Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Umwelt, Verkehr, Energie und Kommunikation UVEK

Bundesamt für Energie BFE

Schlussbericht 26. September 2012

Smart Grids Security

Grundlagen zum Workshop anlässlich der «Smart Grids Week 2012» in Bregenz

Auftraggeber:
Bundesamt für Energie BFE
Forschungsprogramm Elektrizitätstechnologien & -anwendungen
CH-3003 Bern
www.bfe.admin.ch

Kofinanzierung:
Österreichisches Bundesministerium
für Verkehr, Innovation und Technik BMVIT, A-1010 Wien
www.bmvit.gv.at

Auftragnehmer:
Fichtner IT-Consulting AG
Sarweystrasse 3
D-70191 Stuttgart
www.fit.fichtner.de

Autoren:
Albrecht Reuter, Fichtner IT Consulting AG, albrecht.reuter@fit.fichtner.de
Wilson Maluenda Munoz, Fichtner IT Consulting AG, wilson.maluendamunoz@fit.fichtner.de

BFE-Bereichsleiter: Dr. Michael Moser
BFE-Programmleiter: Roland Brüniger
BFE-Vertragsnummer: SI/500572-05

Inhaltsverzeichnis

Inhalt

Zusammenfassung

Die IT-Sicherheit erfährt im Smart Grids Kontext eine neue Dimension, die Energiesysteme vulnerabler macht und sowohl Security wie auch Safety Aspekte in einem neuen Licht erscheinen lassen. Das energiewirtschaftliche Gefüge besteht aus einer komplexen Infrastruktur mit verschiedensten Komponenten, die durch interne oder externe Manipulation Schaden erlangen können. Ebenso können durch kriminelle Absichten Daten verändert und Kundendaten durch Hacker geraubt und zu kriminellen Zwecken verwendet werden. Auf der wirtschaftlichen Ebene lassen sich durch Erpressung oder Datenmanipulation Bedrohungsszenarien ausmalen, die aktuell noch nicht realisierbar sind, da die Smart Grids Implementierung noch nicht so weit fortgeschritten ist.
Es gibt bereits Abwehrmaßnahmen, aber die Einbindung von Sicherheitselementen ist sowohl mit technischen als auch mit organisatorischen Hürden und Grenzen konfrontiert, die es nach und nach zu lösen und zu überwinden gilt. Die technische Sicherheit der Geräte und die Einbindung in die Infrastruktur müssen durch Forschung und Entwicklung angehoben werden. Die Sicherheit der Datenübertragung ist durch die Flut der neu entstehenden Daten durch Smart Grids neuen Angriffspunkten ausgesetzt. Alle diese Faktoren beeinflussen die erfolgreiche Implementierung von Smart Grids, sei es im Bereich der Smart Meters, der Home Automation oder auch andere wie jene der Steuerungs- und Regelungsebene diverser Sensor/Aktuator Systeme. Eine gemeinsame Anstrengung ist daher notwendig um die Sicherheit des Gesamtsystems zu erhöhen. Die Erarbeitung einer Sicherheits-Roadmap für den Smart Grids Bereich ist das Gebot der Stunde und kann helfen, die Entwicklungen in diesem Segment zu steuern und überschaubar zu machen. Die Erarbeitung einer solchen Sicherheits-Roadmap muss aber koordiniert ablaufen, da sonst divergierende Entwicklungen die Folge sein könnten. Der Rahmen der Smart Grids D-A-CH Kooperation wäre hierfür eine geeignete Plattform.

Abstract

IT security in the context of smart grids is an important task to be solved. The energy management structure consists of several components that can be damaged through internal or external manipulation. Similarly, consumer or customer data can be altered or stolen by hackers with criminal intentions. On the economic level, Information can be obtained by extortion or data manipulation. There are various threat scenarios currently not even imaginable, due to the fact that the smart grid implementation has not yet progressed that far.

The integration of security elements, however, is confronted with various limitations and obstacles that need to be solved gradually. The technical safety of equipment and infrastructure must be increased through research and development. The enhancement of data transmission security is limited by the resulting flood of data coming from the smart grids implementation itself. All these factors affect the successful implementation of components of smart grid, either in the field of home automation or others like those of the control and regulation of various sensor and actuator systems. A joint effort is necessary to enhance the security of the entire system. The development of a security roadmap for the smart grid sector is the need of the hour and can help control the developments in this segment and make it manageable. To provide an effective roadmap and obtain usable results, certain safety and energy economics criteria must be considered.

Ausgangslage

Die Perspektiven der IT-Sicherheit im Energiebereich sind angesichts der Smart Grids Entwicklungen extrem komplex. Diverse Berichte in Medien über Hacker-Erfolge eines Smart Meters mit kostenlos verfügbaren Mitteln aus dem Internet haben die Brisanz der Thematik veranschaulicht. Die Angriffsfront auf die Smart Grids Elemente erscheint unter dieser Betrachtung als unendlich groß, da durch den einhergehenden Einzug der IKT sensible Komponenten im Zuge der gesamten Energieerzeugungs-, Übertragungs- und Verteilungskette zukünftig auch davon betroffen sein können. Die Gefahr von kriminellen Eingriffen ist folglich nicht nur auf die Smart Grids Komponenten reduziert, sondern sie breitet sich auf das gesamte System aus. Billing-Systeme, Fahrpläne von Kraftwerken, Demand Side Management und andere Prozesse sind der Möglichkeit ausgesetzt durch externes Einwirken mit dem Ziel der Zerstörung oder krimineller Bereicherung vereinnahmt zu werden.
Um diese Lücke zu schließen müssen sowohl technische als auch organisatorische Maßnahmen in den Firmenorganisationen implementiert werden. Die Verwendung von approbierten Standards aus der IT- Welt, wie COBIT, ISO2700x oder IT-Governance kann helfen, die aktuelle Lage zu verbessern und den Takt für die Lösung der aufkommenden Herausforderungen vorzugeben. Zusätzliche Standards, die sich nur auf die Smart Grids Bereiche beziehen, müssen ebenfalls implementiert werden. Einige dieser Standards werden aktuell durch Gerätehersteller forciert, andere wiederum werden durch regulative Zielsetzungen notwendig. Zusammenfassend kann gesagt werden, dass von all diesen genannten Möglichkeiten nur ein geringer Teil bei den entsprechenden Organisationen implementiert wurde. Es besteht folglich Handlungsbedarf um die vorhandene Sicherheitssituation zu verbessern.

Ziel der Arbeit

Anlass und Ziel dieser Arbeit ist es, das hochrangig besetzte „Strategiegespräch im exklusivem Kreis über die gemeinsame Verantwortung für sichere Smart Grids“ im Rahmen der Smart Grids Week Bregenz 2012 sowohl inhaltlich wie auch organisatorisch vorzubereiten. Als Ergebnis dieses Strategiegesprächs wird erwartet, dass im Rahmen der ausgewählten Diskutanten

- **ein Awareness geschaffen** und die **Kräfte gebündelt werden** (ausgewählte Akteure sind im Bereich Sicherheit: Anwender, Netzbetreiber, Erzeuger, Technologieanbieter, öffentliche Hand)
- **die** sicherheitsrelevanten **Aufgaben identifiziert werden und die Klärung von Verantwortungsbereichen** (Versorger, Anbieter, öffentliche Hand) gelingt, wobei die Kernfrage ist: wer ist für die Sicherheit des Gesamtsystems verantwortlich?
- technologische, ökonomische sowie regulative **Grenzen aufgezeigt** und **mögliche Lösungsstrategien** für die nachhaltige Sicherstellung des Gesamtsystems aus heutiger Sicht aufgezeigt werden
- **ein gemeinsames Commitment** geschaffen wird und eine Übereinkunft für die akkordierte und gemeinsame Sicherstellung der Systemsicherheit erzielt wird

Methode

Die Arbeit wird in 4 Phasen durchgeführt:

Zunächst werden die wichtigsten sicherheitsrelevanten energiewirtschaftlichen Prozesse beschrieben. Dies soll dazu dienen, die Dimension und jeweilige Relevanz der Sicherheitsthematik zu erkennen.
Danach werden die wichtigsten Sicherheitslücken im System aufgezeigt und ihre Auswirkungen bzw. ihre Entstehung beschrieben.
Im nächsten Schritt werden die darauf aufbauenden signifikanten Bedrohungsszenarien dargestellt.
Als letztes werden mögliche Abwehrmaßnahmen entwickelt.

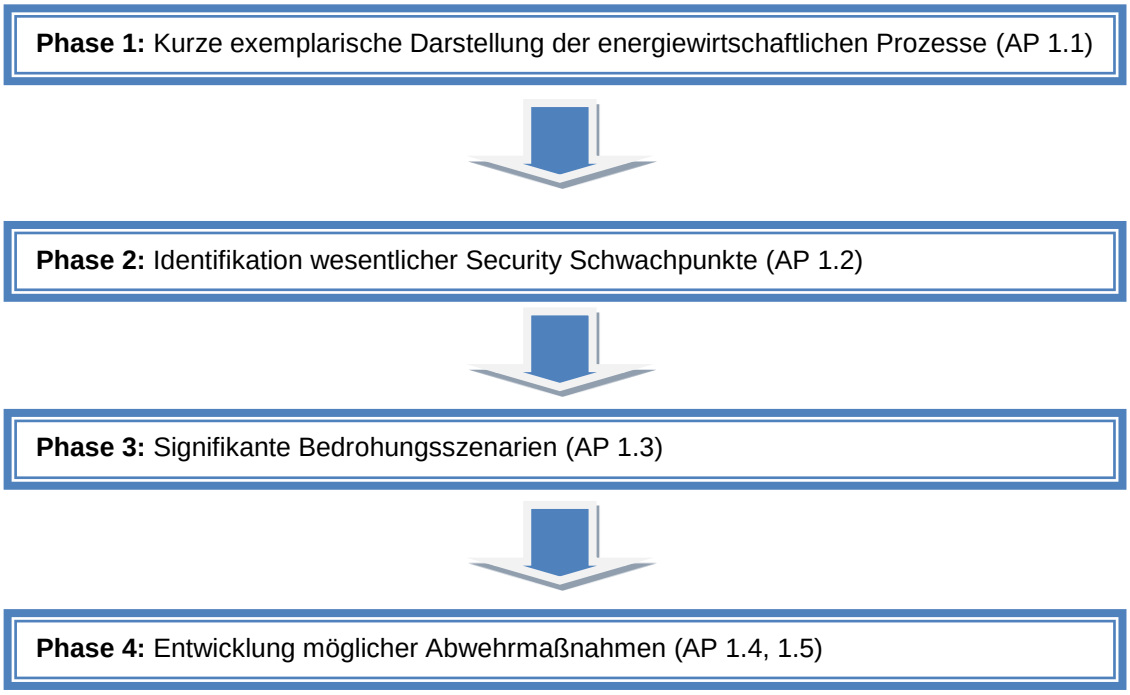

Abbildung 1: Die vier Phasen der Ausarbeitung zur Smart Grids Security

Kurze exemplarische Darstellung der energiewirtschaftlichen Prozesse (AP 1.1)

Die technischen Prozesse in der Energiewirtschaft konzentrieren sich im Wesentlichen auf die Segmente der Erzeugung, Übertragung und Verteilung. Darüber hinaus gibt es weitere Prozesse, nämlich jene von Messstellenbetreibern und -dienstleistern sowie Smart Grids eigene Prozesse, auf die wir im Folgenden näher eingehen werden.

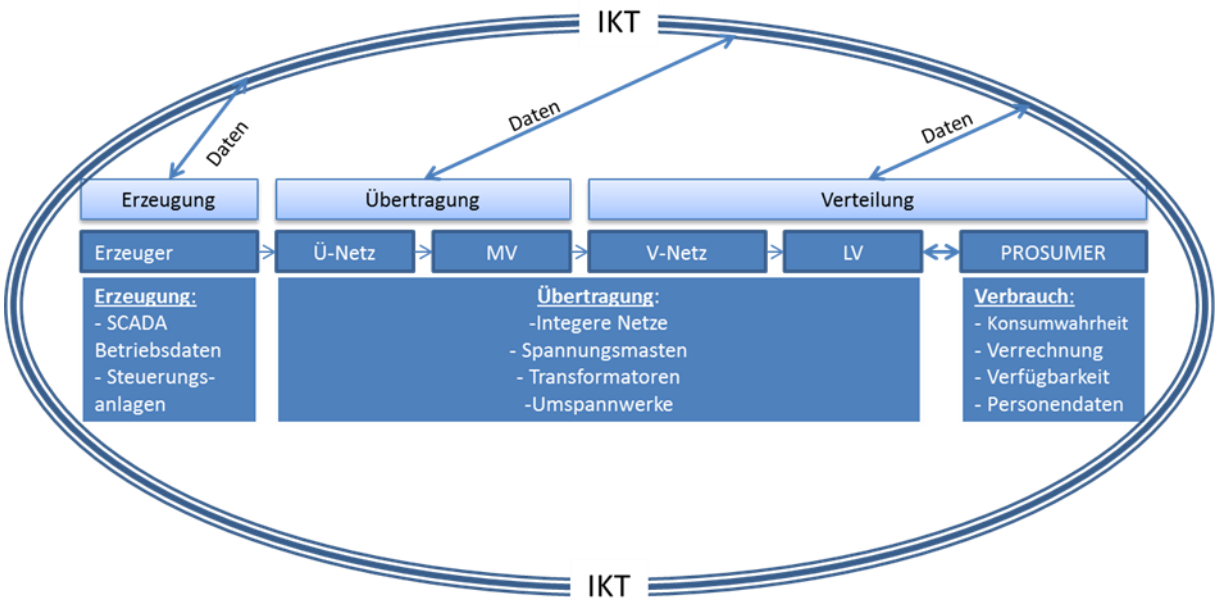

Abbildung 2: Segmente der Energiewirtschaft. In allen Bereichen gibt es potentiell sicherheitsrelevante energiewirtschaftliche Prozesse

Erzeugerprozesse

Als Erzeugerprozesse bezeichnet man jene Prozesse, die zur Energiegewinnung (in der Darstellung nur Strom) durchlaufen werden. Man unterscheidet dabei zwischen technischen und wirtschaftlichen Prozessen. Durch Smart Grids ist das Kommunikationslayer als dritte Säule dazugekommen.
Aus der Sicht von Smart Grids sind alle Prozesse wesentlich bei der Errichtung von geeigneten Sicherheitsmechanismen. Die Vernachlässigung bei der Implementierung von Sicherheitsrichtlinien und Sicherheitsmaßnahmen bei einem Prozess könnte auch den totalen Ausfall der jeweils anderen Prozesse mit sich führen.

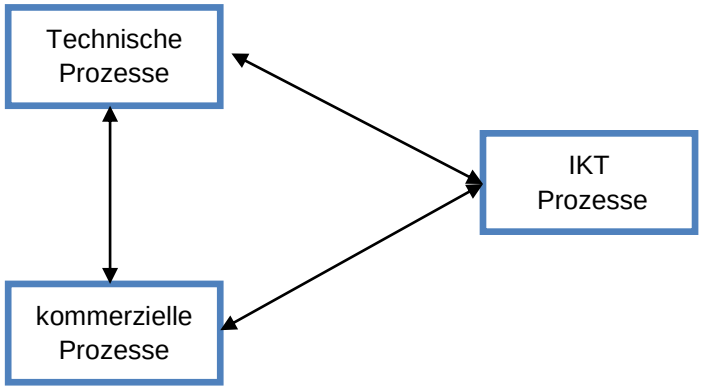

Abbildung 3: Die drei wichtigsten Ebenen der Energiewirtschaft beeinflussen einander stark

Technische Prozesse
Bei den technischen Prozessen unterscheidet man zwischen den thermischen Erzeugungsprozessen, dazu gehören z.B.

- Thermische Kraftwerke (Kohle, Gas, ÖL)
- Solarthermische Prozesse
- Geothermische Prozesse

und den nicht thermischen Erzeugungsprozessen, z .B.:

- Wasserkraft (Flusskraftwerke, Pumpspeicherkraftwerke, Gezeitenkraftwerke)
- Windkraft
- Photovoltaik

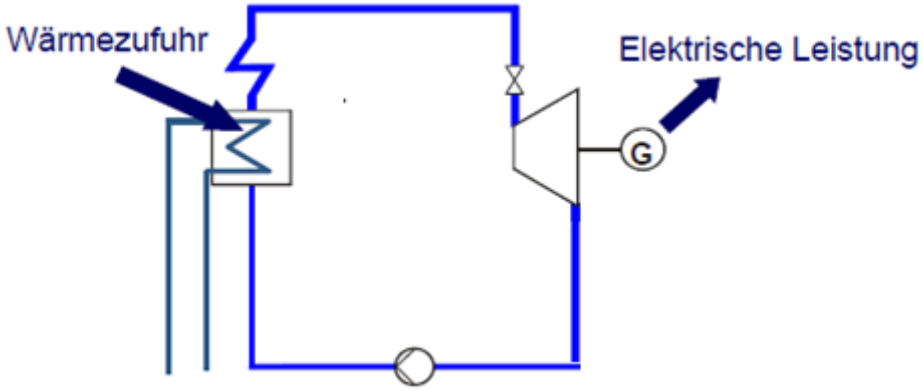

Abbildung 4: Thermoelektrisches Prinzip der Stromerzeugung mit Heizwärmeauskopplung[1]

Alle technischen Prozesse bedürfen diverser Leitsysteme und Betriebssteuerungen. Die Vernetzung dieser Systeme mit der Internetwelt setzt diese Systeme der Angriffsmöglichkeit von extern aus. In der Regel werden Steuerungsprogramme für die leichtere telemetrische Wartbarkeit mit dem Internet oder anderen Kommunikationsnetzen vernetzt.

[1] http://www.ie-leipzig.com/IE/Veranstaltungen/Geothermie/Rohloff.pdf

Wirtschaftliche Prozesse
Neben den aufgezählten technischen Prozessen gibt es übergeordnete wirtschaftliche Prozesse. So kennen wir in Zusammenhang mit der Energieerzeugung folgende Zyklen:

- Fahrplanmanagement oder Kraftwerkseinsatzplanung/Prognose
- Portfoliomanagement
- Zertifikatsverwaltung/Emissionshandel

1) Kraftwerksmanagement

Kraftwerksmanagement liefert Lösungen für den sinnvollen Einsatz von Kraftwerken. Der Kraftwerkseinsatz hat einen direkten Einfluss auf die Nutzung der elektrischen Netzwerke.
In ein elektrisches Netz darf nur so viel elektrische Energie eingespeist werden, wie gerade von den Verbrauchern benötigt wird. Kleinere Abweichungen führen zur Änderung der Netzfrequenz, größere können großräumige Stromausfälle verursachen. Änderungen in der Menge an elektrischer Energie können nur durch verlustbehaftete Umwandlung in andere Energieformen gespeichert werden. Zur Spitzenlastabdeckung wird deshalb in Pumpspeicherkraftwerken oder Druckluftspeicherkraftwerken elektrische Energie in andere Energieformen umgewandelt und zwischengespeichert. Da diese Speicherung elektrischer Energie in großen Mengen unwirtschaftlich ist und nur für den Spitzenbedarf oder für Lastverschiebungen dient, müssen gewisse Kraftwerkskapazitäten jederzeit bereit stehen. Geeignet dafür sind nur Kraftwerkstypen mit kurzen Anfahrzeiten. Unter der Betrachtung der Smart Grids Thematik sind Kraftwerke mit kurze Anfahrzeiten viel mehr gefragt.

Smart Grids Funktionalitäten kann man auf allen Spannungsebenen integrieren. Nur eignen sich bestimmte Kraftwerketechnologien für bestimme Spannungsebenen besser. So werden Pumpspeicherkraftwerke im großen Stil eher bei höheren Spannungseben zu finden sein und kleine Blockheizkraftwerke eher in den Verteilernetzen. Wesentlich ist, dass sie alle ein Fahrplanmanagement benötigen. Das Zu- oder Wegschalten kann dabei automatisch (Voraussetzung: „Intelligenz“ des Erzeugers, vermehrte Nachfrage im Wirkungsbereich, u.a.) geschehen. Das Fahrplanmanagement orientiert sich auf zumindest drei Bezugsgrößen.

1) Leistungsnachfrage
2) Prognosen
3) Wirtschaftlichkeit

Betrachtet man das nun aus dem Blickwinkel der Sicherheit, so findet man in allen Bereichen IKT-Komponenten. Diese bilden gleichzeitig Einstiegspunkte für mögliche Beeinflussung. Wirtschaftlich gesehen würden solche Eingriffe enorme Kosten verursachen. Technisch gesehen natürlich auch, hinzu kommt aber die Gefahr, dass das System aus dem Rhythmus gebracht werden kann, so dass ein Ausgleich aus Erzeugung und Verbrauch nur schwer wieder herzustellen sein könnte. Sicherheitskonzepte und Resilienzstrategien aus Sicherheitssicht werden notwendig sein um diesen Bereich besser zu schützen.

2) Portfoliomanagement[2]

Unter Portfoliomanagement versteht man die Zusammenstellung und Verwaltung eines Portfolios, d. h. eines Bestandes an Investitionen, im Sinne der mit dem Investor vereinbarten Anlagekriterien, insbesondere durch Käufe und Verkäufe mit Blick auf die erwarteten Marktentwicklungen. Es können zwei Grundstrategien unterschieden werden:

[2] http://de.wikipedia.org/wiki/Portfoliomanagement

Der Top-Down-Ansatz (von oben herab) geht von den Zielen aus und versucht auf deren Basis die Strategie festzulegen. Die Strategie ergibt sich aus der Analyse und der darauf aufbauenden Entscheidung. Daraus ergibt sich die Taktik, welche abschließend von der Performanceanalyse untersucht wird. Den umgekehrten Weg nennt man Bottom-Up-Ansatz.

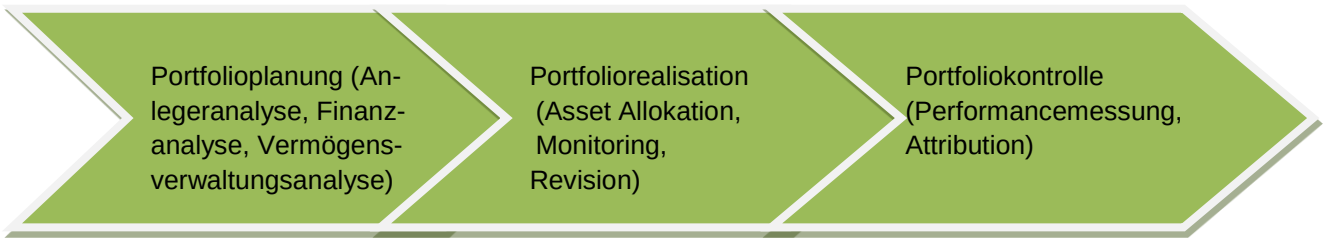

Abbildung 5: Der Portfoliomanagement-Prozess hat drei grundlegende Schritte

In der Energiewirtschaft besteht ein Portfolio aus einem Mix aus Stromprodukten, das vordefiniert ist und entsprechenden Kriterien entsprechen muss. In den meisten Fällen wird eine bestimmte Energiemenge oder Leistung zu einem bestimmten Preis über einen vereinbarten Zeitraum in das Netz eingespeist. Der Verbraucher kauft das Produkt dann übereinstimmend mit den vorgegebenen Rahmenbedingungen

Renewable Portfolio Standard (RPS)
Ein Renewable Portfolio Standard (RPS) ist eine Zusammenstellung an Stromprodukten, die sich aus erneuerbaren Energiequellen, wie Wind, Solar, Biomasse und Geothermie ergibt. Andere gebräuchliche Bezeichnungen für das gleiche Konzept sind Renewable Electricity Standard (RES) in den Vereinigten Staaten und Renewables Obligation in Großbritannien.
Der RPS-Mechanismus verpflichtet die Energieversorger, einen gesetzlich definierten Prozentsatz ihres Strommix aus erneuerbaren Ressourcen zu beziehen.

Betrachtet man die Abbildung über den Portfoliomanagement-Prozess kritisch, kann der größte Schaden durch die Manipulation des zweiten Schrittes, der Portfolio-Realisation erfolgen. Die anderen beiden Prozessschritte können ebenfalls manipuliert werden, die Auswirkungen sind jedoch geringer als beim zweiten Schritt. Werden falsche Produkte durch Manipulation allokiert, so ist der wirtschaftliche Schaden, der dadurch entsteht, groß. Hacker mit dem entsprechenden Fachwissen können in eine Handelsplattform eindringen und das System beschädigen. Der Nachweis über richtige oder falsche Portfolios ist bei nachträglicher Veränderung nicht sehr einfach. Viel mehr als die Hacker, ist aber hier das kriminelle Handeln ein höheres Risiko. Wir werden diese Thematik bei den Bedrohungsszenarien nochmals aufgreifen.

3) Zertifikatsverwaltung[3]

Der Emissionsrechtehandel, kurz Emissionshandel oder auch Handel mit Emissionszertifikaten, ist ein Instrument der Umweltpolitik mit dem Ziel, Schadstoffemissionen mit möglichst geringen volkswirtschaftlichen Kosten zu verringern. In der Europäischen Union wurde der EU-Emissionshandel für Kohlenstoffdioxidemission 2005 gesetzlich eingeführt, wobei die Vorstellung des Emissionshandels bereits 1968 von John Harkness Dales entwickelt worden ist.

[3] http://de.wikipedia.org/wiki/Emissionsrechtehandel

Der Emissionsrechtehandel wird zu den marktwirtschaftlichen Instrumenten der Umweltpolitik gezählt.
Der Emissionsrechtehandel wird zu den Mengenlösungen gezählt, weil die Politik hier eine konkrete Menge für eine bestimmte Emission vorgibt. Somit entfällt die problematische Festlegung der Höhe des Steuersatzes und die Politik kann das Umweltziel direkt beeinflussen. Man spricht daher auch von einer hohen ökologischen Treffsicherheit des Emissionsrechtehandels. Jedoch sind die Preisentwicklung und damit die Belastung von Unternehmen und Verbrauchern schwierig zu prognostizieren.
Die Ausgabe der Zertifikate kann grundsätzlich in zwei Formen unterschieden werden:

- Zuteilung durch die Politik sowie
- Versteigerung.

Bei der Zuteilung durch die Politik wird politisch festgelegt, wer wie viele Zertifikate erhält. Diese Ausgabeform ist nur sinnvoll, wenn es objektive Kriterien für die Zuteilung gibt, da sonst die Gefahr besteht, dass politisch einflussreiche Interessengruppen begünstigt werden. So können zum Beispiel im Rahmen eines internationalen Emissionsrechtehandels, bei dem es darum geht, Schadstoffemissionen mit globalen Auswirkungen (zum Beispiel Treibhausgase) auf die teilnehmenden Staaten zu verteilen, die Zertifikate entsprechend der Einwohnerzahl zugeteilt werden. Staaten mit einem hohen Verbrauch an fossiler Energie müssten dann Zertifikate bei Staaten mit geringem Energieverbrauch nachkaufen.

Emissionsrechtehandel bei Treibhausgasen[4]

Momentan gibt es zwei Handelssysteme für Treibhausgase: Den im Kyoto-Protokoll vereinbarten bilateralen Handel zwischen Annex-I Staaten und innerhalb Europas den EU-Emissionshandel für Unternehmen.
Ausgangspunkt ist die Erkenntnis, dass viele Schadstoffe nicht nur lokal wirken, sondern großräumig, so dass die Minderung von Emissionen nur über große geographische Räume betrachtet und bewertet werden kann.

Ähnlich wie beim vorherigen Kapitel zum Portfoliomanagement kann kriminelles Handeln mit Ökozertifikaten ebenfalls einen wirtschaftlichen Schaden bringen. Dabei können gefälschte Zertifikate in Umlauf gebracht werden. Ähnliche Fälle gab es bereits vermehrt in anderen Branchen[5].

Netzbetreiber

Während die technischen Prozesse mit der Erhaltung der Netzqualität (Spannung, Frequenz, Leistung, u.a.) zu tun haben, definieren und regulieren die ökonomischen Prozesse die Netznutzung sowie die hinterlegte Bilanzierung und Abrechnung. Folgende Prozesse werden dabei durchlaufen:

- Fahrplanmanagement
- Zeitreihenmanagement
- Abrechnung Bilanzkreise

[4] http://de.wikipedia.org/wiki/Emissionsrechtehandel
[5] http://www.taz.de/!82846/

Fahrplanmanagement
Wie beim Kraftwerkseinsatz ist es notwendig die Netze auf die nachgefragte Leistung und Energiemenge einzustellen. Je nach Netzleistung und Netzverfügbarkeit gibt es unterschiedliche Fahrpläne, die auch die Kraftwerkeinsatzplanung beinträchtigen und umgekehrt. Die wichtigste Aufgabe des Fahrplanmanagements aus Netzsicht ist es, das Netz nicht zu überlasten und die Netzressourcen so optimal wie möglich zur Verfügung zu stellen. Die Lastprofile müssen einen Tag vorher beim Netzbetreiber angemeldet werden. Kurzzeitige Kapazitäten können stündlich, halbstündlich oder viertelstündlich zur Verfügung gestellt werden. Über den Engpasshandel können Übertragungskapazitäten erworben werden.

Unter der Betrachtung von Smart Grids können diese Prozesse auch automatisiert stattfinden. Sicherheitssysteme sind folglich notwendig, damit das Netz nicht absichtlich überbelastet wird oder, was noch schlimmer wäre, zum Zusammenbruch gebracht wird, indem wichtige Netzabschnitte durch Hackerangriffe blockiert werden.

Abrechnung und Bilanzkreise[6]
Bilanzkreis ist ein energiewirtschaftlicher Fachausdruck. Im liberalisierten Strommarkt werden Stromlieferanten und Stromkunden in Bilanzkreisen (in Österreich und der Schweiz Bilanzgruppen genannt) zusammengefasst. Bilanzkreise sind virtuelle Energiemengenkonten, die von den Übertragungsnetzbetreibern (ÜNB) geführt werden, um Händlern oder bilanzverantwortlichen Endkunden die Möglichkeit zu geben, alle tatsächlichen Einspeisungen und Entnahmen innerhalb eines Regelgebietes zu saldieren.
Da die dazu notwendige Lastprognose mit einer gewissen Unsicherheit behaftet ist, kommt es praktisch immer zu Abweichungen zwischen der Einspeisung des Lieferanten und der tatsächlichen Abnahme der Kunden. Diese Abweichung wird durch den Übertragungsnetzbetreiber durch Ausgleichsenergie, teilweise auch mit Regelenergie (um die Regelzone bezüglich Spannung und Frequenz stabil zu halten) ausgeglichen. Die Ausgleichsenergie stellt der Übertragungsnetzbetreiber (in Österreich spricht man vom „Regelzonenführer“) dem Lieferanten in einer Bilanzkreisabrechnung in Rechnung.

Bei der Abrechnung der Bilanzkreise besteht die Gefahr der organisierten Kriminalität bzw. dass Kundendaten illegal entwendet werden können. Eine automatisierte Abrechnung kann durch Manipulation die Kunden zu Gunsten eines Anderen unterschiedlich belasten.

Verteilnetzbetreiber
Die Prozesse eines Verteilnetzbetreibers können wie folgt dargestellt werden:

- Zeitreihenmanagement, Vertragsmanagement
- Netzbilanzierung/Bilanzkreismanagement
- Abrechnungsvorbereitung Netznutzungsentgelte/Schattenrechnung (Lieferant)
- Lieferantenwechsel
- Netzprognose
- Messstellenbetrieb

Der Verteilnetzbetreiber hat insofern die größte Exposition, als das im Verteilnetz verschiedene Akteure von dezentralen Energieerzeugern, über Messdienstleister bis zum Konsumenten alle aktiv sind, Daten untereinander austauschen und über automatisierte Systeme verfügen können. Die Angriffsvektoren sind folglich vielfältig. Nicht nur dass das Netz durch

[6] http://de.wikipedia.org/wiki/Bilanzkreis

Manipulation der Lastprofile absichtlich beschädigt werden könnte, kann es auch dazu kommen, dass Kundendaten gestohlen oder dass gehackte Lastprofile einzelner Haushalte für sekundäre Kriminalhandlungen weiterveräußert werden könnten.

Smart Grids relevante Daten und Prozesse, die IKT-Ebene

Betrachtet man nun die vorher beschrieben Funktionen und Aufgaben der verschiedenen Akteure im Energiesystem kommt die Frage auf, welche Prozesse denn nun eigentliche Smart Grids Prozesse sind.
Smart Grids Prozesse kommen in allen Energiewirtschaftssegmenten und Spannungsebenen vor. Sie sind für diese unterschiedlichen Ebenen und Segmente unterschiedlich definiert und erfüllen Aufgaben durch Verwendung von IKT-Komponenten.
Wie in der Abbildung 2 auf Seite 7 dargestellt, fallen in allen Energiewirtschaftssegmenten Daten an. Um eine Automatisierung zu ermöglichen, also ein „Internet der Energie“ zu gestalten, müssen diese Daten erfasst, übertragen, verarbeitet und gespeichert werden. Anbei finden wir eine Übersicht der verschiedenen Datentypen, die von Smart Grids Anwendungen verwendet werden können. Man kann erkennen, dass nicht nur technische Daten in Betracht kommen, sondern auch zusätzlich Daten aus dem Wirtschaftsbereich sowie Wetterdaten, je nachdem, welche Applikation eingesetzt wird.

Personendaten

Datentypus	Verwendung für
Name, Vorname, Anschrift	Personenkennung, Adressenzuweisung, Zugehörigkeit von Geräten Unterscheidung städtischer oder ländlicher Bereich
Alter	Nutzerverhalten: Kind, Erwachsener, Pensionisten
Beruf	Verweildauer in Gebäuden

Energiespezifische technische Daten

Datentypus	Einheit	Wertdarstellung
Temperatur	In °C	Raumtemperatur, Außentemperatur, Wassertemperatur
Durchfluss	Liter/s, m^3/s	Wärmeströmung, Wärmemenge
Spannung	V	Photovoltaik Spannung, Spannung als Messgröße für Sensoren (Druck, Frequenz, etc.)
Strom	A	Leistungsermittlung aus Photovoltaik oder anderen Dezentralen Energieerzeugern Als indirekte Messgröße Als Indikator für Stromkonsum bei Geräten
Leistung	W	Zur Messung aller leistungsbezogenen Größen
Widerstand	Ω	Als direkte oder indirekte Messgröße
Speicherkapazität Strom	KWh	Stromspeicher als Batterie, Kondensator, Pumpspeicherkraftwerke, etc.
Speicherkapazität Gas	m^3	Speicherkapazität für Gas
Speicherkapazität für Wärme	KWh	Speicherkapazität für Warmwasser und Heizsysteme

Wetterdaten

Datentyp	Einheit	Informationsgehalt
Sonneneinstrahlung	W/m^2	Leistung zur Berechnung der Erzeugerleistung von Solarthermie und Photovoltaik
Wind	km/h	Zur Bestimmung des Winddargebots
Helligkeit	Lux	Zur Abschätzung der verfügbaren Sonneneinstrahlung

Energiewirtschaftliche Daten

Datentyp	Einheit	Informationsgehalt
Erzeugung	kWh, MWh	Erzeugte Energiemenge, die in das System eingespeist wird (Dezentrale Erzeugung, Fremdbezug)
Verbrauch	kWh,MWh	Verbrauchte Energiemenge im Haus, Bezirk, Stadtteil, Stadt, Region
Strompreis	€/kWh	Marktwert Strom
Gaspreis	$€/m^3$	Marktwert Gas
Warmwasserpreis	$€/m^3$	Marktwert für Warmwasser und Heizung
Leistungsnachfrage	MW	Nachgefrage Leistung
Übertragungskosten	€/kWh	Transportkosten Strom, Gas, Wärme

Gerätedaten

Datentyp	Einheit	Beschreibung
Hersteller		Name des Herstellers für sämtliche Geräte und Anlagen (€CO2 Manager, Solaranlagen, Wärmepumpen, Sonnenkollektoren, etc.)
Baujahr		Jahr der Erzeugung
Erzeugerkapazität	kWh, MWh	Produzierbare Menge an Energie
Leistung	kW, MW	Verfügbare Leistung installierter Geräte
Versionsnummer		Versionsnummer der installierten Betreibersoftware
Schnittstellendaten, Übertragungskapazität	Byte/s	Zur bidirektionalen Übertragung der Informationen diverser Geräte und Erzeugungsanlagen
Steuerdaten, Regeldaten		Diverse Schaltzustände oder Regelgrößen für dezentrale Einheiten

Netzdaten

Datentyp	Beschreibung
Spannung	Spannungslevel
Frequenz	Aktueller Zustand des Übertragungsverhaltens des Netzes
Kapazität	Ausnutzung der Netzkapazität

Für alle hier dargestellten Daten gibt es Sensoren oder Messeinheiten, welche diese Daten erfassen. Die Übertragung erfolgt dann über verschiedene Medien. Die Übertragungsmedien für Smart Grids Daten hängen im Wesentlichen von der Entfernung ab, die es zu überbrücken gilt und von der Wiederholfrequenz der Ablesezyklen. Als technologische Basis für die Datenübertragung gilt das ISO-OSI Referenzmodell. Übertragungsverfahren nutzen für die Übermittlung der Daten auch verschiedene Übertragungsprotokolle. Diese helfen, dass Sender und Empfänger die gleiche Information erhalten und „verstehen".

Ein wichtiger Aspekt für die Nutzung des Protokolls ist die Unterstützung verschiedener Übertragungsverfahren. Man unterscheidet zwei wesentliche Verfahren, das Push- und das Pull-Verfahren.
Beim Push-Verfahren senden alle Stationen in einem vorgegebenen Takt ihre Daten an die Zentrale bzw. den Datenkonzentrator. Dieses geschieht vollautomatisch ohne Verwendung eines Broadcastsignals. Geht man dabei davon aus, dass sich die Forschungsgruppen auf einen standardisierten Ablesezyklus für Smart Meter (hier nur als Beispiel zur Veranschaulichung der Datenvolumina) von 15 Minuten einigen, müssen je nach Versorgungskreis circa 250.000 Zähler innerhalb von 15 Minuten abgelesen werden. In diesem Fall bietet sich das Push-Verfahren an, da vorhersehbar ist, wann welcher Zähler zu senden hat und welche Daten übertragen werden müssen. Dieses Verfahren setzt jedoch eine ausreichende Bandbreite voraus. Setzt man eine Paketgröße von 200 Byte als gegeben voraus sowie eine gleichmäßig verteilte Sendewelle innerhalb der 15 Minuten, würde dies eine Bandbreite von: Bandbreite MBit/s = (200*8*250.000)/(1024²*15*60) = 0,42 MBit/s voraussetzen.
Dies stellt für einen marktüblichen DSL-Anschluss mit ca. 6 MBit/s keine Schwierigkeit dar. Setzt man die gleichen Vorgaben voraus, geht aber auf einen ein-minütigen Ablesezyklus, kann man von einer Belastung von: Bandbreite MBit/s = (200*8*250.000)/(1024²*60) = 6,36 MBit/s ausgehen. Auch diese Bandbreite ist durchaus mit einer Vielzahl von Medien zu bewerkstelligen. Jedoch werden durch das Push-Verfahren nur die für die Abrechnung zwingend notwendigen Daten übertragen.
Zusätzlich gibt es die Möglichkeit weitere Informationen des Zählers anzufordern. Dazu müssen die Protokolle auf ein entsprechendes Signal hin reagieren können. Bei diesem Verfahren wird also die Leitstelle aktiv, fordert eine Information an, ein entsprechendes Broadcastsignal wird an die Messgeräte oder -gruppen verschickt, die dann, neben dem Betrieb (Übertragung der normalen Messdaten), die gewünschten Daten an die Leitstelle schicken.
Für die Übertragung der Messdaten eignet sich das Push-Verfahren besser, da weniger Daten übertragen werden müssen (Request entfällt) und auch die Einbindung in die Daten- und Zugriffssicherheit unkomplizierter erfolgen kann. Ein weiterer Nachteil des Pull-Verfahrens (außer generelles Broadcast) ist die Notwendigkeit, die Adresse des Zählers zu kennen.[7]

[7] http://winfwiki.wi-fom.de/index.php/Smart_Metering_-_Revolution_der_Messtechnik_in_der_Energiebranche%3F#.C3.9Cbertragungsverfahren

Übertragungstechnologien
Bei der Bewertung des geeigneten Fernübertragungsweges müssen die grundlegende Strategie und die lokalen bzw. regionalen Gegebenheiten des Anbieters beachtet werden. Abhängig von der Bevölkerungsdichte und der Erschließung der Region mit bestehenden Telekommunikationsnetzen ist beispielsweise in ländlichen Gebieten ohne DSL-Netz und aufgrund der relativ geringen Nutzeranzahl auch ohne Powerline-Communication eine Übertragung über die relativ teure GSM-Mobilfunkkommunikation die optimale Technik. In Städten ist dagegen die Kommunikation via DSL, GPRS oder PLC vorteilhafter.

DSL
Aufgrund der geringen Ausgaben für die Realisierung des Datentransports über DSL (Digital Subscriber Line) sowie der rasanten Migration von der Schmalbandigkeit hin zur Breitbandigkeit, kommt dem DSL eine besondere Bedeutung zu.

PLC
Powerline Communication als Datenübertragungsverfahren über das Stromnetz zwischen der Trafostation und dem Hausnetz ist in Deutschland bisher nur wenig verbreitet. Grundsätzlich können über die Powerline-Technologie in einem Umkreis von 350 m um eine Trafostation herum maximal 100 bis 300 Haushalte mit einer maximalen Bandbreite von bis zu 3 Mbit/s versorgt werden. Die Praxis zeigt allerdings, dass die mit Powerline erzielbare Datenrate deutlich niedriger ist, da die maximale Datenrate von der Nutzeranzahl maßgeblich abhängt.

GPRS
"General Packet Radio Service" baut im Wesentlichen auf das bestehende GSM-Netz auf. Es handelt sich dabei um ein Verfahren, Datenpakete mittels Kanalbündelung einzeln zu übertragen. Es besteht somit nur virtuell eine stetige Verbindung zum Server. Jedoch wird das Netz nur während der Übertragung der Pakete belastet. Die Zählermodems vom Typ ZDUE-GPRS-PLUS-IV sind via virtueller Standleitung permanent mit der Leitstelle verbunden. Der zeitaufwendige Verbindungsaufbau vor jedem Auslesevorgang entfällt.

Die Gegenüberstellung der drei Übertragungstechnologien liefert Klarheit über die Möglichkeiten und Grenzen.

Ausgangswerte (Paketgröße = 200 Byte)			Stromleitung via PLC		Funknetz via GSM/GPRS		Telefonnetz via DSL	
Anzahl Ablesungen	Ablesezyklus	nötige Bandbreite	max. Bandbreite	Tauglichkeit	max. Bandbreite	Tauglichkeit	max. Bandbreite	Tauglichkeit
250.000	15-minütig	434,03 kbit/s	3 Mbit/s	ja	171,2 kbit/s	nein	6 Mbit/s	ja
150.000		260,42 kbit/s		ja		nein		ja
50.000		86,81 kbit/s		ja		ja		ja
250.000	1-minütig	6,358 Mbit/s	3 Mbit/s	nein	171,2 kbit/s	nein	6 Mbit/s	nein
150.000		3,815 Mbit/s		nein		nein		ja
50.000		1,272 Mbit/s		ja		nein		ja

Tabelle 1 Gegenüberstellung der Übertragungstechnologien für Smart Grids Daten (in diesem Fall Smart Meter Daten)

Prozesse
Durch die festgehaltenen technologischen Möglichkeiten lassen sich nun verschiedene Prozesse im Smart Grids Bereich definieren. Da die Anwendungen sehr vielfältig sein können, beschränken wir uns hier nur auf zwei Prozesse, den Technischen und den Ökonomischen.

Technischer Prozess
Im Folgenden werden zwei einfache Prozesse einer Smart Grids Applikation dargestellt, wobei im ersten Fall eine Smart Grids Funktionalität nicht unbedingt notwendig sein muss. Will man aber diesen Prozess automatisch und telemetrisch anstoßen, so muss wieder die IKT-Komponente den Datenerfassungsprozess übernehmen. Im zweiten Fall wird ein Smart Grids Kunde für das System als steuerbare Last gesehen und bei vorhandenen Lastspitzen abgeworfen.

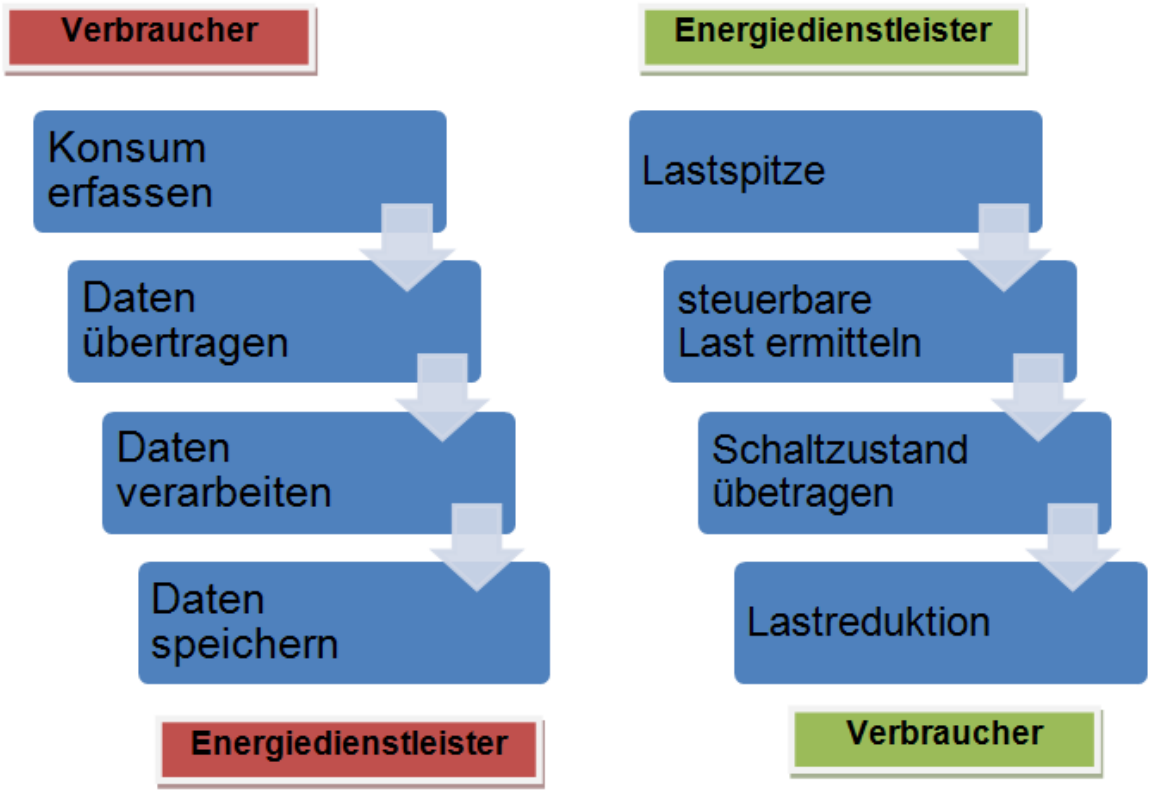

Abbildung 6: Darstellung von zwei einfachen Smart Grid Prozessen

Tarifabhängige Laststeuerung

Unter tarifabhängiger Laststeuerung versteht man die Möglichkeit, dass sich verschiedene Verbraucher auf Basis der Tarifentwicklung an das System zu- oder wegschalten. Speziell im Home Area Bereich werden solche Konzepte für die Reduktion von Lasten in der Spitzenlastperiode verwendet. Dabei geben die Verbraucher (meist über das Verbrauchsgerät selbst) vor, bis zu welchem Preis das Gerät eine Funktion ausüben soll. Tarife, die über einen Schwellwert hinausgehen, werden dem Gerät kommuniziert und der Gerätebetreiber entscheidet, ob er dennoch den Betrieb des Gerätes fortführen (starten) will oder nicht.

E-Mobility Ladeprozesse

Elektrofahrzeuge sind im Smart Grids Kontext eine wichtige Komponente. Zum Einen verschaffen sie bei Einspeisung durch Strom aus erneuerbaren Quellen die Möglichkeit einer CO_2-reduzierten Mobilität, zum Anderen können sie als vorübergehende Stromspeicher zur Verfügung stehen.

Lade- und Entladeprozesse müssen jedoch gesteuert werden. Nicht alle Akkumulatoren, die in verschiedenen E-Cars verwendet werden, sind gleich. Zudem sind die Ladezyklen auf-

grund von Altersmüdigkeit der Akkumulatoren nicht unendlich und daher beschränkt. Die Verfügbarkeit des Elektroautos als Speicher bedarf noch zusätzlich der geeigneten Use Cases und Business Cases. Diese werden gegenwärtig von verschiedenen Forschungseinrichtungen in Verbindung mit der Autoindustrie erforscht.

Ein exemplarischer Ladevorgang für Lithium Polymer-Akkumulatoren kann folgendermaßen aussehen[8]:
Neue Lithium-Polymer-Akkumulatoren werden vom Hersteller vorgeladen ausgeliefert, um eine schädliche Tiefentladung bis zum Einsatz zu vermeiden. Vor dem Ersteinsatz sollten die Zellen/Batterien mit einem geeigneten Ladegerät vollgeladen und eventuelle Spannungsdifferenzen zwischen den Zellen ausgeglichen (balanciert) werden.

Lithium-Polymer-Akkumulatoren reagieren bei Überladung wesentlich empfindlicher als andere Akkutypen (bis hin zur Zerstörung durch Brand) und werden dadurch meist unbrauchbar. Als Maximalspannung wird häufig 4,2 V angegeben, als Minimum 3 V. Aufgrund der Gefahren beim Überladen müssen spezielle Ladegeräte verwendet werden.

Da sich bei tiefen Temperaturen generell die Beweglichkeit der Elektronen verringert und viele Lithium-Polymer-Akkumulatoren unterhalb des Gefrierpunktes unbrauchbar werden, ist meist eine Lagerung/Gebrauch oberhalb 10°C empfohlen. Die durch den inneren Widerstand der Zellen beim Laden auftretenden Verluste führen zur Erwärmung. Daher wird oft beim Laden eine Temperaturüberwachung/Kühlung verwendet.

Der Ladevorgang erfolgt üblicherweise nach dem I/U-Verfahren zunächst mit konstantem Strom von typischerweise 1 C (bei geeigneten Zellen bis zu 6 C). Die Abkürzung „C“ steht hier für die Stromstärke "Kapazität geteilt durch eine Stunde (1 h)" und ist nicht mit der Einheit Coulomb zu verwechseln. Ein Ladestrom von 1 C bedeutet: Eine Zelle, deren Kapazität z.B. mit 2 Ah angegeben ist, wird mit einem Ladestom von 2 A geladen.

Erreicht eine Zelle die Maximalspannung, wird mit konstanter Spannung weitergeladen (um die Maximalspannung nicht zu überschreiten), wobei der Ladestrom langsam absinkt. Ist er auf ein festgelegtes Minimum (z.B. 5 Prozent des ursprünglichen Ladestroms) gesunken, so gilt die Ladung als beendet und die Zelle als voll.

Im Vergleich zu NiCd- oder NiMH-Akkus haben LiPo-Akkus nur eine geringe Selbstentladung und können ein bis zwei Monate ohne nennenswerten Ladungsverlust gelagert werden. Für Langzeitlagerung empfehlen einige Hersteller das (teilweise) Entladen und die Lagerung an einem kühlen Ort.

[8] http://de.wikipedia.org/wiki/Lithium-Polymer-Akkumulator

Zusammenfassung AP 1.1

Bisher bestand die Energieversorgung im Wesentlichen aus sehr gut gekapselten, technisch wie informationstechnisch sehr gut ausgereiften Teilsystemen, die in geschlossenen Kreisen kommunizieren. Damit sind diese Systeme inhärent relativ sicher. Die neue Generation der Smart Grids Technologien hingegen verlangt eine Öffnung der Informationsnetze ins „Internet der Energie“ und ist dadurch sehr viel vulnerabler, und die Auswirkungen etwaiger Attacken ist sehr viel gravierender als in herkömmlichen Energieversorgungsstrukturen.

Früher

Mit Smart Grids

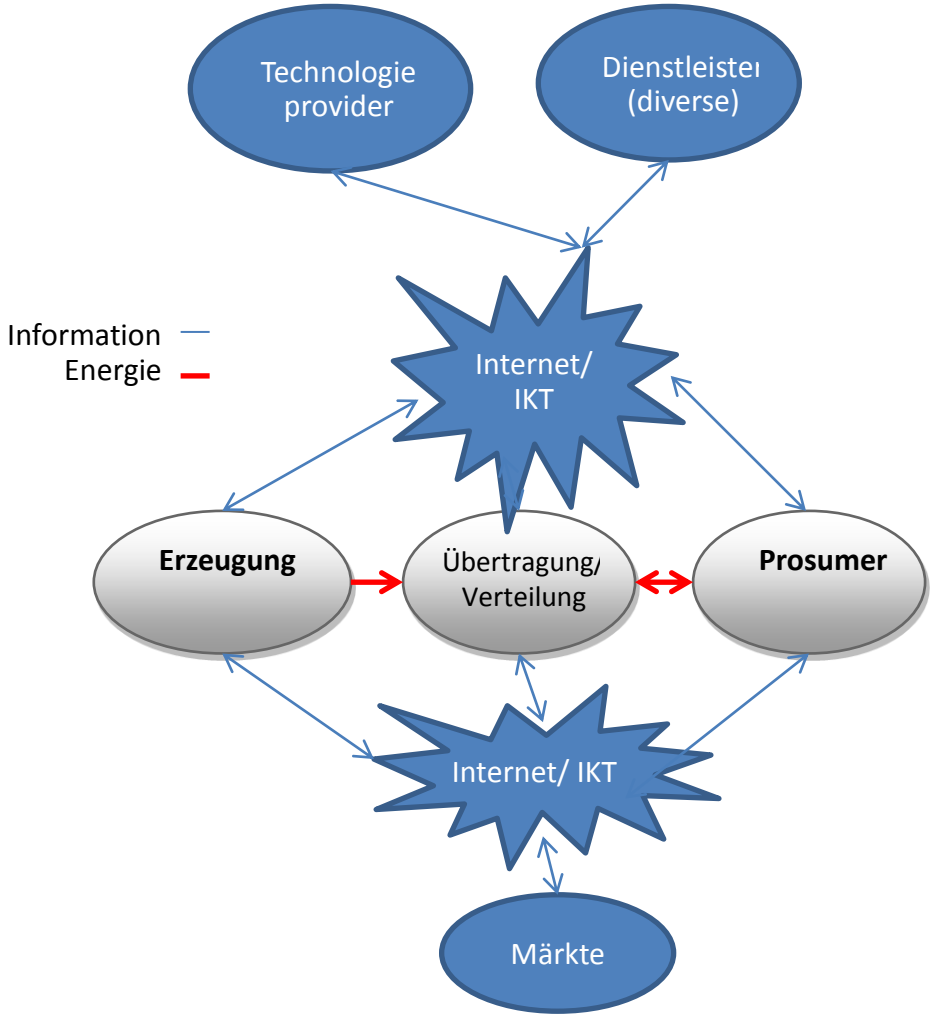

Abbildung 7: Vergleich der Energiesysteme früher und mit Smart Grids

Identifikation wesentlicher Security Schwachpunkte (AP 1.2)

Man kann unschwer erkennen, dass die Einbindung von IKT-Elementen auch unterschiedliche Schwierigkeiten bei der Errichtung eines sicheren Systems mit sich bringt. Aus der Finanz- und Bankenwelt wissen wir, dass der Schutz der Daten (Kundendaten, Kontonummern, Umsätze, usw.) die höchste Priorität genießen muss. Im nachfolgenden Kapitel gehen wir auf diese Thematik ein. Dabei untersuchen wir die personenbezogenen Daten im Smart Grids Kontext genauso wie die auf uns zukommende Datenflut durch den vermehrten Einsatz von Smart Metern und deren Ablesefrequenz. Danach gehen wir kurz auf die Problematik der Datenweitergabe und die notwendige Sicherheit der Endgeräte ein.

Personenbezogene Daten im Smart Grid[9]

Das Datenschutzrecht schützt als einfache gesetzliche Ausgestaltung des Rechts auf informationelle Selbstbestimmung die „Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“. Da das Recht auf informationelle Selbstbestimmung nur natürliche Personen vor der Preisgabe ihrer Daten schützt, gilt das Datenschutzrecht nur für personenbezogene Daten. Klärungsbedarf besteht daher zunächst hinsichtlich der Frage, ob die im Smart Grid verwendeten Daten einen Personenbezug aufweisen, wobei auch auf die Veränderungen durch den Einsatz des Smart Meters und die dadurch geschaffenen Gefährdungslagen eingegangen wird.

Grundsätzlich handelt es sich bei den Messdaten zur Abrechnung des Stromverbrauchs um Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person, dem Betroffenen, und somit um personenbezogene Daten[10]. Betrachtet man den bisherigen Zähler und die damit verbundenen jährlichen Ableseintervalle für eine ebenfalls jährliche Rechnungsstellung, so hatte man es bislang mit wenigen Daten zu tun. Diese boten zudem keine Möglichkeit der Erstellung von besonders sensiblen Personen- und Verhaltensprofilen, da aus dem jährlichen Energieverbrauch kaum Rückschlüsse auf Lebensgewohnheiten der Betroffenen gezogen werden können. Zudem findet bislang keine telemetrische Abfrage der Daten statt. In aller Regel wird turnusmäßig einmal im Jahr durch einen Mitarbeiter des Verteilnetzbetreibers der Zählerstand abgelesen, ergänzend und in einigen Fällen alternativ besteht die Option der Selbstablesung und Einsendung des Zählerstands per Postkarte direkt an den Stromlieferanten, der Übermittlung des Zählerstands via Internet usw. sowie dem Einsatz dritter Dienstleistungsunternehmen (Auftragsdatenverarbeitung).
Den Meseberger Beschlüssen[11] kann entnommen werden, dass die Bundesregierung in Deutschland den Rollout der modernen Smart Meter befürwortet, was zu einer grundlegenden Änderung der bisherigen Praxis geführt hat. Inzwischen ist aber zu erwarten, dass nicht zuletzt der Bericht der BNetzA zum Messwesen[12] für eine gewisse Entschleunigung, zumindest des flächendeckenden Einbaus reiner Smart Meter, sorgen wird. Er hat aber auch klar aufgezeigt, dass gerade systemische Ansätze wie sie in Deutschland in den E-Energy Modellregionen entwickelt werden, sinnvoll sind. Sie gehen von einem intelligenten Gesamtsystem (Internet der Energie) aus und belassen es nicht nur bei einem Zählerwechsel. Dies kann ein guter Weg sein, die Zukunft insbesondere mit Blick auf die Ziele Klimaschutz (CO_2-

[9] http://www.e-energy.de/documents/Empfehlung__Datenschutz-Smart_Grids_VI.pdf, Seite 5 ff.
[10] i. S. d. § 1 Abs. 2 i.V.m. § 3 Abs. 1BDSG
[11] Im Rahmen ihrer Klausurtagung in Meseberg beschloss die deutsche Bundesregierung am 23. August 2007 die Eckpunkte des Integrierten Energie- und Klimaprogramms (IEKP). Dieses Programm ist daher auch unter dem Namen Meseberger Beschlüsse bekannt.
[12] http://www.bundesnetzagentur.de/DE/Sachgebiete/ElektrizitaetGas/Sonderthemen/BerichtZaehlMesswesen/berichtzaehlmesswesen_node.html

Einsparung, höhere und integrierte Einspeisung Erneuerbarer Energien), Lastmanagement, Preissignale und -transparenz zu gestalten.
Dies bringt folgende Wandlungen mit sich: Einerseits werden eine Vielzahl neuer Akteure die Daten benötigen – beispielsweise gänzlich neue Marktteilnehmer wie (Energieeffizienz-) Optimierungsdienste für den Verbraucher. Andererseits wird, bedingt durch die dann mögliche (nicht zwingende) viertelstündlich erfolgende Aufzeichnung der Messwerte[13] im Smart Meter, die Menge der Daten und damit das Datenvolumen in ganz erheblichem Maße steigen. Die Funktion einer viertelstündlichen Erfassung der Messwerte müssen Smart Meter im Fall einer vom Kunden gewünschten feingranularen Tarifierung in jedem Fall erfüllen, da sich nur mit einem solchen Zähler die Möglichkeit des Angebots derartiger dynamischer lastvariabler oder tageszeitabhängiger Tarife[14] umsetzen lässt. Ein so genannter Standardlastprofilkunde kann die Erfassung seines Elektrizitätsverbrauches in 15-minütigen Abständen verlangen, wenn er dies mit dem Messstellenbetreiber vereinbart hat. Technisch grundsätzlich möglich ist jedoch auch die Erfassung des Stromverbrauchs in Quasi-Echtzeit und damit sekundengenau. Zur Verdeutlichung des datenschutzrechtlichen Gefährdungspotentials der Nutzung des Smart Grid wird folgender Vergleich angestellt: Wo bisher einmal im Jahr eine Gesamtverbrauchsangabe erfolgte, fallen künftig bei einer Verbrauchsmessung in Intervallen von 15 Minuten pro Jahr an den Zählpunkten 35.040 Messwerte an. Das Ganze gewinnt an Komplexität, sofern man auch einen Blick auf das sogenannte Smart Home wirft. Hier soll der Zähler sogar den Verbrauch gerätespezifisch erfassen, sodass eine Aufschlüsselung des Verbrauchs einzelner Geräte möglich wird, mit dem Ziel die letztgenannten auch zu steuern, um günstige Tarife optimal auszunutzen. Des Weiteren wird den Daten eine stark erhöhte Aussagekraft zugeschrieben, so dass sie unmittelbar großes Interesse Dritter auf sich ziehen werden. Nimmt man also in den Blick, dass ein Großteil der Handlungen eines Menschen heute Strom benötigt, so geben die oben beschriebenen Daten ein ziemlich genaues Bild von den täglichen Beschäftigungen der in einem Haushalt lebenden stromverbrauchenden Personen. Selbst wenn man den reinen Energiemessdaten aus dem Zähler noch keinen Personenbezug zuschreiben möchte, sind diese jedoch, sobald sie mit den bei den jeweiligen Vertragspartnern wie dem Lieferanten und dem Messstellenbetreiber bzw. Messdienstleister vorhandenen Stammdaten verknüpft werden, als personenbezogene Daten für diese Akteure des Energiesektors einzuordnen.

Datenvielfalt

Die Problematik der Datenvielfalt lässt sich anhand des folgenden Zeitungsberichts besser verstehen[15]:

„Amerika gehen die Frequenzen aus
Nach Berichten der US-Publikation CNN Money geht in den Vereinigten Staaten demnächst das verfügbare Frequenzspektrum zur Neige. Bereits im Jahr 2013 soll ein Frequenz-Bandbreiten-Defizit von rund 90 MHz bestehen. Grund: Die Datenlawine durch Multimedia-Übertragungen mit Smartphones.“

[13] Die Erhebung von 1/4h-Werten ergibt sich aus den Konventionen des Stromhandelsmarktes bzw. der Bilanzierung; sie ist jedoch gekürt, d.h. es könnte auch (fast) jede andere kleine Zeiteinheit gewählt werden.
[14] In Deutschland: nach § 40 Abs. 3 EnWG
[15] http://www.elektroniknet.de/kommunikation/news/article/86086/0/Amerika_gehen_die_Frequenzen_aus/; Stand 23. Februar 2012

Nimmt man diese Meldung Ernst, so wird es jetzt schon für die bestehenden Mobilfunkapplikationen knapp. Das heißt, dass in zunehmendem Maße durch die einhergehende Automatisierung der Netze und Energiedienste die hinzukommende Datenvielfalt das Kommunikationssystem noch zusätzlich belasten wird. Die Auswirkungen der fehlenden Frequenzen wirken sich direkt auf die Qualität der Kommunikation aus. Von fehlenden Informationspaketen bis hin zum völligen Abbruch eines Kommunikationskanals ist alles möglich. Für ein funktionierendes Energiesystem, das Loadshifting im Sinne von Smart Grids betreiben möchte, ist aber eine garantierte Kommunikation zwischen Betreiber und Endkunde (Prosumer) notwendig.
Ein zusätzliches Risiko durch eine Datenlawine ist die schwierige Handhabe der Datensicherheit. Werden die Daten kryptographisch encoded, so wird noch mehr Bandbreite benötigt. In vielen Fällen könnten Provider dazu übergehen, die Chiffrierung zu unterbinden, was zur Folge hat, dass dann die Daten ungesichert übertragen werden. Diese breite und leichte Angriffsfront ist für jeden Hacker ein willkommenes Vergnügen.

Datenweitergabe

In Zeiten der Datenvorratsspeicherung ist das Thema der Datenweitergabe ein wichtiger Punkt, der im Zusammenhang mit der Smart Grids Thematik diskutiert werden sollte. Die Datenvorratsspeicherung geht zumindest in Österreich davon aus, dass alle IP-Adressen und deren Inhalte sowie Telefonnummern und deren Inhalte bis zu 6 Monate lang zu speichern sind. Denkt man an die Übertragungstechnologien der Smart Grids Anwendungen, so sind Ethernet und GSM (GPRS) zwei wichtige Technologien zur Datenübermittlung. Das würde also bedeuten, dass die Konsumdaten eines Haushaltes über 6 Monate gespeichert werden würden, und die Energiedienstleister hätten darüber nicht einmal eine Handhabe, da diese Verantwortung den Kommunikationsdienstprovidern obliegt.
Eine gesetzliche Regelung ist folglich notwendig. Zumal die einfache Weitergabe unter verschiedenen Instanzen der am Energiezyklus beteiligten Akteure auch nicht geregelt ist. Datenverlust könnte die Folge sein. Es gilt also, der Data Leak Prevention (DLP) nicht nur technisch, sondern auch regulatorisch zu entsprechen.

Endgerätesicherheit

Im Bereich der Endgerätesicherheit kann man auf Standards setzen. So kündigte die Standardisierungsagentur IEEE den neuen IEEE C37.239-Standard an, der ein einheitliches Format für den Austausch von Event-Daten, kurz Comfede (Common Format for Event Data Exchange) zwischen Energiesystemen definiert. Der neue Standard unterstützt Energieversorger dabei, Event-Daten von Geräten und Komponenten unterschiedlichster Hersteller effizient zu integrieren und zu analysieren. Auf diese Weise verbessert der neue Standard die Funktionssicherheit und Zuverlässigkeit des Smart Grid in erheblichem Maße. Der IEEE C37.239 Standard definiert ein einfach interpretierbares, XML-basiertes Format für Dateien, die Event-Daten enthalten, beispielsweise Event-Abfolgen oder Fehleranalyse-Reports, die aus den Energiesystemen erhoben werden. Dieses einheitliche Format ermöglicht den reibungslosen Austausch von Daten zwischen Relais-Technikern, Bedienungs- und Maintenance-Personal. Auch die Nutzer eines proprietären Systems können so die digitalen Daten anderer Systeme nutzen.[16]
Die Endgerätesicherheit hat sich in den letzten Jahren aufgrund der Smartphone-Entwicklungen erheblich verbessert. Im Smart Grids Bereich sind aber zusätzliche Maßnahmen notwendig. So reicht es in einigen Fällen, einfach einen Magneten an die „richtige“ Stelle des Gerätes zu legen um die Verbrauchsdaten zu manipulieren[17]. In dem Bericht „Smart Meter und die mögliche Auswirkung auf die nationale Sicherheit“, der von der Vereinigung

[16] http://www.openpr.de/news/505872/Smart-Grid-wird-sicherer-IEEE-C37-239-COMFEDE-STANDARD-verbessert-Sicherheit-intelligenter-Netze.html
[17] http://futurezone.at/future/8445-fbi-warnt-vor-smart-meter-hacks.php

der Cybersecurity Austria veröffentlicht wurde, wird das Thema ausführlich aus österreichischer Sicht behandelt. Dabei werden die Vulnerabilitäten und die Angriffsvektoren genau analysiert. Diese lassen sich in die Bereiche

- Hardware
- Software
- Schnittstellen und
- Kryptographie

unterteilen. Das Papier postuliert die These, dass durch Endgeräte wie ein Smart Meter das gesamte Energiesystem von Hackern durchwandert, und das System durch kriminelles Handeln zum Absturz gebracht werden könnte. Möglich ist das durch die Erlangung der Kundendaten des Nutzers, der IP-Adresse und der Zugangsdaten. Dabei kann ein Hacker mit den erworbenen Daten in das System des Energieproviders eindringen und seinen Konsum oder seine Abrechnung manipulieren. Geschieht das auf breiter Front, so könnten z.B. durch geänderte Lastprofile die Orders verändert und die Lastprofile so verändert werden, dass Systeme überbelastet werden. Umgekehrt könnte die Nachfrage komplett heruntergesetzt und das System unterversorgt werden.

Zusätzliche Sichtweisen

Aus der Sicht von Fr. Prof. Claudia Eckert, der Leiterin des Fachgebiets „Sicherheit in der Informatik“ an der Technischen Universität München sowie Leiterin der Münchener Fraunhofer-Einrichtung für Angewandte und Integrierte Sicherheit, kurz Fraunhofer AISEC (Fraunhofer Research Institution for Applied and Integrated Security), wird die These des vorher genannten Papiers noch untermauert[18]:

„Angriffspunkte und Schwachstellen ergeben sich unter anderem durch eine Vielzahl von ungenügend abgesicherten Smart Metern, die als Massenprodukte in Haushalten, Gebäuden, Anlagen ausgerollt werden. Das dritte Energiepaket, das das Europäische Parlament im April 2009 verabschiedet hat, empfiehlt, dass 80% aller Energiekunden bis 2020 Smart Meter haben sollen. Durch die Vernetzung, mit der Möglichkeit der Fernzugriffe auf Komponenten und Systeme (die z.B. zur kostengünstigen und effizienten Fernwartung sehr erwünscht sind), ergibt sich eine Vielzahl mangelhaft abgesicherter offener Zugangspunkte, wodurch sicherheitskritische Zugriffe auf die Netze/Komponenten des Smart Grid möglich werden. Drittanbieter können ihre Mehrwertdienste in die Energiemarktplätze einbringen, jedoch fehlen derzeit Sicherheits- APIs, einfache Test-Suiten etc., mit denen die Qualität der Dienste, insbesondere deren Vertrauenswürdigkeit, technisch geprüft werden kann. Die Bereitstellung unsicherer Mehrwertdienste, bei deren Nutzung sensitive Kundendaten verarbeitet werden, birgt die Gefahr des Datenmissbrauchs und der unberechtigten Weitergabe von Daten (Data Leakage), so dass sich Gefährdungen der Vertraulichkeit und der Privatheit sowie Compliance und Haftungsprobleme ergeben können.
Es ist aus Kostengründen naheliegend, dass man für die Kommunikationsinfrastruktur zumindest in Teilen auf das bestehende Internet zurückgreifen wird und dass man zur durchgängigen und effektiven Verarbeitung von Energiedaten in dem komplex vernetzten System versuchen wird, die Internet-Protokoll Familie IP als gemeinsame Protokollschicht zu etablieren. Den Vorteilen einer einheitlichen Vorgehensweise stehen zum Einen die bekannten Sicherheitsschwächen der Internet Protokolle (IP Protokolle) gegenüber. Hierfür gibt es aber einige Lösungsansätze, die auch im Smart Grid verwendbar sind. Besondere Bedrohungen ergeben sich zum Anderen aus der IP-basierten „Monokultur“, die eine schnelle, ungehinderte Ausbreitung von Schadenssoftware (Malware) wie Würmer und Viren begünstigt, so dass die Verfügbarkeit von Diensten und Komponenten beeinträchtigt, gefälschte Daten in Umlauf oder aber auch gezielte Sabotage-Aktionen durchgeführt werden können. Das Smart Grid wird IKT-basierte Systeme mit physikalischen Komponenten zu den so genannten Cyber-Physical Systems verbinden. An der Schnittstelle zwischen physischen und IKT-gestützten

[18] Sicherheit im Smart Grid Eckpunkte für ein Energieinformationsnetz; sicherheitimsmartgrid2-120113033743-phpapp01.pdf; Seite 20 ff.

Systemen werden neue Schwachstellen und Verwundbarkeiten auftreten, die für gezielte Angriffe, wie Denial-of-Service, terroristische Attacken etc. ausgenutzt werden können. Mit dem Smart Grid werden Energieversorgungsnetze und Netze, die vordringlich zur Abwicklung von Business-IT verwendet werden (Abrechnung, Mehrwertdienste etc.), gekoppelt. Es besteht die Gefahr, dass die bekannt anfälligen Business-IT-Systeme durch mangelhafte Überwachungen und Isolierungen den gesicherten Betrieb von Versorgungsnetzen und Energiemanagementsystemen bedrohen.
Schwachstellen und Bedrohungen werden durch Angreifer ausgenutzt, die versuchen, ihre jeweiligen Ziele zu erreichen. Ein Smart Grid stellt ein attraktives Angriffsziel dar, so dass zu erwarten ist, dass insbesondere terroristische und kriminell motivierte Angriffe zunehmen werden. Nachfolgend sind einige mögliche Angreifer-Klassen aufgelistet.

Zusammenfassung AP 1.2

Zusammenfassend ist festzustellen, dass die wesentlichen Security Schwachstellen von Smart Grids dominierten Energiesystemen überall dort zu finden sind, wo Daten (Konsumdaten, Betriebsdaten, Marktdaten, usw.) über offene Schnittstellen kommuniziert werden. Gerade dies ist aber das Kennzeichen von Smart Grids. Durch die Kryptographierung werden die bereits heute knappen zur Verfügung stehenden Übertragungsbandbreiten nochmals belastet, was zu einem komplexen Security Problem führen kann.
Die mangelnde Sicherheit einzelner Komponenten im Energiesystem wird jedoch über Kurz oder Lang auch einen direkten Einfluss auf die Versorgungssicherheit haben. Security und Safety sind folglich direkt gekoppelt.

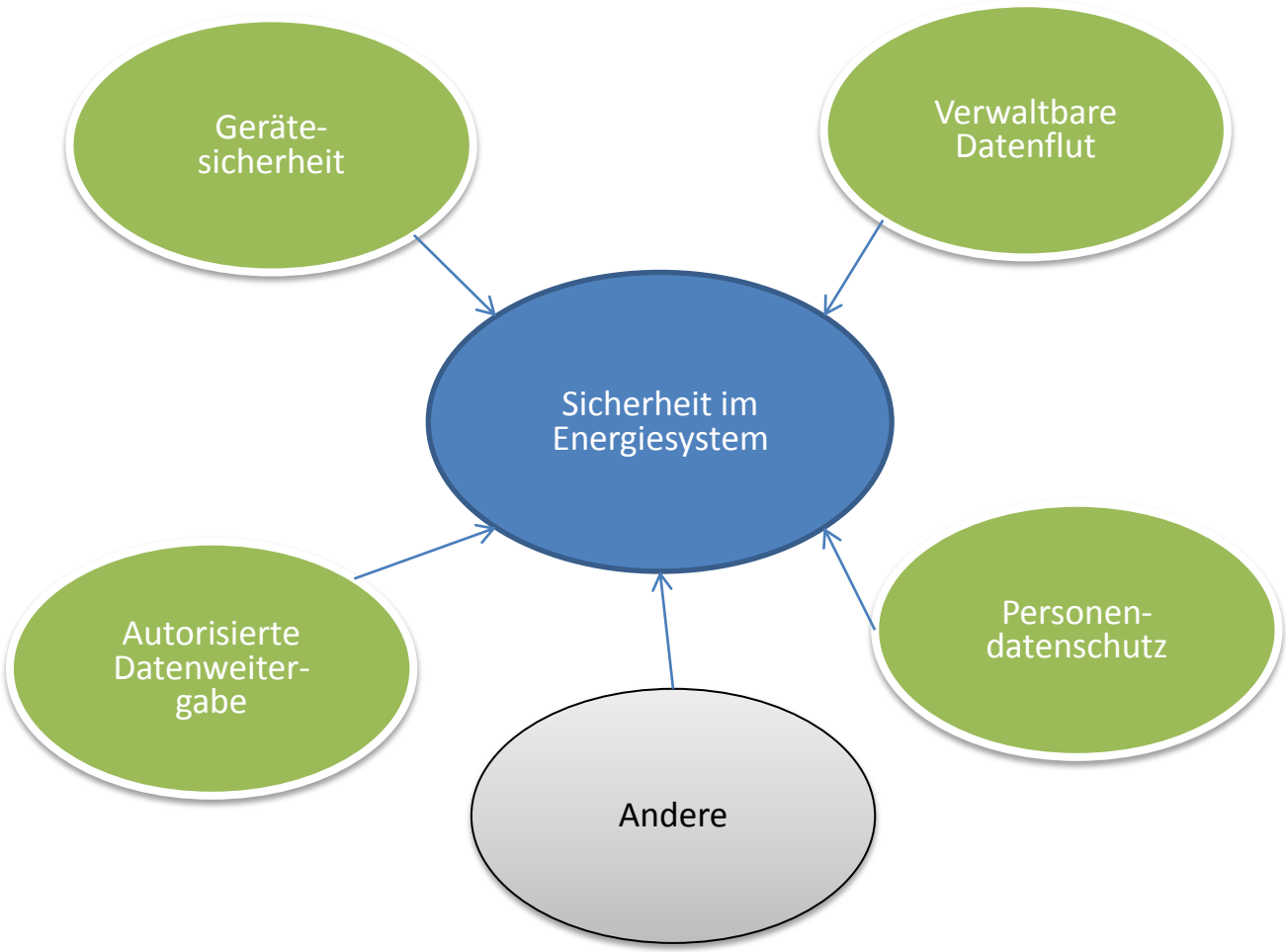

Abbildung 8: Mögliche Schwachpunkte der Sicherheit im Energiesystem

Signifikante Bedrohungsszenarien (AP 1.3)

Die Drohszenarien für Smart Grids bestehen im Wesentlichen in der digitalen Kriminalität mit all ihren Ausdrucksformen. Aus der Studie IT-Sicherheit in Österreich – 2008 geht hervor, dass die kommenden wichtigsten Angriffsvektoren die

- Mobile Security
- E-Mail-Security zur Absicherung gegen Schadcode und
- Phishing sowie Identity Management

sind. Diese Angriffsvektoren werden durch verschiedene Akteure genutzt, um an Daten zu kommen. Diese werden für verschiedenen Zwecke verwendet; so haben Terroristen meistens einen politischen Hintergrund für ihr Handeln. Hingegen ist das organisierte Verbrechen „nur“ an der eigenen Bereicherung interessiert. Der Schaden, der durch beide Gruppierungen entstehen kann, ist gegenwärtig noch nicht quantifizierbar. In der österreichischen Studie „Black Ö1“ wurden verschiedene Szenarien für Blackouts in Österreich[19] untersucht. Dabei wurden auch Aussagen über den wirtschaftlichen Schaden errechnet, die Blackouts mit sich führen können. Eine genaue Schadensquantifizierung hängt laut Studie auch vom betroffenen Gebiet und der Dauer ab. So lassen sich z.B. für Wien folgende Szenarien ausmalen:

Ausfalldauer	Gesamt Schaden
[h]	[in 1000 €]
1	61 135
5	122 159
10	165 269

Abbildung 9: Wirtschaftlicher Schaden eines Blackouts im Wiener Raum

Cyberterrorismus

Unter Cyberterrorismus versteht man Angriffe mittels Internet-Technologien auf Computersysteme. Bei Cyberterrorismus geht es meist nicht um einen monetären Gewinn. Es stecken individuelle Ziele hinter diesen Angriffen, wie religiöse oder politisch orientierte Absichten oder die Profilierung in der „Hacker Community“.

Man unterscheidet 2 Arten von Cyberterrorismus:

- Reine Cyberterroristen, die sich rein auf Computer spezialisieren und nur virtuelle Angriffe starten
- Terroristen, die mit Hilfe von Computertechnologien reale Angriffe auf Infrastrukturen durchführen, oder diese unterstützen.[20]

[19] http://www.energieinstitut-linz.at/dokumente/upload/Endberichtblackoe.pdf
[20] Vgl. http://www.spiegel.de/netzwelt/tech/0,1518,548086,00.html – Letzter Zugriff: 11.5.2012

Die zweite Unterart sind im Kontext von Smart Grids die gefährlicheren Terroristen. Sie können die Versorgung beeinträchtigen oder sogar lahmlegen.
Ein bekannter Fall von Cyberterrorismus ist der „Stuxnet-Wurm“, der für Störungen in Kernkraftwerken, vor allem im Iran, verantwortlich war. Dabei wurde ein Wurm in die programmierbaren Steuerungen eingebracht und somit das Steuerungssystem des Kraftwerks außer Funktion gesetzt. Es wird gemutmaßt, dass dieser schadhafte Wurm von einem anderen Staat in Auftrag gegeben wurde, dass seine Herstellung sehr kompliziert und interdisziplinäres Wirken erforderlich machte. Seine Entwicklungszeit wird auf 3 Jahre geschätzt, was also sehr hohe Kosten verursacht hat.
Die Konsequenz dieser Aktion ist jedoch, dass zukünftig der Cyberterrorismus nicht nur von kleinen isolierten Gruppen verübt werden kann, sonder im großen Stil auch von verfeindeten Staaten.

Auf das Smart Grids System umgelegt, könnte der Cyberterrorismus das gesamte Energiesystem eines Landes oder einer Region lahm legen. Diese Variante ist durch die vermehrten Aktivitäten der Hackergruppe Anonymous für die mittelbare Zukunft als realistisch einzuordnen. Beschränken sich ihre Aktivitäten bislang zwar nur auf Internetseiten, so kann sicher nicht darauf vertraut werden, dass zukünftig auch andere Angriffsziele ins Visier kommen. Gleiches gilt für die massenweise Veröffentlichung von Daten, wie sie Wikileaks betreibt. Zwar ist das eine andere Art des Cybercrimes wie wir sie hier definiert vorfinden, ein Schaden wird aber dadurch dennoch herbeigeführt. Ein integriertes Sicherheitskonzept sollte folglich alle Bedrohungsszenarien beinhalten. Die Erarbeitung eines solchen Konzepts ist jedoch nur gemeinsam in einer interdisziplinären Arbeitsgruppe möglich. Nur so können differenzierte Sichtweisen zum Thema Sicherheit gewonnen und alle Angriffsvektoren abgedeckt werden.

Organized Crime

Organisierte Kriminalität bezeichnet Gruppierungen, die gezielt kriminelle Ziele systematisch verfolgen.
In Deutschland wird der Tatbestand wie folgt definiert:

„Organisierte Kriminalität ist die von Gewinn- oder Machtstreben bestimmte planmäßige Begehung von Straftaten, die einzeln oder in ihrer Gesamtheit von erheblicher Bedeutung sind, wenn mehr als zwei Beteiligte auf längere oder unbestimmte Dauer arbeitsteilig

> a) unter Verwendung gewerblicher oder geschäftsähnlicher Strukturen,
> b) unter Anwendung von Gewalt oder anderer zur Einschüchterung geeigneter Mittel oder
> c) unter Einflussnahme auf Politik, Massenmedien, öffentliche Verwaltung, Justiz oder Wirtschaft

zusammenwirken. Der Begriff umfasst nicht Straftaten des Terrorismus.“[21] Klassisch kennt man organisierte Kriminalität im Rahmen der Mafia.

Im Gegensatz zu Terrorismus, wobei versucht wird politische Ziele zu verfolgen, geht es bei organisierter Kriminalität vor allem um eine Gewinnabsicht.

[21] Gemeinsame Richtlinien der Justizminister/-senatoren und der Innenminister/-senatoren der Länder über die Zusammenarbeit von Staatsanwaltschaft und Polizei bei der Verfolgung der Organisierten Kriminalität In: Richtlinien für das Strafverfahren und das Bußgeldverfahren Anhang E Nr. 2.1. Stand: 2008

Im Smart Grids Bereich kann die organisierte Kriminalität zum Problem werden, wenn ein System gehackt und dann der Energieversorger erpresst wird. Ebenso können Kundendaten zu missbräuchlichen Zwecken verwendet oder verkauft werden, seien es Kreditkarteninformationen oder Kontaktadressen, die mittlerweile auch schon hohe Profite am Schwarzmarkt erzielen.

Consumer Manipulation

Unter Verbrauchermanipulation versteht man die bewusste Indoktrination von Konsumenten um deren Verhalten zu steuern. Sei es in Industrie und Gewerbe um Kunden zu gewinnen, oder in der Politik um die Mehrheit der Wähler auf seine Seite zu bekommen.

„Mittels detaillierter Marktforschung und verschiedensten Studien werden Menschen, ihre Bedürfnisse und Reaktionen explizit analysiert. Die Erkenntnisse von derlei zivilsozialen Studien nutzen Industrie und Verbände sodann bewusst und vorsätzlich zur Generierung neuer Trends. Eine Art “Massengeschmack” wird geschaffen, dessen Erfolg auf vorsätzlicher Verbrauchermanipulation beruht.“[22]

Im Bezug auf Smart Grids ist diese Thematik nicht zu unterschätzen, da intelligente Netze nur implementiert werden können, weil die Prosumer darauf vertrauen, dass alles korrekt abläuft. Durch eine gezielte Manipulation wäre es möglich, die Gefahren in einem Smart Grid so zu thematisieren, dass viele Endnutzer eingeschüchtert werden und sich nicht in das Netz integrieren.

Des Weiteren kann unter Consumer Manipulation der bewusste Versuch, die Abrechnung zu verringern, gesehen werden. Durch verschiedenste Methoden werden die Zähler manipuliert, um den Strompreis zu senken. Zum Beispiel wurden in Puerto Rico Smart Meters manipuliert und dem betroffenen Energieunternehmen entstand ein Schaden von mehreren Millionen Dollar. Es ist derzeit mit geringen Computerkenntnissen möglich einen Smart Meter zu hacken.[23]

Economic Crime

Wirtschaftkriminalität beschreibt Straftaten, die einen wirtschaftlichen Bezug aufweisen.

<u>Manipulationsmöglichkeiten auf den Finanzmärkten</u>
Bei der Sicherheit bei Smart Grids darf es nicht nur um technische Aspekte gehen. Auch die ökonomische Betrachtungsweise muss beachtet werden. Durch das Hacken der Computerprogramme von Energieversorgern kann deren Börsenkurs durch Spekulanten nach deren Willen herabgesetzt werden. So erging es beispielsweise der Firma Sony, die infolge eines Hackerangriffes 100 Millionen Kundendaten verloren hat und deren Börsenkurs daraufhin innerhalb kürzester Zeit extrem abgenommen hat.[24]

<u>Erpressungsversuche</u>
Wenn ein Netzbetreiber vor die Wahl gestellt wird, entweder er bezahlt einen verschmerzbaren Betrag oder die gehackten Daten werden manipuliert, unbrauchbar oder öffentlich gemacht, hat er meist nur kurze Zeit diese Drohung auf ihre Plausibilität zu prüfen, denn natürlich kann es sich auch um einen Täuschungsversuch handeln. Wird dieses Szenario jedoch bei Nichtbezahlung mit Beispielen untermauert, werden andere Netzbetreiber bereit sein

[22] http://renegraeber.de/blog/angriff-auf-unsere-sinne/ - Letzter Zugriff: 11.5.2012
[23] http://futurezone.at/future/8445-fbi-warnt-vor-smart-meter-hacks.php
[24] Vgl. Smart Metering und mögliche Auswirkungen auf die nationale Sicherheit- Cyber Security Austria

dieser Erpressung nachzukommen. Daher entsteht eine größere Abhängigkeit und die Opfer können nur mehr verlieren.

Nicht ausgeschlossen werden kann, dass derartige Praktiken auch zur öffentlichen Diffamierung von bestimmten Marktführern ausgenutzt werden.

Daher sollten sich Hersteller und Netzbetreiber ebenfalls im Vorfeld mit derartigen Szenarien auseinandersetzen und auf mögliche Erpressungsversuche vorbereiten.[25]

Wirtschaftliche Zwänge
Logischerweise will kein Netzbetreiber ein leicht verwundbares System besitzen.
Jedoch werden Sicherheitsanforderungen sehr leicht übersehen bzw. bekommen nicht die entsprechende Priorität. Darüber hinaus handelt es sich um hochkomplexe Zusammenhänge, die wahrscheinlich nur in einem interdisziplinären Ansatz erfassbar sind. Viele Auswirkungen können erst in der Zusammenschau erkannt werden., bzw. wirken sich diese erst im Gesamtsystem aus.[26]

Zusammenfassung AP 1.3

Zusammenfassend kann gesagt werden, dass die größten Bedrohungen in Zukunft von den vier hier dargestellten Bedrohungsszenarien ausgehen. Das Beispiel von Stuxnet oder von der Kundendatenentwendung bei Sony zeigt, dass diese Bedrohungen auch bei uns ernsthafte Realität werden können. Es ist auch davon auszugehen, dass die kriminellen Elemente entsprechend dem Schadensziel viel Energie in die Programmierung von Schadsoftware investieren werden. Der manipulierende User am Smart Metering wird dabei das geringere Übel sein.

[25] Vgl. Smart Metering und mögliche Auswirkungen auf die nationale Sicherheit- Cyber Security Austria
[26] Vgl. Smart Metering und mögliche Auswirkungen auf die nationale Sicherheit- Cyber Security Austria

Entwicklung möglicher Abwehrmaßnahmen (AP 1.4, 1.5)

Arbeitsschritte zur Begegnung der analysierten Bedrohungsmöglichkeiten

Den dargestellten Bedrohungsszenarien kann auf zwei Arten begegnet werden. Zum Einen müssen technische Lösungen im Hardware-, Software- und Schnittstellenbereich erarbeitet werden, und eine sichere Kommunikation und Chiffrieralgorithmen müssen dafür sorgen, dass die technischen Angriffsvektoren reduziert bzw. eliminiert werden.
Auf der anderen Seite sind organisatorische Maßnahmen in den Firmen zu setzen. Sie fokussieren die nachhaltige Sicherheit des Energiesystems und definieren die entsprechenden Verantwortlichkeiten innerhalb der Organisation. Die Verantwortung für das Gesamtsystem ist dann klar geregelt und die wirkenden Handlungsebenen werden aufgefunden, diskutiert und in die Tat umgesetzt. Dies erfordert ein Denken über den eigenen Sicherheitsbereich hinaus im ganzheitlichen Sinne. Das Systemdesign, das neue Herausforderungen aufgreift und einbindet, ist essentiell. Die Einbindung sicherheitsrelevanter Themen im Smart Grids wird die zukünftige Sicht auf das Gesamtsystem konsequent und schrittweise verändern.

Umfassende Sicherheit ist kein unveränderbarer Zustand, der einmal erreicht wird und sich nicht wieder ändert. Insbesondere in sich noch entwickelnden Bereichen wie einem Smart Grid wird der Betrieb der Netzwerke und IKT-Systeme ständigen dynamischen Veränderungen unterworfen sein. Viele dieser Veränderungen betreffen neben Änderungen der Geschäftsprozesse, der IKT, der Fachaufgaben, Infrastruktur und Organisationsstrukturen auch die IT-Sicherheit und den Datenschutz. Dies gilt insbesondere für die Energieversorgung als nationale kritische Infrastruktur, die angemessene Sicherheitsstandards für die nachhaltige, weitere Verbesserung des Sicherheitsmanagements der Systeme aller beteiligten Parteien benötigt.[27]

In den folgenden Kapiteln werden die notwendigen organisatorischen Maßnahmen und Sicherheitsstandards vorgestellt. Diese Standards sind wichtig bei der Errichtung eines Sicherheitsmanagementsystems, das eine nachhaltige Sicherheit gewährleisten kann und die einen permanenten Sicherheitsfindungsprozess anstoßen. Die Begriffe werden zuerst erklärt und anschließend wird ihre mögliche Implementierung in Organisationen untersucht.

IT-Governance

Allgemeine Definition
Unter IT-Governance versteht man im Allgemeinen alle Maßnahmen, Prozesse und Strukturen in einer Organisation, die zum Ziel haben, dass die IT die Unternehmensstrategie und -ziele unterstützt, Ressourcen vernünftig einplant und einsetzt und externe sowie interne Risiken minimiert.

„Das Hauptziel von IT-Governance ist es, die Anforderungen an die IT sowie die strategische Bedeutung von IT aus Sicht der Kern- und Führungsprozesse im Unternehmen zu verstehen, um den optimalen Betrieb zur Erreichung der Unternehmensziele sicherzustellen und Strategien für die zukünftige Erweiterung des Geschäftsbetriebes zu schaffen. IT-Governance zielt darauf ab, dass Erwartungen an die IT bekannt sind und dass die IT in der Lage ist, diese Erwartungen auch zu erfüllen. Dabei sollen mögliche Risiken entschärft werden. In diesem Sinne wäre es richtiger, von der Enterprise Governance over IT als von IT-Governance zu

[27] Sicherheit im Smart Grid Eckpunkte für ein Energieinformationsnetz; sicherheitimsmartgrid2-120113033743-phpapp01.pdf; Seite 20 ff.

sprechen. IT-Governance spielt sich nämlich nicht in der IT-Organisation ab, sondern außerhalb.“[28]

Maturity Model:
Um den Reifegrad einer IT-Governance zu prüfen gibt es ein IT Maturity Assessment, welches auf dem **C**apability **M**aturity **M**odel **I**ntegration – CMMI, aufbaut. Dieses CMMI® wurde bereits im Jahr 1986 ansatzweise definiert und findet seit dem Jahr 2003 die heutige aktuelle Fassung. Spice und Cobit sind Derivate dieses Capability Maturity Models. In diesem Modell werden Stufen eines IT-Prozesses definiert. Diese Stufen sind[29]:

1. **Initial (beginnend)**
   Dies ist der Grundzustand, den jede Organisation erreicht, auch ohne dass ein Prozess für die Softwareentwicklung definiert und umgesetzt wird.
   Kosten, Zeiten und Qualität sind nicht vorhersehbar.
   Es sind keine Key Process Areas (KPA) definiert.
2. **Repeatable (wiederholbar; bei CMMI[30] Managed)**
   Ein grundlegender Prozess existiert. Die Planung neuer Projekte erfolgt anhand der Erfahrungen mit vergangenen Projekten.
   Zeiten sind einigermaßen kontrollierbar. Kosten und Qualität unterliegen starken Schwankungen.
   Key Process Areas (KPA): Requirements management, software project planning, software project tracking and oversight, software subcontractor management, software quality assurance, software configuration management.
3. **Defined (definiert)**
   In der Organisation ist ein typischer Software-Entwicklungs- und -wartungsprozess eingeführt und dokumentiert (Standard-Software-Prozess).
   Eine spezielle Organisationseinheit ist für die Umsetzung verantwortlich.
   Kosten und Zeiten sind hier einigermaßen zuverlässig bewertbar. Qualität ist immer noch Schwankungen ausgesetzt.
   KPA: Organizational process focus, organizational process definition, training program, integrated software management, software product engineering, intergroup coordination, peer reviews.
4. **Managed (gesteuert; bei CMMI Quantitatively Managed)**
   Sowohl für das Produkt als auch für den Prozess werden quantitative Ziele vorgegeben, ihre Erreichung gemessen und überwacht.
   Zeiten, Kosten und Qualität sind zuverlässig kontrollierbar.
   KPA: Quantitative process management, software quality management.
5. **Optimizing (optimierend)**
   Die gesamte Organisation konzentriert sich auf das Finden von Schwächen und die weitere Verbesserung des Prozesses.
   KPA: Defect prevention, technology change management, process change management.

Die Implementierung von IT Governance muss gemäß Forrester Research auf drei wesentlichen Elementen basieren[31]:

1. **Struktur**: Wer trifft die Entscheidungen? Welche Organisationsstrukturen müssen geschaffen werden?

[28] http://de.wikipedia.org/wiki/IT-Governance
[29] http://de.wikipedia.org/wiki/Capability_Maturity_Model
[30] CMMI: Capability Maturity Model Integration
[31] Symons, C. (2005): IT Governance Framework, Forrester Best Practices March 29, 2005.

2. **Prozesse**: Wie werden IT-Entscheidungen getroffen? Wie sind die Entscheidungsprozesse für den Vorschlag, die Bewertung, Durchführung und die Reihung von IT-Investitionen strukturiert?
3. **Kommunikation**: Wie werden die Ergebnisse der Prozesse und Entscheidungen überwacht, gemessen und kommuniziert? Welche Mechanismen werden genutzt, um IT-(Investment)-Entscheidungen zu kommunizieren?

Frameworks wie ITIL und COBIT beschreiben dabei nicht die konkrete Umsetzung, sondern definieren den Rahmen, die Anforderungen und die Ergebnisse des IT-Managements. Die Ausformulierung der operativen IT-Prozesse muss für jedes Unternehmen in Einklang mit den Branchen- und unternehmensspezifischen Geschäftsprozessen erfolgen[32].

COBIT

IT-Governance nach COBIT[33]
COBIT *(Control Objectives for Information and Related Technology)* ist das international anerkannte Framework zur IT-Governance und gliedert die Aufgaben der IT in Prozesse und Control Objectives (oft mit *Kontrollziel* übersetzt, eigentlich *Steuerungsvorgaben*, in der aktuellen deutschsprachigen Version wird der Begriff nicht mehr übersetzt).
COBIT definiert hierbei nicht vorrangig, *wie* die Anforderungen umzusetzen sind, sondern konzentriert sich primär darauf, *was* umzusetzen ist.

Steuerungsansatz[34]
Der Steuerungsansatz von COBIT ist grundsätzlich Top-Down. Ausgehend von Unternehmenszielen werden IT-Ziele festgelegt, die wiederum die Architektur der IT beeinflussen. Hierbei gewährleisten angemessen definierte und betriebene IT-Prozesse die Verarbeitung von Informationen, die Verwaltung von IT-Ressourcen (Personal, Technologie, Daten, Anwendungen) und die Erbringung von Services. Für diese Ebenen (unternehmensweit, IT, Prozess und Aktivitäten) sind jeweils Mess- und Zielgrößen zur Beurteilung der Ergebnisse und der Performance-Driver festgelegt. Die Messung der Zielerreichung erfolgt Bottom-Up und ergibt so einen vorgegebenen Steuerungs-Zyklus.
In Summe definiert das COBIT-Framework COBIT **34** IT-Prozesse, denen die Control Objectives zugeordnet sind. Die Control Objectives sind wesentliche Bereiche, die im Prozess berücksichtigt sein müssen, um das Prozess-Ziel (und somit über das IT-Ziel das Unternehmensziel) zu erreichen. Die Summe der Control Objectives stellt eine verlässliche und dem Unternehmensbedarf angemessene Informationsfunktion sicher.

Das COBIT-Framework definiert detailliert 318 Kontrollziele und Audit-Richtlinien zu 34 kritischen Prozessen in 4 Domänen: Planung und Organisation; Beschaffung und Implementation; Betrieb und Support sowie Überwachung, die einen Lebenszyklus bilden. Das "Implementation Toolset" ist eine Anleitung mit Tätigkeiten und Checklisten für die Umsetzung in einer Organisation.[35]

Im Framework definiert die Management-Richtlinie, wie gemessen werden kann. Dazu werden für die einzelnen Prozesse kritische Erfolgsfaktoren, Kernziele, Leistungsindikatoren und Anzeiger für die Einteilung in das COBIT-Maturitätsmodell gegeben. Dieses Modell zeigt den Reifegrad von Prozessen an.

[32] http://www.ocg.at/ak/governance/files/itgovernance.pdf
[33] http://de.wikipedia.org/wiki/COBIT
[34] http://de.wikipedia.org/wiki/COBIT
[35] http://www.cryptoshop.com/index.php

Die Kontrollziele definieren für die Prozesse, welche Mindestkontrolle ausgeübt werden soll um ein bestimmtes Niveau zu erreichen, während die Audit-Richtlinie definiert, wie geprüft werden soll.

IT Ressourcen[36]
COBIT definiert, welche IT-Ressourcen in Betracht kommen und gesteuert und überprüft werden müssen:
Daten: Datenelemente im weitesten Sinn.

Anwendungen: Als Anwendung bezeichnet man die Summe manueller und programmierter Verfahren.

Technologie: Technologie umfasst Hardware, Betriebssysteme, Datenbankverwaltungssysteme, Netzwerke, usw.

Anlagen: Alle Ressourcen zur Beherbergung und Unterstützung von Informationssystemen.

Personal: Kenntnisse, Bewusstsein und Produktivität zur Planung, Organisation, Beschaffung, Ablieferung, Unterstützung und Überwachung von Informationssystemen und -dienstleistungen.

Kriterien für sichere und ordnungsgemäße IT[37]

COBIT kennt insgesamt 7 Kriterien für sichere und ordnungsgemäße Informationssysteme:

- die 3 allgemeinen Sicherheitsziele: **Vertraulichkeit**, **Integrität**, **Verfügbarkeit**

- Anforderung an die Ordnungsmäßigkeit, Kriterien der Rechnungslegung: **Zuverlässigkeit** und **Compliance** im Sinne von Einhaltung rechtlicher Erfordernisse.

- Qualitätsanforderungen: **Effektivität** und **Effizienz**

Zuverlässigkeit bezieht sich auf die Bereitstellung geeigneter Daten, um die Geschäftseinheit zu betreiben und um dem Management die Ausübung ihrer Verantwortung zu ermöglichen.

Effektivität bedeutet Wirksamkeit. Die Informationen für einen Geschäftsprozess sind wichtig und gehören zu ihm und müssen rechtzeitig in einer fehlerfreien, konsistenten und verwendbaren Form geliefert werden.

Effizienz bedeutet Wirtschaftlichkeit und betrifft die Bereitstellung von Informationen mit einer optimalen Verwendung von Ressourcen.

ISO/IEC 27001ff

ISO/IEC 27001 ist ein internationaler Standard um die Sicherheit von Informationen und Daten zu gewährleisten. Er unterstützt die systematische Identifizierung und Analyse von Risiken, die durch die Nutzung von Informationen entstehen, sowie die Einführung und Aufrechterhaltung angemessener Kontroll- und Steuerungsmechanismen. ISO/IEC 27001 betrachtet die drei wesentlichen Merkmale von Informationen: die Verfügbarkeit, die Vertraulichkeit und die Integrität. [38]

[36] http://www.cryptoshop.com/index.php
[37] http://www.cryptoshop.com/index.php
[38] http://www.maxpert.de/de/profil/education-loesung/

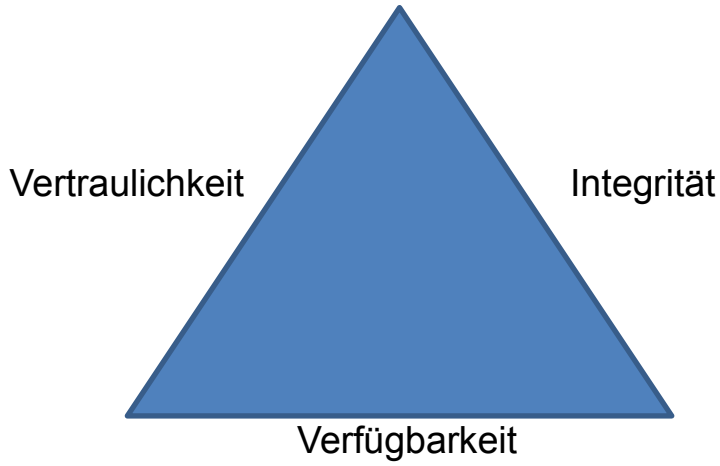

Abbildung 10: Sicherheitsdreieck als Basis für eine integre Sicherheit in der zukünftigen Energiewirtschaft; Quelle: Security Triangle aus: Book: „Securing the Smart Grids“ – Next Generation Power Grid Security.

Ein Informationssicherheits-Managementsystem (ISMS) mit definierten notwendigen Maßnahmen (Controls) liefert dafür den Rahmen. Das Informationssicherheits-Managementsystem (ISMS) basiert auf dem PDCA-Modell (Plan-Do-Check-Act), das die strukturierte Umsetzung und kontinuierliche Verbesserung aller wesentlichen Sicherheitsaspekte unterstützt.
ISO/IEC 27001 gewährleistet somit einen anerkannten Schutz für die Daten und Informationen der Unternehmen, steigert deren Verfügbarkeit, erleichtert das Identifizieren von Schwachstellen und erhöht das Vertrauen in das Unternehmen. Unternehmen können sich nach diesem Standard zertifizieren lassen.

ISO/IEC 27001 sieht sechs Schritte zur Zertifizierung vor:

- **Definition des Geltungsbereiches (Scope) sowie der Grenzen des ISMS**
  Klärung des Geltungsbereiches (Scope) um festzulegen, in welchen Bereichen das Informationssicherheits-Managementsystem zur Anwendung kommen soll.
- **Definition der Informationssicherheitspolitik**
  Festlegen der Informationssicherheitspolitik für den definierten Geltungsbereich
- **Identifizieren und Analysieren von Assets**
  Identifizierung der Unternehmenswerte (Assets) mit den entsprechenden Risiken. Es werden Fragen geklärt wie: Wo sind Schwachstellen? Mit welchen Bedrohungen ist zu rechnen?
- **Risiken steuern**
  Risiken müssen identifiziert, analysiert und gesteuert werden. Dabei muss beachtet werden, wie schwer die Risiken sind und welche von ihnen sind tragbar?
- **Controls festlegen**
  Festlegen der notwendigen Maßnahmen (Controls) mit ihren Zielen.
- **Erstellung des Statement of Applicability**
  Erstellen einer Erklärung zur Anwendbarkeit der Norm ISO/IEC 27001 (Statement of Applicability), sowie eine Zusammenfassung der getroffenen Maßnahmen

Abbildung 11: PDCA Model (Plan-Do-Check-Act), welches dem ISO 27001 zugrunde liegt[39]

Zusammenhänge
Betrachtet man nun alle Komponenten der IT-Sicherheit, kann man folgenden Zusammenhang aller Komponenten ausmachen:

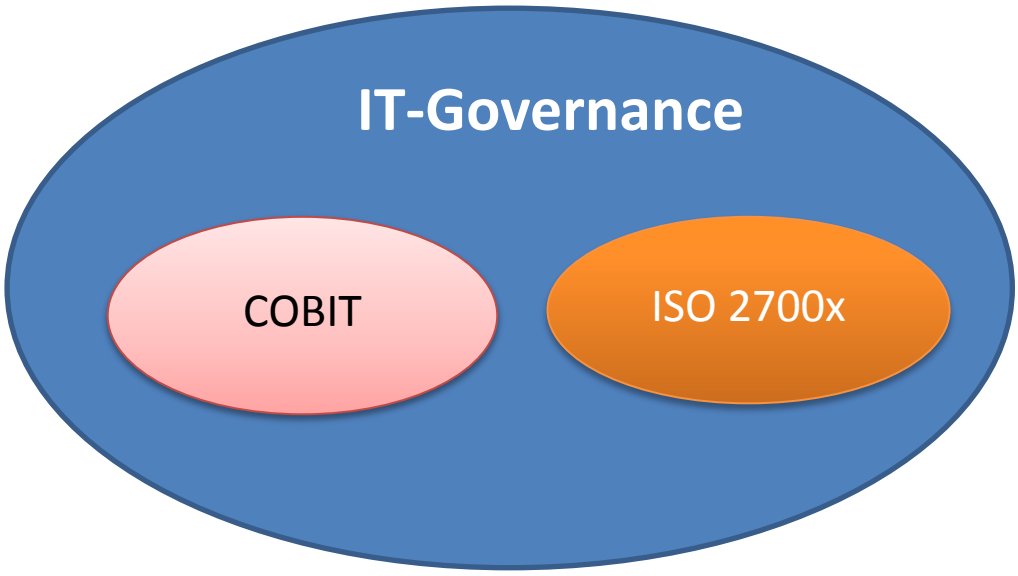

Abbildung 12: Zusammenhang der IT-Sicherheitskomponenten

Die IT-Governance bildet das übergeordnete Feld für die Erreichung der Unternehmensziele. COBIT definiert vorrangig was umzusetzen ist und ISO 2700x identifiziert und analysiert die Risiken, die durch die Nutzung von Informationen entstehen.

IT-Sicherheit in der Energiewirtschaft

Die Energiewirtschaft befindet sich seit geraumer Zeit in einer Umbruchphase. Neue Herausforderungen müssen bewältigt werden, auch jene der IT-Sicherheit. Das Verknüpfen der IKT-Komponente mit der Energiewelt ermöglicht viele Anwendungen, die bislang nicht anzuden-

[39] http://www.maxpert.de/de/profil/education-loesung/

ken waren. Es birgt aber auch einige Gefahren im Bereich der Sicherheit in sich. Steuerungsdaten, Personendaten und Messdaten sind durch die immer voranschreitende Verknüpfung des Internets mit der Energiewirtschaftswelt auch möglichen kriminellen Handlungen und unerlaubten Eindringlingen in das Gesamtsystem ausgesetzt. Die Energieunternehmer sind in vielen Fällen nicht ausreichend dafür gerüstet. Dabei ist jedoch festzuhalten, dass das „Internet der Energie“ sich nicht homogen ausbreitet, sondern sich in verschiedenen Segmenten des Energiewirtschaftssystems unterschiedlich ausbreitet. Im Bereich der zentralen Erzeugung (large scale) ist eine Vernetzung nur geringfügig vorhanden. Im Bereich der Verteilung ist hingegen die Einbindung von IKT-Systemen sehr fortgeschritten.
IT-Sicherheit muss folglich von den Unternehmen aufgegriffen und entsprechend der vorhandenen Standards (IT-Governance, COBIT, ISO27001, oder andere) implementiert werden. Die IT-Security ist jedoch in den österreichischen Unternehmen nur unzureichend ausgebaut. Dazu Hans Jörg Pollirer von Securdata:

»Die KMUs sind das Rückgrat – im IT-Jargon würde man sagen, das »Backbone« – der österreichischen Wirtschaft. Von den insgesamt rund 350.000 österreichischen Unternehmen fallen 99,6% unter den europäischen KMU-Begriff. 261.000 österreichische Unternehmen beschäftigen weniger als 10 Mitarbeiter. Sie beschäftigten aber ca. 2 Mio. Mitarbeiter (ca. 65%) und erwirtschaften 56% der gesamten Wertschöpfung.
Angesichts der Bedeutung der KMUs für die österreichische Wirtschaft erhebt sich die Frage, wie es um die IT-Security bei dieser Unternehmensgruppe bestellt ist. Die Antwort auf diese Frage lautet schlicht und einfach: »schlecht«! Bei den meisten KMUs herrscht Unklarheit darüber, welches Risiko etwa Hackerangriffe, Virenschäden oder Serverausfälle für ihren Betrieb darstellen. Während es für die KMUs selbstverständlich ist, z.B. ihr Lager abzusperren, vernachlässigen die meisten die Frage der IT-Security und setzen sich damit unnötig existentiellen Gefahren aus. Und dass es Gefahren gibt und diese im Steigen begriffen sind, zeigen die verschiedensten Sicherheitsstudien internationaler und nationaler Herkunft ganz deutlich auf.«

Sicherheitsroadmap

Gemäß Prof. Claudia Eckert muss die Erstellung einer Sicherheitsroadmap in 5 Schritten erfolgen:

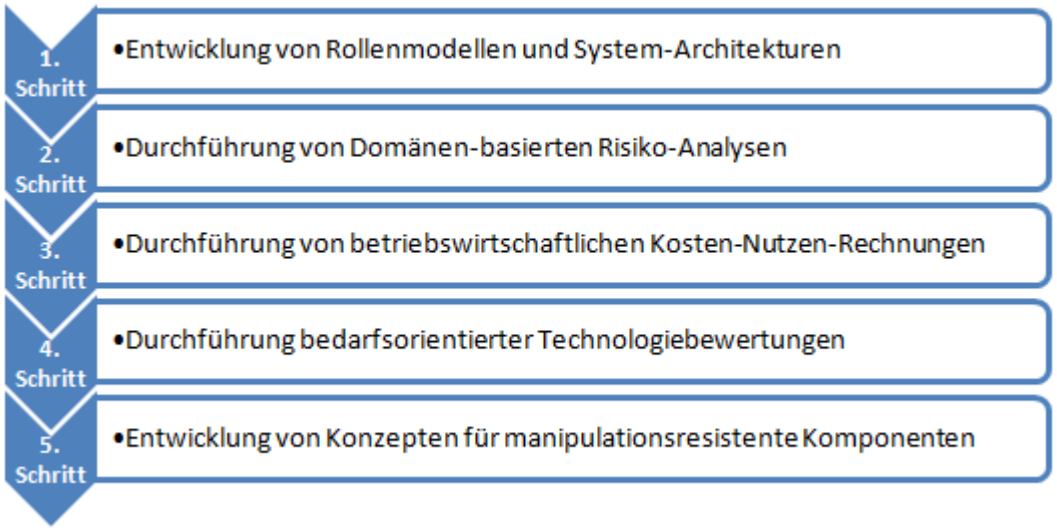

Abbildung 14 Die wichtigsten fünf Schritte zur Erstellung einer Sicherheitsroadmap

1. Schritt[40]
In einem ersten Schritt sollten Rollenmodelle erstellt und Marktteilnehmer-spezifische Subsysteme bzw. Domänen (siehe unten) identifiziert und spezifiziert werden. Das Ziel sollte sein, Verantwortungs- und Aufgabenbereiche abzugrenzen und damit zu beherrschbareren Teilsystemen zu gelangen. Folgende Marktrollen werden in der Regel identifiziert:

- Produzent, Energienutzer, Übertragungsnetzbetreiber,
- Verteilungsnetzbetreiber, Energielieferant
- (Multi-Utility: Strom, Wärme, Gas, Wasser),
- Energiehändler, Messstellenbetreiber, Energiemarktplatzbetreiber,
- Kommunikationsnetzbetreiber,
- Energiedienstleister.

2. Schritt[41]
Das NIST hat u. a. hierzu bereits sehr umfangreiche Vorarbeiten geleistet. Diese gilt es auszuwerten, auf die deutschen bzw. europäischen Gegebenheiten abzubilden und im Sinne eines Handlungsleitfadens für ausgewählte Domänen detailliert auszuarbeiten. Hierzu müssen Angreifermodelle festgelegt und charakteristische Angriffsszenarien definiert werden. Da IT-Sicherheitsangriffe auch gravierende Auswirkungen auf die Betriebssicherheit von Anlagen haben können, sind kombinierte Safety- und Security-Analysen erforderlich, die beispielsweise die Techniken der Fehlerbaumanalyse mit der Risikoanalyse mittels Angriffsbäumen kombinieren. Ausgangspunkt für die Analysen sollten die Architektur-Blueprints für die verschiedenen Domänen sein. Da auch in den abgegrenzten Subsystemen noch eine Vielzahl von Komponenten miteinander interagieren, könnte die Erstellung von Simulationsmodellen hilfreich sein, um multilaterale, kaskadierende Abhängigkeiten nachzubilden und das Ausmaß eines potentiellen Schadens zu verdeutlichen.

3. Schritt[42]
Die Absicherung komplex vernetzter, sicherheitskritischer IKT-Infrastrukturen verursacht erhebliche Mehrkosten. Begleitend zu den Sicherheitsanalysen und Handlungsempfehlungen sollte die Roadmap deshalb auch Kosten-Nutzen-Betrachtungen durchführen, die über die aktuell geführte Diskussion der Anreizmodelle für Endkunden zum Energieeinsparen durch spezielle Tarifmodelle hinausgehen. Hierzu sind Business-Cases (risks versus opportunities) zu entwickeln, die neben den Kosten insbesondere auch die Möglichkeiten der Smart Grid-IKT-Infrastruktur aufzeigen. Vorstellbar ist die Entwicklung von Szenarien für Anwendungsdomänen, die weit über die Energiedomäne hinausreichen. Ein Beispiel wäre der Gesundheitsbereich mit der mobilen, IKT-gestützten, Pflege. In Deutschland sind über 40 Millionen Wohnungen mit einer Smart Meter-Infrastruktur auszustatten, so dass eine rechtzeitige Beachtung von Maßnahmen zur Unterstützung von älteren oder Personen mit Einschränkungen hier wirtschaftlich interessante Mehrwerte für Betreiber von Wohnanlagen und Anreize zur Investition schaffen könnte.

4.Schritt[43]
Um die ermittelten Sicherheitsbedarfe zu erfüllen, sind angemessene Sicherheitstechnologien und Sicherheitsmaßnahmen einzusetzen. Die Roadmap sollte auch hierfür Handlungs-

[40] Sicherheit im Smart Grid Eckpunkte für ein Energieinformationsnetz; sicherheitimsmartgrid2-120113033743-phpapp01.pdf; Seite 30 ff.
[41] Sicherheit im Smart Grid Eckpunkte für ein Energieinformationsnetz; sicherheitimsmartgrid2-120113033743-phpapp01.pdf; Seite 30 ff.
[42] Sicherheit im Smart Grid Eckpunkte für ein Energieinformationsnetz; sicherheitimsmartgrid2-120113033743-phpapp01.pdf; Seite 30 ff.
[43] Sicherheit im Smart Grid Eckpunkte für ein Energieinformationsnetz; sicherheitimsmartgrid2-120113033743-phpapp01.pdf; Seite 30 ff.

empfehlungen beinhalten. Dazu sind die vorhandene Technologien zu analysieren und in Bezug auf ihre Einsetzbarkeit zu bewerten. Das Ziel sollte hierbei sein, erprobte und gut eingeführte Sicherheitsstandards so weit wie möglich zu übernehmen und aufzuzeigen, wo ergänzende Sicherheitsmaßnahmen notwendig werden. Die Roadmap sollte Einsatzempfehlungen für Technologien und Kontrollmaßnahmen enthalten, die zur Erfüllung der spezifischen Sicherheitsbedarfe der Domänen, aber auch einzelner Use Cases, geeignet sind. Der nachhaltig sichere Betrieb von Anlagen und Plattformen wird eine große Herausforderung für Betreiber und Dienstleister werden. Die Roadmap sollte hierzu bereits Muster für betriebswirtschaftlich angemessene Betriebskonzepte erarbeiten, die Empfehlungen für datenschutzrechtliche Prozesse und das Sicherheitsmanagement geben, um das einmal erstellte Schutzniveau über den Lebenszyklus der Anlage aufrecht zu erhalten.

5. Schritt[44]
Die wichtigsten FuE-Bereiche betreffen die Entwicklung von Konzepten für manipulationsresistente Komponenten wie Zähler, die die Daten aktuell, manipulationsgeschützt (gegen Angriffe von innen und außen) und datenschutzbewahrend erheben, (vor)verarbeiten und kommunizieren. Es werden skalierende Identifikations- und Authentisierungsschemata für die Maschine-zu-Maschine-Kommunikation benötigt, die im Smart Grid eine große Bedeutung erlangen wird. Weitere offene Fragestellungen betreffen die Entwicklung effizienter, sicherer Schlüsselmanagementverfahren unter Berücksichtigung betrieblicher Kosten, die Entwicklung von rollenbasierten Zugriffskontroll- und insbesondere Nutzungskontrollverfahren, die auch für ressourcenbeschränkte Komponenten verwendbar sind.

Aus gesellschaftlich-politischer Sicht ist die Erstellung einer Roadmap auch von der Teilnahme aller relevanten Akteure (Erzeuger, Übertrager, Verteiler, Technologieanbieter, u.a.) abhängig. Nur sie können die notwendigen Expertisen einbringen und Erkenntnisse zum aktuellen Stand der Smart Grids Security Forschung liefern. In Österreich und der Schweiz werden Anstrengungen unternommen, die Smart Grids Sicherheit durch konkrete Maßnahmen zu erhöhen. Zur Erreichung der notwendigen Sicherheit im Energiebereich wird eine Roadmap vorgeschlagen, die im Rahmen des Smart Grids Security Workshops mit relevanten Akteuren diskutiert wird.

Abbildung 14: Roadmap zur gemeinsamen Sicherheitsdoktrin für Smart Grids; Quelle: Fichtner IT

1) BMVIT, BFE Workshops

   Im Rahmen der Smart Grids Sicherheit werden in Österreich und der Schweiz verschiedene Workshops abgehalten (in AT z.B. „IKT als Enabler", Februar 2012). Die meisten Aktivitäten sind überwiegend in spezialisierten Unternehmerkreisen zu finden. Insbesondere Sicherheitsberatungsfirmen haben die vorhandene Nachfrage erkannt und organisieren immer mehr Sicherheitsworkshops. Einzelne Untersuchungen zum Thema IT-Sicherheit bei Energieversorgern haben ein hohes Defizit in diesem Bereich erkennen lassen.

2) Smart Grids Week Bregenz 2012

   Im Rahmen der Smart Grids Week Bregenz wurden Workshops zum Thema Sicherheit abgehalten. Diese sollen als Impulsveranstaltung dienen und die Sicherheitsthematik in den Vordergrund rücken. Das Ziel dabei ist es, ein

[44] Sicherheit im Smart Grid Eckpunkte für ein Energieinformationsnetz; sicherheitimsmartgrid2-120113033743-phpapp01.pdf; Seite 30 ff.

gemeinsames Committment zu schaffen und die Sicherheit im Smart Grids als ganzheitliches Thema aufzufassen. Die einzelnen Teilnehmer sind sich ihrer Verantwortung bewusst und tragen aktiv zur Lösung der zukünftig notwendigen Sicherheitslösung bei.

3) Kontinuierliche Arbeitsgruppe oder Plattform

   Als Ergebnis der Aktivitäten in Bregenz sollen in Österreich und in der Schweiz je eine Plattform entstehen, in der die wichtigsten Akteure im Energie- und Sicherheitsbereich die sicherheitsrelevanten Aufgaben aufgreifen und Lösungen erarbeiten. Die Plattformen dienen auch den politischen Akteuren als Ratgeber, um eine länderübergreifende und koordinierte Entwicklung in dieser Thematik zu ermöglichen. Die Erstellung dieser Arbeitsgruppe muss aber international koordiniert werden. Es wird empfohlen einen Sicherheitsberater in Verbindung mit Vereinigungen (z.B. FEEI in AT) aus den teilnehmenden Ländern (z.B. D-A-CH Region) hinzuzuziehen, der dann die Koordination übernehmen sollte.

4) Sicherheitsdoktrin

   Gegen Ende des Jahres 2013 soll als Ergebnis aller vorhergehenden Aktivitäten eine Sicherheitsdoktrin erarbeitet werden. Hier werden alle wesentlichen Erkenntnisse, Vorgaben, Standards, sowie die gesellschaftliche und politische Verantwortung zum Thema der energetischen Versorgungssicherheit festgehalten und entsprechende Vorgaben zum Handeln definiert werden. Die Erarbeitung einer Sicherheitsdoktrin ist jedoch ein langer Prozess, der mit verschiedenen Akteuren aus Politik und Wirtschaft zusammengestellt, diskutiert und beschlossen werden muss. Mehrere Security Workshops werden dazu nötig sein. Eine professionelle Koordination wird empfohlen

Zusammenfassung AP 1.4, 1.5

Zusammenfassend ist zu empfehlen, dass die Ministerien BFE und BMVIT folgende Maßnahmen umsetzen:

- Errichtung einer Arbeitsgruppe „Smart Grids Security“
- Zusammenstellung einer Expertengruppe zur Erstellung einer Sicherheitsdoktrin
- Erarbeitung einer Security Roadmap mit den hier dargelegten Rahmenbedingungen und Zielen

Literatur (Auszug)

1) „Securing the Smart Grids“ – Next Generation Power Grid Security. Tony Flick, Justin Morehouse; Verlag Elsevier, ISBN 978-1-59749-570-7
2) Smart Grids Security – An End to End View of Security in the New Electrical Grid, Gilbert N. Sorebo and Michael C. Echols; CRC Press Taylos & Francis Group; ISBN 978-1-4398-5587-4
3) “Black Out”, Marc Elsberg, Roman, blanvalet Verlag