Smart Grid Security Guidance: Eine Sicherheitsinitiative für Intelligente Stromnetze

Florian Skopik[1], Thomas Bleier[1], Markus Kammerstetter[2], Georg Kienesberger[3]

[1]AIT Austrian Institute of Technology, Safety & Security Department
{florian.skopik|thomas.bleier}@ait.ac.at
[2]Technische Universität Wien, Institut für Technische Informatik
mkammerstetter@auto.tuwien.ac.at
[3]Technische Universität Wien, Institut für Computertechnik
kienesberger@ict.tuwien.ac.at

Abstract: Die Stromversorgung der Zukunft mittels Smart Grids wird weit mehr auf Informations- und Kommunikationstechnologie (IKT) setzen als das bisher der Fall ist. Damit werden Cybersecurity-Risiken auch zu einer Gefahr für die Energieversorgung. Viele Sicherheitsfragen in diesen zukünftigen Netzen sind noch ungeklärt, da die speziellen Umgebungen neuartige Sicherheitsmechanismen und -prozesse erfordern. Dieser Beitrag beschreibt die Eckpfeiler einer österreichischen Smart Grid Security Initiative, dem Projekt *Smart Grid Security Guidance:* $(SG)^2$. Ziel von $(SG)^2$ ist eine systematische Untersuchung von Smart Grid-Technologien in Bezug auf IKT-Sicherheitsaspekte und die Erforschung von Gegenmaßnahmen. Aufbauend auf einer fundierten Bedrohungs- und Risikoanalyse aus einer gesamtstaatlichen Sicht und auf Sicherheitsanalysen von Smart Grid-Komponenten werden Maßnahmen für Stromnetzbetreiber erforscht, die zur Erhöhung der Sicherheit der Computersysteme der Zukunft der kritischen Infrastruktur „Stromversorgung“ dienen.

1 Einleitung

Eine drastische Veränderung der Stromnetze ist derzeit im Gange. Konventionelle Wege zur Bereitstellung von Energie durch zentrale Versorger und bisherige Netztechnologien werden in Zukunft nicht mehr ausreichen, um die Energieversorgung unserer Gesellschaft sicherzustellen. Deshalb werden Informations- und Kommunikationstechnologien (IKT) zunehmend angewendet, um z.B. eine flexible Integration von Wind-, Solar- oder Biomasseenergieerzeuger in das vorhandene Stromnetz zu ermöglichen. Diese Integration von Energieanbieter, Verbraucher, Erzeuger und Netzbetreiber mittels IKT bilden die Grundpfeiler für Smart Grids. Mit dem zunehmenden Einsatz neuer Smart Grid-Technologien entsteht parallel zum Stromnetz ein umfassendes IKT-Netz, das durch seine große Ausdehnung und vielen Teilnehmer und Zugangspunkte ähnlichen Gefahren ausgesetzt sein wird wie beispielsweise derzeit das Internet. Allerdings wird die allgemeine Stromversorgung von diesem IKT-System abhängig sein, und ähnliche Sicherheitsprobleme wie im derzeitigen Internet hätten fatale Folgen. Potenzielle Bedrohungen reichen von Energiediebstahl durch Stromzählermanipulation, Angriffen auf Kontrollelemente der Netzbetreiber

zur Störung des Betriebes bis hin zu großräumigen Abschaltungen des nationalen Stromnetzes, beispielsweise aus terroristischen Motiven. Es ist daher unbedingt erforderlich, dass rechtzeitig Maßnahmen zur Gefahrenabwehr getroffen werden. Nur dann ist eine Zukunft für intelligente Stromnetze (Smart Grids) gewährleistet, ohne die Sicherheit der kritischen Infrastrukturen zu gefährden. Die Initiative *Smart Grid Security Guidance* - $(SG)^2$ - hat das Ziel, solche Maßnahmen zu erforschen. Im Zuge eines Projekts sollen Methoden, Konzepte und Vorgehensmodelle, sowie begleitende Softwarewerkzeuge, untersucht bzw. entwickelt werden, um das Risiko durch die beschriebenen Bedrohungen zu minimieren, und die Sicherheit von Smart Grids, hier speziell in Österreich, zu gewährleisten. Neuartige Ansätze zur Modellierung komplexer IKT-unterstützter Smart Grid-Architekturen werden im Projekt definiert, und bilden die Grundlage für eine Analyse und Evaluierung von primären Angriffsformen und Angriffsflächen, sowie zur Abschätzung von Folgewirkungen.

Das Problem der Absicherung der Energieversorgung gegenüber Cyberangriffen ist weltweit ein Thema, und deshalb arbeiten weltweit auch viele verschiedene Organisationen und Unternehmen an Produkten und Lösungen in diesem Bereich. Auch erste Entwürfe von Richtlinien und Maßnahmen finden sich in Ergebnissen der Arbeiten beispielsweise von NIST in den USA und ETSI in Europa. Diese berücksichtigen jedoch keine spezifischen nationalen Aspekte, wie lokale Regulierungs- und Marktbedingungen, rechtliche Anforderungen und Netzstrukturen, weswegen diese Richtlinien nicht direkt in Österreich eingesetzt werden können. Die breite Zusammenarbeit von Energienetzbetreibern, staatlichen Stellen die mit dem Schutz kritischer Infrastrukturen betraut sind, Smart Grid-Produktherstellern aus der Industrie und Experten im Bereich Informationssicherheit aus dem akademischen und privatwirtschaftlichen Bereich in diesem Projekt gewährleistet eine maximale Einbindung aller bisherigen internationalen und auch nationalen Entwicklungen in diesem Bereich, um darauf aufbauend neuartige, und wo erforderlich auch auf nationale Verhältnisse zugeschnittene Maßnahmen zur Realisierung eines zukünftigen sicheren und intelligenten Stromnetzes zu erforschen.

Dieser Artikel umfasst die folgenden Beiträge:

- Standardisierungsbestrebungen und Normen für Smart Grid Komponenten, insbesondere im deutschsprachigen Raum und der EU.
- Beschreibung des $(SG)^2$ Ansatzes zur Etablierung einer sicheren Smart Grid-Lösung auf nationaler Ebene.
- Technologische und regulatorische Herausforderungen im Zuge von $(SG)^2$.

Im Folgenden behandelt Abschnitt 2 den aktuellen Stand der Technik. Abschnitt 3 geht näher auf Bedrohungen auf technischer Ebene ein um die weiteren Arbeiten zu motivieren. Der darauf folgende Abschnitt 4 beschreibt das allgemeine Sicherheitsproblem auf höherer Ebene und skizziert die Struktur der $(SG)^2$-Initiative als möglichen Lösungsansatz. Konkrete Herausforderungen in den einzelnen Phasen der Initiative finden sich in Abschnitt 5. Abschnitt 6 diskutiert die Bedeutung von $(SG)^2$ und mögliche Auswirkungen. Der Beitrag schließt letztlich mit einer Zusammenfassung und Ausblick in Abschnitt 7 ab.

2 Hintergrund und aktueller Stand

2.1 Standardisierungsmaßnahmen in EU und Österreich

Die Zukunft der europaweiten Standardisierung im Bereich Smart Grids wird von einem Mandat der EU Kommission [ets10] an die Standardisierungsorganisationen geregelt. Dieses schreibt vor, dass im Rahmen der Aufgabenstellung eine Referenzarchitektur installiert werden soll. Mit Hilfe dieser Referenzarchitektur sollen dann bis Ende 2012 erste Standards fertiggestellt werden. Die Organisation haben die drei Standardisierungsorganisationen ETSI, CEN und CENELEC inne. Sie müssen aber, zusammen mit der Smart Grid Task Force garantieren, dass alle relevanten europäischen Akteure in die Arbeit eingebunden werden. In diesem Mandat wird auch die Wichtigkeit von Security in diesem Bereich betont, da derzeit keine ausreichenden Lösungen existieren. Darüber hinaus ist eine europaweite Standardisierung in diesem Bereich nur der erste Schritt zu einer endgültigen Lösung - wie auch im Bereich der Energienetze im Allgemeinen gibt es auch im Security-Bereich im Besonderen aufgrund nationaler Gesetzgebungen und Regulatorien besondere Anforderungen an Sicherheitsmaßnahmen, die auf einer nationalen Ebene Berücksichtigung finden müssen, solange es keine europaweit einheitlichen Regelungen in diesem Bereich gibt.

Auch in Österreich existieren bereits Pilotprojekte im Smart Grid-Bereich, meist aufbauend auf dem vom BMVIT initiierten Strategieprozess „Energie 2050“ [bmv10b]. Eine wesentliche Rolle spielt dabei das sogenannte „Smart Metering“ [bmv10a], das letztlich auch im Zuge der EU-Richtlinie über Endenergieeffizienz und Energiedienstleistungen (2006/32/EG) umzusetzen ist. Beim Smart Metering spielt die Unterscheidung zwischen Energielieferanten und Netzbetreibern eine wesentliche Rolle. Während der Energielieferant lediglich die Energie zur Verfügung stellt und diese an den Kunden verkauft, stellt der Netzbetreiber die notwendige Netzinfrastruktur zur Verfügung, zu welcher auch die für Smart Metering notwendige Kommunikationsinfrastruktur zählt. So ist davon auszugehen, dass nur der Netzbetreiber beim Endkunden Steueraufgaben vornehmen können soll. Gleichsam ist es wichtig, dass der Netzbetreiber und in weiterer Folge der Energielieferant ausschließlich gültige Daten von den Smart Meters der Endkunden erhält, da nicht nur Abrechnung, sondern auch Netzsteuerungsentscheidungen des Netzbetreibers an diese Daten gekoppelt werden können. Smart Metering ist derzeit nicht standardisiert, sodass im Rahmen der in Österreich laufenden Pilotprojekte unterschiedliche Lösungen verschiedenster Hersteller im Einsatz sind.

2.2 Security in Smart Grids

Smart Metering und Smart Grid-Systeme sind eine relativ neue Technologie, die aber in den kommenden Jahren vermehrt von der heimischen Energiewirtschaft (Strom, aber auch Fernwärme, Gas, etc.) eingesetzt werden wird, wobei auch in Österreich Smart Meter Pilot-Rollouts bereits begonnen haben (z.B. Energie AG, Linz Strom AG, Salzburg AG, etc.). Sicherheitsaspekte wurden allerdings bisher aufgrund des Pilot-Charakters der

Projekte oft vernachlässigt. Hersteller von Smart Meter-Systemen verfügen oft über nicht ausreichend Fachwissen über mögliche technische Angriffsvektoren auf ihre Produkte und sind davon überzeugt, dass diese ausreichend gesichert sind. Die Ereignisse nach Bekanntwerden des Stuxnet-Trojaners im Jahr 2010, der SCADA Systeme angegriffen hat [CAN11, Lan11], vermutlich mit dem Ziel, das iranische Atomforschungsprogramm nachhaltig zu sabotieren, hat aber zu einer Steigerung des Sicherheitsbewusstseins bei den Herstellern von industriellen Steuersystemen geführt, zu denen auch die Smart Meter und Smart Grid-Steuersysteme im allgemeinen gehören.

Ein Problem bei Umsetzung von Sicherheitsmaßnahmen sind neben den spezifischen technischen Anforderungen solcher Systeme auch die organisatorischen Gegebenheiten in diesem Umfeld. Während in anderen IKT-Netzwerken wie im Internet weltweit einheitliche Standards verwendet werden und die Innovationszyklen typischerweise im Bereich weniger Jahre liegen, ist in diesem Bereich aufgrund des Investitionsschutzes von einer Lebensdauer der Produkte und Systeme von 20, 30 oder noch mehr Jahren auszugehen, und das muss von Sicherheitskonzepten berücksichtigt werden. Außerdem sind Aufgrund historischer Entwicklungen oft regionale und proprietäre Systemlösungen im Einsatz, die eine einfache Übernahme von Sicherheitsmechanismen erschweren.

Im Bereich des Informationssicherheitsmanagements im Allgemeinen können derzeit im Wesentlichen zwei Ansätze unterschieden werden. Der eine wird prominent beispielsweise durch die ISO 27000 Normenreihe vertreten, die einen risikobasierten Ansatz verfolgt [iso05]. Demgemäß ist der Startpunkt der Risikobetrachtung in einer Organisation eine tiefgehende Risikoanalyse, und auf dieser basierend werden Maßnahmen und Prüfpunkte (sogenannte Controls) individuell erarbeitet und in der Organisation umgesetzt. Demgegenüber steht der „Baseline-Approach“ den beispielsweise auch das Grundschutzhandbuch des deutschen BSI verfolgt [bsi11b]. Hier wurde eine Risikoanalyse für „typische“ Umgebungen bereits durchgeführt (in diesem Fall vom BSI) und die Grundschutzkataloge beschreiben Standardmaßnahmen, die umgesetzt werden sollen und zu einem „Basislevel“ an Sicherheit (eben „Grundschutz“) führen. Darauf aufbauend können für einzelne Bereiche mit höherem Schutzbedarf weiterführende Analysen durchgeführt werden. Die Grundschutzkataloge des BSI geben Handlungsempfehlungen für viele typische IT-Szenarien in Unternehmen, beschränken sich jedoch auf die typische „Business-IT“ und gehen nicht auf Anforderungen oder Szenarien im industriellen Umfeld, beispielsweise in Prozessnetzwerken, ein. Zur Umsetzung der Grundschutzmaßnahmen sind Software-Tools von kommerziellen Anbietern und aus dem Open-Source-Umfeld verfügbar, die bei der Auswahl, Anpassung und Dokumentation der Maßnahmen unterstützen und so die Implementierung innerhalb einer Organisation erleichtern (beispielsweise das GSTool des BSI oder verinice).

3 Sicherheitsbedrohungen und Verwundbarkeiten

Beim Umbau zu Smart Grids, wird ein Datennetz benötigt, welches zur Steuerung und Regelung der Erzeuger, Verbraucher und des Verteilsystems geeignet ist und auch bis in die Haushalte verzweigt ist. Das Datennetz muss dementsprechend parallel zum gesam-

ten Stromnetz ausgebaut werden. Dies bedeutet eine große Angriffsfläche für Cyberattacken - denkbare Angriffsmuster wären etwa Abrechnungsbetrug an den Smart Metern, Störung von Kraftwerken bis hin zu terroristischen Angriffen auf große Teile des Netzes, was mit Black-Outs und hohen wirtschaftlichen Kosten verbunden wäre. In Folge dessen ist die Sicherheit des Stromnetzes der Zukunft untrennbar mit der Sicherheit dieses IKT-Netzwerkes verbunden.

Die Sicherheit in großen IKT-Netzwerken wie z.B. dem Internet ist ein ungelöstes Problem, wie die zahlreichen Cyberangriffe, über die fast täglich in den Medien berichtet wird, eindrucksvoll beweisen – selbst gut absicherte Netzwerke sind immer wieder Ziel erfolgreicher Attacken. Aufgrund der massiven Abhängigkeit der Stromversorgung vom parallelen IKT-Netz muss dieses jedoch von Beginn an so sicher wie möglich gestaltet werden. Im folgenden werden exemplarisch möglichen Gefahren, Risiken und deren Auswirkungen für den Bereich der Smart Meter beschrieben, um die Problemstellungen näher zu erläutern (siehe auch [bsi11a, She10]) - ähnliche Bedrohungen existieren für alle anderen Bereiche des Smart Grid.

Smart Meter Datenmodifikation: Lokale Angreifer (mit Zugang zu zentralen Zählerräumen oder Zählernischen) ändern in der Kommunikation zwischen Smart Meter und Konzentrator Datensätze, schleusen Daten ein, senden diese erneut oder leiten Daten um. Dadurch können wichtige Daten für die Energieabrechnung manipuliert, falsche Informationen bezüglich des Energieumsatzes an den Netzbetreiber gesendet oder falsche Steueraktionen ausgelöst werden.

Zeitmodifikation: Angreifer ändern die Uhrzeit und Zeitstempel im Smart Meter bzw. am Konzentrator, womit die Relation zwischen gemessenem Energieverbrauch und aktuellem Tarif nicht mehr stimmt. Dadurch ist ein Abrechnungsbetrug möglich. Das kann insbesondere bei den angedachten dynamischen Strompreisen in Smart Grids zu erheblichen wirtschaflichen Schäden führen.

Auslesen von fremden Smart Metern: Lokale Angreifer lesen fremde Smart Meter über deren Kommunikationsanbindung aus und gelangen so an sensible Daten über den Stromverbrauch oder Konfigurationsdaten.

Steuerung fremder Smart Meter: Lokale Angreifer steuern fremde Smart Meter, wodurch etwa der Stromfluss des entsprechenden Endkunden unterbrechbar wird.

Datenmodifikation in der Kommunikation: Angreifer ändern Datensätze in der Kommunikation zwischen Konzentrator und Netzbetreiber, schleusen Pakete ein, senden Pakete erneut oder leiten diese um. Dies betrifft nicht nur Datensätze von Smart Metern, sondern auch Konfigurationsdaten für Konzentratoren und Smart Meter, Software Updates, Steuersignale an das Stromnetz, mit unmittelbaren Auswirkungen auf Einrichtungen des öffentlichen Lebens (z. B. Ausschalten der Energiezufuhr in U-Bahnen, Beleuchtungen in öffentlichen Passagen, etc.).

Mithören der Kommunikation: Angreifer schneiden die Kommunikation zwischen Konzentrator und Netzbetreiber mit und gelangen auf diesem Weg zu sensibler Information über den Stromverbrauch, Konfigurationsdaten oder über Software(-updates).

Einbruch in die Kommunikationsinfrastruktur: Angreifer erlangen Kontrolle über Smart

Meter, Konzentratoren oder Netzwerkkomponenten des Netzbetreibers. Durch das Absetzen böswilliger Kommandos ist es möglich, dem Netzbetreiber sowie auch dem Stromnetz massiven Schaden zuzufügen.

Auslesen bzw. Modifikation der Software an Konzentrator und Smart Meter: Angreifer lesen die Konzentratorsoftware aus und modifizieren diese. Während beim schlichten Auslesen ggf. sensible Informationen an den Angreifer gelangen, sind mit der Softwaremodifikation auch finanzielle Schäden bis hin zu schwerwiegenden Angriffsfolgen zu erwarten. So könnte etwa ein (klassischer) IT-Angriff (z. B. ein Wurm) zum Totalausfall des Stromnetzes führen. Dasselbe gilt für die Smart Meter in den Haushalten.

4 Problemstellung und Lösungsansatz

Die beschriebenen tiefgreifenden Änderungen in der Struktur des Energieversorgungsnetzes machen auch ein grundlegendes Überdenken der Sicherheitsaspekte und -vorkehrungen notwendig. Aktuelle Forschungsergebnisse aus Schweden [CTA+11] weisen darauf hin, dass ein Angreifer bereits durch Kontrolle weniger Smart Meters gefährliche Spannungsspitzen verursachen und dadurch permanente Schäden für Energiekunden und Netzbetreiber bewirken kann. Ergebnisse aus anderen Studien weisen hingegen auf die besondere Problematik der kompletten Fernabschaltung hin [Cle08]. In Ländern wie den USA, wo der Smart Meter Rollout schon weiter fortgeschritten ist, konnten bereits 2009 bei einem System gravierende Sicherheitsmängel aufgedeckt werden, aufgrund welcher die praktische Entwicklung und Demonstration eines Smart Meter Wurms möglich war [Dav09, Goo09]. Entsprechende Risikoanalysen fehlen jedoch bis jetzt vollständig obwohl bei einem möglichen „Blackout“ Millionen Konsumentinnen und Konsumenten unmittelbar betroffen wären [Cle08, AF10, CK10].

Die Absicherung der Energienetze ist grundsätzlich Aufgabe der Netzbetreiber, welche Sie auch wahrnehmen. Aufgrund der Wichtigkeit der kritischen Infrastruktur „Stromnetz“ (kaum eine andere Infrastruktur kann ohne Strom funktionieren) gibt es allerdings über die Betrachtung aus Sicht eines Unternehmens hinaus aus gesamtstaatlicher Sicht noch eine viel größere Motivation zur Sicherstellung der Versorgungssicherheit. Daher müssen einheitliche Sicherheitsstandards entwickelt und auch von den Energieversorgern umgesetzt werden, die eine gewisse Qualität der Sicherheitsüberlegungen gewährleisten. Dies ist notwendig um:

- den Schutz dieser kritischen Infrastruktur sicherzustellen (d.h. zu garantieren, dass tatsächlich angemessene Schutzmechanismen eingesetzt werden);
- die Interoperabilität zwischen Komponenten/Netzen gewährleisten zu können, da das Smart Grid aus einer Vielfalt an teilnehmenden Technologien bestehen wird, und Lösungen nicht nur auf einen Netzbetreiber und dessen Situation zugeschnitten sein können;
- Aspekte des Datenschutzes schon im Vorfeld zu klären, und eine einheitliche Auslegung der einschlägigen gesetzlichen Bestimmungen zu gewährleisten;

- das Risiko von Schwachstellen von vornherein zu mindern, da auch hier das beste Netz nur so gut wie seine schwächste Stelle ist;
- den Versorgungsunternehmen, deren Fokus traditionell auf Betriebssicherheit und Ausfallsicherheit (Safety) gelegen ist, eine Hilfestellung bei Fragestellungen im Bereich der Angriffssicherheit (Security) zu geben;
- dieselben Überlegungen zu Sicherheitsthemen nicht mehrfach anzustellen und Securitymechanismen nicht mehrfach zu entwickeln. Die Kosten, die dadurch entstehen und letztlich auf den Energieabnehmer abgewälzt werden müssen, können damit reduziert werden.

Die historische Entwicklung des Internets zeigt ein Negativbeispiel der Entwicklung von Sicherheitsmechanismen. Sämtliche ursprüngliche Protokolle (wie z.B. Telnet, FTP, http, SMTP, POP) sind ungesichert. Security wurde erst nachträglich eingeführt, was zu den bekannten Problemen geführt hat, sodass immer wieder nachgebessert und erweitert werden musste. Im Rahmen von $(SG)^2$ sollen strukturierte Richtlinien entstehen, deren Umsetzung zu einer homogenen Sicherheitsarchitektur für Smart Grids führen. Daraus folgt der Bedarf nach zentral entwickelten Mindeststandards für die Security von Smart Grids. Dies muss speziell für das nationale Umfeld umgesetzt werden, da sich die Gesetze und technologischen wie infrastrukturellen Gegebenheiten von anderen Staaten unterscheiden, wobei natürlich auf bereits bestehende internationale Standards, Richtlinien und Empfehlungen aufgebaut werden muss.

Struktur von $(SG)^2$. Um dieses Ziel zu erreichen werden im Zuge von $(SG)^2$ existierende Architekturmodelle im Hinblick auf Bedrohungen und Verwundbarkeiten untersucht, um die effizientesten Schutzmaßnahmen gegen mögliche Angriffe zu ermitteln. Bisher lag der Fokus von Netzbetreibern hauptsächlich auf Ausfallssicherheit ihrer Systeme – bösartige Angriffe, welche durch die fortschreitende Vernetzung der IT-Komponenten innerhalb ihrer Systeme leichter möglich werden, müssen in Zukunft aber ebenso berücksichtigt werden. Ein wichtiges Ergebnis der Initiative wird daher auch ein Katalog von Schutzmaßnahmen sein, um – nach deren Anwendung – die Sicherheit von Smart Grids gegenüber IKT-basierten Bedrohungen gewährleisten zu können.

Zur realistischen Risikoabschätzung werden weiters Sicherheitsanalysen von Smart Grid-Komponenten durchgeführt, um die Bedrohungen und Verwundbarkeiten praktisch bewerten zu können. Da die Absicherung eines intelligenten Stromnetzes sehr komplex ist, werden weiters basierend auf existierenden Lösungen aus dem „allgemeinen“ IT-Security-Bereich neue Softwarewerkzeuge entwickelt, welche eine effiziente Anwendung der erforschten Richtlinien und Methoden in den speziellen Umgebungen der Energienetzbetreiber unterstützen.

Im Detail werden die folgenden beschriebenen kritischen Phasen zyklisch durchlaufen (siehe Abbildung 1).

1. *Erhebung geeigneter IT-Architekturmodelle* auf Basis existierender nationaler und internationaler Smart Grid-Pilotprojekte, um sicherheitsrelevante Fragestellungen unabhängig von spezifischen Szenarien einzelner Betreiber erforschen zu können.

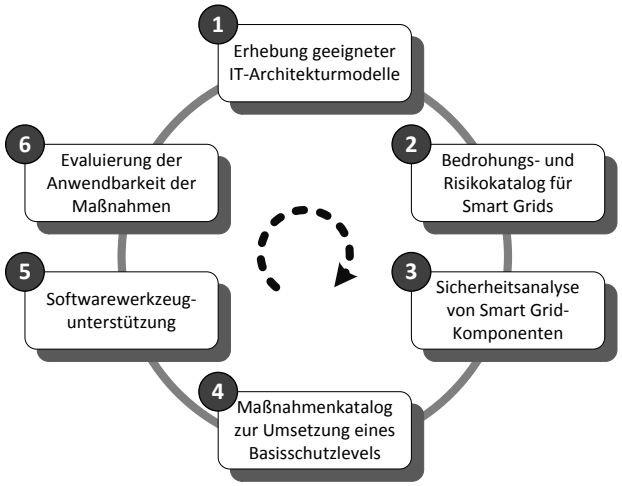

Abbildung 1: Ansatz von $(SG)^2$ zur Absicherung von Smart Grids.

2. *Bedrohungs- und Risikokatalog für Smart Grids* für spezifische Cyber-Bedrohungen von zukünftigen Energienetzen, die sich durch den verstärkten IKT-Einsatz in diesen Netzen entwickeln, zur Ableitung und Bewertung von Maßnahmen.
3. *Sicherheitsanalyse von Smart Grid-Komponenten* zur Bewertung der Bedrohungen und zur Begründung von Handlungsempfehlungen.
4. *Maßnahmenkatalog zur Umsetzung eines Basisschutzlevels* bei einem Energienetzbetreiber gegenüber den zuvor beschriebenen Bedrohungen („Smart Grid-Schutzhandbuch“).
5. *Softwarewerkzeugunterstützung* um die effiziente Umsetzung der erhobenen Schutzmaßnahmen zu gewährleisten.
6. *Evaluierung der Anwendbarkeit der Maßnahmen* anhand von Szenarien.

5 Technologische und Regulatorische Herausforderungen

Dieser Abschnitt geht näher auf die zuvor beschriebenen Phasen des $(SG)^2$-Ansatzes ein. Die speziellen Anforderungen und Ziele sind deutlich hervorgehoben.

5.1 Erhebung geeigneter IT-Architekturmodelle

Für die weitere Analyse von Bedrohungsszenarien für die Stromversorgung ist es essentiell, betreiberunabhängige Architekturmodelle zu entwickeln um eine breite Anwendbar-

keit der Ergebnisse zu gewährleisten. Zentrale Fragestellungen, die in Bezug auf die Architekturmodelle bearbeitet werden müssen, sind: (i) Welche Netzarchitekturmodelle sind derzeit international in Modellregionen und Pilotprojekten im Einsatz? Welche Ansätze können auf nationale Gegebenheiten übertragen werden? (ii) Was sind die zentralen technologischen Komponenten dieser Architekturen sowie deren Features und Funktionen? (iii) Welche dieser Komponenten werden zur Abdeckung neuartiger Anforderungen im Smart Grid mit Datenkommunikationsschnittstellen ausgestattet werden (z.B. für Fernzugriff, Wartung, Fernsteuerbarkeit etc.) und sind damit verbundene mögliche Angriffsziele?

Bereits die Architektur des heutigen Energieversorgungsnetzes ist komplex. Diese Komplexität wird aber mit zunehmenden Einsatz von Smart Grid-Komponenten massiv steigen. Ein Bericht der NIST [nis10] fasst die einzelnen Architekturkomponenten, Stakeholder und deren Interdependenzen anschaulich zusammen: (i) *Freier Energiemarkt:* ermöglicht das Anbieten von Energie über Internetplattformen. Auf diesem Weg kann zum Beispiel der Anbieter sehr flexibel und unkompliziert gewechselt werden. (ii) *Energieerzeugung:* produziert Energie entweder im großen Maßstab (industrielle Kraftwerke), oder im kleinen (z.B. Rückspeisung von durch Windkraft oder Photovoltaik erzeugter Energie ins Netz). In beiden Fällen können Erzeuger zu Energiemarktplattformen gekoppelt sein. (iii) *Energieübertragung:* kümmert sich hauptsächlich um den effizienten Transport von Energie über lange Distanzen. Zu diesem Zweck sind ausgefeilte Regelalgorithmen erforderlich, um das Hochspannungsnetz stabil zu halten. Diese Regelungen erfordern sehr genaue Messdaten (z.B. Spannungshöhe, Phasenverschiebung), die von speziellen Messstellen geliefert werden. (iv) *Energieverteilung:* dient der Verteilung von Energie auf Niederspannungsebene zu den einzelnen Haushalten (den Kunden). (v) *Kunde:* besitzt einen Smart Meter, welcher den Energieverbrauch misst und laufend einem Messstellenbetreiber übermittelt. (vi) *Messstellenbetreiber:* verwaltet Smart Meter-Daten und ist eng mit Produzenten des Energiemarkts verbunden, um diese bei der Abrechnung gegenüber den Kunden zu unterstützen.

Die Herausforderungen bei der Analyse und Modellierung moderner Architekturen und geplanten Beiträge des Projekts sind vielfältig. Ein Schwerpunkt stellt die Erforschung geeigneter neuartiger Ansätze zur **Modellierung der technischen IKT-Komponenten und deren Abhängigkeiten** in Smart Grids dar: (i) *Identifizierung von Kaskadeneffekten*, z.B. Analyse der Auswirkungen wenn eine Komponente (möglicherweise aufgrund eines Angriffs) ausfällt; (ii) Analyse besonders sensitiver Komponenten und damit lohnenswerter Angriffsziele; (iii) *Identifizierung der Assets* in Smart Grids und Konfigurationsmanagement, d.h. Komponententypen und Eigenschaften, um eine genauere Schwachstellenanalyse zu ermöglichen; (iv) Die *Identifizierung von Informationsflüssen* in Smart Grids zum frühzeitigen Abschätzen und Erkennen von Verkehrsengpässen, sowie zum Planen von Kompensationsschritten im Ausfallsfall. Neben den technischen Aspekten ist auch die **Modellierung organisatorischer Verantwortlichkeiten** auf multiplen Ebenen von großer Bedeutung, um die Rollen der einzelnen Akteure festzulegen, z.B. physische Ebene vs. Cyber-Ebene; oder Energietransport auf unterer Ebene und Steuerung/Regelung auf höherer Ebene.

5.2 Bedrohungs- und Risikokatalog für Smart Grids

Verteilte, vernetzte Systeme sind heute allgegenwärtig. Aufgrund neuartiger und sich verändernder Anforderungen, wird in Zukunft die Komplexität noch massiv steigen, gerade auch im Smart Grid. Die Sicherheit in solchen System wird immer schwieriger zu gewährleisten, insbesondere bedingt durch die folgenden Faktoren: (i) Viele Beteiligte, keine zentralen Stellen; (ii) Offene, verteilte Systeme bringen ein höheres Angriffspotential; (iii) Motivation für Angriffe ändert sich; z.B. „Hobby-Hacker", Cybercrime, Cyberwar (politisch/militärisch); und (iv) Methoden für Security Engineering sind in vielen Fällen in der Theorie bzw. im Labor bekannt, werden aber zu oft nicht in der Praxis umgesetzt (zu komplex, zu teuer, Wissen nicht am richtigen Ort, etc.).

Aus diesem Grund ist die strukturierte Bedrohungsanalyse in Smart Grids ein wesentlicher Bestandteil der $(SG)^2$-Initiative. Diese Bedrohungen und Attacken treten auf unterschiedlichsten Ebenen auf und betreffen die verschiedensten technischen Einrichtungen und Stakeholder. Die Herausforderungen bei der Bedrohungsanalyse in diesem Kontext sind daher weit gestreut, beginnend mit der **Evaluierung bereits eingesetzter Bedrohungs- und Risikoanalyseansätze** für IKT-Systeme, wie z.B. OCTAVE oder STRIDE. Diese Ansätze, welche für reine IKT-Strukturen entworfen wurden, müssen modifiziert werden. Weitere Schwerpunkte bilden die Erforschung neuartiger **Smart Grid-spezifischer Ansätze zur Bedrohungsanalyse**: Mithilfe neuer, zu entwickelnder Methoden und in Verbindung mit den zuvor erarbeiteten Architekturmodellen, welche Smart Grid-Komponenten und deren Interaktionen festhalten, können Bedrohungen und Risiken welche mit der Infrastruktur assoziiert sind, erhoben werden; sowie die **Untersuchung der Abhängigkeiten zwischen Safety und Security**: Eine Betrachtung von Security-Aspekten alleine ist nicht ausreichend. In diesem Umfeld ist eine systematische Sicht auf Safety und Security notwendig, um möglichst hohe Ausfallsicherheit zu gewährleisten, unabhängig davon, ob es sich um einen beabsichtigten Fehler (d.h. Angriff) oder unbeabsichtigten Ausfall handelt. Letztendlich ist auch die **Definition eines umfangreichen Katalogs möglicher Bedrohungen, Risiken und Auswirkungen von Angriffen** mit besonderer Berücksichtigung der nationalen Lage, d.h. spezielle vorherrschende Netzstrukturen und eingesetzte Komponenten, erforderlich. Die nationalen Gesetze bilden hierbei eine wichtige Grundlage zur Bewertung der Auswirkungen eines Angriffs, z.B. in Bezug auf Schutz der Privatsphäre.

5.3 Sicherheitsanalyse von Smart Grid-Komponenten

Zur realistischen Abschätzung realer Bedrohungen und Erhebung des aktuellen Schutzniveaus wird eine Sicherheitsanalyse von existierenden Komponenten aus den bereits umgesetzten Smart Grid-Pilotprojekten durchgeführt. Die wesentlichen Ziele in diesem Bereich sind die **Erforschung von aktuellen und zukünftigen Angriffsvektoren** für Smart Grid-Infrastrukturkomponenten auf technischer Ebene; die **stichprobenartige Überprüfung ausgewählter Angriffsszenarien** in einem Blackbox-Ansatz (d.h. ohne Zusatzinformationen über Komponentendetails wie z.B. Konfiguration und Source Code) bzw. einem Glassbox-Ansatz (d.h. mit Zusatzinformationen über Komponentendetails wie z.B. Kon-

figuration und Source Code); sowie die **Erhebung des aktuellen Sicherheitsniveaus der am Markt befindlichen Produkte**, mit dem Rückfluss dieser Erkenntnisse in die Produktentwicklung über die im Projekt beteiligten Netzbetreiber (als „Kunden“ bzw. „Käufer“ der Produkte) und Produkthersteller als kurzfristigen positiven Nebeneffekt.

5.4 Maßnahmenkatalog zur Umsetzung eines Basisschutzlevels

In heutigen und vor allem in zukünftigen Energienetzen werden eine Vielzahl an komplexen Sicherheitsanforderungen an die unterschiedlichen Komponenten und Systeme gestellt. Hierbei können diese Anforderungen aus unterschiedlichen Blickwinkeln erhoben und priorisiert werden, beispielsweise: (i) fundamentale Risikoanalysen für den Netzbetreiber, Kunden, Staat; (ii) aus architektureller-, funktionaler und nichtfunktionaler Sicht; und (iii) auf unterschiedlichen Ebenen, d.h. von der Energieübertragung, über das IKT-Netzwerk bis zur Backend-Logik in Rechenzentren.

Bereits heute existieren viele technische Standardisierungsinitiativen im Smart Grid-Bereich; einige davon berücksichtigen auch Security-Aspekte. Allerdings sind diese oft nicht unmittelbar auf nationale Verhältnisse anwendbar, weil z.B. nicht auf Netzaufbau, Marktsituation oder individuelle Anforderungen eingegangen wird. Existierende Standards und Richtlinien (z.B. BSI - Smart Meter Gateway Protection Profile, DIN 27009, IEC 62351, ANSI/ISA99, NERC CIP, VDI/VDE 2182 etc.) sind auf einen spezifischen Ausschnitt fokussiert (z.B. nur das Managementsystem oder nur ein technisches Protokoll) und berücksichtigen nicht die Gesamtheit der für einen Energieversorger in der praktischen Anwendung notwendigen Sicherheitsmaßnahmen.

Eines der Hauptziele von $(SG)^2$ ist die Erarbeitung eines umfassenden Maßnahmenkatalogs, welcher Netzbetreibern eine praktisch anwendbare Sammlung von Richtlinien und Best Practices bietet, um einerseits deren bestehende Smart Grid-Strukturen besser abzusichern und andererseits die konsequente Berücksichtigung von Security bei Neuplanung zu ermöglichen. Inhaltliche Beispiele für solche Richtlinien und Maßnahmen sind z.B. Schutzmechanismen von Einzelkomponenten in Bezug auf CIA (confidentiality-integrity-availability): (i) Sinnvolle und/oder erforderliche Kombination von Produkten (z.B. eine Komponente welche Daten unverschlüsselt ausgibt muss mit einem Verschlüsselungsmodul (Gateway) versehen werden; (ii) Konfiguration und Features von Schutzmechanismen (Stärke der Verschlüsselung um gegen State-of-the-Art Angriffsmethoden gewappnet zu sein, Konfiguration von Authentifizierungsmechanismen, Zertifikation usw.); (iii) Vernetzungstechnologien, z.B. IP-basierte Kommunikation über öffentliches Telekommunikationsnetz benötigt andere Schutzmechanismen als Power Line Carrier im Hochspannungsbereich; (iv) Einsetzbarkeit von Technologiefamilien innerhalb einer vorgegebenen Netzarchitektur aus Security-Sicht.

Bei der Erarbeitung des Maßnahmenkatalogs hilft die **Erstellung einer Taxonomie von Angriffen und Gegenmaßnahmen** um Attacken und Schutzmaßnahmen strukturiert aufzuarbeiten. Die eigentliche **Erarbeitung eines Maßnahmenkatalogs** („Schutzhandbuch“) geschieht aufbauend auf den in der Modellierungsphase klar identifizierten (System, Be-

drohung, Risiko)-Kombinationen (Tupel). Mit einer solchen Liste können Sicherheitsexperten bereits existierende Richtlinien identifizieren, welche beim Absichern eines Systems herangezogen werden können. Die dokumentierten Tupel werden folgendermaßen verwendet: *System und Bedrohung:* Informationen über System und potentielle Bedrohungen dienen zur Definition von (techn.) Gegenmaßnahmen, *Risiko:* Mit einem Risiko wird eine Wahrscheinlichkeit des Auftretens einer Bedrohung assoziiert; speziell unter Berücksichtigung nationaler Gegebenheiten. Diese Information bildet die Grundlage um die Auswahl angemessener Schutzmaßnahmen, d.h. unter Berücksichtigung von Kosten, Effizienz, und Einfluss auf die Usability, zu ermöglichen. Letztlich ist vor allem die **Evaluierung der Schutzmaßnahmen**, welche in der Taxonomie definiert wurden, im Kontext nationaler Pilotszenarien von besonderer Bedeutung (siehe weiter unten). Hier werden theoretische aber wenig praktikable Konzepte von praktisch besser anwendbaren Maßnahmen getrennt und bewertet. Die Anwendung der Schutzmaßnahmen muss softwaretechnisch unterstützt werden um eine Konformität mit dem Maßnahmenkatalog zeit- und ressourceneffizient zu erreichen.

5.5 Softwarewerkzeugunterstützung

Das Smart Grid wird zunehmend zu einem komplexen System, welches Komponenten des Energieversorgungsnetzes und IKT-Module kombiniert. Aufgrund dieser Komplexität und engen Kopplung wäre eine manuelle Anwendung der in $(SG)^2$ erforschten Richtlinien sehr ressourcenintensiv und damit ein Hindernis für eine breite Anwendung. Insbesondere das Verfolgen der Konformität eines Netzes mit den erarbeiteten Richtlinien über längere Zeiträume gestaltet sich schwierig. Darüber hinaus ändern sich aufgrund neu aufkommender Bedrohungen die Anforderungen an Security-Mechanismen in relativ kurzen Zeitintervallen. Um mit diesen dynamischen Prozessen Schritt halten zu können, ist der Einsatz spezifischer Softwarewerkzeuge unumgänglich. Auch hier werden auf Basis existierender Erkenntnisse aus anderen (IKT-Sicherheits-) Domänen Lösungen entwickelt werden, die auf die spezifischen Anforderungen der IKT-Systeme in Smart Grids zugeschnitten sind. Die wesentlichen Ziele und Ergebnisse dieses Teils sind die **Definition von Standarddatenformaten zur Beschreibung** von Technologien, Netzwerkkomponenten, Bedrohungen und Sicherheitsmaßnahmen; die **Definition von Schnittstellen** um den Datenaustausch zwischen verschiedenen Werkzeugen, aber auch die Interoperabilität zwischen verschiedenen Instanzen (z.B. unterschiedlicher Netzbetreiber) im Bereich Informationssicherheit zu ermöglichen; die **Analyse existierender Ansätze und Werkzeuge** und Untersuchung bzgl. Verwendbarkeit und Erweiterbarkeit, z.B. Microsoft Secure Development Lifecycle (SDL), diverse Werkzeuge zur Modellierung von Bedrohungen, IDMEF, Verinice, usw.; und die **Anpassung existierender bzw. Entwicklung neuer Werkzeuge** zur Unterstützung der Umsetzung des Maßnahmenkatalogs.

5.6 Evaluierung der Anwendbarkeit der Maßnahmen

Basierend auf den erarbeiteten Methoden, Techniken und Maßnahmen wird eine Instanziierung anhand realistischer Szenarien durchgeführt, um einerseits die Anwendbarkeit der erforschten Methoden, Techniken und Maßnahmen zu evaluieren, als auch den Sicherheitsgewinn durch Umsetzung ausgewählter Schutzmaßnahmen zu demonstrieren. Die dabei gewonnen Erkenntnisse sind eine wichtige Grundlage für die weitere, großflächige Umsetzung des Maßnahmenkatalogs und auf $(SG)^2$ aufbauende Folgearbeiten. Dabei lässt sich diese Phase in folgende Hauptaufgaben gliedern: (i) **Definition von Szenarien** (Businessprozesse, Teilsysteme, etc.) die vom Umfang passend für eine aussagekräftige Evaluierung der erarbeiteten Ergebnisse sind und eine repräsentative Evaluierung des gesamten Maßnahmenkatalogs erlauben. (ii) **Anwendung der erarbeiteten Methoden, Techniken, Tools** und Entwicklungen in den Pilotszenarien. (iii) **Ausarbeitung von konkreten Umsetzungsplänen** basierend auf der Anwendung des Maßnahmenkatalogs, und **Evaluierung des Sicherheitsgewinns**; (iv) **Evaluierung der Anwendbarkeit der erarbeiteten Methoden, Techniken und Tools**.

6 Diskussion und Bedeutung von $(SG)^2$

Die wesentliche Innovation von $(SG)^2$ besteht darin, ein fundiertes, direkt anwendbares Rahmenwerk für verschiedene Stakeholder auf nationaler Ebene und auf Ebene der Energieversorger zur Verfügung zu stellen, welches auf praktische Anwendung ausgerichtete Maßnahmen zur Gewährleistung eines einheitlichen Basisschutzlevels für die kritische Infrastruktur „Stromversorgung“ zur Verfügung stellt. Diese Maßnahmen werden durch Sicherheitsanalysen von IKT-Komponenten aus bereits umgesetzten oder in der Umsetzung befindlichen Smart Grid-Pilotprojekten begründet, welche einen in dieser Tiefe ebenfalls noch nicht existierenden Einblick in die Sicherheit der aktuell verfügbaren Systemkomponenten heutiger und zukünftiger Energienetze liefern. Begleitend dazu wird eine umfassende Untersuchung dieser Thematik durchgeführt, die rechtliche und gesellschaftliche Aspekte umfasst aber auch die praktische Anwendung der in $(SG)^2$ erforschten Ergebnisse anhand von Beispielszenarien erprobt und evaluiert.

Die durchgeführten Arbeiten sind ein wesentlicher Schritt hin zu einem „Security by Design“ Ansatz für die Weiterentwicklung unserer Stromversorgung in Richtung Smart Grids. Aufgrund der Kritikalität dieser Infrastruktur ist es von essentieller Bedeutung, bei einem massiven Umbau der Betriebsprozesse in Richtung IKT-Unterstützung wie es in Zukunft geschehen wird, die IT-Security-Aspekte von Beginn an mit zu berücksichtigen. Dies stellt einen wesentlichen Technologiesprung dar, da herkömmlicherweise oft Sicherheit erst im Nachhinein bei schon existierenden Systemen implementiert wurde.

International gibt es einige Initiativen die in eine ähnliche Richtung gehen, von denen sich aber $(SG)^2$ wesentlich unterscheidet. Beispielsweise ist in Deutschland die Definition des Schutzprofils für ein Smart Meter-Kommunikationsgateway derzeit das Thema in diesem Bereich in dem die größten Anstrengungen unternommen werden. Allerdings

fokussierte diese Arbeit auf einen zwar wesentlichen, aber trotzdem nur eingeschränkten Teilausschnitt der Smart Grid-Thematik. Einen breiteren Ansatz stellt die Entwicklung der DIN 27009 (Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung) dar, die gerade begonnen wurde. Allerdings wird hier wiederum der Fokus ganz klar im Sinne der ISO 2700x Normenreihe auf das Managementsystem gelegt, das sich mit dem Informationssicherheitsmanagement beschäftigt, und die notwendige Tiefe zur praktischen Umsetzung muss von einem Energieversorger, der diese Norm umsetzen will, selbst erarbeitet werden. Dadurch ist zum einen natürlich der Blickwinkel im Sinne der Risikobetrachtung ein unternehmenszentrierter und nimmt naturgemäß auf nationale bzw. strategische Aspekte wenig Rücksicht, zum anderen sind die erarbeiteten Lösungen der Energieversorger unterschiedlich und schwer vergleichbar, wie das auch derzeit mit Informationssicherheitsmanagementsystemen nach ISO 27001 der Fall ist. Weiters sind die Rahmenbedigungen in Deutschland, wie auch in anderen Ländern wie Italien oder Frankreich, sehr unterschiedlich - während in diesen Ländern beispielsweise wenige große Betreiber von Energienetzen den Markt im Wesentlichen unter sich aufteilen, ist die Struktur der Energienetze in Österreich eine gänzlich andere (verhältnismässig mehr, kleinere Betreiber), und erfordert damit auch andere Konzepte. Noch viel unterschiedlicher sind die Voraussetzungen im Bereich der Energieversorgung in Ländern wie den USA, China oder Japan, sodass die dort entwickelten Konzepte beispielsweise von NIST und NERC zwar als wichtiger Input für die Entwicklung von Lösungen in Österreich dienen können, aber keine nennenswerte direkte Anwendung finden können.

7 Zusammenfassung und Ausblick

Zusammenfassend sind die wesentlichen Features von $(SG)^2$: (i) Umfassende Erforschung der Bedrohungen, Verwundbarkeiten und Risiken der zukünftigen auf IKT-basierenden Energienetze; (ii) Erarbeitung eines auf die nationalen Rahmenbedingungen abgestimmten Rahmenwerkes für Sicherheitsmaßnahmen bei Energienetzbetreibern; (iii) Entwicklung neuartiger Techniken zur Sicherheitsanalyse von Hard- und Software von realen Smart Grid-Komponenten, unter Einbindung führender nationaler Hersteller; (iv) Tiefer Einblick in die Sicherheit aktuell verfügbarer Komponenten für Smart Grids; (v) Konsolidierte Darstellung der IKT-Architekturen die in Smart Grids Anwendung finden, als Basis für weitere Analysen.

Ziel von $(SG)^2$ ist es, die Stabilität und Verfügbarkeit zukünftiger Smart Grids zu erhöhen und Ausfallsicherheit zu gewährleisten. Durch die entstehenden Sicherheitsinnovationen können existierende Systeme zukünftig besser abgesichert oder neue Systeme von Grund auf mit bestmöglicher Sicherheit vor Angriffen ausgestattet werden. Durch $(SG)^2$ wird vermieden, dass zuerst ein vollständiges Rollout von unsicheren Smart Grid-Lösungen stattfindet und sich im Nachhinein (etwa im Zuge schwerwiegender Angriffe) herausstellt, dass die eingesetzte Infrastruktur nicht ausreichend gesichert war. Während genau dies in der historischen Entwicklung des Internets geschah (wo erst nach und nach Security-Lösungen eingeführt wurden), gilt es diese Entwicklung beim Smart Grid zu vermeiden.

Danksagung

Folgende Organisationen tragen zu $(SG)^2$ bei: Austrian Institute of Technology, Technische Universität Wien, SECConsult GmbH, Siemens AG, Linz Strom GmbH, Energie AG OÖ Data GmbH, Innsbrucker Kommunalbetr. AG, Energieinstitut a. d. JKU Linz GmbH, Bundesministerium f. Inneres, Bundesministerium f. Landesverteidigung u. Sport.

Literatur

[AF10] Ross Anderson und Shailendra Fuloria. Who controls the off switch? In *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2010.

[bmv10a] Intelligente Energiesysteme der Zukunft: Smart Grids Pioniere in Österreich. Bericht, Bundesministerium für Verkehr, Innovation und Technologie, 2010.

[bmv10b] Strategieprozess Energie 2050. Bericht, Bundesministerium für Verkehr, Innovation und Technologie, 2010.

[bsi11a] 20109: Schutzprofil für die Kommunikationseinheit eines Mess-Systems Gateway PP, v0.7.3. Bericht, Bundesamt für Sicherheit in der Informationstechnik, 2011.

[bsi11b] IT-Grundschutz-Kataloge. Bericht, Bundesamt für Sicherheit in der Informationstechnik, 2011.

[CAN11] Thomas M. Chen und Saeed Abu-Nimeh. Lessons from Stuxnet. *IEEE Computer*, 44(4):91–93, 2011.

[CK10] S. Clements und H. Kirkham. Cyber-security considerations for the smart grid. In *Power and Energy Society General Meeting*, 2010.

[Cle08] F.M. Cleveland. Cyber security issues for Advanced Metering Infrasttructure (AMI). In *Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*, 2008.

[CTA+11] Mihai Costache, Valentin Tudor, Magnus Almgren, Marina Papatriantafilou und Christopher Saundersy. Remote control of smart meters: friend or foe? In *European Conference on Computer Network Defense*, 2011.

[Dav09] Mike Davis. SmartGrid Device Security: Adventures in a new medium. In *Black Hat USA*, 2009.

[ets10] Technical Report 102 691: Machine-to-Machine communication; Smart metering Use Cases. Bericht, ETSI, 2010.

[Goo09] Dan Goodin. Buggy 'smart meters' open door to power-grid botnet, 2009.

[iso05] ISO/IEC 27001 - Information technology - Security techniques - Information security management sys-tems - Requirements. Bericht, ISO, 2005.

[Lan11] Ralph Langner. Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Security & Privacy*, 9(3):49–51, 2011.

[nis10] NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0. Bericht, National Institute of Standards and Technology, 2010.

[She10] R. Shein. Security Measures for Advanced Metering Infrastructure Components. In *Power and Energy Engineering Conference (APPEEC)*, Seiten 1–3, 2010.