Eine Architektur für sichere Smart Grids in Österreich

Oliver Jung[1] · Stefan Fenz[2] · Markus Kammerstetter[3] · Aleksandar Hudic[1]

AIT Austrian Institute of Technology[1]
oliver.jung|aleksandar.hudic@ait.ac.at

SBA Research[2]
SFenz@sba-research.org

Technische Universität Wien[3]
Secure Systems Lab Vienna, Automation Systems Group
mk@seclab.tuwien.ac.at

Zusammenfassung

Um die Interoperabilität komplexer Systeme zu gewährleisten, sind Referenzarchitekturen ein geeignetes Mittel, um den Entwicklungsprozess zu erleichtern. Für Österreich wird gerade eine Referenzarchitektur für Smart Grids unter besonderer Berücksichtigun von Sicherheitsanforderungen entwickelt. Diese Architektur basiert auf den internationalen Standards und Richtlinien, aber nimmt auch Bezug auf die spezifischen nationalen Gegebenheiten. Über die eigentliche Architektur hinaus, werden weitere Security-Komponenten wie Risikoanalyse, Risikomanagement und Penetration Testing in der Architektur verankert, die die Entwicklung und den Betrieb von sicheren Smart Grids unterstützen.

1 Einleitung

Die geplante Energiewende, bei der der überwiegende Anteil elektrischer Energie aus erneuerbaren Energiequellen erzeugt wird, stellt eine Herausforderung für unsere Energienetze dar. Durch den zunehmenden Einsatz von Information- und Kommunikationstechnologie werden neue Konzepte der Netzsteuerung ermöglicht, mit denen dieser Herausforderung begegnet werden kann. Dieser unter dem Begriff "Smart Grid" bekannte Ansatz bietet nicht nur viele Vorteile gegenüber den bislang oft manuellen Betrieb der Stromnetze, sondern bringt auch neue Bedrohungen mit sich. Im Rahmen des Forschungsprojektes RASSA (Reference Architecture for Secure Smart Grids in Austria) Architektur wird derzeit eine Referenzarchitektur für sichere Smart Grids in Österreich entwickelt, die neben der Interoperabilität der Komponenten auch den sicheren Betrieb der zukünftigen intelligenten Stromnetze zum Ziel hat.

RASSA-Architektur ist Teil der RASSA-Initiative [MBLL+16], ein von der Technologieplattform Smart Grids Austria initiierter Entwicklungsprozess zur Entwicklung einer Smart-Grid-Referenzarchitektur in Zusammenarbeit mit allen relevanten Interessengruppen. Mitglieder der Technologieplattform sind die neben den großen österreichischen Netzbetreiber auch Technologieanbieter, Forschungseinrichtungen und Interessenverbände.

Die Entwicklung der Referenzarchitektur geht einher mit der Modellierung der Schnittstellen und Komponenten. Dafür wird die SGAM Toolbox [SGA14] verwendet werden, die sich auf

das von einer gemeinsamen Arbeitsgruppe aus Vertretern von CEN, CENELC an ETSI definierten Smart Grid Architecture Model (SGAM) [CENC12] stützt und es ermöglicht, Smart Grid Anwendungen zu modellieren.

Für die sicheren Betrieb von Stromnetzen ist es jedoch nicht ausreichend bei der Definition der Komponenten, Schnittstellen und deren Funktionalität für den Schutz von Datenauthentizität, Datenintigrität und Datenvertraulichkiet zu achten. Da Sicherheit vielmehr ein Prozess ist, der auf aktuelle Entwicklungen wie z.B. das Bekanntwerden von Schwachstellen oder der Integration zusätzlicher betrieblicher Funktionalitäten reagieren muss, sollen weitere Sicherheitskomponenten bei der Modellierung berücksichtigt werden. Diese Komponeneten sind: a) Risikoanalyse, b) Risikomanagement und c) Penetration Testing.

2 Smart Grid Referenzmodell

Zu Beginn der Architekturentwicklung stand die Spezifizierung der zu realisierenden Use Cases gefolgt von der Definition der Anforderungen. Schließlich entstand eine Methodik zur der Architekturentwicklung, die derzeit umgesetzt wird.

Diese Methodik setzt auf den bereits existierende Standards auf, die im Kontext des Smart Grid Mandats M/490 [M4911] der Europäischen Kommission erstellt wurden. Die SGAM Referenzarchitektur ist ein wesentliches Ergebnis dieser Aktivitäten, in dem sie die Darstellung von Smart Grid Anwendungen über mehrere Abstraktions-Ebenen nach dem “Divide and Conquer” Prinzip ermöglicht.

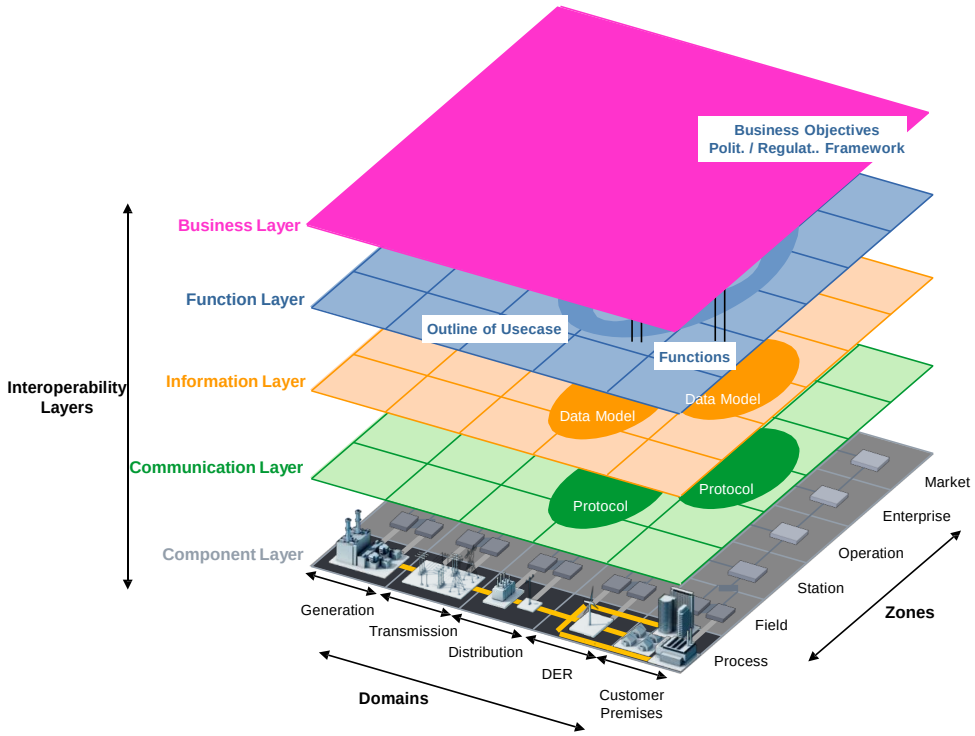

Abb. 1: Smart Grid Architecture Model (SGAM) [CENC12]

SGAM gruppiert in seiner dreidimensionale Darstellung, Funktionen in Zonen, Domänen und Interoperabilitätsebenen, wobei die Zonen das hierarchische Management von Stromnetzen re-

präsentieren (Process, Field, Station, Operation, Enterprise, Market). Die Stromverteilung ist in verschiedene Domänen unterteilt (Generation, Transmission, Distribution, Distributed Energy Resources (DER) und Customer). Die vertikalen Interoperabilitäts-Layer stellen die Kategorien dar, in denen Interoperabilität gewährleistet sein muss (Komponenten, Kommunikation, Information, Funktionalität, und Business).

Das SGAM Modell dient in erster Linie dazu, um Smart Grid Anwendungen zu strukturieren und zu visualisieren. Ziel ist es, auf möglichst viele Use Cases anwendbar zu sein, und als Leitfaden für die Identifizierung von Interoperabilitätslücken zu dienen. Es enthält keine Informationen über die eingesetzten Technologien oder Protokolle.

Die Sicherheitsanforderungen für Smart Grids wurden von der US-amerikanische NIST in der Richtlinie für Smart Grid Cybersecurity [NIST14] beschrieben. Das dort enthaltene Modell legt eine einfacher Struktur mit sieben Domänen (Transmission, Distribution, Operations, Generation, Markets, Customer, und Service Provider) zu Grunde. Anders als das SGAM Modell defniert das NIST Logical Reference Model (LRM) zudem auch 49 verschieden Akteure und logische Schnittstellen zwischen diesen Akteuren. Diese Schnittstellen werden wiederum in 22 Kategorien unterteilt, wobei für jede dieser Kategorie Sicherheitsanforderungen definiert sind.

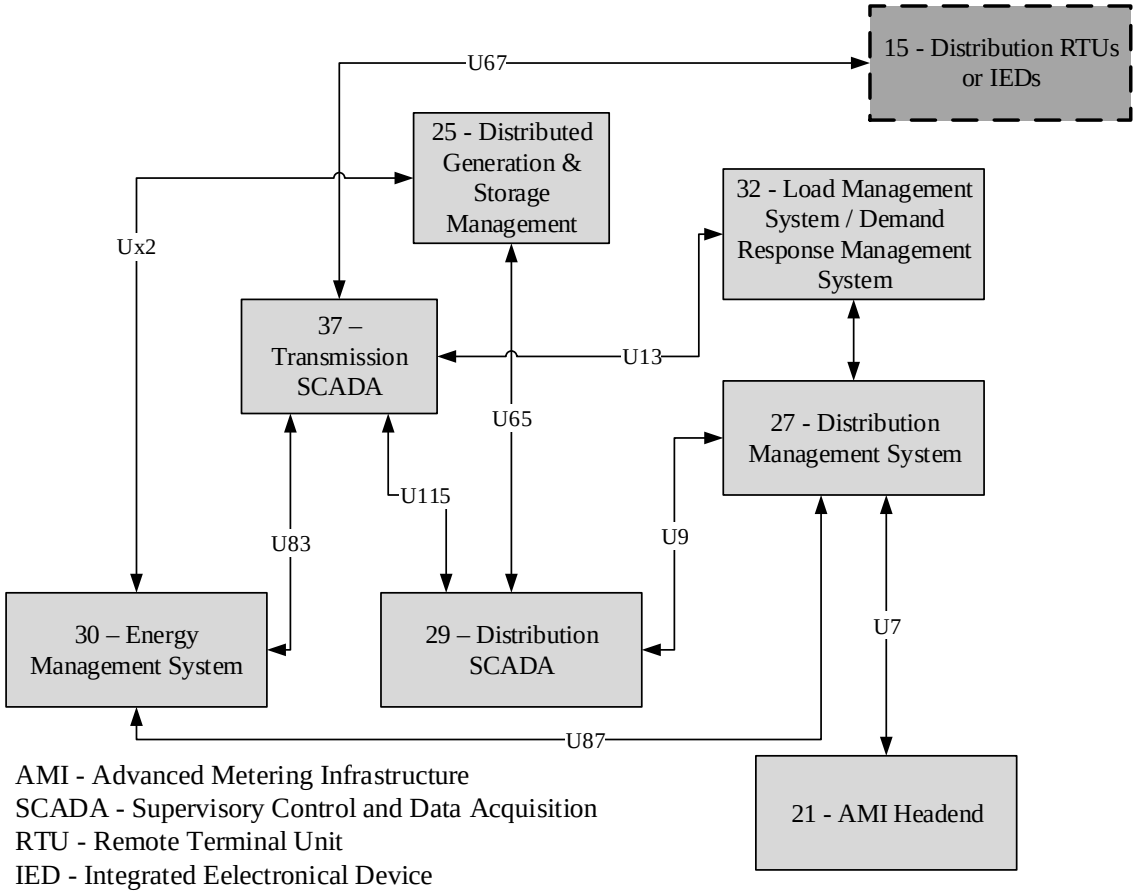

Abb. 2: Logische Schnittstellen der Kategorie 5 [NIST14]

Abbildung 2 zeigt beispielhaft die Schnittstellen der Kategorie 5. Diese Schnittstellen befinden

sich zwischen den Kontrollsystemen innerhalb einer Organisation. Diese Systeme sind durch ihre hohe Anforderungen an Verfügbarkeit und Fehlerfreiheit gekennzeichnet. Die Kommunikationskanäle sind für diese Anforderungen ausgelegt und die Umgebung, in der die Systeme betrieben werden, wird als sicher angesehen. Daraus ergeben sich nach NIST die in Tabelle 1 dargestellten Sicherheitsanforderungen.

Tab. 1: Sicherheitsanforderungen Kategorie 5

Nr.	Bezeichnung	Anforderung
SG.AC-14	Aktionen, die ohne Identifizierung und Authentisierung erlaubt sind	Die Organisation kann Aktionen definieren, die keine Identifizierung und Autenthisierung der Nutzer erfordern
SG.IA-4	Benutzer Identifizierung und Authentisierung	Das Smart Grid IT System identifiziert und authentisiert Benutzer (oder Prozesse)
SG.IA-6	Authentifikator Rückmeldung	Das IT System gibt keine Rückmeldung zu den Authentisierungsinformationen, z.B. Anzeige des Passworts bei der Eingabe
SG.SC-5	Denial of Service Schutz	Das IT System begrenzt oder schwächt die Auswirkungen von Denial of Service Angriffen ab
SG.SC-7	Perimeterschutz	Das IT System des Smart Grids überwacht und kontrolliert den Zugang an den externen Schnittstellen des Systems, z.B. durch Firewalls und Intrusion Detection Systeme
SG.SC-8	Schutz der Integrität	Das IT System schützt die Integrität von elektronisch übermittelten Informationen
SG.SC-17	Voice over IP (VoIP)	Die Organisation führt Regeln für die Verwendung von VoIP ein, basierend of der möglichen um die Beeinträchtigung des Smart Grid IT Systems durch Angriffe über VoIP
SG.SC-29	Aufteilung von Anwendungen	Managementfunktionalität wird von Beutzerfunktionalität logisch oder physich getrennt
SG.SI-7	Integrität von Software und Informationen	Das IT System überwacht und erkennt die unautorisierte Änderung von Software und Informationen

Das NIST Logical Reference Model und das SGAM Modell bilden die Grundlage für die österreichische Referenzarchitektur. In einem ersten Schritt wird eine Konsolidierung beider Modelle durchgeführt. Dazu wird den Akteure des NIST Modells die entsprechenden SGAM Zonen, Domänen und Interoperabilitätsebenen zugewiesen. Zusätzlich sollen dabei auch die Sicherheitsanforderungen der Schnittstellen berücksichtigt werden.

Im nächsten Schritt wird das nun entstandene Modell an die Gegebenheiten in Österreich angepasst. Zunächst müssen die Akteure des NIST Modells an die Akteure des Domänenmodells .AT angeglichen werden, das von Oesterreichs Energie entwickelt wurde. Das Domänenmodell .AT basiert zwar auf dem NIST Modell, die Akteure weichen jedoch von den Akteure des NIST Modells ab. So gibt es im österreichischen Modell weitere Akteure wie z.B. Regulator, Übertragungsnetzbetreiber oder Regelzonenführer. Bei der Entwicklung des Referenzmodells sind auch noch weitere Vorarbeiten wie die detaillierte Beschreibung des Smart Metering Use Case [OEn15] und der Anforderungskatalog Ende-zu-Ende Sicherheit Smart Metering [OEn14] zu berücksichtigen. Auch wenn jetzt eine neue Archtitektur entwickelt wird, so sollte sie trotzdem zu bereits existierenden Lösungen kompatibel sein.

Das Referenzmodell wird zunächst nur eine funktionale Beschreibung der Schnittstellen, Akteure und der Sicherheitsanforderungen beinhalte. Für ausgesuchte Use Cases, die unter Zuhilfenahme der Referenzarchitektur implementiert werden, ist eine konkrete Definition von Protokollen und er Parametrisierung geplant. Geeignete Sicherheitsmechanismen und -protokolle werden beispielsweise durch die Standards der Reihe IEC 62351 [Clev12] beschrieben.

3 Modellkomponenten

Die Referenzarchitektur wird mit Hilfe der SGAM Toolbox entwickelt. Es entsteht dadurch eine digitales Modell der Architektur, dass es ermöglicht, weitere Komponenten zu verknüpfen bzw. im digitalen Modell zu hinterlegen. Neben der eigentlichen Architektur werden das insbesondere sicherheitsrelevante Komponenten wie die Risikoanalyse, Risikomanagement und Penetration Testing sein.

3.1 Risikoanalyse

Im Rahmen des Projektes Smart Grid Security Guidance $(SG)^2$ wurden Smart Grid-Technologien bereits in Bezug auf Sicherheitsaspekte und Schutzmaßnahmen vor Cyber-Attacken untersucht. Aufbauend auf einer fundierten Bedrohungs- und Risikoanalyse von Smart Grid-Komponenten wurden entsprechende Sicherheitsmaßnahmen für Stromnetzbetreiber abgeleitet. Die Ergebnisse von $(SG)^2$ sollen in den Entwurf für die Referenzarchitektur mit einfließen.

Für die Risikoanalyse verfolgte $(SG)^2$ einen architektur-getriebenen Ansatz, um einen Sammlung der vorhanden Risiken zu erstellen. Als Grundlage für die Risikoanalyse diente eine kumulative Architektur, die eine Zusammenfassung der Architekturen aus verschiedenen nationalen und internationalen Smart Grid Projekten [KLSK$^+$14] darstellt. Sie diente als Basis der nachfolgenden Risikoanalyse, in deren Verlauf ein umfassender Katalog der IKT-bezogenen Risiken für Smart Grids aus Sicht eines Verteilnetzbetreibers entstanden ist. Die Vorgehensweise war dabei wir folgt:

1. Erstellung eines Bedrohungskatalogs für Smart Grids
2. Entwicklung einer Bedrohungsmatrix, die relevante Bedrohungen für die Komponenten der Architektur festhält
3. Bewertung der Risikopotentials für jedes Element der Matrix durch Abschätzung von Wahrscheinlichkeit und Auswirkungen eines Angriffs

Der Risikokatalog, der mit Hilfe dieses Ansatzes entwickelt wurde, soll im digitalen Modell der Referenzarchitektur auf Basis der SGAM Toolbox abgebildet werden. Dem Nutzer wird dadurch ein Werkzeug zur Verfügung gestellt, dass eine Risikoabschätzung für die Komponenten und Schnittstellen erlaubt. Aufbauend auf die Risikoabschätzung können einerseits geeignete Maßnahmen wie z.B. Penetration Testing empfohlen werden und anderseits finden diese Abschätzung Verwendung im Risikomanagement.

3.2 Risikomanagement

Um das nachhaltige Risikomanagement innerhalb der Smart Grid Infrastruktur zu ermöglichen, wird basierend auf existierenden SGAM Modellen sowie auf Basis der $(SG)^2$ Ergebnisse das Risiko der einzelnen Smart Grid Komponenten abgeschätzt, um entsprechende Gegenmaßnahmen unter Berücksichtigung vorhandener Kostenbeschränkungen und gewünschter Mindest-Risiko-Level zu identifizieren.

Die Basis für das integrierte Risikomanagement bildet die Security Ontology [FeEk09] welche sowohl grundlegende Beziehungen zwischen Bedrohungen, Schwachstellen und Gegenmaßnahmen als auch deren konkrete Ausprägungen in einer formalisierten Form (W3C OWL) abbildet. Die Security Ontology ist mit mehreren hundert Konzepten die größte öffentlich zugängliche Ontologie im IT Sicherheitsbereich und kann unter http://sec.sba-research.org/ eingesehen werden. In Instanziierungen der Ontologie wird neben dem IT Sicherheitswissen (Bedrohungen, Schwachstellen und Gegenmaßnahmen) auch die konkrete organisatorische und technische Infrastruktur der Organisation bzw. des betrachteten Systems formal abgebildet. Dies beinhaltet unter anderem: (i) zu schützende Assets wie z.B. Daten und IT Systeme, (ii) existierende Gegenmaßnahmen wie z.B. Policies, Zutrittskontrollsysteme, Malware Scanner, Brandlöschsysteme, etc., und (iii) die räumliche, organisatorische und virtuelle Zuordnung von Assets und Gegenmaßnahmen. Diese formale Abbildung der Zuordnung ermöglicht Reasoning Engines automatisierte Aussagen über den Wirkungsbereich einzelner Gegenmaßnahmen zu treffen.

Beispiel: das Control 'Brandmeldeanalagen in Serverräumen' erfordert in jedem Serverraum ein Brandmeldesystem. Ein Raum wird innerhalb der Security Ontology automatisch als Serverraum klassifiziert sobald sich Assets des Typs Server innerhalb des Raums befinden. Das Risiko der im Raum befindlichen Server kann folglich durch die Installation von Brandmeldeanlagen gesenkt werden. Dabei muss jedoch nicht für jeden Server einzeln angegeben werden ob eine Brandmeldeanlage vorhanden ist, es genügt die Modellierung dass eine Brandmeldeanlage im Raum präsent ist. Die Interpretation für welche Controls durch die Installation der Meldeanlage erfüllt sind und welche Assets dadurch aktiv geschützt werden erfolgt automatisiert durch die in der Security Ontology abgebildeten Regeln.

Die Security Ontology wird in einem ersten Schritt basierend auf den $(SG)^2$ Ergebnissen um ausgewählte Smart-Grid-spezifische Bedrohungen, Schwachstellen und Gegenmaßnahmen erweitert. In einem zweiten Schritt werden Methoden entwickelt welche es ermöglichen die Assets einer konkreten Smart Grid Infrastruktur auf Basis vorhandener SGAM Modelle in die Security Ontology und das damit verbundene Risikomanagementwerkzeug AURUM [1] zu laden. Ziel ist es den Modellierungs- und Setupaufwand für das Risikomanagement durch die Verwendung bereits vorhandener SGAM Modelle minimal zu halten und dem Nutzer eventuell vorhandene Schwachstellen aufzuzeigen und entsprechende Gegenmaßnahmen vorzuschlagen. Der Fokus der Forschung liegt auf der Erarbeitung und Erprobung semantischer Risikomanagementmethoden. Eine explizite Toolentwicklung für den innerhalb der kritischen Infrastrukturen angewendeten IEC 62443 Zertifizierungsstandard wird nicht angestrebt, die Forschungsergebnisse können jedoch in Teilbereichen zur Unterstützung der Zertifizierungsvorbereitungen angewendet werden.

Ergänzend zum strategischen Risikomanagement werden geeignete Penetration Testing Methoden identifiziert und testweise an Smart Grid Komponenten evaluiert. Der folgende Abschnitt beschreibt die geplanten Arbeiten im Detail.

3.3 Penetration Testing

Penetration Tests können grundsätzlich Aufschluss über die Sicherheit von Smart Grid Komponenten und die daraus resultierenden Sicherheitsrisiken geben. Je tiefer gehender die Sicher-

[1] https://www.xylem-technologies.com/de/portfolio/aurum-corporate-risk-management/

heitstests sind, desto genauer und aussagekräftiger wird auch der Einblick in die Sicherheit eines Produkts.

Aufgrund der notwendigen Analyse-Aufwände ist es praktisch jedoch nur schwer möglich auf allen Smart Grid Komponenten Sicherheitstests durchzuführen. Innerhalb der Referenzarchitektur erfolgt daher auf Basis des SGAM Modells eine initiale Risikoanalyse um besonders gefährdete Komponenten zu identifizieren und in Folge für Sicherheitstests auszuwählen. Diese Komponenten werden dann in Form einer funktionalen Teststellung mit realen Smart Grid Komponenten aufgebaut sodass auf ihnen Penetration Tests durchgeführt werden können.

Wir unterscheiden dabei zwischen Oberflächen- und Tiefenanalysen. Bei den Oberflächenanalysen werden lediglich die Kommunikationsschnittstellen und Protokolle auf ihre Sicherheit hin überprüft. Dies beinhaltet klassische Sicherheitstests wie Portscans oder das Mitschneiden von Kommunikationsverbindungen und die darauf folgende Analyse der Mitschnitte in einer Protokollanalyse Software wie Wireshark. Je nach identifizieren Services können nun Service spezifische Sicherheitsaudits durchgeführt werden (etwa Web Security Penetration Tests oder Fuzz Testing).

Die Oberflächenanalysen sind jedoch stark limitiert und können keinen Aufschluss über die (Software-) Implementierung von sicherheitskritischen Funktionen oder die genauen Auswirkungen von sicherheitskritischen Fehlern geben. Wird etwa bei einem Fuzz Test eine Schwachstelle identifiziert die auf einer Smart Grid Komponente zu einem Systembsturz führt, so kann nicht beantwortet werden wie es zu dem Fehler kommt, welche Auswirkungen er auf die Sicherheit der Komponente hat und ob er möglicherweise für weitaus schwerwiegendere Angriffe genutzt werden kann.

Um diesen Fragestellungen beantworteten zu können werden auf ausgewählten Komponenten innerhalb der Teststellung Tiefenanalysen durchgeführt. Bei den Tiefenanalysen werden Smart Grid Komponenten geöffnet und deren verbaute Hardware analysiert um in Folge die enthaltene Firmware aus den Geräten extrahieren zu können bzw. Debug-Schnittstellen wie JTAG für weiter gehendere Sicherheitstests zu identifizieren. Die extrahierte Firmware wird daraufhin disassembliert und mit statischer Codeanalyse und Reverse Engineering von sicherheitskritischen Funktionen auf Sicherheitslücken hin überprüft.

Je nach Gerätekonfiguration können zudem auch dynamische Codeanalyse-Verfahren zum Einsatz kommen um etwa mittels Fuzz Testing identifizierte Fehler genauer auf ihre Anwendbarkeit für konkrete Angriffe zu analysieren. Im Vergleich zu Oberflächentests erfordern Tiefenanalysen den Einsatz von spezialisierten Gerätschaften die üblicherweise in einem Hardware Security Labor vorhanden sind.

Trotz des Mehraufwandes sind Tiefenanalysen aufgrund der Abdeckung, der starken Aussagekraft und den präzisen Ergebnissen der alleinigen Anwendung von stark limitierten Oberflächenanalysen vorzuziehen. Nur die Durchführung von Tiefenanalysen erlaubt es auch einen echten Einblick in die Implementierungssicherheit der Smart Grid Komponente zu erlangen. Identifizierte Schwachstellen können so effektiv erkannt und in weiterer Folge entweder vermieden oder mit Hilfe der Herstellers behoben werden.

4 Use Cases

Zur Unterstützung des Modellierungsprozesses sind in Interviews mit den beteiligten Netzbetreibern High Level Use Cases definiert worden. Diese Use Cases dienen nicht nur als Basis für

die Modellierung, sondern im Weiteren sollen ausgesuchte High Level Use Cases unter Zuhilfename der Rezerentsarchitektur prototypisch implementiert werden. Die Use Cases verteilen sich über verschiedene Domänen des Smart Grids und sind angelehnt an die Use Case Sceanrios, die in NIST 7628 [NIST14] definiert sind. Sie können einer der nachfolgenden Kategorien zugeordnet werden.

- Verteilnetzbetrieb und -automatisierung
  - Überwachung
  - Steuerung
  - Firmware Update
- Advanced Metering Infrastructure
  - Use Cases von Österreichs Energie [OEn15]
  - Fernauslesen von Zählerdaten
  - Update Zählerfirmware
- Customer Premises
  - Flexibilisierung von Lasten
  - Ladestationen für Elektrofahrzeuge

Mit den gewählten Use Cases werden verschiedene Domänen des Smart Grids mit unterschiedliche Anforderungen an die Sicherheit abgedeckt. Nach der erfolgter prototypischer Umsetzung der Use Cases soll mit Hilfe des Penetration Testing die Implementierung auf Schwachstellen hin überprüft werden.

5 Zusammenfassung und Ausblick

Wir haben die Schritte beschrieben, die für die Entwicklung der österreichischen Referenzarchitektur für sicher Smart Grids vollzogen werden. Die Referenzarchitektur baut auf existierende internationale Standards und Richtlinien auf, berücksichtigt aber auch die nationale Vorgaben. Durch Verwendung der SGAM Toolbox wird sie auch in digitaler Form vorliegen wodurch der Datenaustausch mit anderen Tools wie beispielsweise AURUM ermöglicht wird. Die Architektur wird durch Komponenten erweitert, die nicht nur die Entwicklung von sicherer Systeme ermöglichen und unterstützen. Risikoanalyse und Risikomanagement helfen dabei, konkrete Maßnahmen gegen Bedrohungen zu identifizieren und Aussagen über deren Wirkungsbereich zu treffen. Das Penetration Testing hilft wiederum dabei, mögliche Schwachstellen der Implementierung zu identifizieren.

Die österreichische Referenzarchitektur soll die Interoperabilität von Smart Grid Technologie verschiedener Hersteller ermöglichen und somit in Österreich einen einheitlichen Markt für diese Technologien schaffen. Da neben den nationalen auch die internationale Vorgaben berücksichtigt werden, hat sie das Potential, österreichischen Unternehmen einen Wettbewerbsvorteil zu verschaffen. Durch die Einbindung wichtiger Akteure und Interessengruppen in Österreich ist zudem die Grundlage dafür geschaffen, zukünftig Smart Grid Lösungen auf Basis der Referenzarchitektur am Markt einzuführen.

Literatur

[CENC12] CEN-CENELEC-ETSI: Smart Grid Reference Architecture (2012).

[Clev12] F. Cleveland: IEC 62351 Security Standards for Power System Information Infrastructure (2012).

[FeEk09] S. Fenz, A. Ekelhart: Formalizing Information Security Knowledge. *In: Proceedings of the 4th ACM Symposium on Information, Computer, and Communications Security*, ACM, New York, NY, USA (2009), 183–194, 978-1-60558-394-5.

[KLSK+14] M. Kammerstetter, L. Langer, F. Skopik, F. Kupzog, W. Kastner: Practical Risk Assessment Using a Cumulative Smart Grid Model. *In: SMARTGREENS* (2014), 31–42.

[M4911] European Commission: Smart Grid Mandate. ftp://ftp.cencenelec.eu/CENELEC/Smartgrid/M490.pdf (2011).

[MBLL+16] M. Meisel, A. Berger, L. Langer, M. Litzlbauer, G. Kienesberger: The RASSA Initiative–Defining a Reference Architecture for Secure Smart Grids in Austria. *In: Energy Informatics: 4th D-A-CH Conference, EI 2015, Karlsruhe, Germany, November 12-13, 2015, Proceedings*, Springer (2016), Bd. 9424, 51.

[NIST14] NIST: NIST IR 7628 - Guidelines for Smart Grid Cyber Security - Volume 1 - Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements (2014).

[OEn14] Oesterreichs Energie Anforderungskatalog Ende-zu-Ende Sicherheit Smart Metering (2014).

[OEn15] Oesterreichs Energie Smart Metering Use-Cases (2015).

[SGA14] SGAM Toolbox. http://www.en-trust.at/downloads/sgam-toolbox/ (2014).