TeleTrusT – Bundesverband IT-Sicherheit e.V.
Der IT-Sicherheitsverband.

TeleTrusT-Eckpunktepapier "Smart Grid Security"

TeleTrusT-Arbeitsgruppe "IT-Sicherheit im Smart Grid"

Autoren

Michael Gröne, Sirrix AG security technologies
Arno Fiedler, Nimbus Technologieberatung GmbH
Stephan Gerhager, E.ON Energie AG
Steffen Heyde, secunet Security Networks AG
Dr. Gunnar Jacobson, Secardeo GmbH
Dr. Willi Kafitz, Siemens Enterprise Communications GmbH & Co. KG
Harald Kesberg, Kesberg Consulting
Dr. Rolf Lindemann, TC TrustCenter GmbH
Klaus J. Müller, Security Consulting
Dr. Thomas Störtkuhl, TÜV SÜD AG

Impressum

Herausgeber:

TeleTrusT – Bundesverband IT-Sicherheit e.V.
Chausseestraße 17
10115 Berlin
Tel.: +49 30 400 54 306
Fax: +49 30 400 54 311
E-Mail: info@ TeleTrusT.de
http://www.TeleTrusT.de

Herstellung:

DATEV eG, Nürnberg

1. Auflage

Inhalt

1 Präambel

Die politisch beschlossene Energiewende in Deutschland erfordert einen tiefgreifenden Umbau der Infrastruktur zur Energiebereitstellung und -verteilung. Entscheidend wird es sein, Angebot, Nachfrage und Verteilung von Energie intelligent zu steuern.

Die Herausforderungen, die sich aus dem Umbau der Energieversorgung ergeben werden, sind gravierend und im Detail noch nicht absehbar. Diese Publikation will daher keine "fertigen" Lösungen anbieten, sondern als Eckpunktepapier Ansatzpunkte aufzeigen und Anregungen geben, wo beim Aufbau vom Smart Grids sichere Lösungen zu entwickeln, zu integrieren bzw. zu betreiben sind.

Kapitel 2 wird beleuchtet, wie insbesondere IKT den Umbau der Energieversorgung hin zu Smart Grids beeinflussen und auch zusätzliche Sicherheitsanforderungen bedingen wird.

Kapitel 3 greift die generellen Branchentrends und -anforderungen der Energiewirtschaft auf und analysiert daraus die branchenspezifischen Sicherheitsanforderungen.

Ab Kapitel 4 werden allgemeine Sicherheitsrisiken des Internets diskutiert und etablierte Schutzmaßnahmen erörtert.

Die vorliegende Publikation entstand während der Erarbeitung des "Common Criteria Protection Profile for the Gateway of a Smart Metering System" des BSI und der Technischen Richtlinie BSI TR 03109. Diese Dokumente enthalten technische Vorgaben insbesondere für den Smart Metering Bereich des Smart Grids, die durch Gesetze und Verordnungen in Zusammenarbeit von Politik, Regulierungsinstitutionen und Wirtschaft noch regulativ ausgestaltet werden.

2 Trends und Anforderungen bei der Energiewende

Die Stromerzeugung aus regenerativen Energiequellen wie Wind oder Photovoltaik und aus anderen Energieträgern wird künftig verstärkt dezentral erfolgen: Zahlreiche Stromverbraucher werden selber zu Erzeugern und speisen ihren Strom in die Netze ein. Damit geht die Zeit zu Ende, in der Strom ausschließlich zentral erzeugt und im Einbahnstraßenprinzip verteilt wurde. Dies muss auch Auswirkungen auf das Nutzerverhalten haben: Die verbrauchsorientierte Erzeugung muss sich zu erzeugungsorientiertem Verbrauch ändern. Eine Grundlage dazu ist ein ausreichendes und verlässliches Informationsangebot.

Die dezentrale Erzeugung, Übertragung und Nutzung regenerativer Energie ist jedoch aufgrund der starken Erzeugungsschwankungen bislang nur sehr schwer plan- und zudem nicht steuerbar – die bisherige konventionelle Netzleittechnik stößt hier an ihre Grenzen.

Ein Umbau der Stromnetze ist daher zwingend erforderlich: Mit den Smart Grids (Intelligentes Stromnetz) und der nötigen Datenbasis wird die Grundlage für eine optimierte Nutzung der Stromnetze geschaffen.

Verbrauchsdaten und Erzeugungsdaten müssen besser aufeinander abgestimmt werden. Dazu ist der Einsatz von Informations- und Kommunikationstechnologie erforderlich. Kommunikationsfähige Komponenten wie beispielsweise Smart Meter (Digitaler Stromzähler), Messstellen- bzw. Aggregationssysteme, aber auch elektrische Schaltungskomponenten, die beispielsweise über Internetprotokolle wie TCP/IP miteinander kommunizieren, machen dies technisch möglich. Smart Grids werden sich insbesondere der Technologie und des Know-hows bedienen, das seit Jahren in der Informations- und Kommunikationstechnologie zur Verfügung steht. So entsteht das "Internet der Energie".

Hierbei ergeben sich aber hohe Anforderungen an die IT-Sicherheit, soll die bisherige Stabilität des Stromnetzes jederzeit – auch in Krisenzeiten – aufrechterhalten werden. Bei der Konzeption und dem Aufbau von Smart Grids als Teil einer volkswirtschaftlich enorm wichtigen und kritischen Infrastruktur muss deshalb sofort zu Beginn im Design die Sicherheitsthematik eine wesentliche Rolle spielen.

Darüber hinaus müssen bei der laufenden Erfassung, Verarbeitung und Übermittlung von Daten jegliche Datenschutzanforderungen erfüllt sein, soll das Internet der Energie Akzeptanz beim Verbraucher finden.

2.1 Smart Grids – Zukunft der Stromwirtschaft mit Sicherheit

Die Stromversorgung in Deutschland und Europa steht vor neuen Herausforderungen: Der fortschreitende Klimawandel, der verstärkte Ausbau regenerativer Energien und die Liberalisierung der Energiemärkte bei Gewährleistung der Versorgungssicherheit machen einen tiefgreifenden Umbau der Elektrizitätsinfrastruktur innerhalb der nächsten Jahre erforderlich.

Um dem Klimawandel wirkungsvoll begegnen zu können, müssen die klimaschädigenden CO_2-Emissionen insbesondere aus Kohle- und Gas-Kraftwerken spürbar gesenkt werden. Politischer Wille ist, Energie effektiver und sparsamer zu nutzen und regenerative Energien massiv zu fördern. In der EU sehen die Energieeffizienzziele bis 2020 eine Reduzierung der CO_2-Emissionen um 20 Prozent sowie den anteiligen Ausbau der erneuerbaren Energien an der gesamten Stromversorgung um 20 bzw. 30 Prozent vor. Die in Deutschland gesetzten Ziele liegen sogar noch darüber.

2.2 "Consumer" werden zu "Prosumer" – Dezentralisierung der Stromerzeuger

Um diese ehrgeizigen Ziele zu erreichen, wird die Stromerzeugung aus regenerativen Energiequellen – z. B. Wind, Photovoltaik, Wasserkraft und Bioenergie – massiv ausgebaut. Das hat erhebliche Folgen für das Stromnetz: Wurde Strom in Deutschland bislang zentral in rund 300 Kraftwerken produziert und in Richtung der Verbraucher verteilt, so wird er künftig verstärkt aus regenerativen Energieträgern an einer Vielzahl von Standorten – also dezentral – erzeugt und nicht mehr nur in eine Richtung verteilt. Es kommt zu einem bidirektionalen Lastfluss, d. h. der bisherige Verbraucher, der "Consumer", wird zum "Prosumer", zum Erzeuger von Energie. Neben den neuen Anbietern von regenerativer Energie, deren Stromeinspeisung verstärkt gesetzlich erleichtert und wirtschaftlich begünstigt wird, wächst insbesondere auch die Zahl der privaten Erzeuger, die Strom z. B. durch eine Solaranlage auf ihrem Dach gewinnen.

Unterstützt wird der Umbruch in der Stromwirtschaft durch die politisch gewünschte und unterstützte Liberalisierung der Märkte. Sie führt zu einer vollständigen Veränderung des Marktgeschehens und der Rollen der Marktteilnehmer. Letztendlich entsteht sowohl auf Anbieter- als auch Verbraucherseite ein vollkommen neuer Marktplatz mit hoher Dynamik. Die Konkurrenz wächst.

Für all diese Anforderungen sind die heutigen Stromnetze nicht ausgelegt, sie stoßen zunehmend an ihre Leistungsgrenzen. Zu Spitzenzeiten sind die Netze bereits heute "verstopft", regenerativ erzeugter Strom kann deshalb nicht sinnvoll genutzt werden.

2.3 Voraussetzung: Lastausgleich im Stromnetz

Eine weitere große Herausforderung ist die Zunahme dezentraler Erzeugungsanlagen mit ihren stark schwankenden Leistungsabgaben. Da die Erzeugung erneuerbarer Energien häufig von externen Umständen, wie z. B. dem Wetter abhängt, sind ihre Erzeugungsleistungen nicht konstant. Sie müssen also mit steuerbaren Erzeugungskapazitäten (Kohle- und insbesondere flexibel steuerbare Gaskraftwerke) kombiniert werden, um eine lückenlose Stromversorgung sicherzustellen. Hierfür müssen die zahlreichen neuen Erzeuger vollständig und effizient in das Stromnetz integriert werden. Dies kann nur gelingen, wenn Stromerzeuger, -verbraucher und -speicher sowie die für die Übertragung und Verteilung notwendige Infrastruktur unter Einhaltung einer hohen Versorgungssicherheit intelligent miteinander vernetzt werden. Das bedeutet z. B., dass Verbraucher über Smart Meter (digitale Stromzähler) im Haushalt in kurzen Zeitabschnitten Verbrauchsdaten übertragen, Erzeuger gleichzeitig Daten zur Erzeugungsfähigkeit melden und Aggregationssysteme nahezu in Echtzeit den Bedarf an Strom in den einzelnen Netzabschnitten prognostizieren, den Energiefluss koordinieren und damit einen Lastausgleich bewirken.

2.4 "Smart Grids" – intelligente und kommunikative Stromnetze

Die Lösung heißt "Smart Grid". Dieses ermöglicht "die Vernetzung und Steuerung von intelligenten Erzeugern, Speichern, Verbrauchern und Netzbetriebsmitteln in Energieübertragungs- und -verteilungsnetzen mit Hilfe von Informations- und Kommunikationstechnik (IKT)". [38]

Im Smart Grid stehen folgende Anwendungsfelder in Kommunikation miteinander:
- Smart Generation (Intelligente Erzeugung)
- Smart Consumption (Intelligenter Verbrauch)
- Smart Distribution and Transmission (Intelligente Stromnetze)
- Smart Storage (Intelligenter Speicher)

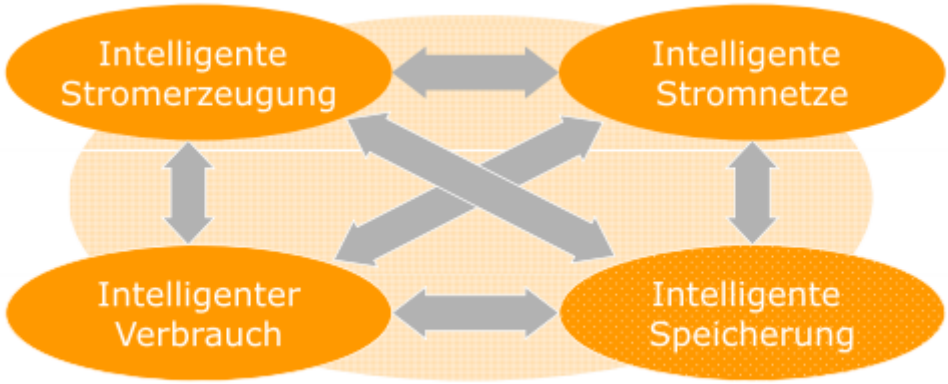


Abbildung 1: Vernetzung der Anwendungsfelder im Smart Grid

2.5 Neue Geschäftsmodelle durch Smart Grids

Der Übergang des derzeitigen Energiesystems hin zu einem Smart Grid ermöglicht nicht nur die Integration dezentraler Energieerzeuger, sondern lässt darüber hinaus eine Vielzahl möglicher neuer Geschäftsmodelle entstehen. So können sich bisherige wie auch neue Marktakteure zukünftig zu Informationsdienstleistern entwickeln, indem sie beispielsweise das Energiemanagement beim Kunden mit anbieten.

Ein heute noch auf wenige Marktakteure und Strombörsen beschränkter institutionalisierter Energiehandel wird zukünftig auch für Endverbraucher geöffnet werden. Auf der Nachfragerseite könnte es für Großhändler attraktiv werden, als Distributoren unterschiedliche Energieressourcen anzukaufen und dann maßgeschneiderte Produkte an große Endkunden, z. B. Stadtwerke, weiter zu verkaufen.

2.5.1 Flexible und kurzfristige Tarifverträge

Eine einheitliche Informations- und Kommunikationsinfrastruktur nach Vorbild und auf Basis des Internets erlaubt einen einfachen, standardisierten, kostengünstigen und zeitnahen Zugang zu Energieinformationen – auch für Verbraucher: Werden im Endkundenbereich momentan noch statische Tarifverträge abgeschlossen, so kann sich dies durch Einführung preisvariabler Tarife grundlegend ändern. Kunden erhalten Echtzeitinformationen über die Energiepreisentwicklung der nächsten Stunden und können dann – zunächst manuell, später durch Hausautomatisierungstechnik unterstützt – die für sie optimalen Tarife wählen.

2.5.2 Smart Home

Die Vernetzung kommunikativer Komponenten im Haushalt kann helfen, den Stromverbrauch intelligent zu steuern. So lassen sich über ein Smart Meter System, genauer über ein Energie Management Gateway mit einer Schnittstelle für Controllable Local Systems (CLS) Energie produzierende oder Energie verbrauchende Geräte überwachen. Auch Haushaltsgeräte, wie beispielsweise Waschmaschinen, lassen sich so steuern, dass sie sich zu Zeiten günstiger Stromtarife, z. B. nachts, einschalten. Mit Hilfe des Smart Meters lassen sich im Haushalt darüber hinaus besonders "stromfressende" Haushaltsgeräte ausfindig machen. Hierbei entstehen schützenswerte personenbezogene und damit datenschutzrechtlich relevante Daten. Verbrauchsprofile sind mittlerweile so genau, dass bei ausreichender Messwertauflösung erkannt werden kann, welcher Sender am Fernseher eingeschaltet ist [31].

2.5.3 E-Mobility

Teil des neuen Smart Grids sind auch Elektrofahrzeuge. Sie sind in erster Linie Stromverbraucher, die sich aber besonders gut zur erzeugungsabhängigen Lastverlagerungen eig-

nen. Da sie zudem sowohl mit Informations- und Kommunikationstechnologie als auch mit hochwertigen Stromspeichern ausgestattet sind, wären sie auch als Zwischenspeicher für Energie nutzbar. Dies wird allerdings skeptisch gesehen, weil durch häufiges Laden und Entladen die Batterielebenszeit sinkt. Laut dem "Nationalen Entwicklungsplan Elektromobilität" sollen in Deutschland bis zum Jahr 2020 mindestens eine Million am Stromnetz aufladbare "Plug-in" Elektro- und Hybrid-Fahrzeuge im Einsatz sein.

Eine Herausforderung ist die Identifizierung und Zuordnung des Fahrzeuges und des Rechnungsempfängers beim Aufladen mit Energie. Die Endverbraucher sind, im Gegensatz zu den klassischen Verbrauchern, mobil – was auch eine internationale Standardisierung erfordert. Die zu schaffende Ladeinfrastruktur ist dabei ein Bestandteil des Smart Grids. Es wird auch in diesem Zusammenhang eine Abrechnung mit dem bevorzugten Lieferanten diskutiert ("Roaming"). Dabei müssen Mobilitätsprofile aus datenschutzrechtlicher Sicht verhindert werden.

2.6 Überblick: Die Vorteile des Smart Grids

Smart Grids ermöglichen

- einen Übergang zur umweltfreundlichen Energieerzeugung.
- einen umfangreichen Ausbau der dezentralen Stromerzeugung. Stromerzeugung und -verbrauch erfolgen in geografischer Nähe, Transportverluste werden reduziert.
- die Abhängigkeit von wenigen zentralen und bei Ausfall nur schwer zu ersetzenden Energiequellen bzw. Kraftwerken zu verringern und so die Versorgungssicherheit zu gewährleisten.
- Energielieferung und -dienstleistung stärker zu vernetzen und vielfältige neue Energiedienstleistungen auf den Markt zu bringen.
- die Gestaltung flexiblerer Tarife und Verträge und stärken die Position von Endenergienutzern als aktive und eigenständig handelnde Teilnehmer im Energiemarkt.
- dem Endverbraucher dann Strom zu nutzen, wenn genügend Strom zur Verfügung steht.
- eine intelligente Nutzung von gespeicherter Energie, wenn erneuerbare Energie nicht ausreichend zur Verfügung steht (Rückspeisung).

Smart Grids sind die Lösung für die zunehmende Komplexität der Steuerung von Erzeugung, Nutzung, Verteilung und Speicherung der Energie durch optimierte Stromflüsse bei hohem Anteil dezentraler Erzeugung. Langfristig wird so eine Energieversorgung durch vorwiegend erneuerbare Energien mit stetig sinkendem Anteil fossiler und nuklearer Kapazitäten möglich. Voraussetzung ist dabei, dass Informationssicherheit und Datenschutz angemessen berücksichtigt wird.

2.7 Zentrale Rolle der IKT

Der Informations- und Kommunikationstechnologie kommt bei der Realisierung des Smart Grids und damit der Entwicklung einer zukunftsfähigen Energieversorgung eine Schlüsselrolle zu. Durch die Entflechtung von Marktrollen und dadurch notwendige Vernetzung können und müssen die einzelnen Teilnehmer Informationen austauschen und miteinander agieren. Dabei wird sich das Smart Grid der Technologie und des Know-hows bedienen, das seit Jahren in der Kommunikations- und Datentechnik vielfältig und preiswert zur Verfügung steht, wie beispielsweise des TCP/IP-Protokolls. Entsprechend wird der kommerzielle Handel und Datenaustausch im Smart Grid als Internet der Energie bezeichnet.

Intelligente, kommunikative Stromzähler, sogenannte Smart Meter inklusive einem Gateway, sind Kernstücke des Smart Grids und werden auch in Privathaushalten Einzug halten. Sie ermöglichen die digitale Erfassung der Verbrauchsdaten und deren Übermittlung zur Abrechnung und Steuerung. Gleichzeitig werden über die Kommunikationsschnittstellen auch Daten wie Tarifinformationen oder Daten zur Steuerung von Verbrauchsgeräten aus

dem Energienetz geladen. Die Steuerung des Energieflusses, zumindest durch deutlich bessere Prognosemodelle infolge besserer Daten, erfolgt auch auf Basis der durch die Smart Meter regelmäßig übermittelten aktuellen Verbrauchsdaten.

Durch die Kenntnis des aktuellen Verbrauchs wird die Lastenregelung vereinfacht, deren Ziel es ist, den Stromfluss zu steuern und ggf. die Stromerzeugung möglichst genau an den Bedarf anzupassen.

Je nach Marktrolle müssen dabei unterschiedliche Daten übertragen und verarbeitet werden, wie z.B.:
- Der Messstellenbetreiber benötigt für die Verarbeitung von Daten keine Detailkenntnisse über die Verbrauchsdaten.
- Der Verteilnetzbetreiber benötigt lediglich kumulierte Messdaten, um die Netznutzungsrechnung an den Lieferanten stellen und darüber hinaus Prognosewerte für dedizierte Netzsegmente abbilden zu können.
- Der Bilanzkreiskoordinator (meist der Übertragungsnetzbetreiber) benötigt über alle in seinem Netzbereich angeschlossenen Kunden eines Lieferanten aggregierte Messwerte in vglw. hoher Auflösung (z.B. 15 Min.) für die Rückkopplung tatsächlich erfolgter Verbrauchsverlagerungen in das Bilanzkreissystem, ohne welche variable Tarife ohne Effekt bleiben würden.
- Der Lieferant benötigt für die Abrechnung je nach Abrechnungsverfahren entweder nur die kumulierten Messwerte je Tarifstufe (einfache Tarifmodelle, z.B. HT/NT), den vorberechneten Gesamtpreis (dynamische Tarife mit Tarifierung beim Kunden) oder die echten Messwerte in der dem jeweiligen Vertrag entsprechenden Auflösung (dynamische Tarife mit Tarifierung im Backend). Darüber hinaus benötigt der Lieferant zur Beschaffungssteuerung dieselben aggregierten Messwerte wie der Bilanzkreiskoordinator.

2.7.1 IKT-basierte Optimierung führt zu Effizienzsteigerung

Im Smart Grid wird zum Zwecke der nachfolgenden Sicherheitsbetrachtungen zwischen
- Verbrauchsoptimierung,
- Netzoptimierung und
- Messoptimierung

unterschieden.

Verbrauchsoptimierung setzt beim Endverbraucher an und kann durch direkte oder indirekte Beeinflussung des Verbraucherverhaltens geschehen.

Unter **Netzoptimierung** wird die bessere Nutzung der eingespeisten regenerativen Energie in einem Verteilnetz oder der energetisch sinnvolle Ausgleich zwischen zwei oder mehreren Verteilnetzen verstanden.

Unter **Messoptimierung** wird die optimale, zeitnahe und repräsentative Bereitstellung von Messdaten verstanden. Dies wird durch Smart Metering und weitere Schritte zur Datenaggregierung und -auswertung unterstützt.

2.7.2 Verbrauchsoptimierung

Bei der Verbrauchsoptimierung haben sich die Begriffe Demand Side Management (DSM) und Demand Response (DR) etabliert.

DSM setzt einen direkten Durchgriff auf die Infrastruktur des Industrie- oder Haushaltskunden voraus, um gezielt Energie verbrauchende Geräte an- oder abzuschalten, ohne dass dadurch dem Kunden Nachteile entstehen. Beispiele sind Kühlhäuser, in denen ein bestimmter Kühltemperaturkorridor nicht überschritten oder unterschritten werden darf, aber

der eigentliche Kühlvorgang durch Anspringen des Aggregats je nach verfügbarem Stromangebot gesteuert werden kann. Dies wird heute schon vereinzelt angewendet und kann als Muster für weitere Beispiele, auch im heutigen Haushaltskundenbereich oder besonders bei Ladevorgängen im zukünftigen E-Mobility-Markt, dienen. Allerdings sind viele Netzbetreiber aus Haftungsgründen zurückhaltend mit den direkten Schaltvorgängen auf der Kundenseite und setzen auf zeitnahe Tarifinformationen, die in Eigenregie des Kunden in dessen Infrastruktur bewertet und umgesetzt werden können. Diese Informationen sind ebenfalls sicherheitsrelevant, weil Manipulationen im Einzelfall und erst recht durch Mengeneffekt zu großen Schäden führen können. Demand Side Management wird dabei über die Controllable Local System (CLS)-Schnittstelle ermöglicht.

Demand Response ist die indirekte Beeinflussung des Kunden durch Anreize, insbesondere Preisanreize. Dabei kann der Kunde manuell oder durch entsprechende Infrastruktur automatisiert auf entsprechende Signale reagieren. Dabei liegt heute die wirtschaftliche Reihenfolge bei zuerst Industrie-, dann Gewerbe- und schließlich Haushaltskunden. Haushalte werden dabei energiepolitisch immer bedeutsamer. Mit dem Einzug von Smart Home Technologien, sogenannter Mikro Kraft-Wärme-Kopplung und Elektrofahrzeugen als Speicher und besonders flexible Verbraucher gehen Fachleute von bis zu 50% Lastverschiebungspotential im Niederspannungsbereich bei Haushaltskunden aus.[32]

Bei der Flexibilisierung der Tarife wird heute auf Mehrtarifzähler gesetzt, die unterschiedliche Saldi für die einzelnen Tarife im digitalen Zähler selbst führen. Zukünftig wird zur Ermöglichung vollständig dynamisierbarer Tarife zunehmend auch das Verfahren der Zählerstandsgangmessung zum Einsatz kommen, bei dem das Tarifierungsverfahren noch nicht abschließend geklärt ist. In jedem Fall handelt es sich bei der Tarifwahl des Endkunden jedoch um zunehmend dynamische und geldwerte Entscheidungen, die durch die Sicherheitsmechanismen des Gateway eines Smart Metering Systems (Smart-Meter-Gateway) selbst ebenso gut geschützt werden müssen, wie etwa ein Lieferantenwechsel.

Das Smart-Meter-Gateway bzw. eine Energie-Management-Funktion kann als Kommunikationskomponente für Demand Response und Demand Side Management eine wesentliche Rolle einnehmen.

2.7.3 Netzoptimierung

Eine Netzoptimierung kann auf elektrischem bzw. elektronischem Wege erfolgen.

Die IKT kann hierbei auf verschiedenen Ebenen, beispielsweise innerhalb eines Micro Grids oder im gesamten Smart Grid durch bessere Prognosemodelle auf Basis besserer Verbrauchs- und Einspeisedaten im Verteilnetz eine Optimierung bewirken. Dafür ist eine gesicherte Datenerfassung und –aggregation nötig.

2.7.4 Messoptimierung

Eine Messoptimierung, hier gemeint als zeitnahe Messung und Übertragung der Daten, ist ohne Smart-Meter-Gateway nicht denkbar. Dabei werden sowohl Daten zum Verbrauch als auch zur Erzeugung z.B. über Photovoltaik-Anlagen übertragen.

Dabei sollte man zwei Instanzen und ihre Begriffe genau differenzieren, die häufig als Smart-Meter-Gateway zusammengefasst werden:

1) Bei der Messdatenkommunikation handelt es sich um ein **Metering Gateway (MG)**, das den strengen Anforderungen des Common Criteria Protection Profiles entsprechen muss. Außerdem wird dem Endkunden (Verbraucher oder Erzeuger) nach §21h EnWG über das Gateway eine abgesicherte Einsicht in seine Daten gewährt. Um verschiedenen

Marktrollen (Lieferant, Verteilnetzbetreiber etc.) Daten in unterschiedlicher Ausprägung zu liefern, ist eine Abbildung von Mandantenfähigkeit, Datenschutz, Manipulationsschutz, Integrität und Authentizität notwendig. Zusätzlich ist ein sicherer Betrieb des Smart-Meter-Gateways durch den Messstellenbetreiber (MSB) zu realisieren.

2) Um Tarifinformationen zu empfangen und ggf. an ein Energiemanagementsystem zu senden sowie um erweiterte Zugriffe durch den Prosumer selbst zu ermöglichen (z.B. Sensorik bzw. Aktorik zur Fernabfrage) wird der Begriff des **Energie Management Gateway (EMG)** verwendet. Diese Komponente liegt in der Betriebsverantwortung des Endkunden. Die Kommunikation kann über die CLS-Schnittstelle abgebildet werden.

Es ist durchaus sinnvoll beide Komponenten zu verknüpfen, da das verpflichtend einzusetzende zertifizierte kryptografische Sicherheitsmodul des MG auch für die sicherheitskritischen Funktionen des EMG genutzt werden kann.

2.8 Stromnetze erfordern eine sichere IKT

Während im Bereich der Übertragungsnetze Informations- und Kommunikationstechnik (IKT) zur Steuerung der Stromflüsse bereits etabliert ist, wird IKT im Bereich der Verteilnetze kaum verwendet. Energie aus kleineren Solaranlagen oder Mikro-Kraft-Wärme-Kopplung (KWK) wird nicht optimal genutzt, weil digital unterstützte Steuerungsmöglichkeiten im Ortsnetz- und Niederspannungsbereich derzeit fehlen. Gerade dort wird aber heute schon und in Zukunft verstärkt erneuerbare Energie erzeugt und eingespeist. Gerade in dieser Domäne der heutigen dezentralen Verteilnetze müssen intelligent gesteuerte Energienetze, sogenannte Micro Grids entstehen.

Dies gilt jedoch auch für andere Domänen. Überall dort, wo in Primärnetzen elektrische Energie bereitsteht, müssen auch zukünftig Daten zur IKT-basierten Steuerung zuverlässig und sicher fließen.

Dies gilt auch für die Steuerung der Einspeisung. Beispielsweise müssen derzeit laut EEG Kraftwerks-Anlagen größer 100kW-Leistung ein Steuersignal erkennen. Künftig werden wohl auch kleinere Anlagen diese Anforderung berücksichtigen müssen. Dies bedeutet, dass alle wesentlichen Messstellen, Komponenten und Betriebsmittel, wie Mess-, Schutz- und Steuergeräte im heutigen Verteilnetz und an seinen Übergängen (Eintarif-/ Mehrtarifzähler, Zwei-Richtungs-Zähler, Maximumzähler, Rundsteuerung für Straßenbeleuchtung, Wandler, aktive Gleichrichter, u.v.m.) auch im Prinzip kommunikationstechnisch vernetzt sein müssen.

Dazu kommen in Zukunft auch neue Aspekte, wie z.B. die Integration der Ladestationen für Elektrofahrzeuge im Verteilnetz. Negative Auswirkungen auf die Netzsicherheit, Betriebssicherheit und letztendlich Versorgungssicherheit bei der Inbetriebnahme neuer Komponenten mit intelligenter IT-Steuerung müssen dabei auch verhindert werden.

"Breitband-Kommunikationsinfrastruktur zu allen Objekten, Anlagen, Geräten wird erforderlich. Verteilnetzbetreiber entwickeln sich zu Betreibern von Telkonetzen. Mit IKT vernetztes Energiesystem ist kritische Infrastruktur ….".[39]

Im Verantwortungsbereich der Stadtwerke München waren z.B. 2007 knapp 900.000 Entnahmestellen auf der Niederspannungsebene zu verzeichnen, die zukünftig informationstechnisch erreichbar und verwaltbar sein müssen.[40]

Ein sicherer Betrieb und das damit verbundene Lifecycle-Management erfordert allein bei der Menge integrierter Komponenten einen sehr hohen technischen und organisatorischen Aufwand.

2.8.1 IT Security als 'Business Enabler'

Dreh- und Angelpunkt für das Gelingen dieses Umbruchs in der Stromwirtschaft ist die Einhaltung von Sicherheitsanforderungen. Dazu zählen die Sicherheit vor Angriffen auf die IT-Infrastruktur ("Security") die Betriebssicherheit ("Safety"), aber auch die Datenschutzaspekte ("Privacy"). Denn mit dem zunehmenden Einsatz von Informations- und Kommunikationstechnologie bei Smart Grids steigt auch die Verwundbarkeit. Voraussetzung für Konzeption und sicheren Betrieb ist ein angemessen hohes IT Security Niveau, um beispielsweise Schutz vor

- Stromausfall,
- Manipulation der Tarifinformationen oder Zählerstände,
- Zahlungsausfällen aufgrund von fehlerhaften bzw. manipulierten Identitätszuweisungen,
- unberechtigter Abstreitbarkeit bei Rechnungsstellungen,
- Fehlsteuerungen des Stromflusses oder
- Missbrauch von Kunden- und Verbrauchsdaten

zu etablieren.

Die Stromversorgung gilt aufgrund ihrer Bedeutung und überlebensnotwendigen Funktion für Bevölkerung und Wirtschaft als kritische Infrastruktur. Die unverzichtbare Kernfunktionalität der Versorgungssysteme muss auch in Krisenlagen ("Graceful Degradation") aufrechterhalten und Mechanismen zur schnellstmöglichen Wiederherstellung nach Totalausfällen (Schwarzstartfähigkeit) vorhanden sein. Dazu ist es notwendig, die einzelnen Netz-Teilstrukturen sehr widerstandsfähig zu konzipieren und aufrechtzuerhalten.

2.8.2 Datenschutz vermeidet gläsernen Verbraucher

Mit der Einführung des Smart Grids werden große Mengen unterschiedlicher Energiedaten auf verschiedenen Aggregationsstufen erzeugt und übertragen. Das Schadpotential bzgl. personenbezogener Daten in einem nicht ausreichend gesicherten Smart Grid ist außerordentlich hoch.

Datenschutz muss deswegen – und auch wegen der hohen Sensibilität und des Misstrauens der Verbraucher – ausdrücklich eine hohe Priorität in der Konzeption und Umsetzung des Smart Grids haben. Vertrauliche Kommunikation zwischen Endkunden und ihren Dienstleistern sowie rechtssichere elektronische Transaktionsmechanismen müssen von vorneherein konzeptioniert und umgesetzt werden. Einmal aufgetretene Fehler und die daraus entstehende Ablehnung machen eine nachträgliche Implementierung unter Umständen nicht mehr möglich oder aufwändig und teuer. Erst eine klare und transparente gesetzliche Regelung von Zugriffsrechten und -beschränkungen sowohl für Daten aus Mess- und Verbrauchseinheiten als auch für den steuernden Zugriff auf Erzeuger und Verbraucher kann die notwendige Akzeptanz für diese neuen Technologien schaffen. In diesem Sinne ist IT Security eine Voraussetzung für den Aufbau und Betrieb eines von allen Beteiligten akzeptierten Smart Grids.

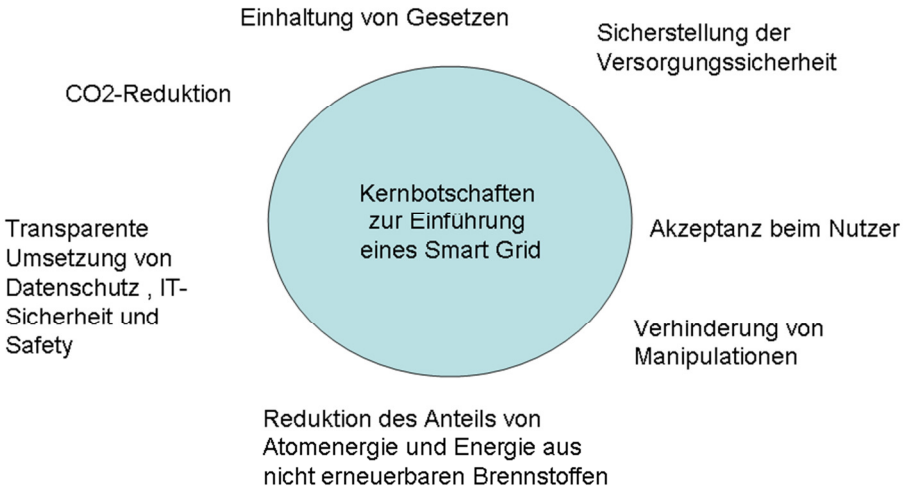
2.9 Akzeptanz braucht Vertrauen und Sicherheit

Jedes neue Thema oder Großprojekt erfordert, dass alle Beteiligten "mitgenommen" bzw. über Änderungen und deren Auswirkungen sachlich und neutral informiert werden. Innerhalb der Gesellschaft muss ein breiter Konsens über die Notwendigkeit zur Realisierung des neuen Projektes geschaffen werden. Dies gilt gerade nach den katastrophalen Auswirkungen von Fukushima.

Die Akzeptanz in der Bevölkerung steht und fällt mit der Sicherheit der Netze und auch dem Schutz der anfallenden Verbrauchsdaten. Erforderlich ist eine offene Kommunikation mit allen Beteiligten – und das bereits während der Konzeption und Errichtung des Smart Grids. Dabei müssen Chancen und auch Risiken aufgezeigt werden. Maßnahmen, die die Eintrittswahrscheinlichkeiten der Risiken reduzieren, sowie sich ergebende Restrisiken müssen dabei plausibel, transparent und verständlich dargestellt werden.

2.10 Kernbotschaften

Insbesondere folgende Kernbotschaften für die Einführung von Smart Grids sollten zusammen mit der Thematik IT-Sicherheit und Datenschutz berücksichtigt werden:



3 Weiterentwicklung des Stromnetzes zu sicheren Smart Grids

Die Entwicklung des heutigen Stromnetzes hin zum sicheren Stromnetz der Zukunft wird ein evolutionärer Prozess sein. Die heutigen sehr heterogenen Stromnetze werden nach und nach um neue intelligente Komponenten erweitert werden. Detaillierte Vorhersagen, welche Funktionen sich in welcher Ausprägung entwickeln werden, sind heute nur schwer möglich. Umso wichtiger ist es daher, bereits heute eine Vision des zukünftigen Smart Grids aus den bekannten Anforderungen abzuleiten. Ein maßgeblicher Faktor beim Design eines Smart Grid Modells muss daher aber die Flexibilität sein, um auf sich ändernde Rahmenbedingungen möglichst schnell und kostenneutral reagieren zu können. Die heute oder morgen eingebaute erste Generation von intelligenten Zählern (Smart-Metern) z.B. muss aus Kostengesichtspunkten weit länger als 10 Jahre im Einsatz bleiben und auch nach dieser Zeit noch die erforderliche Sicherheit gewährleisten. Würde man heutige Sicherheitstechnologien der Meter in Hardware implementieren, so wäre aufgrund der kurzen Halbwertzeiten in der IT ein Austausch vor Ablauf des geplanten Lebenszyklus bereits heute vorprogrammiert.

In einem zweiten Schritt muss das Smart Grid Modell mit den relevanten Playern entlang der Wertschöpfungskette des zukünftigen Smart Grid abgestimmt werden. Die bereits heute bekannten Abläufe und Prozesse müssen dabei möglichst generisch konzeptioniert werden, ohne dabei jedoch zukünftige Entwicklungen und Innovationen zu blockieren.

Darüber hinaus muss das Modell die verschiedenen Bereiche wie Prosumer, Smart Home, Smart Grid und alle darin geplanten und geforderten Rollen, wie z.B. Messstellenbetreiber beinhalten und deren Wechselwirkungen betrachten. Abbildung 2 zeigt neben diesen Rollen und Bereichen sowie deren Kommunikationsbeziehnungen untereinander, exemplarisch einige neue Services, die im zukünftigen Smart Grid Umfeld entstehen könnten.

Anhand eines solchen Modells können dann in einem dritten Schritt die kritischen Daten, Assets oder Abläufe in einem solch komplexen Gesamtszenario identifiziert und mögliche Angriffsmöglichkeiten untersucht werden. Danach können unter Kosten- und Funktionalitäts-Gesichtspunkten individuelle, dem Schutzbedarf angepasste, Sicherheitsfunktionen implementiert und Restrisiken adressiert werden.

Diese Restrisiken können den verantwortlichen Rollen dargestellt und evtl. durch zusätzliche Aufwände weiter minimiert oder akzeptiert werden. Dadurch ist sichergestellt, dass der jeweilig Verantwortliche die Entscheidung treffen kann, welches Risiko er eingehen möchte. So könnte z.B. ein Stromkunde entscheiden, welche Informationen er in welcher Detaillierung welchem Partner zur Verfügung stellen will, oder der Verteilnetzbetreiber könnte entscheiden, welche Risiken er bezüglich der Sicherheit und Stabilität seines Netzes eingehen will und welche nicht.

Erst mit all diesen Informationen kann eine Smart Grid IT-Architektur mit integrierter Informationssicherheit (Security by Design) mit Technologien und Best Practices geplant und implementiert werden.

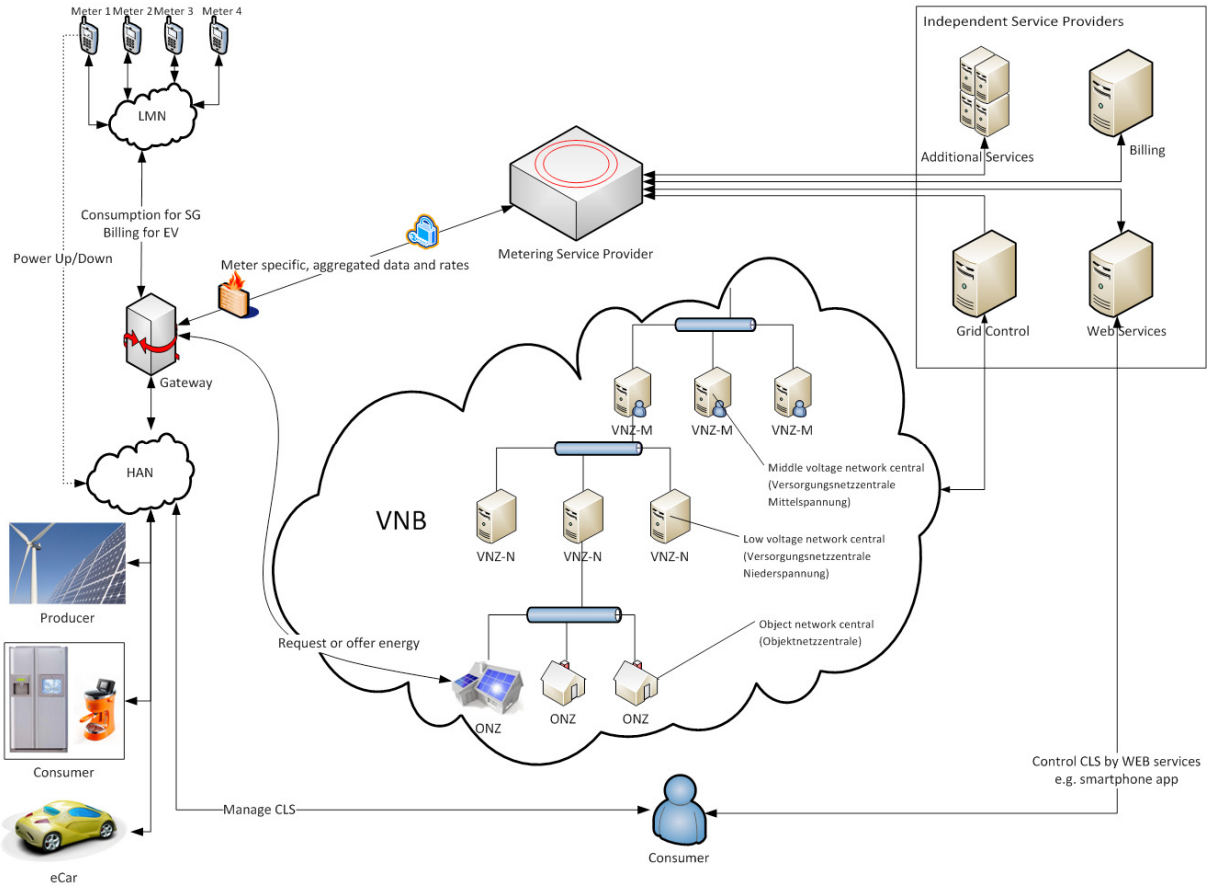


Abbildung 2: Exemplarisches Modell eines Smart Grids

3.1 Folgerungen aus der heutigen Situation

Die heutige deutsche Elektrizitätsinfrastruktur wird gerne mit dem Straßennetz verglichen: Die Autobahnen entsprechen dem Höchstspannungsnetz von 220 und 380 kV und verknüpfen Deutschland mit dem Ausland. Bundesstraßen entsprechen dem Hochspannungsnetz (>60 kV - 220 kV), Kreisstraßen dem Mittelspannungsnetz von größer 1 kV - 60 kV und die Orts- und Stadtverteilnetze (0,4 kV bis max. 1 kV) können analog zu kommunalen Straßen gesehen werden. Diese Verteilungsnetze versorgen Haushaltskunden, kleinere Gewerbekunden und Handwerker oder die Landwirtschaft mit Strom im Niederspannungsbereich.

In diesem Segment wird zunehmend regenerative Energie eingespeist, aber praktisch keine Digitaltechnik zur technischen Messung bzw. Steuerung und zur dezentralen Kommunikation von Marktteilnehmern eingesetzt. Die Verteilnetze stehen deshalb besonders im Fokus bei einer Umgestaltung der Stromversorgung.

Für eine "Energiesenke", z.B. im städtischen Bereich, reichen wenige Messpunkte und Messwerte, um den Netzzustand beurteilen zu können. Bei vielen Einspeisern ist dies aber nicht mehr der Fall. Bewegt sich dabei die Netzsituation in einem kritischen Bereich, z.B. wenn Wolkenbänder über Photovoltaikanlagen (PV) ziehen und damit sogar Ergänzungsenergie aus der Mittelspannungsebene erforderlich wird, so ist die zweifelsfreie Bewertung der Netzsituation auf Basis verlässlicher, nicht manipulierter Daten von entscheidender Bedeutung für die Versorgungssicherheit.

Das Spannungsmonitoring bzw. das Spannungsbandmanagement auf Basis der vorgegebenen Grenzwerte für die Nennspannung (230V +/- 10%) bestimmt in diesem Bereich den Kommunikationsbedarf und nicht asynchrone Datenübermittlung aus dem Mete-

ring. Vorgegeben durch die Belastbarkeit der Kabel ist die sichere Kommunikation Basis für ein Lastflussmanagement zum Schutz der Netzinfrastruktur.

Eine besondere Differenzierung stellen Micro Grids dar. Diese Micro Grids können dabei auf Technologie-Ebene oder aber auch auf Anwendungsbereiche abgebildet werden. Dazu zählen z.B. der 110/20 kV-Einspeisebereich eines Leistungstransformators mit 110 kV Freiluftschaltanlage und 20 kV-Innenraumschaltanlage.

Die Zusammenschaltung der Micro Grids ermöglicht eine bessere Lastflussoptimierung im gesamten Smart Grid und damit ein effizienteres Zusammenschalten von Erzeugern und Verbrauchern. Dabei speisen größere Windkraftwerke, großflächige Photovoltaikfelder etc., die als virtuelle Kraftwerke bezeichnet werden [41], in Netze der Mittelspannungsebene ein, müssen aber zur effektiveren Nutzung ggf. in anderen geografischen Regionen über Hochspannungsnetze in weitere Micro Grids der Mittelspannungsebenen transportiert werden, in denen ein Bedarf an Energie besteht. Bei virtuellen Kraftwerken ist ein vertrauenswürdiges verteiltes Steuerungssystem abzubilden, was eine neue Herausforderung im Bezug auf sichere Zusammenschaltung von geografisch getrennten Mess- und Steuerungskomponenten darstellt.

Die dezentrale Erzeugung, Übertragung und Nutzung regenerativer Energie ist bekanntlich jedoch aufgrund der starken Erzeugungsschwankungen bislang nur sehr schwer plan- und steuerbar. Es dominiert derzeit noch die zentrale Erzeugung nach Bedarf im Einbahnstraßensystem. Um einen dynamischen Ausgleich zwischen (dezentraler) Erzeugung und Bedarf zu schaffen, ist zukünftig auch ein wechselseitiger Energie- und Nachrichtenfluss zu ermöglichen. Die bisherige konventionelle Netzleittechnik stößt derzeit an ihre Grenzen. Die heutigen Einbahnstraßen ohne Infrastrukturkonzept für den Gegenverkehr freizugeben, würde mehr Probleme schaffen als diese zu lösen, d.h. ein Ausbau der Netze alleine löst diese Probleme nicht. Ein innovativer Umbau der Stromnetze und ihrer Sekundärtechnik ist zwingend erforderlich: Mit den Smart Grids (Intelligentes Stromnetz) und der nötigen verlässlichen Datenbasis wird die Grundlage für eine optimierte Nutzung der Stromnetze geschaffen. Z.B. mit der Elektromobilität kommt ein erheblicher, weiterer Faktor dazu. In Verbindung mit PV-Anlagen können Strom-, Lastfluss- und Schutzprobleme für die Verteilnetzinfrastruktur im Prinzip von Haus zu Haus zwischen Überspannung durch Erzeugung und Unterspannung durch e-Mobility bedingte Spitzenlast schwanken.

Kommunikationsfähige Komponenten wie beispielsweise Smart Meter (digitaler Stromzähler), Messstellen- bzw. Aggregationssysteme, aber auch elektrische Schaltungskomponenten, die mit ausreichendem zeitlichen Puffer beispielsweise über Internetprotokolle wie TCP/IP miteinander kommunizieren, machen digitale Kommunikation zwischen aktiven Komponenten im Netz zunehmend technisch möglich.

Dabei werden sich Smart Grids auch der Technologie und des Know-Hows bedienen, das seit Jahren in der existierenden Informations- und Kommunikationstechnologie zur Verfügung steht. Dies gilt vor allem für die Schnittstellen zwischen allen Marktakteuren, bei denen Marktdaten ausgetauscht werden. Sehr kurze Reaktionszeiten im Millisekundenbereich werden hierfür normalerweise nicht benötigt. Der Teil des "Internet der Energie" wird durch Commercial Information Technology (CIT) ermöglicht.

Die Process Information Technology (PIT) erlaubt auch Realtime- oder Neartime-Prozesse zur Steuerung technischer Komponenten. Die PIT ist notwendig, um sehr kurzfristige Schaltungen in Energienetzen realisieren zu können.

Es ergeben sich sowohl im CIT als auch im PIT hohe Anforderungen an die IT-Sicherheit, welche jedoch durch unterschiedliche technologische Maßnahmen abgebildet werden müssen.

CIT kann dabei zum großen Teilen durch IT-Sicherheitsmaßnahmen, die aus der allgemeinen Internet-Sicherheit bekannt sind, zurückgreifen. Zusätzlich sind jedoch im Bereich der PIT weitere neue und Energiebranchen-spezifische Sicherheits-Technologien und sichere Prozesse zu entwickeln und zu etablieren.

Von besonderer Bedeutung sind die gleichermaßen sicheren und wirtschaftlichen Betriebsprozesse. Das BSI-Schutzprofil (Common Criteria Protection Profile, CC PP) und die korrespondierende technische Richtlinie TR 03109 sehen modernste kryptographische Methoden für einen Multimandantenbetrieb vor.

Die Autoren nehmen hier an, dass wesentliche technische Funktionen, die für die Zertifizierung nach CC PP und TR 03109 vorgesehen sein müssen, auch in den rechtlichen Vorgaben Anwendung finden werden, die die Marktrollen und damit in der Konsequenz die resultierenden Betriebsprozesse betreffen.

Hier darf die notwendige Informationssicherheit bei allen sicherheitsrelevanten Betriebs
prozessen nicht zu extremen Kosten führen. Schließlich müssen diese Kosten vom Verbraucher mitgetragen werden. Diese Betriebskosten können entstehen

1) durch normale Vorgänge, wie Umzug, Lieferantenwechsel, Änderungen im Messbetrieb, etc.
2) Wenn der Endkunde in längeren Abständen Daten einsehen will, so können schon ein vergessenes Passwort und der nötige Password-Reset bei Millionen Systemen im Feld einen erheblichen Kostenblock darstellen.
3) Weiterhin kommen allgemeine Faktoren, wie Zertifikatslaufzeit, Eichfristen usw. hinzu.
   Die regulativen Möglichkeiten, die sich aus den Sicherheitsmechanismen von CC PP und TR03109 ergeben, muss die Politik sehr sorgfältig einsetzen. Je nach gesetzlicher Vorgabe können das Verhältnis von Anschaffungskosten zu Betriebskosten zwischen minimal ca. 1 : 3 bis maximal ca. 1 : 7 oder gar mehr angesetzt werden.

Die ersten Schritte in Richtung Smart Grid sind eng verbunden mit der gesetzlichen Entflechtung der Marktrollen durch das Energiewirtschaftsrecht und mit den sich daraus ergebenden Kommunikationsprozessen. Die damit verbundenen Sicherheitsaufgaben sind branchentypisch und damit eine eigene Kategorie von Anforderungen im Smart Grid. Die jeweilige Marktrolle muss sich authentisieren, darf nur Daten bekommen, die der Rolle zustehen und diese müssen vertraulich behandelt werden. Sicherheitsrelevante Use Cases, die immer dann entstehen, wenn betriebswirtschaftliche (z.B. Lieferantenwechsel) oder technische (z.B. Zertifikatswechsel bei einer Marktrolle, Passwort-Reset bei Endkunden) Änderungen erfolgen müssen, müssen in sicheren Betriebsprozessen dokumentiert werden. Dazu kommt noch eine lange Migrationsphase, während der sich der Datenaustausch im liberalisierten Energiemarkt parallel an alten und neuen Marktprozessen und -schnittstellen orientieren muss.

Heute wird die Marktkommunikation im liberalisierten Strommarkt mittels 5 EDIFACT-Nachrichtentypen gewährleistet:

1. Einmalige Stammdatenübertragung beim Lieferantenwechsel (UTILMD)
2. Regelmäßige Zähldatenübertragung an den Lieferanten (MSCONS)
3. Netznutzungsrechnungen (INVOIC) und

4. Zahlungsavise (REMADV) sowie
5. Fahrpläne (DELFOR).

Die Sicherheitsrahmenbedingungen der Marktkommunikation sind im VEDIS-Projekt des BDEW erarbeitet worden. Diese wurden von der BNetzA in einer Verordnung für den elektronischen Datenaustausch in der deutschen Energiewirtschaft als verbindliche Grundlage genannt (Aktenzeichen: BK7-07-067) und definieren somit das heutige Sicherheitsniveau.

3.2 Spezielle Risiken für die Informationssicherheit im Smart Grid

Den traditionellen physischen Risiken des klassischen Energieumfelds muss weiterhin eine hohe Priorität zugewiesen werden. Durch die Einführung von IKT, die erhöhte Komplexität und einer Vielzahl von Schnittstellen entstehen neue Sicherheitsrisiken für Angriffe im und auf das Energienetz und spezielle Internetrisiken rücken vermehrt in den Vordergrund. Die als gesetzt aufzufassende Internetinfrastruktur birgt eine Fülle von Risiken für die Informationssicherheit im Smart Grid und damit auch für die Versorgungssicherheit. Die allgemeinen Internet-Risiken sollen im nächsten Kapitel angesprochen werden. Dabei soll das "Internet der Energie" nicht unbedingt mit dem Internet gleichgesetzt werden. Hier müssen sich die genauen Querverbindungen noch erweisen. Insofern können Risiken im "Internet der Energie" durchaus branchenspezifisch sein, können aber mit den heutigen Methoden nach dem Stand der Technik behandelt werden. An dieser Stelle sollen besonders die Smart Grid-spezifischen IT-Sicherheit-bezogenen Risiken adressiert werden. Dabei werden besonders die engen Abhängigkeiten und Einflüsse auf die Verfügbarkeit des primären Stromnetzes betrachtet. Das primäre Stromnetz stellt eine kritische Infrastruktur dar, welches gegebenenfalls durch einen bewussten oder unbewussten "falschen Mausklick" gefährdet ist.

In dieser kritischen Infrastruktur sind deshalb die Schutzziele, wie Verfügbarkeit des Netzes und der Daten, Integrität der Daten (Unverfälschtheit des Inhaltes), Authentizität des Absenders insbesondere bei steuerungsrelevanten Daten und Kommandos (Echtheit der Herkunft) und Verfügbarkeit (der Daten als Entscheidungsgrundlage und der IKT-Infrastruktur als steuerungsrelevante Instanz) besonders wichtig. Ebenso ist die Vertraulichkeit ein weiteres Schutzziel, welches u.a. aus datenschutzrechtlichen Gründen sichergestellt werden muss, damit System- und Verbrauchsdaten vor dem Zugriff durch Dritte geschützt sind.

3.2.1 Bewusst und unbewusst verursachte Schädigung

Bei der Verursachung von Schäden kann man zunächst zwischen bewussten, also fahrlässigen, mutwilligen oder gar kriminellen Eingriffen Unbefugter in die IKT-Infrastruktur und unbewusstem Fehlsteuerungen unterscheiden.

Bewusste Manipulationen entstehen z.B. durch Hacking. Die Auswirkung der Manipulation kann dabei unterschiedlich sein: Einerseits kann die unberechtigte Übernahme von Steuerungsfunktionen Auswirkungen auf die Primärtechnik haben, andererseits können Manipulationen z.B. von abrechnungsrelevanten Daten erfolgen, um sich finanzielle Vorteile zu verschaffen oder mutwillig Messdaten zu verfälschen, um Störungen der Netzstabilität herbeizuführen.

3.2.2 Auswirkungen auf Safety und Security

Bisher wurden vordringlich Probleme bei der Funktionssicherheit ("Safety") im Kontext von Energieerzeugung, Energietransport und Energienutzung gesehen. Jetzt kommen Sicherheitsaspekte durch die Vernetzung und die verteilten Systeme bei der digitalen Informationsverarbeitung ("Security") hinzu. Branchenspezifische Sicherheitsanforderungen im Smart Grid gehen teilweise weit über Risiken aus der heute bekannten Internetwelt hinaus. Stromtransport gehört im doppelten Sinne zu kritischen Infrastrukturen. Einerseits ist er Grundvoraussetzung für viele wichtige kritische Lebensbereiche, wie Finanzwesen oder

Telekommunikation. Andererseits sind hier unter Sicherheit nicht nur virtuelle Schäden, sondern auch reale Schäden an Anlagen mit möglichen Auswirkungen zu verstehen, die geldwerte Implikationen übersteigen. IKT-basierte unerwünschte oder kriminelle Manipulationen können möglicherweise gesundheitsgefährdende Situationen erzeugen. Entsprechende Risiken, die bei der IT-Sicherheit beginnen können, aber nicht nur Grundwerte aus der Informationssicherheit, wie Vertraulichkeit, Integrität und Verfügbarkeit (von Daten), berühren, sondern notwendige Schutzfunktionen mit Auswirkung auf Gesundheit und Wohlergehen betreffen, sind entsprechend hoch zu bewerten.

3.2.3 Chancen und Risiken von Demand Response

Mit Smart Grid in Verbindung mit Demand Response soll der Verbraucherwille durch Lastverschiebung so einbezogen werden, dass dynamisch zur Verfügung stehende Energieangebote effizient ausgenutzt werden. Dazu stehen bereits heute an Smart Metern unterschiedliche Tarifwahlmöglichkeiten zur Verfügung. Der Gesetzgeber will diese Tarifwahl forcieren und geht dabei in ähnlicher Weise vor, wie bei der Liberalisierung des Telekommunikationsmarktes.

Korrekt am Smart Market prognostizierte bzw. kalkulierte und auf das Lastmanagement im Smart Grid abgestimmte Tarife sind Voraussetzung für eine optimierte, gewünschte Verbrauchersteuerung ohne negative Auswirkungen auf die Wirkleistung. Wenn aber durch fehlerhafte Algorithmen oder Prognosedaten bzw. falsche Grundannahmen zur Laststeuerung fehlerhafte Tarife im Markt existieren und dadurch ein "Schwarmverhalten" hervorgerufen werden bzw. nicht mehr kontrollierbare Masseneffekte entstehen, so kann dies äußerst dramatische Folgen haben.

Dies kann im Extremfall sogar Schäden an Leib und Leben zur Folge haben ("Safety"-Aspekte). Hier muss ggf. im Interesse der Allgemeinheit und eines Funktionieren des Smart Grids korrigierend eingegriffen werden. Smart Market und Smart Grid sind somit nicht voneinander unabhängig.

Regulierende Eingriffe am Smart Market sind somit erforderlich.

3.3 Möglichkeiten und Grenzen der IKT

Eine steuernde Rolle, die aufgrund einer wechselnden Datenbasis wissensbasiert Entscheidungen treffen muss, kann die IKT dort nicht wahrnehmen, wo im Millisekundenbereich reagiert werden muss (siehe auch 4.1.). Es haben sich deshalb die Begriffe CIT und PIT gebildet. Bei PIT enden auch z.B. in der Regel die Securitymöglichkeiten der IKT im Smart Grid, wenn es darum geht, mit rechenintensiven kryptografischen Methoden Daten abzusichern. Selbst Challenge-Response-Verfahren, also Kryptografie ohne Einsatz von Hash-Algorithmen, sind im Millisekundenbereich nicht einsetzbar. Dies gilt erst recht für elektronische Signaturen und Verschlüsselung.

Der Einsatz von mit starker Kryptografie gesicherter IKT muss also im Wesentlichen vorerst und mit bisherigen Lösungen auf den kommerziellen Bereich des Smart Grid (CIT) beschränkt bleiben. Abgesichert werden zudem alle Wide Area Verbindungen, insbesondere über IP. Dazu gehören alle Transaktionen vom Messstellenbetrieb an Marktrollen zu Zwecken der Abrechnung, Prognose und Zustandsbeurteilung auf individueller Basis. Weiterhin müssen, wie oben über Demand Response gesagt, Informationskanäle zuverlässig sein, mit denen bei Kunden ihr Verbrauchsverhalten direkt oder indirekt beeinflusst werden kann.

Messdatenübertragung:

Daten müssen zu bestimmten Marktrollen übertragen werden, um Prognoseprozesse, Wartung/Eichung und/oder Abrechnungsprozesse mit der nötigen Datenbasis zu versorgen.

Informations-, Berechnungs- und Gutschriftenwesen nimmt E-Business-Charakter in einem Marktplatz der Energie an.

DSM- und DR-Nachrichtenübertragung:
Auf dem gleichen physikalischen Weg kann der Endkunde und seine energetischen Systeme direkt oder indirekt adressiert werden.

Sekundärsteuerungsdatenübertragung:
Gleichzeitig dienen aufbereitete Messdaten wiederum zur Steuerung der Prozesse, wo allein elektrisch oder auch elektronisch unterstützte Steuerung der Primärnetze nicht ausreicht, um eine optimale Ausnützung der zur Verfügung stehenden regenerativen Energie zu ermöglichen. Statusinterpretationen müssen dabei letztlich Auswirkungen generieren, die einerseits über die Verteilnetze hinausgehen und Erzeugung und Transmission beeinflussen und andererseits auch wiederum bedingt dem Endkunden zur Verfügung stehen, um sein Verhalten einbeziehen zu können.

Allerdings kann auch eine sehr hohe Qualität und eine sehr hohe Menge an intelligenten Messstellen keinesfalls eine sekundengenaue Spiegelung des Netzzustands liefern. Auf keinen Fall sollte angenommen werden, dass umfassend und zeitnah Metering-Daten zur unmittelbaren Netzsteuerung eingesetzt werden können. Dies fällt eindeutig in den PIT-Bereich. Deutliche Verbesserung können durch zeitnahe Daten aber für die Prognose erzielt werden.

Metering-Daten für One-Day-Ahead Prognosen und Steuerungsanpassung sind gegenüber heute ein erheblicher Fortschritt. Repräsentative Teilmengen aus den Metering-Daten können mittelfristig auch Intra-Day Prognosen unterstützen. Schon die tagesversetzte Verbesserung der Prognosen hilft unter volkswirtschaftlichen und betriebswirtschaftlichen Gesichtspunkten enorm. Dadurch müssen weniger Energiereserven, wie sie heute durch die Bundesnetzagentur reglementiert und als Tarife an der Leipziger Börse gehandelt werden, vorgehalten werden. Die CIT-Informationen sind dabei wegen ihrer Konsequenzen für die Wirtschaftlichkeit und Versorgungssicherheit schützenswert.

3.4 Marktrollen und sichere Betriebsprozesse

Zukünftig überträgt das IKT-Gateway Daten gemäß voreingestellter Parameter und Sicherheitskriterien an die jeweilige Marktrolle selbst. Dabei sind mehrere Mandanten zu berücksichtigen.

1) Messstellenbetreiber
Verantwortlich für den ordnungsgemäßen Betrieb der Messstelle und des Gateways inkl. Eichung der angeschlossenen Zähler ist der Messstellenbetreiber (MSB). Im Sinne des Common Criteria Protection Profiles ist er der "Vertrauenswürdige Administrator" des IKT-Gateways. Diese Rolle benötigt zumindest Zustandsinformationen im laufenden Betrieb. Wesentlich ist jedoch die Inbetriebnahme, Personalisierung, Authentisierung der weiteren Marktrollen und ggf. die einsatzspezifische Parametrisierung. Damit sind wichtige kryptografische Sicherheitsfunktionen verbunden, weil die Kommunikation mit weiteren Marktrollen aus dem Gateway heraus PKI-basiert erfolgen muss. Diese Personalisierungs- und Initialisierungsprozesse sind deshalb genau zu planen und zu beschreiben, weil sowohl die Sicherheit als auch der reibungslose Betrieb von gegenwärtig allein 42 Millionen Stromzählern an zukünftig ca. 30 Millionen IKT-Gateways unter sicherheitstechnischen und wirtschaftlichen Gesichtspunkten eine erhebliche volkswirtschaftliche Herausforderung darstellt. MSCONS-Nachrichten und Direktübermittlung werden über Jahre parallel erfolgen. Bei jeder einzelnen Messstelle wird die Neuinstallation eines IKT-Gateways mit nachgelagerter

Zählerinfrastruktur, z.B. im Rahmen von Eichzyklen, unter Betriebs- und Sicherheitsgesichtspunkten zwischen den Marktrollen neu zu organisieren sein.

2) Lieferant
Der Lieferant benötigt die mittels privatem Schlüssel des Gateways signierten und mittels öffentlichem Schlüssel des Lieferanten verschlüsselten Zähldaten zur Abrechnung mit dem Endkunden.

3 Verteilnetzbetreiber (VNB)
Der Verteilnetzbetreiber ist einerseits an den individuellen, aber kumulierten Zähldaten des Endkunden interessiert, weil er gegenüber dem Lieferanten die Netznutzungsrechnung stellen muss. Andererseits können repräsentative anonymisierte Daten ihn in seiner Prognose für die Energiebereitstellung unterstützen. Zusätzlich muss er selbst eine Sensorik etablieren, welche unabhängig von Messsystemen auf Seite der Verbraucher Daten im Netz aufnimmt.

4) Übertragungsnetzbetreiber (ÜNB)
Übertragungsnetzbetreiber betreiben als Dienstleister die Infrastruktur der überregionalen Stromnetze. Das betriebene Netz ist dabei ein Hochspannungsnetz zum Transport elektrischer Energie über weite Entfernungen und kann durch verschiedene Marktrollen diskriminierungsfrei genutzt werden. Durch aggregierte Daten der einzelnen Verteilnetze wird die Steuerung der Lasten in den Übertragungsnetzen vorgenommen, während für die im liberalisierten Energiemarkt zwingend erforderlich Bilanzierung jeweils über alle relevanten Kunden eines Lieferanten aggregierte Messwerte benötigt werden.

5) Prosumer
Der Endkunde als Verbraucher und ggf. Betreiber von Kleinstkraftwerken (Produzent) ist ebenfalls als Rolle zu berücksichtigen. Hierbei sind verschiedene Arten von Verbrauchern, wie Privathaushalte, gewerblicher Kunde und Industrieunternehmen zu unterscheiden.

Der Endkunde hat immer das Recht, seine Verbrauchsdaten einsehen und seinen Tarif auswählen zu können (Dateneinsicht nach §21 h EnWG). Dazu muss er sich gegenüber dem System authentisieren. In einem Wohnblock können mehrere Mietparteien sich für unterschiedliche Lieferanten und Tarife entscheiden. Dadurch entstehen entsprechend viele zu verwaltende Parametersätze mit sicherheitsrelevanten Änderungsprozessen. Schon alleine die Tatsache, dass ein Reset der Authentisierungsinformationen durch den MSB vorgesehen werden muss, stellt eine erhebliche Anforderung dar. Durch die zunehmend freier zu gestaltende Tarifwahl und durch Entwicklungen bei Controllable Local Systems (CLS) sind schützenswerte Prozesse erkennbar, die heute noch nicht berücksichtigt wurden. Mehrtarifzähler können mittelfristig nicht die Lösung sein, um die berechtigten Interessen der betroffenen Marktrollen (Prosumer, Lieferant, VNB, MSB) wirtschaftlich und sicher abzubilden. Es ist wegen Sicherheit und Verbindlichkeit, aber auch gerade unter Kosten/Nutzen-Gesichtspunkten von zentraler Bedeutung, dass die neu entstehende Sicherheitsinfrastruktur für alle Aspekte zur Verfügung steht. Dazu gehören neben dem Smart Metering das Energieeffizienzmanagement, Controllable Local Systems und die Statusüberwachung und ggfs. Steuerung ("Strangkontrolle"). Daran ist besonders der Prosumer interessiert, weil er Mehrfachkosten für die Sicherheit nicht akzeptieren wird. Suboptimaler Einsatz der Sicherheitsmaßnahmen ist betriebswirtschaftlich und volkswirtschaftlich nicht sinnvoll und wird erheblichen politischen Widerstand erzeugen. Mit diesem Anteil am Strompreis muss verantwortungsbewusst umgegangen werden.

6) Aggregator
Die Aggregation von Daten zur Steuerung des Lastflussausgleiches im Smart Grid muss durch vertrauenswürdige, unabhängige und neutrale bzw. diskriminierungsfreie Institutionen erfolgen. Diese Instanzen werden auch als sogenannte "Datendrehscheiben" [34] bezeichnet. Ob dies eine oder mehrere Instanzen sind, muss diskutiert werden. Der Aggregator bietet eine Aufbereitung von Daten aus verschiedenen Quellen, wie z.B. Messsystem-Daten, aus der Vergangenheit aufbereitete Profildaten, meteorologische Daten und ermittelt daraus ggfs. Prognosen, die zur Steuerung bzw. zur Ableitung von dynamischen Tarifen genutzt werden können.

7) Marktplatz
Am Marktplatz werden Tarife unterschiedlicher Lieferanten angeboten, die über das Smart-Meter-Gateway an den Endverbraucher oder aber auch an das Endgerät (z.B. E-Mobil) übermittelt werden.

8) Weitere Rollen
Insbesondere unter Servicegesichtspunkten steht es einzelnen Marktrollen frei, nach Modellen zu suchen, die die Betriebskosten senken. Hier werden weitere Sicherheitsanforderungen beim Fieldservice, beim IT-Netzbetrieb, bei Managed Services oder Cloud-Services entstehen.

Jede Rolle muss sich zu jedem Zeitpunkt korrekt authentisieren. Verbunden mit denkbaren Use Cases wie Austausch, Umzug, Lieferantenwechsel, Rückbau etc. entstehen Anforderungen an den jederzeit sicheren Betrieb. Sie stellen eine eigenständige Klasse an Sicherheitsanforderungen dar, die durch die Sicherheitsanalyse von weiteren Bedrohungen, wie man sie aus der Internetsicherheit kennt (z.B. Netzwerksicherheit, Denial-of-Service, etc.) ergänzt werden muss.

3.5 Sicherer Betrieb auf Basis existierender und neuer Standards

Das Smart Grid im Sinne einer intelligenten Bewertung und Steuerung aller Netzzustände, basierend auf einer ausreichend guten und zeitnahen Datenbasis, muss gravierende Risiken möglichst ausschließen und mit allen Restrisiken so umgehen, dass Gefahr für Leib und Leben ausgeschlossen wird und die Verfügbarkeit der kritischen Infrastruktur Energieversorgung gewährleistet bleibt. Dies muss auch für jede Verkettung unglücklicher Umstände gelten, wo menschliches Fehlverhalten, technische Defekte oder Unzulänglichkeiten und höhere Gewalt zusammen wirken können.

Im Jahr 2007 lag der durchschnittliche Stromausfall in Deutschland bei 19,25 Minuten (zum Vergleich mit den europäischen Nachbarn: Niederlande 33,1 Minuten, Österreich 45,47 Minuten). [42] Dies sollte mindestens so bleiben. Allerdings muss für das Smart Grid anders priorisiert werden, denn es sollte eine optimale und nicht eine maximale Netzkapazität im Vordergrund stehen. Dieser Paradigmenwechsel spiegelt sich auch im Mandat M/490 EU der EU-Kommision an die europäischen Normungsorganisationen wieder.

Es hat sich dabei herausgestellt, dass die sicheren Betriebsprozesse sich durchaus am weltweit akzeptierten Standard ISO/IEC 27000 orientieren können. Die konkrete Ausgestaltung in der Energiewirtschaft bedarf jedoch einiger branchenspezifischer Anpassungen. So können die Prinzipien aus ISO 27001 für das Informationssicherheitsmanagementsystem (ISMS) übernommen werden. Gleiches gilt für die Maßnahmenkataloge nach ISO 27002, die zur Umsetzung der Kontrollziele im Bereich Organisation, Prozesse, Betrieb und (im übertragenden Sinne) Technik dienen.

Für die Schutz- und Leittechnik von elektrischen Schaltanlagen der Mittel- und Hochspannungstechnik enthält die internationale Norm IEC 61850 bzw. die Norm DIN EN 61850 ein standardisiertes Übertragungsprotokoll. Dabei werden u. a. auch die IT-Schnittstellen für die Überwachung und die Steuerung von Schaltanlagen definiert.

Es müssen die Regelmechanismen angepasst werden, die die SCADA-Systeme bzw. die Prozessdatenverarbeitung (PDV) betreffen. Die PDV ist gekennzeichnet durch die lange Laufzeit der Systeme, die hohen Verfügbarkeitsanforderungen, sowie den hohen Funktions- und Installationstestaufwand. PDV-Systeme im EVU-Umfeld gehorchen dabei z.T. eigenen Gestaltungsprinzipien, wie die Differenzierung nach PIT und CIT in Abschnitt 3.1.1 bereits gezeigt hat. Sie gehen an diesen Stellen über Anforderungen in der "klassischen Büro-Datenverarbeitung" hinaus und sind vergleichbar mit speziellen, zusätzlichen Sicherheitsanforderungen in der Telefonie oder Notfall-Leitstellen (Feuerwehr, Polizei, Notarzt).

Mögliche Fehlsteuerungen, das Fehlen von Daten bzw. das Vorhandensein von fehlerhaften Daten oder gravierende menschliche Fehlentscheidungen können KRITIS-relevante Auswirkungen hervorrufen und müssen sowohl durch das Systemdesign als auch durch die flankierenden Betriebsprozesse verhindert werden. Ein Notfallkonzept zur sicheren Betriebsführung ist deshalb für alle Marktrollen und deren Funktionalitäten erforderlich. Das BDEW-Whitepaper mit Anforderungen und Ausführungshinweisen [45] kann dabei eine erste Grundlage darstellen. Das Whitepaper legt dabei den gesamten Lifecycle eines bisherigen Leitsystems inkl. aller Subsysteme zugrunde. Diese Normungsaspekte liegen auch als Norm-Entwurf E DIN 27009 vor (Stand: 2012-04).

3.6 Domänen innerhalb des Smart Grid

Das Smart Grid als Ganzes kann in unterschiedliche logisch in einzelne Sektoren (Domänen bzw. Handlungsfelder) aufgeteilt werden. Dabei kann eine Einteilung beispielsweise aus den unterschiedlichen Funktionen bzw. Geschäftsprozessen erfolgen.

Es lassen sich beispielsweise folgende Domänen / Handlungsfelder abbilden:
- Smart Metering
- Messstellenbetrieb und –dienstleistung
- Aggregationsdienstleister
- Energieberatung/-steuerung via Controllable Local System (CLS)
- Marktplatz
- Verteilnetz
- Übertragungsnetz/Bilanzierung
- Service
- Groß-Erzeugung.

Jede Domäne fordert einen definierten Schutzbedarf, der sich vom Schutzbedarf einer anderen Domäne unterscheiden kann. Dies resultiert daraus, dass Risiken und Auswirkungen der Bedrohungen unterschiedlich bewertet werden.

Deshalb bietet sich an, dass die unterschiedlichen Domänen mit ihren spezifischen Schnittstellen zu anderen Domänen jeweils als ein Untersuchungsfeld zu betrachten und speziell hinsichtlich des unterschiedlichen Schutzbedarfes gegebenenfalls einzeln zu bewerten.

3.7 Zwischenergebnis: Prinzipielle branchenspezifische Sicherheitsanforderungen

An dieser Stelle können als Zwischenergebnis folgende Sicherheitsforderungen an die IKT von spezifischen Verfügbarkeitsanforderungen für die Energieversorgung abgeleitet werden. Sie sind weitgehend unabhängig von allgemeinen Sicherheits- und Risikobetrachtun-

gen aus der IT- und Internetsicherheit zu betrachten und somit branchentypisch. Sie müssen als technische Anforderung und organisatorisch ausgestaltete Betriebsprozesse angemessen und sorgfältig analysiert und als Grundlage weiterer Maßnahmen dokumentiert werden. Die IT-Sicherheits-Aspekte kommen hinzu, sind aber in der einschlägigen Fachliteratur an vielen Stellen schon umfassend beschrieben.

1. Getrennte einzelne Bewertung der IT-Sicherheit von Smart Market und Prozessleittechnik mit anschließender Bewertung der jeweiligen Abhängigkeiten

2. Sichere Betriebsprozesse bei der Initialisierung und Personalisierung der IKT-Gateways durch den Messstellenbetreiber, sowie mandantenfähige Kommunikation mit den betroffenen Marktrollen unter Berücksichtigung von Konfigurationsänderungen durch verschiedene Use Cases

3. Schutz von personenbezogenen Daten, die Rückschlüsse auf das energetische Verhalten oder die energetische Infrastruktur des Endverbrauchers erlauben

4. Schutz vor Angriffen Dritter beispielsweise über Malware oder andere bewusste Einflussnahmen

5. Schutz vor Datenmanipulation zum Zwecke, wirtschaftliche oder technische Schäden zu verursachen (Korrektur unplausibler Werte aus Messfehlern muss nachvollziehbar und – u.a. auch eichrechtlich – zulässig sein)

6. Schutz vor bewusster oder unbewusster unautorisierter Manipulation der IKT durch interne Verfahrensteilnehmer mittels zweifelsfreier Identifizierung und Authentifizierung am System im Rahmen eines Rollen-, Rechte- und Zugriffsmanagements

7. Schutz vor unkontrollierten stochastischen Effekten in der Automatisierung der Machine-to-Machine Kommunikation zum Zwecke der Netzsteuerung oder im automatisierten Handel mit Energie auf dem "Smart Market" (belastbares Algorithmenverhalten) bzw. Schutz vor "Dominoeffekten" durch massenhaftes, gleichgeschaltetes Handeln von Endverbrauchern

8. Schutz vor negativen Auswirkungen, die durch Verkettung unglücklicher Umstände entstehen können

9. Sicherheitsbezogene Folgeabschätzung bei dem Einsatz neuer Basistechnologien, wie IPv6.

4 Allgemeine Sicherheitsanforderungen für Smart Grids

Bei den nachfolgenden Betrachtungen der IT-Sicherheitsziele wird der Fokus auf die allgemeine IT-Sicherheit gelegt, die weitgehend branchenunabhängig ist. Sie sind aus der Tatsache begründet, dass die Kommunikation im Smart Market und Smart Grid im offenen ("Internet") oder ggf. in teilweise offenen Netzen ("Internet der Energie") erfolgt und mit dieser Einführung von IKT eine Vielzahl von Schnittstellen und damit eine erhöhte Komplexität und neue Sicherheitsrisiken entstehen lassen.

Prinzipiell sind die klassischen IT-Sicherheitsziele zu verfolgen (siehe auch Abschnitt 3.2):
- Verfügbarkeit
- Vertraulichkeit
- Authentizität
- Integrität
- Nachvollziehbarkeit
- Verbindlichkeit / Nichtabstreitbarkeit

4.1 Schutzbedarf

Bedrohungsszenarien für Smart Grids haben insbesondere Einfluss auf die Sicherheitsziele Verfügbarkeit, Authentizität, Vertraulichkeit und Integrität:

Die Verfügbarkeit des Energienetzes (Versorgungssicherheit) hat weiterhin die höchste Priorität und ist zu gewährleisten. Die Vertraulichkeit muss u.a. aus datenschutzrechtlichen Gründen sichergestellt werden, damit System- und Verbrauchsdaten vor dem Zugriff durch Dritte geschützt sind.

Die Authentizität von Komponenten eines Smart Grids und die Integrität bzw. Authentizität der Kommunikation muss für autorisierte Schaltvorgänge sowie sichere und zuverlässige Abrechnungsverfahren sichergestellt werden. Bedrohungsszenarien für Smart Grids können in vier Dimensionen auftreten [32]:
- Vorsätzliche oder unbeabsichtigte externe Bedrohungen sowie
- vorsätzliche oder unbeabsichtigte interne Bedrohungen.

Hierzu sind Schutzziele zu definieren. Das Energiewirtschaftsgesetz (EnWG) besagt: "Zweck des Gesetzes ist eine möglichst sichere, preisgünstige, verbraucherfreundliche, effiziente und umweltverträgliche leitungsgebundene Versorgung der Allgemeinheit mit Elektrizität und Gas, die zunehmend auf erneuerbaren Energien beruht." Daraus leiten sich die Schutzziele im Einzelnen ab, die hier betrachtet werden:

1. Die sichere Energieversorgung,
2. die verbraucherfreundliche Energieversorgung und
3. die effiziente Energieversorgung.

Der Schutzbedarf für die Grundwerte Verfügbarkeit, Vertraulichkeit und Integrität soll für diese Aspekte der Versorgung betrachtet werden:

Die Versorgungssicherheit steht an erster Stelle. Gemäß §2 EnWG sind die Energieversorgungsunternehmen für eine sichere Energieversorgung zuständig. Die Versorgungssicherheit wird vom Bundesministerium für Wirtschaft und Technologie überwacht (§51 EnWG). Die Versorgungssicherheit bei Elektrizität ist in Deutschland sehr hoch [43]. So gab es 2009 in Deutschland nur 14,63 Minuten durchschnittliche Unterbrechungszeit der Stromzufuhr für Endkunden (entsprechend 99,997% Verfügbarkeit). Wegen der Bedeutung der Energieversorgung für das Land gilt diese als "Kritische Infrastruktur" [5] [31].

Die Versorgungssicherheit umfasst sowohl die Verfügbarkeit von Elektrizität, als auch die zugehörigen Safety- und Security-Aspekte. Entsprechend hoch ist auch der Schutzbedarf für alle Komponenten und Prozesse mit direktem oder indirektem Einfluss auf die Steuerung von Primärsystemen (bspw. SCADA-Systeme).

Durch die zunehmende Vernetzung der Systeme – speziell im Rahmen eines Smart Grids – erlangen einerseits zusätzliche Komponenten Einfluss auf die Steuerung von Primärsystemen, andererseits ergeben sich dadurch auch neue Angriffsmöglichkeiten (siehe Abschnitt 4.5). Der Schutzbedarf muss in diesem Rahmen neu bewertet werden.

Insbesondere der Schutz vor einem Ausfall der Systeme und somit die Verfügbarkeit sollte daher mit einem sehr hohen Schutzbedarf bewertet werden. Hinsichtlich der Verfügbarkeit von Verbrauchs- und Kundenstammdaten sind kürzere Ausfallzeiten oftmals zu tolerieren, somit ist hier ein geringerer Schutzbedarf als "sehr hoch" anzusetzen.

Für die Verbraucherfreundlichkeit ist der Datenschutz von großer Bedeutung. Durch eine Einführung von automatisierter Erfassung und Übermittlung von Verbrauchsdaten mittels Smart Metering wird eine sehr feingranulare Erfassung von Messdaten technisch möglich. Derartige technische Möglichkeiten sind auf ihre Verträglichkeit mit dem Datenschutz zu überprüfen [31], siehe Abschnitt 2.8.2 und Kapitel 5. Gleichzeitig müssen die Daten bei der Verarbeitung und Übermittlung durch diese neuen Systeme zuverlässig vor Einsichtnahme Dritter geschützt werden.

Schutz vor Manipulation und Betrug: In Bezug auf die Integrität der Daten besteht im Wesentlichen die Gefahr der Manipulation, einerseits mit dem Ziel eines Ausfalls von (Steuerungs-)Systemen - der Computerwurm Stuxnet ist ein Beispiel hierfür [18] - und anderseits mit dem Ziel eines Abrechnungsbetruges. Erstere Bedrohung ist einer sehr hohen Schutzbedarfskategorie, letztere einem hohen Schutzbedarf im Sinne des Smart Grids bzw. Smart Markets zu zuordnen.

Für eine effiziente Energieversorgung spielt das Monitoring und die Fernsteuerung verteilter Energieerzeuger und die dazu notwendige Datenkommunikation, bspw. bzgl. der Einspeiseleistung dezentraler Erzeuger, eine entscheidende Rolle. Dieses stellt bspw. die Basis für sog. virtuelle Kraftwerke ("Schwarmstrom") dar und ist hinsichtlich der Verfügbarkeit der Kommunikation und der Daten sowie deren Authentizität und Integrität einem hohen Schutzbedarf zuzuordnen.

Für eine gesamtheitliche Sicherheitsbetrachtung und Festlegung des Schutzbedarfs ist auch die Art des Endkunden (Privathaushalt, gewerblicher Kunde und Industrieunternehmen bzw. Betreiber von Kleinstkraftwerken) zu berücksichtigen. Der Schutzbedarf von Industriekunden und deren Energie-Management-Systemen ist ggf. ein anderer als der eines einzelnen Privathaushalts. Trotzdem bestimmt das Datum mit dem höchsten Schutzbedarf den Sicherheitsbedarf des jeweils betrachteten (Teil-)Systems.

Schutzbedarfe der Netzbetreiber beziehen sich auf hohe Verfügbarkeit, hohe Integrität sowie Aktualität und Vollständigkeit der Daten, die für das Lastmanagement benötigt werden. Vordringliche Schutzbedarfe eines Endkunden hingegen sind die Versorgungssicherheit, sowie die Vertraulichkeit und Integrität bzw. Korrektheit von Verbrauchs- und Abrechnungsdaten.

4.2 Sichere Nutzung von Internetprotokollen

IKT-Mechanismen werden zwingend das Internetprotokoll und weitere, darauf aufsetzende Protokolle verwenden. Dies ist betriebswirtschaftlich und volkswirtschaftlich unbestritten, denn Internettechnologie steht aufgrund der weltweiten Verbreitung in Form von Hardware, Software und Know-how preiswerter und ausgereifter als alle sonstigen proprietären Technologien zur Verfügung. Internettechnologie wird besonders für die Kommunikation vom und zum Endkunden und seiner Messeinrichtung eingesetzt werden. Sie wird aber letztendlich jede Nachrichtenübertragung betreffen. Dies gilt für Mensch-Maschine-Schnittstellen und Machine-to-Machine Communication (M-to-M, M2M) und somit für jede Kommunikation im "Internet der Energie".

Das IP-Protokoll kann und wird heute schon in dieser Branche über unterschiedliche Transportmechanismen übertragen. Dabei spielt eine Reihe von drahtlosen Übertragungsmethoden eine Rolle, die abhängig von der physischen Erfordernis, also insbesondere der Reichweite, eingesetzt und abgesichert werden. Dazu kommen drahtgebundene Methoden, wie z.B. die klassischen Internet-Anbindungs-Technologien oder die Powerline-Technologie in ihrer Breitbandvariante. Wenn dabei auch Powerline-Technologie das Problem der "letzten Meile" lösen kann, kann über das "Stromkabel" in Zukunft auch andere Kommunikation wie beispielsweise Telefonie oder Internet-Dienste erfolgen.

Das IP-Protokoll in der heute weltweit am meisten eingesetzten Version 4 mit gut 4 Milliarden Adressen (2^{32}) stößt dabei an Adressierungsgrenzen. Das Internet der Energie geht auch Hand in Hand mit dem Internet der Dinge, d.h. der direkten Adressierbarkeit möglichst vieler technischer Entitäten über das Internetprotokoll. Hier bietet IPv6 einen um gigantische Größenordnungen höheren Adressraum (2^{128}). Das Smart Grid bzw. Smart Metering könnte dafür wichtiger Einführungsimpuls werden.

Die Migration von IPv4 auf IPv6 führt während der Einführungsphase zu neuen bisher unbekannten Sicherheitsproblemen. Diese können auch im Rahmen der Einführung bei Smart Grids bzw. Smart Metering Sicherheitslücken entstehen lassen. Daher ist die Migration proaktiv und reaktiv zu begleiten und mögliche Sicherheitsvorkommnisse zeitnah zu erkennen und Gegenmaßnahmen einzuleiten.

IP wird sicher verbindungsorientiert eingesetzt werden müssen, d.h. um das Transmission Control Protocol (TCP) ergänzt werden. Darüber liegende Protokolle werden derzeit bei den unterschiedlichen Standardisierungen diskutiert. Nötig ist dabei ein Containerprotokoll, das unterschiedliche Formate transportieren kann.

Es zeichnet sich ab, dass Kommunikation von XML-basierten Daten über WebServices verwendet werden wird. Dies ermöglicht eine sichere Übertragung hinsichtlich Integrität, Authentizität und Vertraulichkeit auch im Sinne von Mandantenfähigkeit.

Evtl. können aber auch Protokolle eingesetzt werden, die sich in anderen Anwendungsbereichen mit großem Erfolg bewährt haben. Ein Beispiel ist das in einem internationalen IETF-Standard RFC 3261 genormte Session Initiation Protocol (SIP), das beim Voice over IP (VoIP) Containerprotokoll für weitere benötigte Funktionalitäten ist.

Es darf bezweifelt werden, ob der Einsatz von IKT im Smart Grid erheblichen Normungsbedarf auf der Protokollebene mit sich bringt. Vielmehr haben unterschiedlichste IP-Anwendungsbereiche zahlreiche ausgereifte Schnittstellen und Protokolle geschaffen, die zumindest auf ihre Eignung überprüft werden müssen, bevor nach erneuter Normung gerufen werden darf.

4.3 Identity- und Access-Management

4.3.1 Identitäten

Das heutige institutionalisierte Identitätsmanagement im Energiemesswesen definiert eine genormte Zählernummer, die den Bezug zu eichrechtlichen Vorgängen und abrechnungsrelevanten Vorgängen herstellt. Die Zählpunktbezeichnung besteht aus 33 Stellen, die sich aus folgenden Bestandteilen zusammensetzt:

- Internationale Länderkennung gemäß ISO 3166-1 (2 Stellen, alphabetisch),
- VDEW-Stromnetzbetreibernummer (6 Stellen, numerisch, rechtsbündig angeordnet sowie nach links mit Nullen aufgefüllt),
- Postleitzahl (5 Stellen, numerisch)
- Zählpunktnummer (20 Stellen, alphanumerisch)

Diese Identitätsbeschreibung ist eine eindeutige Beschreibung des Zählers und ist als solche fortzusetzen – sowohl für den Zähler als auch für das zum Messsystem zugehörige Smart-Meter-Gateway. Die bisherige Zählpunktbezeichnung ist ein wesentliches Datenfeld der heutigen EDIFACT-Nachricht MSCONS zur kettenförmigen Übertragung von Zählwerten im liberalisierten Energiemarkt und ist in jeder Transaktion, z.B. zwischen VNB und Lieferant, anzugeben.

Eine eindeutige Identitätsbeschreibung wird zukünftig bei ggf. sternförmiger Datenübertragung – auch bei weitgehender Anonymisierung und Pseudonymisierung – nach wie vor benötigt. Im Gegensatz zum Zählpunkt, Zählwerten und Ableseinformationen spielen andere Datenfelder bei den Privatkunden kaum eine Rolle. Dies ist bei Sondervertragskunden anders, wo z.B. in der MSCONS-Nachricht vielfältige Tarifinformationen hinterlegt sind.

Aber auch für andere Komponenten im gesamten Smart Grid einschließlich der beteiligten Rollen wie beispielsweise zur Wartung der Komponenten sind Identitätsbezeichnungen zu definieren und umzusetzen. Dies betrifft auch die Adressierung von Kommunikationspartnern wie beispielsweise dem Messstellenbetreiber.

Ein umfassendes Identitätsmanagement ist deshalb wesentlicher Teil des Sicherheitskonzeptes. Es bedarf dabei einer erheblichen Erweiterung der bisherigen Identitätsmerkmale und Betriebsprozesse.

Das zukünftige Identitätsmanagement muss sowohl die größere Zahl an technischen Komponenten, ggf. natürliche Personen, juristische Personen / Institutionen als auch Rollen, also Akteure bzw. Marktrollen, einbeziehen.

4.3.2 Berechtigungen

Berechtigungen und Befugnisse müssen prinzipiell neu bzw. erweitert geregelt werden. Dazu gibt § 21g EnWG schon einige rechtliche Hinweise. Weitere Konkretisierungen wird z.B. die derzeit in Novellierung befindliche Messzugangsverordnung (MessZV) liefern müssen. Dabei soll nach neuen Informationen die heutige MessZV in drei Verordnungen aufgegliedert werden. Weiterhin wird die heutige Kommunikationsrichtlinie als Branchenvereinbarung verbindlicheren Charakter bekommen müssen. Hierzu sind dringend Betriebsprozesse im Detail und durch Branchenkenner zu betrachten, die Sicherheit und gleichzeitig eine angemessene Wirtschaftlichkeit garantieren.

Ein konsistentes Identity- und Access-Management erfordert auch eine zweifelsfreie Identifizierung und oftmals eine rollenbasierte Berechtigungsvergabe. Unzulässige wie auch sich

gegenseitig ausschließende Berechtigungen (Plausibilitätskontrolle, Aufgabentrennung/Segregation of Duties) sind zu verhindern.

Einige Beispiele mit besonderen Anforderungen bzw. besonderem Branchenbezug seien hier exemplarisch genannt:

1) Die Berechtigungsvergabe für bestimmte Identitäten wird jede Institution für sich als "Identitätsprovider" machen müssen. Allerdings wird es Szenarien geben, in denen ein mandantenfähiger Zugriff auf technische Entitäten (Ressourcen) erfolgen muss. In diesem Fall wird der "Identitätsprovider" nicht mehr der "Ressourcenprovider" sein. In einem solchen Fall werden sog. Föderationsdienste / Federation Services anzuwenden sein.

2) § 21 h EnWG verlangt, dass der Letztverbraucher Dateneinsicht in seine Energiedaten bekommen muss. Dies muss ebenfalls nach §21 h der Messstellenbetreiber ohne zusätzliches Entgelt gewährleisten. Eine zertifikatsbasierte Authentisierung des Endkunden wird, nach heutigem Stand zumindest in der Anfangsphase, kaum praktikabel sein. Vielmehr wird der Endkunde eine Passwort-basierte Authentisierung verwenden. Schon alleine das Passwort-Reset bei vergessenen Passwörtern, die Aufklärungsmaßnahmen zur Authentisierung und die entsprechende sichere Verwaltung der Authentisierungsinformationen stellen bei der hohen Anzahl der zu erwartenden Nutzern eine enorme Herausforderung dar.

3) § 21 i EnWG sieht spezielle Regelungen zur Einbindung steuerbarer Anlagen vor. Im Smart Grid stellen diese potentielle Kandidaten für Demand Response oder sogar Demand Side Management Ansatzpunkte dar. Das zukünftige Metering Gateway stellt mit der CLS-Schnittstelle und dem TLS-Protokoll eine gewisse sichere Proxy-Funktion für Überwachung und Steuerung dar. Allerdings werden für dynamische Tarife, die helfen können ungenutzte Spitzen bei regenerativen Energieformen besser zu nutzen, eine bessere Synchronisation von Daten aus dem Metering und den Daten für das Energie-Management benötigt, als es ein rein lesender Zugriff erlauben würde. Dies stellt neue Anforderungen an ein umfassenderes Berechtigungsmanagement. Ein Energie-Management-Gateway würde ebenfalls integriert werden müssen.

4.3.3 Key-Management

Zu allgemeinen Aspekten und Sicherheitsaspekten beim Key–Management / Schlüsselmanagement wird hier auf die vielfältige Literatur zu diesem Thema verwiesen. Allerdings sollte man zwei Gesichtspunkten besondere Beachtung schenken und in detaillierten Betrachtungen weiter ausarbeiten:

1. Da das Smart Grid eine kritische Infrastruktur darstellt, ist bei der Nutzung von das Smart Grid beeinflussenden kritischen Funktionen durch Komponenten als auch durch agierende Personen stets eine sichere Schlüssel-Management-Komponente, z.B. ein Sicherheitsmodul / Smartcard, zu verwenden.

2. Es sollte nicht nur auf asymmetrisches Schlüsselmaterial in der jeweiligen PKI geachtet werden, sondern bei jeder Form von Schlüsseln auf die Gratwanderung zwischen Praktikabilität und Sicherheit geachtet werden. Im Anhang B zum Sicherheitsmodul des Metering Gateways ist z.B. mit der Bezeichnung "SM_PKCS_ENC_PRIV" ein privater Schlüssel für die Aushandlung von symmetrischen Schlüsseln, mit dem Administratorkommandos verschlüsselt werden, bezeichnet.

Wird hier ein individueller Schlüssel verwendet, so müsste man bei der Administration von Gateway-Konfigurationen im Feld für möglicherweise Millionen von Clients individuell ver-

schlüsseln. Ist jedoch kein individueller Schlüssel vorgesehen, so erhöht sich das Risiko einer massenhaften Korrumpierung. Auf solche Fragen muss ein Key-Management-Konzept angemessene Antworten geben.

4.4 Nutzung von vorhandener Sicherheitstechnologie

Für die Umsetzung der in Kapitel 5.1 skizzierten Schutzbedarfe im Bereich der CIT und teilweise auch für PIT steht bereits ein umfangreiches Portfolio an nutzbaren technischen und organisatorischen Maßnahmen zur Verfügung.

Entscheidend ist es hierbei, die relevanten nationalen und internationalen Standards in Bezug auf Schlüsselzertifikate, Komponenten, Prozesse und Policies zu berücksichtigen.

Derzeit entwickelt das BSI auf Basis der "Common Criteria" eine Reihe von Schutzprofilen [36], [46] und Technischen Richtlinien für ein Smart-Meter-Gateway und ein zugehöriges Sicherheitsmodul. Hierdurch wird ein sehr hohes Sicherheitsniveau für diese Komponente und deren Sicherheitsmodul definiert. Zusammen definieren Schutzprofile und Technische Richtlinien schon eine Sicherheitsrahmenstruktur, die auch auf das komplette Smart Grid angewandt werden könnten:

- Systemarchitektur
- PKI
- Kommunikationsprotokolle
- Kryptographische Vorgaben
- Zugriffs- und Berechtigungsprofile

Ergänzend zu dem bisherigen Stand der Technischen Richtlinien liefern die Vorgaben der VEDIS Certificate Policy (VEDIS-CP), aufgebaut nach RFC 3647, ein Sicherheitsniveau für die PKI der EVUs. Auf europäischer Ebene bieten sowohl CEN als auch ETSI ein sehr umfangreiches Portfolio an Europäischen Normen, die eine interoperable Implementierung und einen kostengünstigen Betrieb von Sicherheitstechnologien erlauben.

Es ist zu empfehlen, vor der Entwicklung neuer Spezifikation eingehend zu überprüfen, inwieweit auf existierende Standards und Normen zurückgegriffen werden kann. Der daraus resultierende Nutzen ergibt sich nicht nur durch ein größeres Marktpotenzial und die Vermeidung der Diskriminierung von Markteilnehmern (mit dem latenten Risiko eines nachträglich notwendigen Umschwenkens auf Europäische Vorgaben), sondern auch durch die verbesserte Verfügbarkeit von Schnittstellen und Testszenarien.

Im Bereich des strategischen Sicherheitsmanagements ist die ISO 2700x-Reihe weltweit akzeptiert. Neben den Vorgaben für die systematische Optimierung der IT-Managementprozesse werden Empfehlungen zum Betrieb und zum Notfallmanagement getroffen. Auch die spezifischen Erfordernisse der Energiewirtschaft werden zukünftig hierbei berücksichtigt (Siehe Kapitel 4.4). Auf Basis der ISO 20000 Reihe können die Anforderungen an die Service-Level und die Verfügbarkeit definiert werden.

Neben den klassischen Maßnahmen zur Verbesserung der IT-Sicherheit durch den Einsatz von vertrauenswürdigem Personal sowie zertifizierten Komponenten und Diensten kommt der kontinuierlichen Überwachung der kritischen Infrastrukturen eine sehr große Bedeutung zu. Durch die zunehmende Vernetzung der Systeme verändert sich die aktuelle Bedrohungslage kontinuierlich. Die Gefahren durch sich unkontrolliert verbreitende Schadsoftware (z. B. Viren) oder verteilte Angriffe durch Rechnersystemverbünde (DDOS) erfordern kompetente proaktive Gegenmaßnahmen und im Fall des Falles auch Reaktionen innerhalb von Stunden oder sogar Minuten.

Wesentliche Voraussetzung ist hierbei die Planung und Implementierung eines Notfallmanagements auf Netzwerk- und Anwendungsebene. Hierbei bildet auch die Einbindung von Computernotfall-Reaktionskräften (CERTs) einen wichtigen Baustein. Diese überwachen kontinuierlich den Bedrohungsstatus, alarmieren, sprechen Empfehlungen aus und leiten ggf. Gegenmaßnahmen ein.

4.5 SCADA-Sicherheit

SCADA steht für Supervisory Control and Data Acquisition. Es bezeichnet Systeme zur Automatisierung, Prozesssteuerung und Prozessleitung. SCADA bezieht sich gewöhnlich auf zentrale/dezentrale Systeme, die gesamte Installationen überwachen, visualisieren sowie steuern und regeln. Der größte Teil der Regelung wird automatisch durch Fernbedienungsterminals (RTU) oder durch Speicherprogrammierbare Steuerungen (SPS) durchgeführt.

Seit der Entdeckung des Stuxnet-Wurms ist die SCADA Sicherheit in der breiten öffentlichen Wahrnehmung angekommen. Er markiert den Beginn einer neuen Ära von Angriffen auf Computersysteme [1].

Was ist bei dem Stuxnet-Vorfall das besondere? Dieser Wurm hat es letztlich nicht auf Kreditkartennummern, Passwörter etc. abgesehen, sondern auf die Steuerung von physischen Zentrifugen für die Urananreicherung [4].

Insbesondere bei SCADA-Systemen innerhalb von kritischen Infrastrukturen können die Folgen besonders schwerwiegend sein.

Die potentiellen Angriffsflächen von Standardsystemen und Protokollen sind bereits öffentlich bekannt und trotzdem sind sie in den bestehenden Systemen teilweise nicht behoben. Dies kann auch als "tickende Zeitbombe" gesehen werden, sollte die Vernetzung dieser Systeme mit anderen Kommunikationsnetzen (wie auch der Büro-IT des Betreiber- bzw. Versorgungsunternehmens) vorgenommen werden. Durch diese Vernetzung wird es ermöglicht, derartige Angriffsflächen auch von einem entfernten Standort auszunutzen.

Typische Kategorien von SCADA spezifischen Angriffsflächen sind dabei:

Virenscanner

SCADA-Systeme arbeiten im Echtzeit-Betrieb, d.h. sie müssen nahezu verzögerungsfrei in die Systeme eingreifen. Diese Anforderung wird von derzeitigen Sicherheitssystemen für Standard-Betriebssysteme leider noch nicht erfüllt. So reduzieren Virenscanner die Performance und erzeugen zudem ein zeitlich variables Lastprofil. Als Konsequenz daraus werden Virenscanner bei SCADA-Systemen typischerweise nicht eingesetzt [8]. Schadsoftware kann sich daher einfacher ausbreiten [9] [10]. Diese Schwäche wurde auch von Stuxnet ausgenutzt [4].

Patch Management

SCADA-Systeme arbeiten typischerweise ohne Unterbrechungen (24x7) – auch häufig ohne Wartungsfenster für die Software. Jede Änderung an einem funktionierenden System wird als ein Safety-Risiko gesehen und daher vermieden. Demgegenüber werden selbst vergleichsweise unkritische Bürocomputer typischerweise mindestens einmal pro Monat aktualisiert [11], um Programmfehler im Betriebssystem oder den Anwendungen zu beheben. Die damit verbundenen Nicht-Verfügbarkeitszeiten sind bei SCADA-Systemen typischerweise schwer tolerierbar [12]. Als Konsequenz werden Software-Aktualisierungen seltener oder gar nicht durchgeführt. Entsprechend alt und mit öffentlich bekannten Sicherheitslücken behaftet sind auch die eingesetzten Betriebssysteme und Applikationen. Eine Liste einiger bekannter Fehler von SCADA-Produkten wurde z.B. von Luigi Auriemma veröf-

fentlicht [13]. Softwareaktualisierungen sind daher für die Aufrechterhaltung der IT-Sicherheit unerlässlich [14].

Penetrationstests sind bei allgemeinen Computersystemen mittlerweile eine etablierte Methode, um Schwachstellen durch ungewollte Systemänderungen zu erkennen. Bei SCADA-Systemen sind derartige Tests unüblich und haben schwer abzuschätzende und zum Teil sogar katastrophale Folgen [15].

Perimeter Security
Ursprünglich waren SCADA-Systeme nach außen abgeschlossene Netzwerke [16] [17]. Die Steuerungssysteme vertrauten sich untereinander. Es bestand kein Bedarf für umfangreiche interne Schutzmaßnahmen. Bei isolierten Systemen sind vernünftige Schutzmaßnahmen der IT-Systeme weniger wichtig als effektive Zutrittskontrollen am jeweiligen Gebäude selbst. Durch die zunehmende Vernetzung müssen die Sicherheitsmaßnahmen der IT-Systeme deutlich ausgebaut werden. Dazu gehören auch eine gesicherte Datenübertragung inklusive starker Mechanismen zur Authentisierung von Benutzern sowie anderen vertrauenswürdigen Systemkomponenten. Das gilt für jegliche Kommunikation, auch beispielsweise für den Austausch von Daten über einem mobilen Speicher. So ist Stuxnet durch einen USB-Datenträger übertragen worden [18].

Authentisierung
Wenn Netzwerkzugriffe auf Systemkomponenten möglich und die Systeme nicht als völlig isoliert zu betrachten sind, dann ist die starke Authentisierung von großer Bedeutung. Passwörter haben sich häufig als ungeeignet erwiesen [19] [20]. Insbesondere bei der Maschine-zu-Maschine-Kommunikation (M2M) sind Passwörter ungeeignet. So hat Stuxnet u.a. auch fest einprogrammierte Passwörter zur Infektion ausgenutzt [21].

Verschlüsselte Datenübertragung ist bei der Kommunikation von kritischen Komponenten Standard. Bei typischen SCADA-Systemen werden jedoch häufig nicht einmal Passwörter verschlüsselt übertragen [22].

Sicherheitskonzept
Nur für sehr wenige SCADA-Systeme existieren adäquate (IT-) Sicherheitskonzepte [22]. Noch weniger davon sind Teil einer effektiven SCADA-spezifischen Sicherheitsadministration. Die Erfahrung mit allgemeinen IT-Systemen zeigt jedoch, dass sich Sicherheit ohne derartige Konzepte nicht effektiv umsetzen lässt. Das Thema Security muss zukünftig gleichwertig zum Thema Safety behandelt werden.

5 Datenschutz

Mit Smart Grids ergeben sich auch neue Herausforderungen, wenn bundes- oder europaweit eine Infrastruktur ausgerollt wird, die die flächendeckende Erfassung, Auswertung und langfristige Speicherung der Stromverbrauchswerte aller Haushalte vorsieht. Über die Erfassung zeitlich hoch aufgelöster Stromverbrauchsprofile werden intime Einblicke in die Abläufe und Lebensgewohnheiten in einem Haushalt möglich [35].

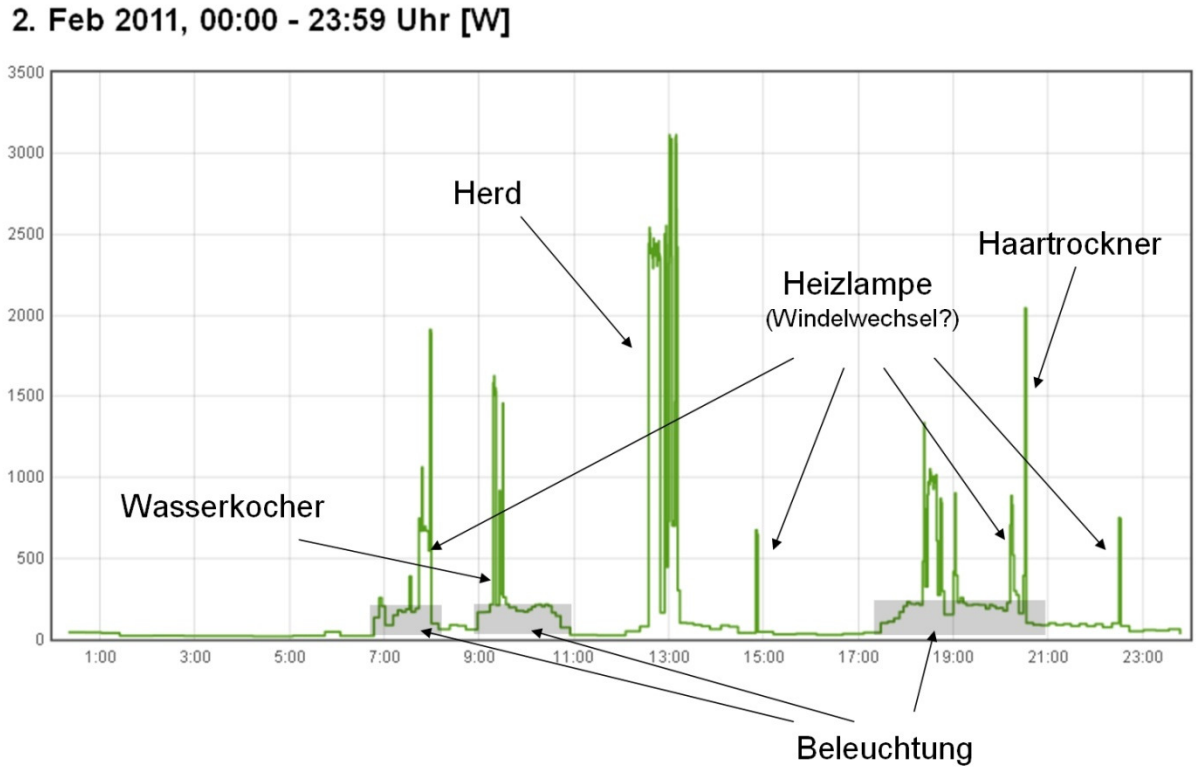


Abbildung 3: Beispielhaftes Lastprofil eines Haushaltes [44]

5.1 Ziele des Smart Metering aus dem EnWG

Die erste Frage in Bezug auf den Schutz der Daten ist die Frage nach der Notwendigkeit der Erhebung der Daten im Kontext des Smart Metering. Sinnvollerweise werden die anfallenden Daten dabei nach den Verwendungszwecken getrennt behandelt.

5.1.1 Primärer Zweck: Verbrauchsminimierung durch Visualisierung

Aus der Definition eines Smart Meters (Messsystem) im Energiewirtschaftsgesetz geht die primäre Forderung hervor:

"§21d Messsysteme:
(1) Ein Messsystem im Sinne dieses Gesetzes ist eine in ein Kommunikationsnetz eingebundene Messeinrichtung zur Erfassung elektrischer Energie, das den tatsächlichen Energieverbrauch und die tatsächliche Nutzungszeit widerspiegelt."

Neben der offensichtlichen Notwendigkeit, den Verbrauch zu erfassen und der neuen Anforderung – der Einbindung in ein Kommunikationsnetz – geht es also um den Zweck, den Verbrauch in Relation zur Zeit darzustellen. Das wiederum soll die Basis für die Verbrauchsoptimierung und -minimierung bilden.

5.1.2 Weitere Zwecke: Betrieb, Abrechnung, Visualisierung, Steuerung

In §21g EnWG sind die weiteren Zwecke ausdrücklich aufgeführt, für die Daten aus dem oder auf dem Messsystem verarbeitet werden dürfen. Diese lassen sich zusammenfassen in:

- Betrieb (Netz, Messsystem)
- Abrechnung
- Steuerung
- Sonstige freie Vertragsverhältnisse ohne konkrete Zweckfestlegung

Zentrale Fragen zur Bewertung hinsichtlich des Schutzes der Privatsphäre sind unter anderen:

- Sind zeitlich hoch aufgelöste Mess- oder Statuswerte verzichtbar?
- Ist die zentrale Verarbeitung der Daten verzichtbar?
- Ist der Personen- bzw. Haushaltsbezug der Daten verzichtbar?
- Ist eine datensparsame Anwendung möglich?

	Sind zeitlich hoch aufgelöste Mess- oder Statuswerte verzichtbar?	Ist die zentrale Verarbeitung der Daten verzichtbar?	Ist der Haushaltsbezug der Daten verzichtbar?	Ist eine datensparsame Anwendung möglich?
Visualisierung	Nein	Ja	Nein	Ja
Betrieb	Nein	Nein	Ja	Ja
Letztverbraucher-Abrechnung	Ja	Nein	Nein	Ja
Steuerung	Nein	Nein	Ja	Ja

Tabelle 1: Beispielhafte Darstellung Verwendungszwecke beim Smart Metering

Wie aus
Tabelle **1** hervorgeht, sind für dedizierte Use Cases nur die Daten bereitzustellen, die unbedingt nötig sind, um die Funktionalität zu erbringen (Need-to-Know). Daher sind Forderungen wie Datensparsamkeit, Aggregation, Anonymisierung, Pseudonymisierung entsprechend dem jeweiligen Uses Case zuzuordnen und zu bewerten.

5.2 Forderungen in Bezug auf den Datenschutz im Smart Grid

5.2.1 Datensparsamkeit – frühestmögliche Aggregation und Anonymisierung der Daten

Für eine datensparsame Realisierung des Smart Grid bzw. dessen datenschutzrechtlich relevanten Teilbereichen sollten die im Haushalt anfallenden Daten möglichst früh aggregiert und anonymisiert werden. Eine Aggregation ist dabei zumindest bei einfachen Tarifmodellen mit einer begrenzten Anzahl langfristig gleichbleibender Tarifstufen bereits in einem Haushalt über die Abrechnungsperiode möglich. So ist die Übermittlung von Mess- und Statuswerten z. B. nur ein Mal pro Abrechnungsperiode zur Abrechnung erforderlich. Im Idealfall ist diese Funktion bereits im Smart Metering Gateway realisiert. Das Schutzprofil des BSI zum Smart Metering Gateway [36] legt hierfür bereits den Grundstein. Für hochdynamische Tarife zur z.B. wetterabhängigen Lastverlagerung ist ein derartiges Vorgehen mangels fixer Tarifstufen und –umschaltzeiten jedoch nicht ohne weiteres möglich. Insbesondere im Hinblick auf die im liberalisierten Energiemarkt zwingend notwendige Bilanzierung sollten hier Mechanismen der pseudonymen und/oder anonymen Datenverarbeitung weiter diskutiert werden.

Auf der Ebene des Verteilnetzbetreibers können Verbrauchsdaten über mehrere Dutzend Haushalte aggregiert werden, um so eine Zuordnung einzelner Vorgänge zu konkreten Haushalten deutlich zu erschweren. Dabei ist eine verzögerungsfreie Verarbeitung der Mess- oder Statuswerte in Bezug auf den Datenschutz unproblematisch.

Durch die Pseudonymisierung und Anonymisierung der Daten wird eine spätere Zuordnung der Daten zu einem Haushalt verhindert bzw. deutlich erschwert. Eine spezifische Regelung erfolgte bereits im novellierten EnWG vom 04.08.2011.

5.2.2 Genaue Reglementierung der Verwendung der Daten

§21g EnWG regelt bereits sehr genau, wer zur Verarbeitung der Daten aus dem Messsystem berechtigt ist und zu welchem Zweck. Eine solch präzise Vorgabe ist auch für die nachgelagerten Prozesse im Smart Grid wünschenswert.

5.2.3 Scharfe Sanktionierung von Verstößen

In vielen prominenten Beispielen der letzten Jahre fielen die bei datenschutzrechtlichen Verstößen verhängten Strafen relativ gering aus, so dass das für die Unternehmen entstehende Risiko überschaubar und die Abschreckung entsprechend gering war. Durch eine scharfe Sanktionierung von Verstößen könnte auch dem Verbraucher die Unsicherheit genommen werden, dass mit seinen Daten leichtfertig umgegangen werden könnte [37].

5.2.4 Schaffung von Transparenz

Jenseits des energiewirtschaftlich zwingend notwendigen Minimums sollte der Verbraucher selbst für bestimmte Zwecke bestimmen können:

- wer
- zu welchem Zeitpunkt
- Zugriff auf welche Daten
- in welcher Granularität hat.

Der Nutzer sollte die Gewissheit haben, dass das Mögliche getan wird, um zu verhindern, dass Unberechtigte Zugriff auf (weitere) Informationen über ihn und sein Verbrauchsverhalten haben. So kann das Vertrauen entstehen, welches die Basis für die Nutzerakzeptanz bildet.

6 Von der Strategie zur Umsetzung

Derzeit arbeiten verschiedenste Organisationen, Unternehmen und wissenschaftliche Einrichtungen z.T. an sehr spezifischen Fragestellungen, oft auch redundant und unkoordiniert.

Es besteht ein besonderer Bedarf an einem nachhaltigen Austausch zwischen allen im Bereich Smart Grid aktiv handelnden Institutionen und Unternehmen in Deutschland. Ein interdisziplinäres und vor allem sektorenübergreifendes Vorgehen ist dabei dringend erforderlich.

Hilfreich ist hierzu insbesondere die Einrichtung einer gemeinsamen Plattform zum Thema IT-Sicherheit und Datenschutz im Smart Grid. Die unterschiedlichen Akteure mit ihren vielfältigen Interessenlagen können sich hier zu einer gemeinschaftlichen zielorientierten strategischen Kooperation zusammenfinden. Vertreter aus Energiewirtschaft, Forschung, IT-Industrie, Gesetzgebung, Politik, IT-Sicherheits-Unternehmen, öffentlicher Hand und Datenschutz-Organisationen sollten sich in einem solchen Rahmen treffen, gemeinsame Ziele definieren, ausgestalten und in die Umsetzung überführen.

Um die Tätigkeiten zu strukturieren, können die unterschiedlichen Domänen / Handlungsfelder
- Smart Metering
- Messstellenbetrieb und –dienstleistung
- Aggregationsdienstleister
- Energieberatung/-steuerung via Controllable Local System (CLS)
- Marktplatz
- Verteilnetz
- Übertragungsnetz / Bilanzierung
- Service
- Groß-Erzeuger

folgenden Bereichen/Arbeitsschwerpunkten
- Forschung
- Standardisierung und Normung
- Rechtssetzung
- Kommunikation (Schaffung der Akzeptanz)

zugeordnet werden. So entsteht eine Matrix, die einen detaillierten Überblick über den Handlungsbedarf liefert.

Dabei sind ausgehend von einer übergreifenden Sicherheitsstrategie unterschiedliche Sicherheitskonzepte für die einzelnen Domänen / Handlungsfelder zu erstellen. Die Arbeit integriert dabei Forschungsaktivitäten, die Realisierung von Lösungen bis zur Integration dieser in die Smart Grids und darüber hinaus auch akzeptanzbildende Maßnahmen.

7 Forderungen von TeleTrusT

TeleTrusT fordert bei dem in Kapitel 6 beschriebenen Vorgehen insbesondere die Beachtung folgender Punkte:

1. Berücksichtigung von IT-Sicherheitsaspekten bereits in der Planungs- und Normierungsphase

2. Etablierung eines hohen bzw. teilweise sehr hohen Niveaus hinsichtlich der Sicherheitsziele im gesamten Smart Grid (Vertraulichkeit, Integrität, Authentizität, Nicht-Abstreitbarkeit, Verfügbarkeit, Verbindlichkeit, Zuverlässigkeit)

3. Vorgaben von IT-Sicherheitsstandards durch Politik, Gesetzgebung und Regulierungsinstitutionen

4. Überwachung der Umsetzung von Sicherheitsvorgaben

5. Regelmäßige Prüfung und Anpassung der Sicherheitsvorgaben an geänderte Rahmenbedingungen

6. Definition von Schutzprofilen und Zertifizierungsprozessen für alle kritischen Komponenten

7. Aufbau und Nutzung von vertrauenswürdigen Sicherheitsinfrastrukturen und –dienstleistungen

8. Angemessene Notfall-/Krisen- und Business Continuity-Konzepte und der Nachweis der Umsetzbarkeit dieser Konzepte

9. Klare und transparente Regelungen zu Zugriffsrechten auf Daten aus Mess- und Verbrauchseinheiten über die gesamte Prozesskette

10. Separate Betrachtung und Behandlung der Verwendungszwecke der Daten

11. Strikte Umsetzung des Grundsatzes der Datensparsamkeit bei der Erfassung und Übermittlung von Daten

12. Offene Kommunikation über Chancen und Risiken sowie akzeptierte Restrisiken.

Referenzen

1. McAfee. McAfee Threats Report: Third Quarter 2010. Labs, McAfee. s.l. : http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2010.pdf, 2010.
4. Stuxnet. Wikipedia. [Online] [Zitat vom: 15. 11 2011.] http://en.wikipedia.org/wiki/Stuxnet.
6. Risiko in den Ingenieur- und Umweltwissenschaften. Wikipedia. [Online] [Zitat vom: 10. 11 2011.] http://de.wikipedia.org/wiki/Risiko#Risiko_in_den_Ingenieur-_und_Umweltwissenschaften.
7. So nah und doch so fern: Die ICS-Security-Fata-Morgana. Sucker, Oliver. Oktober 2011, SCADA-Sicherheit, S. 16-17. ISSN 1862-4375.
8. Chiesa, Raoul und Pennasilico, Alessio L. R. SCADA (in) Security: Hacking Critical Infrastructures. s.l. : http://events.ccc.de/congress/2007/Fahrplan/attachments/1052_hacking_scada.pdf, 2007.
9. Poulsen, Kevin. Slammer worm crashed Ohio nuke plant network. [Online] 19. 8 2003. [Zitat vom: 19. 11 2011.] http://www.securityfocus.com/news/6767.
10. National Institue of Standards and Technology. Guide to Industrial Control Systems (ICS) Security. s.l. : http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf, 2011. NIST SP 800-82.
11. Patch Tuesday. Wikipedia. [Online] [Zitat vom: 7. 11 2011.] http://en.wikipedia.org/wiki/Patch_Tuesday.
12. IT Security & Network Security News. eWeek.com. [Online] 18. 8 2005. [Zitat vom: 17. 11 2011.] http://www.eweek.com/c/a/Security/Zotob-PnP-Worms-Slam-13-DaimlerChrysler-Plants/.
13. Auriemma, Luigi. Vulnerabilities in some SCADA server softwares. Security Focus. [Online] 21. 3 2011. [Zitat vom: 8. 11 2011.] http://www.securityfocus.com/archive/1/517080.
14. Daniel, Dr. Hans. Security in Safety Systems: The need to step beyond Traditional Engineering. s.l. : http://www.ewics.org/attachments/security-subgroup-newcastle-2008/The+Need+to+Step+beyond+Traditional+Engineering.pdf, 2008.
15. Duggan, David P. Penetration Testing of Industrial Control Systems. Albuquerque : http://energy.sandia.gov/wp/wp-content/gallery/uploads/sand_2005_2846p.pdf, 2005.
16. Schairer, Joachim. Verwundbarkeit und Angriffsmöglichkeiten auf SCADA Systeme. s.l. : http://www.joachim-schairer.de/VWEW-Vortrag_Fulda_17_10_07.pdf, 2007.
17. Phoenix Contact. Hacking the industrial network. Harrisburg : http://www.isa.org/FileStore/Intech/WhitePaper/Hacking-the-industrial-network-USversion.pdf, 2009.
18. Symantec. W32.Stuxnet Dossier. Moutain View : http://www.wired.com/images_blogs/threatlevel/2011/02/Symantec-Stuxnet-Update-Feb-2011.pdf, 2011.
19. Microsoft Research. A LargeScale Study of Web Password Habits. s.l. : http://research.microsoft.com/pubs/74164/www2007.pdf, 2007.
20. Forrester. Single Sign-On Dispelling The Myths — Finding The Fit. s.l. : http://www.forrester.com/Events/Content/0,5180,-1230,00.ppt, 2005
21. Vulnerability Summary for CVE-2010-2772. National Vulnerability Database. [Online] [Zitat vom: 5. 11 2011.] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2772
22. Stamp, Jason, et al. Common Vulnerabilities in Critical Infrastructure Control Systems. s.l. : http://www.oe.netl.doe.gov/docs/prepare/vulnerabilities.pdf, 2003.
28. Dr. Peter Bretschneider, Fraunhofer-Anwendungszentrum für Systemtechnik, Ilmenau
29. Augen zu und durch? Das hilft nicht! Beirer, Dr. Stephan. 10 2011, SCADA-Sicherheit, S. 11-13. ISSN 1862-4375.
30. ISA Security Compliance Institute. ISA.99.
31. Greveler, Prof. Dr.-Ing U., Justus, Dr. B. und Löhr, D. Hintergrund und experimentelle Ergebnisse zum Thema "Smart Meter und Datenschutz. Münster : http://www.its.fh-muenster.de/greveler/pubs/smartmeter_sep11_v06.pdf, 2011.
32. Bundesministerium des Innern: "Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)", www.bmi.bund.de/cae/servlet/contentblob/598730/publicationFile/34416/kritis.pdf
33. Sven Garrels: "Smart Grid - Cyber Security elektrisiert das intelligente Stromnetz der Zukunft", http://www.detecon-dmr.com/de/article/smart-grid_2011_02_16/, 2012
34. Bundesnetzagentur: "Smart Grid und Smart Market" – Eckpunktepapier der Bundesnetzagentur zu den Aspekten des sich verändernden Energieversorgungssystems, Dezember 2012
35. Müller, Klaus J.: "Gewinnung von Verhaltensprofilen am Intelligenten Stromzähler, Datenschutz und Datensicherheit (DuD), 6/2010, S. 359-364, http://www.secorvo.de/publikationen/verhaltensprofile-smart-meter-mueller-2010.pdf
36. BSI: Protection Profile for the Gateway of a Smart Metering System, v 1.1.1 (final draft), URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SmartMeter/PP-SmartMeter.pdf?__blob=publicationFile
37. Studie Forsa/VZBV: "Erfolgsfaktoren von Smart Metering aus Verbrauchersicht", http://www.vzbv.de/mediapics/smart_metering_studie_05_2010.pdf
38. Definition nach DKE – Kompetenzzentrum Normung E-Energy/Smart Grids, http://www.dke.de/de/std/KompetenzzentrumE-Energy/Seiten/DasKompetenzzentrumE-Energy.aspx

39. Andreas Kießling, techn. PL moma, MVV Energie AG, Berlin, 6. + 7. Mai 2010, Forum Netzintegration Erneuerbare Energien
40. Aktualisierte Umwelterklärung 2008 der Stadtwerke München, Verteilnetze für Energie und Wasser, Berichtsjahr 2007, Standort-Registernummer DE-155-00268,
41. Positionspapier Virtuelle Kraftwerke BDEW, 15.11.2010
42. VDE-Positionspapier, ITG, Energieinformationsnetze und –systeme, S. 38
43. http://www.bundesregierung.de/Content/DE/Artikel/2011/01/2011-01-24-versorgungssicherheit-strombereich.html
44. DUD 8/2011
45. Whitepaper_Secure_Systems_Vedis_1.0final
46. BSI: Protection Profile for the Security Module of a Smart Metering System (Security Module PP) -V 0.8.3. draft-, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SmartMeter/PP_Security_%20Module.pdf?__blob=publicationFile

TeleTrusT – Bundesverband IT-Sicherheit e.V.

TeleTrusT wurde 1989 gegründet, um verlässliche Rahmenbedingungen für den vertrauenswürdigen Einsatz von Informations- und Kommunikationstechnik zu schaffen und entwickelte sich zu einem bekannten Kompetenznetzwerk für IT-Sicherheit. Heute umfasst TeleTrusT mehr als 140 Mitglieder aus Industrie, Wissenschaft, Forschung und öffentlichen Institutionen sowie Partnerorganisationen aus Deutschland und Europa. In Arbeitsgruppen und Projekten befassen sich die Mitglieder mit aktuellen Themen der IT-Sicherheit und des Sicherheitsmanagements. TeleTrusT äußert sich zu politischen und rechtlichen Fragen, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und ist Trägerorganisation des PKI-Projektes "TeleTrusT European Bridge CA", des Expertenzertifikates "TeleTrusT Information Security Professional" (T.I.S.P.) sowie des Qualitätszeichens "IT Security made in Germany". Hauptsitz des Verbandes ist Berlin. TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI).

Kontakt:

TeleTrusT – Bundesverband IT-Sicherheit e.V.
Dr. Holger Mühlbauer
Geschäftsführer
Chausseestraße 17
10115 Berlin
Tel.: +49 30 4005 4306
Fax: +49 30 4005 4311
http://www.teletrust.de

TeleTrusT
Pioneers in IT security.