White Paper

im Rahmen des Strategieprozess [Smart Grids 2.0]

Sicherheitsaspekte von Smart Grids

DRAFT (Version Juni 2016)

Redaktion und strategische Gesamtkoordination:

- Michael Hübner, bmvit
- Erika Ganglberger, ÖGUT

Mit Beiträgen von:

- Thomas Bleier, Lucie Langer, Austrian Institute of Technology GmbH
- Christoph Kohler, Albrecht Reuter, Fichtner IT Consulting AG
- Dominik Engel, Josef Ressel Center for User-Centric Smart Grid Privacy, Security and Control
- Angela Berger, Technologieplattform Smart Grids Austria

Inhaltsverzeichnis

1 Hintergrund, Zielsetzung und Inhalt

Die Weiterentwicklung der Energieversorgungsinfrastrukturen im Allgemeinen und der Elektrizitätsversorgungssysteme im Besonderen als Backbone unserer Wirtschaft gehört zu den zentralen Herausforderungen unserer Innovationssysteme. Über den evolutionär stattfindenden Prozess der zunehmenden Automatisierung und der damit einhergehenden Durchdringung der Energiesysteme mit Informations- und Kommunikationstechnologien, haben sich unter dem Schlagwort **„Smart Grids“** Initiativen etabliert, die eine optimale Integration neuer Technologien und erneuerbarer Energien (insbesondere aus volatilen und dezentralen Quellen), die Steigerung der Energieeffizient der Versorgungssysteme sowie die Entwicklung technischer Plattformen für neue Dienstleistungen, Akteure und Märkte forcieren.

Der vom bmvit initiierte und koordinierte Strategieprozess „Smart Grids 2.0“ setzt sich zum Ziel bisherige Ergebnisse aus Forschung und Demonstration gemeinsam mit den AkteurInnen auszuwerten und daraus Mittelfriststrategien und konkrete Aktionspläne für Österreich abzuleiten (www.e2050.at/smartgrids). Als Ausgangsbasis wurden zentrale Entwicklungsziele für intelligente Energiesysteme formuliert [1].

Als eines diese Entwicklungsziele wurde dabei das Thema Sicherheit als integraler Designparameter identifiziert. Auch im europäischen Kontext wird Cyber Security bei der Entwicklung und Umsetzung eines flexibleren Energiesystems als zentrales Thema gesehen. Die DG Energy etablierte im Herbst 2015 die Energy Expert Cyber Security Platform (EECSP)[2] um die Resilienz von Energieversorgungssystemen gegen Cyber-Bedrohungen zu gewährleisten. Sowohl die NIS-Richtlinie[3] als auch die allgemeine Datenschutz Verordnung (GDPR)[4] hat einen neuen Rahmen für den Umgang mit Cybersecurity in der EU geschaffen. Auch die Europäische Agenda für Sicherheit 2015-2020[5] betonte die Notwendigkeit Cyber-Bedrohungen auf der bestehenden EU-Cybersecurity-Strategie von 2013[6] zu adressieren.

---

[1] bmvit: Entwicklungsziele für Smart Grids, Präsentation im Zuge der Auftaktveranstaltung zum Strategieprozess Smart Grids 2.0
http://www.nachhaltigwirtschaften.at/e2050/e2050_pdf/events/20131211_fti_smartgrids2020_auftaktveranstaltung_ganglberger.pdf

bmvit: Aktuelle Thesen zur Entwicklung von Smart Grids
http://www.nachhaltigwirtschaften.at/e2050/e2050_pdf/strategieprozess_smart_grids_2020_thesen_zur_entwicklung_von_smart_grids_2015.pdf

[2] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3341 (02.02.2018)

[3] The Strategy of the European Union set up in 2013 a public-private cross-sectoral platform on Network and Information Security (NIS Platform) to contribute to Commission recommendations on good cybersecurity practices, in particular on risk management, information sharing and incident notification. [Zitat vom 28. Januar 2016]
https://www.cert.at/reports/report_2016_chap04/content.html (02.02.2018)

[4] http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0001.01.DEU&toc=OJ%3AL%3A2016%3A119%3ATOC (02.02.2018)

[5] http://europa.eu/rapid/press-release_IP-16-1445_de.htm (02.02.2018)

[6] https://ec.europa.eu/digital-single-market/en/news/communication-cybersecurity-strategy-european-union-%E2%80%93-open-safe-and-secure-cyberspace (02.02.2018)

Das im österreichischen **Strategieprozess Smart Grids 2.0** eingeführte Format der **White Papers** verfolgt das Ziel, zentrale Themenfelder für die Entwicklung intelligenter Energiesysteme aufzubereiten und damit einer breiten Gruppe von Stakeholdern den Einstieg in eine strukturierte Diskussion zu ermöglichen. Die Auswahl der Themen erfolgt dabei insbesondere hinsichtlich der Relevanz in Bezug auf die formulierten „Aktuellen Thesen zur Entwicklung von Smart Grids“[7]. Es wird der Stand des Wissens auf Basis von F&E Ergebnissen dargestellt und ein Überblick über zentrale weiterführende Literaturstellen gegeben. Dabei steht der Themenaufriss, die möglichst allgemeine Verständlichkeit und die konsistente Darstellung im Vordergrund, nicht die Auflistung von Details, Daten und Fakten.

Das **gegenständliche Dokument** will das komplexe Themenfeld der Sicherheitsaspekte von Smart Grids systematisch aufspannen und damit eine Grundlage für die umfassende und zielsichere Bearbeitung des Themas schaffen. Dabei soll sowohl Safety (Schutz von Menschen vor einem System) als auch Security (Schutz des Systems vor Angriffen von außen) und Privacy behandelt und eingeordnet werden. Auch Versorgungssicherheit (Abhängigkeit), Ausfallssicherheit (Verfügbarkeit), Widerstandsfähigkeit (Resilienz), Verletzlichkeit (Vulnerabiltität) sowie Personensicherheit werden systematisch erfasst.

2 Kategorien von Sicherheitsaspekten - Begrifflichkeiten

Sicherheitsaspekte leiten sich aus den bereits dargestellten Bedrohungen und den daraus resultierenden Anforderungen an das intelligente Netz ab. Dabei gilt es zuerst, den Begriff der Sicherheit genauer zu definieren. Im englischen Sprachraum gibt es dafür zwei Übersetzungsmöglichkeiten: **Safety** bedeutet der Schutz der Menschen vor einem System, also die Betriebssicherheit im Sinne von Personen und Anlagenschutz. **Security** gilt dagegen für den Schutz des Systems vor Angriffen von außen[8]. Dies beinhaltet Systeme zur Angriffssicherheit und Informationssicherheit. Des Weiteren wird **Privacy** als Oberbegriff eingeführt, welcher die Einhaltung der Datenschutzrichtlinien zum Ziel hat. Hinzu kommt der Kernpunkt **Versorgungssicherheit** der die Gewährleistung der Versorgungsqualität und Versorgungssicherung beinhaltet. Als letzter Sicherheitsaspekt wird die **Resilienz** des Systems definiert. Er umfasst die Ausfallsicherheit und das Vorgehen bei Systemausfällen sowie die Klärung der Verantwortlichkeiten. Diese Sicherheitsaspekte dienen als Grundlage für die weitere Diskussion der Sicherheitsaspekte.

[7] bmvit: Aktuelle Thesen zur Entwicklung von Smart Grids http://www.nachhaltigwirtschaften.at/e2050/e2050_pdf/strategieprozess_smart_grids_2020_thesen_zur_entwicklung_von_smart_grids_2015.pdf

[8] Bleier, Thomas, et al. BMVIT White Paper Sicherheitsaspekte von Smart Grids. Wien : s.n., 2015.

Abbildung 1: Sicherheitsaspekte von Smart Grids[9]

3 Sicherheit als Prozess und integraler Designparameter

Die Entwicklung von Smart Grids bedingt die Betrachtung verschiedenster sicherheitstechnischer Aspekte. Ein erfolgreicher Entwicklungsprozess muss immer wieder auf die Frage zurückführen, welche Rückwirkungen und Anforderungen sich aus der Bearbeitung der einzelnen Sicherheitsaspekte auf das Systemdesign von Smart Grids ergeben. Diesbezügliche Erkenntnisse sollen immanenter Bestandteil der neuen Systemlösungen werden („Security by Design“). Nur so kann Vorsorge getroffen werden, dass nicht ein „Flickenteppich“ von Einzelelementen entsteht und Sicherheitstechnik aufwendig und letztlich ineffektiv „aufgepfropft“ wird.

In aktuellen öffentlichen Diskussionen steht derzeit oft der Aspekt der IKT Sicherheit im Vordergrund. Aus der Perspektive der Entwicklung von „Smart Grids“ können einzelne Sicherheitsaspekte grundsätzlich nicht isoliert betrachtet werden, sondern müssen im Sinne einer holistischen Systemsicht im Kontext aller relevanten Sicherheitsaspekte und der adressierten Zielstellungen gesehen werden.

[9] Engel, Dominik. Josef Ressel Zentrum FH Salzburg. [Online] 10. Dezember 2014. [Zitat vom: 28. August 2015.] http://www.netz-security.at/docs/ppt/Engel.pdf.

Haber, Alfons und Rodgarkia-Dara, Aria. E-Control. [Online] Dezember 2005. [Zitat vom: 2. September 2015.] http://www.e-control.at/documents/20903/-/-/934de48c-6a57-4095-8d25-297c194901e3.

Es ist dabei entscheidend, den gesamten Lösungsraum systematisch aufzuspannen und damit eine Grundlage für die umfassende und zielsichere Bearbeitung des Themas zu schaffen.

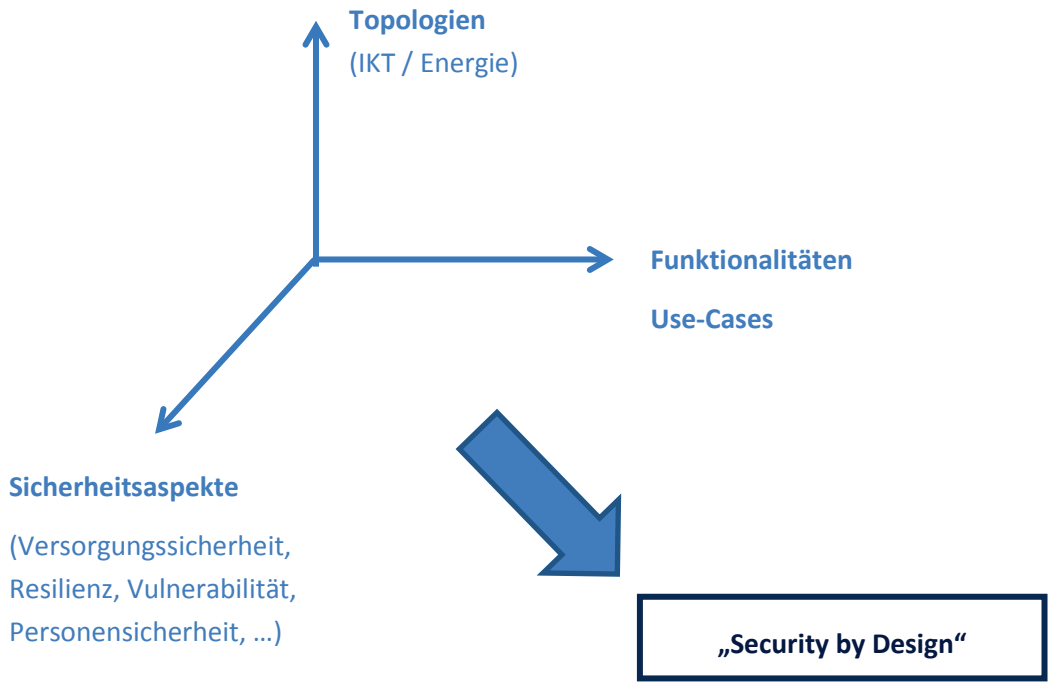

Abbildung 2: Was ist das?

Die heutigen IKT-Systeme in diesem Bereich stellen vorwiegend isolierte Lösungen für einen jeweils spezifischen Aufgabenbereich dar. In Zukunft wird die Anzahl der Akteure, welche (Teil-) Systeme betreiben oder beeinflussen, und auch die Anzahl der Schnittstellen zwischen den verschiedenen Systemen und Komponenten massiv steigen. Dies erfordert eine stärkere Interaktion der Akteure und Systeme bis in die untersten Netzebenen um die interoperable Vernetzung der unterschiedlichen Systemteile miteinander zu gewährleisten. Ein Smart Grid liefert darüber hinaus zukünftig Daten über die aktuellen Netzzustände bzw. den momentanen Verbrauch. Diese Entwicklungen bringen neben einer Reihe von neuen Möglichkeiten und positiven Faktoren aber auch neue Gefahren mit sich. Der Entwicklungsprozess einer sicheren Infrastruktur ist dabei ein iterativer Prozess, der sich am aktuellen Stand der Erkenntnis und Technologieentwicklung orientiert.

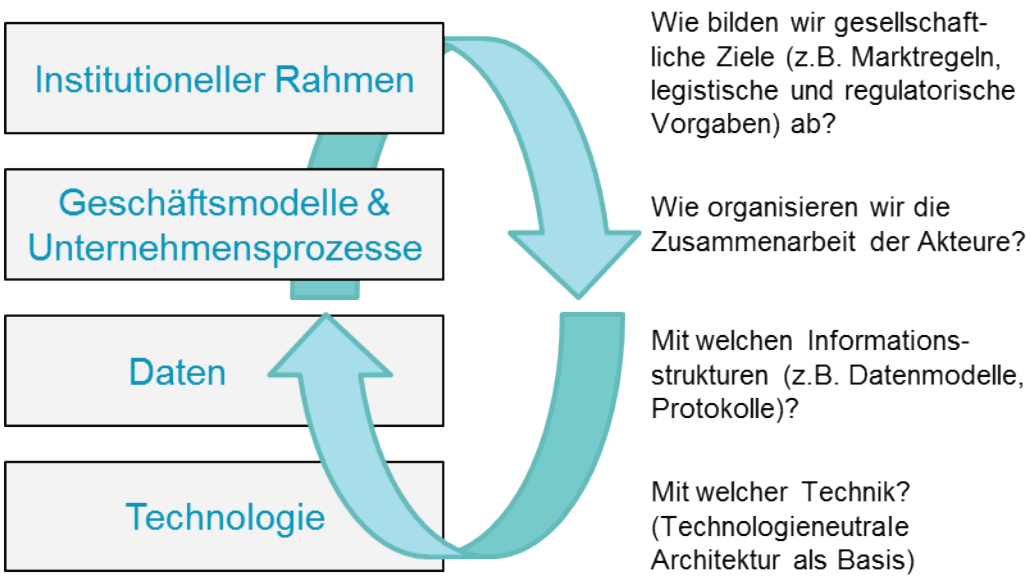

Abbildung 3: Ganzheitlicher Entwicklungsprozess einer sicheren Infrastruktur

Um bei der Entwicklung des zukünftigen Energiesystems Synergien für die beteiligten Akteure und notwendige Standards sicherzustellen ist eine abgestimmte Vorgehensweise unter umfassender Einbindung der relevanten Akteure erforderlich. Die Technologieplattform Smart Grids Austria schlägt dazu als Ansatz die Entwicklung einer Referenzarchitektur mit Bezugnahme auf entsprechende Europäische Entwicklungen vor. Dabei wird der Konsens aller relevanten Stakeholder über Inhalt, Funktionalität und Anwendung einer sicheren Infrastruktur und IKT-Architektur angestrebt. Durch den Prozess soll die Erarbeitung eines gemeinsamen Zielbildes für resiliente Smart Grids unter konsequenter Berücksichtigung von Interoperabilitäts-, Security-, Safety- und Privacy-Aspekten unterstützt werden. Durch die Erarbeitung konkreter Handlungsempfehlungen für die Migration vom heutigen System zu einer zukünftigen Smart-Grid-Infrastruktur soll ein gemeinsames Vorgehen der Akteure unterstützt werden. [Rassa-Quelle]

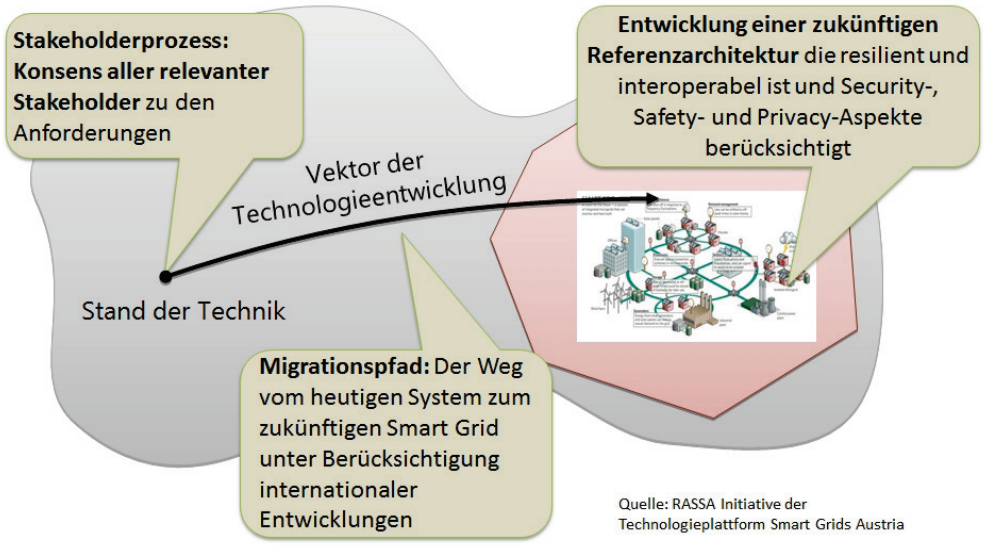

Abbildung 4: Der abgestimmte Weg in die Zukunft- Entwicklung einer sicheren Smart Grids Infrastruktur

4 Sicherheitsaspekte von Smart Grids

Die erwarteten Veränderungen durch die Entwicklung zum Smart Grid bergen neue Angriffspunkte in den Bereichen der Betriebssicherheit, der Versorgungsqualität und der Datensicherheit, die in Abbildung 5 dargestellt sind.

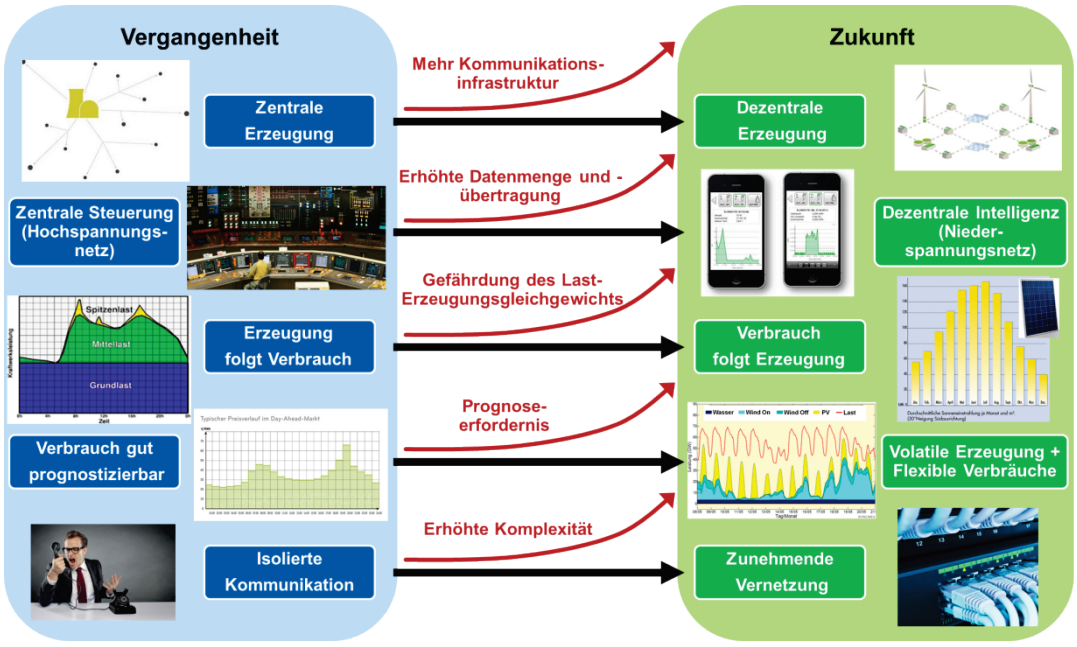

Abbildung 5: Veränderungen im Stromsystem durch Erneuerbare Einspeisung und Dezentralität[10]

[10] Berger, Angela. Smart Grids Austria. [Online] 11. Dezember 2014. [Zitat vom: 11. März 2015.] http://www.netz-security.at/programm.html.

Vor allem das IKT-System bietet Angriffsflächen für Bedrohungen, wie z.B. gezielte Angriffe physischer Natur, mittels Schadsoftware, unautorisierter Zugriff auf Daten, Fehlverhalten des Betriebspersonals oder mangelnde Benutzerakzeptanz. Eine Befragung des Kuratorium Sicheres Österreich (KSÖ) zeigt, welche Cyberrisiken Energieexperten in Österreich als besonders relevant erachten:

- Unsichere Steuerungssysteme (z.B. SCADA)
- Manipulation der IKT-Systeme der Energieerzeugung und -versorgung
- Cyberterrorismus, Cyberwar und Cybercrime
- Fehlendes Fachpersonal
- Fehlender Regulierungsfokus auf IKT-Sicherheit sowie nicht erkannte (IKT-)Anomalien
- Fahrlässiges Verhalten in strategischen Infrastrukturbetrieben
- Fehlende bzw. nicht aktuelle rechtliche Grundlagen[11]

Die Punkte unsichere Steuerungssysteme, Manipulation der IKT-Systeme und Cyberterrorismus zeigen die Notwendigkeit weiterer technischer Innovationen in diesen Bereichen. Dabei sind vor allem die Forschungseinrichtungen gefragt, Methoden und Produkte zu entwickeln, die ein hohes Maß an Sicherheit und Zuverlässigkeit garantieren. Dies ist die Voraussetzung für Benutzer- und Investorenakzeptanz.

Das Risiko durch fehlendes Fachpersonal fordert zum einen die Politik heraus, günstige Rahmenbedingungen zu schaffen, damit die durch die Veränderung des Energiesystems entstehenden Arbeitsplätze frühzeitig und adäquat besetzt werden können. Zum anderen sind die Energieversorgungsunternehmen und Netzbetreiber in der Pflicht, geeignete Fortbildungsmaßnahmen für Mitarbeiter anzubieten, um mit der technischen Entwicklung Schritt zu halten. In diesem Punkt ist eine koordinierte Vorgehensweise der betreffenden Ministerien und Behörden mit der Industrie zur Förderung der Fortbildung angesagten. Dasselbe trifft für den Punkt des fahrlässigen Verhaltens in strategischen Infrastrukturbetrieben zu.

Bei den Kritikpunkten fehlender Regulierungsfokus und fehlende rechtliche Grundlagen steht die Politik in der Pflicht, frühzeitig auf die Entwicklung im Energiesektor zu reagieren. Nur so kann verhindert werden, dass dieser Entwicklungsprozess gehemmt oder gar verhindert wird.

Um den Bedrohungen zu begegnen, muss das Smart Grid im Bereich der IKT-Sicherheit Mindestanforderungen erfüllen. Dazu zählen:

- Eine sichere IKT-Architektur als Grundlage (Security by Design)
- Verschlüsselung der Daten
- Möglichkeiten zu Prüfung der Authentifizierung
- Datenintegrität
- Angriffserkennungssysteme (Intrusion Detection Systeme)

[11] Kuratorium Sicheres Österreich. www.kuratorium-sicheres-oesterreich.at. [Online] 2012. [Zitat vom: 28. August 2015.] http://kuratorium-sicheres-oesterreich.at/wp-content/uploads/2015/02/Cyberrisikoanalyse.pdf

- Standards für Produkte und Dienstleistungen, sowie rechtliche Rahmenbedingungen
- Widerstandsfähigkeit und Wiederherstellung im Katastrophenfall[12]

4.1 Systematisierung der Sicherheitsaspekte

Für die systematische Analyse der Sicherheitsaspekte von Smart Grids wurde vom AIT eine Segmentierung erarbeitet, um daraus systematisch die wesentlichen offenen Fragen zu Sicherheitsaspekten von Smart Grids abzuleiten[13].

Die Segmentierungsmatrix setzt sich aus den Dimensionen des Technologieentwicklungsvektors und den Interoperabilitätsebenen zusammen und ist in Abbildung 6 dargestellt.

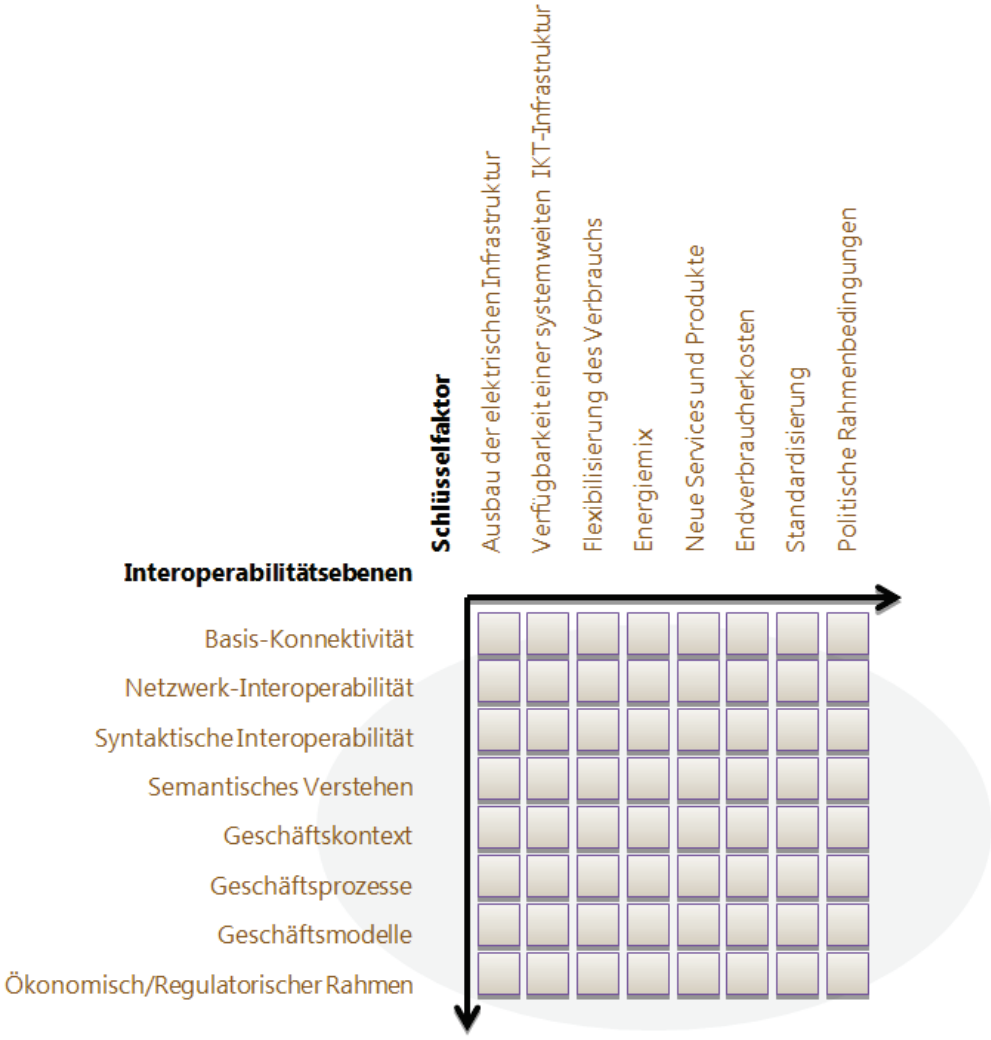

Abbildung 6: Segmentierungsmatrix

[12] Engel, Dominik. Josef Ressel Zentrum FH Salzburg. [Online] 10. Dezember 2014. [Zitat vom: 28. August 2015.] http://www.netz-security.at/docs/ppt/Engel.pdf

[13] T. Bleier, L. Langer, F. Kupzog, G. Kienesberger, M. Meisel. Systematisierung der Sicherheitsaspekte von Smart Grids (Version 13). Nachhaltig Wirtschaften Schriftenreihe des bmvit 41/2015

5 Stakeholder im Smart Grid

Für die Entwicklung eines sicheren Smart Grids wurden folgende Stakeholdergruppen als relevant erkannt:

- Infrastrukturbetreiber
- Nutzer, Markt
- Umsetzer, Innovationstreiber
- Institutioneller Rahmen

Abbildung 7 zeigt die identifizierten Stakeholder und deren individuelle Anforderungen an das Stromnetz.

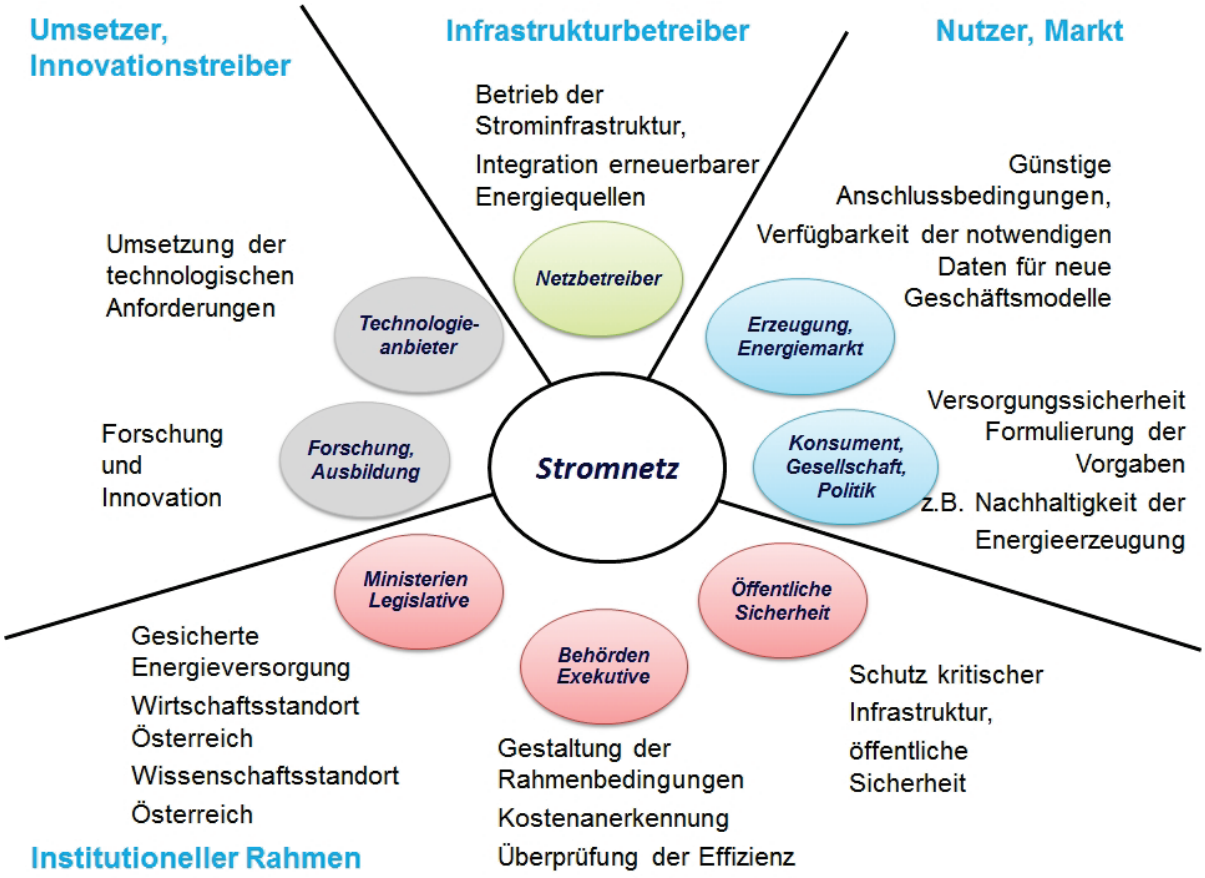

Abbildung 7: Ergebnis der Stakeholderanalyse im Zuge der RASSA Initiative der Technologieplattform Smart Grids Austria

Im Weiteren sind die einzelnen Stakeholdergruppen kurz charakterisiert.

5.1.1 Infrastrukturbetreiber

Die Gruppe der Infrastrukturbetreiber wird in erster Linie durch die Stromnetzbetreiber repräsentiert. Der Netzbetreiber ist auch für die Integration der dezentralen Erzeugung zuständig. Durch den Wandel zum Smart Grid werden zukünftig auch IKT-Infrastrukturbetreiber Anforderungen

haben. Telekom-Gesellschaften werden beispielsweise zukünftig Dienstleistungen für Stromnetzbetreiber anbieten. Interessensvertreter, wie der Verband Österreichs Energie, vertritt die Branche auch Richtung institutioneller Rahmen.

5.1.2 Nutzer, Energiemarkt

Der Energiemarkt, bestehend aus Erzeugern und Stromhändlern, nutzt die Infrastruktur, um seine Geschäftstätigkeit zu erledigen. Erzeuger speisen Strom ins Netz, das diesen transportiert. Händler bekommen über den Netzbetreiber die notwendigen Daten, um ihre Leistungen abzurechnen. Der Endkunde ist heute zum Großteil Verbraucher, das heißt er bezieht Strom aus dem Netz. Zukünftig wird er vermehrt auch zum Erzeuger (Prosumer) aufgrund von z. B. PV-Anlagen. Durch eine mögliche Flexibilisierung in seinem Verbraucherverhalten kann er darüber hinaus aktiver Marktteilnehmer werden.

Die Bevölkerung als Souverän einer Gesellschaft formuliert ebenfalls die politischen Ziele. Somit hat diese auch einen Einfluss auf die Anforderungen, an die Strominfrastruktur, wie Versorgungssicherheit und an die Umsetzung der Energiewende, also eine nachhaltige Energieversorgung.

5.1.3 Umsetzer, Innovationstreiber

Technologieanbieter stellen die Komponenten der Strominfrastruktur technologisch her. Die Anforderungen durch die Integration der erneuerbaren Energien sind teilweise noch nicht gelöst. Dafür leisten in Österreich die Forschungseinrichtungen gemeinsam mit den Technologieanbietern international sichtbare Arbeit. Interessensvertreter unterstützen die Unternehmer bei der Umsetzung ihrer Anforderungen und bei der Umsetzung ihrer Unternehmensziele.

5.1.4 Institutioneller Rahmen

Der institutionelle Rahmen beeinflusst einerseits den operativen Betrieb des Stromnetzes, andererseits werden Maßnahmen legistisch festgelegt, die die Energieversorgung und damit auch die Infrastruktur „Stromnetz“ beeinflussen. Ein weiterer Aspekt ist, das Stromnetz als kritische Infrastruktur der Gesellschaft sicher zu betreiben.

Der institutionelle Rahmen wird durch Ministerien und Behörden innerhalb Österreichs gestaltet, wobei der Rahmen zunehmend bereits durch EU-Richtlinien, die in Folge national umzusetzen sind, vorgegeben wird z. B. die NIS-Richtlinie.

Die Forschung wird durch die Politik unterstützt. Für Forschung und Innovation sind bezogen auf den institutionellen Rahmen, die Ministerien BMWFW und bmvit, gemeinsam mit Klima und Energiefonds (KLIEN) und der Forschungs- Förderungsgesellschaft (FFG) zuständig. Das Wirtschaftsministerium (BMWFW) ist zusätzlich für Fragen bezüglich Energie und den Wirtschaftsstandort Österreich zuständig. Für diesen ist eine gesicherte nachhaltige Energieversorgung ein Standortvorteil. Das Innen- und das Verteidigungsministerium (BMI, BMLVS) sowie das Bundeskanzleramt (BKA) sind für

die öffentliche Sicherheit mit unterschiedlichen Kompetenzen zuständig. Neben den Bundesbestimmungen haben auch die Bundesländer entsprechende Kompetenzen, die den institutionellen Rahmen beeinflussen.

6 Die entscheidenden Forschungsprojekte

6.1 RASSA - Reference Architecture for Secure Smart Grids in Austria

Die RASSA Initiative setzt sich die Entwicklung einer technischen Referenzarchitektur für sichere Smart Grids in Österreich zum Ziel. Das Projekt wird von der Technologieplattform Smart Grids Austria koordiniert. Dabei werden bestehende Arbeiten wie das SGAM-Modell und Regelungen wie das Smart Grid Mandat M/490 umgesetzt. Die Referenzarchitektur wird auf europäischer (v.a. D-A-CH) Ebene abgeglichen und bei der Entwicklung sollen die relevanten Stakeholder mit einbezogen werden.

Die Timeline des RASSA Prozesses sieht vor, bis Ende 2015 die Hauptanforderungen für die Referenzarchitektur zu analysieren. Bis 2017 soll die Referenzarchitektur fertiggestellt und eine sichere Kundenanbindung möglich sein und im Jahr 2018 die Rahmenbedingungen gestaltet sowie alle Security-Standards eingearbeitet werden[14].

6.2 Smart Grid Security Guidance (SG)2

Ein wichtiger Baustein auf dem Weg zum sicheren Smart Grid ist die Smart Grid Security Guidance (SG)2 unter der Leitung des AIT. Das Programm versteht sich als präventive Sicherheitsinnovation zum Schutz vor Angriffen und will Stabilität, Verfügbarkeit und Ausfallsicherheit zukünftiger Smart Grids erhöhen. Dies geschieht durch die Entwicklung einer Sicherheitsanalyse um Gefahren und Risiken für das Netz vorab zu erkennen, analysieren und zu bewerten. Ein Maßnahmenkatalog soll den zukünftigen Umgang mit Gefahren verbessern. Die Schritte zur Absicherung des Smart Grids sind in Abbildung 7 dargestellt.

Das Projekt SPARKS unter AIT Leitung gilt als Weiterführung des im Jahr 2014 geendeten (SG)2-Projekts.

6.3 Risikoanalyse für die Informationssysteme der Elektrizitätswirtschaft

Die unter der Leitung der E-Control entwickelte Risikoanalyse für die Informationssysteme der Elektrizitätswirtschaft in Abbildung 8 zeigt einen ähnlichen Ansatz wie die (SG)2 Risikoanalyse. Sie definiert 15 Gefahrenfelder, bewertet die Risiken und erarbeitet Maßnahmen zur Risikominimierung[15].

6.4 Projekt Smart Grid Security Guidance (SG)2

Aufbauend auf einer fundierten Bedrohungs- und Risikoanalyse aus einer gesamtstaatlichen Sicht und auf Sicherheitsanalysen von Smart Grid Komponenten wurden Maßnahmen für

[14] Berger, Angela. Smart Grids Austria. [Online] 11. Dezember 2014. [Zitat vom: 11. März 2015.] http://www.netz-security.at/programm.html.

[15] E-Control. www.e-control.at. [Online] 27. Februar 2014. [Zitat vom: 15. Juli 2015.] http://www.e-control.at/documents/20903/-/-/3f89d470-7d5e-433c-b307-a6443692d8f7.

Stromnetzbetreiber erforscht, die zur Erhöhung der Sicherheit der Computersysteme in der kritischen Infrastruktur „Energie“ der Zukunft dienen[16].

6.5 Sparks

Sparks[17] – Smart Grid Protection Against Cyber Attacks – ist ein EU FP7 Projekt, dass auf die Absicherung und Sicherstellung der Cybersecurity und Resilienz von Smart Grids abzielt. Es werden Bedrohungs- und Risikobewertungsmethoden untersucht und auch auf ausgewählte Demonstratoren im Mittel- bis Niederspannungsnetzbereich angewendet. Die in diesen fokussierten Szenarien gefundenen Ergebnisse sind allerdings auch für viel weitere Aspekte des Smart Grids übertrag- und generalisierbar.

6.6 Smart Grids Modellregion Salzburg (SGMS)

Die erste Modellregion für Smart Grids in Österreich hat speziell zum Thema Sicherheit und Referenzarchitekturen Vorarbeiten geleistet. Die wesentlichen Elemente für sichere Kommunikation im Smart Grid sind im Erkenntnisbericht der Modellregion zusammengefasst[18]: Technische Security, Datenschutz, Trust, Sicherheit in Organisation und Betriebsführung, Privacy- und Security-by-design.

6.7 SGMS – INTEGRA

INTEGRA ist das bisher letzte Projekt im Rahmen der Smart Grids Modellregion Salzburg und konsolidiert damit alle Vorprojekte der Smart Grids Modellregion Salzburg (~20 Smart Grid Teilprojekte und Demonstratoren) zu einer Smart-Grid-Gesamtarchitektur. INTEGRA erarbeitet aus diesen Einzelanwendungen ein Gesamtkonzept, wobei hier das Hauptaugenmerk auf dem Übergang zwischen Markt- und Netzgeführten Systembetrieb (Ampelmodell) liegt.

6.8 IniGrid

Das laufende Projekt „Integration of Innovative Distributed Sensors and Actuators in Smart Grids“ (iniGrid) versucht die Energieverteilung bis zum Verbraucher einerseits durch innovative Sensorik und Aktorik für aktiv betriebene Verteilnetze durch Schlüsselinnovationen (Smart Breaker, Mittelsspannungssensor) zu verbessern und andererseits durch die Umsetzung neuer Smart-Grid-Anwendungen, die sich durch diese neuen Komponenten ergeben können. Es wurde beispielsweise ein Use Case als Beschreibung eines Regelkreises definiert, der mehrere Sensoren, Aktuatoren und Automationstechnologien beinhaltet, die im Projekt entwickelt werden[19].

[16] Projekt „SG² – Smart Grid Security Guidance“: http://www.kiras.at/en/projects/detail/d/sg2-smart-grid-security-guidance/

[17] https://project-sparks.eu (abgerufen: 1. Feb. 16)

[18] SGMS, Ergebnisse und Erkenntnisse aus der Smart Grids Modellregion Salzburg, Mai 2013, online verfügbar: http://www.smartgrids.at/index.php?download=325.pdf (abgerufen: 1. Feb. 16)

[19] Meisel, M., Xypolytou, E., & Wendt, A. (2016). Ergebnisquerschnitt durch ausgewählte Smart Grids Projekte. In I. f. TUG (Hrsg.), 14. Symposium Energieinnovation (S. 10). Graz, Austria: Verlag der Technischen Universität Graz.

6.9 SGMS – Smart Web Grid

Zukünftige Smart Grids werden auf Datenaustausch zwischen verschiedenen Anwendungen und Marktteilnehmern beruhen. Das Projekt „Smart Web Grid“ untersuchte Nutzerinteraktion, Technik, Wirtschaftlichkeit und Datensicherheit eines solchen Datenaustausches anhand dreier konkreter Use Cases im Rahmen der Smart Grids Modellregion Salzburg (elektrische Lastverschiebung in Gebäuden und bei der Elektromobilität sowie Energieeinsparung durch Smart Metering).[20]

6.10 Smart LV Grid

Niederspannungsnetze müssen bereits jetzt mit Herausforderungen durch hohe Dichten von verteilten Erzeugern (insbesondere Photovoltaik) und Elektrofahrzeuge rechnen. Das Projekt Smart LV Grid zielte auf eine energie- und kosteneffiziente Nutzung vorhandener Netzinfrastrukturen basierend auf intelligenter Planung, Echtzeit-Beobachtung und aktivem Netzmanagement ab. Kommunikationsbasierende Lösungen für den aktiven Betrieb von Niederspannungsnetzen wurden erarbeitet und evaluiert. Ergebnisse sind bereits veröffentlicht[21].

6.11 IRON

Das Projekt „Integral Resource Optimization Network“ (IRON) hat untersucht und demonstriert, wie die Ressource „elektrische Energie“ durch innovative, auf informations- und Kommunikationstechnologie basierende, Services besser genutzt werden kann. Besser war aber nicht nur in dem Sinne der Energieeffizienz zu verstehen, sondern auch im Sinne von Kostenoptimierung mittels neuer Marktmodelle, Eigenlastoptimierung durch aktive Steuerung lokaler Komponenten aber auch Aggregation und Koordination kleiner, verteilter Komponenten als Virtuelles Kraftwerk[22]. Besonders für die Kategorie aktiver Verteilnetzbetrieb sind Erfahrungen aus dem Projekt bezüglich Steuerung und Nutzung von Flexibilität von essentieller Bedeutung.

6.12 ProAktivNetz

Im Projekt ProAktivNetz wurde ein Algorithmus für die optimierte aktive Verteilernetz-Betriebsführung, unter Berücksichtigung des aktuellen und prognostizierten Verhaltens von dezentralen, vorwiegend auf Erneuerbarer Energie basierenden Erzeugungsanlagen, entwickelt und getestet, um die automatisierte Planung für einen gegebenen Planungshorizont zu ermöglichen[23]. Diese Planung soll einerseits alle geplanten Freischaltungen innerhalb des Planungshorizonts, die

[20] Meisel, M., Berger, M., Hofer, T., Judex, F., Jung, M., Kienesberger, G., et al. (2014). SGMS - Smart Web Grid - Konzeption eines Informationsmodells für webbasierten Zugriff auf Smart Grids Daten. Wien: Österreichische Forschungsförderungsgesellschaft mbH (FFG).

[21] Faschang, M., Kupzog, F., Mosshammer, R., & Einfalt, A. (10-13. November 2013). Rapid Control Prototyping Platform for Networked Smart Grid Systems. Industrial Electronics Society, IECON 2013 - 39th Annual Conference of the IEEE, S. 8172-8176.

[22] Kupzog, F., Meisel, M., Derler, K., Traxler, E., & Bruckner, H. (2008). Integral Resource Optimization Network Concept. Wien: Österreichische Forschungsförderungsgesellschaft mbH (FFG).

[23] Xypolytou, E., Leber, T., & Aichholzer, T. (8-11. September 2015). Modeling renewable energy sources to promote proactivity in the distribution grid. Smart Electric Distribution Systems and Technologies (EDST), 2015 International Symposium on, S. 145-150.

Fahrpläne und erwarteten Einspeisungen der dezentralen Erzeugereinheiten umfassen und andererseits die erwarteten Lastverläufe. ProAktivNetz hat die Basis gelegt, zukünftige aktive Verteilernetze mit einem optimalen Fahrplan zu betreiben, der Schaltzustände des Netzes unter Beachtung der zu erwartenden Last- und Erzeugungssituation umkonfiguriert. So kann das Netz zu jedem Zeitpunkt für die anstehenden Aufgaben unter Einhaltung sämtlicher Randbedingungen im sicheren Bereich gefahren und die erwarteten Einspeiseleistungen der dezentralen Erzeuger berücksichtigt werden.

6.13 EigenLastCluster

Das Sondierungsprojekt umfasste die Bewertung der Sinnhaftigkeit neuer Ansätze zur Steigerung des Eigenverbrauchs von Strom und Wärme in bereits datentechnisch erfassten Gebäuden der Gemeinde Großschönau. Gebäudecluster (Gemeindeobjekte, Gewerbe, Haushalte) wurden gebildet und die Verbesserung der Eigennutzung mit und ohne Einsatz von zusätzlichen Batterie und/oder H2-Speichern sowie DSM Maßnahmen bewertet. Das Projekt hat gezeigt, dass eine Clusterung von verschieden Profilen zu einer PV-Anlage durchaus Sinn macht. Durch Clusterung kann die Wirtschaftlichkeit der Anlagen gesteigert werden. Jedoch wird durch diese Technologie den Speichern der ökonomische Vorteil gemildert bzw. komplett entzogen.

6.14 ICT4RobustGrid

Das Projekt ICT4RobustGrid analysierte u.a. die Voraussetzungen der verschiedenen Kommunikationstechnologien und Protokolle für eine Reihe von Smart-Grid-Anwendungen sowie für Demand-Response-Management, Störfallmanagement, Automatisation der Energieverteilung, Vertriebsmanagement, Zählerdatenmanagement usw. mit Hilfe von Multi-Agenten-Systemen (MAS). Beispielhaft wurden reale Netz-Topologien durch vereinfachte Simulationen für die Eignung der MAS-basierten Kommunikation ausgewertet. Die Ergebnisauswertung war auf die Datenrate Gesamtverzögerung (Übertragung, Verbreitung und Routing-Verzögerungen) und die Fehlerrate fokussiert. Weil verschiedene Smart-Grid-Anwendungen unterschiedliche Kommunikationseigenschaften erfordern, wurden die Anforderungen der einzelnen Kommunikationstechnologien für verschiedene Smart-Grid-Anwendungen abgebildet. ICT4Robust Grid Transition Roadmap – von zentralen zu dezentralen Kontrollsystemen[24].

6.15 SORGLOS

Die Erweiterung der Verteilnetze um Smart-Grid-Technologien bietet die Chance mit Hilfe von innovativen Regelstrategien für dezentrale Erzeugungsanlagen neue Beiträge zur Versorgungssicherheit zu leisten[25]. Im Forschungsprojekt „SORGLOS“ wurden daher Methoden und Algorithmen entwickelt, um in einzelnen Netzabschnitten (Microgrids) mittels vorhandener

[24] Faschang, M., Xypolytou, E., Meisel, M., Wendt, A., Kaufmann, T., Litzlbauer, M., et al. (2014). Transition Roadmap — from centralized to massively decentralized grid control systems. (D. M. Bakk.techn., Hrsg.) Wien: Eigenverlag des Institut für Computertechnik der TU Wien.

[25] Fasthuber, D., Litzlbauer, M., Marchgraber, J., Chochole, M., & Gawlik, W. (2015). Analyse des DSM- und V2G-Potentials des Großen Walsertals. 9. Internationale Energiewirtschaftstagung an der TU Wien (S. 10). Wien: IEWT.

dezentraler Erzeuger und Speicher sowie installierter Smart-Grid-Technologien Blackout-Festigkeit zu erreichen. Dabei wurden Schwarzstartfähigkeit bzw. sichere Netztrennung bei einem Blackout, Regelung von Erzeugung und Beeinflussung von Lasten sowie Speicherbewirtschaftung und Unterstützung beim Netzwiederaufbau untersucht. Darüber hinaus wurden im Projekt „SORGLOS“ rechtliche Grenzen und wirtschaftliche Möglichkeiten dieser Betriebsmethoden betrachtet.

6.16 aDSM

Im Projekt aDSM wurden hierarchisch, skalierbare Systeme mit dezentraler Intelligenz entwickelt, welche den Haushalts- sowie den zukünftigen Elektromobilitätsverbrauch flexibel an die lokal erzeugte, erneuerbare elektrische Einspeisung anpassen[26]. Hierbei wurden die Lastverschiebungen bzw. gesteuerte Ladevorgänge aktiv und vorausschauend durchgeführt. Kann kein lokaler Ausgleich erreicht werden, so sollen die oberen Systemebenen (bis hin zum Übertragungsnetz) oder Energiespeicher koordiniert eingreifen. Anhand von Elektrofahrzeugen und einer PV-Anlage wurde eine praktische Demo-Umsetzung des aDSM-Systems für einen einzelnen Netzknoten durchgeführt.

6.17 Technologie Roadmap Smart Grids 2020

Die Themen der Technologie Roadmap Smart Grids 2020[27] sind einerseits die Darstellung des Ist-Standes der Smart-Grids-Entwicklung in Österreich und international und andererseits des Nutzens von Smart Grids für die Industrie, Energiewirtschaft und Gesellschaft. Ausgehend vom aktuellen Stand der Entwicklung wurde außerdem der weitere Technologieentwicklungsbedarf abgeleitet und aufgezeichnet. Der Schwerpunkt lag hier bei den Anforderungen an die Marktentwicklung bis 2020. Dieser Ansatz verfolgt das Ziel für den Zeithorizont der kommenden Jahre, Anforderungen für die Unternehmen, Ausbildungseinrichtungen aber auch für den institutionellen Rahmen und den benötigten Förderbedarf herauszuarbeiten. Ergänzt wird dies in der Roadmap mit den Erkenntnissen aus internationalen Entwicklungen und den daraus entstehenden Chancen für Österreich. Bei der Erstellung der Roadmap ist die Berücksichtigung der Anforderungen an eine Systemarchitektur als Querschnittsmaterie mitbetrachtet worden.

6.18 IEA - Integrating the Energy System

Interoperabilität ist ein wesentlicher Baustein der Energiewende. Das Ziel des Projektes ist die Entwicklung einer modularen Prozesskette zur Erreichung von Interoperabilität im Smart Grid. Diese beginnt mit der Auswahl von Anwendungsfällen und Standards, Spezifikation deren normierter Verwendung, Umsetzung und schließt sich mit einer Demonstration der Prozesse und der Interoperabilitätstests. Dies erfolgt durch die Übertragung und Anpassung einer etablierten, bewährten und standardisierten Methodik aus dem Gesundheitswesen im branchenübergreifenden Wissensaustausch zwischen den Sektoren Gesundheit und Energie. Das Ergebnis des Projektes ist ein

[26] Gawlik, W., Kann, A., Günther, G., Karner, C., Groiß, C., Litzlbauer, M., et al. (2014). aDSM - Aktives Demand-Side-Management durch Einspeiseprognose. Wien: FFG NE2020 5.AS.

[27] Technologie Plattform Smart Grids Austria. (2015). Technologieroadmap Smart Grids Austria - Die Umsetzungsschritte zum Wandel des Stromsystems bis 2020. Wien: Eigenverlag.

detailliertes, dokumentiertes Verfahren zur normierten Anwendung von Standards für Interoperabilität im Smart Grid.

6.19 Smart Grid Modellregionen

Die Smart Grid Modellregionen oder Pionierregionen dienen zum Test der entwickelten Smart Grid Technologien im Feldversuch auf Praxistauglichkeit. Dabei werden alle entwickelten Einzelanwendungen zu einem Gesamtkonzept zusammengeführt. Abbildung 8 zeigt die laufenden Projekte in der Übersicht. Eine erfolgreiche Implementierung kann weiteren Regionen als Vorlage zur eigenen Umsetzung dienen. Die Umsetzung der Referenzprojekte ist Teil der Technologieroadmap von Smart Grids Austria. Das Ziel dabei lautet neben der Implementierung großflächiger Validierungsprojekte auch das Anstreben einer EU-weiten Themenführerschaft im Bereich Smart Grids[28] [29]. Eine Interaktive Beschreibung der Österreichischen Modellregionen findet sich unter www.smartgrids.at

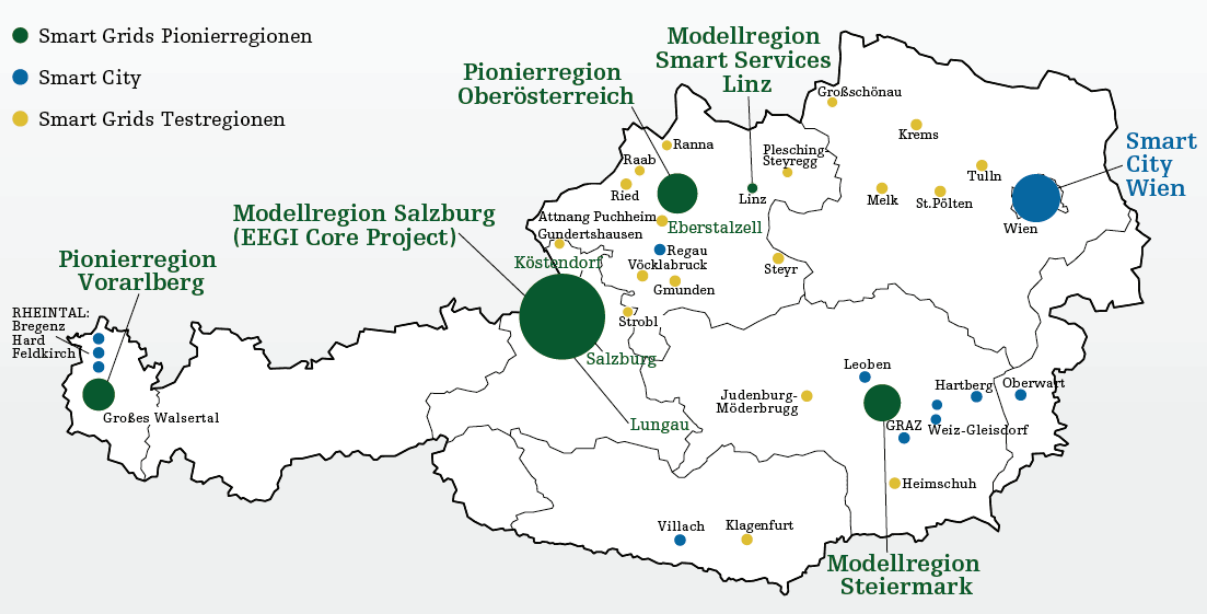

Abbildung 8: Karte der Smart Grid Modellregionen

[28] Technologie Plattform Smart Grids Austria. (2015). Technologieroadmap Smart Grids Austria - Die Umsetzungsschritte zum Wandel des Stromsystems bis 2020. Wien: Eigenverlag.

[29] Berger, Angela. Smart Grids Austria. [Online] 20. Mai 2015. [Zitat vom: 17. Juni 2015.] http://www.smartgridsweek.com/docs/SGW15_Poster_WEB/Poster_Berger.pdf.

7 Abbildungsverzeichnis