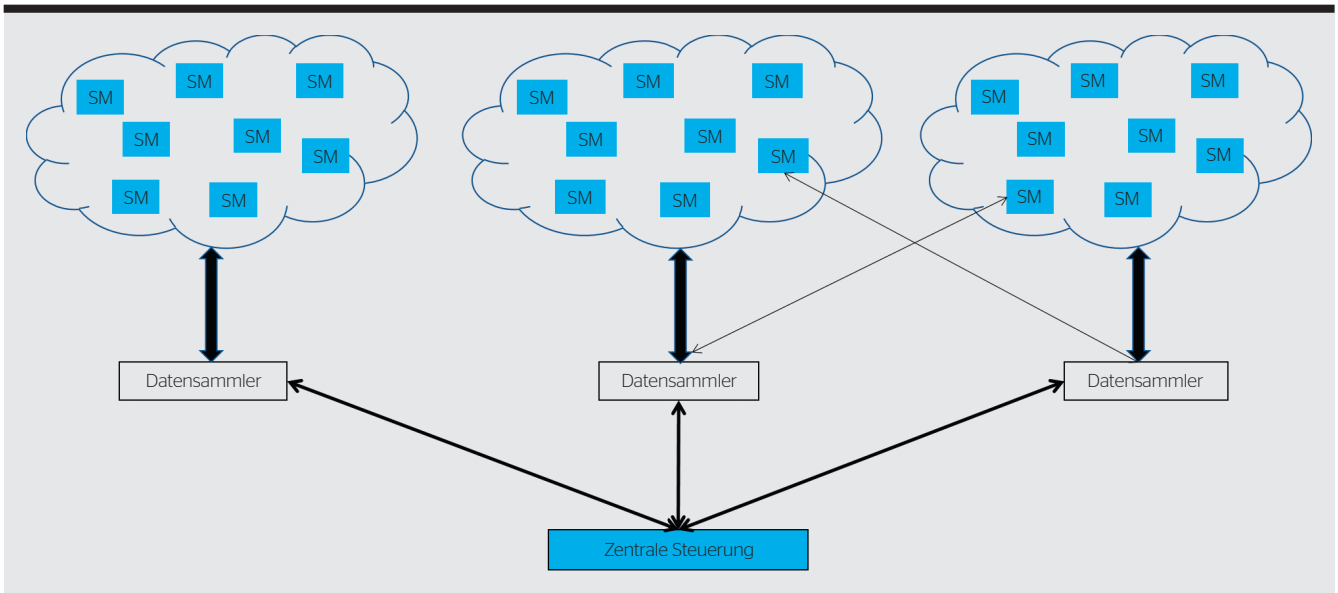

Klassischer Aufbau einer Smart-Grid-Struktur mit Smart Metern (SM) heute.

Resilient in der neuen Energiewelt

Vernetzte Kommunikation | Vernetzung und Dezentralisierung von Verbrauchern und Produktion bringen neue Herausforderungen für die Energieversorgung. Dieser Artikel zeigt auf Basis der Netzwerktheorie mögliche Effekte hochvernetzter Kommunikation auf Cybersecurity und Effizienz der Systeme auf. Resiliente Alternativen werden diskutiert, etwa mittels statistischer Verfahren.

MONIKA FREUNEK, GABRIEL-MIHAI LIPSA

Erneuerbare Energien und zunehmend auch das Internet der Dinge sind heute fester Bestandteil unserer Energiewelt. Dabei werden kleinere private Installationen und Grossanlagen in der Regel mit einem bereits bestehenden Stromnetz verbunden. Über das Europäische Verbundsystem ist damit der Prosumer in der Schweiz mit Windparks in Norddeutschland, Industrieanlagen in Schweden und Kraftwerken in der Türkei verbunden. Unser Energiesystem ist also ein komplexes System weit über die Grenzen des eigenen Energieversorgers hinaus und aus physikalischer Sicht ein chaotisches System. In der Praxis führt dies zu Instabilitäten und Risiken, die ein einzelner Energieversorger oder Prosumer mit den heutigen Methoden kaum beeinflussen kann.

Spätestens seit dem Erreichen signifikanter Anteile statistischer Energieträger an der Gesamtenergieproduktion und mit der internationalen Vernetzung von Energie- und Handelssystemen sind automatisierte und vernetzte Lösungen mit schneller Kommunikation nötig.

Das Smart Grid

Das wohl bekannteste Konzept zum Betrieb vernetzter Energiesysteme ist das Smart Grid. Das Einstiegsbild zeigt eine gängige Umsetzung mit Smart Metern. Feldgeräte sammeln Informationen, die durch den Energieversorger mit einer zentralen Intelligenz unter anderem zu optimierten Steuerbefehlen verarbeitet werden. Ein solches System muss über Jahrzehnte sicherstellen, dass jede Komponente vor Angreifern jeglicher Art aus der ganzen Welt geschützt ist und bleibt.

Die Vernetzung von Komponenten in einem System hat in der Regel zum Ziel, mit einer zentralen Einheit zu kommunizieren, Kommunikation zwischen im Feld verteilten Komponenten zu ermöglichen oder beides. Der Aufbau der Vernetzung ist auch als Netzwerk-Topologie bekannt. Eine vollständig zentralisierte Topologie ist die Sterntopologie. Sie entspricht dem klassischen Verständnis heutiger Smart-Grid-Systeme. Sind alle Komponenten vollständig oder teilweise miteinander verbunden, wird dies als vermaschte Topologie (Englisch: meshed) bezeichnet. Dies entspricht dem Aufbau zahlreicher Smart-Metering-Topologien, wobei die Datenkonzentratoren sternförmig mit dem Energieversorger verbunden sind und mit den Smart Metern vermascht sind (Einstiegsbild). Ähnlich bilden IoT-Komponenten eines

Bilder: BKW

Smart Home miteinander zumeist ein vermaschtes Netz und kommunizieren über einen Backbone in sternförmiger Topologie mit einem Hersteller.

Was bedeutet dies für das resultierende Netz in der Gesamtsicht? Welche Auswirkungen hat der Grad der effektiven Vernetzung auf Gesamtsicherheit und Cybersecurity, aber auch Stabilität und Effizienz?

Eine riesige Angriffsfläche

Aus Sicht eines Angreifers ist diese Architektur gleichzusetzen mit einer nie dagewesenen Angriffsfläche. Die Angriffe jüngster Zeit auf dezentrale Produktionsanlagen oder auch auf Videokameras zeigen, dass wir erst am Anfang stehen, Sicherheit auch dezentral zu verstehen. Das heisst: Die Expositionsfläche sollte, wo immer möglich, minimiert werden. Es kann also durchaus intelligent sein, Geräte bewusst nicht zu vernetzen. Jede nicht benötigte Funktion ist grundsätzlich ein Sicherheitsrisiko. Auch Daten ohne Verwendungszweck zu erheben, zu speichern und zu übertragen, stellt in jedem Schritt neben dem vermeidbaren Energieverbrauch ein Sicherheitsrisiko dar.

Anschaulich untersuchen lässt sich dies aus der Sicht eines Angreifers, der Zugriff auf ein Gesamtsystem oder bestimmte Teile davon möchte. Dazu reicht es unter Umständen, zunächst wenig geschützte Systemteile anzugreifen.

Ein Beispiel für diesen Effekt von Vernetzung ist der Hack eines Casinos in Nordamerika. Hier ermöglichte der Zugriff auf das Netzwerk des Casinos über ein IoT-Thermometer in einem Aquarium den Abzug der persönlichen Daten von Casino-Gewinnern.[1] Durch die effektive Verbindung verschiedener Netze werden als separiert betrachtete Umgebungen tatsächlich zusammengeschlossen, oftmals ohne Bewusstsein der Anwender. Spätestens bei einer Verbindung mit dem Internet entstehen dabei Angriffsflächen von bisher unbekanntem Ausmass.

Quantifizierung der Angriffsflächen

Wie gross sind diese Angriffsflächen nun konkret? Wie viele Möglichkeiten gibt es, sich zu einem Netz Zugriff zu verschaffen? Im vereinfachten Modell ist jede Komponente mit jeder anderen

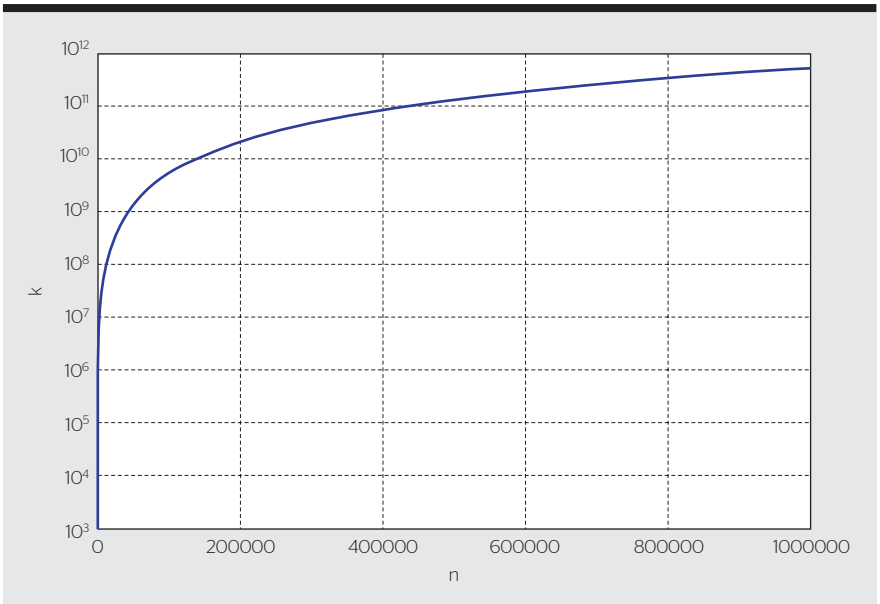

Bild 1 Anzahl der Verbindungen *k* zwischen *n* Komponenten in einem System nach Formel 1.

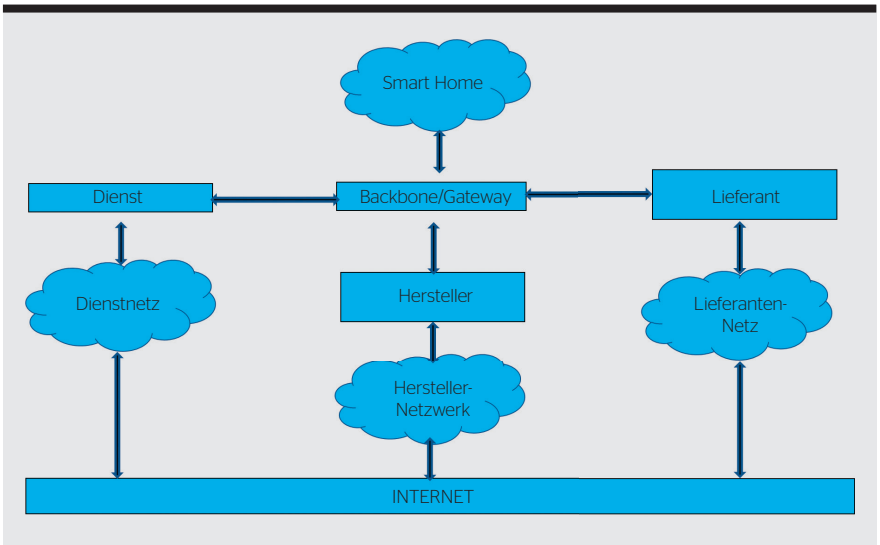

Bild 2 Einbindung eines Smart-Home-Systems in weitere Systeme.

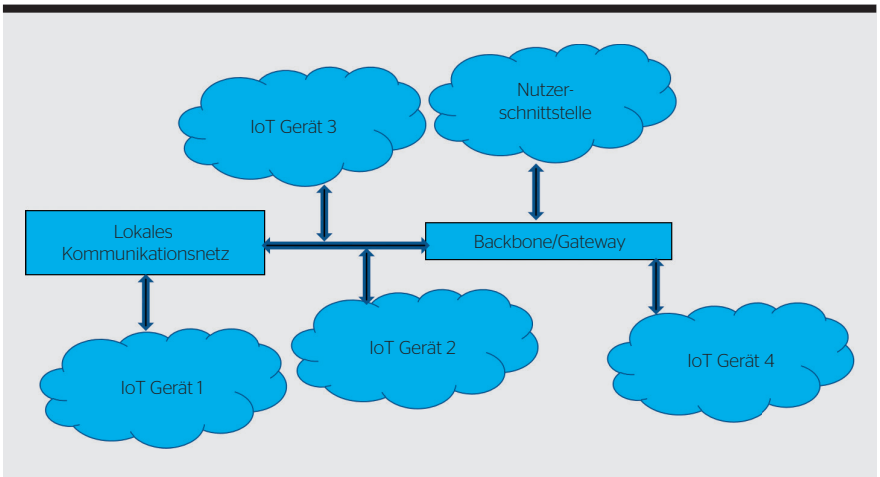

Bild 3 Auf Sicherheit optimiertes Smart-Home-System.

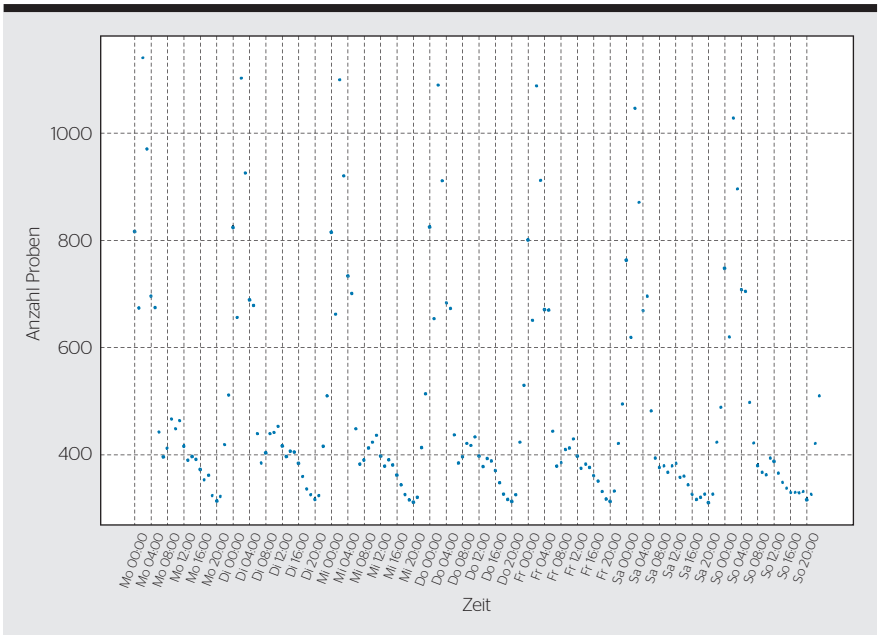

Bild 4 Analyse für 60-Minuten-Profile mit Leistungslimit 15 kW. Eine nötige Stichprobengrösse über 500 ist die Ausnahme im Tagesverlauf.

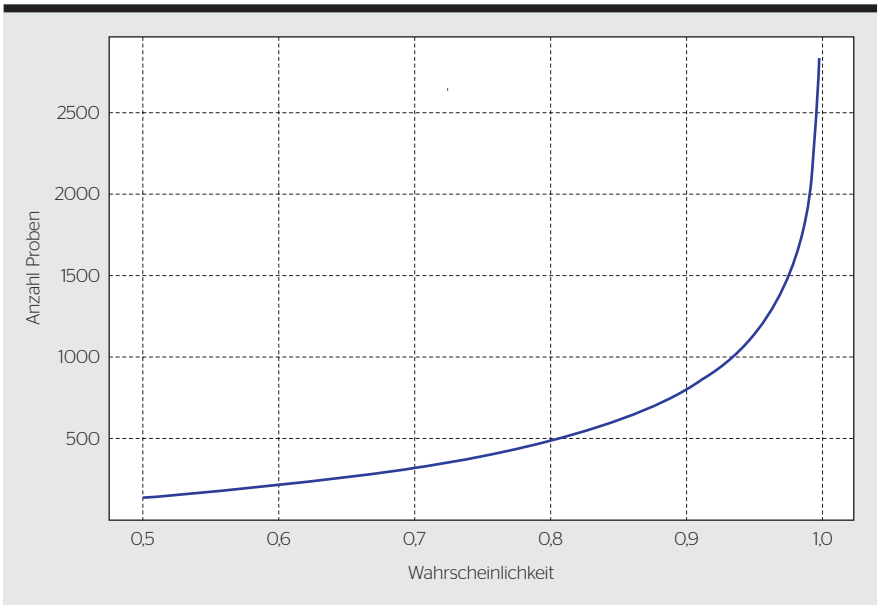

Bild 5 Anzahl der nötigen Proben in Abhängigkeit vom Vertrauensintervall. Mit einer Stichprobe von etwa 500 lässt sich der Mittelwert mit einem Fehler ±10 % zu 80 % Wahrscheinlichkeit vorhersagen.

Komponente direkt vernetzbar. Das System ist also vollständig vermascht. Dann gibt es für n Komponenten k Möglichkeiten, sich miteinander zu verbinden (Formel 1):

$$k = \frac{n(n-1)}{2}$$

Bild 1 zeigt die Anzahl der Verbindungsmöglichkeiten in Abhängigkeit von der Anzahl der Komponenten. Während es für Systeme von 10–100 Komponenten noch einige Hundert bis Tausende möglicher Verbindungen gibt, erreicht dieser Wert für grössere Systeme rasch astronomische Grössenordnungen. Praktisch bedeutet diese enorme Angriffsfläche, dass trotz massiven Schutzes von erfolgreichen Angriffen auszugehen ist. Auch die Netzwerksichtbarkeit ist für ein solches System eine grosse Herausforderung, müssen doch alle Komponenten und Kommunikationsnetze sowie deren Konfigurationen stets bekannt sein. Das aktive Gestalten und Verstehen bestehender und neuer Netzwerke ist damit eine Schlüsselaufgabe sicherer Energiesysteme von heute, sei es durch Energieversorger oder auch durch Anbieter steuernder IoT-Lösungen für Prosumer, E-Mobilität oder intelligenter Gebäude.

Ausdehnung von Systemen

Welche Ausdehnungen erreichen also reale Systeme? **Bild 2** zeigt ein vereinfachtes Beispiel aus der IoT-Welt. Ein Smart Home ist mit mehreren Aktoren und Sensoren ausgestattet, die vermascht mit einem lokalen Gateway kommunizieren. Dieser sendet die Daten an die Plattform des Anbieters, der Visualisierungsdaten an das Smartphone des Kunden sendet, Optimierungen berechnet und Steuerbefehle zurück in das Smart Home sendet. Über das Smart Home kann der Kunde selbst Steuerbefehle senden.

Das Ziel- und vordergründig wahrgenommene Netz, in dem physikalische Steuerungen und Messungen durchgeführt werden, besteht dabei aus einigen IoT-Knoten und einem Gateway. Hier gibt es für rund zehn vernetzte Aktoren oder Sensoren und ein Gateway etwa 50 mögliche Verbindungen. Die Kommunikation erfolgt in der Regel innerhalb des Hauses, sodass die Verbindungen alle innerhalb desselben zu schützenden und zu betreibenden Netzes sind. Bei dieser Betrachtung ausgelassen ist die Kommunikation des Gateways mit dem Server des Anbieters. Zum einen erfolgt diese über einen Kommunikationsanbieter, etwa einen Router eines Internetanbieters, zum anderen steht dieser Server in Verbindung mit dem Netzwerk des Unternehmens. Ist nun etwa der Zugang zum Gateway ein im Internet zugänglicher Standard, entspricht die Anzahl der möglichen Verbindungen auf das Gateway gleich der Anzahl der Verbindungen innerhalb des Haus-Netzwerkes und plus denen des Internets. Dabei sind die Zugriffsmöglichkeiten über das Kommunikationsnetzwerk zwischen Gateway und Server noch vernachlässigt, etwa mittels Router und Internet, und Server und Smartphone, etwa mittels Mobilfunk und Internet. Dabei ist aufgrund der Grösse des resultierenden Gesamtnetzes die Auslegung des angeschlossenen Subnetzes, in diesem Fall das IoT-Netz, vernachlässigbar.

Das Botnetz Mirai, das weltweit private internetfähige Videokameras nutzte, oder regelmässige Angriffe auf verschiedene Internet-Router sind praktische Beispiele solcher Angriffe. Der Nutzer selbst nimmt dabei oft nur das direkt erlebte Netzwerk wahr. Die Beispiele zeigen, wie das Management von Schnittstellen und deren Zugängen die effektive Grösse eines Netzwerks beeinflusst.

Bild 3 zeigt eine auf Sicherheit optimierte Variation. Der Nutzer hat lokal Zugriff auf das Gateway. Dieses führt Optimierungen durch, die durch den Nutzer vorgegeben werden, etwa das Laden eines E-Autos zur Mittagszeit an sonnigen Tagen zur Steigerung des Eigenverbrauches. Angriffe und Störungen sind damit auf lokale Komponenten oder das lokale Kommunikationsnetz reduziert.

Wie aus obigen Untersuchungen ersichtlich, entstehen in heutigen Systemen sehr schnell grosse Netzwerke. Heutige Energiesysteme benötigen damit eine intelligente und zielgerichtete Vernetzung, die an manchen Stellen auch einen bewussten Verzicht enthält.

Künstliche Intelligenz, Big Data

Wie lässt sich dieses Vorgehen mit grossen laufenden Technologieentwicklungen wie Künstlicher Intelligenz und Big Data vereinbaren? Aus Sicht Datenschutz und Datensicherheit lautet die Antwort klar «hervorragend». Für diese Themen ist es essenziell, Kunden, Auftraggebern und Gesellschaft zu garantieren, dass Sicherheit, Rechtsmässigkeit und Datenschutz stets gegeben sind. Dies ist aufgrund obiger Bedrohungslage mit klassischen Ansätzen kaum zu gewährleisten. Eine gezielte Auswahl von Daten in einem kontrollierten Rahmen ist damit auch für obige Technologien deutlich empfehlenswerter als Massenerhebungen in einem faktisch nicht bekannten Netzwerk. Regelmässige Datenlecks auch grosser Anbieter sind ein Beispiel dafür.

Dabei sind Massendatenerhebungen nicht generell notwendig für gelungene KI-Anwendungen. An dieser Stelle lohnt ein Blick auf den statistischen Charakter von Data Science. Die Grundannahme des Maschinenlernens ist das Vorhandensein einer Grundgesamtheit, die sich in eine oder mehrere Gruppen einteilen lässt (Clustering). Abweichungen davon sind Anomalien. Eine Menge, die nur aus hochgradig individuellen Datensätzen besteht, ist also für Data Science nur bedingt geeignet. Unsere elektrischen Netze sind klar gruppierbar, etwa durch ähnliches Nutzerverhalten oder Spannungsebenen. Damit stellt sich die Frage, wie viele Kunden gemessen werden müssen, bis eine Verhaltensgruppe (Cluster) stabil identifiziert ist. Zu diesem Zweck hat die BKW rund 7000 anonymisierte Lastprofile untersucht. Die Lastprofile wurden in 15-Minuten-Intervallen erhoben. Vergleichend wurden die gemessenen Daten auf ein grösseres Intervall von 60 Minuten gemittelt. Kleinere Leistungsschwankungen werden damit geglättet.

Da nicht alle Kunden Boiler betreiben und diese sich in Nennleistung und

Profil, Minuten	Leistungslimit, kW	Cluster	Anzahl Punkte im Cluster	Nötige Stichprobengrösse (Methode 1)	Nötige Stichprobengrösse (Methode 2)
60	5	0	5426	981	831
60	5	1	1212	198	170
60	15	0	6451	1140	969
60	15	1	982	328	247
15	5	0	3757	1151	881
15	5	1	887	328	240
15	15	0	4632	1284	1006
15	15	1	238	517	164

Tabelle 1 Nötige Stichprobengrösse für die identifizierten Cluster bei einem Vertrauensintervall von 95 % und einer Unsicherheit vom Mittelwert von ±10 %.

RÉSUMÉ

Résilient et efficace dans le nouvel univers énergétique

Le défi de la communication en réseau

Les énergies renouvelables et, de plus en plus, l'Internet des objets font désormais partie intégrante de notre univers énergétique. Dans ce dernier, les petites installations privées et les grands systèmes sont généralement raccordés à un réseau électrique existant. Via le réseau européen interconnecté, le prosommateur suisse est ainsi relié à des parcs éoliens dans le nord de l'Allemagne, à des installations industrielles en Suède et à des centrales électriques en Turquie.

Le concept le plus connu pour l'exploitation de systèmes énergétiques en réseau est probablement le smart grid. Les appareils situés sur le terrain collectent des informations qui sont traitées par le fournisseur d'énergie via une intelligence centralisée pour créer, entre autres, des commandes de contrôle optimisées. Un tel système doit garantir pendant des décennies que chaque composant est, et reste, protégé contre toute sorte d'agresseurs issus du monde entier.

Basé sur la théorie des réseaux, cet article présente les effets possibles de la communication fortement interconnectée sur la cybersécurité et l'efficacité des systèmes. Des alternatives résilientes sont discutées, par exemple en utilisant des méthodes statistiques. Les études fondamentales présentées montrent clairement qu'il est aussi nécessaire de repenser la mise en réseau et la collecte de données dans le secteur de l'énergie. De nouvelles approches, innovantes et décentralisées, sont essentielles pour un approvisionnement énergétique résilient, sûr et efficace, aujourd'hui et à l'avenir. NO

Betriebszeitpunkt unterscheiden, wurde in dieser Studie ein Leistungslimit von 5 und 15 kW eingesetzt. Dieses Vorgehen erzielt mit geringem Aufwand eine Vorgruppierung und Plausibilitätsprüfung von Werten. Anschliessend wurde die ideale Anzahl von Clustern für diese Studie untersucht und die Daten wurden mit dem *k*-means-Verfahren auf zwei Cluster verteilt. Für jeden Intervallschritt wurde nun die minimal zu messende Anzahl von Kunden bestimmt, um in einem vordefinierten Vertrauensintervall mit einer festgelegten Genauigkeit beim Mittelwert aller Kunden zu diesem Zeitpunkt zu liegen. **Tabelle 1** fasst die Ergebnisse zusammen.

In der Regel reicht es damit, rund 1000 oder sogar unter 500 Kunden zu vermessen, um alle anderen Kunden mit einer Wahrscheinlichkeit von 95 % bis auf ±10 % Genauigkeit im Messwert zuordnen zu können. Wie in **Bild 4** ersichtlich, trifft dies sogar nur auf wenige Zeiten im Tagesverlauf zu und der Grossteil des Tages lässt sich mit deutlich unter 500 Datenpunkten charakterisieren. Dabei ist die übliche Messunsicherheit von 3–9 % (je nach Aussentemperatur) noch nicht berücksichtigt.

Methode 1 berechnet die nötige Stichprobengrösse für eine grosse Grundgesamtheit, die **Methode 2** für eine begrenzte Stichprobe gemäss folgenden Formeln:

Methode 1

$$N = \frac{Z^2 \cdot \sigma^2}{err^2}$$

Methode 2

$$N = \frac{Z^2 \cdot \sigma^2 \cdot \frac{N_{samples}}{N_{samples} - 1}}{err^2 + \frac{Z^2 \cdot \sigma^2}{N_{samples} - 1}}$$

$N_{samples}$ steht für die Anzahl der Proben in der Grundgesamtheit in Methode 2 und entspricht der Anzahl der Smart Meter in den Clustern. Die Variable Z ist das Standardziel der jeweiligen angestrebten kumulativen Wahrscheinlichkeit, in diesem Fall 0,95. *err* ist der tolerierte Fehler, in diesem Fall ±10 % des Mittelwertes des Profilpunktes.

Die vorgestellten grundlegenden Untersuchungen zeigen deutlich: Ein Umdenken in Vernetzung und Datenerhebung ist grundlegend nötig, auch in der Energiebranche. Neue, innovative und dezentrale Ansätze sind Grundlage für resiliente, sichere und effiziente Energieversorgungen heute und in der Zukunft. Die Zukunft ist vernetzt und digital – bewusst und intelligent.

Referenz

[1] thehackernews.com/2018/04/iot-hacking-thermometer.html?_sm_byp=iVV1SsDqLrtJrq7N

Autoren

Dr. Ing. **Monika Freunek** war Leiterin Datensicherheit und Data Science Verteilnetzmanagement bei BKW.
→ BKW Energie AG, 2560 Nidau
→ monika.freunek@gmx.de

Dr. **Gabriel-Mihai Lipsa** ist Lead Data Scientist bei BKW.
→ gabriel-mihai.lipsa@bkw.ch