Unter Strom

Absicherung verteilter, intelligenter Stromnetze notwendig

Kai-Oliver Detken

In Zukunft werden die Energiesysteme der Zukunft ihren zentralen Charakter verlieren und dezentral Angebot und Nachfrage nach Energie steuern müssen. Diese Entwicklung wird u.a. durch den Bau von Windkraftwerken und Solarkollektoren hervorgerufen, die an dezentralen Standorten Energie erzeugen. Das Energiesystem der Zukunft muss daher ein intelligentes Netz, ein sogenanntes Smart Grid, sein, dass die Energie dort bereitstellt, wo sie gebraucht wird. Ein Hauptaugenmerk muss bei Entwicklung und Planung eines Smart Grid auf seine Absicherung liegen, da diese neue Art der Netzstruktur ganz neue Anforderungen an die IT-Sicherheit stellt.

Prof. Dr.-Ing. Kai-Oliver Detken ist Dozent an der Hochschule Bremen im Fachbereich Informatik sowie Geschäftsführer der Decoit GmbH

Ein intelligentes Stromnetz (engl. Smart Grid) umfasst die kommunikative Vernetzung und Steuerung von Stromerzeugern und -speichern, elektrischen Verbrauchern und Netzbetriebsmitteln in Energieübertragungs- und -verteilungsnetzen zur Elektrizitätsversorgung. Alle miteinander verbundenen Komponenten sollen zur Optimierung und Überwachung des gesamten Energienetzes dienen. Dadurch will man die Energieversorgung auf intelligente Art und Weise dort bereitstellen, wo sie benötigt wird. Zusätzlich soll ein effizienter und zuverlässiger Netzbetrieb gewährleistet werden.

Durch erneuerbare Energien, die beispielsweise durch Solaranlagen in Wohngebieten und Windparks erzeugt wird, entwickelt sich das derzeitige zentrale Stromnetz stark hin zu einem dezentralen Netz, das ganzheitlich verwaltet und gesteuert werden muss. Dieser Trend bringt zwei große Herausforderungen mit sich:

- mangelnde Vorhersagbarkeit, wie viel Energie wann erzeugt wird;
- mangelnde Regelbarkeit der erzeugten Energieleistung.

Die Aufgaben der Zukunft bestehen darin, mehr erneuerbare Energien zu nutzen, die Versorgungssicherheit zu erhalten und die Energieeffizienz in einem liberalisierten Binnenmarkt mit grenzüberschreitendem Stromhandel und zunehmenden Leistungsflüssen in den Übertragungsnetzen zu steigern. Benötigt werden daher dynamische und flexible Netze, die viele dezentrale Erzeuger zu größeren Einheiten, d.h. virtuellen Kraftwerken, vereinen können. Erst das ermöglicht eine planbare Betriebsführung.

Ein weiterer Ansatzpunkt für Smart Grids ist neben der Erzeugungs- und Verteilungsseite auch das Lastmanagement. Künftig könnten auf lokaler und regionaler Ebene verbundene Erzeugungsquellen und Verbraucher

Windpark Dubener Platte
(Foto: Das Grüne Emissionshaus)

über ein Smart Grid mit Zentralrechnern vernetzt werden. In der Industrie durchaus üblich, ist Lastmanagement in Privathaushalten bis auf den bekannten Nachtstromzähler bisher weitgehend unbekannt. Die Grenzen zwischen Erzeugern und Verbrauchern werden damit teilweise sogar verschwimmen und daraus neue Geschäftsmodelle entstehen.

Grundlage für Smart Grids ist eine mittelfristige Investitionsoffensive in die Netzinfrastruktur. Dazu gehören neben intelligenten Stromzählern ein verstärkter Einsatz von IKT-Komponenten (IKT – Informations- und Kommunikationstechnik) und leittechnischer Intelligenz sowie eine Automatisierung der Verteilernetze und Systeme zum dezentralen Energiemanagement.

Dabei befinden sich die TK-Anbieter in einer guten Ausgangsposition, da sie die Herausforderungen dieser Integration adressieren können und über wesentliche Erfahrungen und Fähigkeiten verfügen. Dies beinhaltet u.a. das umfassende Verständnis großer IP-Netze, Erfahrungen mit Cloud Computing, umfangreiches Wissen zu Serviceplattformen sowie Erfahrung mit Kooperationen.

Architektur der Energienetze

Das typische Stromnetz ist ein geografisch weit verwobenes Netz, u.a. bestehend aus Generatoren, Übertra-

gungsleitungen, Wirk- und Blindleistungkompensatoren und Lasten. Dieses vermaschte Hochspannungsnetz verbindet die Generatoren mit den Schaltanlagen, die durch das Verteilungsnetz den Benutzer mit elektrischer Energie versorgen. Hierbei liegen Erzeugung und Verbrauch räumlich weit auseinander. In der Verteilung von Energie dominieren bisher oft regionale Stromnetze mit zentraler Stromerzeugung. Durch den zunehmenden Einsatz regenerativer Energiequellen gibt es einen starken Anstieg der Langstreckenübertragung. Hingegen sind moderne Stromnetze mehr und mehr länderübergreifend vernetzt. Die Deregulierung des Strommarktes hat auch zu einem zunehmenden Energietransfer geführt. Darüber hinaus geht der Trend in Richtung einer dezentralen Stromerzeugung durch zahlreiche Kleinkraftwerke, vor allem durch regenerative Energien, und führt zu einer wesentlich komplexeren Struktur heutiger Netze.

Der Begriff Smart Grid bezeichnet die ganzheitliche Organisation der modernen Stromnetze zur Steuerung, (Lasten-)Verteilung, Speicherung und Erzeugung von elektrischer Energie. Auch sind Aspekte der Abrechnung zu beachten. Ein Bestandteil intelligenter Netze ist die Möglichkeit der Energieversorger, den Stromverbrauch der Endkunden automatisch zu erfassen, ohne Stromzähler vor Ort ablesen zu müssen. Erste Pilotprojekte wurden beispielsweise von der Energie AG in Österreich (**www.energieag.at**) zusammen mit Siemens realisiert.

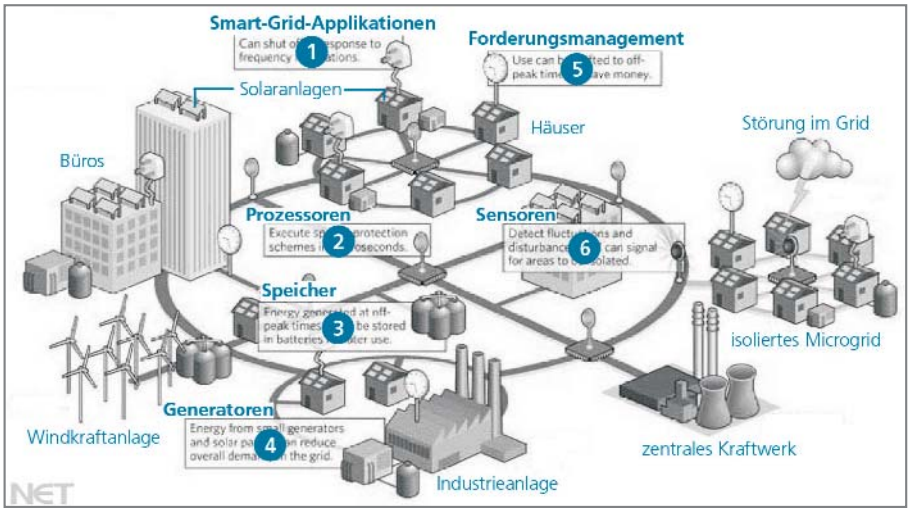
Weitere Versuche erfolgten im Rahmen des Projekts E-DeMa (**www.e-dema.com/de/index.html**), bei dem rund 500 digitale Stromzähler in Privathaushalten installiert wurden. E-DeMa entwickelt Lösungen, um die Stromversorgung intelligenter zu machen. Der Kunde soll künftig seinen Stromverbrauch danach ausrichten können, wann beispielsweise der Preis innerhalb eines Tages am günstigsten ist. Darüber hinaus soll er auch als Anbieter auf dem Energiemarktplatz tätig werden können. Hat er zum Beispiel ein kleines Blockheizkraftwerk oder eine Brennstoffzelle im Keller oder eine Photovoltaikanlage auf dem Dach, kann er überschüssigen Strom in das Netz einspeisen. Der Kunde wird zum „Prosumer", also Verbraucher und Anbieter zugleich.

E-Energy (**www.e-energy.de**), auch „Smart Grids – Made in Germany" genannt, heißt das nationale Leuchtturmprojekt in diesem Bereich in Deutschland. Sein Hauptziel liegt in der Schaffung von E-Energy-Modellregionen, die zeigen sollen, wie das große Optimierungspotenzial der Informations- und Kommunikationstechniken zum Erreichen von mehr Wirtschaftlichkeit, Versorgungssicherheit und Umweltverträglichkeit in der Stromversorgung am besten genutzt werden kann. Hierzu werden integrative Konzepte entwickelt und praxisnah erprobt, die das Gesamtsystem der Elektrizitätsversorgung von der Erzeugung über Transport und Verteilung bis hin zum Verbrauch optimieren.

Ein Smart Grid wird darüber hinaus weitreichende Funktionen erfüllen, wie z.B. das Liefern von Informationen zur Steuerung der lokalen Energieeinspeisung an die verteilten Energieerzeuger. Durch diese Erweiterung ergeben sich deutlich höhere Anforderungen an die IT-Sicherheit und Vertrauenswürdigkeit der einzelnen Komponenten, um einem Ausfall bzw. einer Beeinträchtigung des Gesamtsystems entgegenzuwirken.

Durch die zunehmende Menge an verteilten Erzeugern verwandelt sich das Stromnetz von einem linearen Netz mit seinen Effekten in ein hoch stochastisches Netz, das mit der aktuell noch eingesetzten Scada-Technik (Supervisory Control and Data Acquisition) nicht mehr überwacht werden kann. Somit ist mit der Erfüllung der Smart-Grid-Vision auch ein notwendiger Ausbau der Mess- und Kommunikationsinfrastruktur auf Mittel- und Niederspannungsebene notwendig. Von besonderer Bedeutung sind hierbei die Phasor Measurement Units (PMU). Diese sind im Gegensatz zu Scada-Systemen in der Lage, nicht erst das Bestehen einer Frequenzabweichung zu entdecken, sondern die durch eine Änderung des Phasenwinkels der Spannung sich abzeichnende Differenz. Eine Möglichkeit, die PMUs zu kontaktieren und zu bedienen, besteht über das TCP/IP-Protokoll.

Um die zunehmende Anzahl an Geräten sinnvoll in die Gesamtstruktur zu integrieren, ist es notwendig, sich von



Vision eines Smart Grid
1 – schlaue Anwendungen zum automatischen Ausschalten bei hoher Netzfluktuation
2 – kann zur Verschiebung der Stromabnahme in den geringeren Netzlastbereich genutzt werden
3 – Entdecken von Fluktuationen und Störungen sowie zum Signalisieren, dass bestimmte Bereiche isoliert werden sollen
4 – Ausführen spezieller Schutzschemata in Mikrosekunden
5 – Energie, die bei geringer Netzlast erzeugt wurde, kann für spätere Nutzung gespeichert werden
6 – kleine Generatoren und Solaranlagen helfen den Energiebedarf im gesamten Stromnetz zu minimieren
(Quelle: N. Kuntze, C. Rudolph, M. Cupelli, J. Liu, and A. Monti: Trust Infrastructures for Future Energy Networks, Journal of Latex class files, Vol. 6, Nr. 1, Januar 2007)

einer aktuell zentralen hin zu einer zukünftig dezentralen Regelung zu entwickeln. Hierbei nimmt die Einbeziehung der IT-Sicherheit einen erhöhten Stellenwert ein.

IT-Sicherheit

Der erste Berührungspunkt von Netzbetreibern mit Smart Grids liegt in der Messinfrastruktur (siehe *Grafik* auf Seite 42). Die Kommunikationstechnik und Geräte hinter der Advanced Metering Infrastructure (AMI) bilden eine wichtige Grundlage von Smart-Grid-Techniken. Es ist wesentlich sinnvoller, Advanced Meters (Smart Gateways) als Schnittstelle zu den dahinter liegenden Geräten (Wohnenergiespeicher) und dezentrale Erzeugungseinheiten zur Regelung zu verwenden, als diese direkt anzusprechen. Applikationen für solche Smart Gateways bieten zudem die Möglichkeit zur Umsetzung neuer Geschäftsideen für das Stromnetz der Zukunft, wie z.B. die Kontrolle des Energieverbrauchs elektrischer Geräte durch den Endkunden.

Die Netzbetreiber verwenden zunehmend mehr digitale Geräte in Schaltanlagen. Diese haben die Aufgabe, den Schutz zu verbessern, die Schaltanlagen zu automatisieren sowie die Zuverlässigkeit und Regelgüte zu erhöhen. Allerdings lassen diese aus der Ferne zugänglichen und programmierbaren Geräte Bedenken hinsichtlich der IT-Sicherheit aufkommen. Beispielsweise könnte ein Angreifer durch ein Manipulieren der Smart Gateways ohne Entgelt Strom konsumieren, nicht gelieferten Strom in Rechnung stellen oder auch auf die Verfügbarkeit des Gesamtnetzes Einfluss nehmen sowie die Stromversorgung unterbrechen. Von der North American Electric Reliability Corporation (NERC) wurden Standards entwickelt, die diese Probleme berücksichtigen. Smart Grids müssen eine bessere Integration dieser Geräte, den vermehrten Einsatz von Sensoren und weitere Regelungsschichten bieten. Diese Regelungsschichten haben allerdings ihre eigenen Sicherheitsanforderungen, die eine umfassende, integrierte Sicherheitsbetrachtung benötigen.

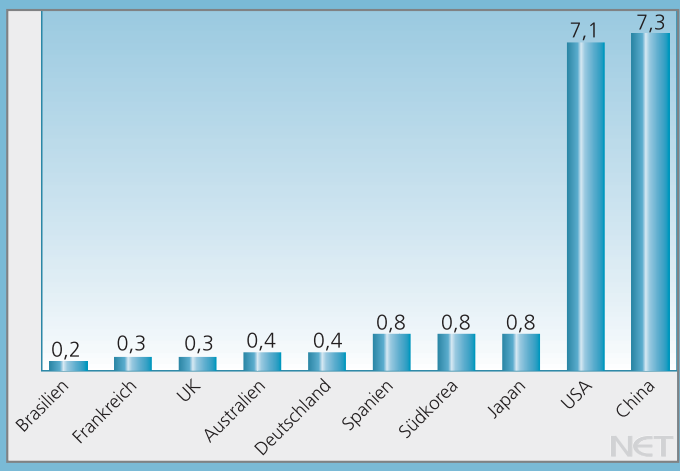
Die Herausforderungen für diese Entwicklung sind nicht nur technischer und wirtschaftlicher, sondern auch organisatorischer Natur. Komponenten eines Smart Grid und IT-Systeme müssen in die Lage versetzt werden, Einbruchsversuche zu erkennen, zu melden und bereits autonom darauf zu reagieren, so dass Auswirkungen minimiert werden. Um die Verlässlichkeit des Gesamtsystems sicherzustellen, ist eine sichere Implementierung der lokalen Systeme unverzichtbar. Teile der elementaren Steuertechnik werden in den direkten physischen Einflussbereich der Endkunden verlagert. Dieser ist im Allgemeinen als potenzieller Angreifer auf das übergeordnete Netz anzusehen.

Als Anforderungen an die IT-Sicherheit in Smart Grids muss daher gelten:

- Messung der Systemintegrität
  Um eine Aussage über die Systemintegrität von Smart-Grid-Komponenten sicher erfassen und ableiten zu können, muss die Systemintegrität unverfälscht festgestellt werden können. Hierbei könnte der Trusted-Computing-Ansatz hilfreich sein, der die Integrität von Komponenten durch einen TPM-Chip überprüft, der unverfälschte Messergebnisse zur Verfügung stellen kann. Anhand dieser Ergebnisse kann

Smart Meter – das unbekannte Wesen

Durch die gezielte Steuerung der Stromnachfrage können Energieversorger vom heutigen ineffizienten und klimaschädlichen Prinzip der Höchstlastvorhaltung abrücken. Allein bei Privathaushalten könnten durch die Einführung von zeitabhängigen Tarifen und die Visualisierung des tatsächlichen Energieverbrauchs an einem Smart Meter nach konservativer Schätzung 9,5 TWh Strom pro Jahr gespart werden. Allerdings, so stellte der Bitkom in einer aktuellen Befragung fest, gibt es in der deutschen Bevölkerung enorme Wissensdefizite über intelligente Stromnetze. Zwar ist das Bewusstsein für einen verantwortungsvollen Umgang mit Energie durchaus vorhanden. Fast jeder Verbraucher versucht, seinen Strombedarf zu reduzieren. Auch die Bereitschaft, sog. flexible Stromtarife zu wählen, bei denen der Strom in Nebenzeiten günstiger ist, ist hoch. 41 % der Verbraucher würden in solche Tarife wechseln, wenn sie dadurch Geld sparten; bei den 30- bis 49-Jährigen sind es sogar 52 %. Die hierzu notwendigen intelligenten Stromzähler, sogenannte Smart Meter, kennen allerdings nur 14 % der Bevölkerung.



Staatliche Fördergelder für Smart Grids im Jahr 2010 (in Mrd. $)
(Quelle: Zpryme Research & Consulting)

„Was die Ausbreitung von Smart Metern im europäischen Maßstab angeht, befindet sich Deutschland nicht in einer führenden Position", konstatierte dann auch Volker Smid vom Bitkom-Präsidium auf der Smart-Grid-Pressekonferenz während der Cebit. Hier müsse mehr getan werden, Lippenbekenntnisse genügten nicht. Ebenso steht Deutschland derzeit mit knapp 400 Mio. € Investitionen in Smart Grids im internationalen Vergleich auf verlorenem Posten (*Grafik*). Andere Länder, allen voran China und die USA, fördern diesen Bereich weitaus stärker.

dann eine Aussage über die Geräteintegrität erfolgen.

- Attestation
  In unterschiedlichen Computersystemen wird in der Regel eine schwache Plattformauthentifizierung, z.B. basierend auf der IP- bzw. MAC-Adresse oder der Rechner- bzw. Betriebssystem-ID, als ausreichend betrachtet. Die Gefährdung des Systems durch den Einsatz von verfälschten bzw. manipulierten Systemen sollte bei Smart Grids allerdings ausgeschlossen werden. Dazu ist eine starke Authentifizierung notwendig, um eine zertifizierte Aussage über die Integrität eines Computersystems vornehmen zu können. Hierfür kann ebenfalls der Trusted-Computing-Ansatz verwendet werden, um die von einem TPM-Chip generierten Messwerte des Systemzustands vertrauenswürdig an eine entfernte Entität (z.B. Server) übermittelt.

Leider werden solche Überlegungen bisher nicht in die Planung von Smart Grids einbezogen. Dass dies notwendig ist, zeigen die Vorkommnisse, die durch den Stuxnet-Virus ausgelöst wurden. Stuxnet ist ein Computerwurm, der im Juni 2010 entdeckt und speziell für ein System zur Überwachung und Steuerung technischer Prozesse (Scada-System) der Firma Siemens entwickelt wurde. Man nimmt an, dass dieses Programm mit dem Ziel geschrieben wurde, die Leittechnik einer Anlage zur Urananreicherung im Iran zu sabotieren. Als bisher einzigartig gilt, dass zum ersten Mal Steuerungsanlagen von Industrieanlagen direkt angegriffen werden konnten, da hierfür eigentlich entsprechendes Expertenwissen notwendig ist. Dies kann sich in Zukunft, gerade durch die Hinzunahme des IP-Protokolls zur Steuerung von Smart Grids, durchaus wiederholen.

Ausblick

Die Einführung von „intelligenten" Stromnetzen wird weltweit als der nächste wichtige Schritt im Bereich der Energieversorgung angesehen. Das Ziel muss es dabei sein, eine ganzheitliche Lösung für die neuen Herausforderungen anbieten zu können. Das wichtigste Element in der Einrichtung eines Smart Grid ist dabei die Etablierung einer gemeinsamen Kommunikationsinfrastruktur, die sich bis zu den Endkunden erstreckt. Hierbei wird es aus Kostengründen Kooperationen zwischen Anbietern von öffentlichen Netzen wie beispielsweise ISDN-, ATM- oder IP-basierten Netzen sowie den Energienetzbetreibern geben.

Erste Schritte auf dem Weg zu Smart Grids und deren Marktdurchdringung können am Beispiel der intelligenten Stromzähler ausgemacht werden. Dabei werden hohe Steigerungsraten erwartet, da bereits im Jahre 2009 ca. 76 Mio. intelligente Stromzähler weltweit verbaut wurden. Dies stellt allerdings lediglich einen Teil der Endgerätebasis dar. In Zukunft werden intelligente Häuser (Smart Homes), Gas-, Wasser-, Stromzähler (Smart Meter) und entsprechende Energienetze (Smart Grids) zusammenwachsen und über Fest- oder Mobilfunknetze der dritten bzw. vierten Generation (z.B. UMTS und LTE) interagieren.

Die Vorteile für alle Marktbeteiligten sind vielfältig und besonders im Hinblick auf die Trends Elektromobilität und regenerative Energieerzeugung interessant. Die M2M-Kommunikation (Maschine zu Maschine) leistet dabei sowohl zur vertikalen Integration der Energieerzeugung bis zum Verbraucher als auch zur horizontalen Integration der „Smart"-Anwendungsfelder den entsprechenden Beitrag. Daraus ergibt sich ein enorm hohes Marktpotenzial für M2M-Anwendungen, das hohe Nutzungspotenziale enthält. Dabei stehen an erster Stelle eine Kosten- (72 %) und Zeitersparnis (53 %) sowie Umsatzsteigerung (31 %) und Wettbewerbsvorsprung (42 %). Allerdings ist die Verbreitung noch sehr gering.

Bei aller Euphorie bei der Implementierung von Smart Grids, muss der IT-Sicherheit eine erhöhte Aufmerksamkeit gewidmet werden. Diese Thematik wird von den Energieerzeugern meistens noch unterschätzt, muss aber umgesetzt werden, will man sich zukünftig gegen Viren wie Stuxnet erwehren. *(bk)*