White Paper

Systematisierung der Sicherheits-aspekte von Smart Grids

Finale Version

AIT Austrian Institute of Technology GmbH • Technische Universität Wien

Dokumenteninformation	
Titel	White Paper „Systematisierung der Sicherheitsaspekte von Smart Grids“
Editor	Thomas Bleier, Lucie Langer
Autoren	Thomas Bleier, Lucie Langer (AIT Digital Safety & Security Department) Friederich Kupzog (AIT Energy Department) Georg Kienesberger, Marcus Meisel (TU Wien, Institut für Computertechnik)
Erzeugt am	12.05.2014
Letzte Änderung am	23.09.2015
Status	☐zur projektinternen Verwendung ☒öffentlich – freigegeben von: Auftragnehmer AIT ☐eingeschränkter Zugriff für:

Inhaltsverzeichnis

1 Executive Summary

Die Entwicklung von intelligenten Energienetzen (Smart Grids) wird insbesondere in Europa als Enabler für die Umsetzung langfristiger Energiepolitik gesehen. Die Implementierung dieser Intelligenz erfordert ein hohes Maß an Informations- und Kommunikationstechnologie (IKT) zur Steuerung der Energieflüsse. Die dadurch entstehende enge Kopplung der Energieversorgung mit dem IT-Netzwerk ist Chance und Risiko zugleich – zum einen ergeben sich dadurch viele neue Möglichkeiten, um automatisiert, schnell und geographisch weit verteilt Steuer- und Regelungsmaßnahmen umzusetzen – zum anderen ist aber damit auch die Energieversorgung möglichen neuen Bedrohungen aus dem IT-Bereich ausgeliefert. Es ergeben sich außerdem Fragen der Zuverlässigkeit, in bestimmten Fällen auch der Personensicherheit und des Datenschutzes. Daher ist für eine erfolgreiche Umsetzung „smarter“ Energienetze eine intensive Auseinandersetzung mit dem umfassenden Thema „Sicherheit“ unumgänglich.

Das vorliegende White Paper präsentiert eine systematisierte Darstellung der Sicherheitsaspekte im Smart Grid, um auf einer strategischen Ebene folgende drei Fragen zu beantworten: a) was ist grundsätzlich notwendig für die Entwicklung sicherer Smart Grids, b) was gibt es schon und c) was soll in Zukunft geschehen. Dabei sollen keine konkreten Lösungen oder Maßnahmen im Fokus stehen, sondern systematisch die Bereiche analysiert und dargestellt werden, die für die Sicherheit intelligenter Energienetze von hoher Bedeutung sind.

Die Umsetzung erfolgte über eine Analyse relevanter Literatur (insbesondere auch die Ergebnisse der ISGAN- und Acatech-Arbeitsgruppen zu diesem Thema) und darauf aufbauenden Expertengesprächen, um eine möglichst breite thematische Abdeckung zu erreichen. Auf Basis von etablierten Darstellungen wie den Acatech-Zukunftsszenarien und den Interoperabilitätsschichten des GridWise Architecture Council (welche auch die Basis für die Entwicklung des Smart Grid Architecture Models(SGAM) [1] gelegt haben) wurde eine Segmentierungsmatrix erstellt, um systematisch alle Aspekte abdecken zu können. Darauf aufbauend erfolgte die Erarbeitung der vorhandenen und noch zu erforschenden Themen, um die Sicherheit zukünftiger Smart Grids in allen Aspekten (Security, Privacy, Safety, Resilienz, etc.) umsetzen zu können.

Auf Basis dieser Untersuchungen wurden eine Reihe von Chancen, sowie Folgerungen und Handlungsempfehlungen erarbeitet, und diese auch mit einem Expertenbeirat diskutiert und abgestimmt. Einige wesentliche Ergebnisse daraus sind:

- Die Integration von Informationstechnologie in Energienetze bietet neben Risiken auch eine Reihe von Chancen zur Steigerung der Resilienz der Energieversorgung gegenüber Ausfällen, die systematisch untersucht und genutzt werden sollten (beispielsweise Reduktion der Abhängigkeiten durch Nutzung lokal vorhandener und erneuerbarer Ressourcen oder zelluläre Konzepte zur Diversifizierung und Erhöhung der Resilienz des Gesamtsystems).

- Die Betrachtung der Sicherheitsaspekte muss von Beginn an in den Entwicklungsprozess integriert werden. Ein „Security by Design“-Ansatz ist kosteneffizient und reduziert Folge- und Kollateralschäden. Andererseits muss zugleich eine Wirtschaftlichkeitsbetrachtung neuer Technologien und Systeme auch unter dem Gesichtspunkt einer Vollkostenbetrachtung stattfinden (inklusive der notwendigen Sicherheitsmaßnahmen zur Gewährleistung eines ausreichenden Sicherheitsniveaus).

- Die gesetzlichen und regulatorischen Rahmenbedingungen müssen eine Betrachtung der Sicherheitsaspekte integrieren, um unterschiedliche Sichtweisen der einzelnen Stakeholder auszugleichen und die Umsetzung der gesellschaftlichen Anforderungen an eine sichere Energieversorgung zu gewährleisten.

2 Einleitung und Problemstellung

Ziel des vorliegenden White Paper ist eine Darstellung eines Gesamtbildes der Sicherheitsaspekte von Smart Grids. Dabei sollen sowohl Aspekte von Safety (Schutz von Menschen vor einem System), als auch von Security (Schutz des Systems vor Angriffen von außen) und Privacy (Schutz personenbezogener Daten) betrachtet und eingeordnet werden. Themen wie Resilienz (Widerstandsfähigkeit gegenüber Störungen) und Reliability (technische Zuverlässigkeit) werden ebenfalls berücksichtigt.

Das White Paper behandelt dabei die folgenden zentralen Fragen:

1. Was ist grundsätzlich notwendig für die Entwicklung sicherer Smart Grids?
2. Was gibt es schon?
3. Was soll geschehen/Empfehlungen?

Zur Beantwortung der ersten Frage wird daher zuerst ein generelles Gesamtbild skizziert, welches im Wesentlichen auf alle relevanten Sicherheitsaspekte (Security, Safety, Versorgungs-, Ausfallssicherheit, Verfügbarkeit, Resilienz, etc.) sowie Privacy eingeht und die entsprechenden Fragestellungen bzw. Herausforderungen systematisch aufbereitet. Die zentrale Fragestellung ist hierbei, welche Rückwirkungen und Anforderungen, welche sich aus der Bearbeitung der einzelnen Sicherheits- und Privacy-Aspekte ergeben, auf bzw. an das Systemdesign und die (Referenz-) Architektur von Smart Grids zu erwarten sind, damit den Zielsetzungen von Smart Grids bezüglich der Sicherheitsthematik entsprochen werden kann. Hierbei wird auch das Spektrum der Einflussfaktoren und Freiheitsgrade, die einzelnen Sicherheitsaspekte betreffend, aufgezeigt und eine Priorisierung der einzelnen Thematiken auch unter dem Kostenaspekt diskutiert.

Des Weiteren werden auch Ansätze dargestellt, in welchen Bereichen neue Smart-Grid-Lösungen trotz der neuen Herausforderungen für das Energiesystem (wie z.B. hohe Durchdringung von volatilen, verteilten Einspeisern) unter den Randbedingungen von Liberalisierung und Unbundling einen positiven Beitrag zu bestehenden Themen wie Versorgungssicherheit und Verfügbarkeit leisten könnten. Jedoch wird auch hinterfragt, inwieweit diese innovativen Technologien auch neue Herausforderungen im Bereich der Security, Safety und Privacy mit sich bringen, und entsprechender Forschungsbedarf festgestellt.

Der Fokus der Betrachtung liegt in dieser Arbeit auf den Elektrizitätsnetzen, wobei soweit nötig auch Querverbindungen zu anderen Versorgungsnetzen für Energie- und Stoffmengen hergestellt werden. Weiters steht die *geschlossene Systemebene* und die *IKT[1]-Infrastrukturebene* im Zentrum (siehe Graphik auf S. 23 der Acatech-Studie Future Energy Grid [2]). Schnittstellen zu den Entitäten der *vernetzten Systemebene* [2] wie z.B. Kraftwerke, Speicher, Elektromobilität, etc. werden zwar ebenfalls betrachtet, die eigentlichen Smart-Grid-Entitäten bzw. -Anwendungen selbst sind aber außerhalb des Rahmens dieser Arbeit.

Ein weiterer Schwerpunkt dieser Arbeit ist die IKT-Sicherheit wobei Ansätze zur Entwicklung einer differenzierten Sichtweise aufgezeigt werden, welche eine grobe Abgrenzung von der im klassischen Netzausbau stattfindenden Durchdringung mit IKT von der zielgerichteten Entwicklung von Smart Grids erlaubt.

Das White Paper basiert grundsätzlich auf dem aktuellen, internationalen State of the Art welcher auch in Grundzügen systematisch dargestellt wird, um einen Überblick über aktuelle, sicherheitsrelevante Smart-Grid-Forschung zu geben. Besonderes Augenmerk wird auf die Ergebnisse von ISGAN Annex 4 [3], die Acatech-Studie Future Energy Grid [2], sowie den Diskussionsinput aus

[1] Informations- und Kommunikationstechnologie

den Smart Grid Security Roundtables des Bundesministerium für Verkehr, Innovation und Technologie (BMVIT) gelegt. Weiters wird ein systematischer Überblick über sicherheitsrelevante Normen und Standards für Smart Grids gegeben.

Abschließend werden grundlegende Handlungsempfehlungen für Forschung, Industrie und den institutionellen Rahmen erarbeitet, fokussiert auf das Themenfeld Smart Grids. Die Empfehlungen betreffen sowohl den Bereich der IKT, als auch den der Energiewirtschaft bzw. -forschung, wobei der bestehende Bedarf an Forschung und Entwicklung genauso wie die Erfordernisse für organisatorische und institutionelle Weiterentwicklung im Fokus stehen. Zusätzlich werden potentielle österreichische Stärkefelder in der Forschung sowie Möglichkeiten für den internationalen Technologietransfer identifiziert.

3 Methodik

Für die Behandlung von Sicherheitsaspekten von Smart Grids ist eine adäquate Segmentierung des Gegenstandes „Smart Grid“ unumgänglich, denn nur so wird eine systematische Analyse möglicher Sicherheitsaspekte möglich. Entsprechend ist der erste Schritt der hier angewandten Methodik, eine solchen Segmentierung zu erarbeiten, um daraus systematisch die wesentlichen offenen Fragen zu Sicherheitsaspekten von Smart Grids ableiten zu können.

Die Segmentierung der Themenbereiche innerhalb von Smart Grids ist eine Fragestellung, die in den vergangen Jahren unterschiedlich beantwortet wurde, weil sich das Bild des Smart Grids mehrfach gewandelt hat. Als ein in diesem Zusammenhang wesentliches Ergebnis der letzten Jahre hat sich eine Konkretisierung dessen ergeben, was ein Smart Grid ausmacht.

3.1 Überblick

Um zu einer Segmentierung der Themenbereiche innerhalb von Smart Grids zu gelangen, ist es zunächst notwendig, die in diesem Bereich vorherrschende Technologieentwicklung abzubilden (vgl. Abbildung 1). In einem fiktiven multidimensionalen Lösungsraum für elektrische Energiesysteme, der alle unter Einhaltung der physikalischen Gesetzmäßigkeiten mögliche Ausprägungen enthält, ist der heute vorzufindende Stand der Technik ein Punkt, der zugleich Ausgangpunkt für den Vektor der Technologieentwicklung hin zu Smart Grids ist. Smart Grids selbst bilden eine Teilmenge des oben beschriebenen Lösungsraums.

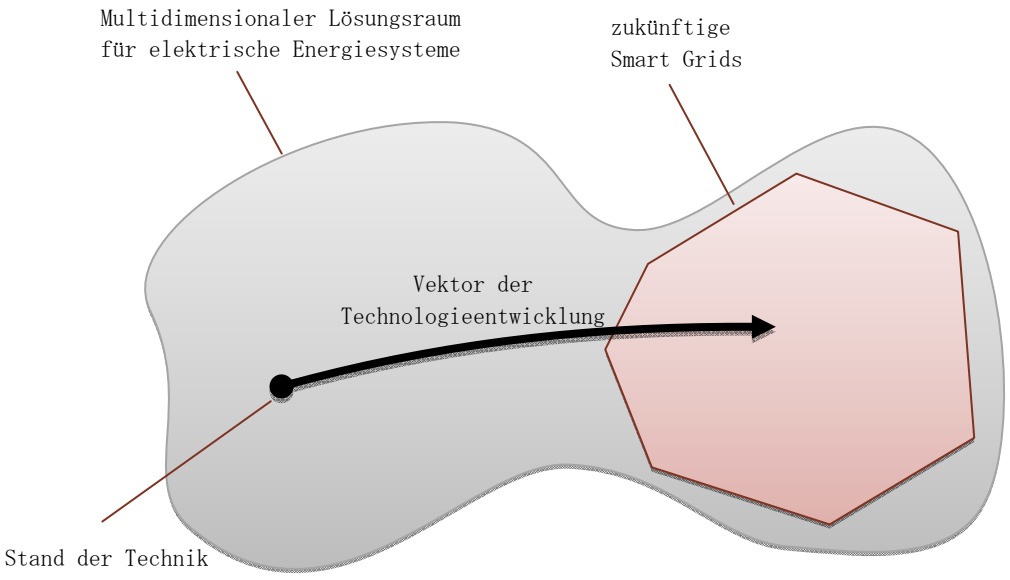

ABBILDUNG 1:MULTIDIMENSIONALER LÖSUNGSRAUM FÜR ELEKTRISCHE ENERGIESYSTEME

Zur Orientierung können in diesen Raum nun die heute vorliegenden Arbeiten zu Sicherheitsaspekten in elektrischen Energiesystemen bzw. Smart Grids zeitlich eingeordnet werden. Dies ist beispielhaft in Abbildung 2 für wesentliche Referenzdokumente dieses White Papers durchgeführt worden.

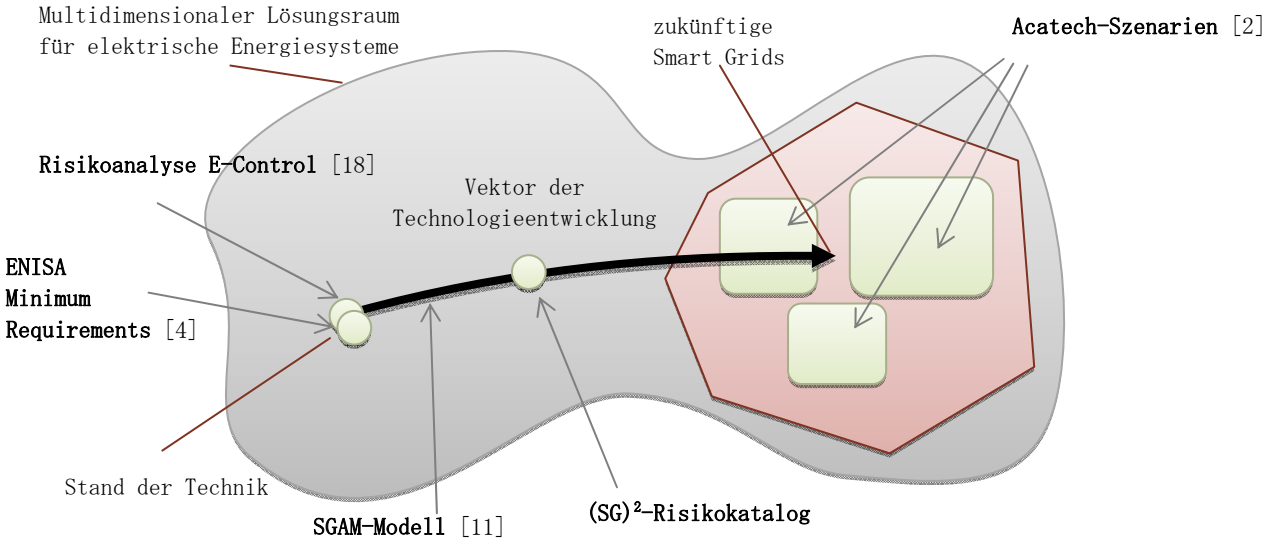

ABBILDUNG 2:EINORDNUNG DER WESENTLICHEN REFERENZDOKUMENTE DIESES WHITE PAPERS IN DEN SMART GRIDS LÖSUNGSRAUM

Es liegt auf der Hand, dass sich heute vorliegende Risikoanalysen vornehmlich auf den Stand der Technik beziehen, und noch nicht auf die aus heutiger Sicht unvollständig geklärte Ausprägung von Smart Grids. Genau hier liegt aber die besondere Bedeutung des in der Abbildung dargestellten Vektors der Technologieentwicklung. Diese wesentliche Frage ist ja: Welche *neuen Aspekte* ergeben sich aus der Entwicklung zu Smart Grids? Entsprechend konzentriert sich dieses White Paper auf die Analyse der Auswirkungen (auf das Delta) dieses Vektors der Technologieentwicklung, und nicht auf die Situation im Startpunkt, die durch andere Studien bereits abgedeckt ist. Dadurch wird eine Analyse von Faktoren wie Security, Safety, Security, Privacy, etc. basierend auf dem Ist-Stand möglich.

3.2 Sicherheitsbegriff

Dieser Abschnitt spannt den Sicherheitsbegriff auf, welcher den folgenden Ausführungen in diesem White Paper zugrunde liegt. Dazu werden einerseits die Einflussfaktoren im Bereich der Sicherheit, und andererseits die Einflussfaktoren im Hinblick auf Sicherheitsbedrohungen zusammengefasst.

Einflussfaktoren Sicherheit (vgl. [4, 5]):

- Organisatorische Maßnahmen und Sicherheitsprozesse
- Sicherheit der Entwicklung und Inbetriebnahme neuer Komponenten
- Sicherheit der Kommunikation
- Sicherheit der Betriebsabläufe und Prozesse
- Physische Sicherheit
- Behandlung von Sicherheitsvorfällen
- Wiederherstellung im Katastrophenfall
- Compliance zu rechtlichen Rahmenbedingungen

Einflussfaktoren Bedrohungen (vgl. [5, 6, 7, 8, 9, 10, 11]):

- Safety (Schutz)
  - Betriebssicherheit – Personenschutz
  - Betriebssicherheit – Anlagenschutz
- Reliability (Technische Zuverlässigkeit)
- Security (Angriffssicherheit):
  - Availability (Verfügbarkeit)
  - Integrity (Integrität)
  - Confidentiality (Vertraulichkeit)
- Privacy (Datenschutz)

3.3 Systematik

Die in diesem White Paper angewandte Systematik zur Segmentierung der Themenbereiche innerhalb von Smart Grids basiert einerseits auf den Dimensionen des Technologieentwicklungsvektors, andererseits auf einer Interoperabilitätseinteilung, wie sie auch beim Smart Grid Architecture Model (SGAM) [1] zur Anwendung gelangt ist.

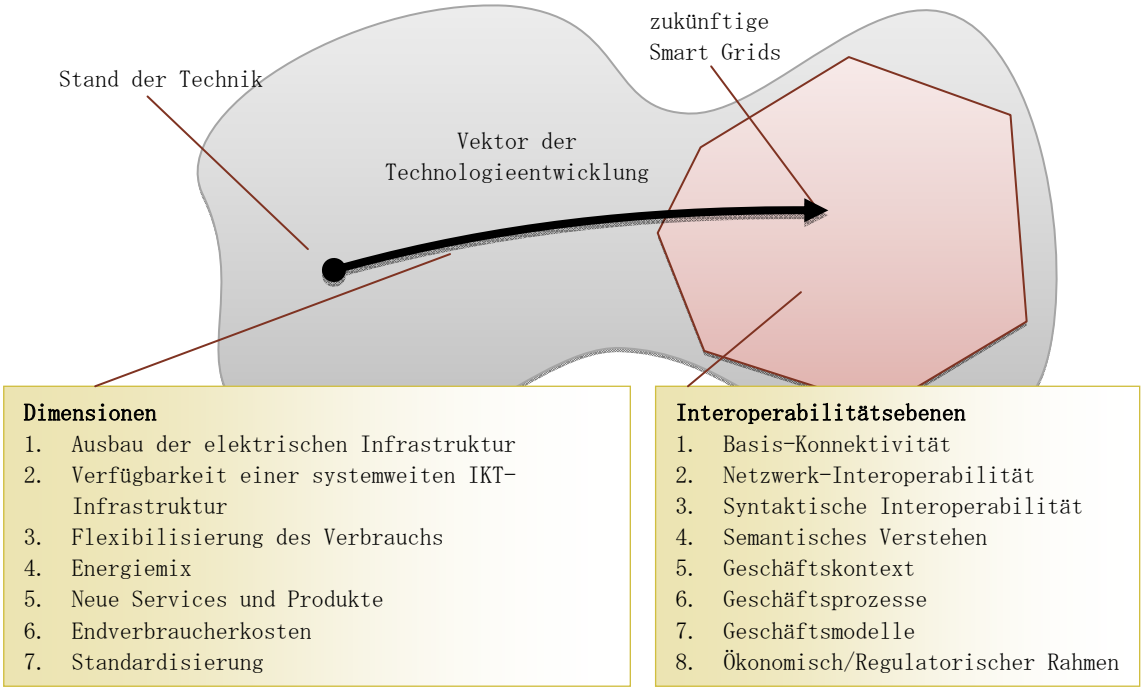

ABBILDUNG 3: DIMENSIONEN DER TECHNOLOGIEENTWICKLUNG UND EBENEN DER INTEROPERABILITÄT ALS ZENTRALE KATEGORIEN FÜR DIE SYSTEMATISCHE UNTERSUCHUNG VON SICHERHEITSASPEKTEN

Dimensionen des Technologieentwicklungsvektors

Die Acatech-Studie [2] definiert acht Schlüsselfaktoren für die Entwicklung von Smart Grids, die hier als Dimensionen des Technologieentwicklungsvektors gewählt wurden (vgl. Abbildung 3). In jedem Schlüsselfaktor gibt es verschiedene mögliche Änderungen, die grob in den Szenarien der Acatech-Studie [2] eingeteilt sind (siehe Abbildung 4): Das Szenario „20. Jahrhundert“ beschreibt eine Situation, in der wesentliche Ansätze des Smart Grids nicht umgesetzt wurden, was zu signi-

fikanten wirtschaftlichen Nachteilen führt. Das Szenario „Komplexitätsfalle“ schildert eine aufgrund von konkurrierenden Einzelinteressen und inkonsistente Rahmenbedingungen unvollständige bzw. nicht einheitliche Lösung. Das Szenario „Nachhaltig Wirtschaftlich“ beschreibt die Situation einer deutlich verstärkten dezentralen Einspeisung aus regenerativen Energiequellen, mit entsprechenden technologischen und marktbasierten Maßnahmen zur Kompensation der Fluktuationen [2]. Mit diesen drei Entwicklungsszenarien ergeben sich verschiedene Ausprägungen für die einzelnen Schlüsselfaktoren, siehe Abbildung 4. Diese Änderungen werden in diesem White Paper genauer auf ihre Auswirkungen auf Sicherheitsaspekte untersucht. Dabei werden auch neu hinzukommende Faktoren bzw. sich ändernde oder wegfallende Faktoren berücksichtigt (Versorgungssicherheit/Abhängigkeit sowie Ausfallssicherheit/Verfügbarkeit, Widerstandsfähigkeit/Resilienz, Verletzlichkeit/Vulnerabilität, Personensicherheit, etc.).

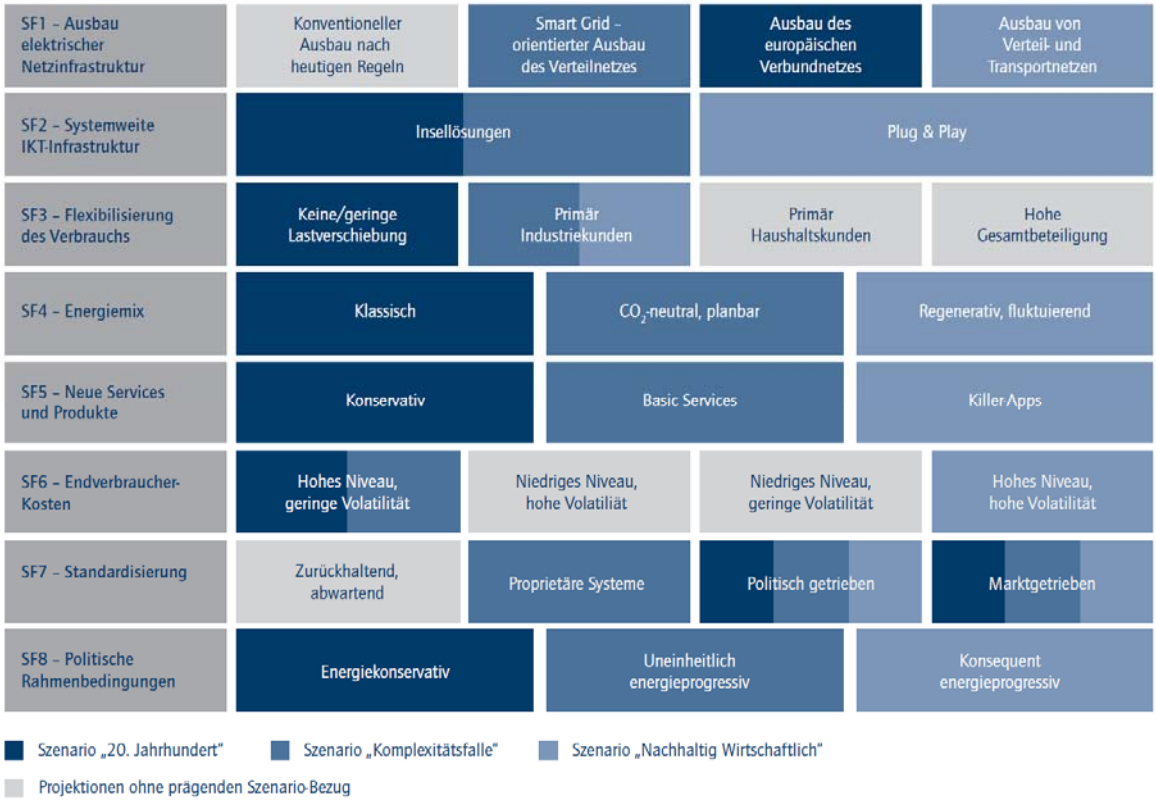

ABBILDUNG 4:EINTEILUNG DER SCHLÜSSELFAKTOREN UND ZUSAMMENFASSUNG IN DREI SZENARIEN (SIEHE [2])

Interoperabilitätsebenen

Das wesentliche Element im Smart Grid ist die Einbindung der beteiligten Akteure und der entsprechenden technischen Komponenten vom Stromzähler über flexible Lasten und Wechselrichter bis hin zu Stufentransformatoren und andere aktive Stromnetzkomponenten in ein oder mehrere IKT-Netze im Sinne einer gemeinsamen Koordination aus Netz- oder Marktsicht. Dementsprechend spielt die Interoperabilität der Komponenten im Smart Grid eine zentrale Rolle. Neue Stakeholder führen zu neuen Schnittstellen, Interaktion kann prinzipiell auf allen Ebenen des Systems auftreten. Dabei spielt sich Interoperabilität nicht nur auf der rein technischen Ebene ab, sondern umfasst weitere Ebenen von der Konnektivität, Syntax, Semantik, bis hin zu Geschäftsprozessen, -modellen und Rahmenbedingungen. Ein geeignetes Modell für die Einteilung der Ebenen von Interoperabilität ist das „GridWise Interoperability Context-Setting Framework“ [12]. Dieses stand selbst Pate bei der Definition der Layer im Smart Grids Architecture Model (SGAM)

[1] und wurde 2007 vom GridWise Architecture Council (GWAC) Interoperability Framework Team veröffentlicht.
Vor dem Hintergrund der steigenden Automatisierung in allen Bereichen des Stromnetzes – von Kraftwerken bis zum Prosumer – sieht der GWAC seine Aufgabe darin, die Interoperabilität zwischen den zahlreichen unterschiedlichen Entitäten, die mit dem elektrischen Energienetz interagieren, sicherzustellen. Das „GridWise Interoperability Context-Setting Framework“ soll dazu dienen, Konzepte und Terminologie zu organisieren und strukturiert festzuhalten, sodass Interoperabilitätsprobleme identifiziert und effizient von den verschiedenen Experten in der (Smart) Grid Community diskutiert werden können, um koordinierte und priorisierte Lösungen zu finden [12].

Im Zentrum dieses Frameworks stehen die Interoperabilitätskategorien oder –Layer wie in Abbildung 5 dargestellt. Diese werden im Folgenden als Zeilen der Segmentierungsmatrix (siehe Abbildung 6) herangezogen und in den folgenden Kapiteln, die Sicherheitsaspekte jeden dieser Layer betreffend, jeweils zu Beginn beschrieben.

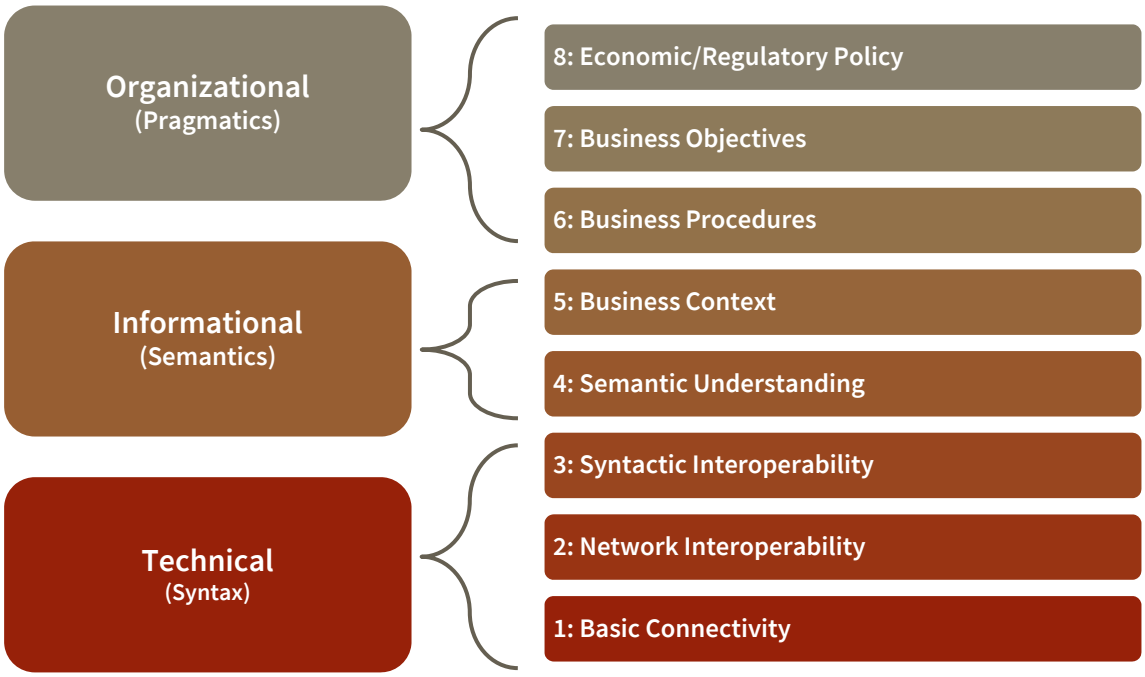

ABBILDUNG 5: GRIDWISEINTEROPERABILITYLAYERS [12]

Resultierende Segmentierungsmatrix

Aus den Dimensionen des Technologieentwicklungsvektors und den Interoperabilitätsebenen ergibt sich die in diesem White Paper verwendete Segmentierungsmatrix, die in Abbildung 6 dargestellt ist.

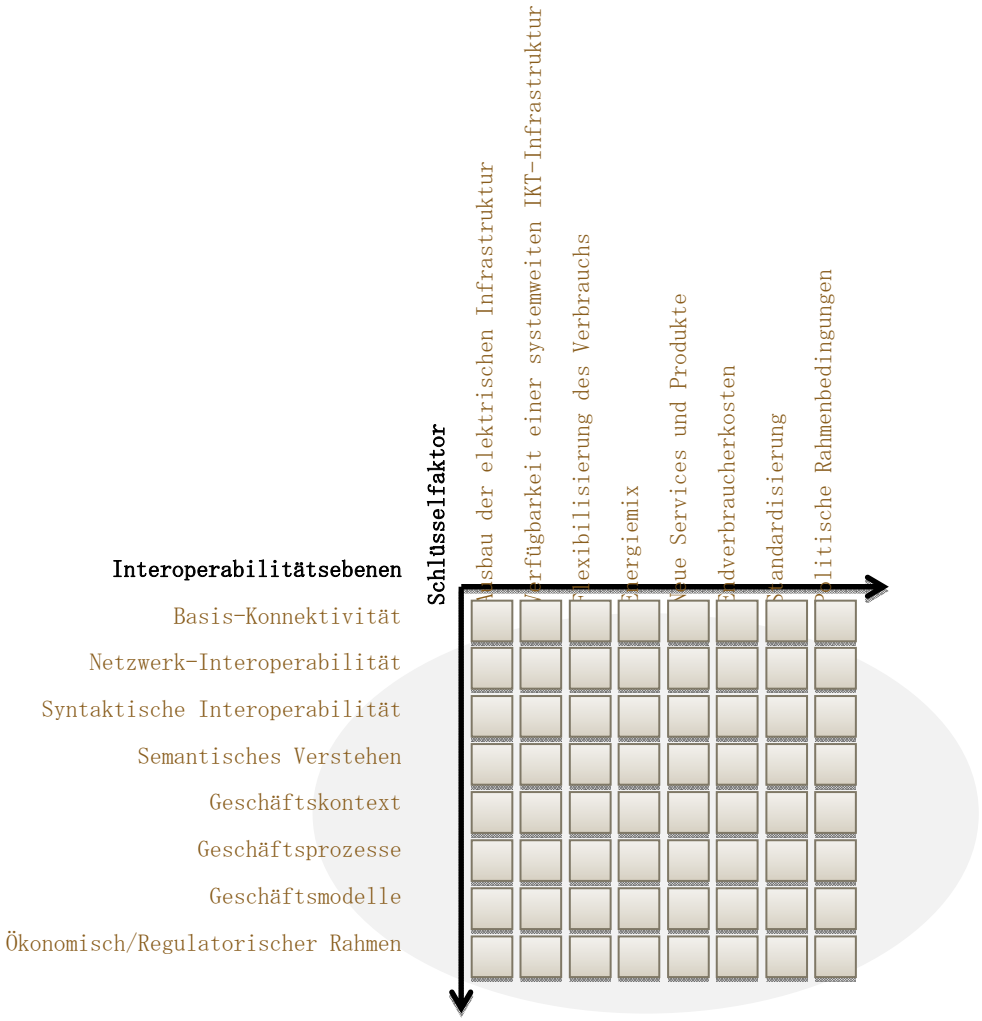

ABBILDUNG 6: SEGMENTIERUNGSMATRIX

Für jede Zelle der Matrix kann untersucht werden:

1. Was ist notwendig, um Sicherheit im Sinne von Security, Privacy, Safety und Resilienz zu gewährleisten?
2. Was gibt es schon?
3. Wo gibt es Forschungsbedarf?

Durch die systematische Bearbeitung dieser Matrix ist sichergestellt, dass keine wesentlichen Aspekte verloren gehen. Dabei wird das Zielbild des Smart Grids einerseits durch die oben bereits diskutierten Acatech-Szenarien, anderseits durch die derzeit in Österreich entwickelten Smart-Grid-Use-Cases definiert. Basis für letztere ist das $(SG)^2$-Referenzmodell [13], welches

aus einer systematischen Analyse der in Österreich und international laufenden Smart-Grid-Projekte entstanden ist.

3.4 Prozess

Auf Basis dieser Systematik wurde im Rahmen von Expertengesprächen eine ausführliche Aufarbeitung der einzelnen Zellen der Matrix durchgeführt, welche die Grundlage für die Darstellung im White Paper darstellen. Die Erarbeitungen wurden durch das Feedback von weiteren Experten sowie dem durch das BMVIT definierten wissenschaftlichen Beirat ergänzt und konsolidiert. Auf Basis der erarbeiteten Ergebnisse zum Forschungsbedarf wurden weiters Handlungsempfehlungen abgeleitet, welche in Kapitel 7 dargestellt sind.

Das White Paper ist dabei wie folgt strukturiert: Nach der Darstellung der Methodik in Kapitel 3 gibt Kapitel 4 einen Überblick über die Ausgangslage und den aktuellen Stand der Technik in Bezug auf die Themen, die durch das White Paper abgedeckt werden. Anschließend wird in Kapitel 5 die eigentliche Analyse der Hauptfragestellungen entlang der beiden Segmentierungsdimensionen durchgeführt. Kapitel 6 identifiziert die Chancen im Smart Grid, indem es erläutert, inwieweit Smart-Grid-Lösungen einen positiven Beitrag zur Versorgungssicherheit leisten können. Abschließend werden in Kapitel 7 Folgerungen und Handlungsempfehlungen abgeleitet.

4 Ausgangslage und Stand der Technik

4.1 Internationale Aktivitäten

Die **Deutsche Akademie der Technikwissenschaften (Acatech)** hat 2012 eine Studie veröffentlicht, welche aufzeigen soll, welcher Migrationspfad hin zum *Future Energy Grid* bis 2030 zu verfolgen ist [2]. Hierzu werden zunächst auf Basis von acht Schlüsselfaktoren (Ausbau der elektrischen Infrastruktur, Verfügbarkeit einer systemweiten IKT-Infrastruktur, Flexibilisierung des Verbrauchs, Energiemix, neue Services und Produkte, Endverbraucherkosten, Standardisierung, politische Rahmenbedingungen) drei Szenarien („20. Jahrhundert", „Komplexitätsfalle", „Nachhaltig Wirtschaftlich") dargestellt, welche dieser Migrationspfad adressieren muss. Hierbei entspricht das Szenario „Nachhaltig Wirtschaftlich" am ehesten den Zielsetzungen der (deutschen) Energiewende. Für jedes Szenario werden die notwendigen Technologiefortschritte bzw. Entwicklungsschritte definiert, wobei wechselseitigen Abhängigkeiten der Technologien während der Entwicklung besondere Aufmerksamkeit geschenkt wird. So steht mit dieser Studie eine Gesamtübersicht für jedes Szenario bereit, welche durch diese Abhängigkeiten eine zeitliche Abfolge der notwendigen Entwicklungsschritte darstellen kann. In diesem White Paper werden, wie bereits in Kapitel 3.3 erwähnt, die acht Schlüsselfaktoren aus der Acatech-Studie verwendet um die Spalten der Segmentierungsmatrix (Abbildung 6) zu bilden.

Im Rahmen des **Smart-Grid-Mandats M/490** der EU wurden 2011 die europäischen Standardisierungsbehörden CEN, CENELEC und ETSI damit beauftragt, die Entwicklung von Standards voranzubringen, welche konsistente, interoperable IKT-Architekturen und Prozesse für Smart Grids in Europa definieren. Als Antwort darauf brachte die CEN-CENELEC-ETSI *Smart Grid Coordination Group* einen umfassenden Bericht hervor, der den aktuellen Stand der Standardisierung in Europa zusammenfasst und Empfehlungen gibt, wie ein geordneter, effektiver Standardisierungsprozess in Europa aussehen sollte. Im Bereich Smart Grid Cybersecurity werden hier neue Methoden gefordert, die mit den funktionalen Entwicklungen in diesem Bereich Schritt halten können. Teil des Berichts ist das *Smart Grid Architecture Model (SGAM)*, siehe Abbildung 7. Hierbei handelt es sich um eine Referenzarchitektur mit den folgenden drei Dimensionen: Die *Domains* beschreiben die verschiedenen Stationen der Energieumwandlung von der Energieerzeugung (*Generation*) über die Übertragung (*Transmission*) und Verteilung (*Distribution*) bis hin zu den Verbraucherhaushalten (*Customer Premises*). Die *Zones* stellen die verschiedenen Bereiche des Informationsmanagements dar, welches sich von Prozessen bis hin zu Märkten erstreckt. Domains und Zones spannen die *Smart Grid Plane* auf, in der sich veranschaulichen lässt, innerhalb welcher Zonen bestimmte Wechselwirkungen zwischen einzelnen Domains auftreten. Als dritte Dimension kommen nun noch orthogonal zur Smart Grid Plane verschiedene *Interoperability Layers* hinzu (*Component, Communication, Information, Function* und B*usiness Layer*). Das Modell ermöglicht so die Darstellung von Informationsflüssen zwischen verschiedenen Entitäten eines Smart Grids.

SGAM stellt eine sehr gute Basis für die Darstellung von Smart Grids innerhalb der EU dar. Für konkrete Analysen ist jedoch eine spezifische Instanziierung je EU-Land nötig, da es teilweise große Unterschiede bezüglich der Architektur bzw. der im jeweiligen Land eingesetzten Technologien gibt. Das SGAM-Modell [1] basiert zum Teil auf einer zusammengefassten Version des Gridwise Interoperability Context-Setting Framework [12].

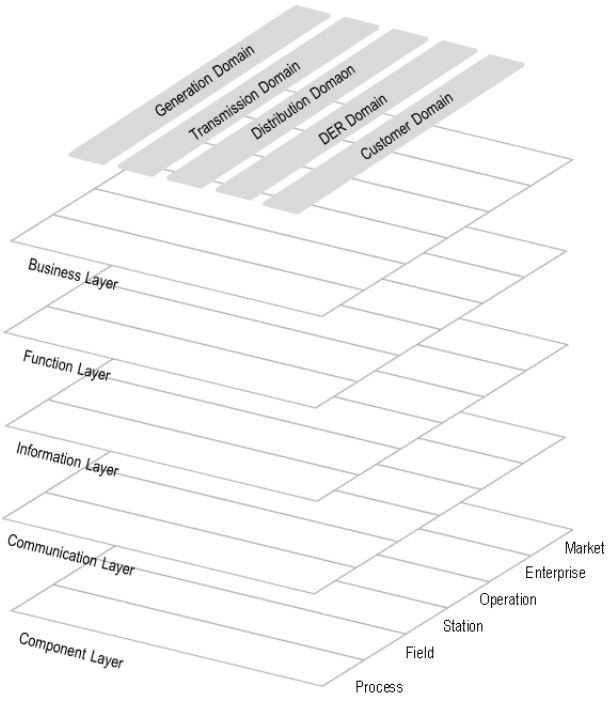

ABBILDUNG 7: DAS SGAM-MODELL [1] BASIERT IN DER Y-ACHSE AUF DEM GRIDWISE INTEROPERABILITY CONTEXT-SETTING FRAMEWORK [12]

Das **International Smart Grid Action Network (ISGAN)** stellt eine weltweite Plattform für den Informationsaustausch auf Behördenebene zur Förderung der Implementierung von Smart-Grid-Technologien dar. Als Teil der Aktivitäten hat ISGAN auch ein White Paper zum Thema „Smart Grid Cyber Security" publiziert [14]. In diesem wird auch auf die Herausforderungen der Entwicklung von Regularien im Bereich Cyber Security im Energiebereich eingegangen. Die zwei wesentlichen Aspekte dabei sind das Thema „Security Economics", also die Wirtschaftlichkeit von Sicherheitsmaßnahmen sowie der Fokus auf „Defense in Depth", also mehrstufige Sicherheitskonzepte, im Gegensatz zu der simplen Erfüllung von Compliance-Maßnahmen.

Die **European Network and Information Security Agency (ENISA)** befasst sich im Rahmen des Zieles, die Informationssicherheit in den EU-Staaten zu erhöhen, auch mit dem Thema Smart Grid Security. So wurden basierend auf existierenden Arbeiten wie NIST-IR 7628 oder ISO 27002 generelle Sicherheitsmaßnahmen für Smart Grids [4] formuliert, welche Netzbetreiber dabei unterstützen sollen, Mindeststandards im Bereich IKT-Sicherheit umzusetzen. Die Maßnahmen sind in zehn Domänen unterteilt und umfassen organisatorische Aspekte ebenso wie Netzwerk-, Betriebs- und Ausfallsicherheit. Um den unterschiedlichen Möglichkeiten bzw. Ressourcen verschieden großer Netzbetreiber Rechnung zu tragen, kann jede Sicherheitsmaßnahme in drei verschiedenen Reifegraden realisiert werden („Frühphase" bis „fortgeschritten"). Neben diesen Maßnahmen hat die ENISA auch generelle Empfehlungen [15] für die Erhöhung der IKT-Sicherheit in Smart Grids formuliert, welche sich an öffentliche wie auch private Institutionen richten. Dabei wird die Bedeutung der rechtlich-regulatorischen Rahmenbedingungen und Einbindung aller relevanter Stakeholder ebenso erkannt wie die Wichtigkeit von Sicherheitstests und Forschungsaktivitäten. Im Dezember 2013 wurde außerdem ein Bericht [16] veröffentlich, der die aktuelle Smart-Grid-Bedrohungslandschaft systematisch aufspannt und konkrete technische wie auch organisatorische Gegenmaßnahmen für die einzelnen Bausteine des Smart Grid definiert.

Im Bereich der **Energieforschung** sowie der **Sicherheitsforschung** gibt es einige Forschungsprojekte, die sich mit dem Thema Smart Grids beschäftigen. Eine Übersicht dazu findet sich z.B. im Report des JRC – Joint Research Center [17].

Die durch das **National Institute for Standards and Technology (NIST)** in den USA eingesetzte Smart Grid Interoperability Panel Cyber Security Working Group (SGIP-CSWG) hat im Rahmen des Standards NIST-IR 7628 [9] Empfehlungen im Bereich Smart Grid Cybersecurity formuliert. Teil 1 definiert ein Architekturmodell, welches die Schnittstellen innerhalb eines Smart Grid kategorisiert; Teil 2 fokussiert auf Datenschutz-Risiken in der Customer Domain, und Teil 3 enthält ergänzendes Material wie z.B. Verwundbarkeitsklassen für Smart Grids. NIST-IR 7628 ist auf US-amerikanische Netze fokussiert und nicht unmittelbar auf die Situation in Österreich übertragbar, da gerade der Security-Bereich sehr stark von nationaler Gesetzgebung abhängt. Dennoch stellt der Bericht eine wichtige Basis für weitergehende Analysen und Konkretisierungen dar.

4.2 Nationale Aktivitäten

Die **E-Control Austria** hat gemeinsam mit der Elektrizitätswirtschaft, vertreten durch Oesterreichs Energie, der Austrian Power Grid (APG), dem Bundeskanzleramt, den zuständigen sicherheitsrelevanten Bundesministerien und dem Kuratorium Sicheres Österreich (KSÖ) eine umfassende Analyse von IKT-Risiken für die nationale Energieinfrastruktur durchgeführt und die Ergebnisse kürzlich im Rahmen eines Berichtes veröffentlicht [18]. In einem strukturierten, auf internationalen Standards basierenden Prozess wurden systemrelevante Risiken für die Versorgungssicherheit durch die IKT-Nutzung identifiziert, klassifiziert und bewertet. Teil der Analyse waren auch Maßnahmen zur Risikominimierung. Als Grundlage für die Risikoanalyse und Erarbeitung von Maßnahmen wurde der Worst-Case-Fall betrachtet; besonderer Fokus lag auf den (Datenschutz-)Risiken, die sich durch die Einführung von Smart Metern ergeben. Die Ergebnisse dieser Analyse werden, soweit verfügbar, als Teil des Technologieentwicklungs-Vektors in das White Paper miteinbezogen.

Im Projekt **Smart Grid Security Guidance (SG)^2**, einem im Rahmen des österreichischen Sicherheitsforschungsprogrammes KIRAS vom BMVIT geförderten Forschungsprojektes, werden Cybersecurity-Risiken im Smart Grid erforscht und entsprechende Sicherheitsmaßnahmen entwickelt. Bisher wurden die Systemarchitekturen von nationalen sowie internationalen Smart-Grid-Pilotprojekten sowie von bestehenden Systemen österreichischer Netzbetreiber analysiert und auf das Smart Grid Architecture Model abgebildet, wobei neben dem aktuellen Stand der Technik auch bereits kurz- bis mittelfristig absehbare Entwicklungen berücksichtigt wurden. Auf diese Weise konnte ein IKT-Architekturmodell für Smart Grids in Österreich definiert werden, welches auf die Sicht der Netzbetreiber (d.h. das Verteilnetz) fokussiert und die Basis für weitere Sicherheitsanalysen bildet. Anschließend wurde auf Basis existierender Arbeiten wie z.B. der Gefährdungskataloge und einschlägigen Schutzprofile des BSI ein Bedrohungskatalog entwickelt und auf die zuvor definierten IKT-Architekturkomponenten angewendet. Durch Schätzung von Eintrittswahrscheinlichkeit und Auswirkungen konnten so die individuellen Risikopotentiale eingeschätzt werden. Komponenten mit besonders hohem Risiko wurden anschließend einer praktischen Sicherheitsanalyse unterzogen, deren Ergebnisse wiederum in den Risikokatalog einfließen werden. Auf diese Weise kann $(SG)^2$ konkrete Hinweise zur Sicherheit aktueller Smart-Grid-Komponenten liefern und praktikable Handlungsempfehlungen für Netzbetreiber formulieren.

Die Nationale Technologieplattform Smart Grids Austria (TP-SGA) koordinierte eine Initiative zur Entwicklung einer Referenzarchitektur für sichere Smart Grids (**RASSA – Reference Architecture for Secure Smart Grids in Austria**). Ziel ist die Entwicklung von Architekturvorgaben, die eine effiziente Entwicklung und Implementierung eines hohen Sicherheitsniveaus für Smart Grid Umsetzungen in Österreich ermöglichen. Dabei soll in einer iterativen Vorgangsweise die Archi-

tektur in verschiedenen Ebenen mit einem breiten Stakeholderkreis diskutiert, niedergeschrieben und auch in Pilotprojekten in der Praxis evaluiert werden. Das erste Projekt dieser Initiative ist im Herbst 2014 gestartet mit dem Ziel, einen Prozess für die Einbindung aller Stakeholder in den Diskussionsprozess zur Entwicklung der Sicherheitsarchitektur zu definieren und zu etablieren.

4.3 Standards und Normierung

Im Bereich der Normierung und der Standardisierungsorganisationen wurde in den letzten Jahren eine schier unüberschaubare Anzahl an Standards entwickelt, die in der einen oder anderen Art und Weise auch Smart Grids betreffen. Inzwischen werden auch Übersichtsdokumente erzeugt, die eine Einordnung der unterschiedlichen Standards ermöglichen, insbesondere zu nennen ist hier die Arbeit der CEN/CENELEC/ETSI Smart Grid Coordination Group [19] sowie von IEC [20] oder auch aus dem STARGRID Projekt [21].

Für den Bereich der Sicherheit im Smart Grid haben verschiedene Standards der folgenden Standardisierungsorganisationen bzw. Standardisierungsgruppen eine wesentliche Bedeutung:

- IEC TC 57 – Standardisierung von Energiemanagementsystemen (z.B. IEC 60870, IEC 61850)
- IEC TC 65 – Standardisierung von Industriellen Kontrollsystemen, auch in Bezug auf Safety (z.B. IEC 61508) und Security-Aspekte (z.B. IEC 62443)
- Sowie weiter Arbeitsgruppen der IEC
- ISO/IEC JTC 1 SC7 – Standardisierung von Informationssicherheitsmanagementsystemen (z.B. ISO 2700x), IT-Sicherheitsverfahren, Kryptographischen Mechanismen und Sicherheitsevaluierungsprozessen (z.B. ISO 15408 – Common Criteria)
- IEEE – Diverse Standards im Bereich elektronische Kommunikation, auch in Bezug auf Sicherheitsaspekte (z.B. IEEE 802.x)
- NERC (North American Electric Reliability Corporation) – CIP (Critical Infrastructure Protection) Standards, ebenso auch NIST (US National Institute for Standards in Technology) – Standardisierung von Sicherheitsaspekten für die USA
- Standardisierungsgremien im Bereich der elektrotechnischen Normung (z.B. CEN/CENELEC) - siehe dazu auch die Übersicht der SGCG [19]
- Standardisierungsgremien im Bereich der Kommunikationsprotokolle (IETF, W3C, aber auch ETSI) gewinnen aufgrund der Verwendung dieser Protokolle im Smart Grid an Relevanz, auch in Bezug auf die Sicherheitsaspekte

5 Forschungsbedarf

Das Stromnetz in ein sicheres Smart Grid zu verwandeln ist eine große Herausforderung auf vielen Ebenen, die nicht ohne weitere Forschung bewerkstelligt werden kann. In diesem Kapitel wird mittels der im Abschnitt Methodik beschriebenen Segmentierungsmatrix der Forschungsbedarf evaluiert.

5.1 Sicherheitsaspekte auf Ebene der „Basis-Konnektivität“

Die Basis-Konnektivität stellt Mechanismen für die Konnektivität zwischen physikalischen und logischen Systemen und den zuverlässigen Datenaustausch bereit. Diese Ebene ist vergleichbar mit der Bitübertragungs- und Datenverbindungsschicht im ISO/OSI-Referenzmodell [22] (z.B.: Regeln für Verbindungsaufbau, Datenkodierung, Fehlerkorrektur). Die Ebene der Basis-Konnektivität kann im Smart-Grid-Kontext aber genauso als physikalische Ebene der Energieübertragung (d.h. Stromleitung) interpretiert werden. Bisher hatte das Stromnetz auf dieser Ebene keine IKT-Sicherheitsanforderungen zu berücksichtigen. Der Security-Aspekt in dieser Ebene wird häufig mit teuren (weil speziell für eine einzelne Anwendung entwickelten) und unflexiblen (weil unveränderbaren oder nicht wartbaren) „Embedded“-Lösungen umgesetzt, die alleine aus entwicklungstechnischen (Kosten-) Gründen keine durchgehende Datensicherheit zur Verfügung stellen können. Das Nachrüsten dieser Eigenschaften bei bestehenden Systeme ist dabei besonders für die Industrie eine generelle Forschungsherausforderung, um Grids schrittweise in Smart Grids zu transformieren.

Schlüsselfaktor „Ausbau der elektrischen Infrastruktur“

Um die Sicherheit im Sinne von Security, Privacy, Safety und Resilienz im Smart-Grid-orientierten Ausbau-Szenario gewährleisten zu können, ist eine Netzwerkkonnektivität nicht nur auf der elektrischen Seite notwendig. Diese Basis-Konnektivität der elektrischen Infrastruktur bildet die physikalische Grundlage des Smart Grids, das aber ohne zuverlässigen Datenaustausch über volatile Systemzustände nicht das volle Potential ausschöpft. Der konventionelle Infrastrukturausbau nach heutigen Regeln benötigt keine neuen Sicherheitsüberlegungen in diese Richtung, bietet aber auch keine Chancen für eine Verbesserung in einem anzunehmenden hochvolatilen Stromnetz.

Schlüsselfaktor „Verfügbarkeit einer systemweiten IKT-Infrastruktur”

Die Integration einer systemweit verfügbaren IKT-Infrastruktur in das Stromnetz ist eine zentrale Voraussetzung für die Existenz von Smart Grids. Obwohl man generelle Aussagen treffen kann, wie z.B. nicht benötigte Konnektivität aus Sicherheitsgründen zu entfernen, hat ein und dieselbe Aussage unterschiedliche Implikationen auf die Sicherheitsaspekte der Ebene der Basis-Konnektivität, wenn man zwei unterschiedliche, extreme IKT-Infrastrukturausprägungen wie z.B. Insellösung und Plug&Play aus der Acatech-Studie [2] betrachtet: Bei Insellösungen ist die Systemgrenze kleiner gefasst. Es gibt keine gemeinsamen Standards; viele proprietäre, inkompatible Realisierungen sind am Markt und führen nur langsam zu lokalen Optima. Damit beschränken sich die Aspekte der Angriffssicherheit auf lokale Maßnahmen, die innerhalb jeder der einzelnen Systemausprägungen getroffen werden müssen. Insgesamt betrachtet nimmt die Diversität eine wichtige Stellung bezüglich Resilienz und Safety ein. Durch die Vielfalt der Infrastrukturumsetzungen ist zwar das einzelne Risiko höher, wird aber zugleich auch die Wahrscheinlichkeit eines Angriffs auf alle Ausprägungen gering. Im Plug&Play-Szenario werden von institutioneller Seite Vorgaben gemacht, oder es wird durch Marktführerschaft eine Lösung als marktkonformer Standard für IKT-Infrastrukturen systemweit angenommen. Dadurch kann eine stärkere Planungssi-

cherheit für langfristige Investitionen erreicht werden, so dass aufgrund größerer Absatzmärkte die Adaption technischer Lösungen beschleunigt und der Nutzen für alle Teilnehmer erhöht wird. In diesem Szenario ist Netzwerkkonnektivität an jeder Stelle gefordert und nur schwer aus Sicherheitsgründen zu entfernen, wodurch existierende und zukünftige Protokolle auf niedrigster physikalischer Ebene bzw. Bitübertragungs- und Datenverbindungsschicht Sicherheit im Sinne der Integrität und Vertraulichkeit unterstützen müssen. Die Versorgungssicherheit betreffend wird in diesem Szenario die Resilienz gegen Angriffe durch eine gut durchdachte, zeitgeprüfte Lösung gesteigert im Gegensatz zum vorherigen Szenario mit vielen unterschiedlichen Herangehensweisen. Für die Umsetzung der zur Verfügung stehenden State-of-the-Art-Techniken ist keine wesentliche Forschung notwendig; vor allem, da auf existierenden Standards und bewährten kryptographischen Methoden aufgesetzt werden kann. Allerdings ist kritisch zu prüfen, ob die Methoden richtig angewandt wurden und somit eine zuverlässige und stabile Nutzung der IKT-Infrastruktur ermöglicht wird.

Schlüsselfaktor „Flexibilisierung des Verbrauchs“

Das Stromnetz der Zukunft benötigt neben planbarer Erzeugung auch steuerbare Lasten, um Blackouts entgegensteuern zu können. Sobald die Lastflexibilität systemrelevant wird, sind auch neue Risiken von hoher Relevanz. Beispielsweise können aufgrund eines Kommunikationsausfalls Daten zur Lastflexibilisierung fehlen. Eine z.B. durch Redundanz resiliente Basis-Konnektivität wird dann notwendig sein. Allerdings ist der Forschungsbedarf schon heute vorhanden, da ein langsamer Übergang von gar keiner Systemrelevanz bis zu einer hohen Systemrelevanz flexibler Lasten stattfindet.

Schlüsselfaktor „Energiemix“

Mit der wachsenden Systemrelevanz volatiler erneuerbarer Erzeugung kommt es zum Teil heute schon zu neuen Risiken (z.B. in Deutschland, aber vor allem auch in Dänemark). In einem Inselbildungsszenario ist die Safety-Relevanz im Bereich der Schutztechnik für dezentrale erneuerbare Erzeugung besonders relevant, da Schutzgeräte sich in kritischen Situationen rekonfigurieren lassen müssen. Die Resilienz der Stromversorgung kann durch dezentrale Anlagen erhöht werden, wenn Demand Response funktioniert und lokale Inseln ermöglicht werden. Bisher ungeklärt ist allerdings die Forschungsfrage, wie viel Konnektivität hierfür tatsächlich erforderlich ist.

Schlüsselfaktor „Neue Services und Produkte“

Die Basis-Konnektivität spielt hier eine Rolle, wenn durch bestimmte Services die physikalischen Netzwerkgrenzen zwischen geschütztem Innen- und weniger geschütztem Außenbereich überbrückt werden müssen. Virtuelle Kraftwerke als Produkte oder Services über unterschiedliche physikalische Netze wären hier als Beispiel zu nennen. Neue Sicherheitsgefahren ergeben sich, wenn über die gleiche Basis-Konnektivität ohne Verschlüsselung kritische Systemkommunikation stattfindet und zugleich andere, weniger kritische Daten (z.B. Marktplattformdaten) ausgetauscht werden. Forschungsfragen in diesem Bereich sind daher, inwieweit eine Trennung von Datenströmen verschiedener Kritikalität, ein Vorrang von Daten höherer Kritikalität, oder eine Zusage zu einer bestimmten Servicequalität erforderlich sind.

Schlüsselfaktor „Endverbraucherkosten“

Bezüglich der Endverbraucherkosten gibt es bei der Basis-Konnektivität einen Trade-off: Entweder investiert man in eine dedizierte, abgeschottete Basis-Konnektivität (teuer), oder man nutzt synergetisch generische Infrastrukturen (günstig, aber mit unklaren Risiken). Hier können möglicherweise Erfahrungen aus anderen Domänen (z.B. vertikal integrierte Modelle aus dem Tele-

kommunikationsbereich – sogenannte „Walled Garden"-Lösungen angewandt werden.[2] Hierzu besteht Forschungs- und Harmonisierungsbedarf, wenn die Lösung über Betreibergrenzen hinweg gehen soll. Dies wirft auch die Frage nach dem Sicherheitslevel auf: Wer ist an welcher Stelle der Verbindung für Sicherheit verantwortlich? Wie viel darf oder muss Sicherheit kosten? Wie viel ist der Kunde oder der Staat bereit zu bezahlen?

Die Endverbraucherkosten sind proportional zu dem Kommunikationsbedarf neuer Services, da sich mit diesem auch die Angriffsfläche vergrößert und die Anzahl möglicher Fehlerquellen steigt. Andererseits, je volatiler die Services werden (Lastabwurf, zeitvariable Tarife, etc.) desto deutlicher wird der Gewinn durch Smart-Grid-Technik. Es besteht dahingehend Forschungsbedarf, dass es herauszufinden gilt, wie in diesem Zusammenhang ein gleichzeitig sicheres und kostengünstiges System auszulegen ist.

Schlüsselfaktor „Standardisierung"

Auf der Ebene der Protokolle ist die Interoperabilitätsschicht der Basis-Konnektivität ausreichend abgedeckt. Ein Forschungsbedarf besteht höchstens hinsichtlich neuer Kommunikationsmedien, die für Smart Grids relevant werden können (z.B. teilweise kontroverse Diskussion um das Thema Breitband-PLC).

Schlüsselfaktor „Politische Rahmenbedingungen"

Die Regulierung von Frequenzbändern für Smart-Grid-Lösungen kann durch politische Rahmenbedingungen gelöst werden (z.B. das Problem WiMAX für Prozessnetze ohne Privatkunden), oder durch Deregulierung im Telekombereich, indem politische Entscheidungen für oder gegen synergetische Infrastrukturnutzung getroffen werden. Forschungsfragen sind hierbei besonders ökonomische Themen im Sinne der wirtschaftlichen Auswirkungen von Entscheidungen im Bereich der Basis-Konnektivität für Smart Grids.

5.2 Netzwerk-Interoperabilität

Diese Ebene fokussiert auf den Datenaustausch zwischen verschiedenen Systemen über unterschiedliche Netzwerke, unabhängig von der übertragenen Information, und entspricht damit der Vermittlungs-, Transport- und Sitzungsschicht im ISO/OSI-Referenzmodell [22]. Energietechnisch sind auf dieser Ebene die verschiedenen Anschlussbedingungen bzw. Grid Codes für den Zugang zur Energieinfrastruktur angesiedelt. Die Aspekte des Infrastrukturmanagements, die alle Netzteilnehmer erfüllen müssen, werden in dieser Ebene aufeinander abgestimmt. Das Management der gesamten Infrastruktur mag im Verantwortungsbereich eines oder mehrerer Betreiber liegen, ist aber nicht Thema dieser Interaktionsebene.

Schlüsselfaktor „Ausbau der elektrischen Infrastruktur"

Die Art des Infrastrukturausbaus (konventioneller oder Smart-Grid-orientierter Ausbau) wirkt sich auf die Anschlussbedingungen aus, die einen sicheren Systembetrieb mit signifikantem Anteil dezentraler Erzeugung sicherstellen. Bidirektionale Energieflüsse haben Auswirkungen auf Schutzkonzepte. Sowohl der Personenschutz, als auch der Anlagenschutz muss weiterhin gewährleistet sein, auch wenn die Netzwerkkommunikation im Smart-Grid-orientierten Ausbausze-

[2] Z.B. die App Stores auf Apple-Geräten, in denen sowohl Entwickler als auch Programme nicht nur digital zertifiziert werden, sondern auch zentral auf Sicherheit überprüft werden; Microsoft Videospielkonsolen, für die Entwickler Lizenzen kaufen müssen, um dafür entwickeln zu können; der Amazon Kindle eBook Reader, welcher weniger als eReader zu sehen ist, sondern eher als ein gesamtes Ökosystem; oder das Verizon Wireless CDMA-Netz in den USA, welches durch Verwendung eigener Hardware und Aktivierungsrichtlinien ausschließlich approbierte Geräte im Netzwerk zulässt.

nario beeinträchtigt ist. Ist die IT-Kommunikation nicht betroffen, eröffnet die Smart-Grid-Infrastruktur neue Möglichkeiten, um Störungen, Überbelastungen oder Fehler der elektrischen Infrastruktur zu lokalisieren, einzudämmen oder zu beheben.

Schlüsselfaktor „Verfügbarkeit einer systemweiten IKT-Infrastruktur"

Smart Grids ohne Netzwerkinteroperabilität sind nur als Micro Grids vorstellbar. Eine systemweite IKT erfordert systemweite standardisierte Sicherheitskonzepte, die alle Use Cases unterstützen und sich von Ländergrenzen nicht aufhalten lassen. Flexible, breit anwendbare Mechanismen erhöhen die Komplexität und damit auch die Fehleranfälligkeit. Dadurch kommt es auch zu einer Vergrößerung der Angriffsfläche und der Verstärkung der Auswirkungen eines erfolgreichen Angriffs. Diesen Gefahren muss in allen Sicherheitsaspekten genügend Aufmerksamkeit gewidmet werden.

Schlüsselfaktor „Flexibilisierung des Verbrauchs"

Die drastische Vergrößerung der Flexibilität auf der Lastseite stellt eine Chance zur Erhöhung der Systemzuverlässigkeit dar. Die Flexibilisierung des Verbrauchs fordert aber notwendigerweise neue Schnittstellen zwischen bisher isolierten Systemen (z.B. Netzleitsystem und lokale Energiemanagement-Systeme). Dies führt zu neuen Sicherheitsrisiken und macht angepasste Sicherheitskonzepte je nach Art der Schnittstelle und Anzahl der beteiligten Stakeholder notwendig (z.B. wenige Industrie- versus viele Privatkunden). Die Verantwortlichkeit für Sicherheits- und Privacy-Fragen ist hierbei zu klären (z.B. Verantwortung der Prosumer, Gerätehersteller und Netzbetreiber).

Schlüsselfaktor „Energiemix"

Durch den Anstieg volatiler Ressourcen kommt es zu einer Diversifizierung des Energiemix. Dies reduziert die Abhängigkeit von einzelnen Energiequellen. Je nach Szenario (klassisch, planbar oder volatil) kommt es zu unterschiedlichen Anforderungen an die Netzwerkkonnektivität sowohl für Monitoring, als auch für die Steuerung und Regelung. Besonders der Paradigmenwechsel von zentral zu dezentral stellt für die Netze eine große Herausforderung im Parallelbetrieb dar.

Schlüsselfaktor „Neue Services und Produkte"

Ähnlich wie im Schlüsselfaktor „Flexibilisierung des Verbrauchs" ergeben sich durch neue Services und Produkte neue Schnittstellen zu Systemen, welche bisher nicht angebunden waren. Dies erfordert neue Sicherheitskonzepte, bzw. die Integration bestehender Konzepte aus anderen Branchen. Durch neue Services und Produkte sind aber nicht nur Mehraufwände, sondern auch neue Möglichkeiten zur Verbesserung der Resilienz zu erwarten.

Schlüsselfaktor „Endverbraucherkosten"

Ist keine einheitliche Netzwerkkonnektivität gegeben, kann mit hohen Kosten gerechnet werden, um entweder Insellösungen umzusetzen oder die Konnektivität trotzdem herzustellen. Eine Einheitliche IKT-Infrastruktur ermöglicht niedrigere Kosten. Im Sinne niedriger Endverbraucherkosten ist auch die zukunftssichere Gestaltung und die Erweiterbarkeit von Sicherheitslösungen von großer Wichtigkeit, um hier ein teures Nachrüsten zu vermeiden.

Schlüsselfaktor „Standardisierung"

Standardisierung von Schnittstellen ist in der Netzwerkinteroperabilität ein unumgänglicher Schritt, um inkompatible proprietäre Lösungen zu verhindern und ein rasches Fortschreiten der

Technologieentwicklung zu ermöglichen. Auch die Schaffung von Mindeststandards in den Bereichen Security, Safety und Privacy ist maßgeblich und durch den Multiplikationseffekt vorhandener Referenzen für die Industrie von hohem finanziellem Wert. Einheitliche oder harmonisierte Standards ermöglichen niedrige Kosten; umgekehrt kann von hohen Kosten ausgegangen werden, falls keine einheitlichen Standards definiert werden.

Schlüsselfaktor „Politische Rahmenbedingungen“

Die Schaffung positiver Rahmenbedingungen kann zur Entstehung einer kreativen Umgebung beitragen, die sich mit der Sicherheit von Smart-Grid-Netzwerken im Sinne von Security, Privacy, Safety und Resilienz befasst. Rahmenbedingungen ohne Spielraum bieten die Gefahr der Überregulierung dar (vgl. BSI-Schutzprofile mit unwartbaren Betriebssystemen und Programmversionen).

5.3 Syntaktische Interoperabilität

Die syntaktische Interoperabilität bezieht sich auf Regeln bzgl. der Datenformate und -strukturen von Informationen, die zwischen verschiedenen Systemen ausgetauscht werden. Wie auch bei sprachlicher Syntax, wo Wörter und Sätze bestimmten Regeln folgen, erlaubt die syntaktische Interoperabilität eine Zerlegung und Verarbeitung von Informationen (unabhängig davon, ob der Informationsgehalt einen Sinn ergibt, siehe Abschnitt 5.4 zum semantischen Verstehen). Die syntaktische Interoperabilität entspricht der Anwendungs- und Darstellungsschicht des OSI-Modells [22]. Aus dieser Schicht findet z.B. die Übersetzung zwischen verschiedenen Datenformaten statt, sowie (anwendungsnahe) Verschlüsselung.

Im Zusammenhang mit Smart Grids bezieht sich syntaktische Interoperabilität auf das Zusammenwirken verschiedener Einzelkomponenten im Sinne eines funktionierenden Gesamtsystems. Da das künftige Energieversorgungsnetz aus einer Vielfalt an Technologien bestehen wird, muss sichergestellt sein, dass einzelne Komponenten reibungslos miteinander kommunizieren können, ohne dass sich dies jedoch negativ auf Security und Privacy auswirkt. Smart-Grid-Komponenten müssen in der Lage sein, Informationen so aufzubereiten und darzustellen, dass Komponenten auf anderen Systemebenen oder anderer Hersteller, welche diese Informationen empfangen, diese verarbeiten können. Durch die wechselseitige Kompatibilität wird gewährleistet, dass die einzelnen Teile zu einem funktionierenden Gesamtsystem kombiniert werden können, und zugleich auch die Entwicklung neuer Technologie- und Servicemärkte unterstützt.

Ein zentrales Erfordernis in diesem Zusammenhang ist die Verwendung verbindlicher Standards im Hinblick auf Schnittstellen und Kommunikationsprotokolle. Nahtlose Interoperabilität im Smart Grid wird insbesondere dadurch zur Herausforderung, dass der Umstieg auf Smart Grids schrittweise stattfindet und Legacy-Systeme und neue Komponenten in ein funktionierendes Gesamtsystem integriert werden müssen. Die Referenzarchitektur kann die notwendigen Interfaces und Best-Practice-Implementierungen dazu aufzeigen.

Bevor entsprechende Standardisierungsarbeit die Definition von Schnittstellen vornehmen kann, ist die Festlegung einer einheitlichen, breit akzeptierten Referenzarchitektur notwendig, damit klar ist, welche Schnittstellen relevant und wie diese abzusichern sind.

Schlüsselfaktor „Ausbau der elektrischen Infrastruktur“

Der Ausbau der elektrischen Infrastruktur ist entscheidend dafür, welche physikalischen Fähigkeiten das Netz zukünftig besitzt und welche „intelligenten“ Funktionalitäten es abbilden kann [2]. Bei einem Ausbau des Übertragungsnetzes mit wenigen großen Anlagen wäre ein höheres Sicherheitsniveau unter Umständen einfacher umsetzbar als bei einem auf Smart Grids orientierten

Verteilnetz-Ausbau. Vorhandene (IKT-)Protokolle sind eher für Übertragungsnetze ausgelegt (z.B. IEC 61850); hier besteht Forschungsbedarf hinsichtlich der Übertragung auf Verteilnetze mit vielen kleinen verteilten Einheiten. Je nach Ausbauszenario ergeben sich unterschiedliche Sicherheitsanforderungen.

Schlüsselfaktor „Verfügbarkeit einer systemweiten IKT-Infrastruktur"

Die Integration einer IKT-Infrastruktur in das Energieversorgungsnetz ist eine zentrale Voraussetzung für die Etablierung von Smart Grids, und steht in direktem Zusammenhang mit der syntaktischen Interoperabilität. Je nachdem, ob diese Entwicklung langfristig geplant oder eher ereignisorientiert erfolgt, ist im Extremfall entweder eine übergreifende, den Erfordernissen angepasste Plug&Play-Infrastruktur zu erwarten, die die einfache Umsetzung vorhandener Anwendungen in einem neuen Kontext ermöglicht, oder auf der anderen Seite eine Fülle von Insellösungen. Im letzteren Fall bedeutet dies, dass bei den Anbietern von Kommunikationslösungen für das Energienetz keine Absprachen bezüglich gemeinsamer Standards erfolgen, und stattdessen eigene, proprietäre Marktstandards miteinander konkurrieren, was sich extrem negativ auf die Interoperabilität auswirkt. Durch die Unsicherheit bezüglich der sich durchsetzenden Technologien adaptieren Hersteller die Entwicklungen nur langsam, was auch negative Konsequenzen für die Übernahme von Sicherheitsvorkehrungen haben kann.

Schlüsselfaktor „Flexibilisierung des Verbrauchs"

Die flexible Laststeuerung erfordert entsprechende Steuerungsmöglichkeiten, welche Gebrauch von der zugrundeliegenden IKT-Infrastruktur machen. Die Bewertung entspricht hier daher im Wesentlichen dem Schlüsselfaktor „Verfügbarkeit einer systemweiten IKT-Infrastruktur".

Schlüsselfaktor „Energiemix"

Die Komplexität der Syntax hängt vom Anteil der volatilen Energiequellen ab: Je stärker volatile Energiequellen im Energiemix vertreten sind, desto stärker muss die die Fluktuation durch Smart Grids und Lastmanagement ausgeglichen werden, und desto komplexer wird auch die erforderliche Syntax. Da sich die Komplexität der Syntax wiederum auf die Sicherheit auswirkt, ergeben sich aus dem Maß an Volatilität des Systems entsprechende Sicherheitsimplikationen. Prinzipiell sind Sicherheitsanforderungen bei komplexer werdender Syntax schwieriger zu definieren und umzusetzen.

Schlüsselfaktor „Neue Services und Produkte"

Die Entwicklung neuer Services und Produkte fällt bei offenen Standards und transparenter Syntax deutlich leichter als umgekehrt. Die Anwendung existierender Protokolle in einem neuen Kontext bzw. neuen Szenarien hat Konsequenzen bezüglich der Systemsicherheit; in der Regel werden Sicherheitseigenschaften nicht einfach an den neuen Kontext „vererbt", sondern müssen erneut überprüft werden. Systemlösungen, die zukünftige neue Services unterstützen, sind komplexer und bieten größere Angriffsflächen durch zusätzliche Features und potenzielle Anwendung in einem nicht-intendierten Kontext (sogenannter „feature bloat").

Schlüsselfaktor „Endverbraucherkosten"

Es ist damit zu rechnen, dass den Endverbrauchern langfristig hohe Kosten entstehen, falls keine einheitliche Syntax gegeben ist; umgekehrt führt eine einheitliche, auf allgemeinen Standards aufbauende Syntax zwar kurzfristig zu höheren Investitionen, ist jedoch langfristig aufgrund der hohen Interoperabilität aus Endverbrauchersicht günstiger. Bezüglich der Erweiterbarkeit und damit Zukunftssicherheit der Sicherheitslösungen gilt die gleiche Problematik, die auch bereits

beim Schlüsselfaktor „neue Services und Produkte“ beschrieben wurde: Erweiterbare, zukünftige Services unterstützende Systemlösungen sind in der Regel komplexer und bieten damit auch größere Angriffsflächen durch zusätzliche Features.

Schlüsselfaktor „Standardisierung“

Dieser Schlüsselfaktor ist von zentraler Bedeutung für die syntaktische Interoperabilität, da diese wesentlich von einer konsequenten Einführung einheitlicher Standards abhängt. In diesem Zusammenhang sind auch Mindeststandards für Security, Safety und Privacy von zentraler Bedeutung. Bei Sicherheitsproblemen ist die Reaktionsgeschwindigkeit unter Umständen abhängig vom Grad der Standardisierung: Während bei einer proprietären Lösung seitens des Herstellers meist kurzfristig ein Patch zur Verfügung gestellt werden kann, ist bei standardisierten Lösungen evtl. erst eine Anpassung des Standards notwendig.

Schlüsselfaktor „Politische Rahmenbedingungen“

Bezüglich der politischen Rahmenbedingungen bietet die Forderung nach syntaktischer Interoperabilität die Chance einer Vereinheitlichung und Harmonisierung der Anforderungen an Smart-Grid-Komponenten, während gleichzeitig auch die Gefahr einer Überregulierung gegeben ist, wenn bei der konkreten Ausgestaltung nicht genügend Freiheitsgrade vorgesehen werden. Eine zentrale Fragestellung in diesem Zusammenhang lautet, ob einheitliche technische Lösungen auch unterschiedliche nationale Rahmenbedingungen unterstützen müssen, oder ob nicht zunächst die Rahmenbedingungen vereinheitlicht werden sollten.

5.4 Semantisches Verstehen

Nach Herstellung einer syntaktischen Interoperabilität ist es notwendig, die Inhalte der Datenstrukturen und Nachrichten auch verstehen zu können. Diese Ebene stellt eine grundlegende Voraussetzung für die Kommunikation oder den Austausch von Daten zwischen unterschiedlichen Systemen dar. Auf Basis einer syntaktischen Interoperabilität können zwar Daten ausgetauscht werden, ohne dass es zu Fehlern gleich beim Beginn der Verarbeitung der Daten kommt, aber erst mit einem gemeinsamen Verständnis können die Systeme auch die Bedeutung der Daten richtig interpretieren und dementsprechende Aufgaben ausführen.

Insbesondere im Bereich der Sicherheit kommt dem semantischen Verstehen von Daten eine besondere Bedeutung zu, da subtile Missverständnisse über die Aussage eines Datums schwer zu diagnostizierende Fehler hervorrufen können und auch für gezielte Angriffe missbraucht werden können. Daher ist es notwendig, im Bereich der Smart Grids umfassende und detaillierte Standards zu etablieren, die auch die Semantik der Datenstrukturen festlegen.

Aus Sicht des Schichtenmodells steht auf dieser Ebene das gemeinsame, eindeutige Verständnis der Konzepte welche in den Datenstrukturen der Nachrichten stecken, im Fokus der Betrachtungen. Daher ist eine Voraussetzung, dass die gemeinsame, korrekte Syntax bereits von Layer 3 sichergestellt ist. Darauf aufbauend ist eine Definition von Entitäten („Dingen“), Konzepten und deren Beziehung zueinander notwendig, also ein Informationsmodell der Domäne welches beschreibt wie diese „funktioniert“.

Zur semantischen Beschreibung von Systemen kommen oft objektorientierte Modelle zum Einsatz. Beispiele für solche Beschreibungssprachen und für semantische Modelle sind:

- XML Schema Definition (**XSD**)
- Universal Description, Discovery, and Integration (**UDDI**)

- Common Information Model (**CIM**) IEC 61970 – basiert auf Resource Description Framework (**RDF**)
- OPC Unified Architecture (**OPC UA**)
- **IEC 61850** (Substation Automation)

Schlüsselfaktor „Ausbau der elektrischen Infrastruktur“

Die Integration von „smarten“ Komponenten beim Ausbau der elektrischen Infrastruktur bedingt, dass diese Komponenten auch miteinander kommunizieren, und daher ist die semantische Interoperabilität ein wichtiger Aspekt beim Ausbau der Smart Grids. Neben den rein funktionalen Aspekten können semantische Beschreibungen von Systemen auch für Sicherheitsfunktionen wie Plausibilitätsprüfungen oder das Erkennen von Abweichungen und Anomalien zur Detektion von böswilliger Manipulation verwendet werden. Der immer weitere Ausbau und die steigende Vernetzung der im Smart Grid integrierten Systeme beispielsweise bis hin zur Integration von Elektromobilität führt zu steigenden Anforderungen auf dieser Ebene.

Beispiele für explizite Forschungsthemen in diesem Bereich sind Fragestellungen wie die effektive Umsetzung (kontextabhängiger) Plausibilitätsprüfungen oder das Verhindern der Ausnützung semantischer Zusammenhänge für Angriffe auf die Systeme.

Neben den IT-spezifischen Aspekten müssen auch die Grid Codes entsprechend adaptiert werden um veränderte Rahmenbedingungen semantisch abzubilden, und die Netzstabilität bzw. Versorgungssicherheit unter veränderten Anschlussbedingungen sicherzustellen (siehe Beispielsweise die 50,2 Hz Problematik im Bereich der starken Verbreitung von Photovoltaik-Einspeisung).

Schlüsselfaktor „Verfügbarkeit einer systemweiten IKT-Infrastruktur”

In einem zukünftigen System unterstützt ein semantisches Verständnis der verwendeten Datenstrukturen auf verschiedenen Ebenen die automatische Entscheidungsfindung, welche für die Verarbeitung der massiv steigenden Datenmengen benötigt wird. Auf der einen Seite ist das notwendig, um die steigenden Datenmengen beherrschen zu können; auf der andere Seite werden dadurch aber Fehlerzustände viel komplexer und ungleich schwerer zu diagnostizieren.

Ein weiteres Risiko einer systemweit verfügbaren IKT-Infrastruktur stellt die einfachere Möglichkeit der Verknüpfung von Daten dar. Dadurch besteht ein höheres Risiko eines Datenmissbrauchs, welches durch adäquate Maßnahmen reduziert werden muss.

Eine Plug&Play-Infrastruktur ermöglicht es, vorhandene Anwendungen/Protokolle/Services/etc. in „fremden“ Anwendungsbereichen einfach umzusetzen. Diesen Vorteilen steht aber ein höheres Risiko für Fehlfunktionen gegenüber, da die Gefahr besteht, dass implizite Sicherheits-Annahmen in diesen Anwendungen/Protokollen/Services in den „neuen“ Anwendungsbereichen keine Gültigkeit mehr haben und dadurch neue Schwachstellen entstehen.

In Bezug auf Sicherheitsanforderungen im Bereich der IKT-Infrastruktur stellt sich die Frage nach der praktischen Umsetzung existierender Standards und Normen. Ein Beispiel dazu: Für das Protokoll IEC 61850 existieren bereits Sicherheitserweiterungen in Form des IEC 62351 Standards, welche aber in der Praxis derzeit kaum eingesetzt werden.

In zukünftigen Systemen müssen viele unabhängige Teilsysteme semantisch interoperabel miteinander verbunden werden. Die grundlegende Forschungsfragestellung hier lautet, wie in solchen Szenarien effizient Sicherheit gewährleistet werden kann.

Schlüsselfaktor „Flexibilisierung des Verbrauchs“

Im Bereich der Flexibilisierung des Verbrauchs sind unterschiedliche Szenarien denkbar, von geringer Lastverschiebung über Haushalts- und Industriekunden bis hin zu einer hohen Gesamtbeteiligung an der Flexibilisierung. Diese unterschiedlichen Use Cases bringen eine Diversifizierung in den Datenstrukturen mit sich, die nur durch semantisches Verständnis der Daten in IKT Infrastrukturen abgebildet werden können. Fehler in diesen Abbildungen können Probleme im Gesamtsystem hervorrufen – als Beispiel sei hier openADR angeführt: kleine Fehler in der semantischen Konfiguration können starke Auswirkungen haben (z.B. falsch konfigurierte Randbedingungen für die Lastverschiebung einer Industrieanlage).

Andererseits bietet die semantische Interpretation elektrischer Größen auch Möglichkeiten zur Erhöhung der Versorgungssicherheit – z.B. kann die Frequenzregelung dadurch auch auf Verbraucherseite unterstützt werden.

Schlüsselfaktor „Energiemix“

Für diesen Schlüsselfaktor sind auf Ebene des semantischen Verständnisses keine relevanten Implikationen auf die Sicherheit des Smart Grid feststellbar.

Schlüsselfaktor „Neue Services und Produkte“

Die Entwicklung neuer Services und Produkte durch Nutzung der vorhandenen Datenmengen bringt eine gegenseitige Beeinflussung verbundener, bisher isolierter Systeme mit sich. Dadurch können Daten in einem anderen Kontext als dem ursprünglich vorgesehenen verwendet werden, was Privacy-Implikationen mit sich bringt. Ebenso können diese Daten von neuen Systemen für kriminelle Zwecke oder für Angriffe auf das System missbraucht werden.

Werden bestehende semantische Modelle auf neue Anwendungsbereiche übertragen, ohne die Randbedingungen und Voraussetzungen der Modelle ausreichend zu untersuchen, kann dies zu Sicherheitslücken führen. Eine weitere Gefahr stellt der Missbrauch von neuen Produkten oder Services durch semantisch korrekte Einflussnahme auf Inputdaten dar (z.B. „Service Hopping“ – Ausnutzen nicht-intendierter Zusammenhänge)

Schlüsselfaktor „Endverbraucherkosten“

In Bezug auf die Kosten bringt die Verwendung von einheitlichen Standards zur Sicherstellung einer semantischen Interoperabilität zwischen unterschiedlichen Services bzw. Ebenen vor allem eine Möglichkeit zur effizienten und damit kostensparenden Umsetzung. Der Einfluss der Endverbraucherkosten auf die Sicherheit ist in diesem Zusammenhang aber eher gering.

Schlüsselfaktor „Standardisierung“

Einheitliche semantische Standards in den Systemen ermöglichen die Verwendung von Komponenten unterschiedlicher Hersteller in einer Prozesskette. Die dadurch entstehende Diversität bringt eine höhere Resilienz gegenüber Angriffen mit sich und ist daher positiv zu bewerten.

Schlüsselfaktor „Politische Rahmenbedingungen“

Für die Etablierung von einheitlichen semantischen Standards gibt es prinzipiell sowohl die Möglichkeit der Etablierung über den freien Markt, als auch über regulative Vorgaben. In Bezug auf die Sicherheit ist die Verfügbarkeit und insbesondere die Verwendung einheitlicher Standards positiv zu bewerten – die Art und Weise, wie diese erreicht werden (ob über Marktmechanismen oder regulative Vorgaben) ist aber nicht ausschlaggebend.

5.5 Geschäftskontext

Der Geschäftskontext ist der zweite informationsbasierte Layer der GridWise Interoperability Layers und baut auf der semantischen Interoperabilitätsebene auf, in der Informationsmodelle im Fokus stehen. Der Geschäftskontext schränkt die Breite der Informationsmodelle auf die Aspekte ein, die relevant für den Kontext sind, um die Semantik auf Geschäftsprozesse anwenden zu können. Weiters beschreibt der Geschäftskontext, wie allgemeine Informationsmodelle die Geschäftsprozessinteraktion beeinflussen. Damit werden domänenbasierte semantische Informationsmodelle auf die Geschäftskontextebene abgebildet und je nach Anwendung weitere Strukturen und Einschränkungen für Geschäftsprozesse hinzugefügt, um das notwendige Wissen für Geschäftsprozesse gesammelt zur Verfügung zu stellen.

Hinsichtlich Security, Privacy, Safety und Resilienz berührt der Fokus des Geschäftskontext einerseits jene Sicherheitsaspekte, die Informationsmodellierung enthalten, wobei die technische Sicherheit durch die erste semantische Interoperabilitätsebene gegeben ist; anderseits wird die Anomalieerkennung durch die Einschränkung auf Informationsmodellsubsets erleichtert.

Schlüsselfaktor „Ausbau der elektrischen Infrastruktur“

Der Geschäftskontext wird von dem Ausbau der elektrischen Infrastruktur besonders in der Smart-Grid-orientierten Ausbauvariante erweitert, da Security- und Privacy-Implikationen nicht an der Protokollsystemgrenze halt machen (vgl. die aktuelle NSA-Prism-Diskussion, wobei physikalische Prismen in Lichtwellenleitern vor großen Datenzentren zu einer nicht feststellbaren Kopie aller übertragenen Daten genutzt wurden). Interface-Spezifikationen im Geschäftskontext müssen Anforderungen an die Verwaltung und das Handling von Daten sowie die Abwesenheit von Daten in den Geschäftsprozessen der interagierenden Teilnehmer festlegen.

Schlüsselfaktor „Verfügbarkeit einer systemweiten IKT-Infrastruktur”

Die Verfügbarkeit einer systemweiten IKT-Infrastruktur lässt die Einschränkung auf spezifische Profilkonfigurationen nicht mehr zu. Dies erhöht die Komplexität des Systems und erschwert das Durchsetzen von Sicherheitsaspekten. Der Weg zu einer systemweiten IKT-Infrastruktur benötigt auch die Vereinigung überlappender semantischer Informationsmodelle. Derzeit werden in unterschiedlichen Communities und Firmen unterschiedliche Modelle entwickelt, aus denen sich ein Subset für die Interaktion von Geschäftsmodellen im Geschäftskontext entwickeln muss, das zusätzlich einen Brückenschlag zwischen den verschiedenen semantischen Verständnissen vollbringt.

Schlüsselfaktor „Flexibilisierung des Verbrauchs“

Durch die Festlegung von Geschäftskontexten wird die Flexibilität für zukünftige Geschäftsmodelle eingeschränkt. Daher sollten entweder abstrakt erweiterbare semantische Konzepte in Betracht gezogen werden, oder ein Mapping verschiedener Informationsmodelle, die damit vereinigt werden können, ohne in Geschäftsmodellen darauf Rücksicht nehmen zu müssen. Dies wird umso wichtiger, je höher der Beteiligungsgrad der Lastverschiebung ist.

Schlüsselfaktor „Energiemix“

Es ist heute schon gängige Praxis, bei Planung und Betrieb von Stromnetzen nur bestimmte technische Szenarien zuzulassen, um die Zuverlässigkeit und Sicherheit zu gewährleisten, z.B. Betrieb von Verteilernetzen als offene Ringe. In einem Energiemixszenario mit vielen regenerati-

ven, fluktuierenden Einspeisern sinkt die Planbarkeit, und vorhandene technische Szenariobeschränkungen müssen neu durchdacht werden (z.B. Inselbetrieb über Haushaltsebene).

Schlüsselfaktor „Neue Services und Produkte“

Wie bei dem Schlüsselfaktor „Flexibilisierung des Verbrauchs“ wird auch hier durch die Festlegung von Geschäftskontexten die Flexibilität für zukünftige Geschäftsmodelle eingeschränkt. Dies stellt zu Beginn einen Sicherheitsgewinn dar, der allerdings auf lange Sicht Geschäftsmodellen kein Wachstum bzw. keine Evolution zugesteht. Geschäftskontexte sollten Schnittstellen unterstützen, die imstande sind zu skalieren und die Servicequalität über die Zeit hinweg zu verbessern, ohne auf die Performanz, Zuverlässigkeit oder Interoperabilität negativ Einfluss zu nehmen.

Schlüsselfaktor „Endverbraucherkosten“

Durch die Festlegung auf bestimmte Szenarien (aus Sicherheitsgründen) im Geschäftskontext wird eine effizienter planbare Infrastruktur bewirkt, die weiterhin konfigurierbar und variabel bleibt, aber insgesamt kostengünstiger für die Verbraucher ist.

Schlüsselfaktor „Standardisierung“

Über die Standardisierung von Geschäftskontexten kann eine Einschränkung eines Wildwuchses der Funktionalität und Mannigfaltigkeit bei Kommunikationsprotokollen und Datenmodellen erreicht werden, wodurch die Komplexität sinkt und die Sicherheitseigenschaften einfacher überprüfbar und durchsetzbar werden.[3] Eine Standardisierung von Geschäftskontexten hilft ebenfalls bei der Koordination effizienter Problemlösungen im Gesamtsystem und der einheitlichen Prüfung unterschiedlich gewachsener Unternehmen.

Schlüsselfaktor „Politische Rahmenbedingungen“

Politische Entscheidungen beeinflussen direkt, wie stark der Geschäftskontext eingeschränkt wird, sei es aus Sicherheits- oder Kostengründen, Energieprogressivität oder -konservativismus.

5.6 Geschäftsprozesse

Auf der pragmatischen Ebene der Geschäftsprozesse findet die Ausrichtung und der Abgleich zwischen operativen Geschäftsprozessen und Geschäftsabläufen statt. Um effektive Informationsinteroperabilität zwischen unterschiedlichen Teilnehmerfirmen und Organisationen gewährleisten zu können, müssen kompatible Prozesse und Verfahren über die Schnittstellengrenzen hinaus existieren. Die Regeln für den Einsatz von derartigen verteilten Geschäftsprozesstransaktionen müssen im Einklang mit den relevanten Geschäftsprozessen innerhalb der Organisationen vereinbart werden. Diese Festlegung der „Spielregeln“ für gemeinsame Geschäftsvorgänge muss für jede Betriebsstruktur mit unterschiedlichen Unternehmenszielen stattfinden. Jede Unternehmenszielkategorie stellt ein Regelwerk zur Verfügung, welches individuelle Prozesse zwischen Organisationen als Schnittstelle unterstützen [12].

[3] Z.B. Festlegung bei der Erstellung von Zufallszahlen auf geprüfte kryptografisch sichere Zufallsgeneratoren wie CSPRNG, Mindestanforderungen bei kryptografischen Funktionen zur Erstellung von geheimen Schlüsseln auf nicht weniger sichere Verfahren als PBKDF2 oder Scrypt, Verbieten von Integritäts- und Authentizitätsüberprüfungen in Protokollumsetzungen, die schwächer als HMAC-SHA256 sind, Verpflichtung zur Verwendung der spezifischen Ed25519 Implentierungsvariante für 64-Bit-Prozessoren zur digitalen Signatur.

Schlüsselfaktor „Ausbau der elektrischen Infrastruktur“

Geschäftsprozesse haben eine inhärente Spannung zwischen der Notwendigkeit zu interagieren und dem Risiko, den Geschäftsprozess und die beinhalteten Informationen preiszugeben. Es muss ein Mittelweg gefunden werden, um die Angriffsfläche zu minimieren und gleichzeitig die Leistungsfähigkeit und Nutzbarkeit für die Geschäftsprozesse zu maximieren. Beim Ausbau der elektrischen Infrastruktur ist besonders der Verantwortlichkeitsaspekt unter den Sicherheitsfragen relevant, da diese eine Art Buchhaltung ermöglichen muss, die zuverlässig nachvollziehbar belegen kann, dass Geschäftsinteraktionen von Geschäftsprozessen stattgefunden haben und nicht einfach abgestritten werden können. Dies ist ein wichtiger Schritt des Smart Grids gegen Angriffe auf die Zuverlässigkeit des Systems.

Schlüsselfaktor „Verfügbarkeit einer systemweiten IKT-Infrastruktur”

Die Verfügbarkeit einer systemweiten IKT-Infrastruktur für Geschäftsprozesse kann im Insellösungsszenario zu einer Vielzahl an Smart-Grid-Komponenten führen, die nur für wenige Geschäftsprozesse nutzbar sind und sich nicht wie im Plug&Play-Szenario nach der Installation anhand der Umgebung konfigurieren, um möglichst zielorientiert zu kollaborieren. Die Verfügbarkeit systemweiter Sicherheitsprozesse, die genutzt werden können, ist nur beim letzteren Szenario gegeben. Die Festlegung der Verantwortlichkeiten für Sicherheitsfragen in Geschäftsprozessen in allen Entwicklungsphasen (Design, Implementierung, Monitoring etc.) muss jedenfalls stattfinden.

Schlüsselfaktor „Flexibilisierung des Verbrauchs“

Sicherheitsrelevante Vorgaben wie z.B. im Rahmen des Informationssicherheitsmanagements sind bei vielen kleinen Einheiten schwieriger umzusetzen, richten aber zugleich weniger Schaden an als ein übereiltes zentrales System. Dies ist besonders im Privacy-Aspekt relevant, da festgelegt werden muss, welche Daten im Rahmen von Geschäftsprozessen übermittelt werden oder lokal bleiben. Der Umbau zu „smarten“ Verbrauchsvarianten erfordert eine Anpassung von Schutzkonzepten. In der Übergangsphase entstehen zuvor nicht dagewesene Gefahren, mit welchen umgegangen werden muss (z.B. der Verlust von Schwungmasse aufgrund der überwiegenden Frequenzregelung durch Lastmanagement).

Schlüsselfaktor „Energiemix“

Der Umbau des Energienetzes zu einem Smart Grid, das durch eine große Menge regenerativer Erzeugung CO_2-neutraler und trotzdem durch „smarte“ Verbrauchsvarianten planbar ist, erfordert eine Anpassung von Sicherheits- und Schutzkonzepten. Auch hier sind in der Übergangsphase Gefahren zu erwarten, siehe auch Schlüsselfaktor „Flexibilisierung des Verbrauchs“. Beispielsweise ist in der Vergangenheit in einigen Fällen das Wachstumspotential einer Technologie unterschätzt worden, vgl. 50,2Hz-Problem.

Schlüsselfaktor „Neue Services und Produkte“

Neue Services und Produkte fordern skalierbare Sicherheit und Resilienz sowie wiederholbare Safety und Privacy von Geschäftsprozessen, um sich entwickeln und wachsen zu können. In diesem Schlüsselfaktor zeigt sich die praktische Brauchbarkeit der festgelegten Kontexte und Modelle im Zusammenspiel. Gegenüber komplizierten, unsicheren oder undurchsichtigen Geschäftsprozessen haben sichere, resiliente Prozesse, Services und Produkte einen klaren Wettbewerbsvorteil in den Investitions- und Erhaltungskosten. Eine mögliche Regelung der Verant-

wortung für Sicherheitsfragen (z.B. durch eine Zertifizierung, vgl. geschlossene App-Store-Konzepte) findet auf dieser Ebene statt.

Schlüsselfaktor „Endverbraucherkosten“

Smart Grids ermöglichen den Endverbrauchern, als aktive Teilnehmer des Stromnetzes zu agieren. Diese höhere Flexibilität ist mit einer höheren Volatilität bei den Endverbraucherkosten verbunden. Komplexere Geschäftsprozesse, Sicherheitsimplikationen, Notfallverhalten, zusätzliche Personenschutzvorkehrungen und Angriffsschutzmechanismen in einem digitalen Zeitalter sind nur einige Kostenfaktoren, die in Geschäftsprozessen zu berücksichtigen sind.

Schlüsselfaktor „Standardisierung“

Standardisierung verbietet keine Innovation, sondern ermöglicht Kollaboration auf der Ebene von Geschäftsprozessen. Insbesondere bringt eine Standardisierung der Geschäftsprozesse auch eine Standardisierung der Sicherheitsprozesse und Produkte mit sich, wodurch sichere Referenzumsetzungen als Multiplikatoren wirken. Besonders organisationsübergreifende Zertifizierungs-, Registrierungs-, Such- und Konfigurationsdienste zu Smart-Grid-Technologien führen zu einer höheren Interoperabilität, und sind im Sinne von Security, Privacy, Safety und Versorgungssicherheit ein Meilenstein auf dem Weg zum erfolgreichen Einsatz von Smart Grids und deren Komponenten. Dies ist vergleichbar mit der Liberalisierung des Elektrizitätsmarktes: Die Geschäftsprozesse von Stromanbietern und Netzbetreibern konvergieren, und die Regeln freier Marktwirtschaft fördern einerseits Innovation, belohnen aber andererseits auch bewährte Sicherheitsaspekte. Ein weiterer Vergleich kann zur vorbildhaften Umsetzung des Rahmens zur Verwendung elektronischer Signaturen im Signaturgesetz gezogen werden, die 1999 für Österreich als Vorreiter nicht nur die sichere Zusammenarbeit (bezüglich Authentizität) innerhalb Österreichs gesteigert hat, sondern überdies erst innovative, ökonomische Know-How-Exportchancen ermöglicht hat.

Schlüsselfaktor „Politische Rahmenbedingungen“

Geschäftsprozesse können von geeigneten politischen Rahmenbedingungen und politischen Entscheidungen stark beeinflusst werden, wodurch gleichzeitig der Markt reguliert wird. Insbesondere ist es eine politische Entscheidung, wie stark die Geschäftsprozesse durch Marktregulierung vorgegeben werden (z.B. aus Sicherheits- oder Kostengründen, energieprogressiv oder -konservativ). Rahmenbedingungen betreffen aber keinesfalls ausschließlich Gesetze, sondern ebenfalls eventuelle Sicherheitsprozesse (vgl. NERC CIP in den USA). Besonders Notfallszenarien und das Verhalten von Geschäftsprozessen in solchen Situationen sind ein gutes Beispiel für die Anwendung von systemschützenden Rahmenbedingungen statt profitorientierter Marktregeln (vgl. Gridcodes, Ampelmodell).

5.7 Geschäftsmodelle

Ein effektiver Informationsaustausch zwischen verschiedenen Organisationen setzt voraus, dass die strategischen und taktischen Ziele dieser Organisationen aufeinander abgestimmt und miteinander kompatibel sind [12]. Diese Schicht stellt einen Rahmen zur Verfügung, innerhalb welchem spezifische Businessprozesse stattfinden. Beispiel sei ein Energieversorgungsunternehmen (EVU), das mit einem seiner Kunden eine Lastreduzierung in Notfällen vertraglich vereinbart hat [2]. Der interaktive Geschäftsprozess des Lastabwurfs dient hier sowohl den strategischen Zielen des Kunden (bezieht kostengünstig Energie) und des EVUs (kann eine Kapazitätserweiterung hinausschieben).

Schlüsselfaktor „Ausbau der elektrischen Infrastruktur“

Die Art des Infrastrukturausbaus wirkt sich auf die Supply Chain und damit auch auf die Versorgungssicherheit aus: Eine durch intelligenten Netzbetrieb und ein ausgereiftes Lastmanagement ermöglichte nationale Energieunabhängigkeit ist eine Möglichkeit, um eine hohe Versorgungssicherheit zu garantieren; das Szenario Ausbau der Übertragungsnetze zu einem transeuropäischen Verbundsystem (bzw. „Supergrid“) eine andere. Neue Geschäftsmodelle (z.B. bilaterale Abkommen „unter Nachbarn“) führen auch zu neuen Fragestellungen hinsichtlich der Haftung und Versorgungssicherheit (vgl. die aktuellen Diskussionen im Bereich Mitfahrbörsen oder private Vermietung von Unterkünften wie z.B. Uber und AirBnB).

Schlüsselfaktor „Verfügbarkeit einer systemweiten IKT-Infrastruktur”

Der Betrieb der für Smart Grids erforderlichen IKT-Infrastruktur ist ein Geschäftsmodell per se, bei dem sich je nach Betreiber (Netzbetreiber vs. Telekommunikationsanbieter) unterschiedliche Synergien ergeben. Durch eine Fokussierung und Professionalisierung bei sicherheitsrelevanten Dienstleistungen ergeben sich Vorteile im Hinblick auf die Gesamtsicherheit des Systems und damit auch die Versorgungssicherheit. Insbesondere stellt gerade in der Anbindung der Endkunden ein Angebot von zusätzlicher (d.h. über regulatorische bzw. gesetzliche Vorgaben hinausgehender) Privacy ein zusätzliches Geschäftsmodell dar, vgl. das aktuelle Angebot sicherer E-Mail-Dienste. Ebenso könnten Verfügbarkeit und skalierbare Resilienz zu neuen Geschäftsmodellen führen (im Sinne von Abstufungen bei der Quality of Service und entsprechenden Service Level Agreements). Die Virtualisierung von Infrastrukturen bzw. Dienstleistungen führt zu einer erhöhten Komplexität und damit verbundenen Zuständigkeits- und Sicherheitsfragen, ähnlich wie bei existierenden Cloud-Diensten.

Schlüsselfaktor „Flexibilisierung des Verbrauchs“

Hinsichtlich der Flexibilisierung des Verbrauchs stehen die damit verbundenen Geschäftsmodelle zum Teil im Widerspruch zu den physikalischen Erfordernissen der Netze (z.B. Ampelmodell, Flexibility Operator [23]). Durch die Wechselwirkung zwischen Markt und Netz ergeben sich Sicherheitsimplikationen; insbesondere hat die Flexibilisierung des Verbrauchs Konsequenzen hinsichtlich der Privacy, da genaue Mess- und Verbrauchsdaten erforderlich sind, um eine effiziente Laststeuerung zu ermöglichen.

Schlüsselfaktor „Energiemix“

Durch die verstärkte Einbindung volatiler Ressourcen ergeben sich zahlreiche neue Geschäftsmodelle, wie z.B. Wettervorhersage, Verstärkung des Ausgleichshandels, oder Öffnung der Regelmärkte für kleinere Einspeiser bei einer Anpassung der Präqualifikationsrichtlinien. Durch diese Öffnung bzw. Erweiterung der Märkte treten viele neue Teilnehmer mit zum Teil unbekannten Sicherheitspolicies und -mechanismen auf den Plan. Die Formulierung verbindlicher Mindestanforderungen erscheint daher in diesem Zusammenhang sinnvoll, siehe dazu auch den Schlüsselfaktor „Standardisierung“.

Schlüsselfaktor „Neue Services und Produkte“

Ähnlich wie beim Schlüsselfaktor „Verfügbarkeit einer systemweiten IKT-Infrastruktur“ ergeben sich bei neuen Services und Produkten Sicherheits-, Privacy- und Resilienz-Themen als neue Geschäftsmodelle. Durch ein höheres Niveau bei Security, Privacy, Versorgungssicherheit und Resilienz kann eine Differenzierung und ein Wettbewerbsvorteil gegenüber konkurrierender Ser-

viceanbieter erreicht werden. Die Investitions- und Erhaltungskosten für die Sicherheit müssen bei neuen Services und Produkten generell mitberücksichtigt werden.

Schlüsselfaktor „Endverbraucherkosten“

Ein Teil der durch Smart Grids eingesparten Kosten für den Netzausbau muss für Sicherheitsmechanismen aufgewendet werden, die durch die stärkere Integration von IKT in das Stromnetz erforderlich werden. Zum aktuellen Zeitpunkt ist unklar, wie hoch diese Kosten sind und wer sie trägt; es ist jedoch davon auszugehen, dass zumindest ein Teil dieser Kosten auf die Endverbraucher abgewälzt wird.

Schlüsselfaktor „Standardisierung“

Eine Standardisierung bzw. Regulierung der Geschäftsmodelle wirkt sich positiv auf Verbraucherschutz und Versorgungssicherheit aus, indem z.B. verbindliche Mindestanforderungen bzgl. der Sicherheit neuer Produkte und Services definiert werden (siehe auch Schlüsselfaktor „Energiemix“).

Schlüsselfaktor „Politische Rahmenbedingungen“

Durch geeignete politische Rahmenbedingungen kann bei Kunden und Endverbrauchern das Vertrauen in neue Geschäftsmodelle und die Akzeptanz derselben gestärkt werden. Dazu zählt beispielsweise die politische Entscheidung, inwieweit neue Geschäftsmodelle reguliert bzw. standardisiert werden, siehe auch den Schlüsselfaktor „Standardisierung“.

5.8 Ökonomisch/Regulatorischer Rahmen

Die Ebene des ökonomischen bzw. regulatorischen Rahmens legt das Rahmenwerk und die Regulierung für die Umsetzung von Smart-Grid-Lösungen fest. Dadurch ergeben sich konkrete Auswirkungen auf die Interoperabilität, wenn bestimmte Standards beispielsweise schon in regulatorischen Vorgaben festgelegt werden (z.B. EN 50160 für Spannungsqualität). Auch im Security-Bereich sollte dieses Werkzeug benutzt werden, um Mindeststandards für Sicherheitsmaßnahmen festzulegen.

Schlüsselfaktor „Ausbau der elektrischen Infrastruktur“

In Bezug auf den Ausbau der elektrischen Infrastruktur ergibt sich Forschungsbedarf in der Fragestellung der Grenzen der Zuständigkeit. Wenn die Energieinfrastruktur auf neue Bereiche erweitert wird (z.B. Elektromobilität oder flexible Lasten), verschwimmen die Grenzen zwischen Zuständigkeitsbereichen beispielsweise im Verkehr (Beispiel Safety-Vorschriften für elektrische Fahrzeuge). Im Sinne der grundsätzlichen Regulierungstiefe ist auch hier die Frage zu stellen, ob sich eine ausreichende Sicherheit durch freie Marktkräfte einstellt, oder neuer Regulierungsbedarf entsteht, und wer gegebenenfalls diesen neuen Regulierungsauftrag wahrnimmt.

Schlüsselfaktor „Verfügbarkeit einer systemweiten IKT-Infrastruktur”

Durch die Verfügbarkeit einer systemweiten IKT-Infrastruktur kann es zu einer Monopolbildung kommen, welcher durch entsprechende Deregulierung und Entbündelung (Unbundling) entgegengewirkt werden kann. In Bezug auf die Sicherheit ist dabei zu beachten, dass durch diese Eingriffe keine negativen Auswirkungen entstehen (beispielsweise wenn für Investitionen in die Sicherheit durch den Markt oder Regulierungsmechanismen zu wenige Incentives erzeugt wer-

den). Wenn notwendig sollten solche Defizite durch verpflichtende Mindeststandards für die Sicherheit ausgeglichen werden.

Schlüsselfaktor „Flexibilisierung des Verbrauchs“

Im Bereich der Verbrauchsflexibilisierung entwickeln sich derzeit erste Märkte und Marktmodelle, und entsprechende Überlegungen im Bereich der Regulierung. In Bezug auf die Sicherheit ist dabei die Fragestellung zu beantworten, welche Auswirkungen sich im regulierten bzw. im deregulierten Flexibilitätsmarkt auf die Versorgungssicherheit ergeben.

Zur Flexibilisierung des Verbrauchs sind entsprechende Steuerungsmöglichkeiten der Verbraucher notwendig, die mit externen Systemen über IKT Gateways angekoppelt werden. Neben funktionalen Aspekten ist auch die Regulierung der Sicherheit und der Interoperabilität von IKT Gateways eine noch zu beantwortende Fragestellung.

Die unterschiedlichen Szenarien für diesen Schlüsselfaktor unterscheiden eine Flexibilisierung primär auf Industrieseite oder primär auf der Seite kleinerer Verbraucher (z.B. Haushalte). In Bezug auf Sicherheitsaspekte und insbesondere Sicherheitsmaßnahmen sind das aber ganz unterschiedliche Szenarien, da die Anzahl der zu steuernden Einzelverbraucher zwischen den beiden Szenarien sehr verschieden ist. Dementsprechend sind bei wenigen, großen Verbrauchern (Industrie) durchaus aufwendigere Sicherheitskonzepte für einen einzelnen Verbraucher implementierbar, als bei massentauglichen Lösungen, da auch der kommerzielle Aspekt nicht außer Acht gelassen werden kann. Für die Sicherheit des Gesamtsystems kann ein Ausfall der Verbrauchsflexibilisierungsmechanismen aber verheerende Folgen haben, egal ob dieser durch wenige große oder durch viele kleine Verbraucher ausgelöst wird.

Schlüsselfaktor „Energiemix“

Der Energiemix hat einen starken Einfluss auf die Versorgungssicherheit, sowohl in Bezug auf die Planungsfähigkeit der Energieerzeugung (z.B. verbrauchsgesteuerte Erzeugung vs. fluktuierende Energiequellen) als auch auf die Sicherstellung der eventuell erforderlichen Rohstoffe für die Energieerzeugung (Import von Rohstoffen). Forschungsbedarf ergibt sich hier in der Fragestellung des Markteinflusses auf die Versorgungssicherheit, von nationaler Eigenständigkeit in Österreich bis hin zu EU Außenabhängigkeiten.

Weiters ist natürlich für die Versorgungssicherheit gerade im Hinblick auf den verstärkten Einsatz von regenerativen, aber fluktuierenden Energiequellen eine Forcierung der Forschung im Bereich der Speichertechnologien sinnvoll.

Schlüsselfaktor „Neue Services und Produkte“

Bei der Entwicklung neuer Services und Produkte ist der regulatorische Rahmen insbesondere für Fragen in den Bereichen Produktsicherheit, Datenschutz und allgemein Konsumentenschutz zuständig. Gerade in Bereichen in denen diese Aspekte einen hohen Stellenwert besitzen besteht die Möglichkeit durch Zertifizierung von neuen Produkten und Services ein gewisses Sicherheitsniveau zu überprüfen.

Schlüsselfaktor „Endverbraucherkosten“

Maßnahmen zur Erhöhung der Sicherheit werden in vielen Fällen auch mit zusätzlichen Kosten einhergehen, daher ist eine wesentliche Frage, die es zu beantworten gilt, wieviel Sicherheit in einzelnen Bereichen notwendig ist, und wie die Kosten dafür aufgeteilt werden.

Abgeleitet davon ist der Grad der Regulierung festzulegen – welche Kosten für die Sicherheit sind Teil des freien Marktes (z.B. vom Energienutzer selbst angeschaffte Geräte oder Services wie werbefinanzierter Strom) und welche sind Teil von regulierter Infrastruktur (z.B. Smart Meter).

Schlüsselfaktor „Standardisierung“

Im Bereich der Standardisierung stellt sich die Frage welche verpflichtenden Standards im Bereich der Sicherheit durch entsprechende Regulierung vorgeschrieben werden sollen (z.B. offene Kryptoalgorithmen). Weiters ist es gerade bei technischen Sicherheitsstandards notwendig, diese am aktuellen Stand zu halten – auch das muss in den entsprechenden Regulierungsmaßnahmen mit berücksichtigt werden. Schließlich sind durch die technischen Neuerungen Migrationen auf neue Sicherheitsstandards notwendig, die zusätzliche Kosten verursachen; hier ergibt sich die Frage nach der Finanzierung dieser Kosten.

Schlüsselfaktor „Politische Rahmenbedingungen“

Die politischen Rahmenbedingungen stellen im Bereich der Sicherheit einen essentiellen Einflussfaktor auf den regulatorischen Rahmen zukünftiger Smart Grids dar. Hier verschmelzen die Aufgaben der mit der nationalen Sicherheit befassten Stakeholder und der für die Versorgung mit kritischen Infrastrukturen zuständigen Stakeholder. Daher ist ein ausführlicher Dialog auf dieser Ebene notwendig, um gemeinsame Rahmenbedingungen für ein hohes Sicherheitsniveau im Smart Grid sicherzustellen.

6 Chancen

Smart Grids gibt es noch nicht. Smart Grids wird es geben. Es gibt jetzt die Chance, die Entwicklung von Smart Grids grundlegend zu beeinflussen, d.h. den Verlauf des Vektors der Technologieentwicklung zu verändern (vgl. Abbildung 1). In zahlreichen Pilotprojekten kann man bereits einen ersten Eindruck über die enormen Möglichkeiten, aber auch die nicht zu unterschätzenden Herausforderungen gewinnen, die Smart Grids mit sich bringen. Dieses White Paper versucht, die Grundlage dafür zu schaffen, diese Chance nutzen zu können, indem es Empfehlungen und notwendige Entwicklungen aufzeigt, damit ein sicheres Smart Grid resultiert und nicht ein fragmentiertes, inkompatibles, unsicheres, instabiles und damit unbrauchbares Smart Grid. In diesem Kapitel wird auf den Sicherheitsbeitrag von Smart Grids eingegangen, auf die Stärkefelder der Österreichischen Industrie und darauf, welchen Beitrag der Innovationsstandort Österreich leisten kann, beziehungsweise was den Standort Österreich zu einem einzigartigen Smart-Grid-Innovationsstandort macht.

6.1 Sicherheitsbeitrag von Smart Grids

Dieser Abschnitt beschäftigt sich mit der Fragestellung, inwieweit Smart-Grid-Lösungen einen positiven Beitrag zur Sicherheit leisten können. Unter dem Begriff „Sicherheit“ sind hier verschiedene Teilkomponenten wie z.B. Versorgungssicherheit, Resilienz, Privacy, Personenschutz etc. zusammengefasst, siehe dazu auch die Definition des zugrundeliegenden Sicherheitsbegriffs in Abschnitt 3.2.

1. Smart Grids sind eine Schlüsseltechnologie zur Integration einer hohen Dichte von erneuerbarer Energie in bestehende Stromnetzinfrastrukturen. Sie verbessern die Leistbarkeit des Umstiegs auf eine nachhaltige elektrische Energieversorgung gegenüber konventionellen Lösungen. Durch ein intelligentes Management der vorhandenen Ressourcen kann die EU-Außenunabhängigkeit erhöht werden und somit, bei geeigneten Sicherheitsmaßnahmen, eine Versorgungssicherheit auf dem bisherigen hohen Niveau gewährleistet werden.

2. Die durch Smart Grids ermöglichte Restrukturierung der elektrischen Energieversorgung von einem auf wenigen zentralen Erzeugungseinheiten beruhenden System hin zu einem Nebeneinander von zentralen und dezentralen Einheiten kann mittelfristig die Systemzuverlässigkeit erhöhen, da es zu einer Diversifizierung von Systemeinheiten und -technologien sowie einer Reduktion der „Single Points of Failure“ kommt. Voraussetzung ist jedoch einerseits ein hohes Maß an Interoperabilität zwischen Komponenten verschiedener Systemebenen und verschiedener Hersteller, und andererseits ein entsprechendes Systemdesign, welches elektrische Inselbildung erlaubt, wie sie in Microgrid-Projekten oder dem dänischen „Cell Projekt“ [24] erprobt wurde.

3. Der steigende Automatisierungsgrad des Stromnetzes bietet zwar eine vergrößerte Fläche für Cyber-Angriffe, jedoch ist bei entsprechend resilientem Design eine deutlich schnellere Steuerbarkeit und somit auch kurzfristigere Reaktion auf besondere Vorkommnisse im Stromnetzbetrieb gegeben. Damit können Ausfallzeiten auf ein Minimum reduziert werden.

4. Durch die Integration einer umfassenden IKT-Infrastruktur in das Energieversorgungsnetz kommt es zu einer Verlagerung von Einflussfaktoren auf die Versorgungssicherheit weg von der Hardware hin zur Software, d.h. die Versorgungssicherheit wird stärker als zuvor von der Qualität, Konfiguration und Wartung von Softwarekomponenten abhängen. Während Software im Vergleich zu Hardware deutlich engere Wartungszyklen (d.h. häufige

Updates) erfordert, so ist die Wartbarkeit zugleich einfacher und kostengünstiger, da sie in der Ferne erfolgen kann und keine physische Anwesenheit von Personal am Einsatzort notwendig macht.

5. Statt sicherheitsrelevante Lösungen im Nachhinein zu bereits bestehenden Produkten oder Prozessen „hinzuzufügen", sollten Security-, Safety- und Privacy-Aspekte von der Entwurfsphase an berücksichtigt werden (Privacy-by-Design, Security-by-Design). Da Smart-Grid-Technologien heute vielfach erst am Anfang stehen, ist diese Möglichkeit noch gegeben und sollte unbedingt genutzt werden. Auf diese Weise kann eine neue Generation von Komponenten mit integrierten Sicherheitskonzepten geschaffen werden, die auf dem Weltmarkt einen Technologievorsprung haben.

6. Die Einführung von Smart Grids geht mit einer zunehmenden Dezentralisierung auf verschiedenen Ebenen (Märkte, IKT, Energietechnik) einher. Durch die immer größer werdende Rolle von erneuerbaren Energieträgern kommt es zu einer Demokratisierung der Produktion, bei der individuelle Haushalte kleine Mengen an Strom in das Netz einspeisen, und aus „Consumern" „Prosumer" werden (vgl. „The Long Tail of Energy"[4]). Durch diese Diversifizierung wird zugleich auch ein höherer Grad an Resilienz erreicht, da die lokale Energieproduktion (Inselbildung) eine gewisse Unabhängigkeit von den umgebenden Netzen bietet.

7. Durch die Diskussion über Sicherheit in Smart Grids hat sich auch eine offenere Diskussionskultur bzw. ein stärkeres Bewusstsein für Herausforderungen bezüglich der ohnehin eingesetzten bzw. geplanten IKT-Durchdringung in der klassischen, bestehenden Energieversorgung entwickelt.

8. Erst durch aktuelle Forschung und Entwicklung, in welcher natürlich zunächst der State of the Art ermittelt werden muss, wird das Ausmaß und die Ausgestaltung der existierenden Vernetzung evident. Smart Grids sind also auch ein Treiber, um bestehende Systeme auf den aktuellen Stand der Technik, speziell in Bezug auf Sicherheit sowie Interoperabilität und Zukunftssicherheit, zu bringen.

6.2 Stärkefelder der österreichischen Industrie

Österreichischer Unternehmen bzw. Akteure im Bereich der Komponentenindustrie für Smart Grids haben in vielen Bereichen erfolgreiche Positionen am europäischen und Weltmarkt eingenommen. Beispielhaft seien Komponenten wie Wechselrichter, Automatisierungstechnik, SCADA-Systeme, Protokollstacks und Sensorik genannt. Österreichische Produkte sind für ihre Qualität, Flexibilität und oft auch für ihre Fähigkeit, nicht alltägliche Anforderungen zu erfüllen, bekannt. Bis auf wenige Ausnahmen liegen diese Stärkefelder jedoch im Bereich der Einzelkomponenten, die zumeist von anderen Anbietern oder den Stromnetzbetreibern selbst zu einem Gesamtsystem integriert werden müssen. Auf der Integrationsebene, welche auch die wesentlichen Sicherheitsfragen umfasst, ist hier noch Potential für den Aufbau weiterer Stärkefelder vorhanden.

6.3 Innovationsstandort Österreich

Der Einsatz von kostengünstigen kohlenstoffarmen Energietechnologien, wie im Europäischen SET-Plan [25] vorgeschlagen, erfordert ein stärkeres, flexibleres, dezentraleres und intelligenteres europäisches Stromnetz, ein Smart Grid. Das Smart Grid soll neue Energiequellen mit End-

[4] http://www.renewableenergyworld.com/rea/blog/post/2009/09/the-long-tail-of-energy

nutzern verbinden, die Verwaltung von komplexen Wechselwirkungen zwischen Energieproduzenten und Nutzern ermöglichen, und dabei nichts an Sicherheit und Zuverlässigkeit verlieren. Diese Anforderung zusammen mit der Integration von Informations- und Kommunikationstechnologien in immer mehr Prozesse des Stromnetzes erfordert gemeinsame Innovationen auf beiden Gebieten, Energie und IKT.

Die Förderlandschaft im Bereich Smart Grids hat in den letzten Jahren bereits eine Vielzahl an ambitionierten Forschern bei der Bearbeitung des Themenkomplexes Smart Grids unterstützt, wodurch der Aufbau von Expertise und hochqualifiziertem Personal im F&E-Standort Österreich ermöglicht wurde. Aufgrund der hohen Dichte an Smart-Grid-Pilotprojekten gilt Österreich als Innovationsstandort und treibende Kraft im Bereich Smart-Grid-Technologien. Die erzielten Ergebnisse dieser ersten Pilotprojekte ermöglichen einen zielgerichteten und effizienten Ausbau von österreichischer Kompetenz im Bereich nachhaltiger Technologie- und Dienstleistungsentwicklung und der entsprechenden Export- bzw. Vermarktungspotenziale. Bei erfolgreicher Entwicklung und entsprechender Bewährung von weiteren, in diesem White Paper identifizierten Forschungsfragen kann eine Vielzahl neuer Smart-Grid-Anwendungen und Geschäftsmodelle bereits antizipiert werden. Unternehmen können damit bereits vor Produktion und Ausrollung gefürchtete hohe Risiken minimieren und damit in stärkerem Maße Neuerungen einführen („innovate“). Dies trägt dazu bei, Österreich den Weg zu einem Kernkompetenzland der nachhaltigen Technologieentwicklung im Smart-Grids- und spartenübergreifenden Dienstleistungsbereich zu ebnen.

Mittelfristig ergibt sich bei allen Partnern von Pilotprojekten ein Know-How-Vorsprung im Bereich von Smart-Grids-Komponenten, -Infrastruktur, -Geschäftsmodellen oder –Anwendungen. Allerdings sind existierende Smart-Grid-Anwendungen und -Pilotprojekte bei österreichischen Netzbetreibern dabei meist auf regionale Bedürfnisse zugeschnitten und stellen häufig Insellösungen dar. Für die Entwicklung von marktreifen, langfristig wirtschaftlichen und vor allem sicheren Lösungen greift das jedoch zu kurz, so dass hier eine gemeinsame richtungsweisende Basis geschaffen werden muss, um Österreichs Standortvorteil auch in Zukunft zu sichern. Diese Basis ermöglicht den Innovationsvorsprung in einen langfristigen wirtschaftlichen Erfolg für zukünftige Industriepartner, eine sichere und nachhaltige Strombereitstellung für Netzpartner, sowie einen wissenschaftlichen Kenntnisvorsprung für Forschungspartner umzusetzen. Das Smart Grid muss ein benutzerzentriertes, marktorientiertes, interaktives, zuverlässiges, flexibles und nachhaltiges Stromnetz ergeben, in dem alle Komponenten und Smart-Grid-Anwendungen zusammen existieren und arbeiten können. Je früher Komponenten umgesetzt und eingesetzt werden, desto wirkungsvoller ist die Maximierung der CO_2-Reduktionseffektivität.

Der in der EEGI Roadmap [26] geplante beginnende schrittweise Einsatz über die Zeit von 2010 bis 2030 lässt dem Standort Österreich noch genügend Raum für Innovation, um die Klimaziele zu erfüllen, die Kosten für hochinnovative Technologien zu senken, und Österreich als Innovationsstandort abzusichern.

Besonders Innovationsprozesse wie die RASSA-Initiative, die sich zum Ziel gesetzt hat, eine gesamtstaatliche sichere Referenzarchitektur für Österreich abzuleiten, haben hierzulande größere Chancen auf Erfolg, da sich der Kreis der Stakeholder im Gegensatz zu anderen, wesentlich größeren Ländern auf eine kleinere Anzahl von Personen beschränkt. Dies bedeutet nicht, dass ein solches gesamtstaatliches Vorhaben keine Herausforderung darstellt, dennoch hat Österreich hier einen Vorteil, welcher zu einer Vorbildwirkung für Europa und damit verbundenem Know-How-Export führen kann.

7 Folgerungen & Handlungsempfehlungen

Basierend auf der dargestellten Ausgangslage sowie dem dargestellten Forschungsbedarf auf den unterschiedlichen Ebene ergeben sich die im folgenden dargestellten Handlungsempfehlungen in Bezug auf die Entwicklung sicherer Smart Grids.

1. Ein wesentlicher Forschungsbedarf, der intensiver adressiert werden muss, ist die Untersuchung der Rückwirkungen von Sicherheitsaspekten auf das Smart-Grid-Systemdesign. Bei Architekturentscheidungen zur Entwicklung von Technologien, Anwendungsfeldern, Märkten, etc. sollte stets auch eine **Betrachtung der dadurch veränderten Risikolandschaft in Bezug auf die Sicherheitsaspekte** (Angriffssicherheit, Betriebssicherheit, Personensicherheit, Verfügbarkeit, Datenschutz, etc.) vorgenommen werden. Diese Betrachtung sollte als weiterer Faktor neben funktionalen, ökologischen und ökonomischen Gesichtspunkten am Anfang jeder Überlegung stehen.

2. Eine Möglichkeit dies umzusetzen wäre eine **verpflichtende Betrachtung von Sicherheitsaspekten** (z.B. über einen taxativ aufgezählten Katalog an Fragestellungen in den Förderprogrammen) in allen Forschungsprojekten im Bereich der Weiterentwicklung von Smart Grids, ähnlich wie dies bisher beispielsweise mit der Betrachtung geistes-, sozial- und kulturwissenschaftlichen Aspekte im Bereich der österreichischen Sicherheitsforschung (KIRAS) umgesetzt ist. Dabei sollte auf existierende Systematiken und Modelle (z.B. das SGAM Referenzmodell) Bezug genommen werden, um eine Gesamtsystembetrachtung zu ermöglichen.

3. Ein weiterer wesentlicher Bedarf ist die Weiterentwicklung des organisatorischen Rahmens für die Sicherheit von Smart Grids, vgl. [27]. Die Priorisierung von Sicherheitsaspekten muss über politische Rahmenbedingungen entsprechend vorgegeben werden, um negative Externalitäten [28] möglichst zu vermeiden. Eine reine Marktbetrachtung der Bewertung von Kosten und Risiko in Bezug auf Sicherheitsfragen greift zu kurz – bei Sicherheitsproblemen im Bereich der Stromversorgung werden negative Effekte, die daraus entstehen, mitunter nicht nur durch das Unternehmen sondern durch unbeteiligte Dritte oder die Gesellschaft als Ganzes getragen**.** Die **gesetzlichen und regulatorischen Rahmenbedingungen müssen diese negativen externen Effekte möglichst ausgleichen**, um ein ausreichendes Sicherheitsniveau sicherzustellen. Damit einher geht die Fragestellung, wie stark **Freiheitsgrade** in der Entwicklung neuer Anwendungen/Dienstleistungen/etc. **eingeschränkt werden dürfen**, um die Sicherheit der Energienetze nicht zu gefährden.

4. Um ein ausreichendes Sicherheitsniveau zu gewährleisten sollte weiters ein regelmäßiges **Monitoring der Incentives für Sicherheitsmaßnahmen** stattfinden, das sowohl die Aktivitäten auf den freien Märkten als auch die Regularien mit einbezieht. Gegebenenfalls können durch Mindeststandards in einzelnen Bereichen Fehlentwicklungen ausgeglichen werden. Ein Beispiel für eine solche Aktivitäten in einem spezifischen Bereich ist die Diskussion über „Data Privacy Impact Assessments“ aus der EU-Empfehlung 2014/724/EU vom 10. Oktober 2014 – ähnliche Aktivitäten sollten in allen Sicherheitsbereichen stattfinden.

5. Zur Umsetzung eines hohen Sicherheitsniveaus ist die Etablierung von Geschäftsprozessen für den sicheren Betrieb von Smart-Grid-Systemen über den **gesamten Lifecycle der Systeme** (von der Konzeption über Entwicklung, Konfiguration und Betrieb bis zur Außerbetriebnahme) notwendig. Teilweise fehlen hier noch entsprechende Rahmenbedingungen, für einzelne Teilbereiche z.B. eine verpflichtende Prüfung bzw. Zertifizierung

der IKT Sicherheit von Geräten die im Smart Grid verbaut werden, wie sie auf anderen Ebenen (z.B. elektrische Komponenten) bereits vorhanden sind.

6. Aufgrund der Komplexität zukünftiger Smart-Grid Systeme ist neben der bisher klassischen Aufteilung in Produktentwickler und Betreiber von Infrastrukturen eine verstärkte Ausprägung der Rolle des „Integrators“ zu erwarten. Auch hier sollte der Security-Focus entsprechend sichergestellt werden - Sicherheitsrisiken entstehen oft erst durch den speziellen Kontext von Systemen bzw. im Zusammenspiel mit anderen Systemen. Deshalb spielt der **Integrator eine entscheidende Rolle für die Sicherheit** des Gesamtsystems.

7. In Bezug auf die nationale Rolle Österreichs ist festzustellen, dass die Anwendbarkeit internationaler Lösungen im Sicherheitsbereich aufgrund nationaler Gegebenheiten nur eingeschränkt möglich ist. Ebenso können österreichische Lösungen als Ganzes nur schwer in anderen Märkten umgesetzt werden. Auch ist aufgrund der Größe des Landes eine Technologieführerschaft in der ganzen Breite von Smart-Grids-Lösungen wohl unrealistisch. Ein großes Potential kann z.B. im Bereich innovativer Komponenten für Smart Grids und Automatisierungslösungen liegen. Allerdings sollten die Vorteile eines kleinen Landes besser genützt werden, beispielsweise um **Leitmärkte für bestimmte Produkte bzw. Services zu etablieren** und so die Technologieführerschaft in einzelnen Bereichen zu erreichen. Trotzdem ist ein nationaler Know-How Aufbau für die gesamte Breite von Technologien erforderlich, zumindest auf Ebene der Bewertung von Lösungen für die nationalen Gegebenheiten. Deshalb ist es notwendig entsprechende **Aus- und Weiterbildungsmöglichkeiten im Bereich Smart Grid (Security)** zu etablieren, um das Vorhandensein ausreichender Kapazitäten für die Bewertung und Umsetzung sicherzustellen.

8. In Bezug auf die Standardisierung von Sicherheitslösungen ist ein Umdenken gefordert. Eine Standardisierung von Sicherheitsprozessen ist nicht möglich, solange die darunterliegenden Prozesse (technisch, kaufmännisch, etc.) nicht vereinheitlicht sind. Daher muss die treibende Kraft zur Vereinheitlichung die Standardisierung der Businessprozesse auf allen Ebenen sein, nicht die Sicherheit. Allerdings besteht natürlich **durch die Standardisierung der Geschäftsprozesse die Möglichkeit, ein hohes Sicherheitsniveau effizient umzusetzen**, da in vielen Fällen Sicherheitsmaßnahmen gut skalierbar sind. So könnten für verschiedene Geschäftsbereiche unterschiedlich hohe Sicherheitsanforderungen postuliert werden (beispielsweise Ende-zu-Ende-Verschlüsselung in Bereichen, in denen personenbezogene Daten verarbeitet werden).

9. Das Erreichen eines hohen Sicherheitsniveaus ist nur durch kontinuierliches Lernen und Verbessern möglich. Ein wichtiger Aspekt dazu ist ein **hohes Niveau an Informationsaustausch**, um aus Sicherheitsvorfällen die richtigen Schlüsse zu ziehen und Verbesserungen des Gesamtsystems anzustoßen. Um dieses „kollektive Lernen“ effizient zu ermöglichen, sind als Basis dafür einheitliche oder zumindest ähnliche Umsetzungen von Sicherheitsmaßnahmen notwendig, die beispielsweise durch Etablierung einer durchgängigen Referenzarchitektur erreicht werden können. Im Sinne einer europaweit einheitlichen Herangehensweise bzw. gemeinsamen Sprache ist insbesondere die Verwendung der innerhalb des M/490-Mandats entwickelten Artefakte zu empfehlen. So erlaubt beispielsweise das weit verbreitete SGAM-Modell [1], eine gemeinsame Sicht auf Smart-Grid-Architekturen zu erlangen und Standardisierungslücken zu identifizieren.

Referenzen

[1] CEN-CENELEC-ETSI Smart Grid Coordination Group: Smart Grid Reference Architecture. Nov 2012.

[2] Acatech (2012): Future Energy Grid. Migrationspfade ins Internet der Energie. Hans-Jürgen Appelrath, Henning Kagermann und Christoph Mayer (Hrsg.). Acatech Studie, Feb 2012.

[3] International Smart Grid Action Network (ISGAN) Annex 4, Synthesis of Insights for Decision Makers, URL: http://www.iea-isgan.org/?c=1/22

[4] European Union Agency for Network and Information Security (ENISA). Appropriate security measures for smart grids, Dec 2012. URL: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/appropriate-security-measures-for-smart-grids.

[5] ISO/IEC 27009 – Information technology – Security techniques – Sector-specific application of ISO/IEC 27001 – Requirements (draft).

[6] ISO/IEC 27000:2014 Information technology – Security techniques – Information security management systems – Overview and vocabulary (third edition).

[7] Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000), StF: BGBl. I Nr. 165/1999

[8] EC 61508 Functional Safety, Edition 2.0, 2010.

[9] National Institute of Standards and Technology: NIST-IR 7628 – Guidelines for Smart Grid Cybersecurity, 2010.

[10] Trivedi, Kishor S., Dong Seong Kim, and Rahul Ghosh. "Resilience in computer systems and networks." Proceedings of the 2009 International Conference on Computer-Aided Design. ACM, 2009.

[11] CEN/CENELEC/ETSI Joint Working Group on Standards for Smart Grids: Standards for Smart Grids – Final Report, 2011

[12] GridWise Architecture Council Interoperability Framework Team: Interoperability Context-Setting Framework, 2007. URL: http://www.caba.org/resources/Documents/IS-2008-30.pdf

[13] Berthold Haberler, Georg Kienesberger, Friedrich Kupzog, Lucie Langer: Smart-Grid-Architekturen in Österreich – Eine Bewertung der IKT-Sicherheitsaspekte relevanter Pilotprojekte. Elektrotechnik & Informationstechnik 2013 (4-5), S.115-120, Springer. DOI 10.1007/s00502-013-0141-5

[14] ISGAN white paper: Smart Grid Cyber Security, Apr 2012. URL: http://www.iea-isgan.org/?c=5/112/369&uid=1306

[15] ENISA: Smart Grid Security – Recommendations for Europe and Member States. July 2012.

[16] ENISA: Smart Grid Threat Landscape and Good Practice Guide. Dez 2013.

[17] JRC Joint Research Center: Smart Grid Projects Outlook 2014, 2014

[18] E-Control Austria et al.: Risikoanalyse für die Informationssysteme der Elektrizitätswirtschaft unter besonderer Berücksichtigung von Smart-Metern und des Datenschutzes, Feb 2014. URL: http://www.e-control.at/de/publikationen/publikationen-strom/studien/IKT_Risikoanalyse

[19] CEN-CENELEC-ETSI Smart Grid Coordination Group: SGCG/M490 Smart Grid Set of Standards, Version 3.1, 2014

[20] IEC Smart Grid Standards Map, http://smartgridstandardsmap.com, Abgerufen 19.12.2014

[21] STARGRID project, EU FP7 318782, D 2.1 – Smart Grid Standardization Documentation Map, 2013

[22] Hubert Zimmermann, OSI Reference Model – The ISO Model of Architecture for Open Systems Interconnection, Communications, IEEE Transactions on , vol.28, no.4, pp.425,432, Apr 1980, doi: 10.1109/TCOM.1980.1094702, URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1094702&isnumber=23925

[23] Rolf Apel et al., Regionale Flexibilitätsmärkte, Marktbasierte Nutzung von regionalen Flexibilitätsoptionen als Baustein zur erfolgreichen Integration von erneuerbaren Energien in die Verteilnetze, ETG VDE Studie, 2014

[24] Sunil Cherian and Valerijs Knazkins: The Danish cell project-part 2: Verification of control approach via modeling and laboratory tests. Power Engineering Society General Meeting, 2007. IEEE. IEEE, 2007.

[25] Strategic Energy Technology Plan (SET Plan), URL: http://ec.europa.eu/energy/technology/set_plan/set_plan_en.htm

[26] European Electricity Grid Initiative Roadmap and Implementation Plan, URL: http://www.smartgrids.eu/documents/EEGI/EEGI_Implementation_plan_May%202010.pdf

[27] Handlungsfelder zur Weiterentwicklung des Institutionellen Rahmens für Smart Grids in Österreich, Berichte aus Energie- und Umweltforschung, 7/2014, BMVIT. URL: http://www.nachhaltigwirtschaften.at/e2050/e2050_pdf/reports/201407_aktionspapier_institutioneller_rahmen_von_smart_grids_in_oesterreich.pdf

[28] Geoffrey Heal and Howard Kunreuther: Interdependent Security. In: Journal of Risk and Uncertainty, March 2003, Volume 26, p 231-249.