Alcatel-Lucent Stiftung für Kommunikations-forschung

Sicherheit im Smart Grid

Eckpunkte für ein Energieinformationsnetz

Claudia Eckert

Sicherheit im Smart Grid

Eckpunke für ein Energieinformationsnetz

Inhaltsverzeichnis

Impressum

Stiftungsreihe 90

Redaktion
Dr. Dieter Klumpp
(Leitung)
Petra Bonnet M.A.

Druck der Broschüre
DCC Kästl GmbH & Co. KG

Postadresse

Alcatel-Lucent Stiftung
Lorenzstraße 10
70435 Stuttgart

Telefon
(0711) 821-45002
Telefax
(0711) 821-42253
E-Mail
office@stiftungaktuell.de

www.stiftungaktuell.de

ISSN 0932-156x

Sicherheit im Smart Grid - Eckpunke für ein Energieinformationsnetz

Claudia Eckert, Christoph Krauß, Peter Schoo

1 Einleitung

Energie gehört zu den Lebensadern der internationalen Wirtschaft. Während die fossilen Energieträger zunehmend knapper werden, steigt in Folge der fortschreitenden Industrialisierung der Energiebedarf gewaltig mit gravierenden Konsequenzen für den Klimaschutz. Die Verknappung der fossilen Energiequellen und die ungelöste Umweltproblematik der Nuklearenergie erfordern nachhaltig wirkende Lösungen, um den steigenden Energiebedarf zu befriedigen und gleichzeitig die Umwelt zu schonen. Notwendig sind Energie-Systeme zur breitflächigen Nutzbarmachung erneuerbarer Energien und die systematische Umsetzung von Energiesparmaßnahmen. Im Gegensatz zu konventionellen Energiequellen weisen aber erneuerbare Energiequellen wie Wind, Sonne oder Wasserkraft ein stark zeitvariantes Verhalten auf und können nur gekoppelt mit Energiespeicherverfahren zum Einsatz kommen. Die klassische Lösung eines Verbundes von Grundlast- und zugeschalteten Spitzenlast-Kraftwerken mit einer hierarchischen Verteilung von Energie zur Verteilnetzebene muss strukturell verändert werden, da erneuerbare Energien beispielsweise durch Photovoltaikanlagen auch auf Verteilnetzebene eingespeist werden und damit die Energiegewinnung nicht mehr hierarchisch sondern dezentral ist. Dies erfordert eine geeignete IKT-Infrastruktur zur Steuerung des Energietransports.

Durch ein dezentrales Management der Verbrauchs- und Angebotsdaten ermöglicht die steuernde IKT-Infrastruktur, den Stromverbrauch nachhaltig zu senken und dabei gleichzeitig die Energiekosten zu reduzieren, aber dennoch die Versorgungssicherheit zu gewährleistet. Dies dient letztlich auch dem Klimaschutz.

Das Energieinformationsnetz ist eine sicherheitskritische Infrastruktur, deren Ausfall oder (partielle) Störung gravierende gesellschaftliche und volkswirtschaftliche Schäden nach sich zieht. Neben den erforderlichen Netzen, um Daten rechtzeitig, korrekt, Privatsphären-bewahrend, vertraulich und vollständig (aus Sicht des Dienstes, der die Daten benötigt) zwischen allen beteiligten Parteien auszutauschen, werden insbesondere auch dezentral betriebene, kooperative Managementsysteme und verteilte Service-Plattformen benötigt, um Angebot- und Nachfrage sowohl auf einer mikroskopischen Ebene (räumlicher Nahbereich) als auch auf einer makroskopischen Ebene (zwischen Energieversorgern, Länder- und Kontinent-übergreifend) zu koordinieren. Im Folgenden bezeichnen wir ein solches komplexes System von Systemen bestehend aus IKT-Infrastrukturen und Energieinformationsmanagementsystemen als Energieinformationsnetz bzw. in Übernahme der englisch sprachlichen Beschreibung als Smart Grid.

Abbildung 1 veranschaulicht ein solches System. Die European Technology Platform Smart Grids (vgl. [ETPS2008]) definiert ein Smart Grid wie folgt: "A Smart Grid is an electronically network that can intelligently integrate actions of all users connected to it – generators, consumers and those that do both – in order to efficiently deliver sustainable, economic and secure electricity supplies." Das National Institute of Standards and Technology (NIST) in den USA nimmt eine etwas erweiterte Sicht auf das Smart Grid ein, die auch diesem Papier zugrunde liegt. Das Smart Grid gemäß NIST (vgl. [EPR2009]) ist: „… modernization of the electricity delivery system so it monitors, protects and automatically optimizes the operation of its interconnected elements, from the central and distributed generator through

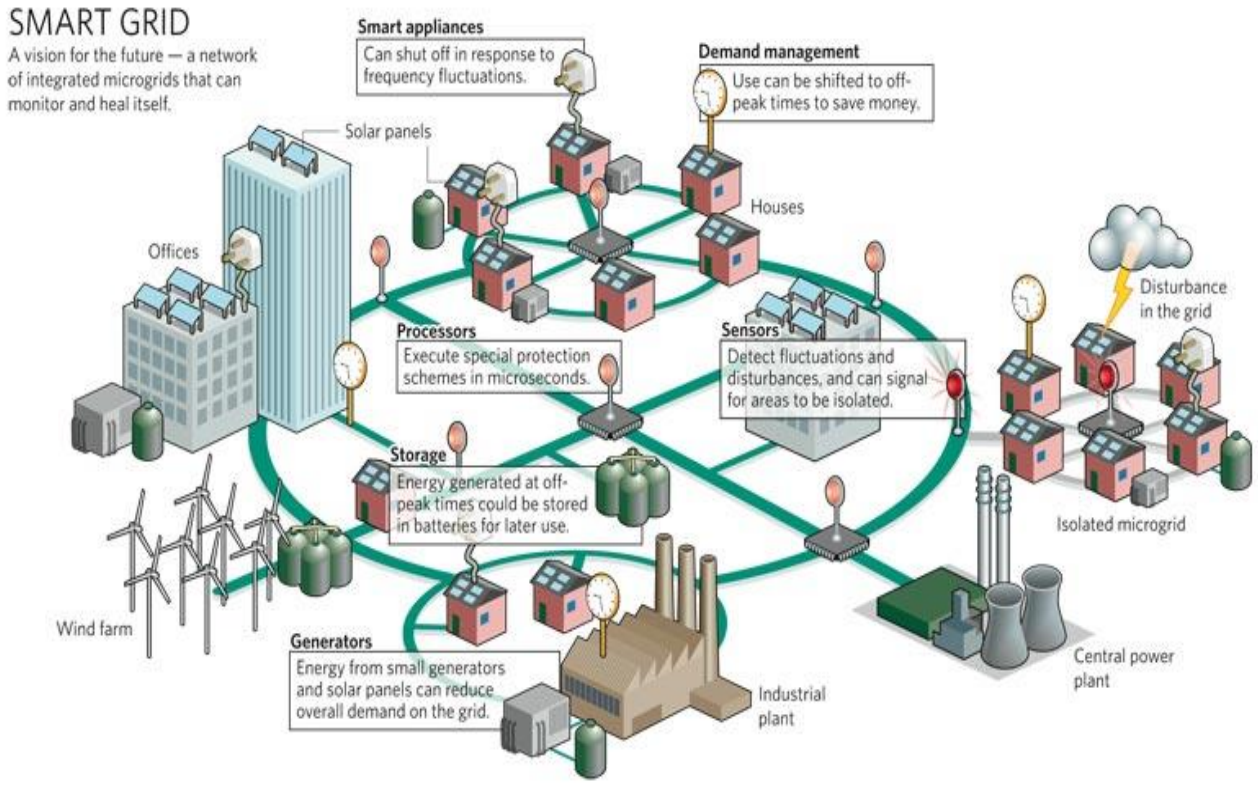


Abbildung 1: Komponenten eines Smart Grid

the high-voltage transmission network and the distribution system, to industrial users and building automation systems, to energy storage installations and to end-use consumers and their thermostats, electric vehicles, appliances and other household devices."

2 Herausforderungen durch das Smart Grid

Während die Energieverteilnetze bereits verhältnismäßig gut ausgebaut sind, ist ein Großteil der Informations- und Kommunikationsinfrastruktur und der Software-Plattformen neu zu gestalten bzw. sind bestehende Infrastrukturen entsprechend auszubauen. Das Energieinformationsnetz der Zukunft ist charakterisiert durch eine dezentrale Struktur (vgl. Abbildung 1). Die Verbrauchsdaten werden dezentral erfasst und abgerechnet, und die Systeme werden vollständig dezentral gesteuert, betrieben und gewartet. Sie bestehen aus einer Vielfalt heterogener Systeme und sind komplex vernetzte Systeme. Steuernde, eingebettete Systeme wie Sensoren und Aktoren und physikalische und betriebliche Prozesse (Physical System) werden integriert und über vielfältige Vernetzungstechnologien unter Einbeziehung des Internets zu einem übergreifenden, vernetzten System, dem Cyber-Physical System (u.a. [Wolf09]) verbunden. Derartige Systeme kombinieren autonome, ressourcenschwache physikalische Geräte, wie u. a. digitale Zähler (Smart Meter) mit ressourcenstarken Backend- und Informationsmanagement-Systemen. Die verschiedenen Komponenten kommunizieren über drahtlose oder drahtgebundene Vernetzungstechnologien, wie WLAN, UMTS oder auch Powerline. Die Systeme sind zudem durch eine hohe Dynamik charakterisiert. Mobile Stromverbraucher und Stromerzeuger in Form von Elektrofahrzeugen

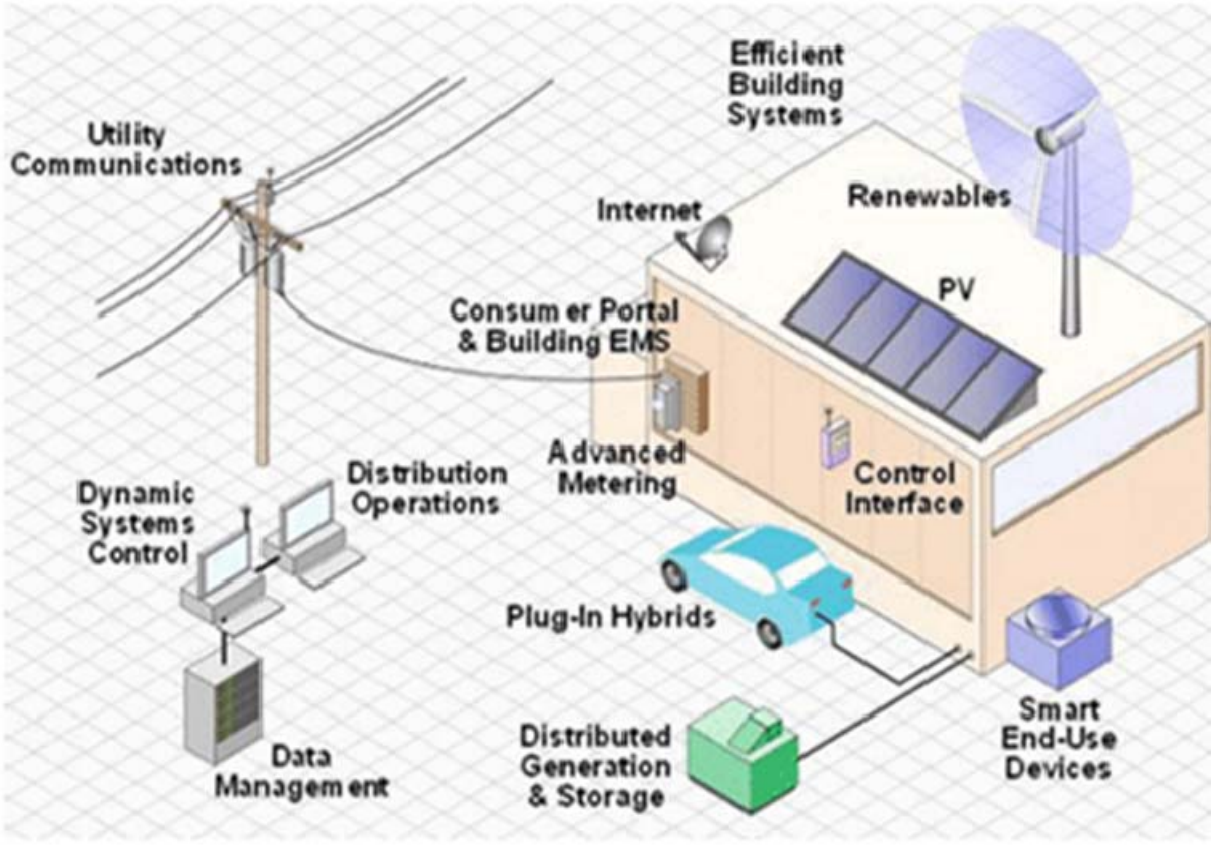


Abbildung 2: Vernetzungsszenarien zukünftiger Smart Grids

(Elektromobilitätsszenarien) und private Strom-Erzeuger, die dynamisch ihren erzeugten Strom in die Netze einspeisen, erfordern ein adaptives, dynamisches Management (Demand Side Management), das in der Lage ist, Lastspitzen zu vermeiden, Energie zwischenzuspeichern und abrufbar zu halten etc.. Der Markt ist dereguliert und muss als ein offener Dienstleistungsmarktplatz für Anbieter und Verbraucher konzipiert und umgesetzt sein.

Abbildung 2 visualisiert eine Vision dieser zukünftigen Energieinformationsnetze bzw. Smart Grids.

Das zu entwickelnde Smart Grid muss die Gesamtheit aller zentralen und dezentralen Energiequellen und -senken sicher und zuverlässig miteinander verbinden. Es muss Komponenten und Dienste anbieten, um den momentanen Energiebedarf und das momentane Energieangebot zu erfassen, und es muss Steuermöglichkeiten zur Verfügung stellen, zur Aktivierung/Deaktivierung von Energieverbrauchern und zur Nutzung gespeicherter Energie. Um diese Aufgaben zu erfüllen, ist die Einführung einer IKT-gestützten Erfassung des dezentralen Energieverbrauchs und ggf. der dezentralen Energieerzeugung zur Einspeisung in das Energienetz durch Smart Meter erforderlich.

Um Interessenskonflikte zu vermeiden, müssen die Zuständigkeiten für die Wahrnehmung der Aufgaben von Erzeugung, Messung, Transport und Abrechnung von Energieeinheiten entkoppelt werden. Gleichzeitig erfordert ein globales Funktionieren eines solch komplexen Systems, dass die beteiligten Parteien Daten austauschen und kooperieren.

Im zukünftigen Smart Grid werden die Funktionsbereiche wie das Erzeugen der Energie[1], der Transport und die Verteilung der Energie, das Messen des Verbrauchs, das Übermitteln der Messdaten oder das Erstellen der Rechnungen, die früher in der Regel in einer Hand lagen, von unterschiedlichen Geschäftspartnern (legal unbundling) ausgeübt. Damit erlangen die Geschäftsbeziehungen zwischen den verschiedenen Teilnehmern am Markt einen immer wichtigeren Stellenwert. Das resultierende Smart Grid ist ein komplexes IKT-System, bestehend aus einer Vielzahl heterogener Subsysteme (Hardware und Software), die dezentral verwaltet werden, teilweise nach Bedarf hinzu- und wieder abgeschaltet werden und sehr unterschiedliche Anforderungen an die zu gewährleistende Sicherheit besitzen (mehrseitige Sicherheit).

Abbildung 3 verdeutlicht die Komplexität der Infrastruktur und die Abhängigkeiten zwischen den Subsystemen. Ein solches Smart Grid stellt hohe Anforderungen an die Qualität der verarbeiteten Daten, die zur Steuerung der gesamten Stromversorgung und der Abrechnung der Leistungen verwendet werden. Die Abbildung beschreibt das von der NIST (vgl. [Lee2009]) entwickelte konzeptuelle Modell einer Referenzarchitektur für das Smart Grid. Die Abbildung verdeutlicht die verschiedenen Akteure in einem solchen Grid. Beispiel für Akteure sind Kunden, Energieversorger, Energielieferanten, Energie-Erzeuger, Service-Anbieter, Marktplatzanbieter etc.. Diese Akteure repräsentieren Rollen, die ähnliche Ziele, einen ähnlichen Schutzbedarf sowie ähnliche Rechte und Pflichten haben. Diese konzeptuelle Bündelung von Aktivitäten zu Rollen ist für eine Sicherheitsbetrachtung sehr nützlich. Sie ermöglicht es, Schutzbedarfe aus Sicht der unterschiedlichen Akteure zu erfassen. So ist beispielsweise eine hohe Verfügbarkeit, hohe Integrität, Aktualität und Vollständigkeit der Daten, die für das Lastmanagement benötigt werden, für die Netzbetreiber essentiell, während für den privaten Endkunden die Vertraulichkeit seiner Verbrauchs- und Abrechnungsdaten und deren Korrektheit sicherlich vordringliche Schutzbedarfe darstellen.

Das konzeptuelle Modell liefert darüber hinaus einen guten Ansatzpunkt, um Abhängigkeiten zwischen Subsystemen zu identifizieren und Domänen gegeneinander abzugrenzen. So werden beispielsweise im Bereich der Steuerung der Energieübertragung vielfach SCADA[2]-Netze eingesetzt, die in Smart Grid-Szenarien nicht mehr wie bislang noch üblich isoliert betrieben werden, sondern vermehrt an das Internet angebunden und darüber mit anderen Subsystemen gekoppelt sind. Ein Angriff auf ein verwundbares SCADA-System kann sich damit kaskadierend in die angeschlossenen Netzsegmente ausbreiten, bzw. über diese Netze können gezielt Angriffe auf verwundbare SCADA-Systeme durchgeführt werden. Die Abbildung veranschaulicht auch, dass die digitalen Zähler (im Bild im Kasten rechts unten als eine Komponente im Bereich der Heimautomatisierung) lediglich ein Baustein in dem Gesamtsystem eines Smart Grid sind. Die Abbildung verdeutlich zudem, dass die Sensoren, Zähler oder aber auch lokalen Energieerzeugungs-Komponenten eines Haushaltes (rechter Kasten unten) zum einen miteinander mittels Kommunikationstechnologie wie WLAN vernetzt sind und zum anderen über verschiedene Netze an die Außenwelt angekoppelt sind. Ein bidirektionaler Datenverkehr ist möglich wie beispielsweise ein Fernzugriff über ein IKT-Netz auf einen Sensor.

[1] Mit Energie-Erzeugung ist hier und im Folgenden die Umwandlung von Primärenergie in Nutzenergie gemeint.

[2] SCADA: Supervisory Control And Data Acquisition

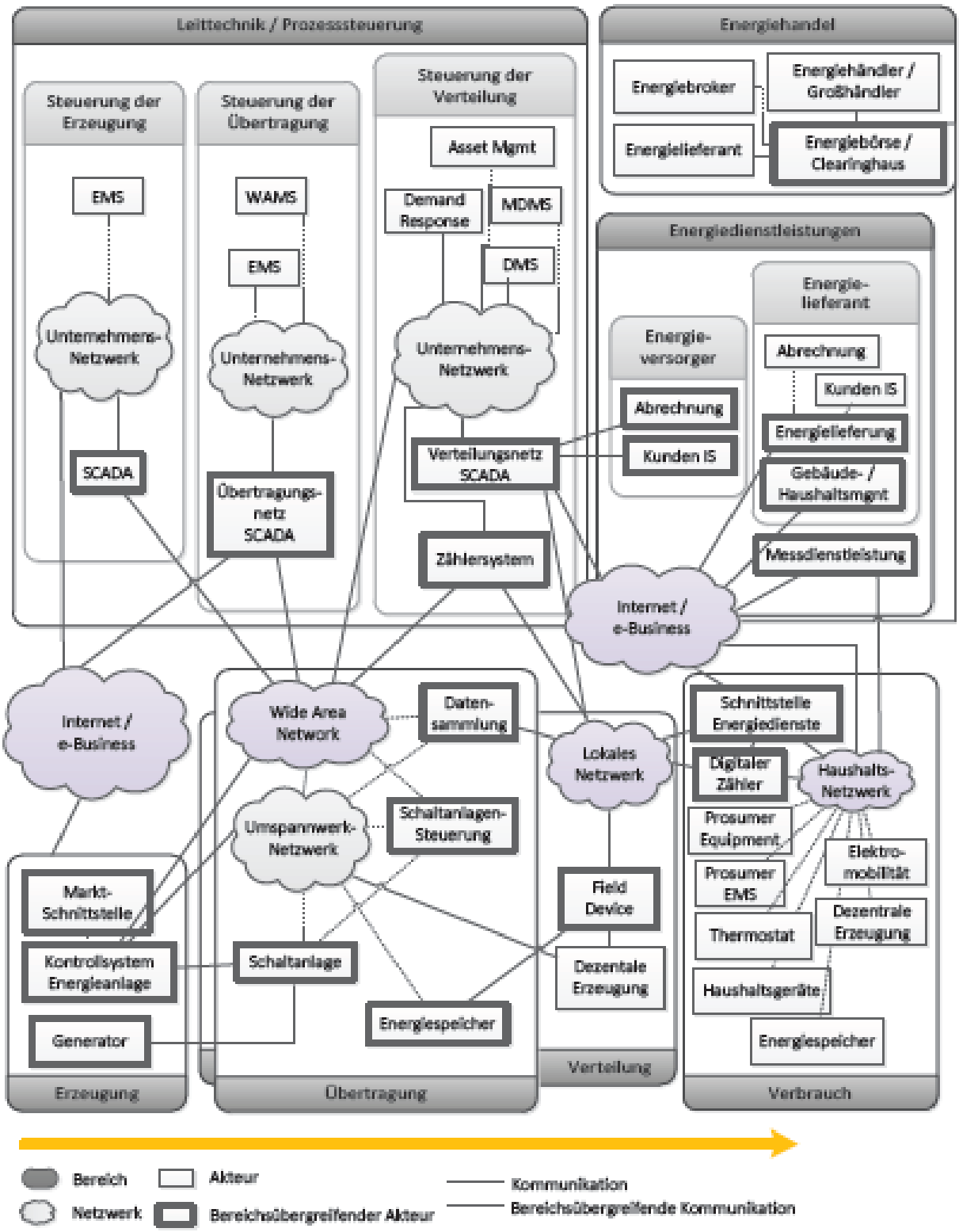


Abbildung 3: Konzeptuelles Modell des Smart Grid (Quelle [Bee2010, Lee2009])

3 Sicherheit und Datenschutz

Die Integration von geeigneten Sicherheitsmaßnahmen [Eck2009] zur Wahrung der Vertraulichkeit der ausgetauschten Daten und des Schutzes der Privatsphäre, aber auch zur Sicherstellung der Korrektheit, der Vollständigkeit der außerhalb des eigenen Kontrollbereichs verarbeiteten Daten sowie die Rechtzeitigkeit der Erbringung der gewünschten Dienstleistungen sind eine unabdingbare Voraussetzung dafür, dass ein solches Smart Grid funktionsfähig und nutzbar ist. Dies ist notwendig, um von den Verbrauchern auch akzeptiert zu werden und damit die gewünschten Effekte hinsichtlich Energieeinsparung und Umweltschutz erfüllen zu können.

Das Smart Grid muss von Anfang an so konzipiert werden, dass es angriffsresistenter als bisherige Infrastrukturen ist, da ein Smart Grid in besonderer Weise eine schützenswerte kritische Infrastruktur darstellt, die vielfältige Angriffsziele bietet. Mit der zunehmenden Abhängigkeit von einem zuverlässigen und robusten Smart Grid für die Versorgungssicherheit steigt die Verletzlichkeit und Verwundbarkeit durch gezielte Angriffe (Terroranschläge, Hackeraktivitäten, Manipulationsversuche).

Eine Herausforderung ist zudem die systematische Integration von geeigneten Maßnahmen, um auch in Ausnahme- und Notfällen das komplexe, vielparametrige System noch zu beherrschen. Die dezentrale Infrastruktur erfordert kooperative Konzepte und eine Kombination aus lokalen und globalen Maßnahmen, deren jeweilige Abhängigkeiten und Auswirkungen verstanden und beherrscht werden müssen. Um ein rechtzeitiges und teilautonomes Handeln zu ermöglichen, werden zudem in stärkeren Maß selbstorganisierenden Prinzipien eingesetzt werden müssen.

Der Datenschutz steht häufig im Konflikt zum Bedarf an Daten für die Steuerbarkeit des Energieverbrauchs. Mangelhafter Datenschutz behindert andererseits die Bereitschaft der beteiligten Parteien, Daten kooperativ auszutauschen. Die geltenden Datenschutzgesetze verbieten bereits heute eine Profilbildung des Endverbrauchers hinsichtlich seiner Lebensgewohnheiten. Ein Smart Grid erfordert somit Lösungskonzepte und Architekturen, um diese rechtlichen Auflagen zu erfüllen. Dazu ist zu klären, welche Daten überhaupt sinnvoll zu erheben sind, wie eine geeignete Aggregierung und Anonymisierung zu gestalten ist und wie durch dezentrale Verarbeitungsschritte eine Profilbildung systematisch verhindert werden kann. Für das kooperative Management sind Maßnahmen zu entwickeln, so dass kritische Daten auch zwischen konkurrierenden Unternehmen vertrauensvoll ausgetauscht werden können, um globale Lagebilder zu erstellen, ohne den Datenschutz zu gefährden.

3.1 Rechtliche Rahmenbedingungen

Das Datenschutzrecht hat bei der Stromversorgung bisher eine eher untergeordnete Rolle gespielt [Ro2010]. Für die Durchführung und Abrechnung der Stromversorgungsverträge wurden nur wenige personenbezogene Daten verwendet. Insbesondere wurde der Energieverbrauch in der Regel nur einmal jährlich erfasst. Die Einführung des Smart Grid verursacht jedoch vielfältige Risiken für die informationelle Selbstbestimmung sowie für die Entscheidungs- und die Entfaltungsfreiheit [Cav2010], so dass sich die Bedeutung des Datenschutzrechts enorm erhöhen wird [Ro2010b]. Insbesondere die Einführung tageszeit- und lastvariabler Tarife und die für die Optimierungsbestrebungen erforderliche detailgenaue Erfassung der Energieverbrauchswerte führen dazu, dass der Umfang der Erhebung (personenbezogener) Daten erheblich steigen wird. Die Daten werden eine neue Qualität aufweisen, die vor allem in der inhaltlichen und zeitlichen Nähe zum realen Geschehen sowie in der Dichte der Angaben liegt, so dass ihnen bei einer Auswertung eine erhöhte Aussagekraft zukommt und damit das Risiko der Erstellung von Persön-

lichkeitsprofilen steigt. Da die Stromversorgung zudem zu den elementaren Lebensbedürfnissen gehört und praktisch jeder Haushalt, jedes Unternehmen, jede Behörde und jede öffentliche Einrichtung ständig und dauerhaft Energie bezieht, wird nahezu jeder Lebensbereich von den Datenerhebungen erfasst.

Die Anzahl der beteiligten Akteure, zwischen denen ein Datenaustausch stattfindet, wird vor allem aufgrund der gesetzlichen Vorgaben zur Entflechtung der Energieversorgungsbetriebe und zur Öffnung des Messwesens anwachsen. Schließlich werden aufgrund der Vervielfältigung der Zwecke, für die die Daten zukünftig benötigt werden, die Anzahl der Datenverarbeitungsvorgänge erheblich zunehmen.

Die datenschutzrechtlichen Risiken können nur durch eine datenschutzkonforme, technische und organisatorische Gestaltung des Energieinformationsnetzes vermieden oder zumindest gemindert werden. Um eine möglichst hohe Effektivität zu erreichen, muss diese datenschutzkonforme Technikgestaltung bereits im Entwicklungsprozess vorgenommen werden. Eine datenschutzrechtliche Bewertung auf der Grundlage gesetzlicher Einzelfallprüfungen bei gleichzeitig klarer Rollenverteilung zwischen verarbeitender Stelle und Betroffenen ist vor dem Hintergrund der besonderen datenschutzrechtlichen Risiken des Energieinformationsnetzes nicht mehr realisierbar. Zudem greifen sie in der Schutzintensität für die informationelle Selbstbestimmung zu kurz.

Zur Unterstützung und Ergänzung einer datenschutzgerechten Gestaltung des Energieinformationsnetzes sollte der Gesetzgeber Rahmenregelungen vorsehen, die die Chancen der informationellen Selbstbestimmung trotz der beschriebenen Risiken erhöhen. Die besondere Schutzbedürftigkeit der Energiedaten könnte durch die Einführung eines Energieinformationsgeheimnisses, eine strenge Zweckbindung, die durch zusätzliche Transparenzanforderungen gestützt wird, sowie gesetzlich manifestierte Anforderungen an die Datensicherheit entsprechend dem jeweiligen Stand der Technik normativ gewährleistet werden. Der verfassungsrechtliche Auftrag des Staates erfordert es, die Interessen der Allgemeinheit an einer zukunftssicheren Energieversorgung und dem Schutz der Umwelt zu fördern und gleichzeitig das individuelle Grundrecht auf informationelle Selbstbestimmung angemessen zu berücksichtigen. Inzwischen fordern die Datenschutzbeauftragten des Bundes und der Länder eine gesetzliche Regelung für die Erhebung der Verbrauchsdaten.

3.2 Technische Rahmenbedingungen

Die wesentlichen technischen Rahmenbedingungen lassen sich wie folgt klassifizieren:

- Energiegewinnung aus erneuerbaren Quellen und Energiespeicherung,
- Messtechnik zur Online-Erfassung von Energieflüssen einschließlich zugehöriger Datenverarbeitung (zeitliche Verläufe, Statistiken, Speicherung),
- Kommunikationsinfrastrukturen zur Verbindung von Energieerzeugern, Energieverbrauchern (inklusive der Web-Schnittstellen zum Zugriff auf die persönlichen Energiedaten), Messstationen, Energiemanagementsystemen und -administrationen,
- Energiemanagementsysteme zur dezentralen Steuerung (z.B. in einem Unternehmen oder privaten Haushalt) sowie zur übergeordneten Gesamtsteuerung,
- Verfahren zur Sicherstellung eines ungestörten Betriebsablaufs bei Teilausfall, vorsätzlichen Angriffen oder Katastrophenszenarien.

Ein wichtiges Elemente in der zukünftigen IKT-Landschaft der Energiebranche ist die kommunikationstechnische Vernetzung, also ein Kommunikationsnetz [Orl2009], das parallel zum Ener-

gienetz für die Übermittlung von z.B. Mess- und Steuerdaten sowie Tarifinformationen sorgen soll.

Dabei sind zwei Bereiche für die Kommunikation von großem Interesse:

(1) der lokale Bereich beim Kunden, der auch Teil einer Heimautomatisierung sein kann, und

(2) der Bereich zwischen dem Kunden und dem Versorger.

Das Kommunikations-Gateway stellt das Bindeglied zwischen diesen beiden Bereichen dar. Es wird als Protokollwandler die Kommunikation über diese Grenze hinweg erlauben, gleichzeitig aber auch als Filter agieren und die Bereiche gegeneinander abschotten. Weiterhin könnte dieses Gateway auch als Plattform für zukünftige Dienste dienen. Je nach Gegebenheiten und Erfordernissen sind unterschiedliche Architekturen möglich. So kann ein solches Gateway dediziert einen Kunden, aber auch mehreren Kunden bedienen, z.B. in einem Mehrfamilienhaus, oder sogar in einer Vorfeldeinrichtung untergebracht sein, wie der Trafostation des Energieversorgers, um dann mehrere Häuser abzudecken. Ein solches Gateway lässt sich zudem nicht nur für den Bereich der Stromversorgung einsetzen, sondern kann im Sinne einer „Multi-Utility Unit" auch für die Bereiche Gas, Wasser und Fernwärme zuständig sein.

Die Vernetzung im Heimbereich, also zwischen Verbrauchsmessung mittels elektronischer Messtechnik, dem Gateway und eventuellen weiteren Elementen einer Heimautomatisierung, kann mittels unterschiedlicher Technologien erfolgen. Zur Auswahl stehen bereits heute verschiedene drahtgebunden Technologien, wie M-Bus, Konnex, LON, oder aber auch die Mitbenutzung der Stromleitung (z.B. Digitalstrom, X10, PLC auf OFDM-Basis), sowie verschiedenste Funktechniken wie Bluetooth, Zigbee, WLAN, Wireless-M-Bus, oder aber auch Glasfaser (POF) und Freiraumoptik (IrDA). Alle diese Techniken haben ihre spezifischen Vor- und Nachteile und in jedem europäischen Land werden andere Auswahlprioritäten gesetzt [Li2010]. Benötigt werden Empfehlungen und Handlungsanleitungen für charakteristische Einsatzszenarien.

Der zweite Bereich betrifft die Kommunikationsnetze zwischen dem Energieinformations-Gateway beim Kunden und einer zentralen Instanz des Versorgers, dem Energieinformationsmanagementsystem. Auch hier gibt es eine Reihe von Optionen wie das Telefonnetz (PSTN, ISDN), DSL-Anschluss, Kabelnetz, oder aber auch den Mobilfunk. Auch neue oder heute noch selten eingesetzte Techniken sind mögliche Kandidatenwie Powerline-Übertragung (Nutzung der Stromleitung), drahtloser Festnetzanschluss (Wireless Local Loop WLL, WiMAX), Glasfaser direkt in die Nähe oder ins Haus (Fiber to the X FTTX). Wie für den Heimbereich müssen auch hier Empfehlungen und Handlungsanleitungen erarbeitet werden, um unter Berücksichtigung der jeweiligen vorhandenen anlagenspezifischen Eigenschaften und den Anforderungen eine geeignete Auswahl und Kombination von Technologien zu treffen.

3.3 Organisatorische Rahmenbedingungen und Sicherheitsmanagement

Umfassende Sicherheit ist kein unveränderbarer Zustand, der einmal erreicht wird und sich nicht wieder ändert. Insbesondere in sich noch entwickelnden Bereichen wie einem Smart Grid wird der Betrieb der Netzwerke und IKT-Systeme ständigen dynamischen Veränderungen unterworfen sein. Viele dieser Veränderungen betreffen neben Änderungen der Geschäftsprozesse, der IKT, von Fachaufgaben, Infrastruktur und Organisationsstrukturen auch die IT-Sicherheit und den Datenschutz. Dies gilt insbesondere für die Energieversorgung als nationale kritische Infrastruktur, die angemessene Sicherheitsstandards für die nachhaltige, weitere Verbesserung des Sicherheitsmanagements der Systeme aller beteiligten Parteien benötigt.

Um dauerhaft ein einmal erreichtes bzw. festgelegtes Sicherheitsniveau aufrecht zu erhalten, muss das Sicherheitsmanagement aktiv betrieben werden. Ein mögliches Vorgehensmodell hierzu wird beispielsweise in den IT-Sicherheitsprozessen des „PLAN-DO-CHECK-ACT"- Regelkreises (ISO 27001) beschrieben. Die Umsetzung der Sicherheitsprozesse erfolgt heute unter Berücksichtigung des Best Practice-Standards ITIL V3 und ist die Basis für das Managementsystem für Informationssicherheit (ISMS) nach ISO 27001. In der Planungsphase des Sicherheitsmanagements werden Sicherheitsmaßnahmen definiert und vorbereitet und ihre konkreten Sicherheitsmaßnahmen werden in der Ausführungsphase den jeweiligen systemischen Anforderungen angepasst bzw. durch neue Maßnahmen bereichert. Hier wird entschieden, welche Maßnahmen angemessen und für den konkreten Fall effektiv wirksam sind. Um derartige Fragen zu beantworten, werden die Methoden aus dem Risikomanagement verwendet, um letztlich Gegenmaßnahmen zu definieren und Entscheidungen unter Abwägung des verbleibenden Restrisikos treffen zu können.

Die heute verwendeten Methoden des Risikomanagements basieren auf Best Practice-Vorgehensmodellen und stellen ein Rahmenwerk dar, um die Sicherheit und Verfügbarkeit in Energieinformationsnetzen nachhaltig zu gewährleisten. Ob diese Normen und Vorgehensweisen auch im Smart Grid anwendbar sind, ist jedoch noch zu klären. So werden durch neue Geschäftsmodelle Abhängigkeiten, Verantwortungsbereiche und Schnittstellen und damit auch das jeweilige Risikomanagement neu zugeschnitten. Zusätzlich entstehen im Smart Grid durch die Kommunikationsinfrastrukturen und Energiemanagementsysteme ganz neue und bisher im Risikomanagement noch nicht erfasste und berücksichtigte Abhängigkeiten und Anforderungen. Die Methoden des Risikomanagements und die dabei verwendeten Werkzeuge müssen erweitert werden, so dass sie auch im laufenden Betrieb eines Smart Grid eingesetzt werden können (z.B. Lagebild und Health-Monitoring). Zudem werden in den bisherigen Ansätzen die domänenspezifischen Standards wie IEC 62351, ISA SP99, NERC CIP oder domänenspezifische Normen für das Sicherheitsmanagement wie VDI/VDE 2182, IEC 6244 nur unzureichend in die Betrachtung mit einbezogen.

4 Stand der Technik

Forschung und Entwicklung zur Gewinnung und Speicherung erneuerbarer Energien erfolgen bereits seit Jahren. Diese Entwicklungen sind nicht abgeschlossen, werden aber im Folgenden nicht weiter ausgeführt, da sich das Papier auf IKT-Aspekte beschränkt. Mit der Einführung von IKT-Lösungen für die vernetzten Teilsysteme der Energieversorgung wurden und werden den rein betrieblichen Anforderungen nach Betriebssicherheit und Systemverfügbarkeit neue Anforderungen hinzugefügt. Wie in vielen anderen Fällen überwogen häufig Time to Market-Ziele, und es wurden durch die neuen Technologien veränderte Anforderungen übersehen und IT-Sicherheit eher vernachlässigt [SP2010]. Spätestens seit dem Ausfall der elektrischen Fernversorgung im Westen der Vereinigten Staaten von 1996 ist die Notwendigkeit von Sicherungsmaßnahmen und der Schutz vor kaskadierenden Effekten allen Betreibern vor Augen geführt worden, und die Gesellschaft konnte von der Abhängigkeit von kritischen Infrastrukturen erfahren [KO2003].

Welche Konsequenzen ein gezielter Angriff für den Betrieb schutzloser Anlagen haben kann, zeigt das durch das US-amerikanische Aurora-Projekt bereits im Jahr 1977 ausgeführte Experiment eines Hacking-Angriffs, der eine gezielte Überlastung eines Generators herbeiführte[3]. Stu-

[3] http://www.cnn.com/2007/US/09/26/power.at.risk/index.html

dien wie [Lu2009] zeigen, dass auch europäische Betreiber ihre Anlagen mittlerweile entsprechend untersuchen und Konsequenzen ableiten. So sieht ENEL, ein in Italien ansässiger und multinational operierender Energieerzeuger, einen deutlichen Handlungsbedarf, die eigenen Anlagen besser gegen

- Denial of Service-Angriffe auf ihre Internet Gateways und das interne Netzwerk der Produktionsanlagen,
- Übernahme von Anlagenteilen durch Angreifer, mittels eingeschleuster Trojaner,
- Manipulation interner Infrastrukturdienste (z.B. DNS Poisining) ,
- Ausnutzen bisher unentdeckter Schwachstellen (zero day exploits) sowie
- Angriffe auf das SCADA-Kommunikationsprotokoll

zu schützen. Dass derartige Sorgen berechtigt sind, hat Mitte 2010 Stuxnet aufgezeigt, ein Wurm, der die Computer von SCADA-Systemen (Leitwarten-Technologie) befallen kann, Teilsysteme gezielt übernahm und außer Betrieb setzte [Fa2010], [Br2010].

Es kann seit geraumer Zeit beobachtet werden, dass eine Reihe von neuen Anstrengungen, sowohl national als auch auf europäischer Ebene, getroffen werden, um neue Lösungen für den innovativen und zuverlässigen Betrieb von Anlagen zur Energieversorgung zu entwickeln. Nationales Beispiel ist das BMWi-Programm *E-Energy: IKT-basiertes Energiesystem der Zukunft* mit seinen über Deutschland in Modellregionen verteilten Projekten[4].

In den USA ist diese Entwicklung ebenfalls zu beobachten. 2007 veröffentlichte die ISA (*International Society of Automation*), eine der führenden non-profit Organisationen im Bereich der Industrieautomation, zwei wichtige Dokumente[5], die Grundlagen beschreiben und Bewertungsverfahren für IT-Sicherheit in Industrieanlagen vorschlagen. Mit einem weiteren Dokument[6] wird versucht, Betreibern Möglichkeiten zur Sicherung der IT-Infrastrukturen ihrer Anlagen an die Hand zu geben. Sie berücksichtigen jedoch nicht die Problematik der Rückeinspeisung durch Prosumer, also von Nutzern, die sowohl Energieverbraucher als auch -lieferanten sind. Ebenso wenig werden in diesen Dokumenten die neuen Anforderungen, die sich durch Elektrofahrzeuge und deren Consumer- (Batterie aufladen) und Producer- Verhalten (Batterieleistung zur Verfügung stellen) ergeben, oder aber nationale Normen berücksichtigt.

4.1 Smart Meter und Messtechnik

Durch die Nutzung intelligenter Stromnetze und -zähler soll eine effizientere Energieversorgung sowie ein transparenteres Abrechnungsmodell für die Verbraucher geschaffen werden. Intelligente Stromzähler sind über öffentliche Netze an die Kommunikationsnetze der Energieversorger angeschlossen und ermöglichen so einen elektronischen Datenaustausch. Zudem bieten sie dem Nutzer eine transparente Verbrauchsanzeige, auf deren Basis er seinen Energieverbrauch steuern und beeinflussen kann. Daher müssen Smart Meter hohen sicherheitsrelevanten Ansprüchen genügen.

Intelligente Zähler erfassen den Stromverbrauch und bereiten die gewonnenen Messwerte zur digitalen Verarbeitung und für die Übertragung zum Messstellenbetreiber auf. Von dort aus können sie auch dem Nutzer, beispielsweise mittels Webzugriff, wieder zur Verfügung gestellt werden. Dabei werden folgende Informationen von

[4] http://www.e-energy.de/

[5] ANSI/ISA-99.00.01-2007, ANSI/ISA-TR99.00.01-2007

[6] ANSI/ISA-99.02.01-2009

der Messung bis zur Abrechnung verarbeitet (vgl. [Sch2010]):

- Verbrauchsdaten, die von der Messstelle erfasst und zum Messstellenbetreiber zum Zwecke der Abrechnung übertragen werden,
- Gerätedaten, die zur Erstellung und Übermittlung der Verbrauchsdaten notwendig sind und den Nutzer für die Abrechnung eindeutig identifizieren,
- Nutzerdaten, die den Verbraucher kennzeichnen und für die Abwicklung der Abrechnung erforderlich sind oder ihn einen Zugang zu einem möglichen Webinterface beim Betreiber der Messstelle gestatten und
- Daten, die Informationen über das zur Abrechnung genutzte System liefern, wie z.B. Verbrauchsumsätze, Systemzustand und Topologie, Zulieferer des Wirksystems oder einzelner Geräte, Ausbreitung und geographische Verteilung des Systems.

Der Betrieb eines solchen verteilten Abrechnungssystems liegt in der Verantwortung des Betreibers. Verschiedene Untersuchungen haben gezeigt, dass marktgängige intelligente Zähler ganz erhebliche Sicherheitsprobleme aufweisen. Sie sind nicht manipulationssicher und können aus der Ferne kontrolliert abgeschaltet werden [An2010]. Bei den smarten Zählern sind noch einige weitere Grundsatzfragen unbeantwortet. Dazu gehören die Fragen nach der Häufigkeit und Frequenz der Messungen oder aber nach der Granularität der zu erfassenden Parameter.

Die 80. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat auf ihrer Sitzung im November 2010 eine gesetzliche Regelung für die Erhebung, Verarbeitung und Nutzung der durch digitale Zähler erhobenen Verbrauchsinformationen gefordert. Die Konferenz der Datenschutzbeauftragten fordert weiter: „Die Anforderungen an den technischen Datenschutz und die IT-Sicherheit sind durch verbindliche Standards festzuschreiben, die der Sensitivität der Daten und den zu erwartenden Missbrauchsrisiken Rechnung tragen. Für die Datenverarbeitungssysteme ist zudem ein integriertes Datenschutz- und Sicherheitsmanagementsystem aufzubauen.“[7]

Die Sicherheit und Vertrauenswürdigkeit dieser elektronischen Zähler, die in Deutschland gemäß dem geltenden Energiewirtschaftsgesetz bei Neubauten und bei Totalsanierungen bereits seit Januar 2010 eingebaut werden müssen, ist ebenfalls noch nicht zufriedenstellend geklärt. So sind diese Komponenten beispielsweise bidirektional mit ihrer Umgebung verbunden. Das heißt, dass sie nicht nur die erfassten Daten der von ihnen überwachten Einheiten (Einzelhaushalte, Gebäude, Liegenschaften) zur Weiterverarbeitung zu den Betreibern senden, sondern selber auch direkt via Fernzugriff durch die Betreiber gesteuert und beeinflusst (z.B. Stromabschaltung) werden können.

Um sicherzustellen, dass bei der Nutzung von intelligenten Stromzählern verbindliche Datenschutz- und Datensicherheitsstandards greifen, wurde das Bundesamt für Sicherheit in der Informationstechnik (BSI) im September 2010 vom Bundesministerium für Wirtschaft und Technologie (BMWi) damit beauftragt, ein entsprechendes Schutzprofil (Protection Profile) zu erstellen. Am 28. Januar 2011 wurde eine erste Version des Schutzprofils für die Kommunikationseinheit (Gateway) des Messsystems vorgestellt. Kern des Schutzprofils des BSI ist eine Bedrohungsanalyse sowie eine Beschreibung von Anforderungen zur Abwehr dieser Bedrohungen. Derzeit ist geplant, das Schutzprofil noch im Jahr 2011 fertig zu stellen. In die Entwicklung eingebunden sind unter anderem der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, die Bundesnetzagentur sowie die Physikalisch-Technische Bundesanstalt.

---

7 http://www.datenschutz.hessen.de/k80.htm#entry3316

Multi-Utility, Heimautomatisierung

Der digitale Stromzähler ist eine Komponente, deren Einführung vom deutschen Gesetzgeber verpflichtend vorgeben ist. Das angesprochene, in Entwicklung befindliche Protection Profile für den Zähler, deckt die Bereiche ab, die durch den Gesetzgeber zu regulieren sind. Dazu gehört der Zähler an sich, der eichrechtliche Anforderungen zu erfüllen hat, sowie seine Schnittstellen (Gateway) nach außen und den Sicherheitsanker (Hardware-Modul). Der Zähler besitzt eine Schnittstelle zu einem Kommunikations-Gateway, an das, wie weiter oben bereits ausgeführt, weitere lokale Geräte der Heimautomatisierung angeschlossen werden können. Das Smart Metering IKT-Gateway (MUC), das vom VDE spezifiziert wird, ist eine solche Gateway-Komponente, mit der, wie in Abbildung 4 aufgezeigt, vorhandene Zähler und Sensoren wie Gas-, Wasserzähler, Heizungsregler, Sonnenkollektoren, aber auch zukünftige Komponenten der Heimautomatisierung Daten austauschen können.

Aus der An- und Einbindung der Geräte der Heimautomatisierung versprechen sich die Experten ein breites Feld für neue Geschäftsmodelle und Dienstleistungsangeboten, nicht nur durch Energienetzbetreiber, sondern auch durch Anbieter von Telekommunikationsdiensten, Wasserversorger, etc. Um diese Vielzahl von Geräten zu unterstützen (multi-utility) sowie zur Anpassung von Protokollen, werden Multi-Utility-Controller bzw. Gateways eingesetzt. Das Protection Profile bezieht sich nicht auf diese Geräte, die beispielsweise zu komplexeren Energiemanager-Komponenten erweitert werden können. Beispiele für solche Energiemanager werden derzeit in den E-Energy-Projekten des BMWi erarbeitet.

Abbildung 4: Multi-Utility bzw. Smart Metering Gateway (MUC) (Quelle: RWE)

4.2 Kommunikationsinfrastrukturen

Die erforderlichen Kommunikationsinfrastrukturen müssen nicht komplett neu konzipiert werden. Hier kann auf den existierenden vergleichsweise technologisch hohen Stand der Kommunikationstechnik aufgebaut werden wie z.B. digitale Anschlussnetze (DSL-Techniken), Mobilfunknetze der 2. und 3. Generation, lokale Funknetze, Sensornetze, lokale Rechnernetze (LAN) und das Internet.

Demgegenüber sind Neuentwicklungen erforderlich zur Vernetzung der (Strom)verbrauchenden Geräte (z.B. über das Stromnetz selbst, die so genannte "Powerline Communication") und für die Übertragung von Steuerdaten in den bestehenden Kommunikationsinfrastrukturen, damit die Übertragung sicher und robust ist und die erforderlichen Steuerungsaufgaben vertrauenswürdig und zeitgerecht erfolgen können. Dies zielt insbesondere auf die Absicherung von SCADA-Systemen ab, die wichtige Bestandteile eines Smart Grid sind (siehe Abbildung 3).

SCADA-Netze

SCADA-Netze werden in der Leittechnik zur Überwachung von Anlagen, Versorgungsleitungen etc. eingesetzt. Dazu werden Sensoren und Aktoren so vernetzt, dass diese über das Feldbus-basierte SCADA-Netz[8] mittels eines PCs oder Programmable Logic Controller (PLC) gesteuert und kontrolliert werden. Derartige Systeme müssen häufig Daten in Echtzeit verarbeiten, sind in der Regel ressourcenbeschränkt (wenig Speicher, wenig CPU-Leistung) und werden in hochsicherheitskritischen Umgebungen betrieben. Die SCADA-Systeme verwenden eigene Protokollfamilien zur Kommunikation, wie CAN (Controller Area Network), CIP (Common Industrial Protocol) oder PROFIBUS (Process Fieldbus), die keine Sicherheitsmaßnahmen wie beispielsweise Verschlüsselung anbieten. SCADA-Systeme haben sich von ursprünglich sehr stark isoliert betriebenen Netzen zu offenen Systemen weiterentwickelt, die mit Standard Soft- und Hardware, sogenannte COTS[9]-Produkte, betrieben werden, über offene Kommunikationsstandards kommunizieren und an das Internet angeschlossen sind. Für die Internet-Anbindung werden spezielle Gateway-Komponenten verwendet, die die Schnittstelle zwischen den Feldbus-basierten SCADA-Protokollen und dem Internet-Protokoll (IP) realisieren. Zu ihren Aufgaben gehört die Umsetzung zwischen den unterschiedlichen Protokollfamilien (Feldbus, IP) sowie auch die Zwischenspeicherungen der Daten, um die Performanz der Gateways zu erhöhen. Durch diese Ankopplung an IP-basierte Netze sind SCADA-Systeme damit den üblichen Gefährdungen derartiger Netze ausgesetzt.

Da SCADA-Netze ursprünglich in isoliert betriebenen Kontrollbereichen zum Einsatz kamen, wo weniger die Sicherheit als die Echtzeit- und Leistungsfähigkeit der Systeme eine Rolle spielte, wurde weitestgehend auf die Integration von Sicherheitsmaßnahmen in derartige Systeme verzichtet. Klassische Sicherheitskonzepte, wie man sie in der herkömmlichen Business-IT findet, wie starke Zugangs- und Zugriffskontrollen, Firewalls und Einbruchserkennungsverfahren (Intrusion Detection) oder aber auch Logging- und Monitoring-Verfahren, kommen in SCADA-Systemen nicht oder nur sehr eingeschränkt zum Einsatz. Da die Daten in Echtzeit verarbeitet werden müssen, führen Filterungen und aufwändige Kontrollen oder Ver- und Entschlüsselungsoperationen zu Verzögerungen, die wiederum für die Betriebssicherheit der Systeme problematisch sind und deshalb in der Regel nicht eingesetzt werden. Häufig wird zudem ganz bewusst auf starke Maßnahmen zur Authentisierung des Bedienper-

[8] Es gibt über 150 meist proprietäre Protokolle in diesem Bereich, jedoch werden zunehmend offene Protokollstandards eingesetzt.

[9] Commercial of the Shelf

sonals an den Kontroll-Systeme verzichtet, und es werden Passwort-basierte Verfahren eingesetzt, um den gefürchteten Lock-out-Effekten zu begegnen. Diese Effekte beziehen sich auf operative Notsituationen, in denen das Bedienpersonal sehr schnell eingreifen und mit entsprechenden Steuerungskommandos die in Echtzeit betriebenen Anlagen abschalten oder andere Notfallmaßnahmen vornehmen muss. Das Personal muss sehr schnell einen direkten Zugriff auf die Anlage haben; Verzögerungen durch vergessene lange Passworte, nicht verfügbare Zugangstoken wie Smartcards, versagende biometrische Authentisierungen etc. werden häufig als zu hohe Risiken eingestuft. Verbesserte Authentisierungsverfahren, die auch in den sehr zeitkritischen Notsituationen zuverlässig funktionieren, werden also dringend benötigt.

Verzögerungen werden auch durch Firewalls, die Daten filtern, verursacht. Darüber hinaus müssten sie auch noch auf die oben genannten speziellen SCADA-Protokolle zugeschnitten werden und kontinuierlich, z.B. per Fernadministration, aktualisiert werden. Dies eröffnet wiederum Angriffsmöglichkeiten. SCADA-Systeme erfordern Echtzeitfähigkeit und verfügen in den beteiligten Sensoren häufig nur über sehr geringe Speicher- und Rechenressourcen sowie über geringe Datenraten bei der Übertragung, so dass auf eine Datenver- und Datenentschlüsselung in der Regel verzichtet wird. Es werden also keine gesicherten Kommunikationskanäle zwischen den Komponenten eines SCADA-Netzes etabliert, so dass keine Komponentenidentifizierung stattfindet und Daten abgehört, verändert oder auch neue Daten eingeschleust werden können. Darüber hinaus fehlen auch Lösungen für ein effizientes, automatisiert durchführbares Schlüsselmanagement. Die Sensorik eines SCADA-Systems wird häufig in Umgebungen eingesetzt, in denen ein potentieller Angreifer physischen Zugriff auf die Komponenten erhält. Somit ergeben sich hier analoge Anforderungen an die Sicherheit derartiger Sensoren, wie wir sie im Speziellen für die digitalen Zähler bereits ausgeführt haben. Eine ausführliche Taxonomie möglicher Angriffe auf SCADA-Netze findet sich u.a. in [Igu2006].

4.3 IKT-gestützte Energiemanagementsysteme

Im Gegensatz zur Kommunikationsinfrastruktur existieren Energiemanagementsysteme, wie sie in einem Smart Grid notwendig sind, bislang nicht. Erste systemische Lösungen werden derzeit im Rahmen des BMWi E-Energy-Programms erstellt. Ein solches Management findet auf verschiedenen Ebenen statt. Bereits in den einzelnen Privathaushalten sind lokale Managementsysteme erforderlich (vgl. Abbildung 5), um die Energie-Ströme im Haushalt zu steuern und ressourcensparend einzusetzen.

Die Privathaushalte werden in lokalen Management-Zentren zusammengeführt und koordiniert. Diese regionalen Zentren müssen untereinander sowie mit überregionalen Zentren koordiniert zusammen arbeiten. Noch schwieriger und komplexer wird das Szenario, wenn das Energiemanagement über Landesgrenzen hinweg funktionieren muss. Auf europäischer Ebene muss dafür die bereits bestehende Vielzahl verschiedener Arten der Energieerzeugung geeignet eingebunden werden. So verwendet Norwegen vorwiegend Wasserkraft, Deutschland setzt einen hohen Anteil erneuerbarer Energien ein[10], Frankreich besitzt einen hohen Anteil an Atomenergie, während Polen ausschließliche fossile Brennstoffe nutzt. Die komplexen Systemstrukturen, aber auch die unterschiedlichen Anforderungen an die Erfassung, Auswertung sowie Speicherung von Daten, der Umfang der Datenflüsse und ihre Echtzeitanforderungen sowie die erforderlichen Regelkreise erfordern ein überaus umfangreiches

[10] Vgl. http://www.erneuerbare-energien.de/files/pdfs/allgemein/application/pdf/ee_in_deutschland_update_bf.pdf

verteiltes System. An dieses Managementsystem werden höchste Anforderungen gestellt, die nicht nur technischer Natur sind. Zu dessen Entwicklung werden detaillierte Kenntnisse der Informatik, Informationsverarbeitung, Steuerungs- und Regelungstechnik sowie der Hardware- und Software-Systemtechnik erforderlich sein.

Ebenfalls spielen juristische und ökonomische Fragestellungen eine große Rolle, so dass Juristen und Wirtschaftsinformatiker bzw. Betriebswirte frühzeitig in den Prozess der Entwicklung der Managementsysteme des Smart Grid einzubinden sind. Obwohl es in verwandten Anwendungsgebieten ähnliche Systeme bereits gibt, wie z.B. integrierte Produktionssteuersysteme, Verkehrsmanagementsysteme (Luftfahrt, Bahnsysteme, Flottenmanagement) oder Logistiksysteme (Supply Chain Management, Event Management), stellt das Smart Grid sehr viel komplexere und weitreichendere Anforderungen, so dass die bekannten Systeme nicht direkt nutzbar sein werden.

Insbesondere im Bereich der Sicherheit und des Datenschutzes ergeben sich höhere Anforderun-

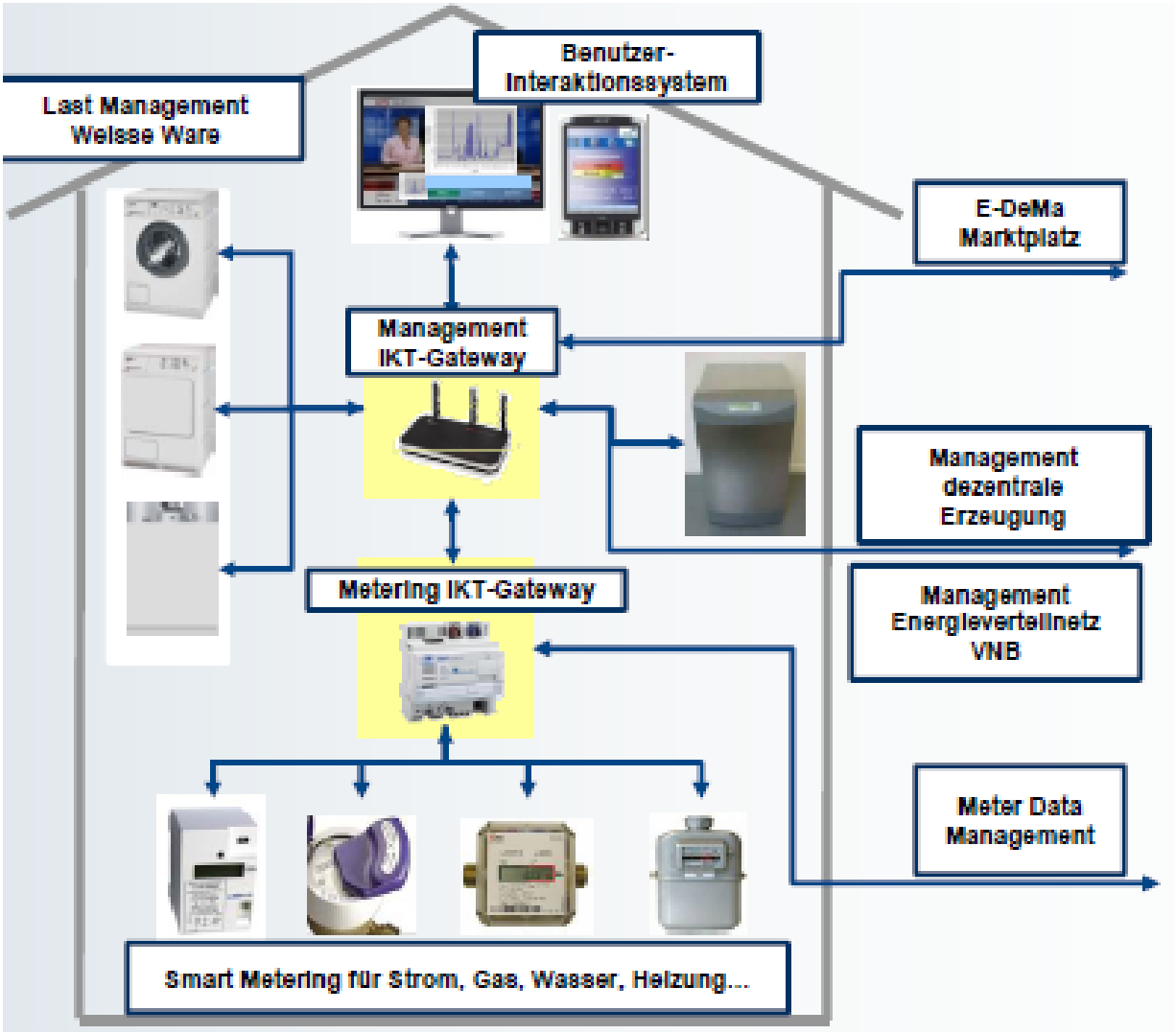


Abbildung 5: Energiemanagementsysteme in Privathaushalten (Quelle: Siemens AG)

gen als in den oben genannten verwandten Szenarien. Grund sind die Charakteristika des Smart Grid wie Heterogenität und Vielzahl der beteiligten Parteien, die Dezentralität der Verwaltung, die Sensibilität der erfassten Daten etc.. Gleichzeitig müssen Sicherheit und Datenschutz die besonderen betrieblichen Anforderungen von traditionell autark betriebenen Anlagenteilen berücksichtigen.

Bestandteil der Energiemanagementsysteme sind die Energiemarktplätze, über die im zukünftigem Smart Grid Mehrwertdienste angeboten werden. Mehrwertdienste werden in Zukunft nicht nur flexible Tarifmodelle umfassen, sondern sehr viel weiter reichende Dienste bzw. ganze Dienstleistungsbündel (Packages) abdecken. Über die Multi-Utility Gateways kann die gesamte Heimautomatisierung in die Entwicklung neuer Geschäftsmodelle u. a. für Telekommunikationsanbieter einbezogen werden, so dass beispielsweise eine Fernsteuerung der heimischen Geräte über Mobiltelefone ermöglicht wird.

Ein sehr großes Potential wird im Bereich der Gesundheitsversorgung und der IKT-gestützten Pflege bei der Unterstützung von älteren und mobilitätseingeschränkten Personen im Sinne des Ambient Assisted Living gesehen. Zum Hintergrund: In Deutschland ereignen sich mehr als 70% aller medizinischen Zwischenfälle und Unfälle im eigenen Haushalt. In der Gruppe der Betroffenen sind mehr als die Hälfte über 65 Jahre alt, die in privaten Haushalten häufig alleine leben. Das Smart Grid zusammen mit seinen Marktplätzen wird eine umfassende und flächendeckende IKT-Infrastruktur zur Verfügung stellen, die in einem weiteren Schritt auch für medizinische Unterstützungsdienstleistungen genutzt werden könnte. In solchen Szenarien werden eine Vielzahl hochsensibler Daten ausgetauscht. Über z.B. Fernzugriffe durch medizinisches Personal, wie Notfallpraxen, könnten darüber hinaus auch direkte Eingriffe in die Abläufe in einem Privathaushalt vorgenommen werden, indem spezielle Sensoren an- und abgeschaltet werden etc..

Die IKT-Infrastruktur und die Managementsysteme des Smart Grid müssen deshalb frühzeitig auch auf solche Anwendungsszenarien vorbereitet werden und Maßnahmen vorsehen, um äußerst sicherheitskritische und datenschutzrelevante Mehrwertdienste in Zukunft unterstützen zu können. Neben der klaren Trennung von Daten, die für unterschiedliche Dienstleistungen erhoben, übermittelt und verarbeitet werden (Zweckbindungs- und Datensparsamkeitsprinzipien des Datenschutzes), dem Einsatz starker Ende-zu-Ende-Verschlüsselungskonzepte für die vertrauliche Übermittlung der Daten, werden insbesondere auch starke Verfahren zur wechselseitigen Identifizierung der Akteure und nichtumgehbare, auditierbare, rollenbasierte Zugriffskontrollen erforderlich sein. Die Identifizierung und Authentisierung der Akteure bezieht sich dabei sowohl auf die so genannte Maschine-zu-Maschine-Kommunikation (M2M), bei der sich Geräte, Dienste, Plattformen identifizieren und als korrekt ausweisen müssen, als auch auf die Identifizierung der agierenden natürlichen Personen bzw. der Rollen, in denen sie aktiv sind. Digitale Ausweisdokumente mit integrierten Identifizierungsfunktionen wie der neue Personalausweis (nPA) oder die elektronische Gesundheitskarte (eGK) und der Heilberuflerausweis (HBA) (vgl. [Eck2009]), wie sie in Deutschland entwickelt und zum Teil bereits ausgerollt werden, könnten hierfür eine Vorreiterrolle einnehmen und die europäische Standardisierung prägen. Konkrete Schritte in dieser Richtung sind den Autoren des Papiers jedoch bislang nicht bekannt.

4.4 Normungsaktivitäten

Das NIST-Papier [EPR2009] hat unter anderem 14 zentrale Themenbereiche identifiziert, in denen neue oder überarbeitete Standards benötigt werden. Der Bereich IT-Sicherheit wird hierbei besonders hervorgehoben. Dies greift das DKE-Papier [DKE2010] auf und entwickelt Empfehlungen für eine Normungsroadmap für die Themen

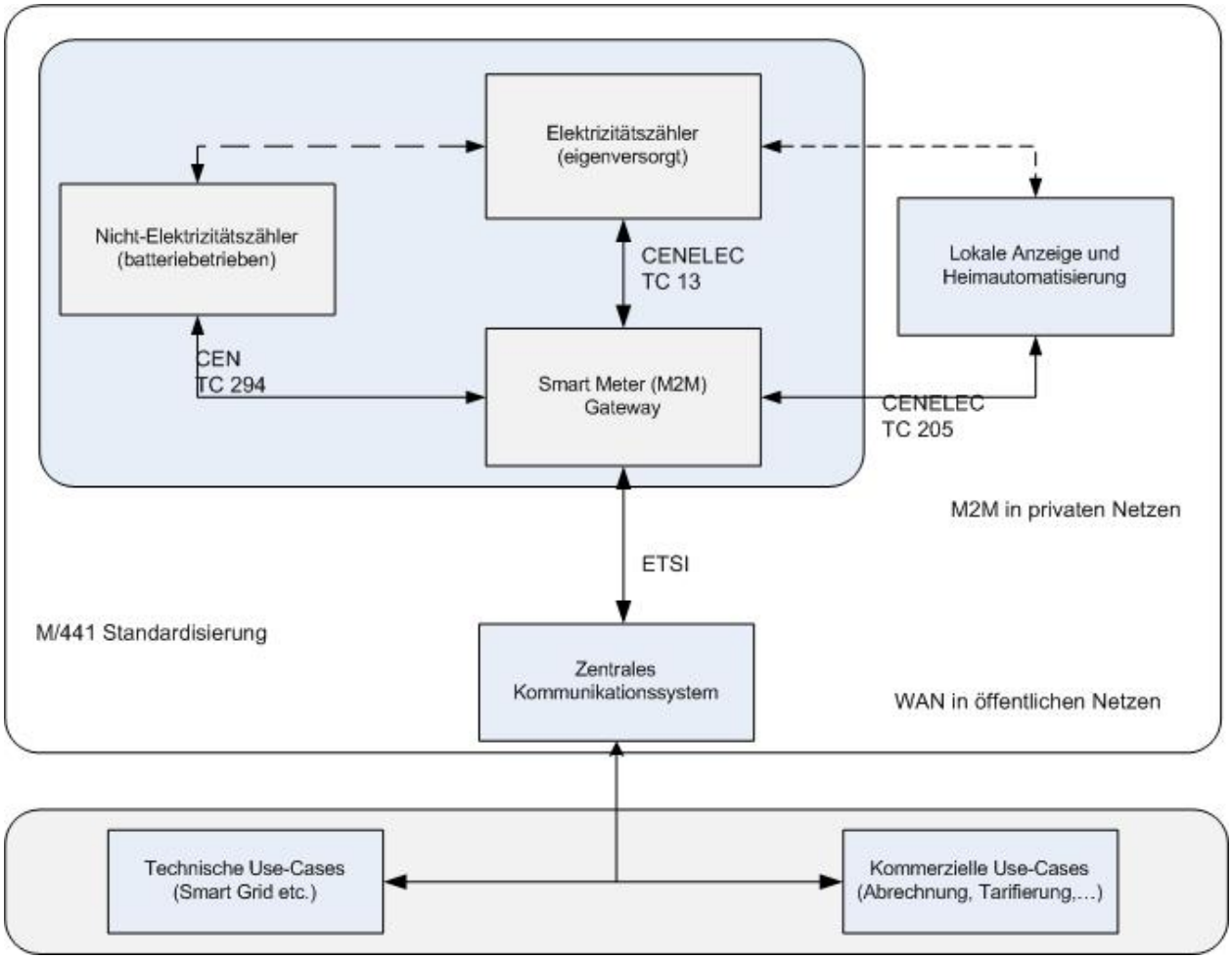


Abbildung 6: Referenzarchitektur der Smart Meters Coordination Group (Quelle [DKE2010])

IT-Sicherheit und Datenschutz. Hierbei wird ebenfalls auf die entstehenden Zielkonflikte zwischen dem Datenschutz mit dem Ziel der Datensparsamkeit einerseits und den Stakeholdern andererseits, die möglichst viele Informationen zur Bereitstellung von Mehrwertdiensten benötigen, hingewiesen. Weiterhin wird gefordert, dass IT-Sicherheit als Kernthema bei der Architekturentwicklung betrachtet werden muss.

Wesentliche Themen, die identifiziert werden, betreffen rollenbasierte Zugriffskontrolle, Identitätsmanagementfragen sowie die sichere Kommunikation. Zudem wird ein Bewertungssystem gefordert, so dass die Vergleichbarkeit und Anwendbarkeit von Sicherheitslösungen möglich ist. Mit den Common Criteria steht ein solcher international anerkannter Bewertungskatalog bereits zur Verfügung.

Weltweit wird bereits jetzt mit hohem Druck an der Entwicklung von Roadmaps und Frameworks für Smart Grid-Systeme und -Infrastrukturen gearbeitet. Der Fokus der bislang vorangetriebenen Aktivitäten lag auf der Entwicklung funktionaler IKT-Infrastrukturen und Komponenten [Jav2010]. Die Frage der Sicherheit, Robustheit und Verlässlichkeit einer solchen Infrastruktur spielte bislang, auch international, nur eine untergeordnete Rolle. Angesichts der immer stärker zu Tage tretenden Risiken durch Angriffe auf solch ein Energieinformationsnetz werden aber u.a. in den USA

bereits massive Anstrengungen unternommen, um die Sicherheit der Energienetze zu gewährleisten. So befassen sich verschiedene Standardisierungsgremien (wie das US National Institute of Standards and Technology NIST) derzeit hauptsächlich mit der Erarbeitung von Anforderungsspezifikationen [Lee2009], [NIST2010], [Mc2009], [Khu2010].

Europäische Standardisierung

Um einen Europaweit einheitlichen Standard für Smart Metering-Infrastrukturen zu erhalten, hat die Europäische Union den Organisationen ETSI, CEN und CENELEC ein Mandat zur Ausarbeitung von Standards erteilt[11]. Die diesen Standardisierungsbemühungen zugrunde liegende Referenzarchitektur ist in Abbildung 6 dargestellt (vgl. [DKE2010]). Das Ziel der Standardisierung ist es, Normen festzulegen, um eine Interoperabilität zu gewährleisten. Die Normungsarbeiten werden sich auf sechs Bereiche beziehen:

(1) Das Auslesen von Messwerten,

(2) die bidirektionale Kommunikation zwischen Zähler und Marktteilnehmer,

(3) die Unterstützung unterschiedlicher Tarifmodelle und Zahlungssysteme,

(4) die Zählerfernabschaltung und der Versorgungsstart und das -ende,

(5) die Kommunikation mit Geräten der Heimautomatisierung und

(6)das Display zum Anzeigen der Zählerstände in Echtzeit.

Diese Normierungsaktivitäten stecken noch in den Anfängen. Mit zeitnahen Entwicklungen von deutschen Referenzaktivitäten, wie dem Protection Profile für Smart Meter, könnte Deutschland in dieser Phase starken Einfluss auf die europäischen Normierung nehmen. Hier werden sehr gute Chancen für die deutsche Wirtschaft gesehen, die kommenden Standards mit zu prägen.

Der skizzierte Stand der Technik hat gezeigt, dass im Bereich der Sicherheit und des Datenschutzes noch ein erheblicher Nachholbedarf besteht. Bei der Konzipierung und Umsetzung eines Smart Grid müssen Sicherheits- und Datenschutzfragestellungen von Anfang an einbezogen werden, da eine Nachbesserung nur Stückwerk erzeugt, mit hohen Kosten verbunden ist und lückenhaft bleiben wird.

5 Ausgewählte Angriffsszenarien

Das Smart Grid der Zukunft wird vielfältigen Bedrohungen und Angriffen ausgesetzt sein (vgl. u.a. auch [Mc2009, Khu2010, Bee2010]). Eine US-amerikanische Studie aus dem Jahr 2008 kommt zu dem Ergebnis „the energy sector is most vulnerable to cyberattack". Nachfolgend werden einige allgemeine Angreiferklassen skizziert. Die offenen, dezentralen Architekturen der zukünftigen Smart Grids vergrößern die potentiellen IT-Angriffsflächen und eröffnen Angreifern neue und „attraktivere" Möglichkeiten des direkten Manipulierens und Eingreifens.

Angriffspunkte und Schwachstellen ergeben sich unter anderem durch eine Vielzahl von ungenügend abgesicherten Smart Metern [Hei2009, Law2010], die als Massenprodukte in Haushalten, Gebäuden, Anlagen ausgerollt werden. Das dritte Energiepaket, das das Europäische Parlament im April 2009 verabschiedet hat, empfiehlt, dass 80% aller Energiekunden bis 2020 Smart Meter haben sollen. Durch die Vernetzung, mit der Möglichkeit der Fernzugriffe auf Komponenten und Systeme (die z.B. zur kostengünstigen und effizienten Fernwartung sehr erwünscht sind), ergibt sich eine Vielzahl mangelhaft abgesicherter offener Zugangspunkte, wodurch sicherheitskritische Zugriffe auf die Netze/Komponenten des Smart Grid möglich werden. Drittanbieter können ihre Mehrwertdienste in die Energie-

[11] EU Mandat M/441

marktplätze einbringen, jedoch fehlen derzeit Sicherheits-APIs, einfache Test-Suiten etc., mit denen die Qualität der Dienste, insbesondere deren Vertrauenswürdigkeit, technisch geprüft werden kann. Die Bereitstellung unsicherer Mehrwertdienste, bei deren Nutzung sensitive Kundendaten verarbeitet werden, birgt die Gefahr des Datenmissbrauchs und der unberechtigten Weitergabe von Daten (Data Leakage), so dass sich Gefährdungen der Vertraulichkeit und der Privatheit sowie Compliance und Haftungsprobleme ergeben können.

Es ist aus Kostengründen naheliegend, dass man für die Kommunikationsinfrastruktur zumindest in Teilen auf das bestehende Internet zurückgreifen wird und dass man zur durchgängigen und effektiven Verarbeitung von Energiedaten in dem komplex vernetzten System versuchen wird, die Internet-Protokoll Familie IP als gemeinsame Protokollschicht zu etablieren. Den Vorteilen einer einheitlichen Vorgehensweise stehen zum einen die bekannten Sicherheitsschwächen der Internet Protokolle (IP Protokolle) gegenüber. Hierfür gibt es aber einige Lösungsansätze, die auch im Smart Grid verwendbar sind. Besondere Bedrohungen ergeben sich zum anderen aus der IP-basierten „Monokultur“, die eine schnelle, ungehinderte Ausbreitung von Schadenssoftware (Malware) wie Würmer und Viren begünstigt, so dass die Verfügbarkeit von Diensten und Komponenten beeinträchtigt, gefälschte Daten in Umlauf oder aber auch gezielte Sabotage-Aktionen durchgeführt werden können.

Das Smart Grid wird IKT-basierte Systeme mit physikalischen Komponenten zu den so genannten Cyber-Physical Systems verbinden. An der Schnittstelle zwischen physischen und IKT-gestützten Systemen werden neue Schwachstellen und Verwundbarkeiten auftreten, die für gezielte Angriffe, wie Denial-of-Service, terroristische Attacken etc. ausgenutzt werden können. Mit dem Smart Grid werden Energieversorgungsnetze und Netze, die vordringlich zur Abwicklung von Business-IT verwendet werden (Abrechnung, Mehrwertdienste etc.) gekoppelt. Es besteht die Gefahr, dass die bekannt anfälligen Business-IT-Systeme durch mangelhafte Überwachungen und Isolierungen den gesicherten Betrieb von Versorgungsnetzen und Energiemanagementsystemen bedrohen.

Schwachstellen und Bedrohungen werden durch Angreifer ausgenutzt, die versuchen, ihre jeweiligen Ziele zu erreichen. Ein Smart Grid stellt ein attraktives Angriffsziel dar, so dass zu erwarten ist, dass insbesondere terroristische und kriminell motivierte Angriffe zunehmen werden. Nachfolgend sind einige mögliche Angreifer-Klassen aufgelistet.

(1) Cyber-Terrorist

Die Palette der möglichen Angriffe ist vielfältig. Das nachfolgende Zitat verdeutlicht das Potential, auch wenn die skizzierten Szenarien so in Deutschland derzeit nicht auftreten: "Plant control networks (and their programmable logic controllers) should be disconnected from the Internet," said Peter Zatko, technical director of the national intelligence research unit at BBN Technologies. "These are the things lifting and lowering the plutonium rods into the water to make steam...It's on the Internet. This is terrifying."

Die möglichen Angriffspunkte für terroristische Angreifer sind bereits Gegenstand internationaler Fachkonferenzen, wie der erste Cyber-Security Gipfel in 2010 verdeutlicht. Auf dem Gipfel haben Experten realistische Angriffe diskutiert, bei denen Angreifer versuchen, gezielt gefälschte Daten einzuschleusen, um z.B. die Energieversorgung bei sicherheitskritischen Anlagen zu stören. Überwachungsnetze (z.B. SCADA [Igu2006]) können manipuliert werden, um die Weitergabe von Daten zu verzögern, oder durch falsche Daten Notfallszenarien wie das Abschalten oder Herunterfahren von Anlagen auszulösen. Die Verfügbarkeit von Diensten kann gezielt gestört werden durch so genannte Denial of Service-Angriffe, z.B. durch das Etablieren von Bot-

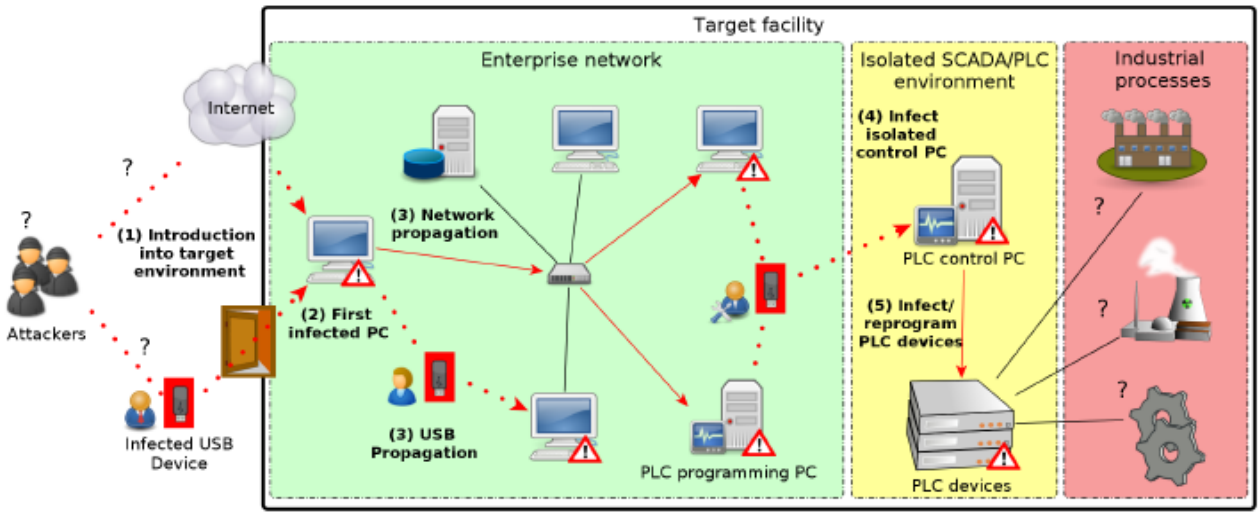


Abbildung 7 Angriffspfad des Stuxnet-Virus

Netzen [Sto2009], um gezielte Stromausfälle mit hohen volkswirtschaftlichen Schäden herbei zu führen. Bereits 2009 hatte der Sicherheitsspezialist Mike Davis auf der Black Hat Konferenz mit einer Simulation demonstriert, dass innerhalb von 24 Stunden 15 000 Smart Meter von einem Wurmprogramm infiziert werden und damit auch von dem Angreifer kontrolliert werden können. Ferngesteuerte Smart Meter, die in einer Größenordnung von tausenden Geräten durch einen solchen Angriff zu einem Zeitpunkt an- oder abgeschaltet werden, können die Stabilität eines großen Bereichs des Versorgungsnetzes massiv beeinträchtigen und damit die Versorgungssicherheit ganzer Regionen gefährden.

Die IT-Systeme können somit ihrerseits als „Tatwaffen" genutzt werden, um Sabotage-Angriffe durchzuführen, die zum Beispiel die physikalische Zerstörung von Komponenten durch Steuerungs-Komponenten (z.B. Überhitzen, Fluten etc.) zum Ziel haben können. Der Stuxnet-Wurm (vgl. Abbildung 7), der im Sommer 2010 iranische Atomkraftwerke bedroht hat, war ein markantes Signal dafür, dass sicherheitskritische Infrastrukturen wie industrielle Kontrollsysteme, PCSs (Process Control Systems) oder auch SCADA-Systeme zunehmend gefährdet sind. Der Stuxnet-Angriff verlief in mehreren Stufen, wobei in der ersten Stufe unter Ausnutzung klassischer Angriffsmethoden Schwachstellen in Windows-PCs ausgenutzt und diese PCs mit dem Virus infiziert wurden. Auf diesem Weg wurden dann auch PCs infiziert, die zur Programmierung von PLCs (Process Control Systems) verwendet werden. Da mit derartigen PCs Kontrollprogramme für Steuergeräte (PCLs) erstellt werden, deren Programmcode dann auf die eigentlichen Steuergeräte geladen und ausgeführt wird, ist hier der kritische Schritt erfolgt. Beim Stuxnet-Angriff wurden die Steuergeräte, wie eine SIMATIC, also nicht selbst infiziert, sondern es wurde ein Programmcode auf die Rechner geladen, der Steuerbefehle enthielt, die die Betriebssicherheit der durch die PCs gesteuerten Anlagen gefährdet haben. Eine detaillierte Darstellung des Angriffs und seiner Konsequenzen für Energieversorgungsnetze und ähnlicher Netze ist in dem technischen Bericht [Br10] zu finden.

(2) Endkunde/Bürger als Täter

Digitale Zähler und andere Komponenten des Smart Grid werden direkten physischen Angriffen ausgesetzt sein, da sie leicht zugänglich sind. Zählerkomponenten und Vernetzungsinfrastrukturen können zum einen Ziel von Manipulationsangriffen durch die Kunden des Smart Grid sein. Zum anderen können sie von den Endkunden gezielt dazu missbraucht werden, um andere Beteiligte zu schädigen. So können digitale Zähler, die in Privathaushalten direkt physisch zugreifbar sind, von deren Besitzern gezielt manipuliert werde, um die eigenen Verbrauchsdaten zu verändern. Die Energieinformations-Infrastrukturen, können zudem gezielt genutzt werden, um Energiedaten und Nutzungsprofile Dritter (Mieter, Nachbarn etc.) auszuspähen. Angreifer können aber auch versuchen, sich geldwerte Vorteile (Betrug) zu verschaffen, indem sie beispielsweise manipulierte Daten, die eine Energieeinspeisung vorgeben, in das Netz einbringen. Denkbar sind auch Angriffe, wie das „Umleiten" von Verbrauchsdaten auf andere Nutzer, so dass deren Konto belastet wird. Das sind Ausprägungen von Angriffen, die auf einen Identitätsdiebstahl hinaus laufen. Da die Kommunikationsverbindung zwischen den Zählern und den Managementsystemen bidirektional ist, kann man auch versuchen, von außen die Zähler fremder Personen zu manipulieren, z.B. durch eine gezielte Sabotage durch Missbrauch der Infrastruktur, um beispielsweise unautorisiert eine Stromabschaltung bei Dritten herbei zu führen.

(3) Organisierte Kriminalität

Da ein Smart Grid eine Vielzahl von geldwerten Objekten und Informationen verwaltet, wird es ein lukratives Angriffsziel für die organisierte Kriminalität werden. Beispiele für Angriffe, mit denen sich Geld verdienen lässt, umfassen den Diebstahl von Leistungen wie zum Beispiel die kostenlose Energienutzung, die preiswerte Einrichtung von Bot-Netzen, um das Smart Grid zu kontrollieren und um auf dieser Basis erpresserische Geldforderungen zu stellen. Weitere Beispiele kriminell motivierter Angriffe sind das widerrechtliche Akquirieren von sensitiven Verbraucherinformationen und deren Verkauf.

Neben diesen direkten Angriffen auf die ITK-Infrastruktur mit den unmittelbaren Problemen für die Versorgungssicherheit etc. können kriminelle Angriffe, die nicht direkt gegen die Infrastruktur gerichtete sind, negative Auswirkungen auf das globale Energieversorgungssystem haben. So haben die im Januar 2011 publik gewordenen Angriffe, bei denen Kriminelle durch einfache Phishing-artige Angriffe bis zu zwei Millionen Emissionsberechtigungen im Wert von 28 Millionen Euro gestohlen haben sollen, dazu geführt, dass der Handel mit diesen Rechten vorübergehend ausgesetzt wurde. Dies hatte erhebliche finanzielle Schäden zur Folge. Mangelnde Identitätsüberprüfungen und andere mangelhafte Sicherheitsvorkehrungen sowie fehlendes Sicherheitsbewusstsein bei den verantwortlichen Stellen (aufgrund einer manipulierten E-Mail haben sie sich beispielsweise massenhaft bei einem gefälschten Server mit ihren jeweiligen Zugangsdaten neu registriert) waren die Ursache dieser massiven Diebstähle.

(4) Mitarbeiter/Dienstleister

Mitarbeiter von Infrastrukturbetreibern oder deren Dienstleister könnten beispielsweise klassischen Social Engineering-Angriffen ausgesetzt werden. Über USB-Sticks, E-Mail-Attachements oder manipulierte Web-Seiten könnte versucht werden, Schadsoftware auf PCs/Notebooks und anderen Endgeräten von Service-Mitarbeitern einzuschleusen. So hat ein Experte auf der RSA Conference 2009 einen Einbruch in ein Kraftwerk demonstriert, indem ein Kernkraftwerks-Mitarbeiter durch Social Engineering dazu gebracht wurde, einen Link in einer E-Mail anzuklicken, so dass Schadsoftware auf den PC des Mitarbeiters geladen wurde. Durch diese Manipulation erlang-

te der Angreifer Zugriffsrechte an Kernkraftwerks-internen Wartungsdiensten, die dem Mitarbeiter zugänglich waren.

Durch Phishing-Angriffe könnten Angreifer versuchen, sich Zugangsdaten von Mitarbeitern anzueignen und sich unter der gefälschten Identität des Mitarbeiters einen nicht-autorisierter Zugang zu beschaffen. Der oben bereits angesprochene Diebstahl von Passwörtern für Emissionskonten deutscher Unternehmen[12] ist ein weiteres Beispiel von Social Engineering-Angriffen. Unsicher konfigurierte Remote-Zugänge für die Fernwartung von Netzen eröffnen für Angreifer die Möglichkeit, unter der Identität des berechtigten Mitarbeiters den Fernzugriff z.B. auf Privathaushalte oder aber auch auf Service-Einrichtungen durchzuführen und beispielsweise Daten zu manipulieren.

Die skizzierten Angriffe stellen lediglich einen Ausschnitt der möglichen Bedrohungen dar. Diese sind in systematischer Weise zu erfassen und zu bewerten. Dazu ist es erforderlich, charakteristische Einsatzszenarien und Systemarchitekturen zu identifizieren und anhand derer eine Bedrohungs- und Risikoanalyse durchzuführen. Weiterführende, vertiefende Arbeiten sind erforderlich, um anhand charakteristischer Szenarien derartige Analysen durchzuführen, Sicherheitskonzepte zur Absicherung der Architekturen zu entwerfen und Handlungsempfehlungen für deren Umsetzung in realen Einsatzszenarien zu geben. Für derartige Szenarien sind die unterschiedlichen Interessen der beteiligten Parteien zu erfassen, und es sind Architekturausprägungen zu entwerfen, die den zum Teil widersprüchlichen Anforderungen der Marktteilnehmern Rechnung tragen. So ist beispielsweise eine dezentrale Lösung, bei der die Verarbeitung der personenbeziehbaren Verbrauchsdaten vollständig in der Hand des Kunden, also in einem Endgerät beim Kunden verbleibt, aus datenschutzrechtlichen Gründen ideal, widerspricht aber dem Bedarf von Betreibern an möglichst vielen Informationen über Verbrauchs- bzw. Nutzungsprofilen, um diese in Mehrwertdienstleistungen zu vermarkten.

[12] http://www.zeit.de/wirtschaft/2010-02/hacker-emissionshandel-datendiebstahl

6 Forschungsbedarf

Wie dargestellt, umfasst ein Smart Grid eine Vielzahl von Sensoren wie Smart Metern zur Datenerfassung und zur Überwachung, die in nicht-vertrauenswürdigen Umgebungen sowohl in Privathaushalten als auch in gewerblich betriebenen Gebäuden und Liegenschaften als Massenprodukt zum Einsatz kommen werden. Die Geräte sind in der Regel unbeschränkt zugänglich, so dass erhebliche Probleme durch diesen direkten physischen Zugriff auftreten. Durch die starke Dezentralisierung durch die Anbindung von Mikro BHKWs, Elektro- und Hybridfahrzeugen, erneuerbaren Energiequellen etc. kommt es zu Kontrollverlusten der Netzbetreiber. Die Energiemanagementplattformen sind offene Marktplätze, in die Mehrwertdienste durch Dritte dynamisch eingebunden werden und über Cloud-Dienste IT-Dienstleistungen durch Dritte erbracht werden.

Die Problembereiche im Smart Grid sind sehr vielschichtig. Es müssen unterschiedliche, skalierende und auf die jeweiligen Anforderungen zugeschnittenen Lösungskonzepte entwickelt, in ihrem Zusammenspiel analysiert und in eine Gesamtsystem-Lösung sicher integriert werden. Es gibt zwar bereits eine Vielzahl von Einzellösungen und Schutzmechanismen, die jedoch noch nicht so nahtlos in die Systeme des Smart Grid integrierbar sind, dass das gewünschte, durchgehend hohe Sicherheitsniveau nachhaltig gewährleistet werden kann. Hier sind noch weitere Forschungs- und Entwicklungsarbeiten notwendig.

Nachfolgend werden für die in diesem Papier angesprochenen Themenbereiche Smart Meter, Kommunikationsinfrastruktur und Energiemana-

gementsysteme einige offenen Forschungsfragen skizziert. Diese müssten in einem nächsten Schritt systematisch erarbeitet und in einer Forschungsagenda zur Sicherheit im Smart Grid ihren Niederschlag finden.

6.1 Smart Meters, Gateways, Sensorik

Derzeit fehlt es noch an geeigneten Maßnahmen für den Manipulationsschutz von Smart Metern und Gateways. Das angesprochene Protection Profile des BSI sieht den Einsatz von Hardware-Sicherheitsmodulen im Gateway vor. Noch ist offen, in welcher Weise derartige Sicherheitsmodule in das Gateway eingebunden sein werden (z.B. als Chipkarte, die einfach ersetzt werden kann, wenn sich die Rahmenbedingungen ändern, oder als fest integrierter Chip). Die Gewährleistung einer sehr langen operativen Laufzeit derartiger Gateways, die Fernwartung, sichere System-Updates und sicheres Nachrüsten von zusätzlichen Sicherheitsfunktionen umfassen muss, sind noch zu klärende Fragen.

Heutige Gerätetechnologie muss somit konsequent weiterentwickelt werden. Erforderlich sind zum einen zugeschnittene Sicherheitsmechanismen wie Verschlüsselungsfunktionen, Schlüsselmanagementdienste, Zugriffskontrollmechanismen, Datenfilterungskonzepte, die zur Härtung bestehender Komponenten eingesetzt werden können. Zum anderen sind innovative Produkte und Sicherheitstechnologien zu entwickeln, die als vertrauenswürdige Kommunikationsendpunkte im Energieinformationsnetz eingesetzt werden können. Es werden Sicherheitslösungen benötigt, die unterschiedliche Grade an Sicherheit unterstützen, jeweils zugeschnitten auf die Einsatzszenarien. Erforderlich sind somit Technologien zusammen mit integrierten Kontroll- und Überwachungsdiensten, so dass die eingesetzten Systemkomponenten besser gegen Manipulationsversuche geschützt und gehärtet werden (Manipulationsresistenz). Die Komponenten müssen mit zusätzlichen Fähigkeiten wie beispielsweise leichtgewichtige Hardware-Sicherheitsmodule für sichere Schlüsselspeicher versehen werden. Sie müssen in der Lage sein, Nachweise über die Integrität ihrer Soft- und Hard-ware so zu erstellen, dass diese Nachweise von dritter Seite überprüft werden können (z.B. leichtgewichtige Attestierung von Sensoren und Aktoren).

Die beteiligten Komponenten müssen sich zudem effizient wechselseitig identifizieren und authentisieren können. Dementsprechend sind skalierende Identifikations- und Authentisierungsschemata für Komponenten zu entwickeln, wie beispielsweise leichtgewichtige PKI[13]-Lösungen für ressourcenschwache Sensoren und Geräte und deren Schlüsselmanagement, oder neuartige Lösungen, die eine Identifikation auf der Basis der eindeutigen physischen Objekteigenschaften ermöglichen.

Test-Methoden und -Werkzeuge

Die in sicherheitskritischen Domänen eingesetzten Geräte müssen Sicherheitstests durchlaufen. Hierfür wird derzeit vom BSI das Protection Profile für Smart Meters festgelegt. Technische Richtlinien zur Entwicklung und Validierung von intelligenten Zählern werden im nächsten Schritt sicherlich folgen. Weitere Testszenarien fehlen jedoch noch. So sollten nach den jetzigen Stand der Technik die eingesetzten Komponenten resistent gegenüber Seitenkanal-Angriffen sein, die es ermöglichen, sensitives Schlüsselmaterial aus eingebetteten Komponenten, wie Chips, zu extrahieren. Entsprechende Untersuchungen und Testmethoden werden unter anderem vom Fraunhofer-Institut SIT in München angeboten (vgl. Abbildung 8) und in Projekten, wie dem BMBF-Konsortialprojekte RESIST mit Firmen wie Infineon, Giesecke&Devrient oder aber auch Rhode und Schwarz (vgl. http://www.resist-projekt.de) weiter entwickelt. Im SIT-Testlabor

[13] Public-Key Infrastruktur

werden derzeit auch Smart Meter Komponenten in Bezug auf ihre Sicherheit getestet. Neben den reinen Sicherheitstests werden Interoperabilitätstests notwendig; hierfür sind ebenfalls Testrahmen zu erstellen und Testumgebungen aufzusetzen.

6.2 Kommunikationsinfrastruktur

Das Energieinformationsnetz der Zukunft umfasst eine Vielzahl von Messwertgebern, Feldsensoren und (drahtlosen) Netzen, um bestehende Systeme und Prozesse der Energieversorger aus Leitwarten heraus zu steuern und zu regeln (SCADA) oder mittels Fernwartung zu prüfen und ggf. sogar zu reparieren. Die entsprechenden Steuerungssysteme greifen in die Abläufe der Energieversorger ein. Dabei eröffnet die Fernwartung Zugänge zu sicherheitskritischen Komponenten und Diensten, so dass hier besondere Schutz- oder Isolationsmaßnahmen integriert werden müssen. In Zukunft werden diese Aufgaben aufgrund der zunehmend dezentralen Energieerzeugung komplexer. Gleichzeitig müssen diese Aufgaben durch die absehbare Deregulierung der Märkte im Kontext einer größeren organisatorischen Heterogenität bewältigt werden.

Die Frage, welche Sicherheitslösungen für die Kommunikation zwischen verteilten Anlagenteilen für die Übertragung von Informationen über drahtlose, mobile oder Festnetzverbindungen geeignet sind, ist noch nicht vollständig geklärt. Aus technischer Perspektive sind besonders die Nahtstellen zwischen unterschiedlichen Technologien problematisch. So ist durch geeignete Maßnahmen sicherzustellen, dass ein gewünschtes Maß an Sicherheit durchgängig und nahtlos über verschiedene Technologien und Betreiberdomänen hinweg garantiert wird. Die Vergangenheit hat gezeigt, dass es gerade an den Nahtstellen unterschiedlicher Technologien und an den Nahtstellen zwischen unterschiedlichen Betreibern zu erheblichen Sicherheitsproblemen kommt, wie z.B. bei der Kopplung von GSM/UMTS und WLAN-Netzen.

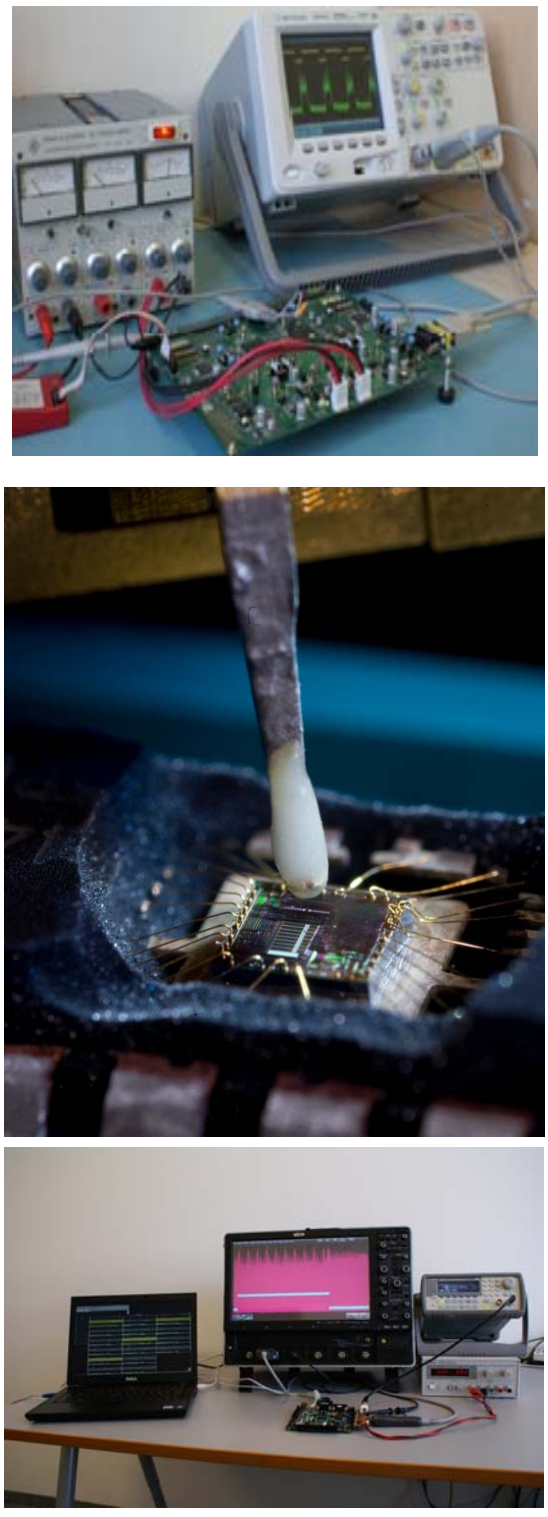


Abbildung 8: EM-Sonde zum Messen der elektromagnetischen Abstrahlung auf einem geöffneten Chip (Mitte), Messplatz zur Poweranalyse eines Mikrocontrollers und FPGA-Platine zu dessen Steuerung (oben und unten) im Testlabor des Fraunhofer SIT-München

Ferner müssen gemeinsam genutzte IKT-Infrastrukturdienste (z.B. DNS) besondere Sicherheits- sowie Zuverlässigkeitsanforderungen erfüllen und Migrationsmöglichkeiten zulassen.

Die Sicherheitsimplikationen, die sich aus der zunehmenden Vernetzung für SCADA-Netze ergeben, werden von den aktuellen SCADA-Lösungen noch nicht geeignet erfasst (vgl. u.a. [St2003, Igu2008]]. Die Einbettung echtzeitfähiger Sicherheitskonzepte in SCADA-Netze und Gateways, die Unterstützung einer effizienten und sicheren Maschine-zu-Maschine-Kommunikation (M2M) in derartigen Steuerungssystemen sowie die Einbettung effizienter Verschlüsselungs- und Entschlüsselungsmaßnahmen zusammen mit einem effizienten Schlüsselmanagement fehlt. Ansätze hierzu könnten Varianten von leichtgewichtigen PKI-Lösungen sein, die auf die Einsatzdomäne zuzuschneiden sind. Die Schlüssel müssen vertrauenswürdig in den ressourcenschwachen Geräten gespeichert werden, so dass sich hier wiederum der Bedarf an angriffsresistenten, vertrauenswürdigen leichtgewichtigen Hardware-basierten Sicherheitsanker ergibt. Hoch performante Überwachungs- und Filterungskomponenten, wie beispielsweise integrierte Micro-Firewalls in ressourcenbegrenzte SCADA-Netze werden ebenso benötigt wie effiziente, echtzeitfähige Überwachungsfunktionen, zur frühzeitigen Erkennung und Abwehr von Angriffsversuchen auf und in SCADA-Netzen. Für die sichere Einbindung von Bedienpersonal werden verbesserte Authentisierungsverfahren benötigt, die auch in zeitkritischen Notsituationen zuverlässig funktionieren.

Für das Smart Grid ist zudem die Entwicklung dedizierter, in nahe Echtzeit agierender Überwachungsprotokolle im Sinne kooperativer Frühwarnsysteme erforderlich, um aufkommende Probleme frühzeitig zu erkennen und rechtzeitig geeignete Abwehrmaßnahmen einzuleiten. Benötigt werden technische Lösungen (u. a. Schalenmodelle, Stufenmodelle) mit abgestuften Kontrollen (Identität, Zugriffskontrolle) zur gezielten Isolierung von Teilbereichen und für kontrollierte Bereichsübergänge. Notwendig werden ferner Betriebskonzepte zur Angriffs- und Ausfalltoleranz durch geeignete Isolierungs- und Redundanzmaßnahmen.

6.3 Energiemanagementsysteme

Das Smart Grid erfordert komplexe Managementsoftware, um die Fülle der erhobenen Daten auf dezentralen Serversystemen bei Stromunternehmen, aber auch bei Dienstleistern (z.B. über Cloud-Services) zu verarbeiten. Neue digitale Marktplätze entstehen mit neuen Dienstleistungen und Geschäftsmodellen, um Energie kostengünstig und sparsam zu produzieren und zu nutzen.

Für die zu entwickelnden Energiemarktplätze bzw. Energie-Clouds und die Mehrwertdienste, basierend auf der Smart Grid IKT-Infrastruktur, sollte soweit wie möglich und anwendbar auf bestehende Standards im Bereich der Web-Services, der Service-orientierten Architekturen etc. zurückgegriffen werden. Um mandantenfähige, vertrauenswürdige Services über eine gemeinsame Plattform anzubieten, sind die gleichen Sicherheitsfragestellungen zu lösen, wie sie derzeit auch in einem allgemeineren Kontext beim Cloud-Computing bearbeitet werden. Die Lösungen des Cloud-Computing sollten in die Energie-Domäne übertragen werden. Zentrale Sicherheitsherausforderungen betreffen die sichere und vertrauenswürdige Identifizierung und Authentisierung der Marktteilnehmer und die rollen- und aufgabenbasierte Zugriffs- bzw. Nutzungskontrollen. In Deutschland werden mit dem neuen Personalausweis (nPA) flächendeckend sichere Identifizierungstokens ausgerollt. Daneben gibt es eine Vielzahl anderer Authentisierungstechniken, so dass ein umfassender Dienst im Sinne von Identity-as-a-Service wünschenswert wäre, der ein einheitliches Identitätsmanagement z.B. in der Energy-Cloud ermöglicht.

Zur Umsetzung von rollenbasierten Zugriffs- und Nutzungskontrollen müssen die jeweiligen Zugriffsregeln (Policies) für die Marktplatzteilnehmer für die unterschiedlichen Dienstleistungen, die sie anbieten und wahrnehmen sollen, definiert werden. Hierzu kann auf Standards wie WS-Policy zur einheitlichen Beschreibung zurückgegriffen werden. Die wesentliche Aufgabe wird dann aber darin bestehen, vertrauenswürdige Plattformen zu realisieren, die Sicherheitsdienste bereitstellen, die die Einhaltung der Regeln nachvollziehbar, auditierbar garantieren. Hierzu sind u. a. bestehende Virtualisierungsansätze um Überwachungsfunktionen und Attestierungstechniken zu erweitern. Mit solchen Techniken ist es möglich, die Manipulationssicherheit der Plattform, also der Ausführungsumgebung der Services, nachzuweisen. Die Plattformen müssen „betreibersicher" sein. Das bedeutet, dass sensitive Daten nur verschlüsselt transferiert und gespeichert werden dürfen und bei deren Bearbeitung besondere Vorkehrungen auf der Plattform zu treffen sind, um eine unzulässige Informationsweitergabe zu verhindern (Data Leakage Prevention).

Die im Energiemanagementsystem erhobenen und verarbeiteten Daten besitzen unterschiedliche Einstufungen (u.a. Vertraulichkeitsgrad, Grad der Kritikalität für kritische Systemprozesse, Lebensdauer, Zeitkritikalität), so dass Verfahren zur (semi)-automatisierten Klassifikation von Daten und zur überwachten Weiterleitung (fortgeschrittenen Filterungstechniken) an und Verarbeitung durch dazu berechtigte Dienste zu entwickeln sind. Der verschlüsselte Datenaustausch zwischen den Marktteilnehmern erfordert ein skalierendes Schlüsselmanagement, beispielsweise basierend auf einer PKI für die Energiedomäne.

Existierende Methoden des Risikomanagements sind zu erweitern, so dass sie auch im laufenden Betrieb eines Smart Grid eingesetzt (z.B. Lagebild und Health-Monitoring) werden können. Benötigt wird ein Lebenszyklus-übergreifendes Risikomanagement, in dem organisatorische, betriebswirtschaftliche, technische und regulatorische Aspekte berücksichtigt werden. Zudem wird ein technisch unterstütztes Security Level Management benötigt, das die Planung, Umsetzung und Überwachung von Garantien für Sicherheitseigenschaften unterstützt. In Anlehnung an das Software-as-a-Service-Paradigma (SaaS) könnten allgemeine Sicherheitseigenschaften und –funktionen in der Energiedomäne als Dienste im Sinne von „Security as a Service" bereit gestellt werden. Ein Beispiel für einen solchen Basisdienst könnte der Dienst „Privacy as a Service" sein, der persönliche Daten benutzerzentriert kontrolliert. Bestandteile eines solchen Dienstes sind etwa Anonymisierungs- und Pseudonymisierungs-funktionen, die die Erhebung und Verarbeitung von Daten ohne die Bildung von Nutzerprofilen ermöglichen. Die Grundlage für eine bedarfsgerechte Bereitstellung von Sicherheit ist ein Dienstentwicklungs-Framework, welches die vertrauenswürdige und sichere Orchestrierung von kontextorientierten Sicherheitsdiensten übernimmt. Zudem können so komplexe und rechenintensive Dienste in einer Integrationsschicht abstrahiert werden. Gleichzeitig unterstützt dieser Ansatz die Standardisierung und Modularisierung von Sicherheitseigenschaften, was Grundlage für eine Zertifizierung der Sicherheit bzw. Verifizierung der Rechtskonformität ist.

7 Erstellen einer Roadmap „IT-Sicherheit im Smart Grid"

Auf dem Weg zum sicheren Smart Grid müssen, wie die vorherigen Kapitel aufgezeigt haben, etliche Maßnahmen ergriffen werden. Diese sollten aufeinander abgestimmt sein und ein angemessenes Sicherheitsniveau für die Akteure in den unterschiedlichen Domänen definieren. Den beteiligten Akteuren im Smart Grid fallen dabei unterschiedliche Aufgaben und Verantwortlichkeiten zu. Diese sind abhängig von der jeweiligen Domäne, in der sie aktiv sind, und abhängig von den Dienstleistungen, die sie anbieten oder in Anspruch nehmen.

Abbildung 9 visualisiert die Sicht der Forrester Group aus dem Jahr 2009 auf das Smart Grid und veranschaulicht ganz allgemein wichtige Akteure und deren Beteiligung am Smart Grid.

Die Abbildung verdeutlicht noch einmal die verschiedenen Domänen, die sowohl den klassischen Bereich der Energiewirtschaft mit den Aufgaben der Energieversorgung, dem Lastmanagement und der Abrechnung als auch die neuen Anwendungsdomänen der dezentralen Energieeinspeisung und mobilen Energieabnahme, beispielsweise durch Elektromobilität, abdecken. Das Smart Grid beeinflusst alle diese Bereiche; zusätzliche Investitionen und eine Neugestaltung der IKT-Infrastrukturen ist für weite Teile des Smart Grid erforderlich. Hierbei sollte von Anfang an die Sicherheit und der Datenschutz Beachtung finden. Auch die Frage der Sicherheit beeinflusst alle diese Bereiche. Die NIST-Roadmap [NIST2010] greift diese Problematik auf, jedoch enthält sie lediglich eine (sehr umfangreiche) Liste von Sicherheitsfragestellungen, ohne für die Akteure konkrete Handlungsempfehlungen daraus abzu-

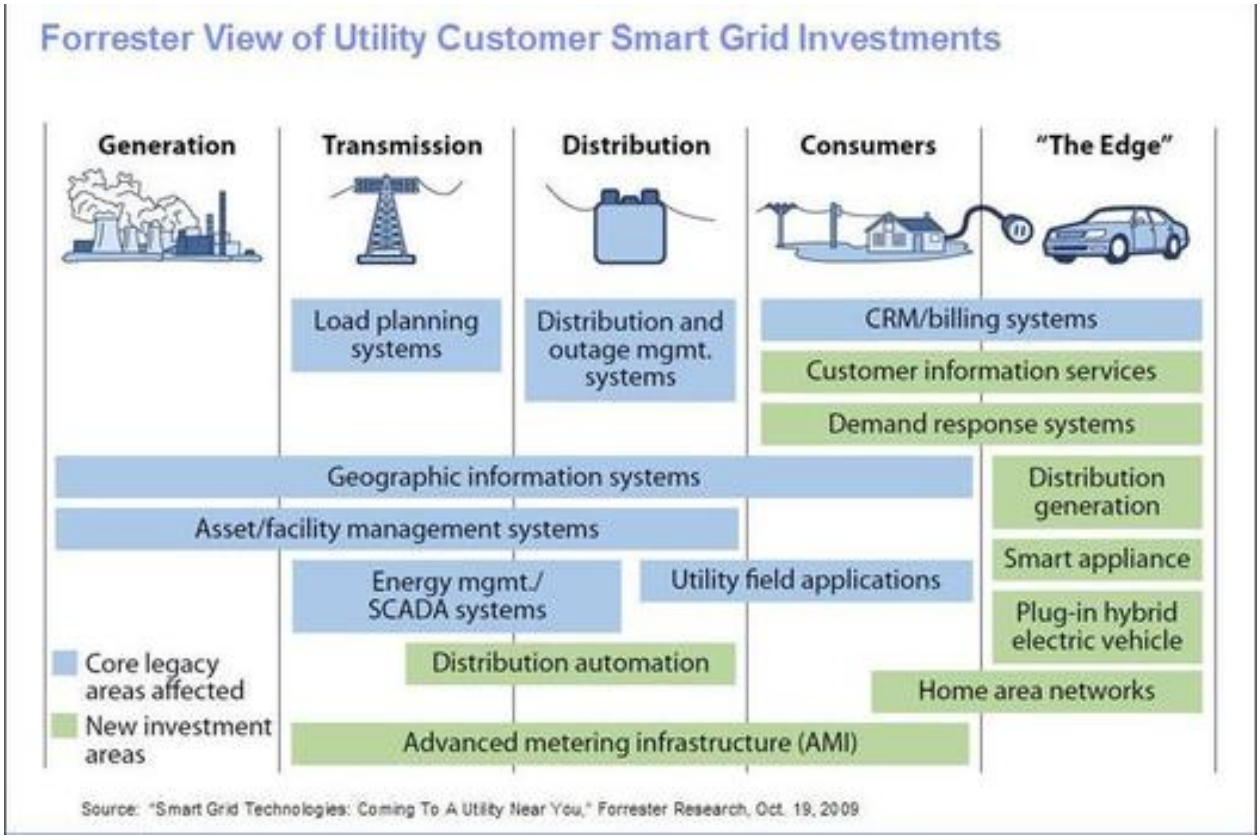


Abbildung 9: Akteure mit ihren angestammten Domänen und neuen Aktivitäten (Quelle Forrester Research)

leiten. So beschreibt die Roadmap beispielsweise acht verschiedene Authentisierungsfragestellungen, die von der Authentisierung der Techniker, die Wartungsarbeiten Vorort am Smart Meter durchzuführen haben, über die Authentisierung von Außendienstmitarbeitern, die SCADA Netze im Feldeinsatz zu warten haben, bis hin zur Authentisierung von Kunden oder auch einzelner Geräte in einer Maschine-zu-Maschine-Kommunikation. Diese Auflistung der Problembereiche ist für einen Überblick sicherlich sehr nützlich, hilft aber den einzelnen Akteuren im Smart Grid wenig, um deren jeweiligen Rechte, Pflichten, Handlungsoptionen sowie die möglichen Bedarfe und Wünsche ihrer Kunden zu verstehen und um auf dieser Basis Entscheidungen für Investitionen abzuleiten, die zukunftssicher und nachhaltig sind.

Benötigt wird deshalb eine nationale Roadmap *IT-Sicherheit im Smart Grid*, die den Akteuren aufzeigt, welche Handlungsoptionen sie haben, welche Investitionen ggf. notwendig sind und welche Mehrwerte (Geschäftsmodelle) möglich sind.

Nachfolgend werden einige Handlungsempfehlungen skizziert, deren Umsetzung zu einer solchen Roadmap führen könnte. Dazu werden einige der in Kapitel 6 aufgezeigten Forschungsfragen aufgegriffen und um weitere Aspekte ergänzt. Zur Erstellung einer solchen Roadmap wird ein Team benötigt, das aus Vertretern aller relevanten Akteure der E-Energy-Domäne zusammengesetzt ist, damit deren Interessen angemessen vertreten und berücksichtigt werden.

7.1 Handlungsempfehlungen zur Erstellung einer nationalen Sicherheits-Roadmap

Entwicklung von Rollenmodellen und System-Architekturen

In einem ersten Schritt sollten Rollenmodelle erstellt und Marktteilnehmer-spezifische Subsysteme bzw. Domänen (siehe unten) identifiziert und spezifiziert werden. Das Ziel sollte sein, Verantwortungs- und Aufgabenbereiche abzugrenzen und damit zu beherrschbareren Teilsystemen zu gelangen.

Folgende Marktrollen werden in der Regel identifiziert: Produzent, Energienutzer, Übertragungsnetzbetreiber, Verteilungsnetzbetreiber, Energielieferant (Multi-Utility: Strom, Wärme, Gas, Wasser), Energiehändler, Messstellenbetreiber, Energiemarktplatzbetreiber, Kommunikationsnetzbetreiber, Energiedienstleister.

Für eine Sicherheitsbetrachtung sind diese Rollen weiter zu untergliedern. Beispielsweise sollte die Rolle des Kunden untergliedert werden in: Privathaushalt, gewerblicher Kunde und Industrieunternehmen.

Die Rolle Energieproduzent kann untergliedert werden in: zentrale und dezentrale Erzeuger (z.B. Photovoltaikanlagen in Privathaushalten), oder auch in Strom- oder Wärmeerzeuger.

Diese Akteure repräsentieren Rollen, die ähnliche Ziele haben, damit einen ähnlichen Schutzbedarf sowie ähnliche Rechte und Pflichten besitzen. Diese konzeptuelle Bündelung von Aktivitäten zu Rollen ist für eine Sicherheitsbetrachtung sehr nützlich. Sie ermöglicht es, Schutzbedarfe aus Sicht der unterschiedlichen Akteure zu erfassen. Sie bietet zudem die Grundlage für die Umsetzung der Rechte und Pflichten auf der technischen Ebene durch eine rollenbasierte Zugriffs- und Nutzungskontrolle.

In einem nächsten Schritt sind die Rechte und Pflichten der verschiedenen Rollen zu identifizieren. Dazu müssen die nationalen und europäischen Gesetzesvorgaben, insbesondere daten-

schutzrechtlicher Vorgaben etc. sowie organisatorische, unternehmerische und sonstige relevante Vorgaben erfasst und auf die Rollen und die Domänen, in denen die Rollen aktiv sind, abgebildet werden. Ausgehend von diesen Rahmenbedingungen und der Identifikation der zu schützenden Güter (assets) ist der jeweilige Schutzbedarf der Akteure unter Berücksichtigung der erfassten rechtlichen, unternehmerischen oder sonstigen Anforderungen und Auflagen abzuleiten. Aus dem Schutzbedarf müssen dann rollenbezogene Sicherheits-Policies (Regelwerke) abgeleitet und spezifiziert werden, die sowohl Rechte der Rollenmitglieder als auch deren Verpflichtungen (obligations) und Verantwortlichkeiten enthalten.

Die relevanten Domänen sind festzulegen. Eine Domäne beschreibt ein abgrenzbares Subsystem innerhalb des Smart Grid, das Aktivitäten von speziellen Use-Cases bündelt. In dem Papier der NIST [Lee2009] sind bereits etliche Use-Cases aufgeführt und auch in den E-Energy-Projekten des BMWi werden punktuell bereits Use-Cases erarbeitet. Dieses Material sollte aufbereitet, homogenisiert und dann für die domänen-bezogene Sicherheitsanalyse herangezogen werden. Eine Domäne ist durch die beteiligten Akteure/Rollen (Stakeholder) der Domäne und deren Zusammenwirken zu definieren. Beispiele für solche Domänen könnten die Energieerzeugung und -verteilung oder auch die Energiemarktplätze sein. Für die Domänen müssen die akteurspezifischen Sicherheits-Policies zu den jeweiligen Domänen-Policies zusammengeführt, Widersprüche in den Regelwerken aufgedeckt und beseitigt werden. Kriterien für die Auflösung von Widersprüchen könnten beispielsweise eine Priorisierung oder aber auch eine Kosten-Nutzen-Abwägung sein. Mit einer solchen Vorgehensweise könnte man für die verschiedenen Akteure einer Domäne die Rechten und Pflichten transparent machen, so dass beispielsweise ein Stromerzeuger die Sicherheitsbedarfe der Kunden vor Augen hat und sich mit seinen zu ergreifenden Maßnahmen darauf einstellen kann.

Ausgehend von den domänen-spezifischen Policies sollten verschiedene Architekturvorschläge/Blueprints ausgearbeitet werden, denen beispielsweise eine unterschiedliche Priorisierung der Anforderungen zugrunde gelegt werden kann. Die Roadmap sollte datenschutzfördernde Gestaltungsansätze für Szenarien unter Anwendung von datenschutzrechtlichen Prinzipien der Datensparsamkeit, Zweckbindung, Erforderlichkeit, Transparenz, Datensicherheit, Kontrolle und Wahlfreiheit als Handlungsempfehlungen entwickeln. Beispiele für solche Architekturvorschläge könnten sein: Umsetzung eines konsequenten Privacy-by-Design-Prinzips, also eine sehr hohe Priorisierung von datenschutzrechtlichen Anforderungen, so dass beispielsweise alle personenbezogenen Verbrauchsdaten dezentral in den Privathaushalten vorverarbeitet und nur in anonymisierter, aggregierter Form kommuniziert werden, oder User-Managed-Privacy, also individuell steuerbare Privacy-Einstellungen, so dass ein Kunde individuell entscheiden kann, welche Daten er welchem Dienstleister wofür zur Verfügung stellen möchte, um dafür im Gegenzug spezifische Vorteile zu erhalten.

Durchführung von domänen-basierten Risiko-Analysen

Das NIST hat u. a. in [Lee2009, NIST2010] hierzu bereits sehr umfangreiche Vorarbeiten geleistet. Diese gilt es auszuwerten, auf die deutschen bzw. europäischen Gegebenheiten abzubilden und im Sinne eines Handlungsleitfadens für ausgewählte Domänen detailliert auszuarbeiten.

Hierzu müssen Angreifermodelle festgelegt und charakteristische Angriffsszenarien definiert werden. Da IT-Sicherheitsangriffe auch gravierende Auswirkungen auf die Betriebssicherheit von Anlagen haben können, sind kombinierte Safety- und Security-Analysen erforderlich, die beispielsweise die Techniken der Fehlerbaumanaly-

se mit der Risikoanalyse mittels Angriffsbäumen kombinieren. Ausgangspunkt für die Analysen sollten die Architektur-Blueprints für die verschiedenen Domänen sein. Da auch in den abgegrenzten Subsystemen noch eine Vielzahl von Komponenten miteinander interagieren, könnte die Erstellung von Simulationsmodellen hilfreich sein, um multilaterale, kaskadierende Abhängigkeiten nachzubilden und das Ausmaß eines potentiellen Schadens zu verdeutlichen.

Aus der Risikoanalyse sind die sich für die verschiedenen Akteure (u. a. Stromversorger, Gerätehersteller, Infrastrukturbetreiber, Stadtwerke, Unternehmen, Privathaushalt) ergebenden Konsequenzen abzuleiten.

Die Roadmap sollte Empfehlungen für gesetzliche Rahmenbedingungen erarbeiten, so dass frühzeitig die rechtlichen Anforderungen klar sind und diese Anforderungen in der Gestaltung der technischen Systeme und Prozesse direkt umgesetzt werden können.

Die Ergebnisse der Risikoanalyse zeigen den Handlungsbedarf für die Absicherung der Komponenten und Geschäftsprozesse der verschiedenen Domänen auf. Die Architektur-Blueprints sind entsprechend zu verfeinern. Von besonderer Bedeutung sind hierbei die Schnittstellen der Domänen zu anderen Domänen. Beim Domänenübergang ergeben sich spezifische Sicherheitsanforderungen, so dass die Roadmap auch Empfehlungen zu deren Behandlung für die verantwortlichen Akteure erarbeiten sollte. Beispielsweise könnte eine Empfehlung sein, besonders sicherheitskritische Domänen physisch vollständig von weniger kritischen Domänen zu entkoppeln, auch wenn dies zusätzliche Investitionen in die IKT nach sich ziehen würde. Weitere Empfehlungen könnten die gezielte Einführung von Fail-safe-Konzepten sein, um sicherzustellen, dass eine kritische Domäne auch beim Eintreten von Fehlern bzw. Angriffen seine Mindestfunktionalität noch aufrechterhalten kann (Fehler- bzw. Angriffsresistenz).

Durchführung von betriebswirtschaftlichen Kosten-Nutzen-Rechnungen

Die Absicherung komplex vernetzter, sicherheitskritischer IKT-Infrastrukturen verursacht erhebliche Mehrkosten. Begleitend zu den Sicherheitsanalysen und Handlungsempfehlungen sollte die Roadmap deshalb auch Kosten-Nutzen-Betrachtungen durchführen, die über die aktuell geführte Diskussion der Anreizmodelle für Endkunden zum Energieeinsparen durch spezielle Tarifmodelle hinausgehen. Hierzu sind Business-Cases (risks versus opportunities) zu entwickeln, die neben den Kosten insbesondere auch die Möglichkeiten der Smart Grid-IKT-Infrastruktur aufzeigen. Vorstellbar ist die Entwicklung von Szenarien für Anwendungsdomänen, die weit über die Energiedomäne hinausreichen. Ein Beispiel wäre der Gesundheitsbereich mit der mobilen, IKT-gestützten Pflege. In Deutschland sind über 40 Millionen Wohnungen mit einer Smart Meter-Infrastruktur auszustatten, so dass eine rechtzeitige Beachtung von Maßnahmen zur Unterstützung von älteren oder Personen mit Einschränkungen hier wirtschaftlich interessante Mehrwerte für Betreiber von Wohnanlagen und Anreize zur Investition schaffen könnte.

Durchführung bedarfsorientierter Technologiebewertungen

Um die ermittelten Sicherheitsbedarfe zu erfüllen, sind mit angemessene Sicherheitstechnologien und Sicherheitsmaßnahmen einzusetzen. Die Roadmap sollte auch hierfür Handlungsempfehlungen beinhalten. Dazu sind die vorhandene Technologien zu analysieren und in Bezug auf ihre Einsetzbarkeit zu bewerten. Das Ziel sollte hierbei sein, erprobte und gut eingeführte Sicherheitsstandards so weit wie möglich zu übernehmen und aufzuzeigen, wo ergänzende Sicherheitsmaßnahmen notwendig werden. Die Roadmap sollte Einsatzempfehlungen für Technologien und Kontrollmaßnahmen enthalten, die zur Erfüllung der spezifischen Sicherheitsbedarfe der

Domänen, aber auch einzelner Use-Cases, geeignet sind. Der nachhaltig sichere Betrieb von Anlagen und Plattformen wird eine große Herausforderung für Betreiber und Dienstleister werden. Die Roadmap sollte hierzu bereits Muster für betriebswirtschaftliche angemessene Betriebskonzepte erarbeiten, die Empfehlungen für datenschutzrechtliche Prozesse und das Sicherheitsmanagement geben, um das einmal erstellte Schutzniveau über den Lebenszyklus der Anlage aufrecht zu erhalten.

7.2 Entwicklung einer Forschungsagenda

In Kapitel 6 dieses Beitrags wurden bereits wesentliche Bereiche identifiziert, die noch Forschungs- und Entwicklungsbedarf aufweisen. Die wichtigsten FuE-Bereiche betreffen die Entwicklung von Konzepten für manipulationsresistente Komponenten wie Zähler, die die Daten aktuell, manipulationsgeschützt (gegen Angriffe von Innen und Außen) und datenschutzbewahrend erheben, (vor)verarbeiten und kommunizieren. Es werden skalierende Identifikations- und Authentisierungsschemata für die Maschine-zu-Maschine-Kommunikation benötigt, die im Smart Grid eine große Bedeutung erlangen wird. Weitere offene Fragestellungen betreffen die Entwicklung effizienter, sicherer Schlüsselmanagementverfahren unter Berücksichtigung betrieblicher Kosten, die Entwicklung von rollenbasierten Zugriffskontroll- und insbesondere Nutzungskontrollverfahren, die auch für ressourcenbeschränkte Komponenten verwendbar sind.

Im Bereich der Kommunikationsinfrastrukturen besteht der Bedarf zur Entwicklung dedizierter, in nahe Echtzeit agierender Überwachungsprotokolle im Sinne kooperativer Frühwarnsysteme, um aufkommende Probleme frühzeitig zu erkennen und rechtzeitig geeignete Abwehrmaßnahmen einzuleiten. Um der verteilten Verarbeitung von kritischen Daten Rechnung zu tragen, sind existierende Konzepte zur Isolierung, Attestierung und zum Manipulationsschutz zu erweitern und mit abgestuften, insbesondere auch verteilten Kontrollen (Identität, Zugriffskontrolle, Abschottungen) zu kombinieren, um nicht einen einzigen Sicherheitskontrollpunkt mit entsprechender Verwundbarkeit zu etablieren. Zudem ist der Bedarf an der Entwicklung von Betriebskonzepten zur Angriffs- und Ausfalltoleranz erkennbar.

Im Bereich der Energiemarktplätze wird die sichere Entwicklung und Bereitstellung von Dienstleistungen für Smart Grid noch weitere Forschungsfragen aufwerfen. Es ist zu klären, welche Sicherheitsdienstleistungen im Sinne des Security-as-a-Service-Paradigmas für solche Marktplätze sinnvoll und zur Verfügung zu stellen sind. Beispiele könnten Identitätsdienste (Identity-as-a-Service), Anonymisierungsdienste, Schlüsselmanagement und PKI-Dienste, aber auch Policy-Desicion-Dienste sein, die Regelwerke verwalten und Zugriffsentscheidungen zentral treffen, deren Durchsetzung dann dezentral durch Enforcement-Komponenten umzusetzen ist. Für bereits bestehende Dienste sind ggf. dedizierte Sicherheitsdienste zum Wrappen/Härten von Diensten oder zum Filtern von Daten, um Data Leakages zu minimieren, zu entwickeln. Für die Nutzung sicherheitskritischer Mehrwertdienste durch Verbraucher, z.B. den Zugriff auf die eigenen Profildaten auf dem Marktplatz, sollte die Einbindung des digitalen Personalausweis untersucht und mit prototypischen Umsetzungen dessen Einbindung in Geschäftsprozesse aufgezeigt werden.

Ein dringender Forschungsbedarf besteht noch im Bereich des kontinuierlichen Testens. Es müssen Testmethoden und Testszenarien zur Durchführung von, „Gesundheitschecks“ für Dienstleistungsangebote im Energiemarktplatz, in der Energie-Cloud, entwickelt und erprobt werden. Existierender Methoden des Risikomanagements sind zu erweitern, so dass sie auch im laufenden Betrieb eines Smart Grid eingesetzt (z.B. Lagebild und Health-Monitoring) werden können. Die Roadmap sollte deshalb auch Vorschlägen für

Test- und Prüfnormen und -verfahren umfassen, die neben den Tests der Informations- und Funktionssicherheit (security und safety) auch Interoperabilitätstests, Tests der Robustheit gegenüber Angriffen, wie Seitenkanalattacken etc. umfassen.

Die Roadmap sollte die wichtigsten Forschungsbedarfe identifizieren und eine Forschungsagenda erarbeiten.

8 Zusammenfassung

Die Energieversorgungssysteme der Zukunft erfordern komplexe Informations- und Kommunikationssysteme zu deren Steuerung und Verwaltung. Derartige Systeme müssen in der Lage sein, die zur Steuerung erforderlichen Daten zu erheben, über Kommunikationsnetze zu transportieren und mittels Energiemanagementsystemen zu verarbeiten. Die systematische Integration von geeigneten Sicherheitsmaßnahmen ist unabdingbare Voraussetzung für die Akzeptanz und Wirksamkeit derartiger Systeme. Nur wenn die Privatsphäre bewahrt und die Vertraulichkeit der ausgetauschten Daten, aber auch deren Korrektheit und Manipulationssicherheit gewährleistet wird, das System zuverlässig arbeitet und rechtzeitig die gewünschten Dienstleistungen erbringen kann, sind die gewünschten Effekte hinsichtlich Energieeinsparung und Umweltschutz erfüllbar. Dieser Beitrag hat die technischen, organisatorischen und juristischen Rahmenbedingungen eines Energieinformationssystems beleuchtet, die Bedrohungslage analysiert und wichtige Forschungsfragen identifiziert sowie Handlungsbedarfe in Bezug auf die Etablierung des erforderlichen technischen Sicherheitsstandards identifiziert.

Als nächster Schritt wird die Erarbeitung einer umfassenden, nationalen Roadmap zum Thema Sicherheit und Datenschutz im Energieinformationsnetz empfohlen. Kapitel 7 versuchte hierfür Anregungen und Empfehlungen zu geben. Eine solche Roadmap sollte die wichtigsten Fragestellungen aufbereiten, den IST-Stand in Deutschland (Angebote/Entwicklungen in der Industrie, Forschungseinrichtungen) systematisch erfassen und mit dem Stand der Entwicklung und Umsetzung im europäischen und außer-europäischen Umfeld in Beziehung setzen und die skizzierten Handlungsempfehlungen systematisch ausarbeiten. Das Ziel ist es, einen Handlungsleitfaden für die Politik, die Wirtschaft und die Wissenschaft zu erarbeiten, so dass die offenen Punkte gezielt und mit gebündelten Kräften bearbeitet werden können.

Zur Umsetzung der Handlungsempfehlungen scheint die deutsche Wirtschaft und Forschung gut aufgestellt zu sein. Eine zögerliche Haltung, die nächsten erforderlichen Schritte tatsächlich auszuführen, birgt jedoch die Gefahr, dass branchenübergreifende Annäherungen zum Erkennen gemeinsamer Lösungswege unterbleiben und letztlich fehldimensionierte Lösungen favorisiert oder sogar standardisiert werden.

Danksagung

Wir bedanken uns herzlich für die wertvollen Beiträge zum vorliegenden Papier bei Harald Orlamünder (Ingenieurbüro für IKT), Aleksei Resetko (Alcatel-Lucent Deutschland AG), Prof. Dr. Alexander Rossnagel und Dr. Silke Jandt (Universität Kassel), Prof. Dr. Paul Kühn (Universität Stuttgart) und Dr. Petra Beenken (OFFIS Oldenburg).

Referenzen

[An2010] R. Anderson, S. Fuloria, Who controls the off switch?, 2010, http://www.cl.cam.ac.uk/~rja14/Papers/meters-offswitch.pdf

[Bee201015] P. Beenken, H. Appelrath, C. Eckert. Datenschutz und Datensicherheit in intelligenten Energienetzen. In DACH Security 2010, Viena, Austria, September 2010

[Br2010] M. Brunner, H. Hofinger, C. Krauß, C. Roblee, P. Schoo, S. Todt, Infiltrating Critical Infrastructures with Next-Generation Attacks - W32.Stuxnet as a Showcase Threat, Version 1.4, Fraunhofer-Institut für Sichere Informationstechnologie SIT, München, December 2010

[Cav201010] Cavoukian, Polonetsky, Wolf, Smart Privacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation, 2010, 9 ff.

[DKE2010] DKE, Die deutsche Normungsroadmap E-Energy/Smart Grid, 2010

[Eck2009] C. Eckert, "IT-Sicherheit: Konzepte - Verfahren - Protokolle", 6.Auflage, ISBN 3486589997, Oldenbourg, 2009

[EPR2009] Electronic Power Research Institute, Report to NIST in the Smart Grid Interoperability Standards Roadmap, 2009, www.nist.gov/smartgrid

[ETPS2008] ETP Smart Grids, Smart Grids – Strategic Deployment Document for Europe's Electricity Networks of the Future, Sept. 2008, www.smartgrids.eu

[Fa2010] N. Falliere, L. O Murchu, E. Chien, W32 Stuxnet Dossier, Whitepaper Version 1.0, Symantec, September 2010

[Hei2009] Heise Online, Intelligente Stromnetze: Ich weiß, ob du gestern geduscht hast, 19.11.2009 http://www.heise.de/newsticker/meldung/Intelligente-Stromnetze-Ich-weiss-ob-du-gestern-geduscht-hast-864221.html

[Igu2006] V.M. Igure, S. A. Laughter, R. D. Williams, "Security issues in SCADA networks", Computers & Security, Vol 25, No 7, S. 498--506, 2006

[Jav2010] Shahram Javadi, Shahriar Javadi, "Steps to smart grid realization", Proceedings of the 4th WSEAS international conference on Computer engineering and applications, Cambridge, USA, Pages: 223-228, 2010, ISSN 1790-5117

[Khu2010] H. Khurana, M. Hadley, N. Lu, D. A. Frinck, "Smart-Grid Security Issues", IEEE Security and Privacy, Volume 8, Issue 1 (January 2010), Pages: 81-85, 2010, ISSN 1540-7993

[KO2003] A. Krings and P, Oman, A Simple GSPN for Modeling Common Mode Failures in Critical Infrastructures, Proceedings der 36th Hawaii International Conference on System Sciences, 2003

[Law2010] N. Lawson, Reverse-engineering a smart meter, 15.02.2010 http://rdist.root.org/2010/02/15/reverse-engineering-a-smart-meter/

[Lee2009] The Cyber Security Coordination Task Group, A. Lee, T. Brewer (Eds), "Smart Grid Cyber Security Strategy and Requirements", Draft NIST IR 7628, September 2009

[NIST2010] The Smart Grid Interoperability Panel, Cyber Security Working Group, "Guidelines for SmartGrid Cyber Security Vol 3, Supportive Analyses and References", Draft NIST IR 7628, August 2010

[Orl2009] H. Orlamünder, "Der Einsatz von Informations- und Kommunikationstechnik in Stromnetzen -- ein Nachhaltiges Energieinformationsnetz", Stiftungsreihe 85, 2009

[Ro2010] A. Roßnagel, S. Jandt, "Datenschutzfragen eines Energieinformationsnetzes", Stiftungsreihe 88, 2010

[Sto2009] B. Stone-Gross, M. Cova, L. Cavallaro, B. Gilbert, M. Szydlowski, R. Kemmerer, C. Kruegel, G. Vigna, "Your botnet is my botnet: Analysis of a botnet takeover", Proceedings of the 16th ACM conference on Computer and communications security, S. 635--647, 2009

[Li2010] D. Lill, A. Sikora, Wireless Systemarchitekturen für Multi Utility Smart Metering unter Nutzung von Wireless M-Bus, Fachtagung Smart Energy 2010, Innovative, IKT-orientierte Konzepte für den Energiesektor der Zukunft, 29. Oktober 2010, Dortmund

[Lu2009] G. Luft, Energy security challenges fort the 21st century, a reference handbook, ABS-CLIO, 2009

[Mc2009] P. McDaniel, S. McLaughlin, "Security and Privacy Challenges in the Smart Grid", IEEE Security and Privacy, Volume 7, Issue 3 (May 2009), Pages: 75-77, 2009

[Ro2010] A. Roßnagel, S. Jandt, Datenschutzrisiken eines Energieinformationsnetzes, Alcatel-Lucent Stiftung, 2010, 6 ff.

[Sch2010] P. Schoo, Smart-Energie: Wieviel Datenschutz und Datensicherheit wollen wir uns leisten?, Fachtagung Smart Energy 2010, Innovative, IKT-orientierte Konzepte für den Energiesektor der Zukunft, 29. Oktober 2010, Dortmund

[SP2010] E. H. Spafford, Remembrances of Things Pest, Commun. ACM 53 35--37 (2010)

[St2003] J. Stamp, P. Campbell, J. DePoy, J. Dillinger, W. Young, Sustainable Security for Infrastructure SCADA, Sandia National Laboratories, 2003

[Wolf09] W. Wolf. Cyber-physical systems. IEEE Computer, 42(3):88– 89, 2009.

Autor/innen

Prof. Dr. Claudia Eckert ist Leiterin des Fachgebiets Sicherheit in der Informationstechnik des Fachbereichs Informatik an der Technischen Universität in München sowie Leiterin des Fraunhofer-Instituts für Sichere Informationstechnologie München.

Dr. Christoph Krauß und **Peter Schoo** sind wissenschaftliche Mitarbeiter am Fraunhofer-Institut für Sichere Informationstechnologie, München.

Projekt NEWISE

Das Bundesministerium für Wirtschaft und Technologie mit dem Förderprogramm „E-Energy: IKT-basiertes Energiesystem der Zukunft“ (www.e-energy.de) und die Alcatel-Lucent Stiftung für Kommunikationsforschung veranstalteten am 17. Juni 2010 im Konferenzzentrum des Ministeriums im Rahmen der NEWISE-Veranstaltungsreihe der Stiftung die zweite große Konferenz. Thema war „Nutzerschutz im Energieinformationsnetz. Daten- und Verbraucherschutz in Smart Grids“.

Das transdisziplinäre Projekt NEWISE (Nachhaltiges Energieinformationsnetz - Wettbewerb, Information und Sicherung für die Energieversorgung) wurde von der Alcatel-Lucent Stiftung im Mai 2009 gestartet und trägt mit Unterstützung des Fördervereins Stiftungs-Verbundkolleg durch Sachstandsanalysen und Diskursveranstaltungen wichtige Erkenntnisse und Ergänzungen zum Themenfeld bei. In engster Kooperation mit dem Förderprojekt E-Energy ergänzt das Diskursprojekt insbesondere für kommunale Entscheider in Politik und Verwaltung diverse Themenschwerpunkte wie

- Erfordernisse und Anforderungen für Datenschutz, Privatheits- und Verbraucherschutz,
- Potentiale der Sicherung von versorgungskritischen Infrastrukturen,
- Potentiale des Wettbewerbs sowie der Regulierung im „Konvergenzraum“ von Energie-, Informations- und Kommunikationsversorgung.

Auf der Basis wissenschaftlicher Erkenntnisse sollen konkrete Empfehlungen für die Praxis folgen. Dies kann im Entstehungsstadium neuer Systeme am ehesten geleistet werden, um zwischen den Polen einer realitätsblinden Begeisterung einerseits und einer realitätsverneinenden Ablehnung andererseits gangbare Wege zu öffnen.

Als hilfreiches Leitbild für die Diskussion in der NEWISE-Arbeitsgruppe hat sich ein Mittelweg herausgestellt, der die notwendigen und hinreichenden interdisziplinären Analysen im Zusammenwirken der gesellschaftlichen Subsysteme mit diskursgestützten konsensuellen Empfehlungen verbindet. Dies ist das hoch anerkannte Bestreben der Stiftung als „interessenneutrale Plattform“ seit über drei Jahrzehnten. Dabei ist klar: Nicht alle innovativen Impulse sind dergestalt in gemeinsame Strategien umsetzbar, gerade im globalen Wettbewerb können bei aller Betonung des nationalen Standorts und dessen infrastruktureller Ausstattung die europäischen Bezüge bis hin zu der globalen Verflechtung der Wirtschaft nicht außer Acht gelassen werden.

Hier setzen gerade am Standort Deutschland die Aktivitäten von Initiativen, Verbänden, Vereinigungen und Stiftungen an, die das konsensuelle Vorgehen in gemeinsam definierten Rahmen unterstützen.

In dieser StiftungsReihe der Alcatel-Lucent Stiftung wird der Diskussionsstand des Projekts NEWISE über die Eckpunkte der IT-Sicherheit für ein nachhaltiges Energieinformationsnetz dargestellt. Das Projekt NEWISE verwendet den darin erstmals geprägten Begriff „Energieinformationsnetz“ nicht als Alternative (bzw. Übersetzung) zu „Smart Grid“, sondern bezeichnet damit die zu gestaltende künftige Struktur des Netzes. Die vorliegende Publikation ergänzt in hervorragender Art und Weise die aus NEWISE bereits hervorgegangenen StiftungsReihen „Der Einsatz von Informations- und Kommunikationstechnik in Stromnetzen - ein Nachhaltiges Energieinformati-

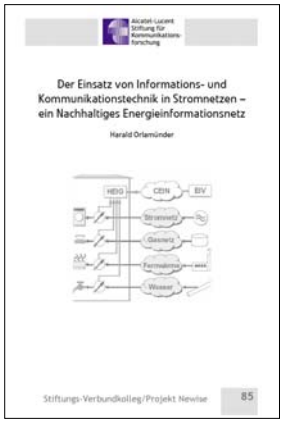
onsnetz (Harald Orlamünder; Nr. 85) sowie „Datenschutzfragen eines Energieinformationsnetzes“ (Alexander Roßnagel, Silke Jandt; Nr. 88).

Dem Kuratorium der Stiftung und hier insbesondere Alf Henryk Wulf, Vorstandsvorsitzender der Alcatel-Lucent Deutschland AG, ist das NEWISE-Projekt auch für das persönliche Engagement zu großem Dank verpflichtet. Der Dank für zahlreiche Hilfestellungen und Ermunterungen gilt ganz besonders auch Dr. Andreas Goerdeler und Dr. Michael Zinke vom Bundesministerium für Wirtschaft und Technologie.

Jürgen Reichert
Projektleiter NEWISE

Weitere Publikationen des Projekts NEWISE

Die Publikationen können kostenfrei über die Geschäftsstelle der Alcatel-Lucent Stiftung bezogen oder unter www.stiftungaktuell.de abgerufen werden:



Harald Orlamünder:
Der Einsatz von Informations- und Kommunikationstechnik in Stromnetzen - ein Nachhaltiges Energieinformationsnetz,
StiftungsReihe Nr. 85

Alexander Roßnagel, Silke Jandt:
Datenschutzfragen eines Energieinformationsnetzes,
StiftungsReihe Nr. 88

Alcatel-Lucent Stiftung

Die Alcatel-Lucent Stiftung für Kommunikationsforschung ist eine gemeinnützige Förderstiftung für Wissenschaft insbesondere auf allen Themengebieten einer „Informationsgesellschaft“, neben allen Aspekten der neuen breitbandigen Medien speziell der Mensch-Technik-Interaktion, des E-Government, dem Medien- und Informationsrecht, dem Datenschutz, der Datensicherheit, der Sicherheitskommunikation sowie der Mobilitätskommunikation. Alle mitwirkenden Disziplinen sind angesprochen, von Naturwissenschaft und Technik über die Ökonomie bis hin zur Technikphilosophie.

Die Stiftung vergibt jährlich den interdisziplinären "Forschungspreis Technische Kommunikation", Dissertationsauszeichnungen für WirtschaftswissenschaftlerInnen sowie Sonderauszeichnungen für herausragende wissenschaftliche Leistungen.

Die 1979 eingerichtete gemeinnützige Stiftung unterstützt mit Veranstaltungen, Publikationen und Expertisen ein eng mit der Praxis verbundenes pluridisziplinäres wissenschaftliches Netzwerk, in dem wichtige Fragestellungen der Informations- und Wissensgesellschaft frühzeitig aufgenommen und behandelt werden.

www.stiftungaktuell.de

Kontakt

Alcatel-Lucent Stiftung
Lorenzstraße 10, 70435 Stuttgart
Telefon 0711-821-45002
Telefax 0711-821-42253
E-Mail office@ stiftungaktuell.de
URL: http://www.stiftungaktuell.de