FAKULTÄT FÜR !NFORMATIK
Faculty of Informatics

# Modellierung komplexer Smart-Grid-Lösungen mittels der Referenzarchitektur RASSA

DIPLOMARBEIT

zur Erlangung des akademischen Grades

**Diplom-Ingenieur**

im Rahmen des Studiums

**Media and Human-Centered Computing**

eingereicht von

**Stefan Christian Wilker, B.Eng.**
Matrikelnummer 00920293

an der Fakultät für Informatik

der Technischen Universität Wien

Betreuung: Univ.Prof. Dipl.-Ing. Dr.techn. Hermann Kaindl
Mitwirkung: Univ.Ass. Dipl.-Ing. Marcus Meisel, Bakk.techn.

Wien, 23. Jänner 2019

| Stefan Christian Wilker | Hermann Kaindl |
|---|---|

FAKULTÄT
FÜR !NFORMATIK
Faculty of Informatics

# Modeling Complex Smart Grid Solutions Using the Reference Architecture RASSA

DIPLOMA THESIS

submitted in partial fulfillment of the requirements for the degree of

**Diplom-Ingenieur**

in

**Media and Human-Centered Computing**

by

**Stefan Christian Wilker, B.Eng.**
Registration Number 00920293

to the Faculty of Informatics

at the TU Wien

Advisor: Univ.Prof. Dipl.-Ing. Dr.techn. Hermann Kaindl
Assistance: Univ.Ass. Dipl.-Ing. Marcus Meisel, Bakk.techn.

Vienna, 23rd January, 2019

| Stefan Christian Wilker | Hermann Kaindl |
|---|---|

# Erklärung zur Verfassung der Arbeit

Stefan Christian Wilker, B.Eng.

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Wien, 23. Jänner 2019

Stefan Christian Wilker

# Danksagung

An erster Stelle möchte ich mich herzlichst bei Univ.Prof. Dipl.-Ing. Dr.techn. Hermann Kaindl bedanken, der mir das Einreichen und den Abschluss der Diplomarbeit am Institut für Computertechnik möglich gemacht hat. Das wertvolle und schnelle Feedback über mehrere Iterationen hinweg war ein großes Erfolgskriterium im Entstehungsprozess dieser Arbeit.

Weiters möchte ich mich bei Univ.Ass. Dipl.-Ing. Marcus Meisel, Bakk.techn. herzlichst bedanken für seine Kompetenz als Leiter der Energy&IT Group und den zahlreichen fachlichen Diskussionen und Herausforderungen, mit denen ich in die Domäne der Smart Grids hineinwachsen konnte. Für die Möglichkeit des Besuchs von mehreren Konferenzen, Präsentationen oder Workshops bin ich sehr dankbar, in welchen ich mein Wissen fachlich diskutieren oder neues Wissen in kürzester Zeit von Expert_innen erwerben konnte.

Großer Dank gebührt meinen Eltern, Sandra und Frank Wilker, die mich während meiner Studienzeit und auch zuvor schon bei meinen Entscheidungen unterstützt haben. Durch den frühen Zugang zu meinem ersten eigenen Computer war die Studienrichtung und Wissensdurst für Informatik schon von klein auf naheliegend. Ohne euch, eure Liebe und Unterstützung wäre ich nicht wo ich heute bin.

Meine restliche Familie verdient mindestens genauso viel Dank, die mich mit Motivation, Zuspruch und Liebe durch mein bisheriges Leben begleitet haben.

Ein herzlicher Dank geht an Mag.[a] Sabrina Zandl und Nadine Zandl. Das unkomplizierte und familiäre Zusammenleben mit euch war ein wichtiger Anker in den ereignisreichen Jahren meiner Studienzeit in Wien.

Vielen Dank, Manuel Schrempf B.Eng., für die fachlichen Diskussionen und der teilweise gemeinsamen Bestreitung des Bachelor- und Masterstudiums.

Großer Dank geht auch an meine langjährigen Freunde und Freundinnen. Eure Gesellschaft und der Austausch mit euren Erfahrungen half mir, die Herausforderungen des Lebens zu meistern und notwendigen Ruhezeiten zu genießen.

# Kurzfassung

Das europäische Stromnetz steht durch den massiven Zuwachs von erneuerbaren Energiequellen vor immer größeren Herausforderungen. Um weiterhin eine sichere und stabile Stromversorgung in Europa zu garantieren, muss das Stromnetz durch den Ausbau der bestehenden Infrastruktur verstärkt oder die Belastung durch intelligente Steuerung von Verbrauchern und Erzeugern verteilt werden. Für eine intelligente Steuerung sind neue Komponenten notwendig, die über bestehende oder neue Kommunikationsformen miteinander kommunizieren, zugleich aber eine breitere Angriffsfläche und damit ein höheres Risiko für Sabotage oder kriminelle Aktivitäten darstellen. Durch die Modellierung und Verwendung einer Referenzarchitektur, die auf nationalen und internationalen Standards beruht, können neue Systeme, Komponenten und deren Schnittstellen interoperabel und sicher (im Sinne von *secure*) in die bestehende Infrastruktur eingeführt werden.

Diese Diplomarbeit beantwortet für das Themengebiet der intelligenten Stromnetze die Frage, wie komplexe Smart-Grid-Lösungen für ein gemeinsames Verständnis modelliert werden können. Darüber hinaus wird die Frage beantwortet, ob die in Österreich geschaffene Referenzarchitektur geeignet ist, Sicherheitsstandards für neu entwickelte Komponenten abzuleiten und für verschiedene Interessensgruppen einsehbar zu machen.

Die in dieser Arbeit präsentierte Herangehensweise erfordert eine abstrakte Abbildung der Realität, da es im Stromnetz zu viele Komponenten und Teilsysteme sowie auch (sicherheitstechnische) Vorgaben gibt. Für einzelne Personen ist das Zusammenspiel nur schwer zu überblicken. Für die Schaffung eines einheitlichen Verständnisses sind Kompetenzen und Domänenwissen erforderlich, die nur in Zusammenarbeit und Abstimmung mit Netzbetreibern, Energielieferanten, Komponentenherstellern, Forschung und Politik zusammengetragen werden können. Dies konnte durch die Abhaltung von mehreren Workshops und Präsentationen der Referenzarchitektur erreicht werden, in welchen auch die Wichtigkeit eines gemeinsamen Verständnisses der Materie gefördert wurde.

Anhand realer Anwendungsfälle für die Entwicklung und Integration von neuen Smart-Grid-Komponenten wird die Referenzarchitektur hinsichtlich ihrer Tauglichkeit für bislang unbekannte Systeme und Komponenten evaluiert. Mit Hilfe der Referenzarchitektur können Nutzer_innen in wenigen Schritten Checklisten für Sicherheitsanforderungen oder eine Dokumentation des Systems erstellen sowie Risikoanalysen durchführen. Diese Funktionalitäten werden in dieser Arbeit erläutert und evaluiert.

# Abstract

The European power grid is facing increasing challenges as a result of the massive expansion of renewable energy sources. In order to continue to guarantee secure and stable electricity supply in Europe, the power grid needs to be strengthened through the reinforcement of existing infrastructure, or the load between consumers and producers has to be distributed in a smart way. Intelligent control requires new components that communicate with one another via existing or new forms of communication, but these are vulnerable against attacks and pose security risks of sabotage or criminal activity. By modeling and using a reference architecture based on national and international standards, new systems, components, and their interfaces can be interoperable and securely introduced into the existing infrastructure.

For the area of intelligent power grids, this thesis answers the question of how complex smart grid solutions can be modeled for facilitating a common understanding. In addition, the question is answered whether the created Austrian reference architecture is suitable for deriving security standards for newly developed components and for making them accessible to various stakeholders.

The approach presented in this work introduces abstract models of the real power grid and its environment. This is necessary to handle the increasing amount, variety, and complexity of new components and subsystems now posing not only security but also new cyber-security requirements which are otherwise too difficult to follow for single individuals. Creating a unified understanding requires skills and domain knowledge that can only be compiled in collaboration and coordination with network operators, energy suppliers, component manufacturers, research institutions and policymakers. This was achieved by holding several workshops and giving presentations disseminating the reference architecture. It also helped to emphasize the importance of a common understanding of the discussed subject.

Based on real use cases for the development and integration of new smart grid components, the reference architecture is evaluated for its suitability for previously unknown systems and components. Based on the reference architecture, users can create checklists for security requirements, documentation of the system, or risk analyses in a few steps. These features are explained and evaluated in this work.

# Inhaltsverzeichnis

# Abkürzungen und Akronyme

**ADM** Architecture Development Methodology

**BSI** Bundesamt für Sicherheit in der Informationstechnik

**CEMS** Customer Energy Management System (Kundenenergiemanagementsystem)

**CEN** Comité Européen de Normalisation (Europäisches Komitee für Normung)

**CENELEC** Comité Européen de Normalisation Électrotechnique (Europäische Komitee für elektrotechnische Normung)

**CIA** Confidentiality, Integrity, Availability

**DPIA** Data Protection Impact Assessment

**DSML** Domain Specific Modeling Language

**ENISA** European Union Agency for Network and Information Security (Europäische Agentur für Netz- und Informationssicherheit)

**ENTSO-E** European Network of Transmission System Operators for Electricity (Verband Europäischer Übertragungsnetzbetreiber)

**EPRI** Electric Power Research Institute

**ETSI** European Telecommunications Standards Institute (Europäisches Institut für Telekommunikationsnormen)

**GWAC** GridWise Architecture Council

**IEC** International Electrotechnical Commission

**IIC** Industrial Internet Consortium

**IIRA** Industrial Internet Reference Architecture

**IKT** Informations- und Kommunikationstechnik

**iniGrid** *Integration of Innovative Distributed Sensors and Actuators in Smart Grids* (Integration innovativer verteilter Sensoren und Aktuatoren in Smart Grids)

**LRM** Logical Reference Model

**MBE** Model Based Engineering

**MDA** Model Driven Architecture

**MDD** Model Driven Development

**MDE** Model Driven Engineering

**MSRA** Microgrid Security Reference Architecture

**NIST** National Institute of Standards and Technology

**NISTIR** National Institute of Standards and Technology Interagency Report

**RAMI 4.0** Referenzarchitektur Industrie 4.0

**RASSA** Reference Architecture for Secure Smart Grids Austria (Referenzarchitektur für sichere Smart Grids Österreich)

**SGAM** Smart Grid Architecture Model

**SGCG** Smart Grid Coordination Group

**SPARKS** Smart Grid Protection Against Cyber Attacks

**SysML** Systems Modeling Language

**TOGAF** The Open Group Architecture Framework

**TPSGA** Technologieplattform Smart Grids Austria

**TÜV** Technischer Überwachungsverein

**UCMR** Use Case Management Repository

**UML** Unified Modeling Language

**US** United States (Vereinigte Staaten)

**ZVEI** Zentralverband für Elektrotechnik- und Elektronikindustrie e.V.

KAPITEL 1

# Einleitung

Strom ist in Mitteleuropa eine rund um die Uhr verfügbare Ressource, die jeder Mensch schon von Kindestagen an zu benutzen lernt. Jedoch befindet sich das Stromnetz unter immer größeren Herausforderungen durch die massiven Zuwächse in der Anzahl erneuerbarer Energiequellen, durch energieintensive Veränderungen von gleichzeitig ladenden Elektrofahrzeugen, sowie auch dem Atom- beziehungsweise Kohleausstieg bei der Energieerzeugung. In diesem Kapitel werden die Motivation, die Problemstellung, das methodische Vorgehen sowie der Aufbau der vorliegenden Diplomarbeit beschrieben.

## 1.1 Motivation

Zu Beginn des Jahres 2018 hat sich schleichend eine Zeitverschiebung in vielen Uhren Mitteleuropas eingestellt. Die Uhren gingen bis nahezu sechs Minuten nach, wie Mitte März 2018 von dem *European Network of Transmission System Operators for Electricity (Verband Europäischer Übertragungsnetzbetreiber)* (ENTSO-E) vermeldet wurde [1]. Dies betraf Uhren, deren Zeitsynchronisierung an die Stromfrequenz gekoppelt war, wie es beispielsweise oftmals in Backofenuhren der Fall ist. Dieses Problem war nach [2] auf einen politischen Disput zwischen Serbien und dem Kosovo zurückzuführen.

Obwohl die Situation im April 2018 [3] korrigiert wurde, sind wiederkehrend zu große Abweichungen der Netzfrequenz eingetreten [2]. Ein neu initiiertes Kompensierungsprogramm der ENTSO-E [2] soll dabei helfen, einer Netzzeitabweichung von mehr als 60 Sekunden zukünftig entgegenzuwirken, sodass sich Vorfälle wie diese nicht wiederholen.

Durch dieses aktuelle Beispiel soll verdeutlicht werden, dass das europäische Stromnetz alle teilnehmenden Partner braucht, um gemeinsam für eine sichere und stabile Stromversorgung zu sorgen. Dies ist auch im Sinne des *Integration of Innovative Distributed Sensors and Actuators in Smart Grids (Integration innovativer verteilter Sensoren und Aktuatoren in Smart Grids)* (iniGrid)-Projekts [4], an welchem ich mitgearbeitet habe und

mir so ein Verständnis über die derzeitige Lage des Stromnetzes in Österreich verschaffte. Die Vielseitigkeit der Neuerungen und Neuentwicklungen (Mittelspannungssensoren und sogenannte „Smart Breaker“) erforderten entsprechende Softwarelösungen, die verlässlich mit erhaltenden Messwerten umgehen können und so während eines Feldtests in einem Museum in Niederösterreich auch Teile des Gebäudes „intelligent“ gesteuert haben. Schnell war in diesem Projekt klar, dass viele unterschiedliche Domänen involviert sind und miteinander auf verschiedenen Ebenen kommunizieren müssen.

Dies spricht die Ziele der *Reference Architecture for Secure Smart Grids Austria (Referenzarchitektur für sichere Smart Grids Österreich)* (RASSA)-Initiative an. Im RASSA-Architektur Projekt konnte ich mir durch meine Tätigkeit Wissen darüber aneignen, wie komplex die regulatorischen Richtlinien sind. Herausforderungen gab es durch die Anpassungen und Übertragung von Modellen an einen EU-Mitgliedsstaat und dessen Markt (in diesem Fall Österreich). Die Kommunikation mit anderen Domänen war ein zusätzliches Erschwernis.

Im Bereich der Stromnetze gilt es, mit langjährigen eingefahrenen Benutzerverhalten umzugehen und an den richtigen Punkten anzusetzen, um ein Umdenken in den Konsument_innen oder Endanwender_innen aber auch bei den Netzbetreibern und Regulatoren hervorzurufen. In dieser Arbeit ist daher die Nützlichkeit ein Thema, da die Kommunikation von Use Cases über verschiedene Domänen hinweg viele Expertinnen und Experten involviert und der Umgang mit einem Tool eine flache Lernkurve benötigt. Dies liegt vor allem daran, dass die Arbeitslast meist schon hoch ist und ein Erlernen neuer Expertisen für jede/n der teilnehmenden Gesprächspartner_innen in den Stakeholdertreffen nur schwer in den Arbeitsalltag integrierbar ist. So wäre es ideal, möglichst viele Informationen bereits auch als Einsteiger_in aus einer Software bekommen zu können. Der notwendige Aufwand für die Informationsbeschaffung sollte mit relativ geringem Arbeitsaufwand für die jeweiligen Nutzerinnen und Nutzer durchgeführt werden können.

## 1.2 Problembeschreibung

Die aktuelle Stromnetz-Infrastruktur eignet sich nur bedingt zur Erreichung der Klimaziele der Europäischen Mitgliedsstaaten, da sie sich schon jetzt öfters am Rande der möglichen Kapazitäten befindet. Das Netz muss intelligent entlastet werden, um einen teuren Ausbau der Infrastruktur zu vermeiden. Daher beschäftigten sich viele aktuelle Forschungsprojekte mit der Entwicklung von neuartigen Sensoren und Aktuatoren (fernschaltbare Stromsicherungen) für das Stromnetz, um dieses intelligenter gestalten zu können. Dadurch werden neue Anwendungen ermöglicht, wie das Erfassen der Netzauslastung für das intelligente Ab- oder Zuschalten von Lasten und Energiespeichern.

Durch entsprechenden Einsatz von Ressourcen und (Arbeits-)Zeit lassen sich die Entwicklungen, welche für die Umsetzung der Use Cases notwendig sind, lassen sich auf technischer Ebene lösen. Allerdings ist die Kommunikation mit anderen involvierten Domänen bei der Integration solcher Lösungen oft die größte Hürde. Dies stellt vor allem ein Problem dar, wenn neue, teils sicherheitskritische Komponenten auf den Markt kommen. Das Ziel der

Diplomarbeit ist es, firmenspezifische Komponenten oder Anpassungen und die daraus resultierenden Sicherheitsanforderungen (im Sinne von Security Requirements) auf Basis eines gemeinsamen Verständnisses an verschiedene Partner_innen und Expert_innen von unterschiedlichen Domänen kommunizieren zu können.

Ein Vorschlag für eine Standardisierung wurde innerhalb der aktuellen RASSA-Initiative [5] erarbeitet, indem internationale Standards für den Österreichischen Markt angepasst wurden. Als Grundgerüst dient das *Smart Grid Architecture Model* (SGAM) [6]. Die vorliegenden *Unified Modeling Language* (UML) Modelle aus RASSA sollen den ersten Schritt für ein gemeinsames Verständnis auf europäischer Ebene setzen. Denn es ist eine der großen Herausforderungen, dass verschiedene Abstraktionsebenen zu der selben geplanten Lösung gleich verstanden werden müssen. Das SGAM definiert solche Ebenen und ermöglicht mit Software die Kollaboration zwischen verschiedenen Partnern. So gilt es für ein und denselben Gerätetyp Profile für Schnittstellen und Security Requirements einheitlich zu definieren, zu standardisieren und zu etablieren. Nach dieser Festlegung müssen die Informationen in geeigneter Weise für Endanwenderinnen und Endanwender mit verschiedenem (technischen) Hintergrund nachvollziehbar dargestellt werden, um die große Anzahl von Security Requirements und sonstigen Anforderungen bewältigen zu können. Dadurch soll erreicht oder zumindest unterstützend erwirkt werden, dass das europäische Stromnetz nicht durch die Einführung von neuen intelligenten Geräten als leichtes Ziel von etwaigen Sabotage- oder Terroraktionen angegriffen werden kann.

Für die Umsetzung werden in dieser Arbeit Use Cases aus dem Forschungsprojekt iniGrid [4] als Basis genutzt, die sich mit der Integration von neuen intelligenten Komponenten im Stromnetz beschäftigen. Ein Use Case aus dem iniGrid Projekt wurde einem Sicherheitstest unterzogen, allerdings eröffnen die weiteren Use Cases noch mehr mögliche Schwachstellen aufgrund der eingesetzten Sensoren, Aktuatoren und Komponenten. Durch die Abbildung der Use Cases innerhalb einer standardisierten Referenzarchitektur versucht diese Arbeit zusätzliche Sicherheitsanforderungen zu erheben, die während des Projekts nicht näher betrachtet wurden. Folgende Fragestellungen wurden im Rahmen beantwortet:

- Wie kann der Transfer von vorhandenen Use Cases am Beispiel von Sensoren und Aktuatoren in eine Referenzarchitektur mit der SGAM-Toolbox stattfinden?
- Wie können sich die Darstellung und Modellierung von Smart-Grid-Anwendungsfällen, auf andere Konzepte übertragen lassen (zum Beispiel unternehmensspezifische Anforderungen, Lösungen)?
- Wie wird der Export von Use Cases oder herstellerspezifischen Anforderungslisten adaptiert und generiert?
- Wie können neue Anforderungen an Akteure oder Geräte (wie beispielsweise gesetzliche Bestimmungen oder zum Schließen von Sicherheitslücken) mit geringem Aufwand beziehungsweise Vorwissen eingearbeitet werden?

- Welche Stärken und Schwächen haben bestehende Softwarelösungen? Welche Funktionen sollen für weiterführende Entwicklungen berücksichtigt werden?
- Welche Lehren können aus anderen Domänen gezogen werden?
- Welche Funktionen fehlen für den breiten Einsatz in der Industrie?
- Welche Informationen, Kataloge oder Standards sollen integriert werden?
- Welche Informationen, Funktionen oder Materialien (wie beispielsweise Handbücher) benötigen zukünftige Anwenderinnen und Anwender, um effizient mit den Tools arbeiten zu können?

## 1.3 Ergebnisse

Die Arbeit fasst zunächst die wesentlichen Erkenntnisse für die Systemmodellierung im Smart Grid anhand des SGAM zusammen und hebt die wichtigsten Punkte hervor. Es werden verschiedene Modelle und Konzepte auf nationaler und internationaler Ebene vorgestellt.

Ein Transfer eines demonstrativen Use Case aus dem Projekt iniGrid [4] in die Referenzarchitektur nach der RASSA-Initiative [5] wurde durchgeführt. Damit einhergehende zusätzliche Möglichkeiten werden diskutiert. Dabei handelt es sich um einen Use Case zur Integration von innovativen verteilten Sensoren und Aktuatoren in das Smart Grid. Bestehende Modelle wurden um die notwendigen, oft neuen Akteure erweitert.

Es werden offene Punkte der RASSA-Initiative angesprochen, welche die Anwendbarkeit von firmenspezifischen Verwendungszwecken betreffen. Die Use Cases aus iniGrid können solche Zwecke ebenso darstellen, indem einzelne Lösungen (hier die Komponenten innerhalb der Use Cases) auf Herstellerebene individuell abgebildet werden können. Ein erarbeiteter individualisierter Export von Security Requirements aus den modellierten Use Cases bieten einen großen potentiellen Mehrwert für die Wirtschaft.

Die Use-Case-Komponenten wurden innerhalb der Referenzarchitektur mit Informationen der Standardisierung verknüpft. So wurden Use-Case-spezifische Security Requirements abgeleitet und aufgelistet. Die Basis hierfür wurde durch Schnittstellen erhoben, wie sie durch das *National Institute of Standards and Technology* (NIST) *Logical Reference Model* (LRM) [7] aufgrund der Art der Komponenten (Sensor, Meter, Aktuator, etc.) definiert wurden. RASSA bietet hierzu die Ausgangsbasis, da im Zuge des Projekts die Informationen von [7] digitalisiert wurden, wie in Abbildung 1.1 beispielhaft zu sehen ist. Die Grafik zeigt eine Auflistung der Schnittstellen und einen Verweis auf die ableitbaren Security Requirements die als Ordner-Element im Diagramm dargestellt sind. In diesem Ordner befindet sich ein weiteres Diagramm mit den Security Requirements, wie in 3.3.3 näher erläutert ist. Jedoch benötigen Entwickler_innen oder Prüfer_innen eine übersichtlichere Darstellung wie beispielsweise eine tabellarische Auflistung der Anforderungen, um effizient arbeiten zu können. Eine solche Darstellung der Use Cases zur Integration von Sensoren und Aktuatoren wurde im Zuge der Diplomarbeit erarbeitet.

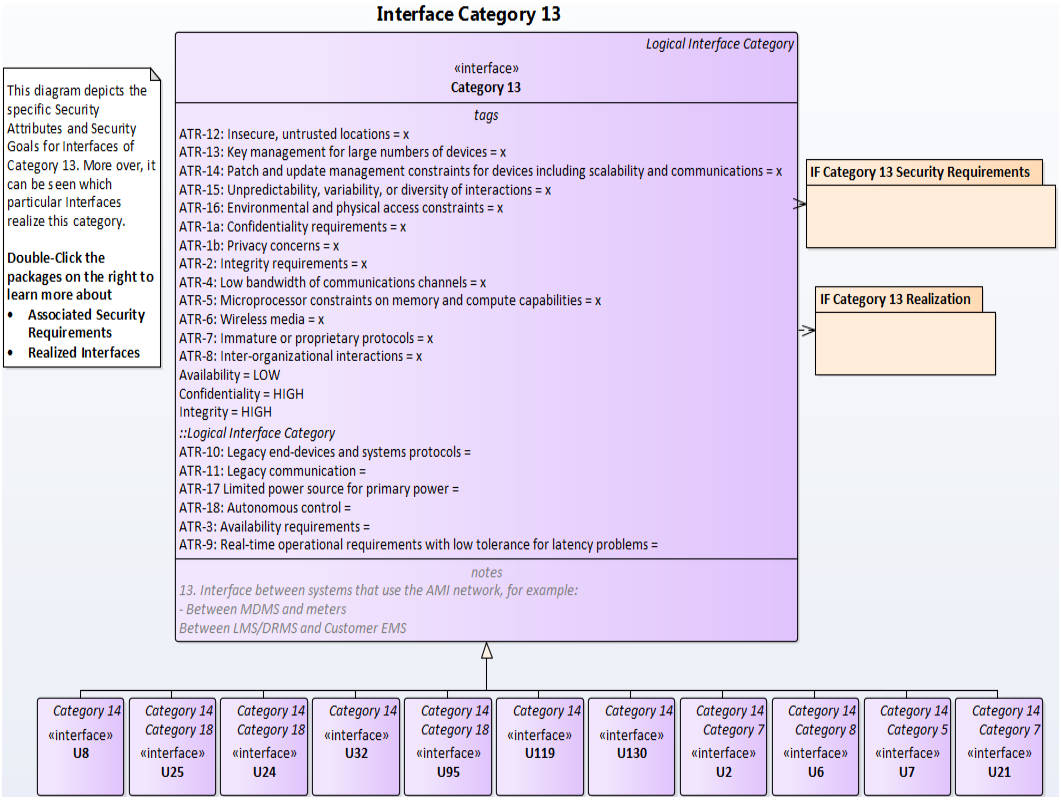



Abbildung 1.1: Modellierte Informationen für Schnittstellen der „Category 13“ des NIST LRM

Als Ergebnis eines Stakeholder-Treffens konnte die Richtigkeit und der Mehrgewinn der gewonnenen Daten aus den Use-Case-Exports und der Herangehensweise mittels der Referenzarchitektur bestätigt werden. Zusätzlich erlangte Ergebnisse von mehreren Abstimmungstreffen und Ergebnisvorstellungen sind für die zukünftige Weiterentwicklung in Hinsicht auf die Stärken, Schwächen oder fehlende Informationen besonders wertvoll.

## 1.4 Methodisches Vorgehen

Um die erwarteten Resultate der Diplomarbeit zu erreichen, wurden die nachfolgenden Bereiche ausgearbeitet:

- Eine ausführliche Erarbeitung von aktuellen Forschungsergebnissen und Umsetzungen wurden in Literatur und Publikationen zum Thema Referenzarchitekturen im Bereich Smart Grids gesucht und identifiziert. Die erarbeiteten Erkenntnisse geben weiterführende Anhaltspunkte bei der Umsetzung für die Modellierung von Use Cases. Grundbegriffe aus dem Smart-Grid-Bereich wurden abgegrenzt und erläutert, um Unklarheiten mit anderen Domänen auszuschließen.

- Für den Entwurf von Use Cases mit Hilfe von Tools wurden die Grundlagen der SGAM-Modellierung mittels UML erörtert. Es ist notwendig, die Modellierung der verschiedenen Schichten des SGAM zu beschreiben, sodass die Resultate der Modellierung nachvollziehbar sind. Sowohl Vorteile als auch Nachteile wurden erörtert. Dies beinhaltet die Verwendung des entworfenen Use Case für etwaige sicherheitsrelevante Abschätzungen mittels Analysetools sowie auch Funktionen, die innerhalb des verwendeten *Enterprise Architect* Tools zur Verfügung stehen. Die Informationsextrahierung und Repräsentation des modellierten Use Case wurden auf vordefinierte Zwecke abgestimmt und erarbeitet. Dies beinhaltet eine übersichtliche Auflistung von Security Requirements, die anhand des modellierten Use Case abgeleitet wurden und einen großen Nutzen für zukünftige Anwenderinnen und Anwender darstellen.

- Es wurde die Modellierung der iniGrid Use Cases innerhalb der Referenzarchitektur durchgeführt. Anhand eines repräsentativen Use Cases wurden die Schwächen und Herausforderung einer bestehenden Modellierung aufgezeigt und anschließend in die Referenzarchitektur überführt. Die Darstellung des Use Case in UML wurde entsprechend der Ergebnisse aus NIST LRM und RASSA für das SGAM angepasst.

- Analysetools wie das *Data Protection Impact Assessment* (DPIA)-Tool und das AURUM-Tool werden vorgestellt. Die hinterlegten Informationen eines Modells können verwendet werden, um etwa Evaluierungen und die Erstellung von Auswertungen durchführen zu können. Darüber hinaus werden Tools zum Entwurf von Use Cases präsentiert und analysiert. Diesbezüglich wird auf verwandte Arbeiten, die sich speziell mit den angeführten Tools auseinandersetzen, eingegangen.

- Um die Annahmen über den potenziellen Nutzen evaluieren zu können, wurden die Ergebnisse von Stakeholdertreffen erörtert. Diese fanden vor allem mit Domänenexpert_innen aus der Österreichischen Energiewirtschaft, die zugleich zukünftige Anwender_innen sein können, und mit Expertinnen und Experten aus der Domäne für Cyber-Security statt. Dabei wurden beispielhafte Use Cases auf den Ebenen des SGAM aufgezeigt und die Ergebnisse der generierten Exports für die Erhebung von Security Requirements diskutiert sowie Stärken und Schwächen aufgenommen.

## 1.5 Abgrenzung

Hier wird eine Erläuterung zur Abgrenzung der gegenständlichen Arbeit von der RASSA-Initiative und den Vorarbeiten vorgenommen. Die Grundlagen zum Stand der Technik sind ausführlich in Kapitel 2 beschrieben.

Abbildung 1.2 soll zur Abgrenzung veranschaulichen, welche Ziele während der laufenden RASSA-Initiative angestrebt werden. Dabei wurden die Ergebnisse der SGAM-Erkenntnisse (siehe 2.2.7) und die des NIST (siehe 2.2.6) konsolidiert. Unter besonderer Berücksichtigung des Bezugs zu Österreich wurde in enger Zusammenarbeit zwischen dem Institut für Computertechnik der TU Wien und dem AIT Austrian Institute of

Technology eine sogenannte Feldgeräteliste erstellt, auf deren Basis die Referenzarchitektur modelliert werden konnte. Desweiteren wurden die (vorhandenen) iniGrid Use Cases in RASSA modelliert und die Referenzarchitektur evaluiert. Anhand eines repräsentativen Beispiels konnte die Erstellung von eigenen Spezifikationen demonstriert werden. Ergebnisse beziehungsweise Modelle Dritter sind als solche gekennzeichnet.

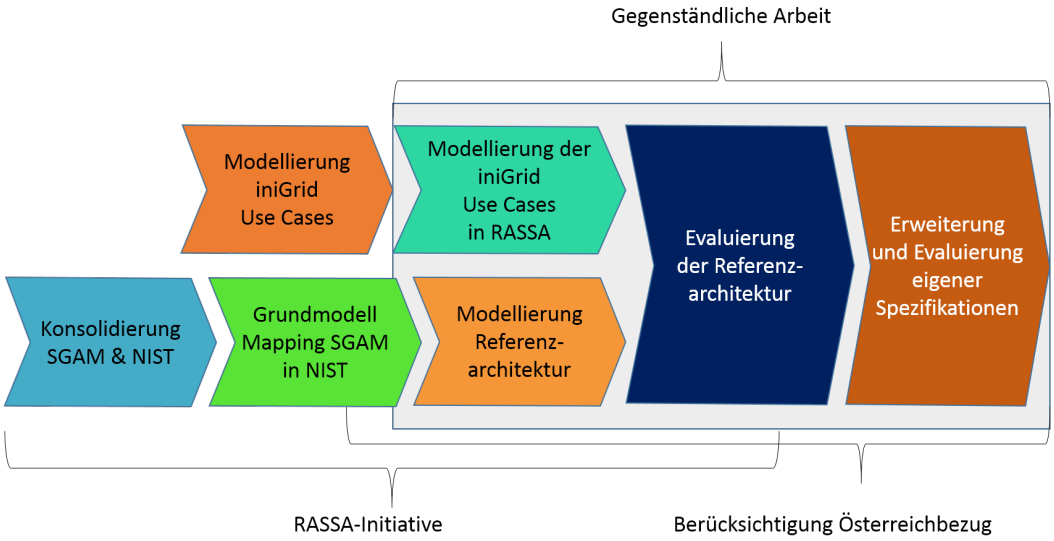



Abbildung 1.2: Eigene Darstellung zur Abgrenzung der Arbeit in Anlehnung an [8]

Die gegenständliche Arbeit beschreibt die von mir durchgeführten Modellierungen und wendet die RASSA-Methodik außerhalb des RASSA-Architektur Forschungsprojekts auf die Use Cases zur Integration von innovativen Sensoren und Aktuatoren im Smart Grid an. Dadurch wurde eine universelle Anwendbarkeit für die vorgeschlagene Herangehensweise weiter untersucht.

## 1.6 Aufbau der Arbeit

Der Stand der Technik sowie Forschung zu Modellierung und Referenzarchitekturen mit ihren Einsatzgebieten werden in Kapitel 2 beschrieben. Darüber hinaus werden dort gebräuchliche Begriffe, die für das Verständnis dieser Arbeit und den Themenbereich notwendig sind, erläutert.

Darauffolgend sind in Kapitel 3 die Herausforderungen beim Entwurf von komplexen Smart-Grid-Lösungen beschrieben, es wird auf die verwendete Modellierungssoftware eingegangen und vorhandene Konzepte und Modelle werden beschrieben. Das Kapitel schließt mit einer Beschreibung der in iniGrid entwickelten Use Cases ab und untersucht fehlende Bausteine.

In Kapitel 4 findet eine Evaluierung der modellierten Use Cases und Modelle statt. Diese wurde mit den technischen Möglichkeiten für Berichte, Analysetools und der Ergebnisse der Stakeholdertreffen durchgeführt.

In Kapitel 5 werden die Ergebnisse diskutiert. Abschließend werden in Kapitel 7 eine Zusammenfassung und ein Ausblick für weitere Forschungsprojekte gegeben.

KAPITEL 2

# Stand der Technik

Dieses Kapitel beschäftigt sich mit den Vorarbeiten und dem Schaffen eines gemeinsamen Begriffsverständnisses. Aufgrund der domänenübergreifenden Einflüsse ist eine gleiche Auffassung von Begriffen und Terminologie als überaus wichtig anzusehen.

Die Motivation dieser Arbeit liegt in der Schaffung des gemeinsamen Begriffsverständnisses. Dieses zielt auf Stakeholder aus der (Energie-) Wirtschaft ab, angefangen von der Chefetage bis hin zu den Techniker_innen, Behörden, sowie diverse Gerätehersteller mit unterschiedlichen Endprodukten und Zielgruppen.

Daher wird hier der aktuelle Stand der Technik über verfügbare Softwärelösungen beschrieben. Es werden auch englischsprachige Begriffe erläutert, wie diese im Bereich der Smart Grids und der Modellierung verstanden werden. Darüber hinaus wird auf Architekturlösungen, Referenzarchitekturen und Analysetools eingegangen, die sich mit der Beschreibung, Darstellung, Anbindung bzw. Auswertung von Smart-Grid-Modellen beschäftigen.

## 2.1 Begriffsklärung

Dieser Abschnitt dient zur Begriffsklärung von verwendeten Definitionen und Terminologie, die innerhalb dieser Arbeit verwendet werden. Dies dient vor allem dazu, auf die Anwendung und korrekte Verwendung von Modellierungsergebnissen innerhalb der Smart-Grid-Domäne besser eingehen zu können. Dieser Abschnitt umfasst die Erörterung von englischen Fachbegriffen oder Begriffen, die keine selbsterklärende Übersetzung im Deutschen besitzen.

### 2.1.1 Referenzarchitektur

Der Begriff Referenzarchitektur ist im Kontext dieser Arbeit als eine Art „Blaupause“, also einer digitalen Vorlage zu verstehen. Eine Referenzarchitektur bietet ein Regelwerk,

eine Struktur oder einen Rahmen, mit deren Hilfe sich Lösungen für unterschiedliche Probleme finden lassen. Werden dabei die Elemente und möglichen Interaktionen der Referenzarchitektur verwendet, so ist die entwickelte Lösung konform zu der verwendeten Referenzarchitektur [9].

Wenn man wie in [10] das Smart Grid mit einem weniger abstrakten Thema wie dem Bauwesen vergleicht, sind die Parallelen zur Bedeutung verständlicher, wie in Tabelle 2.1 aufgezeigt.

Tabelle 2.1: Vergleich zwischen Bauwesen und Smart Grid angelehnt an [10]

| | **Architekturbeschreibung** | | | **Architekturentwicklung** | |
|---|---|---|---|---|---|
| | *Architektur Framework* | *Architektur Modellierung / Viewpoints* | *Abstraktions-level* | *Referenzar-chitektur* | *Konkrete Architektur* |
| **Bauwesen** | Einheitliche Darstellung (z.B. *Grundriss*) | Modellierung mit CAD Werkzeugen → beliebige Ansichten | Elektro- oder Wasserinstal-lationen, o.ä. | *„Blaupause“* | Individuelles Haus |
| **Smart Grid** | Funktionale und technische Aspekte (Schichtenmo-dell) | Modellierung mit SGAM Toolbox oder anderen Tools | Elektrover-teilung, IKT Netzwerk, Security, etc. | *RASSA* | Individuelle Lösung |

Im Bauwesen hat man sich auf Begriffe wie beispielsweise *Grundriss, Vorderansicht* oder *Seitenansicht* geeinigt. Für die Verantwortlichen ist durch eine gemeinsame Sprache die Darstellungsweise klar definiert. Bei den Entwicklungen im Smart Grid hingegen ist durch die zahlreichen Entwicklungswege und Einbindung neuer Branchenzweige noch kein allgemein akzeptiertes Übereinkommen von Begriffen entstanden. Im Smart Grid wird dies zum Beispiel durch das Schaffen eines Schichtenmodells, wie es im SGAM definiert wurde, erreicht. In dem Schichtenmodell für das Smart Grid handelt es sich um die *Business*, *Function*, *Information*, *Communication* und *Component Layer*, welche näher in 2.2.7 erläutert werden.

Die verschiedenen Ansichten im Bauwesen werden durch *Computer Aided Design* (CAD) Programme geschaffen und erleichtern es den Nutzerinnen und Nutzern zwischen den unterschiedlichen Ansichten zu wechseln. Für das Smart Grid können Tools wie die SGAM Toolbox oder das DISCERN SGAM Tool verwendet werden, um Arbeiten in den verschiedenen Schichten durchführen zu können. Die SGAM Toolbox ist in 3.2.1 beschrieben. Das DISCERN-Projekt sowie das DISCERN SGAM Tool werden in 2.3.4 behandelt.

Verschiedene Abstraktionslevel sind im Bauwesen durch zusätzliche Pläne für die Elektro- oder Wasserinstallationen gegeben. Vergleichbares gibt es für das Smart Grid durch Pläne

für das Stromnetz, die *Informations- und Kommunikationstechnik* (IKT)-Netzwerk oder die *Security*. Diese können in entsprechenden Tools gefiltert angezeigt werden.

Bei der Architekturentwicklung ist laut Neureiter [10] der Begriff der Referenzarchitektur als eine *„Blaupause“* zu verstehen. Durch Vorschriften, Gesetze, Materialverhalten, Statik, etc. ergeben sich Rahmenbedingungen, die ein_e Bauträger_in für individuelle Wünsche in der konkreten Architekturumsetzung wie z.B. einem Eigenheim anpassen kann. Im Smart Grid stellt RASSA eine solche Referenzarchitektur dar, welche für die Entwicklung oder Einpflegung der individuellen Smart-Grid-Anwendungsfälle für eine konkrete Architekturlösung verwendet werden kann.

In Tabelle 2.1 sind die Parallelen von Begriffen im Bauwesen und in der Smart-Grid-Domäne aufgeführt. Doch der Begriff *Architektur* selbst benötigt noch eine genauere Ausführung für eine gemeinsame Auffassung, auf die im Folgenden eingegangen wird.

### Architektur

Architektur wird oftmals als Fachwort verwendet, allerdings wird selten auf die Bedeutung hinter dem Wort selbst eingegangen. Ein passender Vergleich zu dem, was eine Architektur leisten muss, geht auf den römischen Architekten Marcus Vitruvius Pollio zurück, der im Deutschen als *Vitruv* höhere Bekanntheit genießt. Dabei sind drei zentrale Anforderungen für eine gute Architektur relevant [11]:

- *Firmitas* (Festigkeit)
- *Utilitas* (Nützlichkeit)
- *Venustas* (Schönheit)

Wenn man diese Anforderungen in die heutige Zeit transferiert, muss eine Architektur ein durchdachtes Regelwerk zur Erstellung eines Systems bieten (Erfüllung von *Firmitas*). Weiters muss sie eine möglichst hohe Nützlichkeit offerieren, was nach [12] durch eine Reduktion der Komplexität mittels Abstraktion in eine Architektur gegeben sein soll. Die Beispiele aus Tabelle 2.1 zeigen eine derartige Abstraktion. Schönheit innerhalb einer Smart-Grid Architektur kann man auf vielen Ebenen als solche verstehen. Beispielsweise die schöne Anordnung der Symbole, die vereinfachte Abstraktion der Realität oder die Methodik, die es unterschiedenen Domänen zu kommunizieren ermöglicht kann schön sein.

In der Smart-Grid-Domäne bewegt man sich bei technischen Lösungen meist im Software-Bereich. Eine Software-Architektur enthält nach [12] systemrelevante Verbindungen zwischen den Teilen, Elementen und Komponenten für die Systementwicklung So wird geklärt, welche der Komponenten wie miteinander (direkt) verbunden sind. Dabei sind, wie auch im Bauwesen, technische Vorgaben zu erfüllen, damit das gestaltete System funktionieren kann. Doch es bleibt die Frage offen, wie solche Vorgaben abgebildet werden können. In einer Smart-Grid-Architektur kann ein Ergebnis die visuelle Darstellung von

komplexen Use Cases sein. Als Beispiel sei auf Abbildung 2.7 weiter unten verwiesen, in der eine dreidimensionale Visualisierung der Interaktion von Komponenten im SGAM dargestellt ist. Im Beispiel der Smart-Grid-Architekturen hat sich die Nutzung von komplexen Use Cases und deren visuelle Darstellung als System mit verschiedenen Sichtweisen und dazugehörigen Interaktionen als nützlich herausgestellt [13].

#### Architektur-Framework

Der Begriff *Framework* wird oft zusammen mit *Architektur* verwendet. Nach [14, S. 5] ist es das »notwendige Rahmenwerk für die Entwicklung einer Architektur«. Der Autor gibt als Beispiel das *Zachman Framework for Enterprise Architecture* an, »welches alle möglichen Aspekte beinhaltet, um die Komplexität eins [sic!] Unternehmens darstellen zu können.« [14, S. 5]. Im 2.2 wird auf bestehende Arbeiten eingegangen, welche für die Komplexität ihres jeweiligen Fachgebiets eine standardisierte Darstellung verfolgen, angefangen von Industrie 4.0 bis hin zu Smart Grids.

### 2.1.2 Domain Specific Modeling Language

Bevor die Unterscheidung von *Model Driven Architecture* und *Model Driven Engineering* diskutiert wird, muss zunächst der Begriff rund um die Modellierung und die verwendete Modellierungssprache geklärt werden. Um etwas modellieren zu können, braucht es eine Art und Weise Informationen festzuhalten, die von Stakeholdern und der Technologie „verstanden“ werden kann. Hierzu benötigt es nach [15], dass die Struktur, Begriffe, Notationen, Syntax, Semantik und Integritätsregeln der zu repräsentierenden Information für das Modell gut definiert und konsistent sind. Mit der Einhaltung und Abdeckung aller Punkte in der vorangegangenen Aufzählung kann eine Modellierungssprache definiert werden. Weit bekannte Vertreter sind zum Beispiel UML oder *Systems Modeling Language* (SysML).

Dabei gibt es zwei wesentliche Gruppen von Modellierungssprachen [15]: Die erste ist die Gruppe der *General Purpose Modeling Languages*, zu denen auch UML zählt, welche für jegliche Domäne oder Problemstellung für den Modellierungsprozess herangezogen werden kann. Die zweite Gruppe der *Domain Specific Modeling Language* (DSML) hingegen beinhaltet Sprachen, die auf eine spezielle Domäne, einem Kontext oder sogar ein Unternehmen abgestimmt wurden, um den involvierten Personen die Beschreibungsarbeit in ihrer Domäne zu erleichtern.

### 2.1.3 Model Driven Architecture und Model Driven Engineering

Neureiter [16] behandelt Ansätze für sogenannte modellgetriebene Entwicklung, bekannt als *Model Driven Engineering* (MDE). Durch die ähnlichen Abkürzungen ist im Buch von Brambilla et al. [17] daher die Rede von einem wahren Dschungel von Akronymen. Um die Bedeutungen der *modellgetriebenen Ansätze* voneinander unterscheiden zu können, soll Abbildung 2.1 zur Unterstützung dienen.


Abbildung 2.1: Eigene Darstellung von modellgetriebenen Ansätzen, angelehnt an [16, 17].

Auf der linken Seite der Abbildung 2.1 ist eine bildliche Darstellung der Beziehung der jeweiligen Ober- und Untermengen der beschriebenen *Model Based Engineering* (MBE), MDE, *Model Driven Development* (MDD) und *Model Driven Architecture* (MDA) dargestellt. Auf der rechten Seite der Abbildung befinden sich die frei übersetzten Definitionen aus dem Buch von [17]. Die Unterscheidung, ob man von MBE, MDE, MDD oder MDA spricht, hängt von der Verwendung der Modelle ab und, ob sie der hauptsächliche Treiber bei der Entwicklung sind. Auch, wie es zum Beispiel unter Zuhilfenahme von MDA der Fall ist [18], ob ein Code mehr oder weniger automatisch aus den Modellen generiert werden kann. Die Beschreibung von MDA ist in dem entsprechenden Dokument der Object Management Group [15] gegeben. Weiterführende Informationen sind zum Beispiel in den Arbeiten [19] und [20] zu finden.

### 2.1.4 Security und Safety

Die englischen Begriffe *Security* und *Safety* sind in dieser Arbeit absichtlich in ihrem englischem Original wiedergegeben. Das liegt vor allem daran, weil die erstbeste Übersetzung *Sicherheit* hierbei nur ungenügend aussagekräftig in ihrer Bedeutung ist. Daher wird in deutschen technischen Texten und im Fachjargon *Security* und *Safety* verwendet.

Beim deutschen *Technischer Überwachungsverein* (TÜV) Nord [21] wird *Security* als Kriminalprävention verstanden und *Safety* als Unfallvermeidung.

Innerhalb der RASSA-Initiative wird *Safety* als Betriebssicherheit und *Security* als Angriffssicherheit gesehen. Angriffssicherheit kann durch Kriminalprävention erreicht werden sowie durch die Aussicht auf möglichst unattraktive Belohnungen bei dem Versuch eines Einbruchs in das System. Attraktive Belohnungen könnten im Energiesektor beispielsweise

Lastprofildaten von Kunden sein, da es sich mit diesen wesentlich einfacher vorhersagen lässt, wann Personen sich in einem Haushalt aufhalten und wann nicht. Eine hohe Betriebssicherheit kann erreicht werden, wenn jegliche Unfälle vermieden werden können. In dieser Arbeit wird in weiterer Folge die Interpretation von *Security* und *Safety* aus der RASSA-Initiative verwendet.

### 2.1.5 RASSA-Initiative

Die RASSA-Initiative[1] wurde durch die *Technologieplattform Smart Grids Austria* (TPSGA) [22] gestartet, wobei die Technologieplattform 2008 gegründet wurde. In den Jahren

> »2010 bis 2013 [wurde die Plattform] vom FEEI – Fachverband der Elektro- und Elektronikindustrie und Oesterreichs Energie als Trägerorganisationen unterstützt« [23].

Die Gründung in der Rechtsform als Verein folgte im Jahr 2013. Im Impressum der TPSGA steht der Tätigkeitsbereich des Vereins geschrieben, der einen passenden Rahmen zur Zielsetzung und auch der Wichtigkeit hinter der RASSA-Initiative setzt:

> »Die Technologieplattform Smart Grids Austria vereint alle relevanten Akteure aus der Energiewirtschaft, der Regulierungsbehörde, Industrie und F&E Einrichtungen. Die Plattform schafft den Rahmen für eine koordinierte Abstimmung der österreichischen Akteure und damit eine einheitliche österreichische Perspektive zum Thema Smart Grids«[24].

Alleine die breite Aufstellung der Vereinsmitglieder als relevante Akteure ist ein Zeichen des interdisziplinären Themas. Nach heutigen Stand sind laut [22] folgende Branchen und Unternehmen Mitglieder der Technologieplattform:

- **Energiewirtschaft**: Oesterreichs Energie vertritt als Interessensvertretung der österreichischen Elektrizitätswirtschaftschaft rund 140 Mitgliedsunternehmen, welche Transport- und Verteilnetze Österreichs sowie Energielieferanten inkludiert.
- **Technologieanbieter**: FEEI - Fachverband der Elektro- und Elektronikindustrie; ABB AG; ArgoNET; Beckhoff Automation; cyberGRID; Eaton GmbH; Fronius International GmbH; IMENDO GmbH; Kapsch Smart Energy; Moosmoar Energies OG; Nokia; Schrack Technik Energie GmbH; Siemens AG Österreich; Sprecher Automation; S&T Smart Energy GmbH; Tiani „Spirit“ GmbH; Venios
- **Forschung**: Austrian Institute of Technology (AIT); Alpen-Adria Universität Klagenfurt; Fachhochschule Salzburg; Fachhochschule Technikum Wien: Institut für Erneuerbare Energien; Energieinstitut der Johannes Kepler Universität Linz;

[1] Die Idee von RASSA wurde durch Georg Kienesberger, TU Wien, Institut für Computertechnik, ins Leben gerufen.

Montanuniversität Leoben – Lehrstuhl für Energieverbundtechnik; SBA Research; Technische Universität Wien: Institut für Computertechnik; Technische Universität Wien: Institute für Energiewirtschaft (Energy Economics Group) und Elektrische Anlagen; Technische Universität Wien: Institut für Telekommunikation; Technische Universität Wien: Institute of Computer Engineering - Automation Systems Group

- **Öffentliche Stellen**: Die E-Control ist seit 2001 der Regulator des österreichischen Energiemarkts und sorgt für die Einhaltungen und Überprüfungen von Regulierungen für die Versorgungssicherheit und Nachhaltigkeit.
- **Netzwerkpartner**: Der offizielle Vertreter der IEC und Cenelec ist der österreichische Verband für Elektrotechnik (OVE) und unterstützt die Plattform in Hinsicht auf die Bildung des Netzwerkes auf nationaler Ebene.
- **Andere Plattformen**: Technologieplattform Photovoltaik Austria; Arbeitsgruppe Kleinwindkraft Österreich

Angesichts der großen Anzahl an starken Partnern konnte die Plattform Roadmaps veröffentlichen, wie zum Beispiel die Technologieroadmap Smart Grids Austria *Die Umsetzungsschritte zum Wandel des Stromsystems bis 2020* [25], welche maßgebliche Zielrichtungen für Forschung und Industrie in Österreich aufzeigt. Dabei hat sich die RASSA-Initiative nachfolgenden Zielen verschrieben. Die Entwicklung einer Referenzarchitektur durch die Übereinstimmung und den Konsens von relevanten Stakerholdern, sowie die Schaffung eines Migrationspfades. Darüber hinaus werden sicherheitsrelevante Anforderungen an die verschiedenen Rollen und Akteure in Anbetracht der (kritischen) Strominfrastruktur in Österreich erhoben. Die potenziell betroffenen Akteure werden in die Schaffung der Referenzarchitektur miteingebunden und es soll eine Sensibilisierung zum Thema (Cyber-)Security stattfinden. Dies kann beispielsweise durch die Zusammenarbeit in Form von Workshops passieren. In diesen können bestehende Prozesse für den Schutz des Stromnetzes ausgearbeitet werden, um an diesen anzuknüpfen und branchenübergreifend einen Konsens zu finden.

## 2.2 Relevante Forschungsarbeiten zu Referenzarchitekturen

In diesem Abschnitt wird auf eine Auswahl bestehender Arbeiten eingegangen, die sich mit dem Thema Referenzarchitekturen oder Architekturentwicklung im Allgemeinen im Sinne der Systementwicklung im Softwarebereich befassen. Diese sind nicht nur in der Smart-Grid-Domäne vorhanden oder als Softwarelösung verfügbar, sondern können auch nur konzeptionell dokumentiert sein.

### 2.2.1 RAMI 4.0

In einem anderen technischen Gebiet rund um Industrie 4.0 hat sich in kurzer Zeit die *Referenzarchitektur Industrie 4.0* (RAMI 4.0) etabliert. RAMI 4.0 hat sich aus den

Grundzügen des SGAM entwickelt [26]. Aufgrund des großen Marktpotenzials und auch der relativ jungen Thematik (im Vergleich zwischen dem Stromnetz im Allgemeinen und den neuen Entwicklungen in Bereich der Industrie-Automatisierung) wurde diese Referenzarchitektur rasch von großen Unternehmen akzeptiert. Das liegt vor allem daran, dass das:

> »Potenzial [...] allein für die sechs Branchen Maschinen- und Anlagenbau, Elektrotechnik, Automobilbau, chemische Industrie, Landwirtschaft und Informations- und Kommunikationstechnologie auf einen zusätzlichen jährlichen Effekt von 1,7 Prozent geschätzt [wird]. Dies entspricht allein für diese ausgewählten Branchen bis 2025 mindestens 78 Mrd. Euro mehr Bruttowertschöpfung am Standort Deutschland.« [27, S. 5].

Es besteht daher ein begründetes hohes Interesse an einer Standardisierungsmaßnahme für Industrie 4.0 mit Hilfe einer Referenzarchitektur.

Der grundsätzliche Aufbau von RAMI 4.0 und dem SGAM ähneln einander stark. Im RAMI 4.0 konnte die grundlegende Struktur von SGAM übernommen werden und die Anpassungen wurden durch die Initiatoren von dem *Zentralverband für Elektrotechnik- und Elektronikindustrie e.V.* (ZVEI) für die Thematik der Industrie 4.0 vorgenommen [26] und die Schichten und Achsen entsprechend der Domäne angepasst [28].

Die erste Dimension mit der Sicht auf das System entspricht wie im SGAM den Schichten beziehungsweise Layern. Die *Business-*, *Functional-*, *Information-* und *Communication-*Schichten sind erhalten geblieben. Für den Industrie 4.0 Kontext wurde der *Component Layer* in *Asset Layer* umbenannt und das Modell mit einer zwischenliegenden Schicht, dem *Integration Layer*, erweitert. Dabei werden die physischen Objekte im Kontext von Industrie 4.0 als *Assets* angesehen und die Integration von Assets ins System im *Integration Layer* angesiedelt. Der *Integration Layer* hat nach [29] die Hauptaufgabe eine sogenannte Administrationsschale für die anderen Schichten für alle physischen Assets zur Verfügung zu stellen. Hier können Verbindungen zwischen den Objekten in der realen Welt (Assets) und der virtuellen Welt eingetragen werden.

Anstelle der in SGAM beschriebenen Zonen und Domänen Achsen, befindet sich im RAMI 4.0 zum einen die Achse *Life Cycle & Value Stream*. Für den Lebenszyklus in der *Life Cycle & Value Stream* Achse wird die Norm IEC 62890 herangezogen, mit der Unterscheidung zwischen *Type* und *Instance*. In der zweiten Dimension befindet sich im RAMI 4.0 die weitere Achse der *Hierarchy Levels*. Hier werden die Normen IEC 62264 und IEC 61512 für die Einordnung der funktionalen Zuordnungen innerhalb einer Fabrik oder der Anlage verwendet. Nähere Informationen zu der Anwendung der beiden Achsen sind in [28] beschrieben.

Beispielsweise wurden im Projekt openAAS verschiedene Modelle mit Hilfe des RAMI 4.0 umgesetzt [30] und zeigten so die ersten Realisierungen mit Hilfe der Referenzarchitektur für Industrie 4.0. So konnte »gemäß der Referenzarchitektur RAMI 4.0 (DIN SPEC 91345) eine funktionsfähige Verwaltungsschale, das heißt ein digitales Abbild eines realen Produkts/Geräts« [30, S. 3] geschaffen werden.

### 2.2.2 IIRA

Die *Industrial Internet Reference Architecture* (IIRA) wurde im Juni 2015 zum ersten Mal unter der Versionsnummer 1.7 durch das *Industrial Internet Consortium* (IIC) veröffentlicht [31]. Sie basiert auf dem ISO/IEC/IEEE 42010:2011 Standard, um als Vorlage und Methode in den verschiedenen Industriesektoren mit teils einzigartigen oder hochspezifischen Anforderungen eingesetzt werden zu können, damit ein gemeinsames Verständnis und eine interoperable Kommunikation für das Gesamtsystem von allen beteiligten Interessensgruppen geschaffen werden kann.

Dabei wurde darauf Wert gelegt, dass die Architekturbeschreibung und -darstellung möglichst generisch gehalten wurde, um flexibel genug für die Verwendung in der Industrie zu sein. Durch die Beschaffenheit von IIRA sollen technologische Lücken schneller identifiziert werden und somit Neuentwicklungen zu mehr Interoperabilität verhelfen, um die Technik im Allgemeinen zu verbessern.

In IIRA gibt es anstelle der Schichten insgesamt vier sogenannte *Viewpoints*. Dabei ähnelt der Aufbau des IIRA Modells mit seinem *Business-*, *Usage-*, *Functional-* und *Implementation Viewpoint* des SGAM und dem des RAMI 4.0. Weitere Details zur IIRA sind in der Spezifikation [31] nachzulesen.

Es gibt schon Bestrebungen seitens der IIC (Initiator hinter IIRA) und ZVEI (Initiator hinter RAMI 4.0), eine Brücke zwischen den beiden Architekturen zu finden und die Interoperabilität noch weiter zu erhöhen [32], vor allem, da immer mehr und mehr Geräte auf den Markt kommen.

Um das Ziel einer übergreifenden Domänen-Interoperabilität zu erreichen, wurden folgende Punkte durch die IIC und der Plattform Industrie 4.0 vereinbart, um ineffiziente Parallelarbeiten auszuschließen [32]:

- Gemeinsames Verfassen von Anforderungen für Standardisierungsgremien.
- Einen technischen Austausch aufrecht erhalten, um Zuordnungen, Unterschiede oder Verbesserungen auf beiden Seiten zu identifizieren.
- Zusammenarbeit für den Nutzen der Interoperabilität von Systemen aus unterschiedlichen Domänen.

Dabei wurde laut der Verlautbarung [32] auch erkannt, dass es unvorteilhaft wäre, wenn die IIC oder die Plattform Industrie 4.0 unterschiedliche Anforderungen in die Mitwirkung und globalen Standards bringen würden.

Auch um die Begriffe von *Industrie 4.0* und *Industrial Internet* im Kontext der Referenzarchitekturen besser auseinanderhalten zu können, soll das folgende Zitat das Verständnis schärfen:

> »In a nutshell, Industrie 4.0 is about *making* things smartly, while the industrial internet is about making things *work* smartly. In other words, Industrie 4.0 is

> about making products by managing the entire value chains along with product lifecycles, while the industrial internet is about building, deploying and operating large connected systems« [33, S. 3].

Um die Unterschiede zwischen RAMI 4.0 und IIRA zu verdeutlichen, muss man sich das Hauptgebiet der jeweiligen Architekturen ansehen [32]. IIRA zielt auf die Interoperabilität zwischen vielen Anwendungsbereichen ab, während RAMI 4.0 den Fertigungsprozess detailliert behandelt. Die Industrie als ganzes gesehen ist dabei nicht nur auf einen Bereich beschränkt wie es im RAMI 4.0 der Fall ist, sondern erstreckt sich über mehrere Bereiche. Weiters gibt es in den jeweiligen Domänen des IIRA eigene Anforderungen, die eine Fusion der Architekturen schlicht zu kompliziert und praxisfern machen würden. Ein weiteres Ziel der Abstimmung war es, eine Marktverwechslung zu vermindern, da sich auf den ersten Blick einige Konzepte überlappen, bei genauer Analyse sich diese allerdings stark in der Anwendung unterscheiden [33].

### 2.2.3 MSRA

Die *Microgrid Security Reference Architecture* (MSRA) ist eine Referenzarchitektur, die ihren Fokus hauptsächlich auf Security-Empfehlungen und Richtlinien für die Implementierung eines möglichst sicheren Microgrid-Steuerungssystems ausgelegt hat [34]. Ein Microgrid ist ein eigenständiger Netzabschnitt, der an einem größerem Stromnetz angeschlossen sein kann. Das Microgrid ist in der Lage, durch Batteriesysteme und (meist erneuerbaren) Stromerzeugern in einem sogenannten Inselmodus betrieben zu werden und so einen hohen Grad an Autarkie im Bereich der Stromversorgung zu erreichen.

Innerhalb des *Smart Grid Protection Against Cyber Attacks* (SPARKS) Projekts wurde eine Vielzahl von Arbeiten eingehend analysiert, die sich mit der Widerstandsfähigkeit und Security innerhalb von Smart Grids beschäftigten. Neben Ergebnissen von NIST und SGAM wurde auch das MSRA in einem Whitepaper [35] in SPARKS betrachtet. Dabei wurde festgestellt, dass das MSRA nicht explizit die Standpunkte der im Rahmen des SGAM identifizierten Akteure berücksichtigt und auch nicht auf die Bandbreite der Subsysteme wie sie in den *National Institute of Standards and Technology Interagency Report* (NISTIR) 7628 Richtlinien angeführt werden, eingeht. Die Ergebnisse des MSRA konzentrieren sich auf die Sicherheitsprozesse, Technologien und Bedrohungen im Zusammenhang mit Security im Microgrid.

In MSRA steht zunächst ein übergeordnetes Konzept für die Operationen innerhalb eines Microgrids. Dabei werden auch die Akteure im Stromsektor, Kommunikationsprotokolle und Betriebsmodi angegeben. Die Dokumentation [34] beschreibt Schwachstellen für allgemeine Netzwerksysteme bzw. industrielle Kontrollsysteme. Ein Konzept für ein Bedrohungsmodell wird im weiteren Verlauf des Dokuments erläutert und eine Bedrohungsmatrix [34, S. 45] erstellt. Bemerkenswert ist allerdings, dass das Konzept der Bedrohungsmatrix der MSRA im NIST LRM aufgegriffen wurde. Wegen der beigemessenen Bedeutung der Bedrohungsmatrix durch das NIST wird die Definition zur Bedrohungsmodellierung im Folgenden im Original wiedergegeben:

> »Threat modeling is a technique which identifies a set of potential attacks on a particular product or system and describes how those attacks might be perpetrated and the best methods of preventing potential attacks. Threat models are used as input to the creation of test plans and cases.« [36, S. 66]

Mit Hilfe der Anfertigung solcher Bedrohungstabellen kann die Positionierung eines Akteurs innerhalb eines Use Cases besser bewertet werden. In MSRA wird das Konzept sogenannter Cyber-Akteure (im Prinzip technischen Geräte wie Switch, Router, Authentifizierungsserver, etc.) eingesetzt, um eine bessere Netzwerksegmentierung durchsetzen zu können und damit die Sicherheit im Microgrid zu erhöhen.

Die unterteilten Segmente werden im MSRA als *Enklaven* bezeichnet. Hier wird Wert auf die potenziellen Sicherheitslücken gelegt und, in welcher Art und Weise der Datenaustausch stattfindet. Dabei handelt es sich im MSRA-Projekt um definierte Tabellen, die folgende Daten beinhalten [34]:

- Ursprungsgerät/-akteur und Zielgerät/-akteur
- **Austausch:** Typ, Intervall, Methode, Priorität, Latenztoleranz
- **Daten:** Typ, Genauigkeit, Größe, Ausfallsicherheit
- **Einstufung der Informationsabsicherung:** *Confidentiality*, *Integrity*, *Availability*

Der Stellenwert der Begriffe *Confidentiality*, *Integrity* sowie *Availability* und deren Bedeutung ist in 3.1.2 näher beschrieben.

### 2.2.4 GridWise Architecture Council

Das *GridWise Architecture Council* (GWAC) verfolgt die Bestrebungen eines besseren Verständnis und Systementwurfs in der Smart-Grid-Domäne. Das vorgeschlagene GridWise Transactive Energy Framework [37] besitzt derzeit allerdings keine (öffentliche) Softwarelösung, welche verwendet werden kann. Es werden vielmehr in Europa unter der *Flexiblepower Alliance Network* bestehende Framework Standards weiterentwickelt und neue Schnittstellenstandards eingeführt [38].

Die Ergebnisse des von der GWAC vorgestellten *Transactive Energy Frameworks* sind ebenso bei der Erarbeitung des SGAM sowie auch in das NIST *Framework and Roadmap for Smart Grid Interoperability Standards* [39] eingeflossen.

Um die Grundkonzepte ableiten zu können, die oftmals als *GWAC stack* bezeichnet und zitiert werden [40], wird das Konzept [37] wie folgt beschrieben.

Es gibt drei Kategorien, die zugleich als Treiber agieren. Diesen sind zwei beziehungsweise drei von insgesamt acht Schichten inklusive näherer Beschreibung von GWAC in absteigender Reihenfolge zugeordnet.

Die Nummerierung stellt dabei die oberste bzw. unterste Ebene dar, weswegen die achte Schicht als erstes genannt wird (diese ist als „oberste“ Schicht weiter unten in Abbildung 2.2 dargestellt), und die „unterste“ Schicht mit der Nummer eins beschrieben wird.

- Organisatorische Kategorie

  8. **Ökonomische / Regulatorische Richtlinien**
     Politische und ökonomische Ziele in Richtlinien und Verordnungen verfasst
  7. **Geschäftsziele**
     Strategische und taktische Zielsetzung zwischen Firmen
  6. **Geschäftsprozesse**
     Abstimmung zwischen operativen Geschäftsprozessen

- Informatorische Kategorie

  5. **Geschäftskontext**
     Kenntnis des Geschäftsumfelds in Bezug auf eine spezifische Interaktion
  4. **Semantisches Verständnis**
     Verständnis der in den übertragenen Datenstrukturen enthaltenen Konzepte

- Technische Kategorie

  3. **Syntaktische Interoperabilität**: Verständnis der Datenstrukturen von ausgetauschten Nachrichten zwischen Systemen
  2. **Netzwerk Interoperabilität**: Mechanismen zum Austausch von Nachrichten zwischen mehreren Systemen in einer Vielzahl von Netzwerken
  1. **Grundlegende Anschlussmöglichkeit**: Mechanismus zur Herstellung physikalischer und logischer Verbindungen zwischen Systemen

Dazu gibt es eine Reihe von themenübergreifenden Problemen, die sich über alle Ebenen und Kategorien erstrecken. Die zehn identifizierten Probleme wurden in drei Sektionen unterteilt [40]. Da jene Probleme von NIST LRM und SGAM in dieser oder erweiterter Form wieder aufgegriffen werden, sind sie im Folgenden aufgelistet:

- Zu der ersten Sektion, der Konfiguration und Entwicklung, gehören die gemeinsame Bedeutung von Inhalten im Sinne von Semantik, die Ressourcenidentifikation, Entdeckung und Konfiguration, sowie Systementwicklung und Skalierbarkeit.
- Der zweiten Sektion des Betriebs und der Ausführung wurden die Zeitsynchronisation und Sequenzierung, die Transaktions- und Statusverwaltung sowie die Servicequalität zugeordnet.
- In der dritten Sektion Security und Safety sind die Themen Security, Safety, Rechnungswesen und Systemerhaltung beinhaltet.

Eine kompakte Übersicht der beschriebenen kategorieübergreifenden Probleme sowie des *GWAC stack* ist in Abbildung 2.2 gegeben. In der Grafik sind die themenübergreifenden Probleme gruppiert wiedergegeben sowie eine farbliche Zuordnung der Interoperabilitätskategoriegruppen.

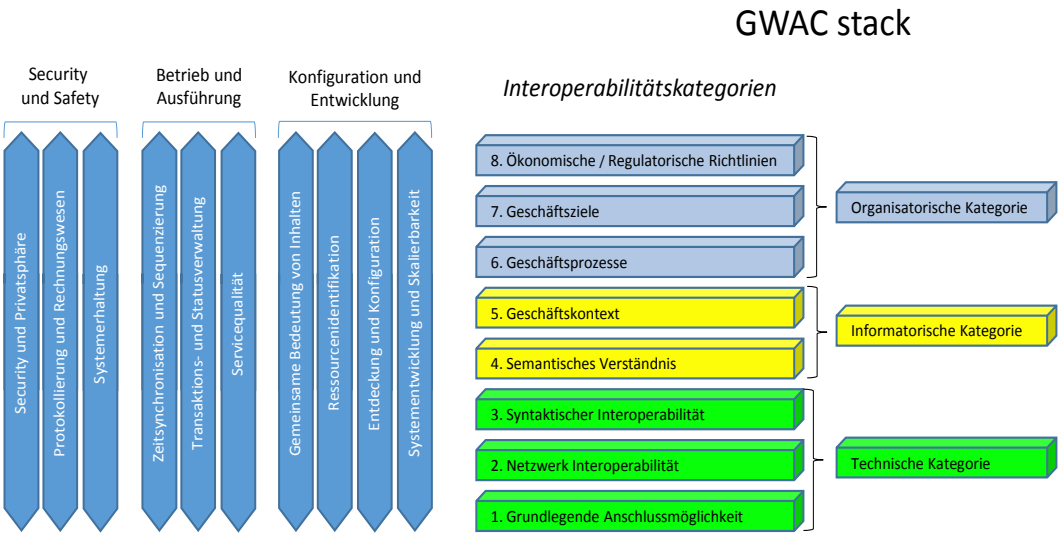



Abbildung 2.2: Eigene Darstellung des GWAC Stack und den themenübergreifenden Problemen, angelehnt an [40, S. 17].

Eine praktische Anwendung des *GWAC stack* ist für 25.000 US-Dollar (oder kostenfrei für Finanzierungsmitglieder) als technischer Bericht erwerbbar, in welchem der *GWAC stack* »as a model for utility IT project execution« [41] zur Unterstützung der *IntelliGrid* Methodik für Projektmanagement eingesetzt wurde. Dabei wird versprochen [41], dass das Whitepaper aufzeigt, wie man einen verwendbaren Use Case erhält und wie man ihn in die verschiedenen Schichten des *GWAC stacks* zerlegen kann, um so eine Projektplannung zu erstellen. Um ein erfolgreiches und gut durchdachtes Projekt zu gewährleisten, sei auf jedes der kritischen Probleme des *GWAC stacks* eingegangen worden. Mögliche Einblicke hierzu gewährt lediglich eine Präsentation [42], die auf der Grid-Interop 2011 Tagung vorgestellt wurde. Allerdings konnte für diese Arbeit der Bericht [41] nicht angeschafft werden, daher kann auch nicht näher darauf eingegangen werden, ob in der praktischen Anwendung auch hinreichend auf *Safety* und *Security* eingegangen worden ist. Die angesprochene *IntelliGrid*-Methodik wird in 2.3.2 näher beschrieben.

### 2.2.5 TOGAF

*The Open Group Architecture Framework* (TOGAF) Standard [43] (Vers. 9.2) definiert ein Unternehmensarchitektur-Framework. Der Standard bietet Werkzeuge und Methoden für den Entwurf, das Planen, die Implementierung und das Steuern der (IT-)Architektur innerhalb von Unternehmen [44].

TOGAF unterstützt vier sogenannte Architekturdomänen, die laut der Spezifikation als allgemein anerkannte Teilbereiche einer Unternehmensarchitektur zu sehen sind. Diese Architekturdomänen sind folgende [45]:

- Die Business-Architektur-Domäne wird durch die Geschäftsstrategie, die Geschäftsführung, die Organisation und wichtige Geschäftsprozesse definiert.
- Die Datenarchitektur-Domäne wird durch die Struktur von logischen und physischen Datenbeständen innerhalb einer Organisation und den zugehörigen Datenverwaltungsressourcen beschrieben.
- Die Anwendungsarchitektur-Domäne bietet einen Entwurf für die individuell zu entwickelnden Applikationen. Darüber hinaus wird ihr Zusammenspiel und ihre Verbindung zu den Prozessen des Kerngeschäfts der Organisation beschrieben.
- Die Domäne der Technologiearchitektur beinhaltet die logischen Hard- und Softwaremöglichkeiten, welche notwendig sind, um die verschiedenen Geschäfts-, Daten- und Anwendungsdienste verfügbar zu machen. Die Infrastruktur der Informationstechnologie, Middleware, Kommunikation und Netzwerk, (Daten-)Verarbeitung, Standards und vieles mehr gehört dieser Domäne ebenso an.

Mit der TOGAF *Architecture Development Methodology* (ADM) wird eine Art Lebenszyklus definiert, der sich in zehn Phasen einteilen lässt. Mit diesen Phasen kommt man von der Vision der Geschäftsidee bis hin zur Aufrechterhaltung und Wartung in einem Architekturprozess [39]. Die Vorbereitungsphase initiiert den Prozess [45] für den Lebenszyklus einer Architektur:

- Phase A: Architekturvision
- Phase B: Geschäftsarchitektur
- Phase C: Architektur der Informationssysteme
- Phase D: Technologiearchitektur
- Phase E: Chancen und Lösungen
- Phase F: Migrationsplanung
- Phase G: Implementierungsführung
- Phase H: Änderungsmanagement in der Architektur

Die Phasen sind dabei immer mit dem durchgehend laufenden Anforderungsmanagement abzugleichen. Der durch TOGAF ADM definierte Kreislauf ist in Abbildung 2.3 zu sehen, in welchem die Phasen A bis H iterative durchlaufen werden.

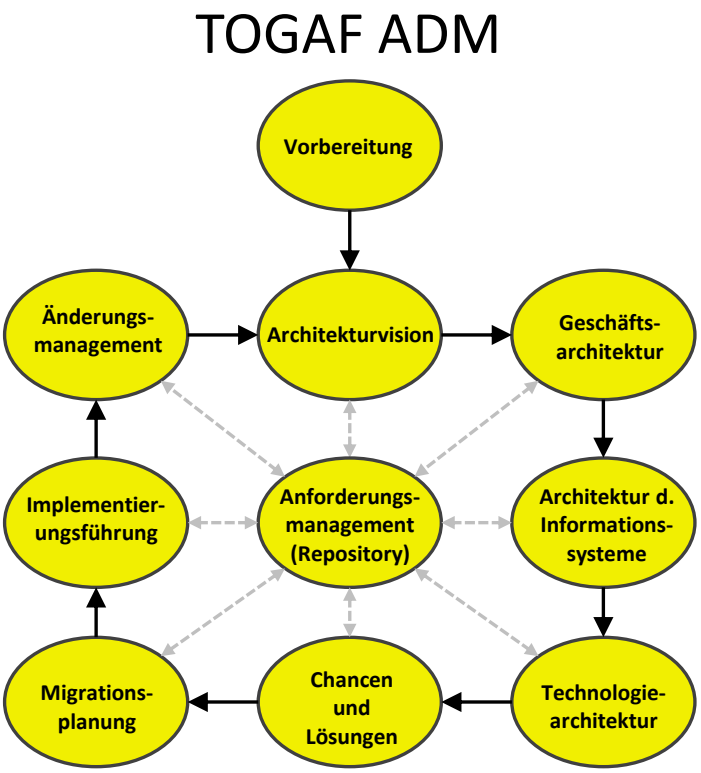



Abbildung 2.3: Eigene Darstellung von TOGAF ADM angelehnt an [44].

### 2.2.6 NIST LRM

Im Jahr 2010 wurde von NIST durch eine groß angelegte Kooperation[2] von hunderten Wissenschaftler_innen und Stakeholdern des Energiesektors der NISTIR 7628 Bericht [46] veröffentlicht und damit die grundlegende Spezifikation für das *NIST Logical Reference Model* (LRM) festgelegt.

Insgesamt wurden sieben Domänen identifiziert, die allerdings noch weiter unterteilt werden können. Diese Domänen sind im Folgenden auch mit ihrer englischen Originalbezeichnung nach [46] angeführt:

- Übertragung (*Transmission*)
- Verteilnetz (*Distribution*)
- Betrieb (*Operation*)
- Großangelegte Energieerzeugung (*Bulk Generation*)
- Märkte (*Markets*)

[2] An den Inhalten des NISTIR 7628 waren namentlich 484 Mitwirkende beteiligt.

- Kunde (*Customer*)
- Dienstleister (*Service Provider*)

Im LRM ist verallgemeinert von *Actors*, also Akteuren die Rede. Diese Akteure können über Schnittstellen zwischen zwei Elementen Informationen austauschen. Die Akteure/Elemente können dabei Gruppierungen von Organisationen, Gebäuden, Personen, Systemen, Softwareprogrammen oder Geräten widerspiegeln. Das LRM zeigt die Verbindungen zwischen den Akteuren auf, die mit sogenannten *Logical Interfaces* verbunden sind. In Abbildung A.1 im Anhang ist das NIST LRM [46] dargestellt, welches die Verbindung der Akteure mit den Interfaces verdeutlichen soll. Weiters sind die verschiedenen Domänen mit Farben hinterlegt worden, die *Oesterreichs Energie* konzeptionell übernommen hat (siehe 3.2.3 und 3.3.2). Die eingezeichneten Interface-Verbindungen sowie deren textuelle Beschreibung lieferten auch eine Ausgangsbasis für die RASSA-Architektur.

In Abbildung A.1 sind die Verbindungspfeile nach dem Schema *UXX* aufgebaut, wobei das *U* für *Universal* steht. *XX* ist der Platzhalter für die zugeordnete Interface-Nummer. Dabei sollte erwähnt werden, dass es sich um eine Überblicksansicht handelt und lediglich Teile des komplexen und sich stetig weiter entwickelnden Smart Grid darstellt.

In den NISTIR 7628 Guidelines wird als Basis für Security-Betrachtungen das *NIST LRM* herangezogen. Hierbei handelt es sich um eine Sammlung von logischen Akteuren und deren Interfaces zueinander. Auf Basis spezifischer Security-Attribute werden die einzelnen Interfaces konkreten Interface Categories zugeordnet. Diese stellen die Basis für die Entwicklung von Security Requirements dar. »Der große Mehrwert des LRM besteht darin, dass über den Umweg der Interfaces [...] und Interface Categories für jeden Aktor Security Requirements zur Verfügung stehen« [47].

Diese Security Requirements umfassen für das im NIST LRM definierte Modell für die 46 hinterlegten Akteure oder Geräte insgesamt 137 Interfaces, welche in 22 *Interface Categories* eingeteilt wurden und mit 194 Security Requirements verbunden sind.

Der NISTIR 7628 Bericht beinhaltet in seiner Ursprungsfassung von 597 Seiten weitere sicherheitsrelevante Aspekte wie zum Beispiel ein generisches Modell für Risikoquantifizierung, Cyber-Security Zielsetzungen, Kryptografie und Schlüsselmanagement sowie Klassifizierung von potenziellen Schwachstellen. Im weiteren Verlauf dieser Arbeit werden die wichtigsten Punkte aufgegriffen und erläutert. So sind die Beschreibung der Domänen des NIST LRM unten im Zusammenhang mit dem SGAM näher ausgeführt.

### 2.2.7 Smart Grid Architecture Model (SGAM)

*Comité Européen de Normalisation (Europäisches Komitee für Normung)* (CEN), *Comité Européen de Normalisation Électrotechnique (Europäische Komitee für elektrotechnische Normung)* (CENELEC) und *European Telecommunications Standards Institute (Europäisches Institut für Telekommunikationsnormen)* (ETSI) sind europäische Standardisierungsinstitute, die sich zu der CEN-CENELEC-ETSI *Smart Grid Coordination*

*Group* (SGCG) zusammen geschlossen haben [6], um das EU Mandats M/490 [48] zu erfüllen. Ein Ergebnis dieser Arbeitsgruppe war das *Smart Grid Architecture Model*. Das Modell baut darauf auf, Smart Grid Use Cases aus geschäftlicher, technischer, sicherheitstechnischer und standardisierungstechnischer Sicht zu dokumentieren und gegebenenfalls Lücken aufzuzeigen. Es gibt eine Reihe von Lösungen, die sich mit der Methodik rund um SGAM beschäftigen und individuelle Stärken und Schwächen aufweisen. Diese werden in 5.1 dieser Arbeit näher erläutert.

Die Einsatzmöglichkeiten des SGAM sind gemäß [49, S. 11] wie folgt. Das SGAM kann zur Standardisierung verwendet werden als auch zusätzlich zur strukturierten Analyse von Smart Grid Use Cases. Dieser Vorgang erleichtert es, verschiedene Ansätze zu Smart-Grid-Architekturen, Paradigmen, Roadmaps und Standpunkten sowohl zu visualisieren als auch vergleichen zu können. Der strukturierte Ansatz kann als Wegweiser für die Erstellung neuer möglicher Umsetzungspläne verwendet werden. Wie in den vorherigen Abschnitten bereits erwähnt wurde, gilt es auch bei SGAM ein gemeinsames Verständnis zwischen den verschiedenen Interessengruppen zu gewährleisten. SGAM soll helfen Standardisierungslücken zu identifizieren und zugleich den Umfang von Smart-Grid-Projekten zu visualisieren. Schließlich gilt es, die Komplexität des Smart Grid zu bewältigen.

Dabei wurden in der Beschreibung der *CEN-CENELEC-ETSI Smart Grid Coordination Group* [49] auch Einschränkungen angeführt. Die volle Stärke des SGAM liegt in der Modellierung von Interaktionen und Verbindungen zwischen den Domänen und Zonen und verbessert nicht notwendigerweise eine bewährte Architektur in einem der einzelnen Segmente. Eine detaillierte Anforderungsspezifikation muss erstellt werden, auch wenn SGAM die Ableitung von Systemanforderungen vereinfacht. Selbiges gilt für Entwicklungsspezifikationen. Das Hauptaugenmerk liegt auf der Abbildung der Gesamtarchitektur. Detaillierte Probleme oder Herausforderungen wie zum Beispiel die Auswirkungen von Oberschwingungen werden nicht näher für einzelne Zonen betrachtet. Darüber hinaus ersetzt es keine detaillierten Beschreibungen zu Sicherheitsvorschriften oder Betriebsbedingungen.

Diese Einsatzmöglichkeiten, Stärken und Schwächen des SGAM ergeben sich aus den Einflüssen, die wie folgt aufgelistet sind [49]. So konnten die Materialien des NIST LRM (siehe 2.2.6) eingebettet werden, sowie auch die in 2.2.4 beschriebenen Interoperabilitätskategorien des GWAC stack für die Zwecke des SGAMs angepasst werden. Die mit eingeflossene IntelliGrid-Methode [IEC PAS 62559:2008-01] ist in 2.3.2 erläutert. Auch der Architektur-Standard TOGAF (beschrieben in 2.2.5) ist mit eingeflossen.

Die Einflüsse und deren konzeptionellen Verknüpfungen zwischen TOGAF, GWAC stack und dem SGAM ist in Abbildung 2.4 dargestellt. Dadurch werden die Konzepte der Interoperabilitätskategorien und die fünf Interoperabilitätsschichten des SGAM besser nachvollziehbar. Sieht man sich zum Beispiel den Kreis *Geschäftsarchitektur* des TOGAF ADM an, so ist dieser sowohl mit der *6. Geschäftsprozesse*-Kategorie von GWAC stack verbunden als auch mit dem *Business Layer* des SGAM.

Nachdem Abbildung 2.4 schon auf die verschiedenen Ebenen des SGAM mit den Ver-

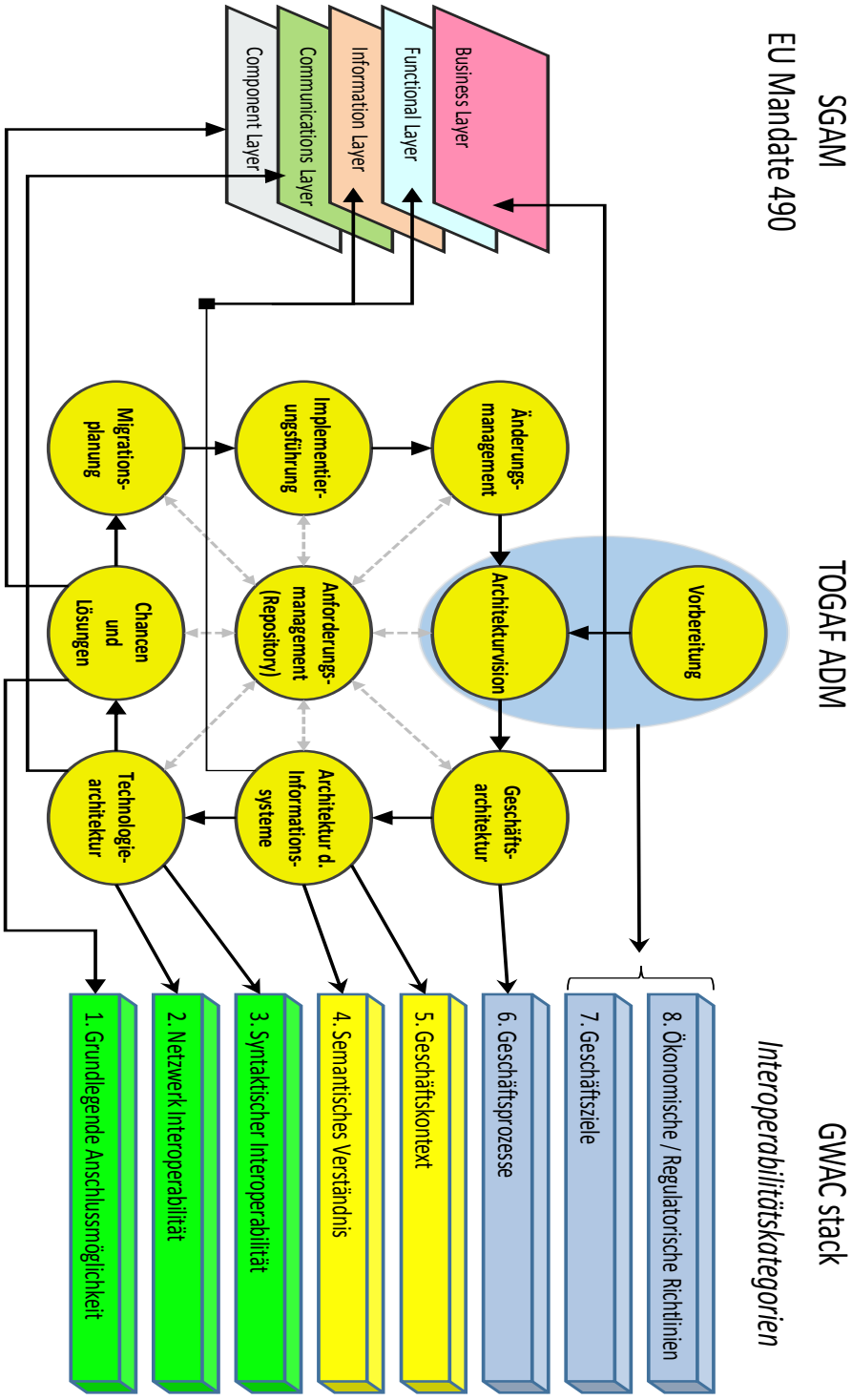



Abbildung 2.4: Verknüpfung von Architektur Konzepten. Eigene Darstellung angelehnt an [39].

knüpfungen von TOGAF hinweist, wird im Folgenden auf den Aufbau des sogenannten *SGAM Würfel* eingegangen. Zunächst stammen wesentliche Inhalte aus dem in 2.2.6 beschriebenen Modell. Die Überführung der Ergebnisse des *NIST Conceptual Model* an den europäischen Markt ist vor allem durch die Einführung der Domäne der Verteilten Energieerzeuger gekennzeichnet [50, S. 196], welche ein notwendiger Entschluss nach der Liberalisierung des Energiemarktes war. Vergleicht man die Erstversion [51] mit der letzten Version [39] des *NIST Framework and Roadmap for Smart Grid Interoperability Standards* vergleicht, sieht man auch, dass die Rolle des Verteilten Energieerzeugers auch im NIST zwar Anwendung gefunden hat, eine eigens geschaffene Domäne gibt es hier allerdings immer noch nicht. In [39, S. 202] wird zum Beispiel die Übertragungsdomäne beschrieben, die solche verteilten Energieerzeuger und (Klein-)Speichersysteme beinhalten kann.

Abbildung 2.5 ist eine eigene Darstellung des *SGAM Würfels*. Auf der linken Seite sind die fünf sogenannten Interoperabilitätsschichten eingezeichnet, die wie folgt beschrieben werden können [6, 13]: Der *Business Layer* bildet mithilfe von Business-Akteure Geschäftsbedürfnisse und Business Cases ab. Der *Function Layer* beschreibt Funktionen und Dienste, welche unabhängig von der physikalischen reellen Implementierung sind, mit Use Cases. Der *Information Layer* beschreibt Informationsobjekte innerhalb von Datenmodellen, die es für die Kommunikation zu übertragen gilt. Der *Communication Layer* beschreibt verwendete Protokolle für die Kommunikation zwischen Endgeräten. Der *Component Layer* beinhaltet physische Komponenten oder Gesamtsysteme sowie deren Funktionen und Informationen.

Der *SGAM Würfel* behandelt zwei weitere Achsen. Eine Achse beschreibt die verschiedenen Domänen, die wie folgt nach [6, 13] beschrieben werden können:

- (Haupt-)Erzeugung: Großkraftwerke, die von Kernkraftwerken bis zu großen Wasserkraftwerken reichen
- Übertragung: Transport der erzeugten Energie über große Entfernungen
- Verteilung: Verteilung der transportierten Energie von und zu Verbrauchern
- Verteilte Energieerzeuger: können Energie erzeugen und speichern und sind an das Verteilungsnetz angebunden
- Kundendomäne: Kunden, die von der Industrie, Unternehmen und privaten Haushalten als Endverbraucher einzuordnen sind

Die andere Achse, genannt Zonen, entspricht den hierarchischen Ebenen des Managements von Energiesystemen [6, 13]: *Prozess* reicht von Generatoren bis zu Kabeln, Sensoren und Umwandlung von Energie in Form von Wärme, Strom und Wasser. *Sektor* deckt alle Arten von Geräten ab, die das elektrische Stromsystem überwachen, steuern oder schützen. *Station* ist der Ort, an dem zum Beispiel Daten von SCADA-Systemen zusammengefasst

oder die für die Stationsautomatisierung verwendet werden. *Betrieb* ist die Steuerung der Energiesysteme; *Unternehmen*, entspricht der Unternehmensebene. *Markt* bietet Raum für den Verkaufsbereich, der Einzelhandelsmärkte, Energiehandel oder Preisgestaltung am Vortag beinhalten kann. Im Verlauf der Arbeit wird auf die Schichten, Domänen und Zonen anhand von Beispielen näher eingegangen.

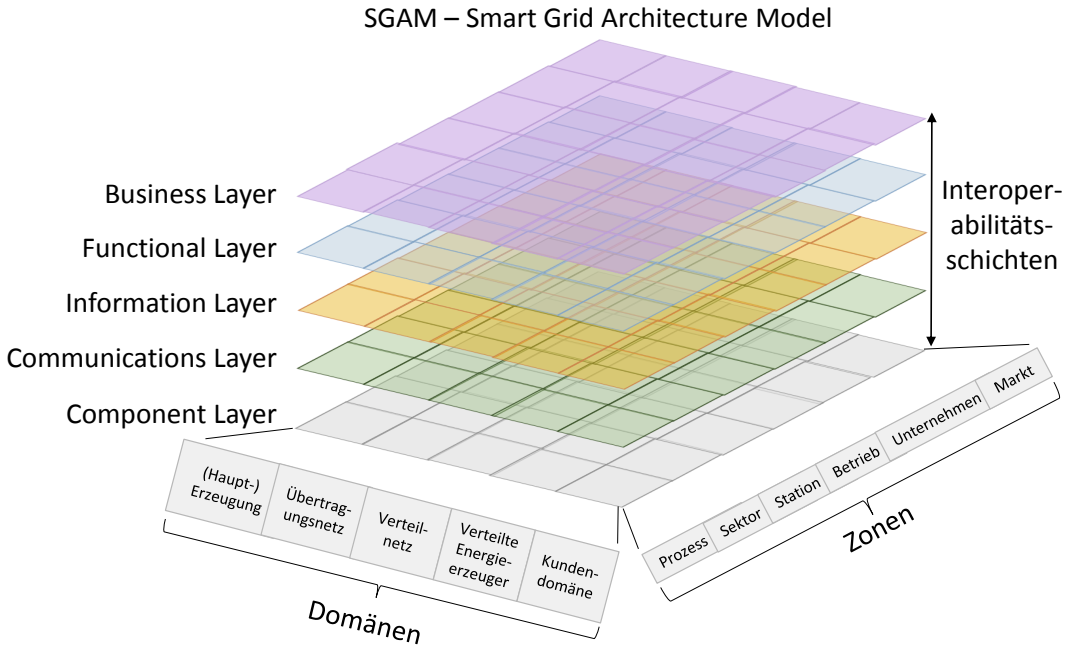



Abbildung 2.5: Eigene Darstellung des SGAM Würfels aufbauend auf [6, S. 30].

ArchiMate (Version 2.1) [52] ist ein weiteres Tool, dass zur Schaffung von SGAM laut [49] beigetragen hat. Der ebenfalls von der Open Group definierte Spezifikation behandelt dabei intensiver das Thema der Unternehmensarchitekturen. Da auf die relevanten Konzepte für das Gesamtverständnis bereits eingegangen worden ist, wird ArchiMate in dieser Arbeit nicht näher behandelt.

## 2.3 Lösungen für Use Case Management

Hier wird auf verschiedene Varianten und Lösungen für das sogenannte Use Case Management eingegangen.

Um auf der Geschäftsebene zu neuen Projektideen, Produktsparten oder Features zu kommen, werden oft *Use Cases* verwendet. Diese bieten eine gute Möglichkeit, um Rahmenbedingen zu diskutieren oder Abläufe und Interaktionen beziehungsweise Abhängigkeiten zu visualisieren. Dabei gibt es verschiedene Arten, wie solche Use Cases dargestellt und verwendet werden können. Im Folgenden werden die unterschiedlichen Herangehensweisen vorgestellt.

### 2.3.1 Textuelle Use Case Sammlungen

Eine mögliche Form zur Verfassung und Verbreitung von Use Cases ist geschriebener Text. Hierbei können Use Cases in Schriftform erfasst werden, um die Zuständigkeiten, involvierten Personen, Akteuren oder Systemen zu dokumentieren. Dies reicht von formlosen Beschreibungen bis hin zu strukturierten Formblättern. In der Smart-Grid-Domäne ist der flächendeckende Einsatz von Smart Meter, den neuen intelligenten Stromzählern, ein großes Thema. Vor allem die Aspekte und Spezifikationen rund um die Sicherheitsanforderungen sind dabei im Vordergrund. Die Zertifizierungsstelle des deutschen Bundesamts für Sicherheit in der Informationstechnik [53] führte Ende 2018 noch immer keine zertifizierten Kommunikationseinheiten von intelligenten Messsystemen an. Für das sogenannte Sicherheitsmodul gibt es schon erste ausgestellte Zertifikate [53]. Für das Sicherheitsmodul wurde eine textuelle Ansammlung von Use Cases bereitgestellt [54] und zeigt damit die Wichtigkeit, die Use-Case-Beschreibungen spielen können.

In Österreich ist die Elektrizitätswirtschaft durch die Interessenvertretung *Oesterreichs Energie* vertreten. In den vergangenen Jahren wurden von der Vertretung einige Use Cases erarbeitet und nun als Arbeitsgrundlage auf ihrer Webseite [55] bereitgestellt für die Erstellung eines Lastenhefts zu dem sogenannten *Advanced Meter Communication System*. Es ist eine Vorlagenansammlung für das Kommunikationssystem fortschrittlicher Messgeräte mit wichtigen Vorgaben und Richtlinien. Dort sind Quellenangaben zu Datensicherheit und Anforderungen zum Datenschutz, Authentifizierung und Autorisation, EU-Normen, Applikationsprotokolle für Smart Metering, Powerline Communication und vieles mehr hinterlegt.

Darüber hinaus wurden auch Smart Metering Use Cases definiert [56], die zusammen mit der Arbeitsunterlage als »[...] Empfehlungen [zu sehen sind] und *können* von den Netzbetreibern als Referenz für deren Ausschreibungen verwendet werden« [55]. Die Use Cases [56] basieren auf den Anforderungskatalogen von Österreichs Energien wie dem Ende-zu-Ende Sicherheit Smart Metering Anforderungskatalog oder dem Elektrizitätswirtschafts- und Organisationsgesetz (ELWOG) sowie andere Verordnungen. Die Use Cases werden in dem Dokument mit elf Feldern in einer Tabelle vordefiniert. Auf die Einhaltung von gesetzlichen Vorgaben wurde besonderen Wert gelegt.

Dadurch, dass die tabellarischen Spezifikationen gleiche Struktur haben, können sie auch in Programme importiert werden. Dieser Aspekt wird in 2.3.4 näher ausgeführt.

### 2.3.2 EPRI Use Case Repository

Das öffentlich zugängliche *Electric Power Research Institute* (EPRI) Use Case Repository [57] beinhaltet eine Sammlung von 185 Use Cases (Stand: 17.August 2018), die sich auf sieben Kategorien aufteilen lassen. Die zugängliche Sammlung wurde innerhalb der EPRI Smart-Grid-Demonstrationsinitiative [58] erstellt und durch Use Cases der Industrie ergänzt. Das gelistete Konsortium bestand aus 23 internationalen Partnern. Die Ziele der Demonstrationsinitiative waren die Erstellung von Use Cases für die Entwicklung von

Standards, das Festlegen von Anforderungen für Lastmanagementintegration und das Schaffen einer verbesserten Rollendefinition in verschiedenen Marktumgebungen.

Nutzer_innen aus Firmen oder Organisationen können nach Hinterlegung ihrer Kontaktinformationen Use Cases hochladen. Dabei werden sie angehalten, das *IntelliGrid* Use-Case-Template [59] zu verwenden. Die Microsoft Word Vorlage enthält sechs große Punkte in tabellarischer Form, wie sie schon in 2.3.1 angesprochen wurde:

1. Beschreibung des Use Case
2. Diagramme der Use Cases
3. Technische Beschreibung
4. Schritt für Schritt Analyse des Use Case
5. Beschreibung von ausgetauschten Informationen
6. Abschnitt zur Festlegung für ein gemeinsames Begriffsverständnis

Die hochgeladenen und verfügbaren Use Cases wurden allerdings nicht alle nach dem zur Verfügung gestelltem Use Case Template angefertigt. Die inhaltliche Präsentation von einigen Use Cases (*Distributed Energy Resource Controller Generates and Executes Substation Blackstart Sequence; Version 1.2; January 13, 2010* oder *Real-Time Pricing - Top Level*) deuten auch auf eine Vorversion des Templates hin. Inhaltlich beinhalten sie allerdings die wesentlichen Punkte. Betrachtet man jedoch beispielsweise den Use Case *Energy Scheduling Billing and Settlement* oder den Use Case *Inter-Area Oscillation Damping*, so fällt auf, dass in diesen jedoch ein Diagramm für den Use Case fehlt.

Nichtsdestotrotz ist die Sammlung der Use Cases hilfreich. Zum einen bietet sie Einblicke, wie die internationalen Firmen bestimmte Use Cases definiert haben und diese verstehen. Zum anderen bietet die sieben-jährige Initiative eine lange Laufzeit mit fünf gelieferten Berichten im Zeitraum von 2010 bis 2014. Dies ermöglicht Einblicke in den Verlauf eines langfristig angelegten Projekts sowie die gewonnenen Erkenntnisse und Resultate, da es zu jedem der Projekte innerhalb der Demonstrationsinitiative eine Kurzfassung [60] gibt. Darüber hinaus gibt es den Link zu den jeweiligen Fallstudien, bei denen kostenfreie und auch kostenpflichtige Dokumente vorzufinden sind, die die jeweiligen Projekte detailliert beschreiben.

### 2.3.3 Smart Grids Standards Map

Die sogenannte Smart Grids Standards Map [61] ist ein weiteres Online Tool der *International Electrotechnical Commission* (IEC). Es bietet zwei verschiedene Ansichtsmöglichkeiten.

Die erste ist die *Architecture View*. Hierbei handelt es sich um eine aufgezeichnete Rasterkarte nach den SGAM-Zonen und -Domänen mit der zusätzlichen *Crosscutting*

Spalte, die zu den Domänen eingereiht wurde. Dabei wurden Cluster gebildet, die gewisse Themenbereiche darstellen, wie zum Beispiel der Cluster *Home & Building Automation*. In den Clustern befinden sich die Systeme und Komponenten und ihre Protokolle zueinander, angeordnet auf der aufgezeichneten SGAM-Ebene. Die Nutzerinnen und Nutzer können sich die IEC-Standards als Kurzbeschreibungen zu den Systemen anzeigen lassen. Darüber hinaus sind die Komponenten größtenteils mit den Use Cases wie in 2.3.2 beschrieben verlinkt. In Abbildung A.2 im Anhang ist der Link zu der online-verfügbaren Smart Grids Standards Map innerhalb der RASSA-Referenzarchitektur in einem Diagramm als Bild hinterlegt, da die Informationen für die Vollständigkeit des Modells relevant sind. Eine Überführung der Informationen zu den Kommunikationsprotokollen ist ein offener Entwicklungspunkt der RASSA-Initiative (siehe Kapitel 7).

Die zweite Ansichtsmöglichkeit ist die *Mapping View*. Dies ist eine ordnerähnliche Struktur mit einer Auflistung der erwähnten Cluster. Insgesamt gibt es 16 Cluster mit 195 zugeordneten Systemen und Komponenten, die sich wiederholen können (z.B. ist ein *Router* in mehreren Clustern vertreten). Die *Mapping View* bietet darüber hinaus auch eine Standard-sortierte Sicht in der Ordnerstruktur, in der sich insgesamt 512 verlinkte Standards befinden.

### 2.3.4 Use Case Management Repository und SGAM Visio Tool

Dieser Abschnitt setzt sich mit dem *Use Case Management Repository* (UCMR) und dem SGAM Visio Tool auseinander, welche beide im Zuge des DISCERN (*Distributed Intelligence for Cost-effective and Reliable Solutions*) Projekts entwickelt wurden [62].

Für SGAM gibt es zwei Programme, die Nutzer_innen die Modelle auf Diagrammbasis anfertigen lassen. Die SGAM Toolbox ist in 3.2.1 erläutert aufgrund der Abhängigkeit zu Enterprise Architect. Hier wird das DISCERN SGAM Tool [63] erläutert, welches ermöglicht mit Microsoft Visio (Visio 2010 oder neuere) SGAM-Modelle zu erstellen und welches einen Export für das UCMR ermöglicht.

Die Vorlagen im DISCERN SGAM Tool [63] enthalten in einer Archivdatei mehrere unterschiedliche Schablonenvorlagen für jede der SGAM-Schichten, sowie eine Datei für das SGAM-Modell. Die Modellierung erfolgt in sechs Schichten, während der *Information Layer* hier in eine Schicht für das kanonische Datenmodell und eine Schicht für den Geschäftsbezug aufgeteilt ist. Die Schichten des DISCERN SGAM Tools können und sollen durch eine extra hierfür zur Verfügung gestellten Funktion synchronisiert werden. Dadurch können positionierte Elemente auf der SGAM-Ebene (Domänen und Zonen) erfasst und die Information über die Elemente diesen zugeordnet werden. Links in Abbildung 2.6 ist ein Beispiel gegeben, welches zwei Elemente im *Component Layer* zeigt. Das DISCERN SGAM Tool ermöglicht eine Navigation durch die SGAM Schichten, was durch die oben in der Abbildung 2.6 Tool-interne Pfeilpositionierung gekennzeichnet ist. Dadurch ergibt sich die Möglichkeit einer Gesamtansicht über die Schichten hinweg. Rechts in Abbildung 2.6 ist der synchronisierte *Communication Layer* dargestellt, in dessen Ansicht nun der darunterliegende *Component Layer* eingeblendet ist [13].

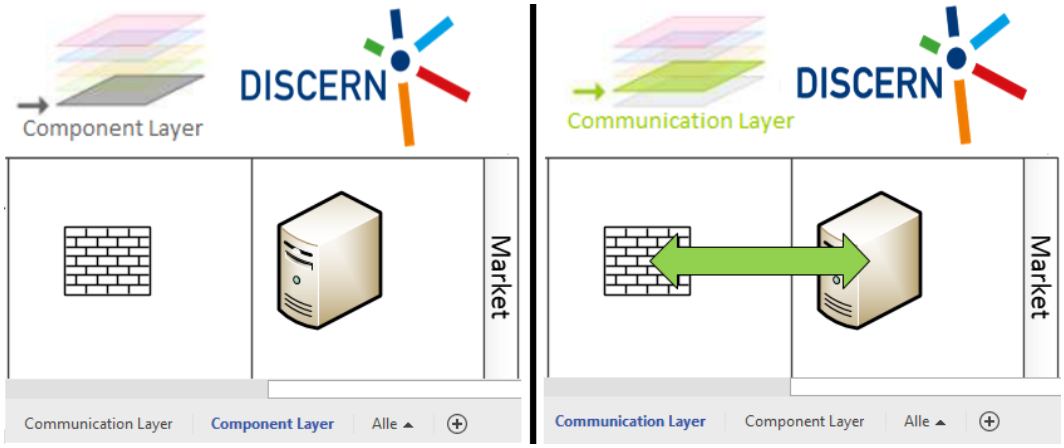



Abbildung 2.6: Screenshot des DISCERN SGAM Tools mit Elementen im *Component Layer* und *Communication Layer* [13].

Das UCMR wurde von OFFIS entwickelt. Es handelt sich dabei um eine Webapplikation [64], die nach Registrierung für derzeit laufende und aktuelle Projekte von verschiedenen Forschungs- und Kooperationspartner_innen Zugang zu den dort angelegten Use Cases bietet. Dabei kommt ein internationaler Standard der IEC zur Anwendung. Der IEC 62559-2:2015 [65] ist ein Standard, der die Use Case Methodology beschreibt und in welchem die Vorlagen für Use Cases, Akteur- und Anfordungslisten definiert sind. Dieser Standard hat dabei den IEC PAS 62559:2008 [66] ersetzt, der von EPRI im Rahmen der IntelliGrid Architektur definiert wurde. Die in 2.3.2 beschriebene Spezifikation von Use Cases gibt einen Einblick, wie der Standard spezifiziert sein soll.

Bei dem Entwurf des IEC 62559-2:2015 Standards wurde darauf Wert gelegt, dass das Prinzip des UCMR für viele Domänen und Branchen eine Rolle spielen kann. So wird in [67] die Unterstützung für Normungsarbeit im Bereich des umgebungsunterstützenden Lebens (Ambient Assisted Living) und die Rolle des UCMR beschrieben. Hier kommen ebenso Use Cases zum Einsatz, mit dem Ziel die Interoperabilität mit Systemen von Drittanbietern zu erhöhen. Vor allem in diesem Bereich gibt es viele spezielle Bedürfnisse, die nicht durch einen Hersteller allein abgedeckt werden. Ein Entwurf für ein System mit kompatiblen Schnittstellen für die Komponenten für einen korrekten Informationsaustausch kann daher sowohl kompliziert als auch komplex werden.

Für diese Arbeit ist speziell die Energiedomäne das Thema. Für die RASSA-Initiative, deren Hintergründe in 2.1.4 beschrieben sind, wurde daher für eine vorläufige technische Evaluierung ein projektspezifisches Repository angelegt. In diesem können Use Cases angelegt und Smart Grid relevante Einordnungen wie die Zonen und Domänen des SGAM vorgenommen werden. Dabei eröffnet das Onlinetool die Interaktion und Befüllung von Tabellen, Drag&Drop Kommandos und vor allem eine mögliche dreidimensionale Darstellung von Use Cases [13].

In Abbildung 2.7 ist die Funktion der interaktiven Visualisierung im Webbrowser darge-

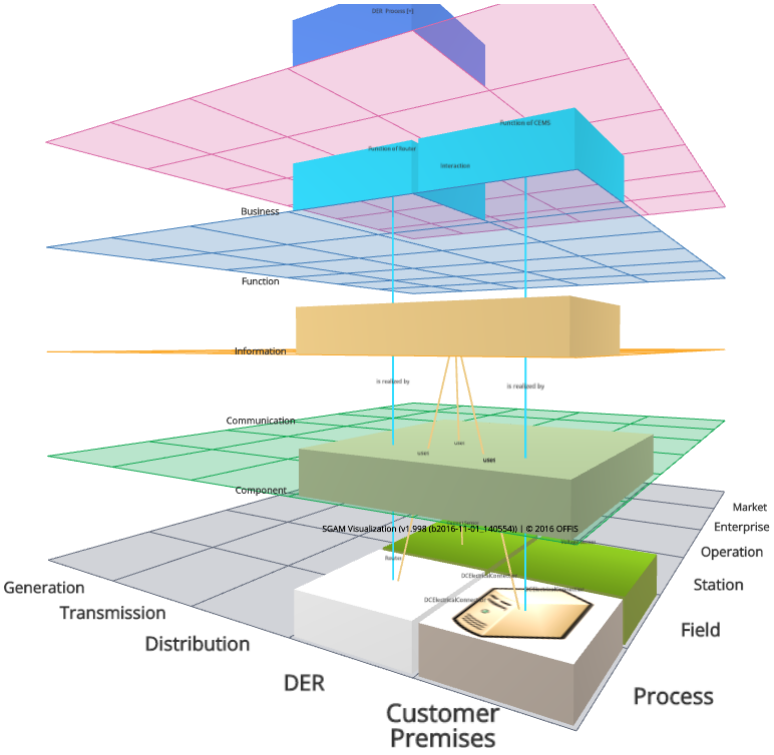



Abbildung 2.7: Screenshot der interaktiven SGAM Visualisierung nach dem Datenimport [13].

stellt. Dabei sind Komponenten und ihre Verbindung in den verschiedenen Schichten, Domänen und Zonen mit einem einfachen Datenset eines Use Cases dargestellt, der mit dem DISCERN SGAM Tool erstellt wurde. Das Visio Tool bietet einen SGAM XML Export an, der für den Import in das UCMR für die Erstellung der Abbildung 2.7 verwendet wurde.

## 2.4 Lösungen für Analysen durch Drittanbieter

Hier werden fünf Lösungen kurz vorgestellt, die sich mit dem Thema Risikoabschätzung und -managment, Informationssicherheit und Folgenabschätzungen beschäftigen. In 4.4 werden diese Lösungen noch einmal aufgegriffen.

### 2.4.1 Data Protection Impact Assessment Tool

Das vom Austrian Institute of Technology entwickelte *Data Protection Impact Assessment* (DPIA) Tool dient zur Abwicklung einer Datenschutzfolgenabschätzung [68]. Die Motivation, die hinter der Entwicklung des Tools steckt, ist die Europäische Datenschutzverordnung, die fordert, dass alle Dienste, welche personenbezogene Daten erheben oder verarbeiten, einer Datenschutzfolgenabschätzung unterliegen müssen [69]. Im Falle des

Smart Grids und neuen Sensoren werden Messdaten über den Verbrauch der Kund_innen möglicherweise erfasst und müssen daher diesen Prozess durchlaufen.

Das entwickelte Tool ist eine Webbrowser-basierte Anwendung, welches die Zusammenarbeit im Team ermöglichet [68]. Benutzerfreundlichkeit wird durch Tooltips über das notwendige Format oder Inhalte bei der Eingabe von Daten unterstützt und darüber hinaus durch eine Beschreibung der durchzuführenden Schritte in der Benutzeroberfläche begleitet. Eine automatisierte Auswertungsmöglichkeit und Dokumentenerstellung wird zur Verfügung gestellt, um insgesamt den notwendigen Aufwand für eine Datenschutzfolgenabschätzung zu reduzieren.

Auf das DPIA Tool wird in 4.4.2 nochmals eingegangen.

### 2.4.2 AURUM

Im RASSA-Architektur Projekt wurde durch den Konsortialpartner SBA Research das Tool AURUM verwendet. Ziel des Tools ist es Risikoanalysen als Entscheidungsunterstützungssystem für kleine und große Unternehmen, Auditoren und Risikomanager bereitzustellen [70].

> »AURUM basiert auf einer Security Ontology, die ein höchst ausdifferenziertes Infrastrukturmodell zur Verfügung stellt. Die Basisversion dieser Ontologie bietet dem Benutzer eine umfassende Informationssicherheitswissensbasis.«[71, S. 3]

Die Webseite von AURUM [70] bietet Funktionen wie Echtzeitberechnung des Risikoniveaus mitsamt Visualisierung oder Voraussagen für potenzielle (negative) Auswirkungen aufgrund eines (Security Risks).

In [72] wurde das unten beschriebene Tool *CRISAM*® und das GSTOOL des Bundesamts für Sicherheit in der Informationstechnik BSI mit AURUM verglichen. Beim GSTOOL wurde allerdings sowohl der Vertrieb als auch die Unterstützung eingestellt [73].

### 2.4.3 CRISAM®

Eine Lösung für die in Österreich ansässigen Netzbetreiber ist die weit verbreitete IT-Risikomanagement-Software *CRISAM*®, was für *Corporate Risk and IT-Security Application Method* steht [74]. Dabei ist die Zielsetzung wie folgt beschrieben:

> »*CRISAM*® ist kein neuer Standard oder Best Practice Ansatz, der für die Prüfung und Auditierung angewendet wird. Zielsetzung von *CRISAM*® ist, eine nachvollziehbare Methodik (unterstützt durch den CRISAM®-Explorer, einer SW-Applikation in der die *CRISAM*®-Methodik operationalisiert wurde), bereit zu stellen, mit der ein Risikomanagement Prozess implementiert werden kann, der den Anforderungen der Prüfer und Auditoren genügt «[74].

*CRISAM*® bietet auf der Webseite eine Reihe von Produktlösungen und Paketen mit zusätzlichen Inhalten an. So kann etwa durch Analyseberichte nachgewiesen werden, ob

das Informationssicherheitsmanagementsystem konform zu den Standards der *ISO/IEC 27001* ist und dadurch das Unternehmen unterstützen, sich nach dieser Norm zertifizieren zu lassen [75]. Speziell für das Tätigkeitsfeld der Netzbetreiber wird ein Paket für Industrielle Steuerungssysteme sowie Überwachungssteuerung und Datenerfassung angeboten, welches Risiken technischer oder organisatorischer Natur für Steuerungssysteme und Kommunikationsprotokolle für Endgeräte als Informationselemente beinhaltet [76].

### 2.4.4 verinice

Das *verinice* Tool ist eine Open Source Software für das Management von Informationssicherheit [77]. Es handelt sich dabei um ein Informationssicherheitsmanagementsystem, das vom deutschen BSI lizenziert ist. Der größte Teil des Quellcodes ist öffentlich zugänglich und auch eine Grundversion zu Testzwecken ist kostenfrei erhältlich. Diese ist allerdings in der Funktionalität eingeschränkt, so können etwa keine Daten importiert oder Berichte erstellt werden.

Als zusätzliche (kostenpflichtige) Inhalte werden Datenschutzmodule und Risikokataloge als importierbare Dateien angeboten. Diese sind nicht öffentlich als Quellcode zugänglich.

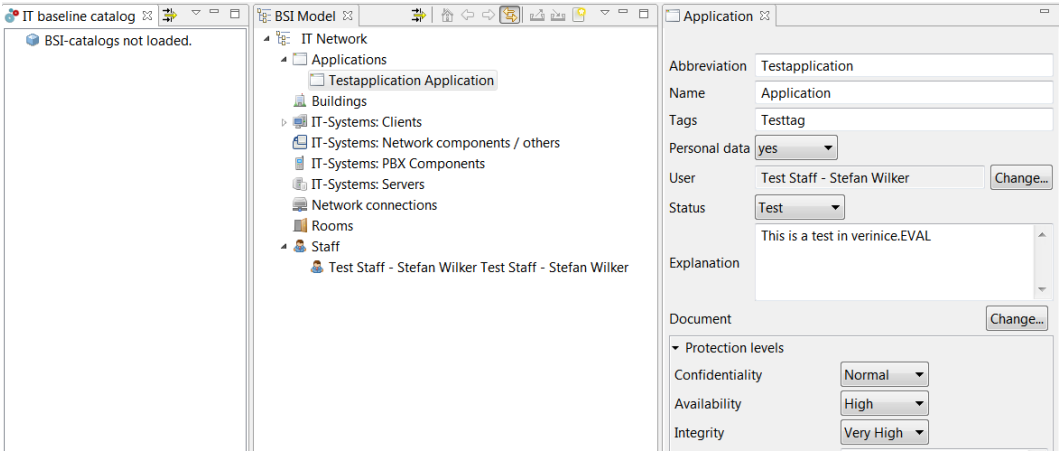



Abbildung 2.8: Screenshots vom verinice.EVAL Tool [77]

In Abbildung 2.8 ist rechts unten die Kategorisierung einer beispielhaften Applikationssoftware mit Werten für *Confidentiality*, *Availability* und *Integrity* einzugeben. Auf diese wird in 3.1.2 näher eingegangen. Darüber hinaus können viele weitere Attribute zugewiesen werden, wie beispielsweise finanzielle Konsequenzen und eine Einschätzung der zeitlichen Auswirkung in unterschiedlichen Zeitstufen (8, 24, 48, 96, 168, 720, mehr als 720 Stunden). Auf der linken Seite der Abbildung ist zu sehen, dass kein BSI-Katalog geladen wurde.

Das BSI hat mehrere IT-Grundschutz-Kataloge [78] definiert, die in Deutschland und Österreich aufgrund ihres Umfangs einen hohen Stellenwert haben. Da dieses Modul allerdings kostenpflichtig ist, wurde es im Rahmen dieser Arbeit nicht näher betrachtet.

Durch den Erwerb des Moduls kann zwar eine von verinice bereitgestellte Beispielfirma importiert werden und es werden Beispiel-Reports zur Verfügung gestellt. Ohne die kostenpflichtigen Module ist die Auswertung eines Beispiels vermutlich ohne Expertenwissen und Einpflegung von Datensätzen wenig aussagekräftig und wird daher in dieser Arbeit nicht näher ausgeführt.

### 2.4.5 Self Assessed Risk Profiler

Ein Ergebnis im Zuge des *Self Assessed Risk Management* [79] Projekts ist der *Self Assessed Risk Profiler*. Durchgeführt wurde das Projekt von der *European Union Agency for Network and Information Security (Europäische Agentur für Netz- und Informationssicherheit)* (ENISA). Ziel war es, eine einfach verwendbare Anleitung bereitzustellen, welche die Komplexität versteckt ohne dabei auf Vollständigkeit oder Richtigkeit der durchgeführten Bewertungen zu verzichten [79].

Der *Self Assessed Risk Profiler* ist ein Microsoft Office Excel Tool, welches einen *Basic*- und *Expert*-Modus anbietet. Hierfür werden Makros verwendet, welche die Nutzer_innen durch die Anwendung führen. In dieser kann im *Basic*-Modus anhand von 15 Fragen eine vorläufige Einschätzung des IT-Security-Risikos eines Unternehmens erstellt werden. Die erste Frage richtet sich beispielsweise an die Größe und Komplexität der Unternehmensstruktur mit vier gestuften Antworten zur Unternehmensgröße an sich, Anzahl der Vertragspartner, Büros und ansässiger Staaten.

Der *Expert*-Modus richtet sich an Expert_innen für Risikoabschätzung und Risikomanagement. Die vorher erwähnten 15 Fragen werden hier detailliert aufgeteilt. Im Gegensatz zu einer einschätzenden Antwort müssen am Beispiel der ersten Frage nun acht Einzeleinschätzungen abgegeben werden.

In beiden Fällen gibt es die Möglichkeit einer grafischen Auswertung. Anhand einer Netzdiagrammdarstellung können die Antworten visualisiert und mit Methoden wie der *ISO/IEC 27005:2008*, einem Standard für den Prozess für *Security Risk Management*, verglichen werden. In Abbildung 2.9 ist links oben eine Frage aus dem *Basic*-Modus angegeben, rechts oben ein Auszug aus dem *Expert*-Modus und unten ein Ausschnitt des Netzdiagramms.

Abbildung 2.9: Screenshots vom Self Assessed Risk Profiler [79]

KAPITEL 3

# Grundlagen und Modellierung komplexer Smart-Grid-Lösungen

Wie der Titel dieser Arbeit schon beschreibt, werden komplexe Smart-Grid-Lösungen modelliert. In diesem Kapitel wird auf die Herausforderungen bei dem Entwurf von Smart-Grid-Lösungen, notwendige Grundlagen, Begriffe, Symbole und Konzepte eingegangen und wie diese modelliert wurden.

## 3.1 Herausforderungen beim Entwurf von Smart-Grid-Lösungen

Durch das komplexe Umfeld, das sich durch Smart-Grid-Lösungen erschließen lässt, gibt es einige Herausforderungen zu meistern. Vor allem durch die Verbundenheit der europäischen Stromnetze gilt es eine Reihe an gesetzlichen Bestimmungen von europäischer Ebene aus zu beachten, sowie auch die Bestimmungen und Gesetze der eigenen Nation. Eine gestufte Darstellung mit individuellen nachvollziehbaren Stufen der Anforderungen, die an Geräte oder Services gestellt werden, gab es bislang aufgrund der Komplexität nicht. Nachfolgend wird sowohl die Problematik der gemeinsamen Sprache mit den Stakeholdern beschrieben als auch das Konzept *Security by Design*, in welches sich beide als Herausforderungen für den Entwurf von Smart-Grid-Lösungen darstellen.

### 3.1.1 Gemeinsame Sprache mit Stakeholder

In 2.1.5 ist die RASSA-Initiative erklärt. Die notwendigen Grundinformationen für die Schaffung einer Referenzarchitektur wurden über das Projekt RASSA-Stakeholderprozess erhoben. Während des RASSA-Architektur-Projekts stellte sich in den Konsortiumsmeetings immer wieder ein unterschiedliches Verständnis von Projektschritten und Zielgruppen heraus. Eine der großen Herausforderungen war dabei, eine gemeinsame Sprache

mit den Stakeholdern zu finden. Die Komplexität, die bei dem Entwurf von Smart-Grid-Lösungen betrachtet werden muss, erschwert die Erreichung dieses Ziels zusätzlich. Beim Thema Strom und Aufrechterhaltung der (elektrischen) Grundversorgung sind viele rechtliche und technische Anforderungen bei der Schaffung einer neuen Lösung zu betrachten, die sich allerdings auch wirtschaftlich rechnen müssen. Und so treffen Experten und Expertinnen aus der Informationstechnologie, Elektrotechnik, Wirtschaft und Behörden mit unterschiedlichen Hintergründen aufeinander. Eine gemeinsame domänenübergreifende Sprache ist für eine erfolgreiche Umsetzung notwendig.

Beispielsweise haben die Autoren von [80] dieses Problem erkannt und mit der Schaffung eines Marktmodells für die Ukraine versucht, eine Ausgangsposition für die Diskussion und Schaffung von zukünftigen Geschäftsprozesse zu etablieren. Dabei stützten sich die Autoren auf das *Harmonized Electricity Market Role Model* der ENTSO-E, welches in 3.3.1 näher beschrieben ist.

### 3.1.2 Security by Design

Im Wesentlichen ist *Security By Design* ein Sicherheitsansatz, der die Infrastruktur (eines Unternehmens, einer Produktlösung) beschreiben lässt. Die modellierten Smart-Grid-Lösungen, welche in dieser Arbeit vorgestellt werden, zielen auf diesen Ansatz ab, um aufgrund der beschreibbaren Lösungen Rückschlüsse zu Security Requirements eines Systems oder einer Lösung zu erlauben. In [81] wurde das Prinzip *Security By Design* anhand der Verknüpfung der Security Requirements des NIST LRM mit dem SGAM als Konzept vorgestellt. Die Ableitung der Security Requirements des von [81] vorgeschlagenen Prozesses beinhaltet dabei fünf Schritte, um ein Modell für eine Security-Bewertung heranziehen zu können:

1. Identifizierung und Spezifizierung des Use Case
2. Identifikation und Abbildung logischer Schnittstellen, Kommunikationsverbindungen und Schnittstellenkategorien
3. Integration von logischen Schnittstellen in die SGAM Functional Layer Schicht
4. Security Requirements für die Use Cases zuweisen
5. Abbildung in anderen Schichten des SGAM

Die Herausforderungen für den Entwurf von Smart-Grid-Lösungen ist durch die Anzahl an notwendigen Security Requirements erschwert. Die Anzahl von potenziellen Bedrohungen wird unweigerlich kontinuierlich steigen, da neue Kommunikationsmöglichkeiten technisch entwickelt werden. Neue Angriffswege werden täglich entwickelt und entdeckt. Diese sind manchmal hochspezialisiert auf einen bestimmten Gerätetyp, die daraus abzuleitenden Security Requirements lassen sich aber in manchen Fällen verallgemeinern. In dieser Arbeit wird gezeigt, wie *Security By Design* diese Herausforderung erleichtern kann.

Für die im Rahmen der RASSA-Initiative vorgestellte Security-Bewertung stehen vor allem die Begriffe *Confidentiality*, *Integrity* und *Availability* im Vordergrund. Diese lassen sich laut [46] wie folgt definieren:

- *Confidentiality* (Vertraulichkeit): Der Verlust der Vertraulichkeit ist die unbefugte Weitergabe von Informationen.
- *Integrity* (Integrität): Ein Integritätsverlust ist die unbefugte Änderung oder Zerstörung von Informationen.
- *Availability* (Verfügbarkeit): Ein Verlust an Verfügbarkeit ist die Unterbrechung des Zugriffs auf Informationen oder eines Informationssystems oder deren Verwendung.

Diese drei Begriffe werden oft als *CIA*-Werte abgekürzt und mit den drei Stufen *low*, *moderate* oder *high*, also niedrigem, moderaten oder hohem Auswirkungsgrad im Falle einer Kompromittierung oder eines Ausfalls bewertet.

Innerhalb des RASSA-Architektur-Projekts wurde die methodische Herangehensweise für das Prinzip *Security by Design* und deren universelle Anwendbarkeit für die Anwendung neuer, ausserhalb des RASSA-Architektur-Projekts liegenden Smart-Grid-Lösungen, hinterfragt. In dieser Arbeit wird deshalb auf die notwendigen Schritte für die Modellierung solcher komplexen Smart-Grid-Lösungen eingegangen. Die Einbettung der *CIA*-Werte in einem Modell wird in 3.3.3 beschrieben und die nützliche Ableitung für Smart-Grid-Lösungen in 4.3 erläutert.

## 3.2 Verwendete Modellierungssoftware

Die in dieser Arbeit präsentierten Modelle sind durch spezielle Programme und eigens angefertigte Symbole entstanden. Um die Hintergründe zu verstehen, wird in diesem Abschnitt auf die verwendete Modellierungssoftware, die Verzeichnisstruktur in der Modellierungssoftware und die Bedeutung der verwendbaren Symbole eingegangen.

### 3.2.1 Eingesetzte Software

Entscheidend für die eingesetzte Software und deren Auswahl sind die Vorarbeiten des RASSA-Architektur-Projekts innerhalb der RASSA-Initiative, in dem ein technischer Anforderungskatalog erarbeitet wurde.

Ein wichtiges Kriterium für die Auswahl der eingesetzten Software war die Produktqualität. Diese wurde nach [82] in *Brauchbarkeit* und *Wartbarkeit* unterteilt. In einem vorangegangenem Stakeholder-Prozess wurde eine Vorauswahl für die wichtigsten Kriterien getroffen:

- Änderbarkeit: »Das Architekturframework muss darauf ausgelegt sein, fortlaufende Änderungen zu erfahren.« [8, S. 26]

- Portabilität: »Das Architekturframework muss darauf ausgelegt sein, portabel zu sein. Dies bezieht sich sowohl auf die Portierung in andere Einsatzgebiete (Domänen, Länder) als auch auf die Geräteunabhängigkeit.« [8, S. 26]

- Nützlichkeit: Das Architekturframework soll für die Anwendern und Anwenderinnen in unterschiedliche Anwendungsszenarien nützlich sein. [8]

- Bedienbarkeit: Das Architekturframework soll für die Anwender und Anwenderinnen benutzerfreundlich sein. [8]

Diese Eigenschaften stellen sich als wichtige Kriterien für die Interoperabilität der Referenzarchitektur heraus.

#### Enterprise Architect

Die aktuellste Version der Sparx Systems Modellierungssoftware *Enterprise Architect* verfügt über eine Reihe von Funktionen [83], welche die oben angeführten Anforderungen erfüllt und sich dadurch in der RASSA-Initiative als Software-Tool zur Modellierung durchgesetzt hat. So bietet das Tool Unterstützung für alle

> »in der UML 2.5 spezifizierten Modelle [...], das Sammeln von Requirements und das Erstellen von test und maintenance Modellen [...] welches als ein Mehrbenutzer, Windows basierendes, graphisches Werkzeug, [...] [die] Erstellung robuster und wartbarer Software unterstützt« [83].

Allgemein bietet Enterprise Architect als Modellierungssoftware die Möglichkeit, für die Betrachtung der Diagramme rein- und rauszuzoomen, was vor allem die Betrachtung von größeren Diagrammen erleichtert. Darüber hinaus können Erweiterungen entwickelt werden, wie zum Beispiel die SGAM Toolbox.

Weitere genutzte und notwendige Funktionen werden im Kontext der jeweiligen Anforderung in weiterer Folge angeführt.

#### Beziehungen zwischen Modellelementen

Ein Großteil dieser Arbeit beschäftigt sich mit den Beziehungen zwischen den Elementen in UML und wie diese zu verstehen sind. Am wichtigsten ist hierbei die *Generalize*-Beziehung, also die Generalisierung.

Generalisierungsbeziehung liegt vor, wenn eine Elternklasse die Generalisierung einer Kindklasse ist und diese deren Attribute erbt, aber auch zusätzliche hinzufügen kann. In der UML-Darstellung und auch in Enterprise Architect zeigt der Pfeil von der spezialisierten Kindklasse auf die generelle Elternklasse.

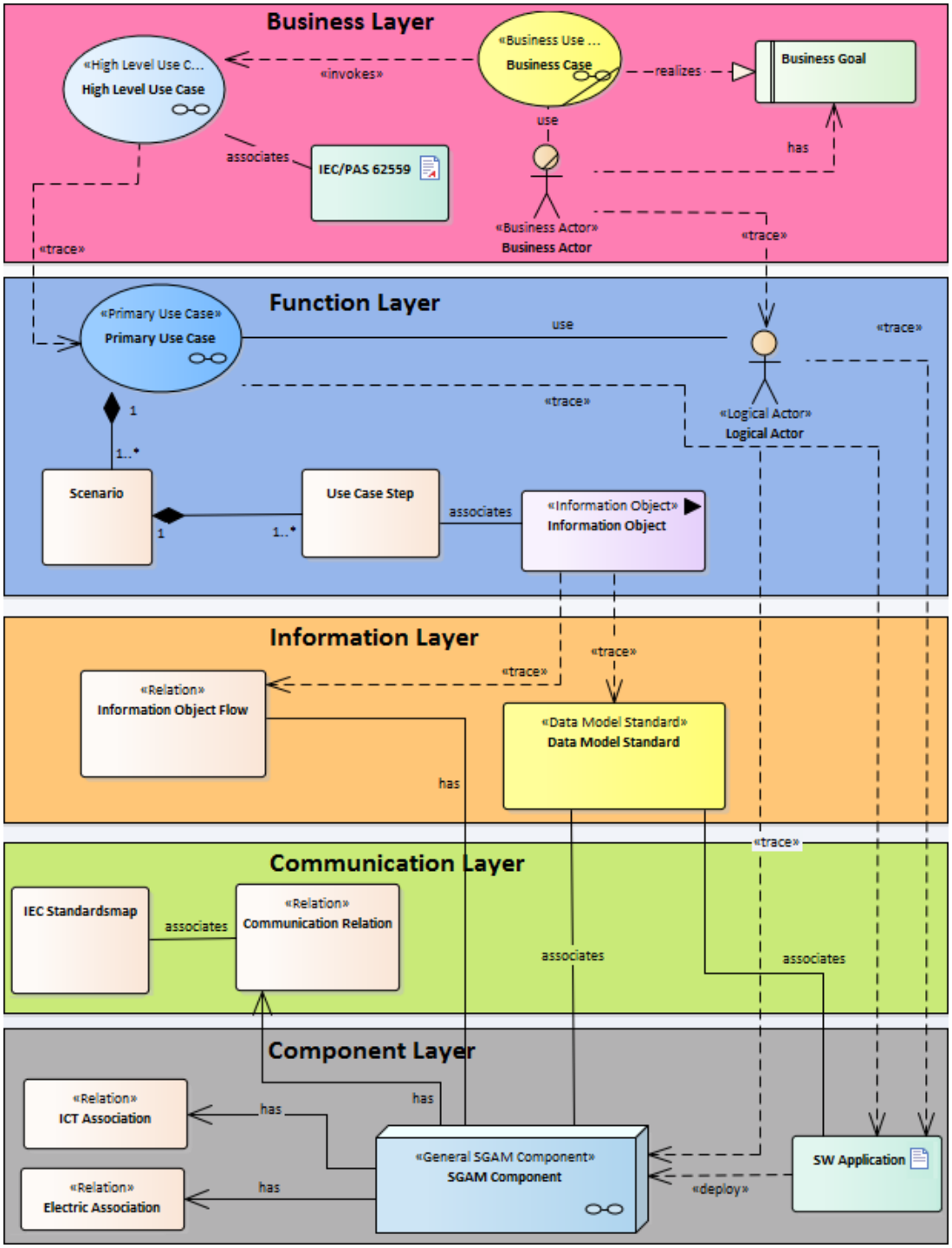



Abbildung 3.1: Eigene Darstellung [13] der SGAM Toolbox Framework Architektur basierend auf [85]

#### SGAM Toolbox

Die SGAM Toolbox ist eine Erweiterung für Enterprise Architect, die auf der Webseite [84] der Entwickler des *Josef Ressel Center for User-Centric Smart Grid Privacy, Security and Control* zum Download verfügbar ist. Dabei wird Version 9.3 oder eine höhere Version des Enterprise Architect für die Verwendung vorausgesetzt. Durch die Schaffung einer eigenen Erweiterung konnte eine Domänen-spezifische Anpassung für SGAM zur Schaffung einer DSML durchführt werden (siehe 2.1.2), welche für die Modellierung der Referenzarchitektur erforderlich ist [14].

In Abbildung 3.1 (siehe vorherige Seite) ist die SGAM Toolbox Framework Architektur dargestellt. Es sind darin die vorgesehenen Beziehungen zwischen den Interoperabilitätsschichten und den unterschiedlichen UML-Elementen zu sehen. So wird ein *Business Case* durch *High Level Use Cases* im *Business Layer* beschrieben. Der *Business Actor* erfüllt einen *Business Case*. Ein *Logical Actor* ist für die Beschreibung in den Use Cases im *Function Layer* vorgesehen. Eine *SGAM Component* stellt im *Component Layer* eine Komponente dar. Auf die Verwendung dieser unterschiedlichen Akteur-Arten wird in 3.4.3 näher eingegangen.

### 3.2.2 Bestehende Modellstruktur von SGAM und RASSA

Im Rahmen der Erklärung der verschiedenen Schichten um das SGAM in 2.2.7 wird im Folgenden auf die bestehende Modellstruktur von SGAM und der Referenzarchitektur eingegangen.

Bei der Erstellung eines neuen Projekts mit der SGAM Toolbox können sowohl die fünf verschiedenen Schichten als auch *Security Requirements* als Ausgangsmodell erstellt werden, in denen sich einige Beispielelemente befinden. Wie in Abbildung 3.2 zu sehen ist, befinden sich alle SGAM-Schichten eines Pakets mit dem Namen *Model Repository*. In dieser Abbildung sind weitere Symbole zu sehen, die optisch ähnlich den Ordner-Symbolen aus Windows sind und dieselbe Funktion für die Diagramme und Elemente des Modells inne haben. Die RASSA Use Cases sind beispielsweise im *SGAM Communication Layer* in einem aufgeklappten Ordner zu sehen. Die weiteren Ebenen des SGAM-Würfels, *SGAM Business Layer*, *SGAM Function Layer*, *SGAM Information Layer*, *SGAM Communication Layer* und *SGAM Component Layer* bilden weitere größere Ordner, in denen Modelle für die entsprechende Ebenen zu finden sind. Im *SGAM Component Layer* sind die Vorarbeiten des NIST LRM zu finden, die in 2.2.6 erläutert sind.

Weitere SGAM-unabhängige Modelle sind im *Model Repository* zu finden. Das *Harmonized Electricity Market Role Model* [86] der ENTSO-E wurde ebenso modelliert, da es während der ersten Hälfte des RASSA-Architektur-Projekts noch nicht online als Model verfügbar war. Die hinterlegte Modellierung bezieht sich dabei auf Version 2015-1 [86] und ist im ersten Ordner des *Model Repository* Pakets in Abbildung 3.2 zu sehen. Auf das *Harmonized Electricity Market Role Model* wird näher in 3.3.1 eingegangen. Die vorangegangenen Beschreibungen gewähren einen ersten Einblick in den Aufbau der Referenzarchitektur innerhalb der *SGAM Toolbox*.

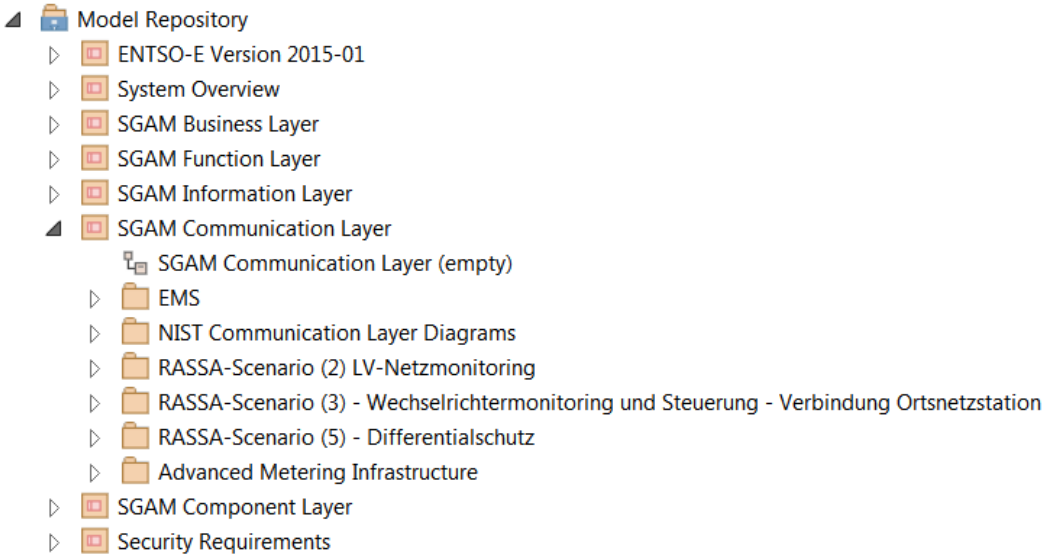



Abbildung 3.2: Einblick in Ordnerstruktur der RASSA-Referenzarchitektur (Screenshot von Enterprise Architect)

### 3.2.3 Bedeutung der Symbole

Einige der abgebildeten Symbole, die schon in 3.2.2 gezeigt wurden, sind durch Enterprise Architect selbst bestimmt, wie sie in der Projektstruktur in Abbildung3.2 zu sehen ist. Andere Symbole hingegen sind entweder durch die SGAM Toolbox definiert oder im Zuge der RASSA-Initiative entstanden. Dieser Abschnitt dient zur Erläuterung, um die Symbole der modellierten Elemente in den Abbildungen verständlicher zu machen.

#### SGAM Toolbox Symbole

Innerhalb der SGAM Toolbox gibt es zum einen die Grundelemente, welche durch die programmierte Erweiterung verfügbar sind. In Abbildung 3.3 sind diese nebeneinander dargestellt, wie sie in der installierbaren Version der SGAM Toolbox (Version 0.6.2) verfügbar und mit dem entsprechenden Namen des *Stereotypen* versehen sind. Stereotypes sind eine Möglichkeit, eine neue Art von Element zu definieren, die auf den vorhandenen Elementtypen von UML aufbauen um eine domänen- oder plattformspezifische Terminologie zu ermöglichen [87]. Diese können für Klassen, Beziehungen zwischen Elementen oder Pakete in Enterprise Architekt definiert werden und bieten so einen spezifischeren Zugang zu den Begriffen in der Smart-Grid-Domäne. Die in Abbildung 3.3 gezeigten SGAM Toolbox Elemente sind spezialisierte Stereotypen der Elementtypen *Actor* und *Node*. Die Elementtypen definieren die möglichen Optionen bei der Verknüpfung zu anderen Elementen, die innerhalb von Enterprise Architect durch ein Kontextmenü beim Ziehen eines Verbindungspfeils von einem Element zum anderen verfügbar sind.

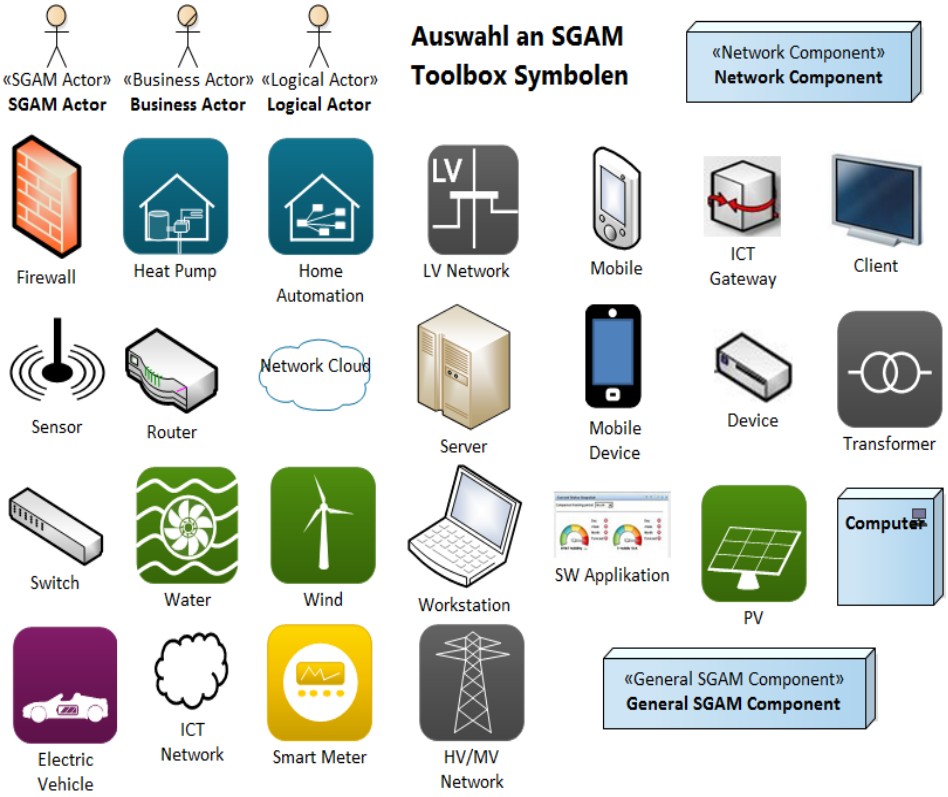



Abbildung 3.3: Zusammenstellung der verschiedenen SGAM Toolbox Symbole in der Downloadversion (Version 0.6.2)

### Symbole für das NIST LRM

Die Ausgangsgrundlage für die Referenzarchitektur ist das NISTIR LRM, welches als SGAM-Modell abgebildet ist. Dieses ist als Enterprise Architect Datei [88], sowie als Browserversion [89] verfügbar.

Abbildung 3.4 zeigt die SGAM Toolbox Elemente für die Domäne der *Customer Premises*, wie sie durch [46] definiert wurde. Zur Illustration von neuen Symbolen eignet sich das Symbol des *2 - Customer*, der in der verwendeten SGAM Toolbox Version (Version 0.6.2) nicht standardmäßig verfügbar ist. Die Abbildungen können über die Definition von neuen Stereotypen geschaffen sowie individualisiert werden und sind über das (lokale) Projekt in sogenannten *UML - Types* abgespeichert.

Die Nummerierung im Namen der Elemente geht ebenfalls auf [46] zurück und wurde als Konzept beibehalten. In Abbildung 3.4 wird zweimal das Symbol des Sensors für *11 - Water/Gas Metering* und *10 - Submeter (EUMD)* verwendet. Die jeweiligen Security-Requirements können sich stark unterscheiden, obwohl sich diese Elemente den selben Stereotyp teilen. Dieser Aspekt wird in 3.3.3 näher ausgeführt.

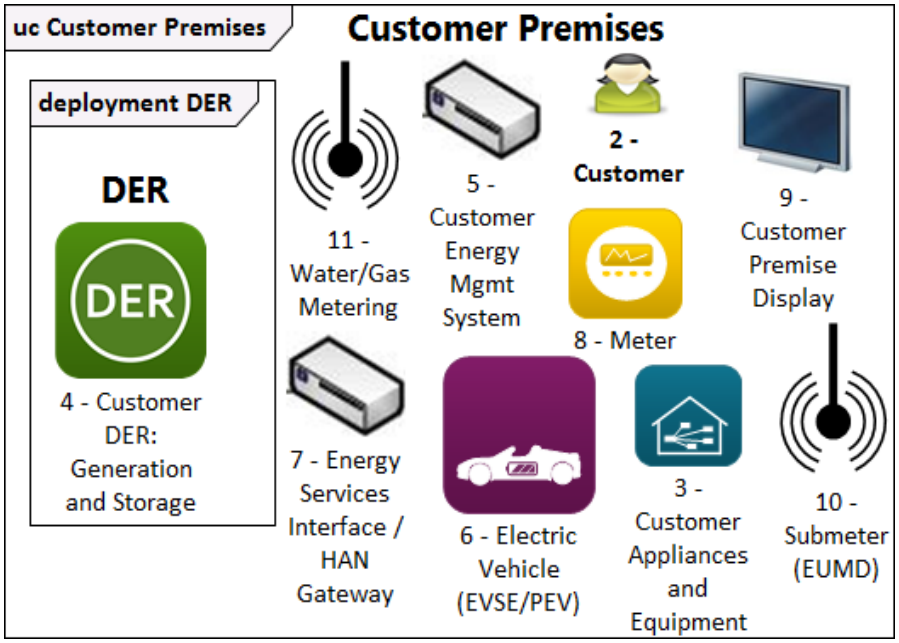



Abbildung 3.4: Screenshot der modellierten NISTIR 7628 Komponenten für die Domäne *Customer Premises*

## 3.3 Vorhandene Konzepte neu modelliert

Die in dieser Arbeit vorgestellten Konzepte wurden bislang nur textuell beschrieben oder zumindest nur öffentlich zugänglich gemacht. Aus diesem Grund werden die vorhandenen Konzepte, die für die Erarbeitung der Referenzarchitektur neu modelliert werden mussten, erläutert.

### 3.3.1 Harmonized Electricity Market Role Model

Ein Ausgangspunkt für die RASSA-Initiative war das sogenannte *Harmonized Electricity Market Role Model* der ENTSO-E. Dieses soll eine Erleichterung für den Dialog zwischen Marktteilnehmer_Innen zwischen unterschiedlichen Ländern durch eine eindeutige Rollen- und Domänendefinitionen darstellen [90]. Der Begriff der Domäne ist in diesem Modell frei übersetzt als *die Darstellung von abstrakten Objekten, die auf dem Strommarkt verwendet werden und für die Verwaltung verschiedener Prozesse, Ressourcen oder Bereiche erforderlich sind* [86]. So soll auch die gemeinsame Terminologie eine gemeinsame IT-Entwicklung ermöglichen. Daher war dieses Modell die Grundlage, um die Rollen und Domänen für den österreichischen Markt darzustellen.

Zu Beginn des RASSA-Architektur-Projekts gab es ein öffentlich zugängliches PDF-Dokument, welches die Version 2015-01 beschreibt [86]. Im Zuge der Kommunikation durch das RASSA-Projekt mit Verantwortlichen der ENTSO-E zwischen März und September 2017 wurde daraufhin eine Diagramm- sowie eine Browseransicht für die

Version 2014-01 online gestellt. Mittlerweile gibt es die Versionen 2017-01 und 2018-01 ebenso auf der Webseite [90]. Für die Version 2018-01 ist ein universelles Datenformat verfügbar, welches sich zum Beispiel in Enterprise Architect importieren lässt. So lassen sich mögliche Änderungen über ein solches Austauschformat besser kommunizieren und diskutieren, da eine direkte Ansicht innerhalb dieses Modellierungstools möglich ist.

Die Arbeiten im Zuge der RASSA-Initiative erstreckten sich auf die oben angeführte Version 2015-01 des *Harmonized Electricity Market Role Model*. Diese ist ausführlich in [86] beschrieben und behandelt im Wesentlichen die Beziehungen und Aufgaben in der europäischen Stromwirtschaft auf abstrahierter Ebene.

Die in dieser Arbeit auf Basis von [86] modellierte Version 2015-01 innerhalb des entworfenen RASSA-Modells ist in Abbildung 3.5 gegeben, welches aufgrund der Diagrammgröße nur in einem kleinen Ausschnitt dargestellt werden kann. Dort besitzt beispielsweise der Akteur *Meter Operator* (der Messstellenbetreiber) die Beziehung zu *Meter* (Stromzähler) mit der Aufgabe, diese zu betreiben und zu warten. Ebenso ist die Multiplizität im Diagramm dargestellt, welche in diesem Beispiel besagt, dass der *Meter Operator* mindestens einen oder mehrere *Meter* betreibt und wartet.

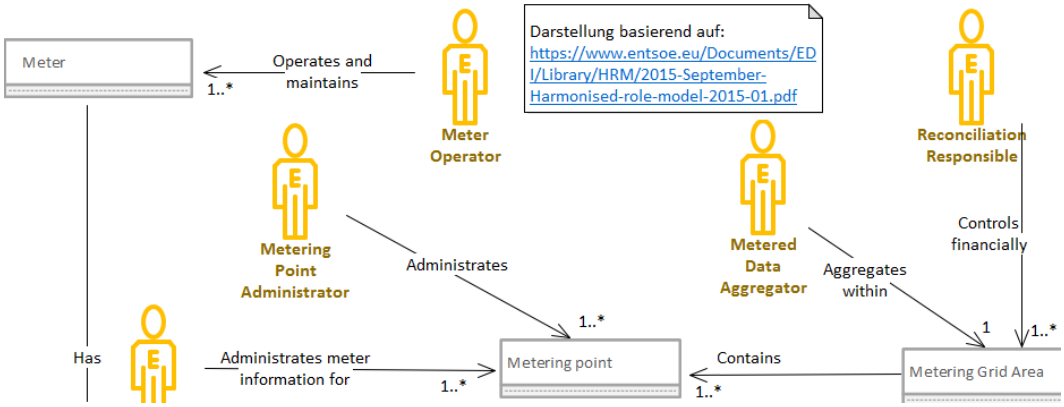



Abbildung 3.5: Ausschnitt des in der eingepflegten ENTSO-E Harmonized Electricity Market Role Model (Version 2015-1)

Das so angefertigte Modell ist in der Referenzarchitektur im Ordner *ENTSO-E Version 2015-01* zur Verwendung hinterlegt, welcher an erster Stelle innerhalb des *Model Repository* aus Abbildung 3.2 steht.

Aufgrund der Tatsache, dass es sich um ein Modell in Enterprise Architect handelt, wurden die Standard-Aktore (Strichmännchen) in Abbildung 3.5 durch einen eigenen Stereotyp mit der Darstellung als gelbe Strichmännchen-ähnliche Figuren mit einem “E” (stellvertretend für ENTSO-E) versehen, sodass die Herkunft der modellierten Informationen klar dokumentiert ist.

Die anderen Symbole, wie zum Beispiel die des *Meter* wurden ähnlich gestaltet, wie sie in dem Dokument [86] der ENTSO-E dargestellt wurden. Ausgehend von diesem

Modell konnte die österreichische Marktsituation modelliert, diskutiert und adaptiert werden. Die dafür notwendigen Änderungen in der symbolischen Darstellung sind in 3.4.3 entsprechend beschrieben.

### 3.3.2 Domänenmodell .AT

Im Bericht [91] wurden die NISTIR-Richtlinien für eine Gefahrenidentifikation herangezogen. Dabei wurden sieben Bereichsgruppen abgeleitet. Diese bilden das *Domänenmodell .AT* mit insgesamt 58 unterschiedlichen Elementen, die in [91] als *funktionale Einheiten* bezeichnet werden. Zur Veranschaulichung zeigt Abbildung 3.6 modellierte beispielhafte *funktionalen Einheiten* des Domänenmodell .ATs. Die Form und Farbgebung der Elemente stammen ursprünglich aus den NIST LRM Diagrammen zu den sogenannten *Logical Interface Categories* [46], auf die in 3.3.3 genauer eingegangen wird.

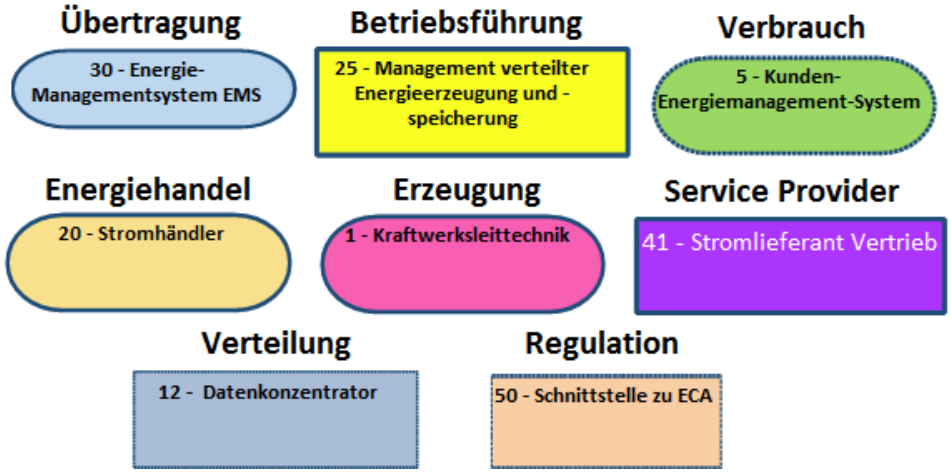



Abbildung 3.6: Beispiele von funktionalen Einheiten des Domänenmodells .AT und deren Bereichszuordnung

Der Bereich der *Regulation* und der Rolle *50 - Schnittstelle zu ECA* wurden neu geschaffen, da diese nicht im NIST LRM vorhanden sind. Zusätzlich sind die *funktionalen Einheiten* in dem Risikoanalysebericht [91] übersetzt worden, wie es in Abbildung 3.6 zum Beispiel an dem Element *20 - Stromhändler* links in der Mitte unter dem Bereich *Energiehandel* zu sehen ist. Nach der RASSA-Methodik wurden die Elemente durch die UML-Generalisierung mit den jeweiligen Ursprungselementen aus dem NIST LRM verbunden. Die vorangestellten Zahlen lassen den ursprünglichen Akteur leicht wiedererkennen und diese Designentscheidung durch [91] wurde auch im Modell beibehalten. Das komplette Domänenmodell .AT ist in Abbildung 3.7 zu finden. Um den *20 - Stromhändler* als Beispiel noch einmal aufzugreifen, ist in [91] eine Kurzbeschreibung der funktionalen Einheiten angeführt. Für das Beispielelement lautet diese »Stromhändler. Eine natürliche oder juristische Person oder Erwerbsgesellschaft, die Elektrizität in Gewinnabsicht verkauft« [91, S. 45].

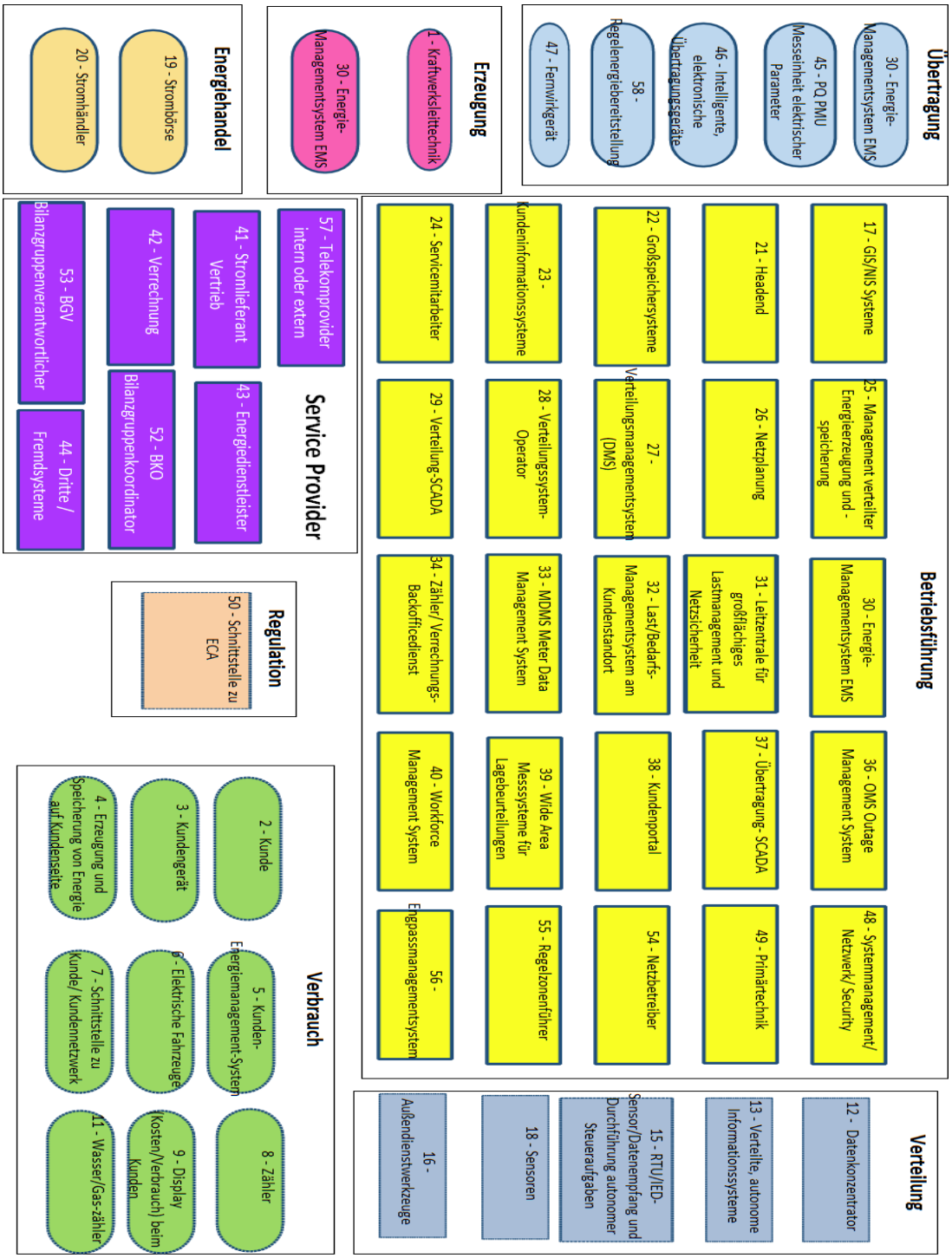



Abbildung 3.7: Modellversion des *Domänenmodell .AT* mit 58 unterschiedlichen funktionalen Einheiten und sieben Bereichsgruppen

### 3.3.3 NIST LRM Modell

Nachfolgend wird auf die Konzepte des downloadbaren NIST LRM Modells [88] eingegangen. Das Modell kann auf der Webseite ohne Enterprise Architect betrachtet werden [89]. In Abbildung 3.8 ist das Diagramm der *Logical Interface Categorie 16* dargestellt.

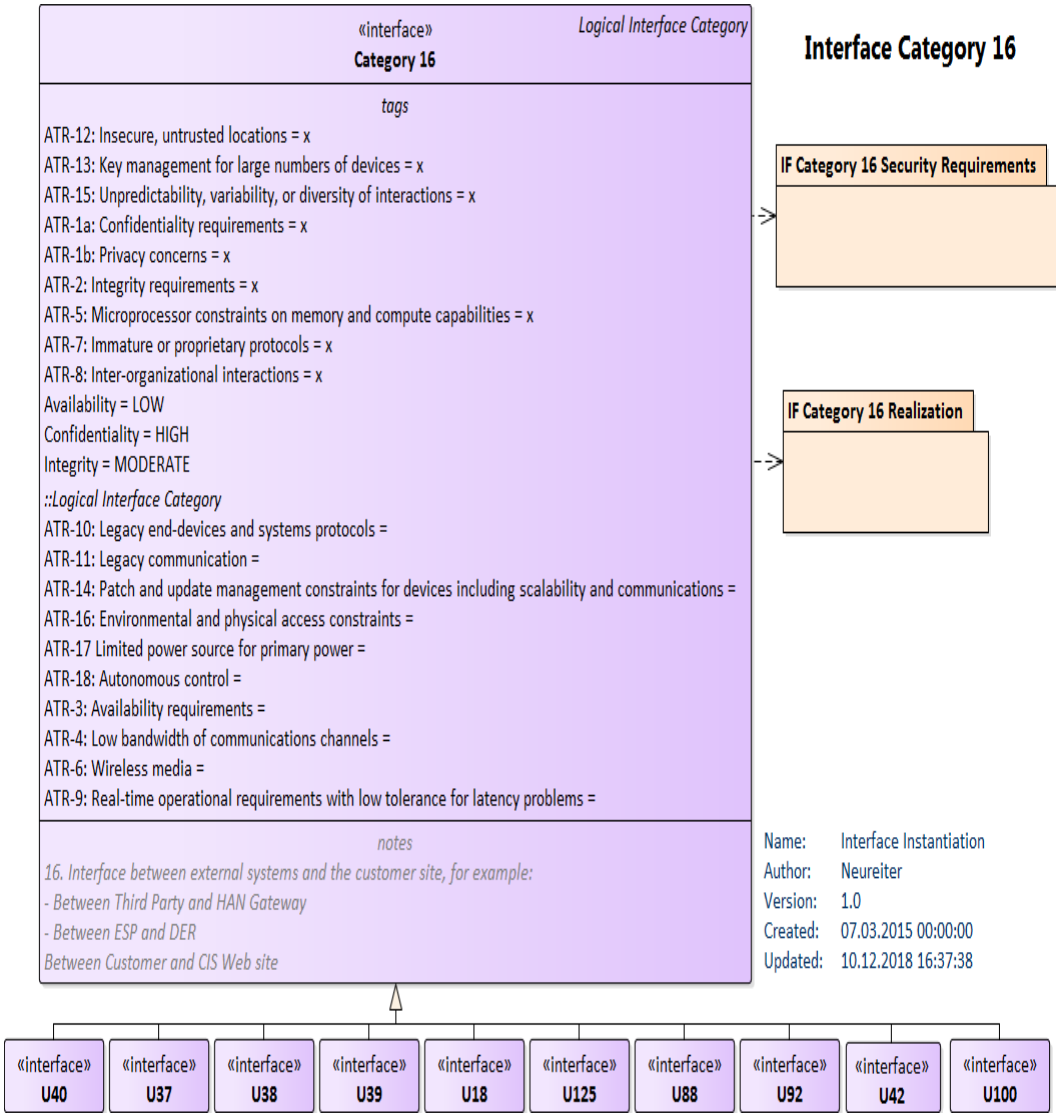



Abbildung 3.8: Screenshot der *Category 16* des NIST LRM, Autor: Christian Neureiter

Im Element *Category 16* sind die *CIA*-Werte für diese Kategorie angegeben, in diesem Fall wurde die Kategorie mit *HIGH* für *Confidentiality*, *MODERATE* für *Integrity* und *LOW* für *Availability* eingestuft. Darüber hinaus befinden sich zutreffende Sicherheitsattribute in den *Tags* des Elements. Durch *Tags* können Informationen mit einem Element verknüpft werden und lassen eine höhere Flexibilität bei der Strukur zu.

Im Beispiel der *Category 16* ist das erste Sicherheitsattribute *ATR-12: Insecure, untrusted locations* mit einem *X* gekenntzeichnet, was bedeutet, dass dieses Attribut für die Kategorie zutrifft [16]. Weiter unten in der Elementbeschreibung befinden sich weitere Sicherheitsattribute, die aber im Falle der *Category 16* nicht zutreffend sind. Sie werden aber im Enterprise Architect durch eine *Generalize*-Beziehung zu dem Elternelement *Logical Interface Categorie* dargestellt. Im unteren Teil des *Category 16*-Elements sind die näheren Beschreibungen zu der Kategorie gegeben, welche in diesem Fall die Schnittstellen zwischen externen Systemen und dem Kundenstandort miteinbezieht.

In Abbildung 3.8 sind unten 10 Schnittstellen-Elemente als Spezialisierung der *Category 16* zu sehen. Durch die Generalisierungsbeziehung hat jedes einzelne der *UXX*-Elemente die Informationen des *Categorie 16* und die dazugehörigen Security Requirements, die auf der rechten Seite der Abbildung mit einer Abhängigkeitsbeziehung in einem Enterprise Architect Paket spezifisch für die Kategorie 16 enthalten sind, wie sie von NIST spezifiziert wurden [46]. In der unten gezeigten Abbildung 3.9 ist ein Auschnitt der Security Requirements von Kategorie 16 gezeigt. Die Darstellung basiert auf [89], wurde aber für eine leserliche Darstellung neu angeordnet.

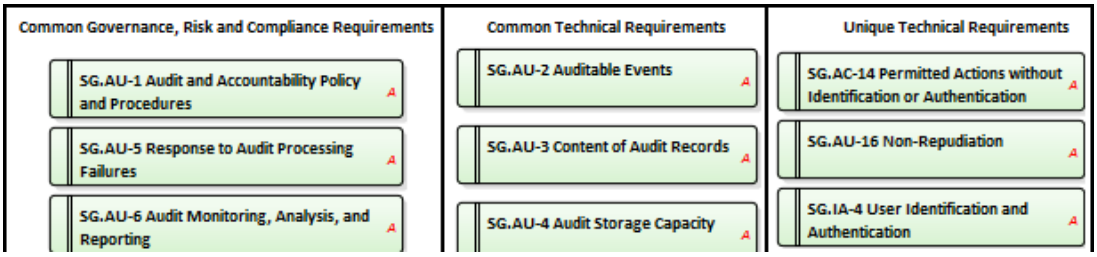


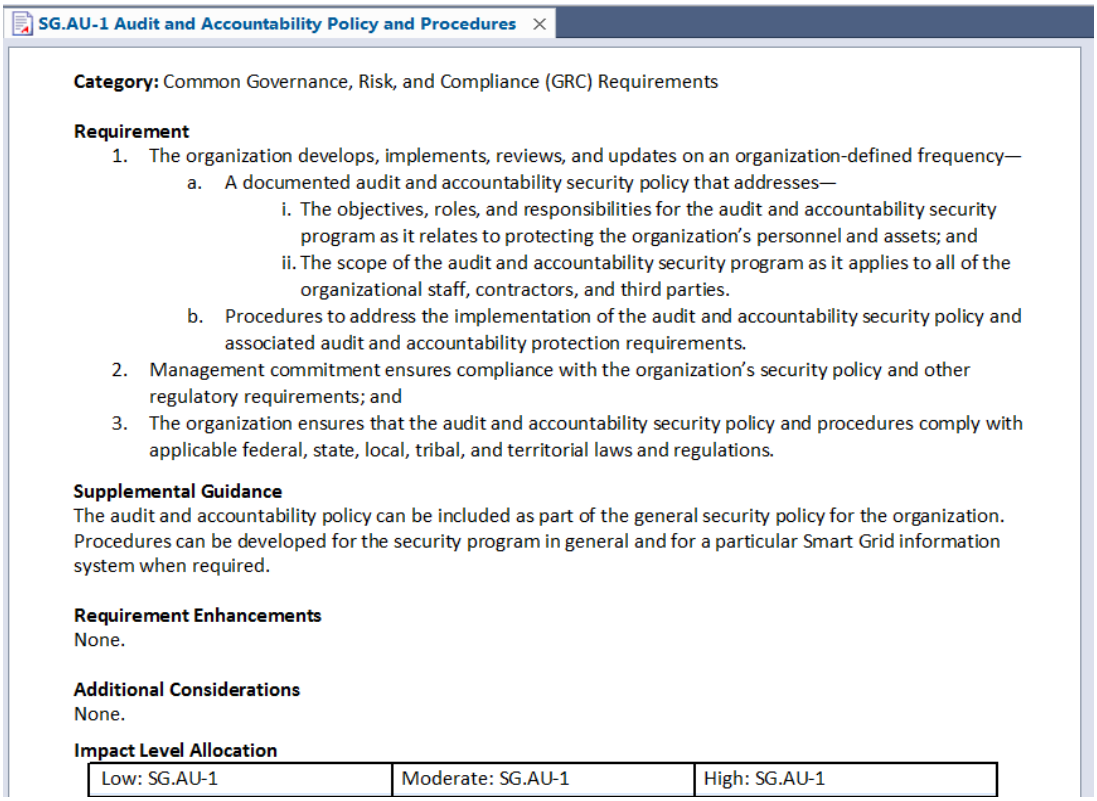

Abbildung 3.9: Ausschnitt der Security Requirements von Kategorie 16 [89]

Die einzelnen Security Requirements sind jeweils mit der Beschreibung aus [46] in einem verlinkten Dokumentsabschnitt in Enterprise Architect einsehbar. Das Vorhandensein eines verlinkten Dokuments ist durch das kleine rote Zeichen im Element gekennzeichnet. So kann die Verlinkung des ersten Elements links oben aus der Abbildung 3.9 *SG.AU-1 Audit and Accountability Policy and Procedures* in Abbildung 3.10 eingesehen werden.

Darin sind sieben verschiedene Informationen enthalten [46]. Als erstes, ein eindeutiger Name (in Fall der Abbildung 3.9 oben als geöffneter Reiter zu sehen). Als zweites *Category*, um welche Art von Security Requirements es sich handelt. Als drittes beschreiben hier *Requirement* die Security-bezogenen Aktivitäten oder Aktionen, die von einem Unternehmen, einer Organisation oder dem System selbst durchgeführt werden müssen.

Als viertes sind *Supplemental Guidance* als zusätzliche Anleitungen zu verstehen, die zum Verständnis der Security Requirements beitragen sollen. In den *Requirement Enhancements* (sofern vorhanden) sind Erweiterungen zu den Security Requirements gelistet, wenn es die damit verbundene Komponente einen erhöhten Schutz benötigt. Die *Additional Considerations* beschreiben zusätzliche Möglichkeiten, die von der Organisation umgesetzt werden sollten aber keine spezielle Security Requirement darstellt. Als siebtes ist der

*Impact Level Allocation* stellvertretend für die Einordnung der Auswirkung bei Eintreten eines Ausfalls. Diese sollten jeweils von der implementierenden Organisation in einem Bewertungsprozess überprüft werden.


SG.AU-1 Audit and Accountability Policy and Procedures

**Category:** Common Governance, Risk, and Compliance (GRC) Requirements

**Requirement**

1. The organization develops, implements, reviews, and updates on an organization-defined frequency—
   a. A documented audit and accountability security policy that addresses—
      i. The objectives, roles, and responsibilities for the audit and accountability security program as it relates to protecting the organization's personnel and assets; and
      ii. The scope of the audit and accountability security program as it applies to all of the organizational staff, contractors, and third parties.
   b. Procedures to address the implementation of the audit and accountability security policy and associated audit and accountability protection requirements.
2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and
3. The organization ensures that the audit and accountability security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.

**Supplemental Guidance**
The audit and accountability policy can be included as part of the general security policy for the organization. Procedures can be developed for the security program in general and for a particular Smart Grid information system when required.

**Requirement Enhancements**
None.

**Additional Considerations**
None.

**Impact Level Allocation**

| Low: SG.AU-1 | Moderate: SG.AU-1 | High: SG.AU-1 |
|---|---|---|

Abbildung 3.10: Screenshot des verlinktes Dokuments, Quelle des Textes: [46, S. 107]

### 3.3.4 Konzept der Referenzarchitektur RASSA

Das Konzept der Referenzarchitektur RASSA besteht aus einer verknüpften Auswahl für Österreich relevanter, komplexer Modelle. Um eine Referenzarchitektur zu entwickeln werden eine Reihe von unterschiedlichen Spezifikationen und Informationsquellen benötigt. Als Voraussetzung für die Diskussion und Evaluierung mit Stakeholdern mussten diese allerdings erst modelliert vorliegen um später genutzt werden zu können. In die Referenzarchitektur sind deswegen folgende Inhalte eingepflegt:

- NIST LRM: Akteure, Interfaces, Interface Kategorien, Security Requirements (Modelliert durch die Mitarbeiter von [92]) und deren Mapping auf SGAM gemäß Mandat M490 [6]
- *Harmonized Electricity Market Role Model* der ENTSO-E, Version 2015-01 [86]
- NIST Cyber Security Framework Core modelliert nach [93]

- Gefahrenkatalog der Risikoanalyse für die Informationssysteme der Elektrizitätswirtschaft [91]
- Domänenmodell .AT [91]
- Anforderungskatalog Smart Meter Ende-zu-Ende Sicherheit nach [94]
- Smart Grids Standards Map [61]
- Detailliertes und kompaktes RASSA-Marktrollenmodell für Österreich [8]

Die aufgelisteten Quellen und deren Modellierung in der Referenzarchitektur RASSA sind in 3.11 schematisch dargestellt. Hierbei ist die Zuordnung der Informationen in den jeweiligen Interoperabilitässchichten gekennzeichnet. Ein Doppelpfeil bedeutet, dass hierbei immer wieder Gespräche und Überarbeitungen stattgefunden haben, vor allem in Hinsicht auf den Bezug zu Österreich (dargestellt durch die eingezeichnete Flagge). Ein einfacher Pfeil bedeutet die Durchführung der Modellierung. Diese wurden nach und nach im Rahmen der RASSA-Initiative eingearbeitet und dem Konsortiums oder Stakeholdern in mehreren Projekt-internen und externen Workshops zur Diskussion präsentiert. Das Prinzip ist in einigen wissenschaftlichen Publikationen mehreren Peer-Review Prozessen unterzogen worden [95, 13, 69].

[96]

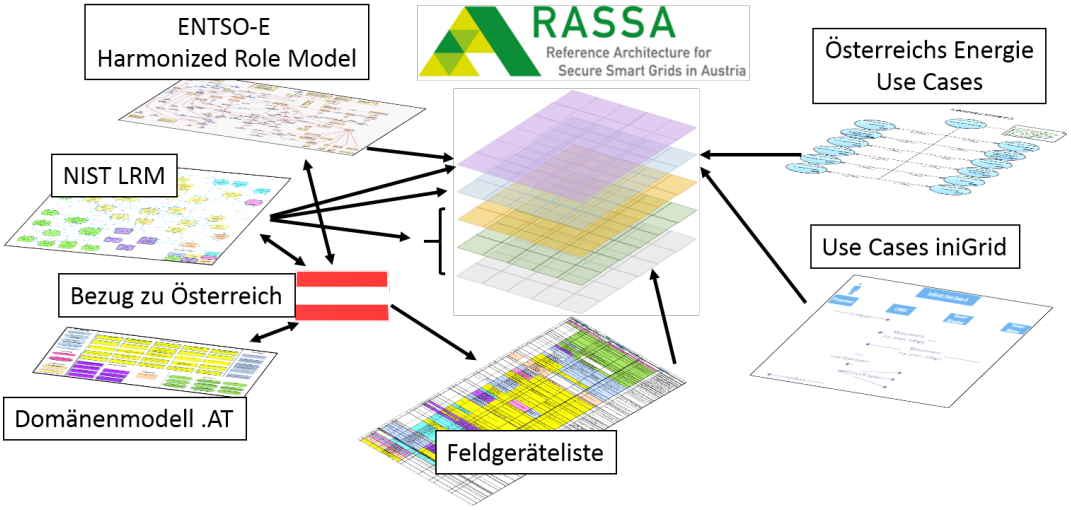



Abbildung 3.11: Eigene Darstellung des Konzepts der Referenzarchitektur RASSA aufbauend auf [10]

Die Feldgeräteliste ist ein Dokument, das durch das RASSA-Konsortium erarbeitet wurde. Anhand dessen wurde das Konzept der RASSA-Methode, wie sie hier vorgestellt ist, in einer Microsoft Excel Tabelle erarbeitet. Im Wesentlichen fand hier die Aufzählung der NIST-Elemente statt, die dann dem Domänenmodell .AT gegenübergestellt wurden.

Auch die Domänenzuordnung, ob ein Element zum Beispiel der Domäne *Betriebsführung* zuzuordnen ist, wurde hier berücksichtigt. Auch Informations- und Erklärungstexte für die Zuordnung oder die genauen Aufgaben des jeweiligen Elements sind hier aufgeführt. Die Feldgeräteliste definiert auch, ob es sich um *Business Akteur*, *Logischer Akteur* oder eine *Physische Komponente* handelt. In 3.4.3 werden diese Begriffe näher erläutert. Der Grund für diese Kategorisierung ist die notwendige Berücksichtigung der UML-Typen und die Zuordnung anhand des SGAM.

## 3.4 Entwickelte Smart-Grid-Lösungen in iniGrid

Das Projekt *Integration of Innovative Distributed Sensors and Actuators in Smart Grids (Integration innovativer verteilter Sensoren und Aktuatoren in Smart Grids)* (iniGrid) versuchte die Energieverteilung bis zum Verbraucher durch innovative Sensorik und Aktorik für aktiv betriebene Verteilnetze durch Schlüsselinnovationen (Smart Breaker, Mittelsspannungssensor) zu verbessern. Desweiteren wurde in diesem Projekt untersucht, wie neue Smart-Grid-Anwendungen umgesetzt werden können, die sich durch diese neuen Komponenten ergeben können.

Die Beschreibung dieser neu ermöglichten Smart-Grid-Anwendungen durch Use Cases können für die RASSA-Initiative als Evaluierungsbeispiel herangezogen werden und sind daher hier näher ausgeführt. In der Anfangsphase wurden fünf Use Cases definiert, welche im Laufe des Projekts weiter zusammengefasst werden konnten. Der erste Use Case umfasst das Energiemanagement auf Prosumer-Ebene, wobei ein *Prosumer* ein Energiekonsument und ein Energieerzeuger zugleich ist. Der zweite Use Case behandelt eine Optimierung des Niederspannungsnetzes. Der dritte und vierte Use Case beschreiben die Mittelspannungsoptimierung aus der Sicht eines Ortsnetzstransformators und des Netzoperators. Im Laufe des Projekts hat sich herausgestellt, dass sich diese zwei Use Cases nur in der Perspektive unterscheiden. Es sind die selben Akteure notwendig, was eine Zusammenfassung der Use Cases zulässt. Der letzte Use Case beschreibt die anderen Use Cases in einem Gesamtbild, somit ist eine weitere nähere Betrachtung als redundant anzusehen. In dieser Arbeit wird der erste Use Case als repräsentatives Beispiel herangezogen, da sich mit diesem die Vorgehensweise ausreichend belegen lässt.

### 3.4.1 Use Case A: Home/Commercial Energy Management

Use Case A: *Home/Commercial Energy Management* ist der erste Use Case des iniGrid-Projekts. Er beinhaltet noch keine Netzwechselwirkung und stellt somit ein typisches lokales Optimierungsszenario da, welches eine lokale Steuerung erfordert, um die Funktionen von Smart Breakers und Smart Meter zu nutzen, den Verbrauch durch den Endanwender_innen lokal auf ein definiertes Ziel hin zu optimieren. Es wird davon ausgegangen, dass die Smart Breakers in diesem Use Case eine beliebige Anzahl von Gerätetypen steuern können. Da das Szenario in einem *Prosumer*-Setup definiert ist, wird erwartet, dass die Smart Breaker entweder Lasten oder Erzeuger wie etwa Batterien und Photovoltaik hinzu- oder wegschalten können.

In Abbildung 3.12 ist das Sequenzdiagramm von Use Case A: *Home/Commercial Energy Management* dargestellt. Die Grafik ist an eine Darstellung aus dem Konsortium des iniGrid-Projekts angelehnt [97]. In diesem vereinfachten Sequenzdiagramm ist der erste Schritt des Prosumers mit der Konfiguration des *Customer Energy Management System (Kundenenergiemanagementsystem)* (CEMS) angegeben. Das CEMS erhält von den in iniGrid neu entwickelten Smart Breakern Messwerte wie zum Beispiel die Spannung und Stromstärke. *Smart Breaker* sind die in iniGrid neuentwickelten intelligenten fernsteuerbaren Stromschutzschalter durch Halbleitertechnik mit integrierten Messsensoren, die eine Reihe von wichtigen Funktionen mit nur einem Gerät erfüllen:

- Messungen (Ampere, Spannung, Leistung,...)
- Statuskontrolle (An/Aus/Ausgelöst)
- Schutz gegen Über- und Unterspannung sowie Kurzschlüsse
- Bietet Erdschlussschutz, Personenschutz, und Phasenschutz
- Schnelles Bypass-Relais ($< 200\mu$s) für 45 und 125 Ampere [4]

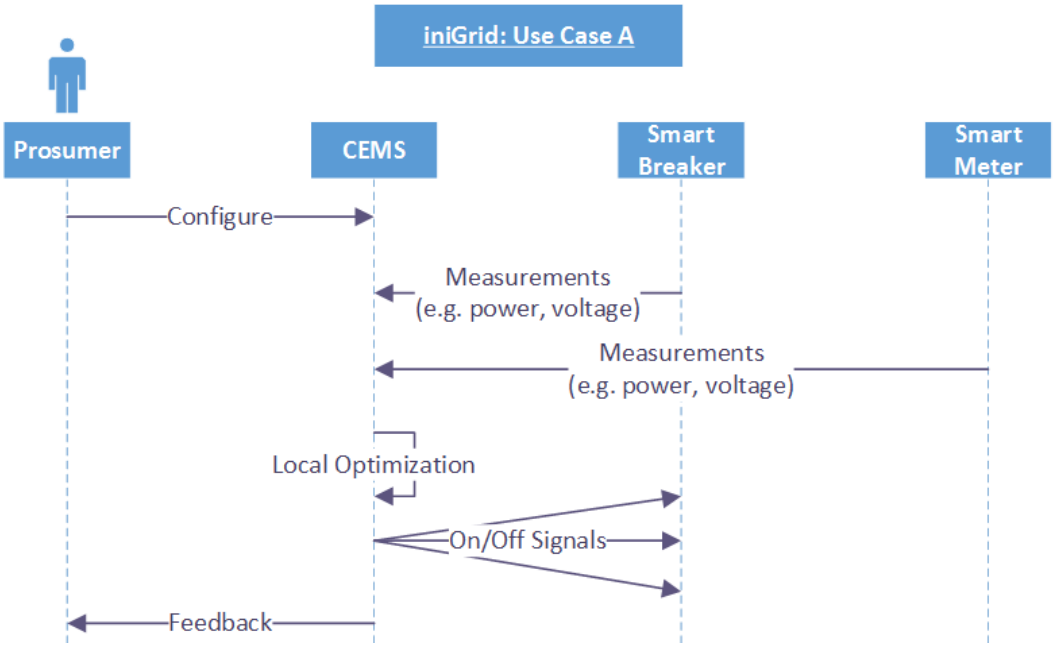



Abbildung 3.12: iniGrid Use Case A: Vereinfachtes Sequenzdiagramm basierend auf [97]

Der *Smart Meter* ist ein moderner Stromzähler, der Daten empfangen und senden kann. Das *CEMS* ist ein Konfigurations- und Kundenportal zur Steuerung der Endgeräte und Ablesung des aktuellen Verbrauchs und der Kosten. Der *Prosumer* kann das *CEMS* nach den persönlichen Vorlieben konfigurieren. Dieses erhält sowohl vom *Smart Meter* als

auch den *Smart Breakern* Messwerte über die lokale Spannung und Leistung. Das *CEMS* optimiert anhand dieser Daten den Verbrauch und sendet Schaltsignale an die *Smart Breaker*. Anschließend wird der *Prosumer* über das *CEMS* über den aktuellen Stand informiert.

Die Modellierung im NIST LRM ist in 4.2.1 beschrieben, um im Anschluss auf die Schwächen des Ausgangsmodells eingehen zu können. In 4.2.4 wird der Use Case in der Referenzarchitektur vorgestellt.

### 3.4.2 Verortung im Domänenmodell .AT

Der Bericht [91] stellt primär eine Risikoanalyse dar. In diesem wurden sowohl das Domänenmodell .AT definiert als auch ein Gefahrenkatalog mit insgesamt 114 Einzelgefahren erarbeitet.

Der Gefahrenkatalog ordnet die Gefahren in einem oder mehreren der 15 identifizierten Gefahrenfelder zu. Wie diese Gefahrenfelder definiert wurden, zeigt folgender Ausschnitt aus [91]:

- »Gefahrenfeld I: Maschinen-Maschinen Kommunikation mit/ und /oder hohem Rechenaufwand/ und/ oder Bandbreitenanforderung« [91, S. 25]
- »Gefahrenfeld II: Gefahren an der Schnittstelle Steuerungs- und Kontrollsysteme innerhalb einer Organisation« [91, S. 25]
- »Gefahrenfeld X: Gefahren, die sich aus der Nutzung externer Systeme ableiten lassen, die eine „direkte“ Beziehung zum Endverbraucher haben« [91, S. 25]

Der Aufbau des Gefahrenkatalogs wird anhand von zwei Einzelgefahren beschrieben. So lässt sich die Gefahr 1 »Gefahr einer absichtlichen, aber nicht autorisierten Auslösung von Schalthandlungen, die keine User Identifizierung oder Authentifizierung benötigen« [91, S. 28] den Gefahrenfeldern, I, II und III zuordnen, Gefahr 2 »Gefahr, dass Unbefugte Zugang zu nicht privilegierten Remote-Access-Accounts, LAN- Accounts mit Privilegien oder Remote- Access- LAN- Accounts mit Privilegien erhalten« [91, S. 28] jedem Gefahrenfeld ausser VII und XIII. Im Anhang des Dokuments sind die Einzelgefahren gelistet, allerdings nur mit ihrer Gefahrenbeschreibung ohne die Zuordnung. Diese wurde wohl bewusst aufgrund von Sicherheitsbedenken nicht öffentlich zugänglich gemacht.

Die Verortung der iniGrid Use Cases bringt daher hier keinen Mehrwert für die Endnutzer_innen, sofern man sich auf die alleinige Ausgangslage des Domänenmodell .AT und der (öffentlich) nicht zugeordneten Einzelgefahren stützt. Des weiteren fehlt eine Zuordnung der Gefahren zu den jeweiligen *funktionalen Einheiten*. Aus diesem Grund empfiehlt es sich die vorgeschlagene Herangehensweise aus 3.3.4 anzuwenden.

### 3.4.3 Definition von neuen RASSA-Symbolen

Bei der Darstellung des Domänenmodell .AT sind allerdings Informationen, die für die Darstellung von Use Cases im SGAM-Kontext wichtig wären, verloren gegangen. Anhand der Darstellung kann im Domänenmodell .AT nicht unterschieden werden, ob es sich bei einem Element um eine echte (physische) Komponente handelt oder nicht. Ob es sich bei einem Element um eine juristische Person (im rechtlichen Kontext) wie beispielsweise einen Kunden handelt, lässt sich durch die Elementdarstellung im Domänenmodell .AT nur durch den Wortlaut erfassen [98]. Daher wurde für die RASSA-Referenzarchitektur die Darstellung weiter differenziert und in folgende Kategorien unterteilt:

- Business-Akteure
- Logische Akteure (Systeme)
- Physische Komponente

Diese Unterteilung und Zuordnung der unterschiedlichen funktionalen Einheiten beruht auf den Arbeiten innerhalb der RASSA-Initiative, in der andere Sichtweisen und länderspezifische Zuordnungen festgelegt und begründet sind. Die Darstellung in Abbildung 3.13 zeigt die Symbole der unterschiedlichen Kategorien und gleichzeitig die Zugehörigkeit zu einer Domäne. Diese ist als *Tag* im Element speicherbar. Auf der linken Seite der Darstellung sind drei Akteure zusammengestellt als Repräsentation einer *Party with multiple actors*. Dieses Element dient für die Zusammenfassung von Akteuren unter einer Identität, die im österreichischen Markt mehrere Funktionen nach dem *Harmonized Electricity Market Role Model* einnehmen (näher erläutert in 4.1.2) und so visuell den Nutzer_innen darüber Informationen auf den ersten Blick gibt. Das zweite Symbol repräsentiert einen Business-Akteur, in diesem Fall *2 - Kunde*, bei dem in der Darstellung als Figur ersichtlich sein soll, dass es sich um eine Person, natürlich oder juristisch, im rechtlichen Kontext handelt.

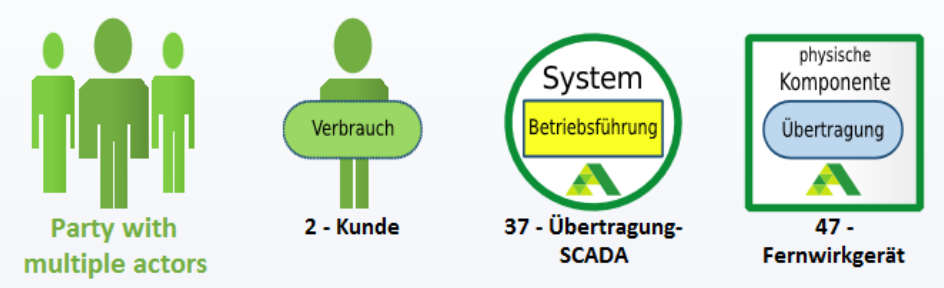



Abbildung 3.13: Die verschiedenen RASSA Symbole mit eingebetteter Domänenzuordnung

Die logischen Akteure (gewählter Stereotyp in Enterprise Architect) und die Bezeichnung *System* benötigen eine intensivere Erklärung. Die Darstellung des System-Elements *37 - Übertragung-SCADA* aus Abbildung 3.13 soll auf ein komplexes Gesamtsystem

hindeuten. So ein System kann seine Funktion nicht als einzelne physische Komponente beziehungsweise Endgerät erfüllen, sondern nur als Zusammenschluss von diesen zu einem System, da die vorgesehene Funktion erfüllen kann. Innerhalb der Elementdefinition von Enterprise Architect sind diese System-Elemente allerdings als logische Akteure abgebildet. Diese Zuordnung ist durch die Feldgeräteliste des RASSA-Konsortiums entstanden. In 5.1 wird auf die Herkunft der Feldgeräteliste nochmals eingegangen.

Die Darstellung der physischen Komponenten wurde, wie rechts in Abbildung 3.13 zu sehen ist, eckig gewählt und angefertigt. Die in Abbildung 3.13 präsentierten Symbole wurden von mir mithilfe der sogenannten *Shape Scripts*, einer Skriptsprache zur Elementdarstellung in Enterprise Architect, entworfen und beruhen auf Konzeptvorschlägen[1].

[1]Konzeptvorschläge zur grafischen Gestaltung der RASSA Symbole wurden von Marcus Meisel entworfen

KAPITEL 4

# Evaluierung der iniGrid-Modellierung in der Referenzarchitektur

In diesem Kapitel wird zuerst das Beispiel des europäischen Marktrollenmodells herangezogen und einer österreichischen Version gegenüber gestellt. Im Anschluss daran wird auf die Modellierung der iniGrid Use Cases näher eingegangen und diese anhand von bestehenden Konzepten erläutert und evaluiert.

Anhand der Modellierung der iniGrid Use Cases mittels RASSA werden die verwendbaren Dokumentationsmöglichkeiten für Berichte aufgezeigt. Darüber hinaus wird auf die möglichen Anwendungen anhand einer Auswahl an Analysetools näher eingegangen, welche durch die Struktur der RASSA Referenzarchitektur möglich ist. Abschließend werden die Erkenntnisse aus Stakeholdergesprächen über die mögliche Verwendung und Limitierungen der Referenzarchitektur beschrieben.

## 4.1 Evaluierung der Marktrollenmodelle für Europa und Österreich

Im Folgenden Abschnitt wird das Marktrollenmodell für Europa beschrieben und erläutert die Überführungen in eine Version für Österreich.

### 4.1.1 Harmonized Electricity Market Role Model (ENTSO-E)

In 3.3.1 ist das Konzept und die Neumodellierung des *Harmonized Electricity Market Role Model* der ENTSO-E Version 2015-01 vorgestellt. Die neue Version 2018-01 des Modells konnte aufgrund des Vertragsendes des RASSA-Architektur-Konsortiums zum

Projektende keine weitere Iteration des Marktrollenmodells für Österreich mit den Stakeholdern erfahren. Diese kann stattdessen unter [99] oder als importierbare Datei für Enterprise Architect [100] betrachtet werden.

Abbildung A.3 im Anhang zeigt das finale modellierte Rollenmodell nach Version 2015-01. Die Elementanordnung ist der Darstellung aus [86] nachempfunden.

### 4.1.2 Harmonized Electricity Market Role Model für Österreich

Das europäische Energienetz erstreckt sich über viele unterschiedliche Breiten- und Längengrade, Nationen und Kulturen. Selbst in den Ländern mit annähernd gleichen Landessprachen (Deutschland, Schweiz, Österreich) gibt es große Unterschiede in der rechtlichen und regulatorischen Auslegung von internationalen Empfehlungen. Um die Versorgungssicherheit aufrechtzuerhalten, wurde der Verband Europäischer Übertragungsnetzbetreiber ENTSO-E eingerichtet und deren Aufgaben im Jahr 2009 im dritten Energiepaket der Europäischen Union gesetzlich festhalten sind [101].

Eine der Entwicklungen zur Unterstützung der internationalen Kommunikation mit einer einheitlichen Terminologie war das *Harmonized Electricity Market Role Model* [86]. Als Versuch, den österreichischen Markt auf Basis der EU-Vorlage modellieren zu können, wurden aufgrund der Komplexität wurde in zwei Schritten ein Modell des österreichischen *Harmonized Electricity Market Role Models* mit unterschiedlichen Darstellungen für RASSA geschaffen.


Abbildung 4.1: Screenshot von hinterlegten Informationen des *Messstellenbetreibers* im erweiterten RASSA-Marktrollenmodell für Österreich

Abbildung A.4 im Anhang gibt dabei den detaillierten Einblick in die Interaktion und Rollenverteilung für Österreich. Es handelt sich hierbei um eine Anpassung an den österreichischen Markt, der mit nahezu alle Akteure des ENSTO-E Modells beinhaltet. Die großen Umrandungen mit der Beschriftung wie links oben der *Netzbetreiber* enthält mehrere andere Akteure und die Beziehungen untereinander. Abbildung 4.1 zeigt aus dieser Modelldarstellung die Rolle des *Messstellenbetreibers* (im *Harmonized Electricity Market Role Model* mit *Meter Operator* bezeichnet) und die zugehörigen Relationen. Auf der rechten Seite der Abbildung ist der *Meter Operator* zu sehen, der durch die *Generalizes*-Beziehung Informationen an die Rolle des *Messstellenbetreibers* vererbt.

Eine weitere Besonderheit in diesem Modell ist die Notiz *„In Deutschland“*, die mit dem *Messstellenbetreiber* verbunden ist. In Österreich übernimmt der Netzbetreiber die Tätigkeit der durch die *ENTSO-E* definierten Aufgabe einen Zähler zu betreiben und warten. In Deutschland ist dies eine ausgegliederte Aufgabe, bei der die Endkonsumenten den Messstellenbetreiber auf Wunsch auch wechseln können.

Tabelle 4.1 ist die Aufteilung der von ENTSO-E definierten Domänen und dem korrespondierenden österreichischen Element. Etwaige Unterschiede sind auf der rechten Seite hervorgehoben. Ein großer Block zeigt keinen Unterschied und die Bezeichnung in der Tabelle bleibt englischsprachig. In den Treffen mit den Stakeholdern wurde kommuniziert, dass die Bezeichnungen (sofern sie Englisch sind) diese auch so in der Praxis Verwendung finden oder keine passende Übersetzung bekannt ist.

Tabelle 4.1: Vergleich der Domänen des ENTSO-E & RASSA Modell [8].

| **ENTSO-E** | **Österreichisches Modell** | **Unterschiede** |
|---|---|---|
| Accounting Point | Accounting Point | Identisch |
| Allocated Capacity Area | Allocated Capacity Area | |
| Capacity Market Area | Capacity Market Area | |
| Common Capacity Area | Common Capacity Area | |
| Control Block | Control Block | |
| Coordination Center Zone | Coordination Center Zone | |
| ITC | ITC | |
| Market Area | Market Area | |
| Metering Grid Area | Metering Grid Area | |
| Register | Register | |
| Reserve Resource | Reserve Resource | |
| RGCE Interconnected Group | RGCE Interconnected Group | |
| Balance Group | Bilanzgruppe | Name unterschiedlich |
| Control Area Center Zone | Regelzone | |
| Control Entity | Steuereinheit | |
| Local Market Area | Strombörse | |
| Market Balance Area | Verrechnungsstelle | |
| Meter | Zähler | |
| Metering point | Zählpunkt | |

Für die Domänen ist demnach die Beschreibung trivial, muss aber für die Vollständigkeit angeführt werden. Die Tabelle 4.2 zeigt die Aufstellung der unterschiedlichen Rollen zwischen dem *Harmonized Electricity Market Role Models* nach der ENTSO-E und dem österreichischen Markt. Das Beispiel des *Messstellenbetreibers* ist in der Abbildung 4.1 beschrieben, wobei der Name unterschiedlich zum ENTSO-E Modell ist und die Rolle für

den *Netzbetreiber* mit anderen Rollen gemeinsam vereinigt wurde. Durch die tabellarische Darstellung der Rollen und Akteure lassen sich alle Änderungen des Ausgangsmodell zu Tabelle kompakten Rollenmodell für Österreich nachvollziehen und einfacher diskutieren. Tabelle 4.2 stellt die Unterschiede der Akteure dar. In der zweiten Spalte ist beispielsweise die Rolle des *Prosumers* als neu geschaffene Rolle eingetragen. Auf die Bedeutung und Notwendigkeit des *Prosumers* wird in 4.2.2 und 4.2.3 näher eingegangen.

Abbildung A.5 im Anhang zeigt die kompakte Version des österreichischen *Harmonized Electricity Market Role Models*. Hier konnten viele Akteure aufgrund der Aufgabenverteilung in Österreich konsolidiert werden. In Abbildung 4.1 ist diese Information bei dem *Netzbetreiber* hinterlegt, der ebenso in der *Generalizes*-Beziehung zum *Messstellenbetreiber* steht. In der kompakten Version ist der *Netzbetreiber* (sowie auch weitere Rollen) als *Party with multiple actors* aus Abbildung 3.13 dargestellt. Um das vorherige Beispiel des *Messstellenbetreibers* aufzugreifen, sieht man in Abbildung A.5 im Anhang im linken oberen Viertel die direkte Verbindung zwischen dem *Netzbetreiber* zu dem Zähler mit derselben Aufgabe, sie zu betreiben und zu warten.

Die Modelle wurden im RASSA-Konsortium sowie in Stakeholdertreffen mit der Austrian Power Grid, dem Österreichischen Übertragungsnetzbetreiber, diskutiert und entsprechend der Ergebnisse angepasst. Abbildung A.5 im Anhang zeigt die kompakte Version des kompakten österreichischen *Harmonized Electricity Market Role Models* [8].

Tabelle 4.2: Beschreibung und Unterschied der Akteure in ENTSO-E & RASSA Modell und Konsolidierung in kompakte Rollen für den österreichischen Markt [8]

| **ENTSO-E** | **Marktrollen in Österreich** | **Unterschiede der Modelle** | **Vereinigte Rolle in Österreich** |
|---|---|---|---|
| — | Prosumer | Neue Rolle und vereinigt | Stromlieferant-Vertrieb |
| Balance Supplier | Lieferant | Name unterschiedlich und vereinigt | |
| Block Energy Trader | Energiedienstleister | | |
| Party Connected to the Grid | Netzteilnehmer | | |
| Producer | Produzent | | |
| – | Verteilungssystem-Operator | Neue Rolle und vereinigt | Netzbetreiber |
| Grid Operator | Netzbetreiber (DSO/Stadtwerke) | ENTSOE-E Rolle geteilt | |
| | Übertragungsnetzbetreiber | | |
| Grid Access Provider | Grid Access Provider | Name identisch und vereinigt | |
| Meter Administrator | Meter Administrator | | |
| Metered Data Responsible | Metered Data Responsible | | |
| Metering Point Administrator | Metering Point Administrator | | |
| Reconciliation Accountable | Reconciliation Accountable | | |
| Reconciliation Responsible | Reconciliation Responsible | | |
| Meter Operator | Messstellenbetreiber | Name unterschiedlich und vereinigt | |
| Metered Data Aggregator | Bilanzkoordinator (BIKO) | | |
| Metered Data Collector | Messdienstleiser | | |
| Balance Responsible Party | Bilanzgruppenverantwortlicher (BGV) | Name unterschiedlich und vereinigt | Bilanzgruppenverantwortlicher (BGV) |
| Trade Responsible Party | Stromhändler | | |
| Consumption Responsible Party | Consumption Responsible Party | Name identisch und vereinigt | |
| Interconnection Trade Responsible | Interconnection Trade Responsible | | |
| Production Responsible Party | Production Responsible Party | | |
| Scheduling Coordinator | Scheduling Coordinator | | |
| System Operator | Übertragungsnetzbetreiber | Name unterschiedlich und vereinigt | TSO |
| Nomination Validator | Nomination Validator | Identisch und vereinigt | |
| Imbalance Settlement Responsible | Bilanzgruppenkoordinator (BKO) | Name unterschiedlich und vereinigt | BKO |
| MOL Responsible Merit | Order List Verantwortlicher | | |
| Reserve Allocator | Reserve Allocator | Identisch und vereinigt | |
| Capacity Coordinator | Capacity Coordinator | Identisch und vereinigt | Joint Allocation Office (JOA) |
| Capacity Trader | Capacity Trader | | |
| Transmission Capacity Allocator | Transmission Capacity Allocator | | |
| Control Block Operator | Control Block Operator | Identisch und vereinigt | Europäische Union |
| Coordination Center Operator | Coordination Center Operator | | |
| Consumer | Konsument | Name unterschiedlich | – |
| Control Area Operator | Regelzonenführer | | |
| Market Operator | Strommarktbetreiber | | |
| Resource Provider | Regelreserveanbieter | | |
| Market Information Aggregator | Market Information Aggregator | Identisch | – |
| Billing Agent | – | Rolle Abwesend | – |
| Data Provider | – | | |

## 4.2 Evaluierung des Fallbeispiels iniGrid in vorgestellten Modellen

Die Use Cases von iniGrid bieten ein Beispiel dafür, wie Sicherheitsstandards für neu entwickelte Komponenten abgeleitet werden können und diese für unterschiedliche Stakeholder in ihrer gesamten Komplexität ersichtlich zu machen. Hier wird auf die Ausgangslage von bestehenden SGAM-Modellierungen eingegangen, Schwächen des Domänenmodell .AT werden anhand eines Beispiels erläutert und die Kompatibilität der Use Cases mit RASSA wird aufgezeigt. Im Anschluss wird die Modellierung der Use Cases in der Referenzarchitektur vorgestellt. Anhand der Erstellung eines neuen, beispielhaften, firmenspezifischen Security Requirements soll die Herangehensweise für Erweiterungen demonstrieren.

### 4.2.1 iniGrid Use Cases im NIST LRM

Das Konzept von SGAM und der SGAM Toolbox waren aufgrund der zeitgleichen Projekte unter den Mitwirkenden bekannt. Das Wissen über die Security Requirements wurde anhand der Modelle händisch nachverfolgt und zusammengetragen wie in 4.2.3 weiter ausgeführt ist.

Nachfolgend werden die Use Cases und wichtigsten Elemente des SGAM-Modells[1] vorgestellt. Abbildung 4.2 zeigt die Verbindung von NIST LRM Elementen mit ausgewählten SGAM Toolbox Elementen für die iniGrid Use Cases. Das Diagramm ist im *Component Layer* positioniert. Es wird im linken oberen Viertel ein *2 - Customer* mit einem Business Akteur *Prosumer* mittels einer *Trace*-Verbindung verbunden. Andere Elemente wie zum Beispiel das *5 - Customer Energy Mgmt System* sind mit einem CEMS-Element durch den gleichen Verbindungstyp verbunden. Die im Projekt neu entwickelten Smart Breaker sind unten links durch das Schaltersymbol dargestellt, weisen allerdings keine Verbindung zu einem Element aus dem NIST LRM auf. Es sind drei Smart Breaker eingezeichnet, da auch hierarchische Versuchsaufbauten mit den Use Cases dargestellt werden sollten.

Um einen Überblick auf die Notation in Enterprise Architect zu bekommen wird in Abbildung 4.3 nur ein Teil der Business Use Cases dargestellt, im speziellen den Business Use Case *Energy Management on Prosumer Level* auf dem *Business Layer* von iniGrid. Die Geschäftsziele, dargestellt als grüne Kästchen mit dem Stereotype *Business Goal*, beinhalten Ziele wie die Energieeffizienz oder den Eigenverbrauch zu erhöhen (links und rechts zu sehen). Dieser Stereotype ist für den *Business Layer* geschaffen worden, wie es in Abbildung 3.1 dargestellt ist.

In [102] wird beschrieben, wie ein Szenario ein Verhalten beschreiben kann, um das Ziel einer Funktion zu erfüllen. Es wird eine weitere Unterscheidung zwischen *Goals* und *Purpose* (also einem Ziel und einer Absicht oder Zweck) die in der SGAM Toolbox nicht so detailliert unterschieden werden. Die hier beschriebenen Use Cases und *Business Goals*

[1] Modellierung und Bereitstellung des iniGrid SGAM-Modells durch Ewa Piatkoswka, AIT Austrian Institute of Technology GmbH, Projektpartner in iniGrid [4]

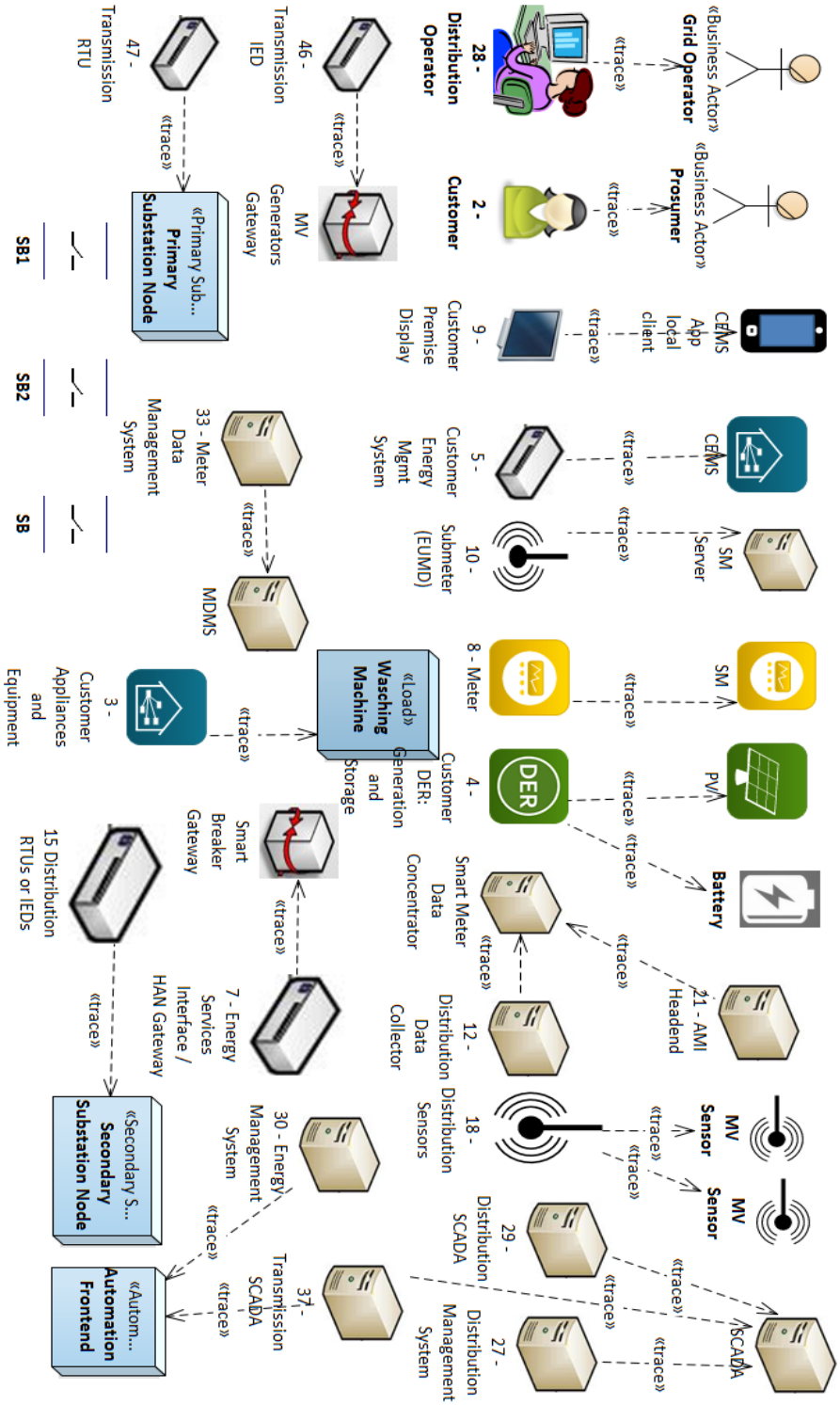



Abbildung 4.2: Mapping von iniGrid - Elementen zu NIST LRM durch *Trace*-Beziehungen

lassen allerdings einen Rückschluss zu, ob es sich um ein wirkliches *Goal* oder *Purpose* nach [102] handelt.

Der Business-Akteur *Prosumer* wird mit der *Has*-Verbindung zu diesen Zielen verbunden. Um den Business Use Case zu erfüllen benötigt es zwei *High Level Use Cases*, die beschreiben, wie dieses Ziel erreicht werden kann. Nachfolgend wird weiter unten der erste *High Level Use Case* des *Home/Commercial Energy Managements* näher betrachtet und erläutert.

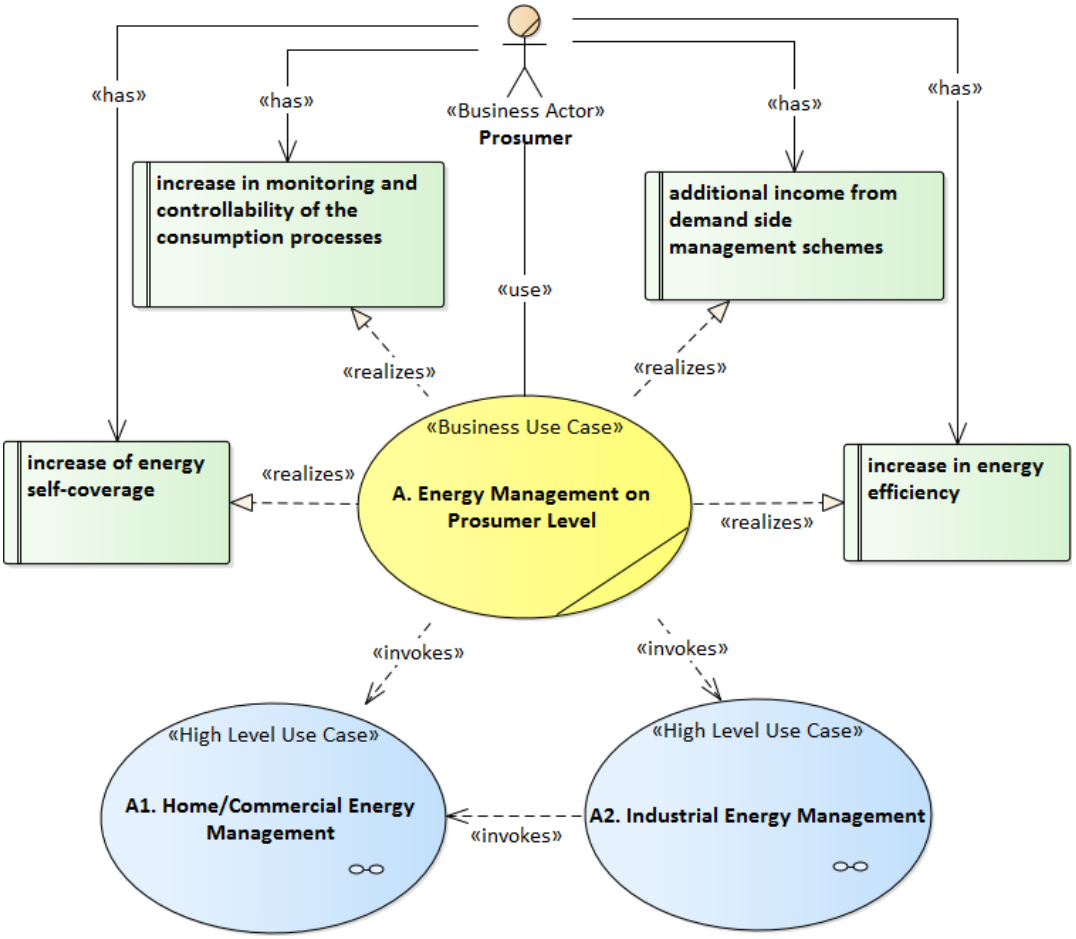



Abbildung 4.3: Ausschnitt des *Business Layer* mit Ansicht des Business Use Cases und Zielen für den *Prosumers*

Nach dieser Einführung ist in Abbildung 4.4 der komplette *Business Layer* mit den Use Cases und Zielen des *Prosumers* und *Grid Operators* vollständig dargestellt. Es besteht hier die selbe Struktur wie in Abbildung 4.3.

Nachdem der *Business Layer* vorgestellt ist, wird in Abbildung 4.5 der Use Case *Home/Commercial Energy Managements* im *Function Layer* dargestellt. Im Use Case kann

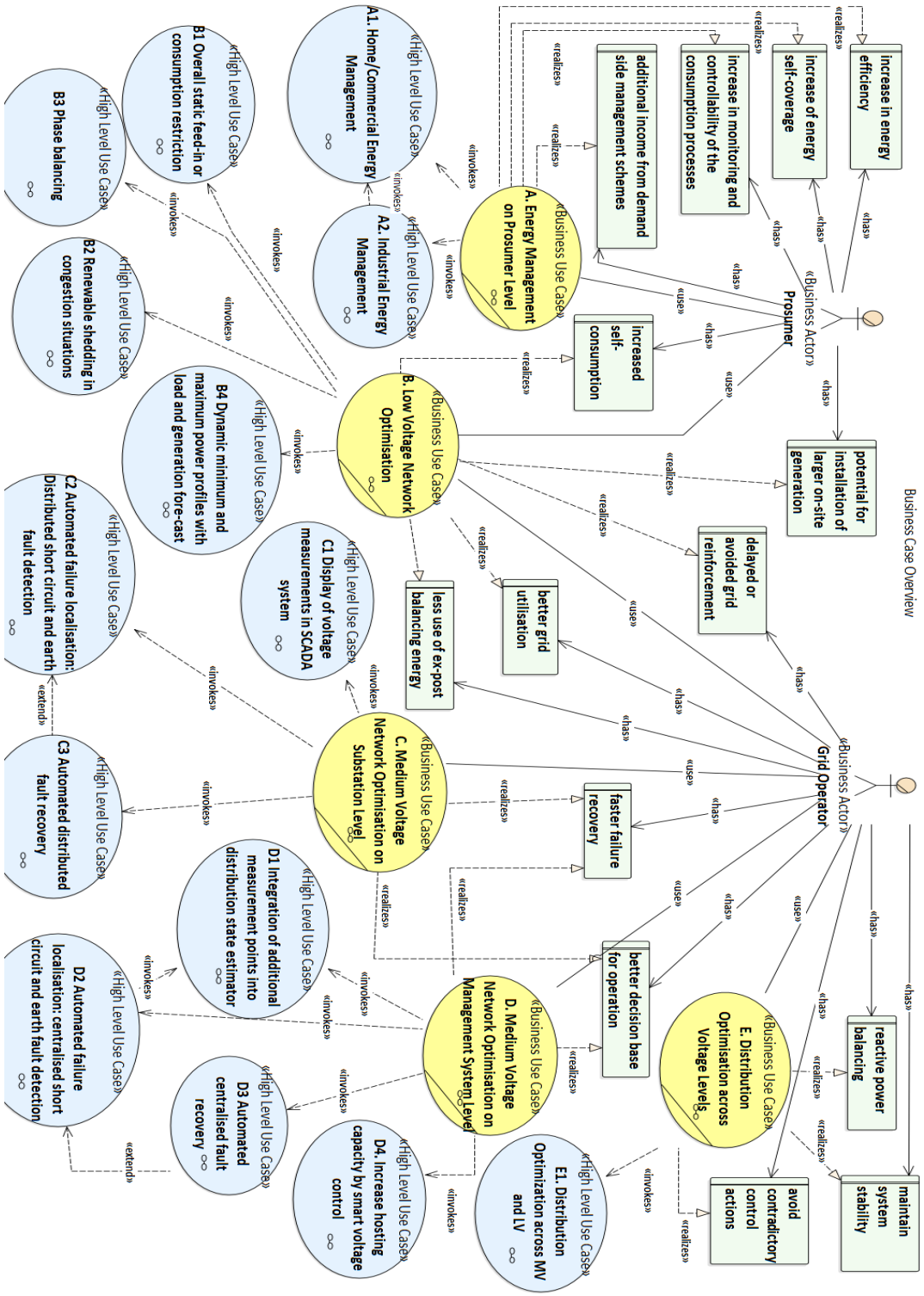



Abbildung 4.4: Darstellung des *Business Layer* mit den Use Cases und Zielen des *Prosumers* und *Grid Operators*

unter dem Menüpunkt „Scenarios“ eine Szenariobeschreibung (rechts im Bild) eingegeben werden, entweder durch das von Enterprise Architect zur Verfügung gestellte Formular oder über den Import von Textdateien. In dem illustrierten Beispiel werden neun Schritte beschrieben, die das Szenario des Use Cases *A1. Home/Commercial Energy Managements* beschreiben. Es ist zu sehen, dass die Elementnamen in der Szenariobeschreibung blau und unterstrichen hinterlegt sind. Durch einen Pattern-Matching-Abgleich mit dem (links im Bild) dargestellten Diagramm des Use Cases werden die Elemente automatisch identifiziert. Die beschriebenen Schritte sind hilfreich, wenn man ein Sequenzdiagramm aus dem Szenario erstellen möchte. Es werden die Linien und Elemente durch Enterprise Architect ebenfalls automatisch angeordnet. Abbildung 4.6 zeigt das Sequenzdiagramm zu dem Use Case Szenario von *Home/Commercial Energy Managements*.

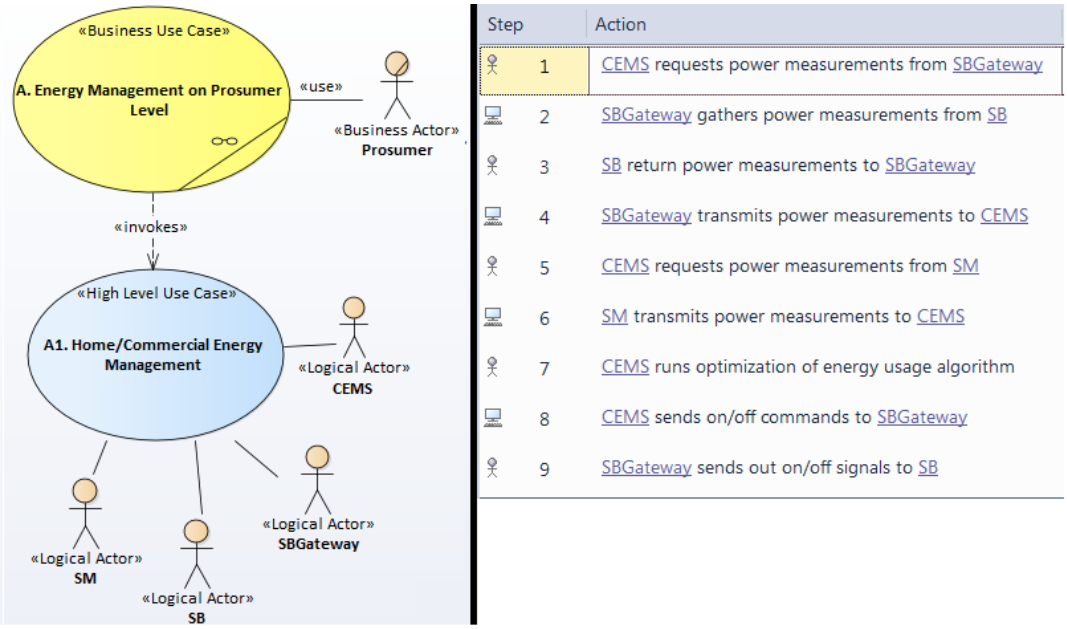



Abbildung 4.5: Darstellung des Use Case *Home/ Commercial Energy Management* im *Function Layer* mit Szenariobeschreibung

Abbildung 4.7 zeigt den *Communication Layer* des *Home/Commercial Energy Managements* Use Case. In diesem sind die Elemente auf der sogenannten SGAM-Ebene eingezeichnet, also zu welcher Domäne und welcher Zone die Elemente zugeordnet sind. Zwischen den Elementen werden die Kommunikationsprotokolle festgehalten. Zwischen dem Element *SM Server* und dem *CEMS* ist gemäß Zeichnung ein IEC 61850 Protokoll empfohlen.

In Abbildung 4.8 ist der *Information Layer* des *Home/Commercial Energy Managements* Use Case präsentiert. In diesem wird festgelegt, welche Informationen zwischen den Elementen (also den Komponenten und Systemen in der realen Umsetzung) ausgetauscht werden sollen. So soll das *CEMS* die Leistungsmessungen vom Smart Meter durch das

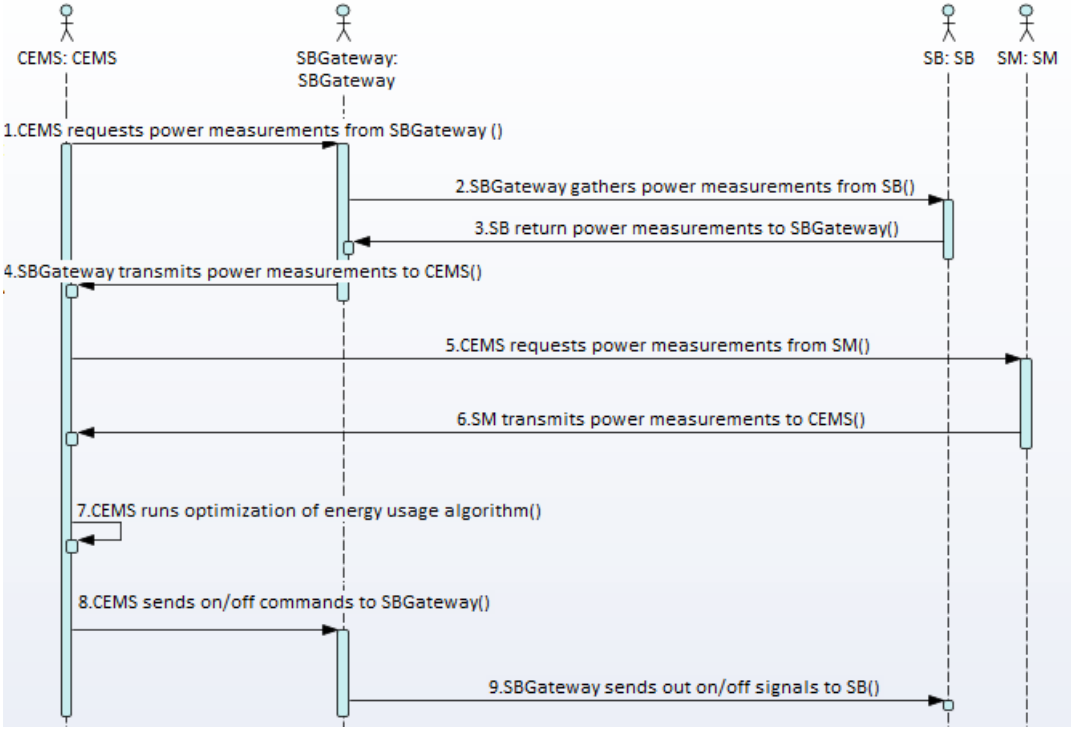



Abbildung 4.6: Generiertes Sequenzdiagramm aus einer Szenariobeschreibung

Element *SM Server* erhalten. In dieser Schicht kann auch die grundlegende Struktur der ausgetauschten Informationen durch das *Information Object* definiert werden.

Der *Component Layer* des *Home/Commercial Energy Management* Use Case ist in Abbildung 4.9 skizziert. Neu hinzugekommen sind die Elemente *LV Grid*, *PV*, *Battery* und *Wasching Maschine*. Die roten Verbindungslinien stellen eine elektrische Verbindung dar, die über die Smart Breaker entweder die Photovoltaikanlage, eine Batterie oder eine Waschmaschine den Strom zuschalten oder die Zufuhr trennen kann.

### 4.2.2 Implizite Abbildung im Domänenmodell .AT

Für eine Darstellung im Domänenmodell .AT würde sich eine Fortführung auf den Arbeiten aus 4.2.1 anbieten. Allerdings ist in der Formulierung für die *funktionalen Einheiten* aus [91] nur die Anpassung der NIST LRM-Elemente auf den Österreichischen Markt zielführend.

Durch die Entwicklung der innovativen, verteilten Sensoren und Aktuatoren können diese neuen Endgeräte aufgrund ihrer vielfältigen Funktionen klarerweise nicht in das bestehende Domänenmodell .AT-Modell Einzug finden. Dies wird vor allem dadurch erschwert, dass die Vorgehensweise des Domänenmodell .AT die Aufsplittung einer *Funktionalen Einheit* erlaubt. So ist in 3.3.2 erwähnt, dass sich die Einheit *30-Energiemanagementsystem* in den Domänen *Betriebsführung*, *Übertragung* und *Erzeugung* jeweils als eigenes Element

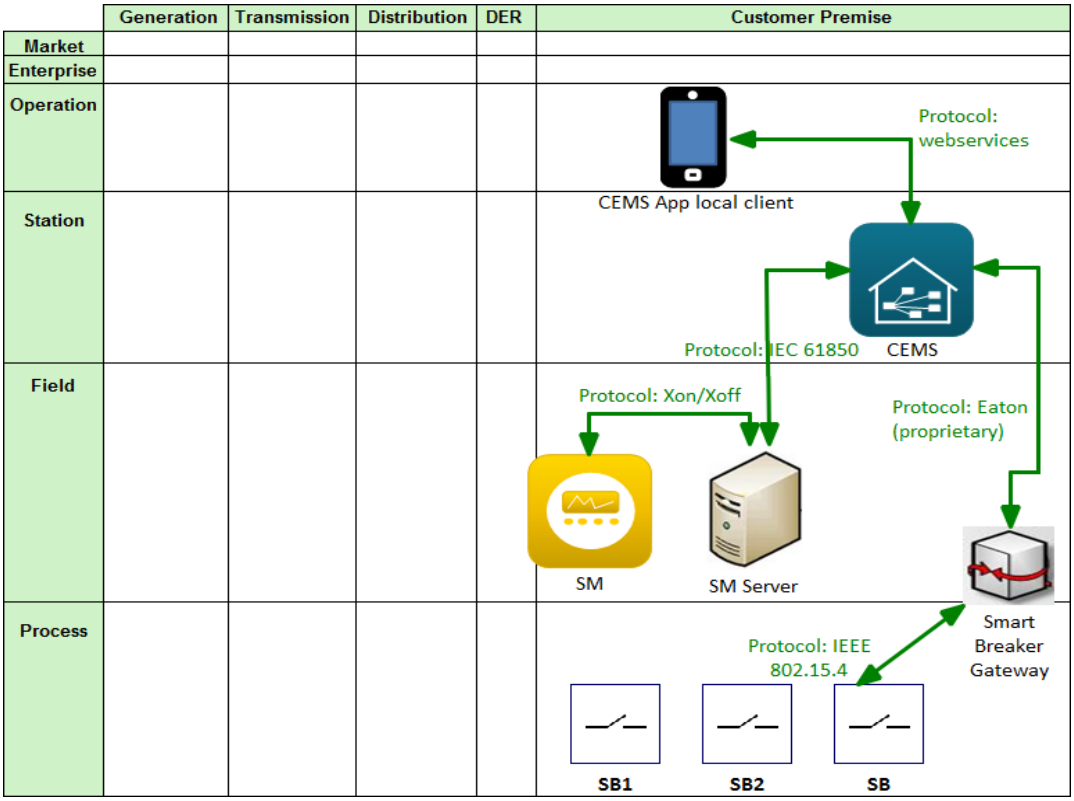



Abbildung 4.7: *Home/Commercial Energy Managements* Use Case: *Communication Layer*

befindet. Im Falle des Prosumers könnte sich die Domänenzuordnung auf sechs der sieben vorhandenen Domänen erstrecken und die Platzierung von sechs Elementen im Domänenmodell .AT bedeuten. Diese strikte Vorgehensweise würde zu einer Überfüllung des Diagramms führen und macht das Modell unnötig absurd, wenn alle Elemente in jeder Domäne enthalten sind. Durch die in dieser Arbeit vorgestellten Methodik und der Generalisierungsbeziehung in der Referenzarchitektur lassen sich die Rückschlüsse auf die Elemente im Domänenmodell .AT implizit rückschließen, weshalb eine eigene Darstellung auf dieser Ebene wegfallen darf.

### 4.2.3 iniGrid Use Cases Kompatibilität mit dem RASSA-Modell

Vorausgehend sind in 4.2.1 die iniGrid Use Cases beschrieben, wie sie durch das iniGrid-Konsortium modelliert wurden. Im Projekt wurden die Security Requirements händisch durch einen Abgleich der Akteure mit den NIST LRM-Akteuren vollzogen. Diese Herangehensweise ist in einem Forschungsprojekt für wenige Use Cases durchaus vertretbar, allerdings nicht geeignet um in den Arbeitsalltag von Unternehmen integriert werden zu können.

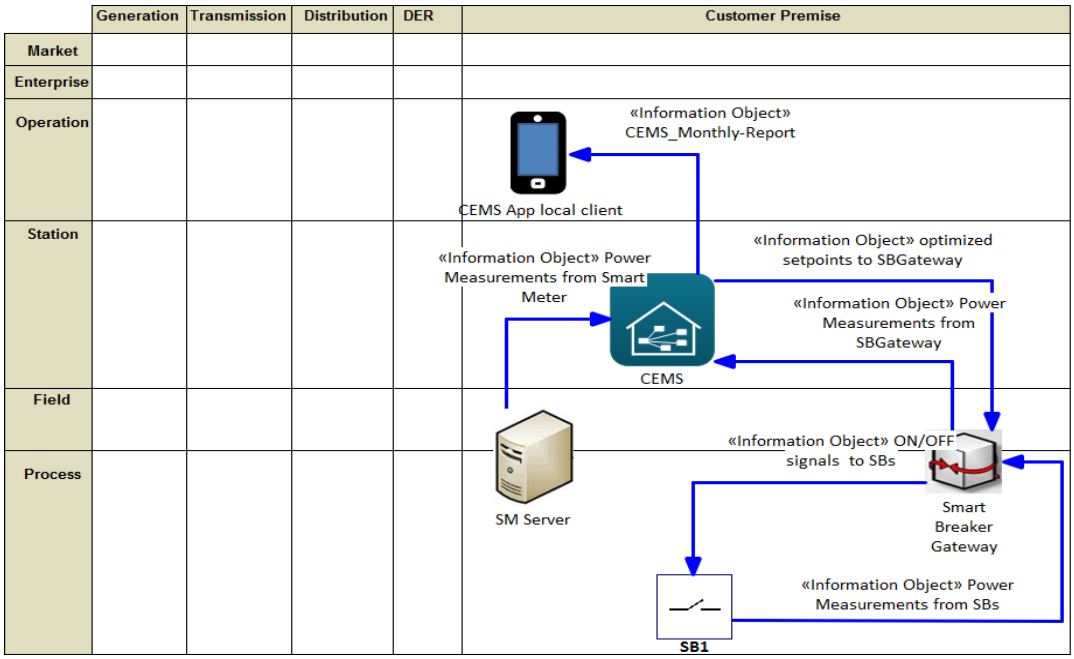



Abbildung 4.8: *Home/Commercial Energy Managements* Use Case: *Information Layer*

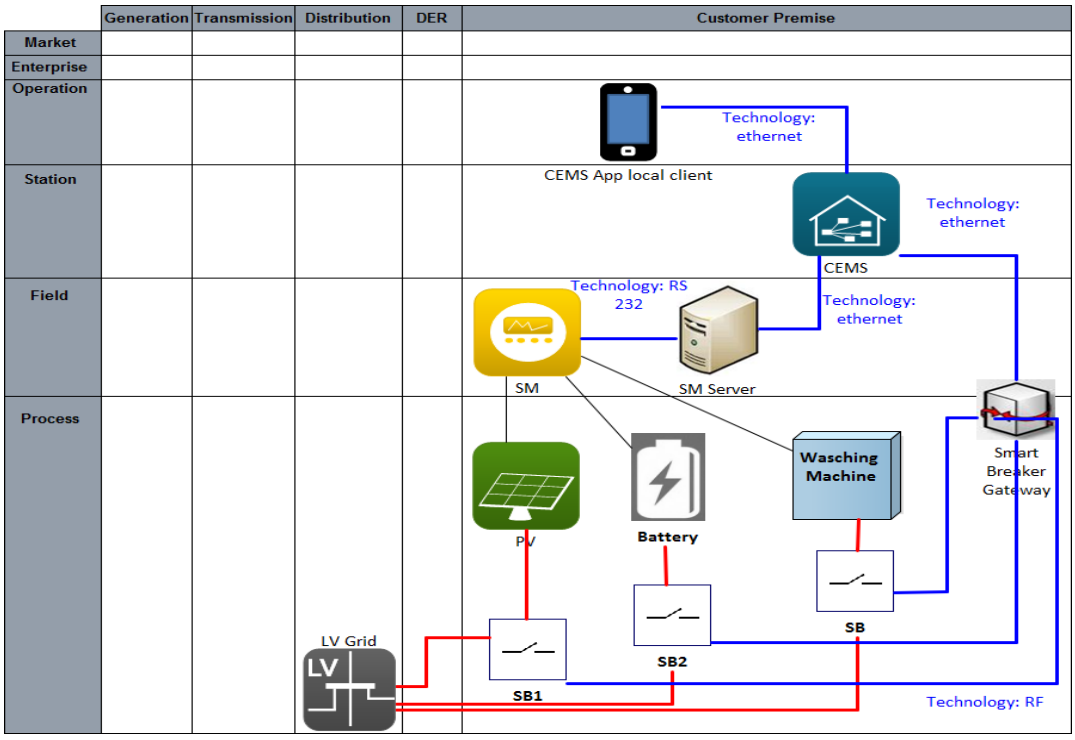



Abbildung 4.9: *Home/Commercial Energy Managements* Use Case: *Component Layer*

### Probleme der Modellierung ohne RASSA-Methodik

Die Use Cases von iniGrid verwenden modellierungstechnisch nur wenige der zur Verfügung stehenden Funktionen und nützen damit nicht das volle Potential der Modelle aus. Nachfolgend wird erläutert, welche Probleme bei einer halbautomatischen Analyse durch externe Tools auftauchen können und warum die Verwendung der *Generalize*-Beziehung wichtig ist.

In Abbilung 4.10 sind die zwei unterschiedlichen UML-Verbindungen *Trace* und *Generalize* zwischen dem Element *5 - Customer Energy Mgmt System* aus dem NIST LRM und einem neuen Element *CEMS* mit dem Stereotyp *Home Automation* dargestellt. Im Unterschied dazu wurden in iniGrid die Elemente in einem eigenen Diagramm mit Hilfe einer *Trace*-Beziehung verbunden, um über diese Verbindung einen Kontext zu NIST LRM zu schaffen. Die *Trace*-Beziehung wird von Enterprise Architect interpretiert als:

> Die Trace-Beziehung ist eine Spezialisierung einer Abstraktion. [...] Traces werden häufig zum Nachverfolgen von Anforderungen und Modelländerungen verwendet, normalerweise in einem Traceability-Diagramm [...].
>
> Da Änderungen in beiden Richtungen auftreten können, wird die Reihenfolge von *Trace* normalerweise ignoriert. [103].

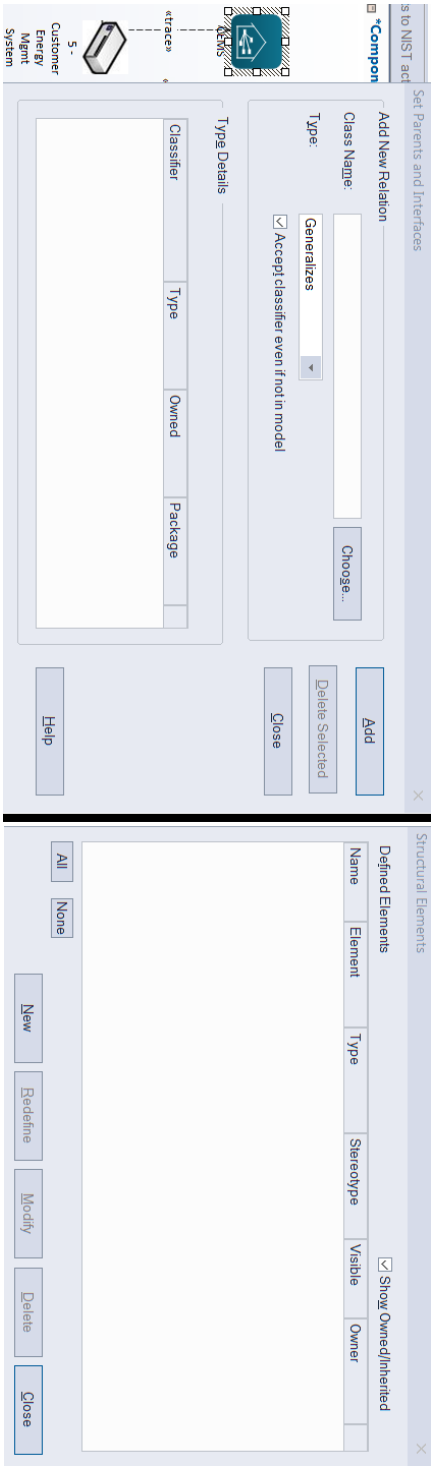
Eine Nachverfolgung der NIST LRM Security Requirements ist prinzipiell so möglich aber unpraktikabel. In Abbildung 4.10a ist der Fall der *Trace*-Beziehung dargestellt, bei dem kein Elternelement zugeordnet ist aber derart auch keine *Structural Elements* abgeleitet und ins Diagramm eingefügt werden können. In Abbildung 4.10b ist dies als Verbesserungsvorschlag anders, da eine *Generalize*-Beziehung zwischen den Elementen besteht und so die geerbten Ports über das *Structural Elements*-Fenster eingefügt werden können. Die Ports stellen die im NIST LRM definierten Schnittstellen dar, die für die Kommunikation zwischen zwei Elementen verwendet wird. Diese Ports sind in weiterer Folge an die erwähnten Security Requirements gekoppelt.

Die Abhängigkeitsbeziehungen über mehrere Ebenen nachzuvollziehen ist auch für den Modell-Export und den Import in Drittanbieterlösungen problematisch, da hier zusätzliche Beziehungen abgefragt und für das aufwendigere Parsen programmiert werden müssten.

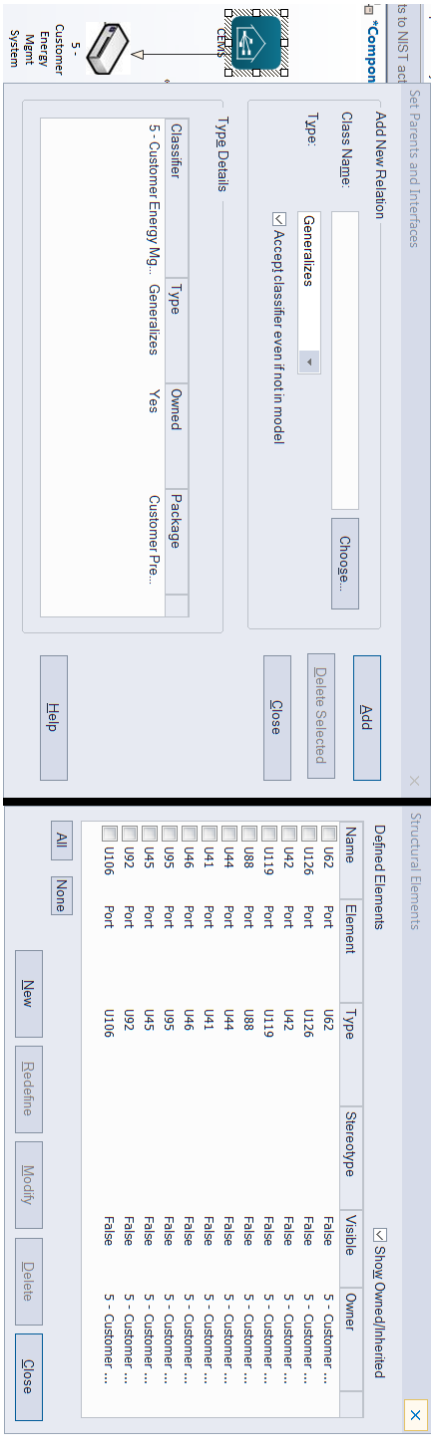
Ein weiteres Problem stellt die Verwendung von Elementen als *Link* in einem Diagramm dar. Wenn das Hauptelement vervielfältigt als *Link* in Diagrammen verknüpft wird, entsteht eine große Anzahl an Artefakten, die das Ergebnis von anderen Use Cases verfälschen können. Darum ist die Verwendung einer *Instanzierung* mitsamt der dazugehörigen Ports (und dadurch verbundenen Security Requirements) für eine halbautomatische Dokumentation oder einen Modellexport wichtig. Das Beispiel stellt die Wichtigkeit der RASSA-Vorgehensweise dar.

### Definition neuer Akteure am Beispiel des Prosumers

Im Folgenden werden die notwendigerweise neu modellierten Elemente und Akteure, die für die Anwendung der iniGrid Use Cases unerlässlich waren, erläutert. In weiterer Folge wird die Notwendigkeit der fehlenden Elemente begründet.



(a) Ausgangslage: *Trace*-Beziehung zwischen zwei *iniGrid*-Elementen



(b) Nach Änderung: *Generalize*-Beziehung zwischen zwei *iniGrid*-Elementen

Abbildung 4.10: Gegenüberstellung von ableitbaren Informationen durch *Trace* und *Generalize* UML-Beziehungen

Das *Harmonized Electricity Market Role Model* sieht keine dezidierte Rolle für den *Prosumer* vor. Ein Prosumer ist ein Verbraucher, der ebenfalls als Erzeuger fungiert. Mit dem stetig steigenden Zuwachs an durch den Endkunden erzeugt erneuerbaren Energien, die sowohl leistungstechnisch als auch marktwirtschaftlich durch die Kombination mit Gebäudebatterien einen Einfluss auf das Stromnetz haben, sollte diese Rolle aus der Sicht der RASSA-Initiative als eigenes Element in der Referenzarchitektur zur Verfügung stehen.

Die Auslegungsmöglichkeiten sind vielfältig, je nachdem wie weit man den Begriff und die Rolle des Prosumers fassen möchte. In Abbildung 4.11 ist ein Auschnitt eines Detaildiagramms für den *60 - Prosumer* zu sehen. In diesem befinden sich fünf Elemente, von denen *60 - Prosumer* erbt. Im Folgenden sind die Gründe aufgeführt, welche die Wahl der Eltern-Elemente erläutern:

- Da der neu definierte Prosumer definitiv die Rolle eines Konsumenten, also Kunden einnimmt, ist *60 - Prosumer* eine Spezialisierung von Element *2 - Kunde*.
- Der Prosumer kann mit entsprechender technischer Ausstattung auch als Stromhändler am Markt agieren. Deshalb ist die Spezialisierung von *20 - Stromhändler* naheliegend.
- Bei Bereitstellung von Energie für andere Kunden kann man den Prosumer auch zu den *41 - Lieferanten* zählen.
- Im Falle eines isolierten Netzabschnitts im Inselbetrieb kann der Prosumer auch die Rolle des *54 - Netzbetreiber* für die Einhaltung der Netzstabilität inne haben.
- Werden die Prosumer durch ein sogenanntes *Virtual Power Plant* zusammengefasst und können sozusagen auf Abruf Regelenergie bereitstellen, ist die Spezialisierung durch *58 - Regelenergiebereitstellung* relevant.

Die Auswahl der zugrundeliegenden Elternelemente ist in diesem Beispiel breit gefächert, um den Vorteil der in dieser Arbeit gezeigten Herangehensweise ersichtlich zu machen. Im Folgenden wird daher auf das Beispiel innerhalb des Modells anhand eines Diagramms des *60 - Prosumer* eingegangen.

Um die Abbildung 4.11 (siehe nächste Seite) so übersichtlich wie möglich zu halten, ist nur der relevante Ausschnitt der Schnittstellen nach dem NIST LRM [46] über *2 - Kunde* dargestellt. In diesem Diagramm wird der Abhängigkeitspfad deutlich. Zunächst wird von dem in RASSA definierten Kunden (Darstellung als grüne „Person“ und Beschriftung *Verbrauch*) eine Verbindung zu dem Element mit der symbolischen Darstellung aus dem Domänenmodell .AT geknüpft. Dieses wiederum ist mit dem Element der NIST Modellierung verbunden, welches als *Customer Premises: 2 - Customer* in der Abbildung 4.11 zu sehen ist. Dieses enthält aufgrund des Enterprise Architect sogenannte *Ports*, wie sie durch die kleinen rechteckigen Kästchen rund um das Element des *Customer Premises:*

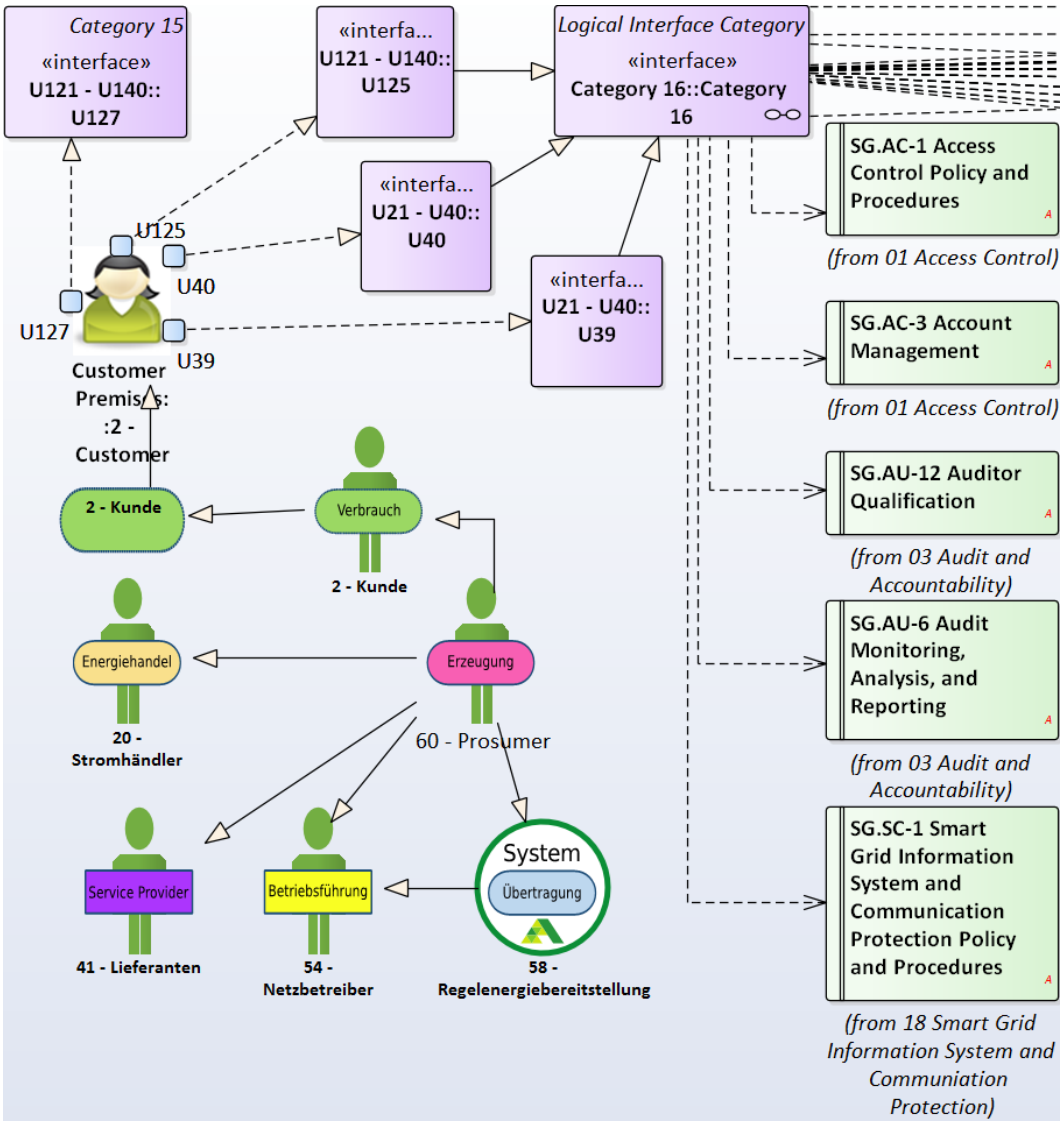



Abbildung 4.11: Angeordneter Ausschnitt aus dem Diagramm des *60 - Prosumer* und dessen definierten Spezialisierungen sowie zusätzlich eingeblendete Schnittstellen, Kategorien nach NIST LRM und deren Security Requirements

*2 - Customer* zu sehen ist. Diese Ports sind mit Gruppierungen von Schnittstellen verbunden, wie die Gruppe *U121 - U140*. Diese Gruppen sind einer *Logical Interface Category* zugeordnet, in diesem Fall *Category 16*. Durch die Kategorie können die im NIST LRM definierten Security Requirements nachverfolgt werden, sowie auch die Wertigkeit von *Confidentiality*, *Integrity* und *Availability*. Aufgrund der beschränkten Darstellungsmöglichkeiten auf Papier sind nur fünf der insgesamt 63 definierten Security Requirements von *Category 16* durch die grünen Boxen auf der rechten Seite in Abbildung 4.11 dargestellt.

Bei der Darstellung der Security Requirement Elemente aus Abbildung 4.11 sind detaillierte Beschreibungen als Verlinkung innerhalb jeder der Elemente eingebettet. Jedes der Security Requirements umfasst in der Spezifikation [46] etwa eine halbe bis ganze DIN A4 Seite, mit detaillierten Informationen zu Kategorisierung, Security Requirements, ergänzende Anleitungen, erweiterten empfohlenen Sicherheitsmaßnahmen, zusätzlichen Sicherungsabläufen und die Zuordnung der Auswirkungsstufen. Letzteres ist die Einschätzung. ob mit einer leichten, mittleren oder schweren Auswirkung im Falle eines technischen Ausfalls oder Cyberangriffs zu rechnen ist. Die jeweiligen Auszüge der Beschreibungen der Security Requirements sind als verlinkte Dokumente über jedes der insgesamt 194 Security Requirements Elemente in der Referenzarchitektur abrufbar.

### 4.2.4 iniGrid Use Case A in RASSA

Die Modellierung des *Business Layer* erfordert für die Elemente *60 - Prosumer* und *54 - Netzbetreiber* sowohl die Verknüpfung zu den Business Use Cases als auch den Business Goals. Nachfolgende Abbildung zeigt den relevanten Ausschnitt des Diagramms. Da der *60 - Prosumer* auch Energie zur Verfügung stellen kann, wurde er zu der Domäne *Erzeugung* durch den *Tag „Zugehörigkeit“* zugewiesen. Der *54 - Netzbetreiber* ist wie durch das Domänenmodell .AT der *Betriebsführung* zugeordnet.

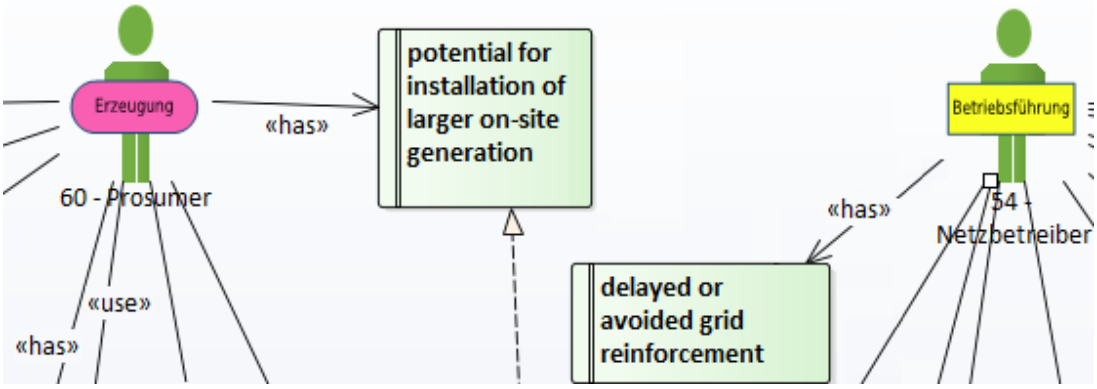



Abbildung 4.12: Ausschnitt des *Business Layer* von iniGrid Use Case A in RASSA

Abbildung 4.13 zeigt den *Function Layer* des Use Case A. Auf der linken Seite ist der Use Case mit den vier im Szenario involvierten Elementen gezeigt. Diese sind in dieser

Darstellung bereits mit den RASSA Symbolen zu sehen und durch die Instanzierung der RASSA-Blaupausenelemente können die *Generalize*-Beziehungen dieser Elemente über alle Generalisierungsebenen nachverfolgt werden. Beim Element *Smart Breaker* wurden drei Elemente für die *Generalize*-Beziehung herangezogen, die beim *Component Layer* erklärt werden. Auf der rechten Seite ist zu sehen, dass der Szenariotext für die neuen Elementnamen angepasst werden musste.

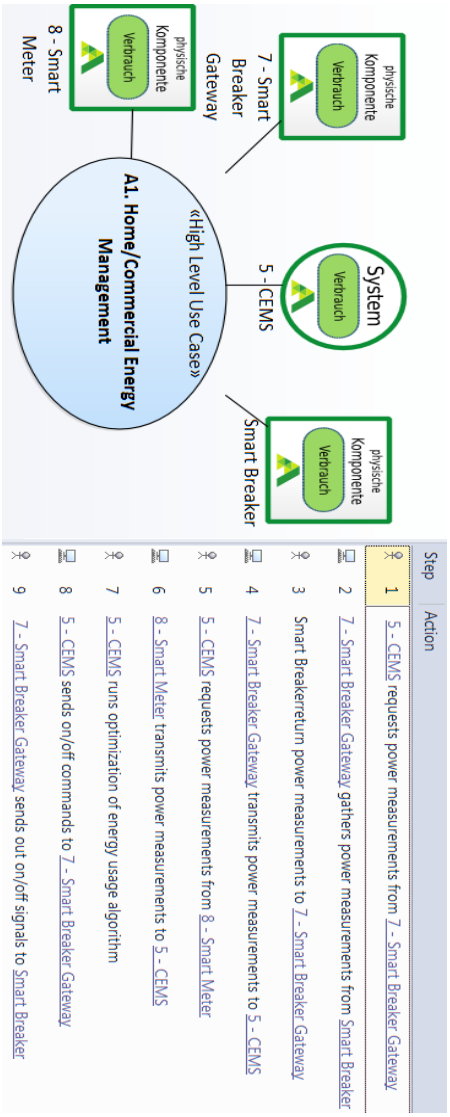



Abbildung 4.13: Screenshot des *Function Layers* von iniGrid Use Case A in RASSA mit Szenario-Beschreibung

Die angepasste Szenariobeschreibung kann durch Enterprise Architect in ein Sequenzdiagramm überführt werden. Die detaillierte Abbildung 4.14 zeigt das neu generierte

Sequenzdiagramm mit den vier Elementen. Dort ist zu sehen, dass das *5 - CEMS* noch generisch als Strichmännchen dargestellt ist, da diese Art von Diagrammen keine modifizierten Symbole durch die definierten Stereotypes zulassen und somit das System einem logischen Akteur entspricht. Dies ändert aber nichts an dessen Eigenschaften.

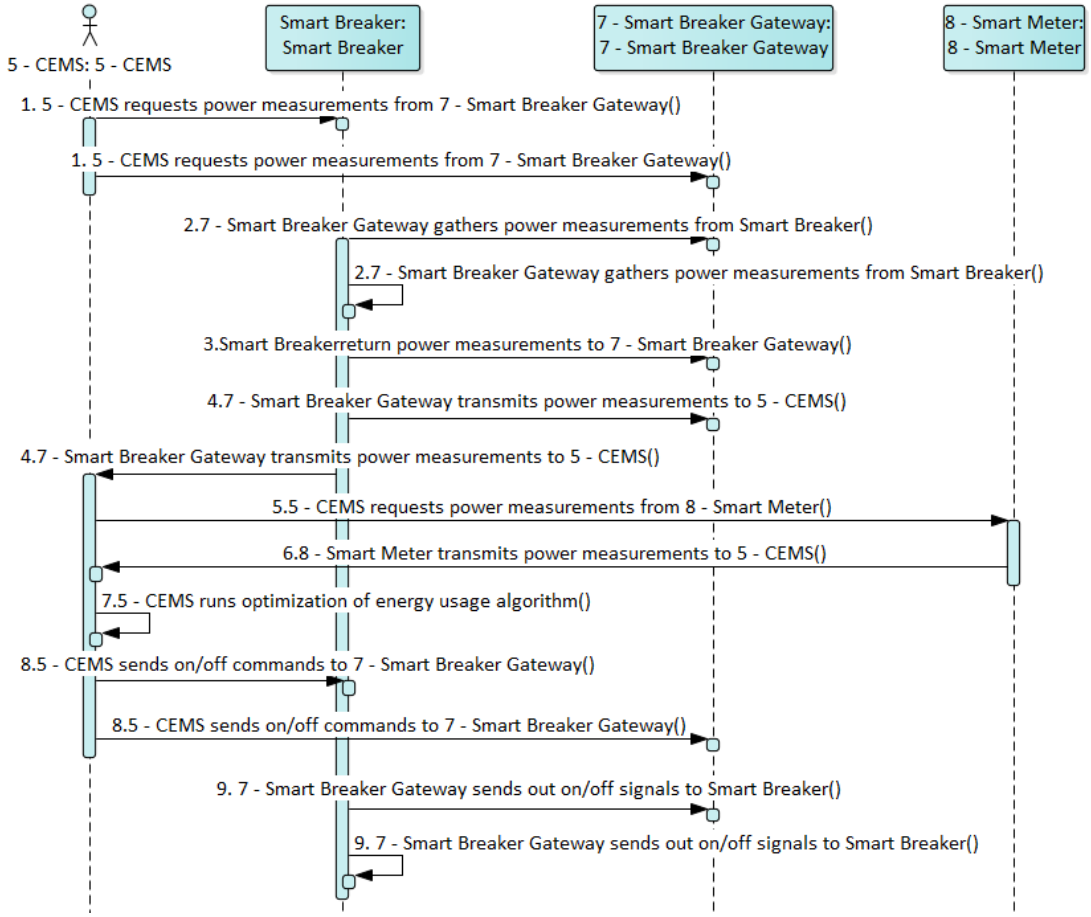



Abbildung 4.14: Neu generiertes Sequenzdiagramms von iniGrid Use Case A in RASSA

Der *Smart Breaker* hat als Multifunktionsgerät *Generalise*-Beziehungen zu den folgenden Elementen in dem Modell in der Referenzarchitektur:

- *4 - Erzeugung und Speicherung von Energie auf Kundenseite*: Als fernschaltbares Trennelement für dezentrale Energieerzeuger und Speicher sollte der *Smart Breaker* hier die Schnittstellen und Security Requirements in Betracht ziehen.
- *8 - Zähler*: Aufgrund der Messfunktionen soll der Smart Breaker ähnliche Anforderungen erfüllen, wie der *8 - Meter* oder *10 - Submeter (EUMD)* des NIST LRM und zusätzlich Anforderungen auf europäischer und österreichischer Ebene. Für diesen Use Case werden die Anforderungen des *8 - Meters* herangezogen.

- *3 - Kundengerät*: Da die *Smart Breaker* auch bei Kund_innen verbaut werden können um (optimierend) den Haushalt und Geräte zu steuern, sollten die hier hinterlegten Security Requirements in Betracht gezogen werden.

Der in Abbildung 4.15 dargestellte *Information Layer* zeigt den iniGrid Use Case A mit fünf Elementen. Die Informationsobjekte sind bei die Modellierung in der Referenzarchitektur unverändert geblieben.

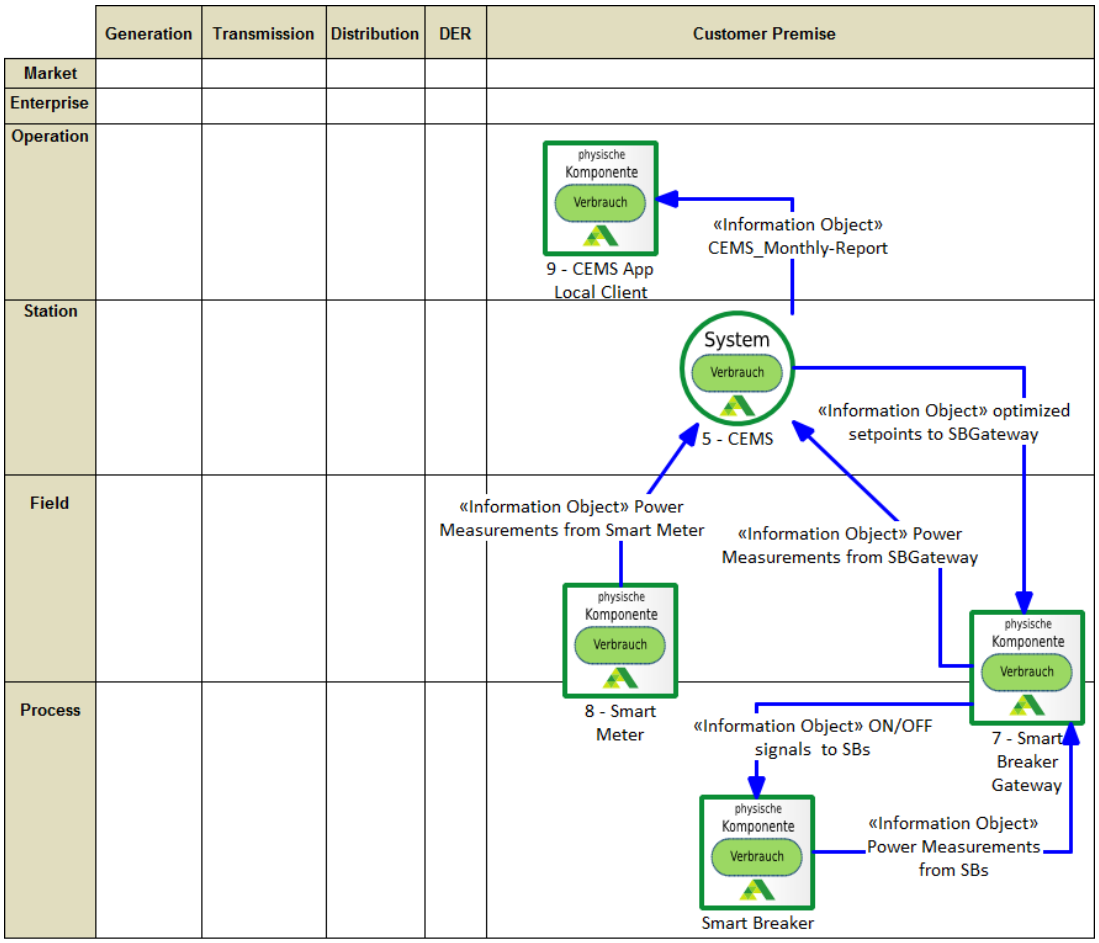



Abbildung 4.15: Screenshot des *Information Layers* von iniGrid Use Case A in RASSA

Die Informationsobjekte halten beschreiben dabei zum Beispiel bei der Verbindung zwischen dem *Smart Breaker* und dem *7 - Smart Breaker Gateway* die Messung über die Leistung die durch die Messfunktion des *Smart Breakers* erhalten werden kann. Das *7 - Smart Breaker Gateway* sendet diese gebündelt an das *5 - CEMS*, wo es zusammen mit den Messungen *8 - Smart Meter* zusammenläuft.

Nach Erhalt, kann das *5 - CEMS* die Schaltstellung der *Smart Breaker* optimieren, wobei

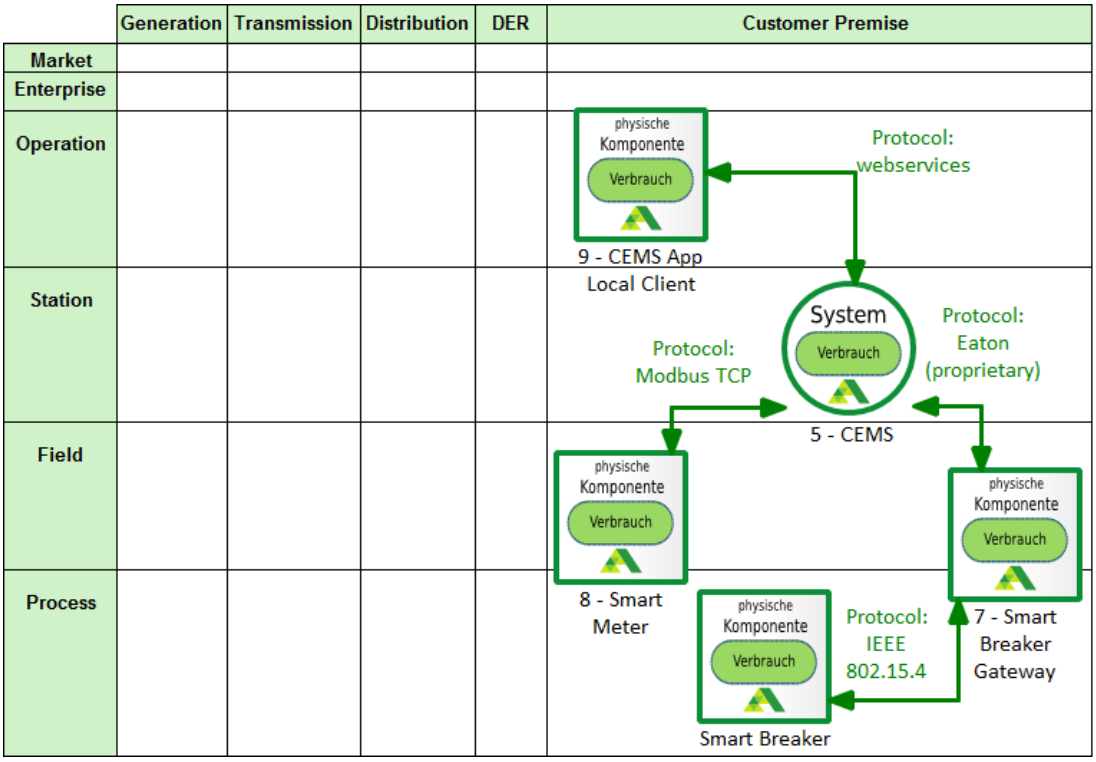



Abbildung 4.16: Screenshot des *Communication Layer* von iniGrid Use Case A in RASSA

die Information zunächst an das *7 - Smart Breaker Gateway* gesendet werden muss. Dieses interpretiert die Information und sendet die An- oder Abschaltbefehle weiter.

Der *Communication Layer* in Abbildung 4.16 hat sich inhaltlich, gegenüber seiner ursprünglichen Form im NIST LRM, verändert. Da es sich um einen Use Case mit dem Ziel der lokalen Optimierung handelt, gibt es eine durch das *5 - CEMS* eine Direktverbindung mit dem *Modbus TCP*-Protokoll zum *8 - Smart Meter*. Für die Entwicklungen in iniGrid war diese Ausführung zur Demonstration ausreichend und die Kommunikation über einen Smart Meter Server (wie in 4.2.1 dargestellt) nicht notwendig. Dass dadurch möglicherweise neue Risiken (im realen Feldeinsatz) entstehen würden, sollte hier zumindest angesprochen werden, allerdings liegt dazu eine tiefergehende Analyse nicht im Umfang dieser Arbeit.

Abbildung 4.17 zeigt den *Component Layer* des iniGrid Use Case A modelliert in der Referenzarchitektur. Analog zum *Information Layer* und *Communication Layer* ist der Smart Meter Server nicht mehr vorhanden, aufgrund der oben angeführten lokalen Optimierung. In diesem Diagramm sind die *PV* und die *Batterie* nicht als RASSA-Komponenten unter *4 - Erzeugung und Speicherung von Energie auf Kundenseite* dargestellt. Der Use Case sieht keinerlei Kommunikation zu diesen Elementen vor und steuert diese über Hinzu- oder Wegschalten durch den *Smart Breaker*.

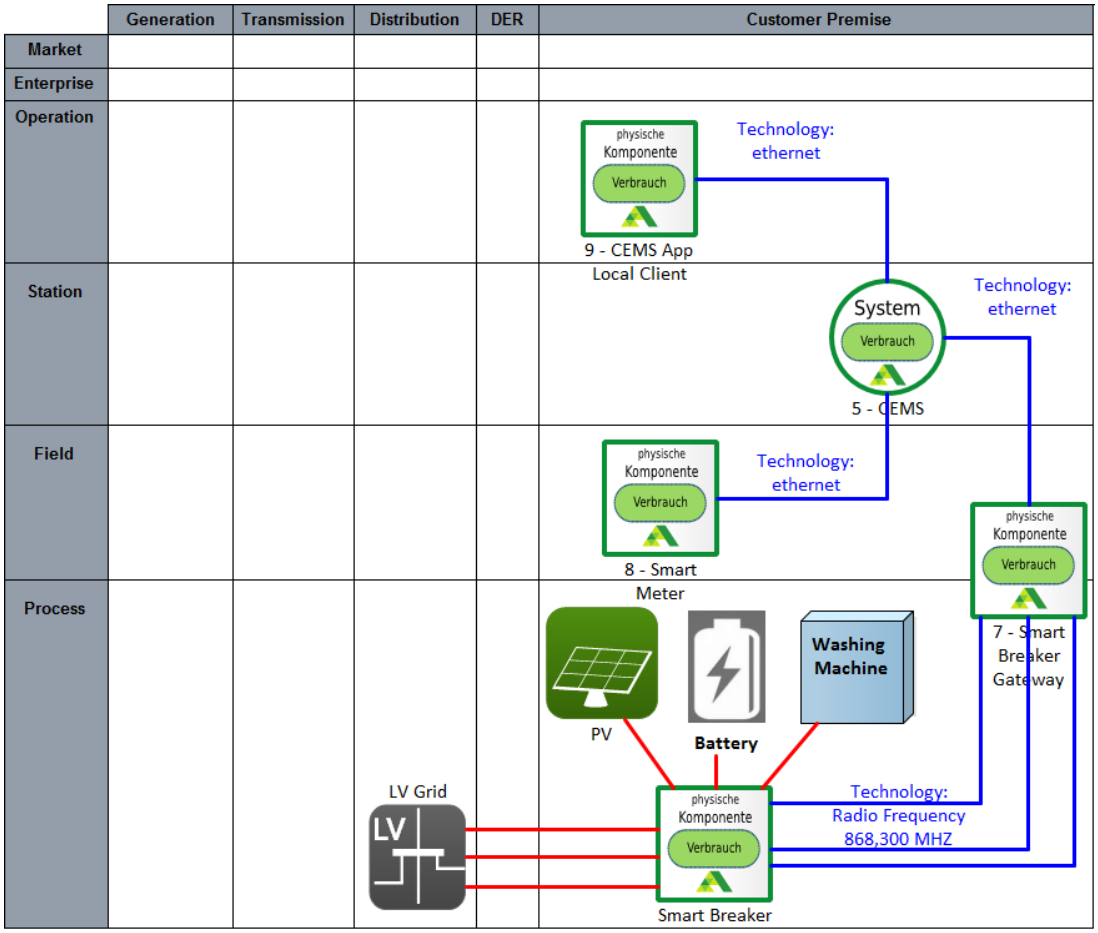



Abbildung 4.17: Screenshot des *Component Layer* von iniGrid Use Case A in RASSA

Dies schließt die Modellierung eines iniGrid Use Cases auf allen SGAM-Ebenen ab. Diese Modellierung ist der beispielhafte Versuch für eine neu entwickelte Komponenten wie dem Smart Breaker eine Zuordnung durchzuführen, die nationale und internationale Konzepte berücksichtigen und Sicherheitsanforderungen umsetzen soll.

### 4.2.5 Beispielhafte Modellierung von unternehmensspezifischen Anforderungen

Nachdem der iniGrid Use Case A exemplarisch mittels RASSA modelliert wurde, bleibt die Frage nach der Modellierung von unternehmensspezifischen Anforderungen noch offen. Diese Frage wird hier beantwortet.

Da die im Domänenmodell .AT angeführten Einzelrisiken und Gefahrenfelder aufgrund des fehlenden öffentlichen Informationszugangs nicht zugeordnet werden konnten, bieten diese Elemente eine Möglichkeit für die exemplarische Modellierung neuer Anforderungen. Die Vorgehensweise lässt sich anhand der Verwendung von eigenen Blaupausen-Komponenten wiederholen, sofern die *Generalize*-Beziehung entsprechend verwendet wird. Da dieser Abschnitt die nachvollziehbare Modellierung beschreibt, ist in Abbildung 4.18 die Ordnerstruktur für die neuen Elemente des Domänenmodell .ATs dargestellt. In diesem ist das erstellte *Erste unternehmensspezifische Security Requirement* in einem dazugehörigen Ordner angelegt. Dieser befindet sich in einer neuen Kategorie *UK 1*, dass wie das Interface *F1* ebenso in einem aussagekräftigen Ordner ist. Die Platzierung der Elemente wurde im *Component Layer* vorgenommen.


Abbildung 4.18: Ordnerstruktur nach Definition einer neuen Interface-Kategorie und Security Requirement auf der Ebene des Domänenmodell .AT

Die Definition der Security Requirements wurde wie von Neureiter (siehe 3.3.3) mit dem SGAM Modell für das NIST LRM vollzogen. Das Interface *F1* ist eine Spezialisierung der Kategorie *UK 1* wie in Abbildung 4.19 zu sehen ist. Die Kategorie ist mit dem Ordnersymbol der *UK 1 Security Requirements* verbunden.

In Abbildung 4.20 ist die Verbindung zwischen der *Unternehmensspezifischen Kategorie 1* mit dem neuen Element *Erstes unternehmensspezifische Security Requirement* verbunden.

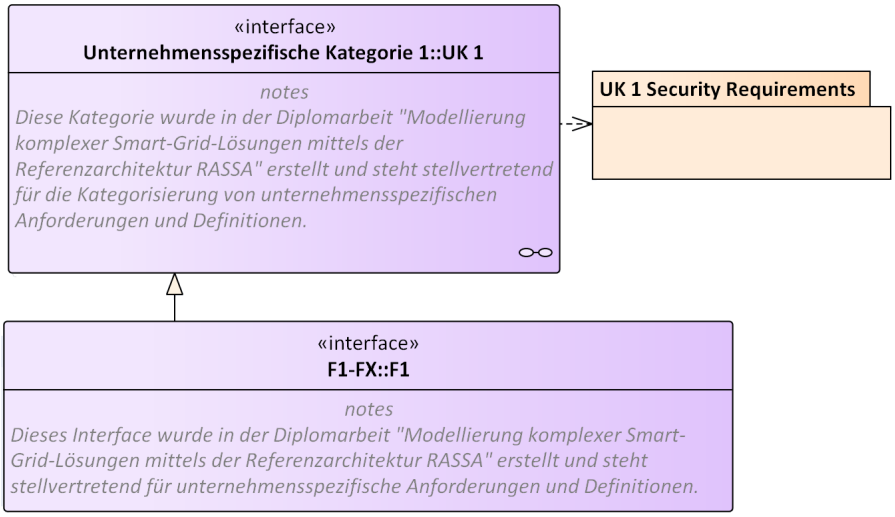



Abbildung 4.19: Screenshot der unternehmensspezifischen Kategorie UK 1

Durch Platzierung und Verbindung weiterer Elemente kann die Kategorie darüber hinaus mit eigenen Anforderungen bereichert werden. Auch die *Tags* lassen sich frei wählen, weshalb in diesem Fall die Zuordnung mit dem Wert *Unbekannt* stellvertretend steht.

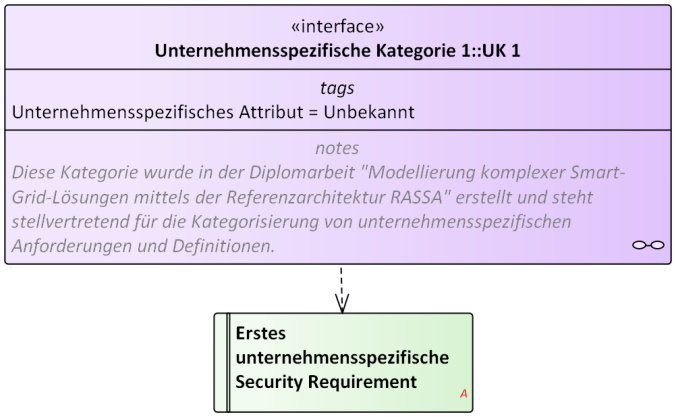



Abbildung 4.20: Screenshot des firmenspezifischen Interface F1 und einem neuen stellvertretenden Security Requirement

In Abbildung 4.21 ist abschließend das Diagramm mit der Detailansicht des *8 - Zähler* abgebildet. Im unteren Teil der Abbildung ist das geöffnete Menü mit den *Ports* zu sehen. Für das Element wurde das Interface *F1* beispielhaft neu hinzugefügt. Für die Übersichtlichkeit sind nur der *F1-Port*, das Interface, die dazugehörige *Unternehmensspezifische Kategorie 1 (UK 1)* und die verbundenen Security Requirements abgebildet. Dies zeigt ist eine mögliche Darstellung der erfolgreichen Modellierung von neuen selbst-definierten Anforderungen, wie sie durch die Stakeholder als wünschenswert erachtet wurde.

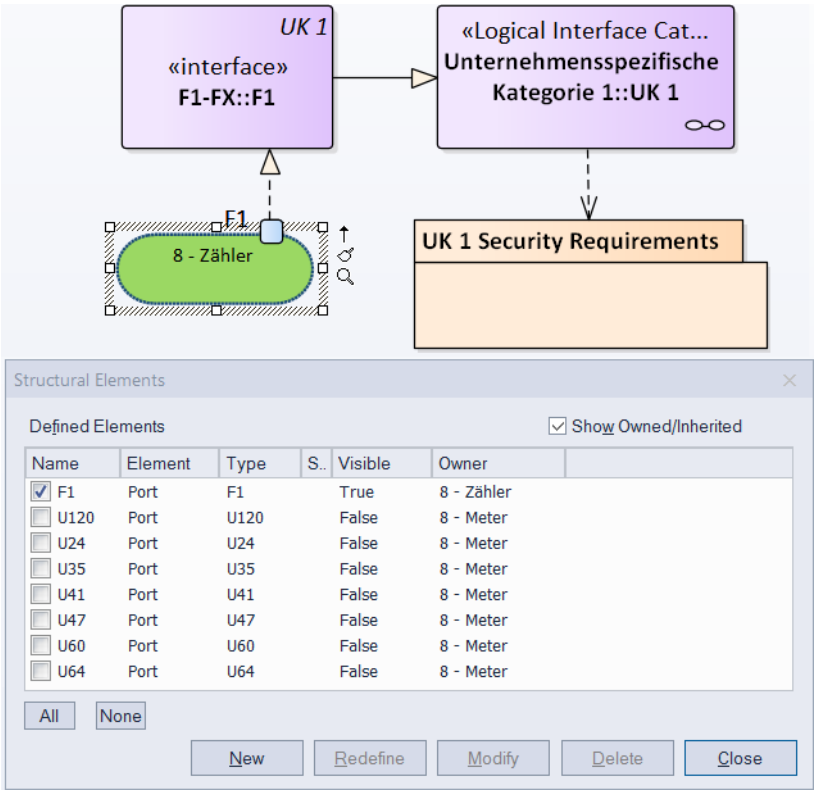



Abbildung 4.21: Erweiterung des *8 - Meter* im Domänenmodell .AT

## 4.3 Evaluierung der Bericht-Generierung

In diesem Abschnitt wird die von Enterprise Architect und SGAM Toolbox zur Verfügung gestellte Funktion für Berichtsgenerierung präsentiert. Die Ergebnisse basieren auf eigens für diese Domäne geschaffenen Vorlagenschemata.

### 4.3.1 Reports zur Gesamtübersicht

Ein umfangreicher Einblick in die Modelle ergibt sich bei der Erkundung einer generierten Dokumentenbeschreibung, die nach vorgefertigten und in der SGAM-Toolbox hinterlegten Definitionen sämtliche Inhalte der Referenzarchitektur in eine PDF-Datei oder ein Microsoft Word-Dokument packen können. Eine beispielhafter Bericht der Referenzarchitektur mittels der *SGAM Project – Section (detailed) Report* Vorlage, die im Funktionsumfang der SGAM Toolbox enthalten ist, umfasst hierbei 1.125 Standard-DIN A4 Seiten mit knapp 125.000 Wörtern. Ein Teil davon entfällt auf das Grundmodell von NIST LRM, welches in die SGAM Toolbox importiert wurde. Angesichts dieser großen Zahl an Seiten wird ersichtlich, dass der modellgetriebene Ansatz zur Verarbeitung und Hinterlegung solcher Informationen Vorteile gegenüber sonst üblicher Tabellen oder Textdateien bietet.

Auflistungen wie diese sind nicht allein für einzelne Geräte maßgeschneidert, sondern auf vollständige Use Cases anwendbar. Hierbei werden die Informationen der jeweiligen verwendeten Elemente nach dem definierten Schema aufgelistet. Enterprise Architect bietet vielerlei Optionen und Filtermöglichkeiten bei der Anpassung der Dokumentengenerierung, die allerdings Einarbeitungszeit und ein Verständnis der verwendeten UML-Typen für ein brauchbares Ergebnis voraussetzen.

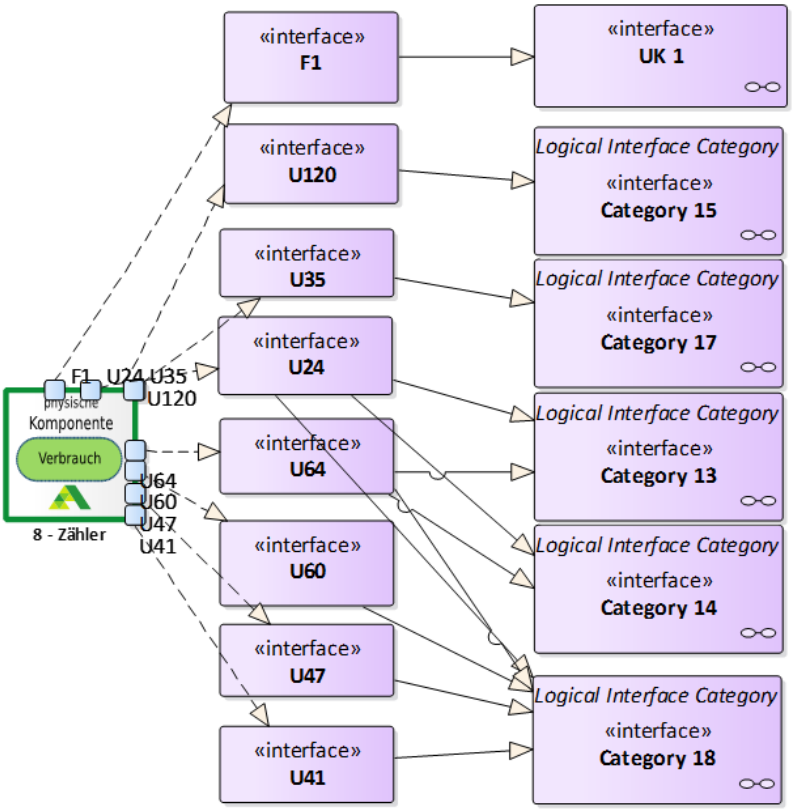
In Abbildung 4.22 ist ein Ausschnitt einer weiteren Darstellungsmöglichkeit für die verwendeten Elemente aus einem Use Case dargestellt. Die Darstellung bereitet jene hinterlegten Informationen sowohl tabellarisch als auch grafisch in Diagrammen auf, die in den Interfaces und Kategorien der im Use Case verwendeten Komponente hinterlegt sind. An erster Stelle zu sehen sind die gesondert positionierten *CIA*-Werte für die *Categorie 13* nach deren Beschreibungstexten. Die Attribute haben in diesem Export ebenso die Kurzbeschreibungen mitgeliefert.

Bei dem Export muss erwähnt werden, dass bei dieser großen Seitenzahl immer wieder Wiederholungen vorkommen. Diese hängen zum einen trivialerweise von der Modellierungsgranularität ab als auch dem „Aufräumverhalten“ der Nutzer_innen. Werden neue Elemente in Use Cases spezifiziert und später nur vom Diagramm gelöscht, bleiben diese im Projekt Browser weiterhin enthalten und würden je nach Dokumentationsvorlage mit ausgegeben werden. Hier ist derzeit noch ein aktives Nachverfolgen von nicht verwendeten Elementen notwendig.

### 4.3.2 Semiautomatische Generierung von Checklisten

Anhand der oben genannten großen Anzahl an Textseiten ist die Frage nach reduzierten und spezifischen Informationen, wie etwa zur Abarbeitung der Sicherheitsanforderungen eines modellierten Use Cases als Checkliste naheliegend. Die Regeln der Berichtgenerierung lassen sich individuell für die jeweiligen Bedürfnisse der Endnutzer und Zielgruppen anpassen. Diese beginnen bei der Erstellung von formlosen Checklisten und reichen bis hin zu einheitlichen Spezifikationen im Corporate Design. Nachfolgend ist in Abbildung 4.23 eine formlose Checkliste beispielhaft angeführt. In dem generierten Originaldokument stehen 73 Aufzählungspunkte zu Sicherheitsanforderungen, welche sich aus dem NIST LRM aufgrund der vorgestellten Modellierungsweise ableiten lassen. Die drei Punkte in der Mitte der Abbildung stehen für die zu Darstellungszwecken ausgelassenen weiteren Security Requirements. An erster Stelle ist das in 4.2.5 definierte Security Requirement unter dem Text des *Smart Breakers* zu sehen.

Die Funktionalität der Dokumentengenerierung ist im Zuge eines Stakeholdertreffens mit einem Netzbetreiber (KNG) vorgestellt worden und hat zu Anregungen des vorhandenen Prozesses bei Dokumentierungsvorgängen vor allem hinsichtlich Ausschreibungen geführt. Hier kann ein standardisierter Prozess mit der Hinterlegung einer Vielzahl von Informationen als Dokumentationsgrundlage und Abstimmung der Mindestanforderungen für einen (Teil-)Bereich der Ausschreibung in einem einheitlichen Stil helfen.




8 - Zähler

| Category 13 | | |
|---|---|---|
| 13. Interface between systems that use the AMI network, for example:<br>• Between MDMS and meters<br>Between LMS/DRMS and Customer EMS | | |
| Availability | Confidentiality | Integrity |
| HIGH | HIGH | HIGH |
| ATR-12: Insecure, untrusted locations | Devices or systems in locations which cannot be made more secure due to their physical environment or ownership, pose additional security challenges. For instance, hardware-based cryptography may be necessary. | x |
| ATR-13: Key management for large numbers of devices | Key management for large numbers of devices without direct access to certificate management may limit the methods for deploying, updating, and revoking cryptographic keys. | x |
| ATR-14: Patch and update management constraints for | Patch management constraints may limit the frequency and processes used for updating security patches. | x |

Abbildung 4.22: Auszug einer beispielhaften Auflistung von *CIA*-Kriterien und Sicherheitsattributen aufgrund des NIST LRM.

Security Requirement Check List für: A Customer Energy Management Security Requirements List

| Name des Security Requirements | Wurde geprüft |
|---|---|
| **Requirements für: Smart Breaker** | |
| • Erstes unternehmensspezifische Security Requirement | |
| • SG.AC-1 Access Control Policy and Procedures | |
| • SG.AC-11 Concurrent Session Control | |
| • SG.AC-12 Session Lock | |
| • SG.AC-13 Remote Session Termination | |
| ⋮ | |
| • SG.SI-6 Security Functionality Verification | |
| • SG.SI-7 Software and Information Integrity | |
| • SG.SI-8 Information Input Validation | |
| • SG.SI-9 Error Handling | |

Dokument erstellt am 03.01.2019 16:51:44 durch: wilker

Unterschrift Prüfer_in:

Abbildung 4.23: Ausschnitt einer gerätespezifischen Checkliste mit abgeleiteten Security Requirements aufgrund des NIST LRM.

## 4.4 Evaluierung durch Analysetools

Die Modelle der RASSA-Referenzarchitektur können durch Enterprise Architect und die SGAM Toolbox für die Verwendung in anderen Softwarelösungen exportiert werden, um beispielsweise Risikoanalysen oder Datenschutzfolgenabschätzungen durchzuführen. Hier wird eine Evaluierung für die Verwendung von Analysetools und -möglichkeiten, die mithilfe des Referenzarchitekturmodells durchgeführt wurden, beschrieben.

### 4.4.1 Evaluierung in AURUM

Die in 4.3 vorgestellten Funktionen dienen zur Ableitung von Security Requirements, welche in der Referenzarchitektur modelliert wurden. Allerdings müssen diese gewartet und auf dem aktuellen Stand gehalten werden, um eine Risikoanalyse gemäß dem Stand der Zeit gewährleisten zu können.

AURUM hat in der RASSA-Initiative gezeigt, wie anhand eines exportierten SGAM-Modells durch den Import in das Tool, der Eingabeaufwand gesenkt werden konnte. Darüber hinaus wurden in den Risikoberechnungen alle Modellierungsschichten berücksichtigt (RASSA → Domänenmodell .AT → NIST LRM). Eine Erweiterung um eine firmeninterne Schicht mit Anforderungen des Unternehmens ist daher ohne weiteres denkbar. Abbildung 4.24[2] zeigt den Import eines SGAM-Modells in AURUM mit einem Use Case, der aus sechs Elementen besteht. Auf der linken Seite ist das Navigationsmenü von AURUM abgebildet. Auf der rechten Seite wird ein Use Case dargestellt, der die Instanzierung von herstellerspezifischen oder anbieterspezifischen Geräten demonstriert.

[2]Screenshot aus Präsentation von Stefan Fenz für das RASSA-Konsortium, Darstellung modifiziert für bessere Lesbarkeit. Mit Dank für Wiederverwendung in dieser Arbeit.

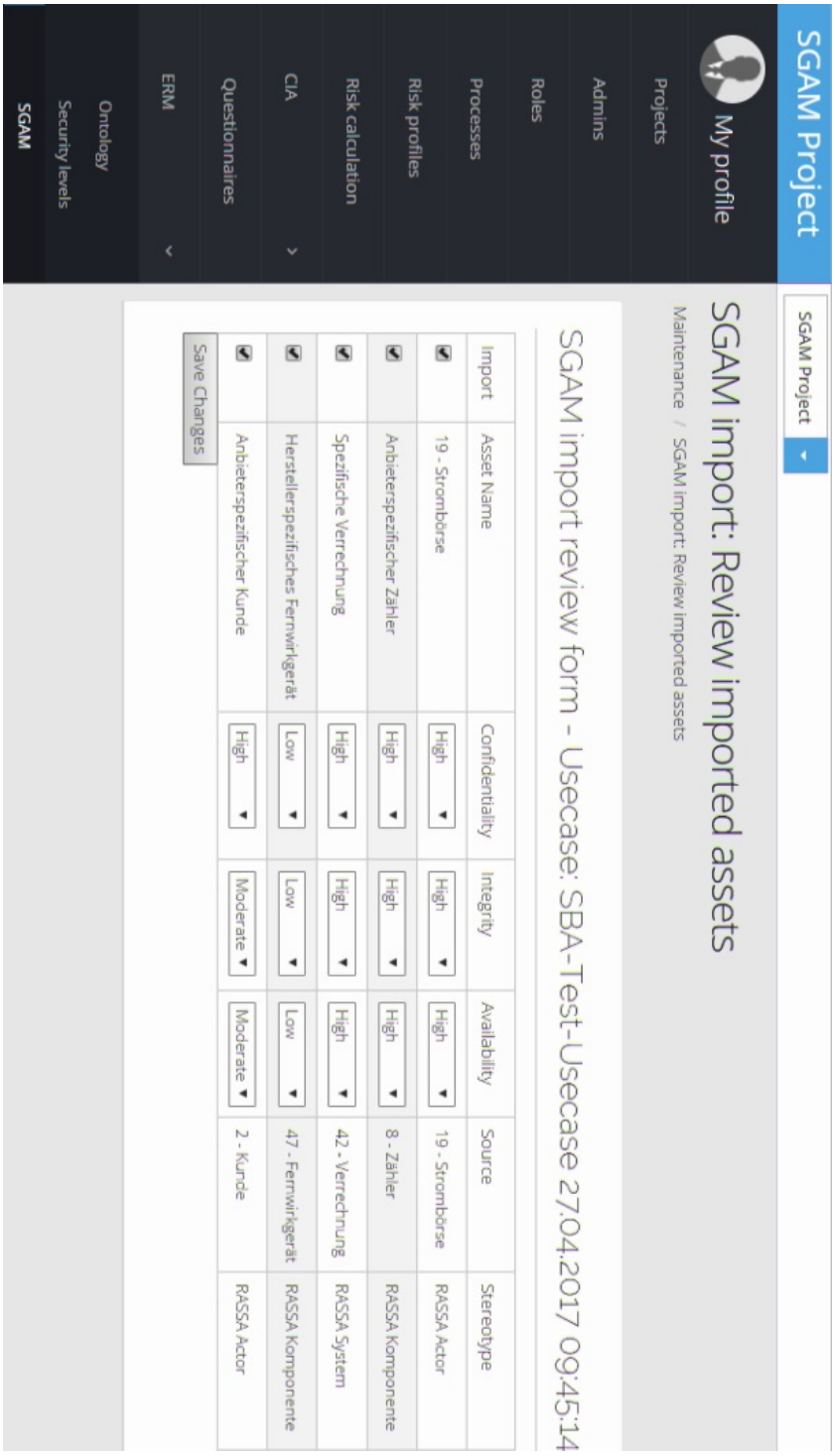



Abbildung 4.24: Import eines SGAM-Modells in AURUM

In der Abbildung 4.24 sind darüber hinaus die erfolgreich durch den Import übernommene *CIA*-Werte der einzelnen Elemente ersichtlich. Das Eltern-Element kann rechts unter *Source* gefunden werden. Der Stereotyp der Elemente steht rechts davon mit der Unterscheidung zwischen: Business-Akteuren (in Enterprise Architect als RASSA Actor deklariert), den logischen Akteuren (RASSA System) und den physischen Komponenten (RASSA Komponente).

In AURUM wurden Ergebnisse des Smart Grid Security Guidance $(SG)^2$ - Projekts [104] eingearbeitet, die Bedrohungen, Schwachstellen und Gegenmaßnahmen beinhalten. Durch eine semantische Wissensdatenbank können Bedrohungen und potentielle Gegenmaßnahmen besser identifiziert werden [70]. Speziell in Bezug auf ein importiertes SGAM-Modell konnten Kontrollfragen durchgeführt werden, die auf den unterschiedlichen Klassen des Modells beruhen. Für die Komponenten, die eine große Bedrohung darstellen, konnten Gegenmaßnahmen vorgeschlagen werden.

Durch AURUM konnte die Verwendung eines nicht modifizierten SGAM-Modells für die Risikoanalyse demonstriert werden. Eine Evaluierung der Ergebnisse einer derartigen Risikoanalyse für die iniGrid Use Cases liegt außerhalb des Rahmens dieser Diplomarbeit, in welcher die Modellierung und Kompatibilität zu anderen bestehenden Lösungen im Vordergrund steht.

### 4.4.2 Evaluierung im DPIA Tool

Das im 2.4.1 beschriebene DPIA Tool kann Enterprise Architect Modelle importieren, weshalb auch damit eine Evaluierung der iniGrid Use Cases durchgeführt werden kann. Aus dem exportierten SGAM-Modell können drei unterschiedliche Arten von Informationen im DPIA Tool importiert werden:

1. Primäre Systeminformationen, die in einem System ausgetauscht oder gespeichert werden. Hier werden auch persönliche Daten der Kund_innen herangezogen.
2. Unterstützende Systeminformationen, die alle Komponenten der Systeminfrastruktur wie Software, Hardware oder Netzwerkgeräte darstellen.
3. Assoziationen zwischen primären und unterstützenden Systeminformationen, wie zum Beispiel durch Lastprofilinformationen, die im Kundenenergiemanagementsystem gespeichert sind, werden der entsprechenden Hardware und Software zugeordnet.

Eine Evaluierung wurde in [69] durch Ewa Piatkowska[3] durchgeführt. Für die RASSA-Initiative wurde diese Evaluierung anhand eines Use Cases, der mittels SGAM Toolbox erstellt wurde, durchgeführt. Dabei handelt es sich um das Beispiel eines Energieportals und die Beurteilung des potenziellen Risikos der Privatsphäre für Kunden.

[3]Mitarbeiterin am AIT Austrian Institute of Technology GmbH, Projektpartner im RASSA-Architektur Projekt

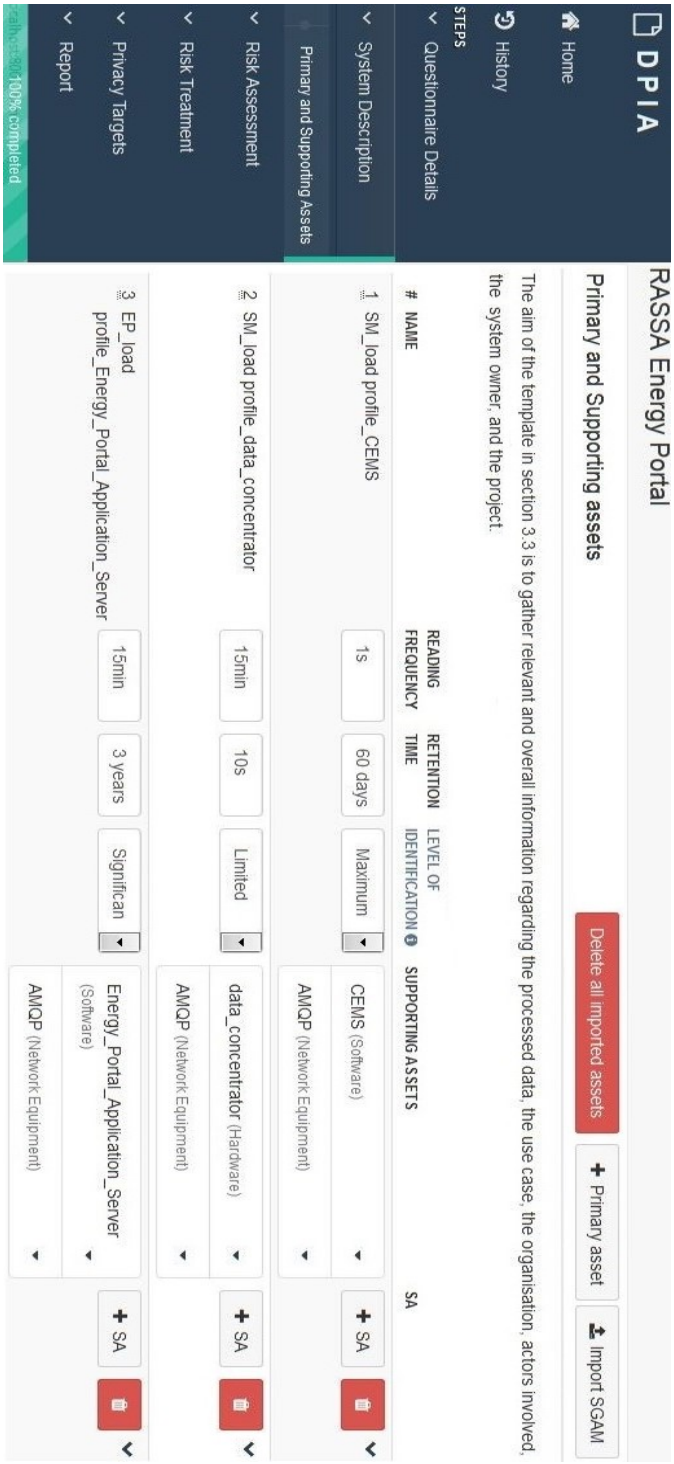



Abbildung 4.25: Screenshot des DPIA-Tools mit geöffnetem Tab zur Systembeschreibung und importierten Daten von SGAM-Elementen aus einem Use Case [69].

Wie in Abbildung 4.25 ersichtlich, können für die primären Systeminformationen (in diesem Ausschnitt drei unterschiedliche) weitere Daten zur Datenlesehäufigkeit, der Speicherdauer und der Gewissheit der Identifikation eingegeben werden. Diese sind spezifisch für die Datenschutzfolgenabschätzung, falls es zu einer Kompromittierung des Systems kommt.

### 4.4.3 Evaluierung der SGAM Toolbox Risikoabschätzung

Die SGAM Toolbox ermöglicht eine Risikoabschätzung. Ein Ausschnitt dieser ist zur Veranschaulichung in Abbildung 4.26 dargestellt. Die roten Kästchen kennzeichnen Risiko-Elemente, welches beim Modellieren verwendet werden kann.

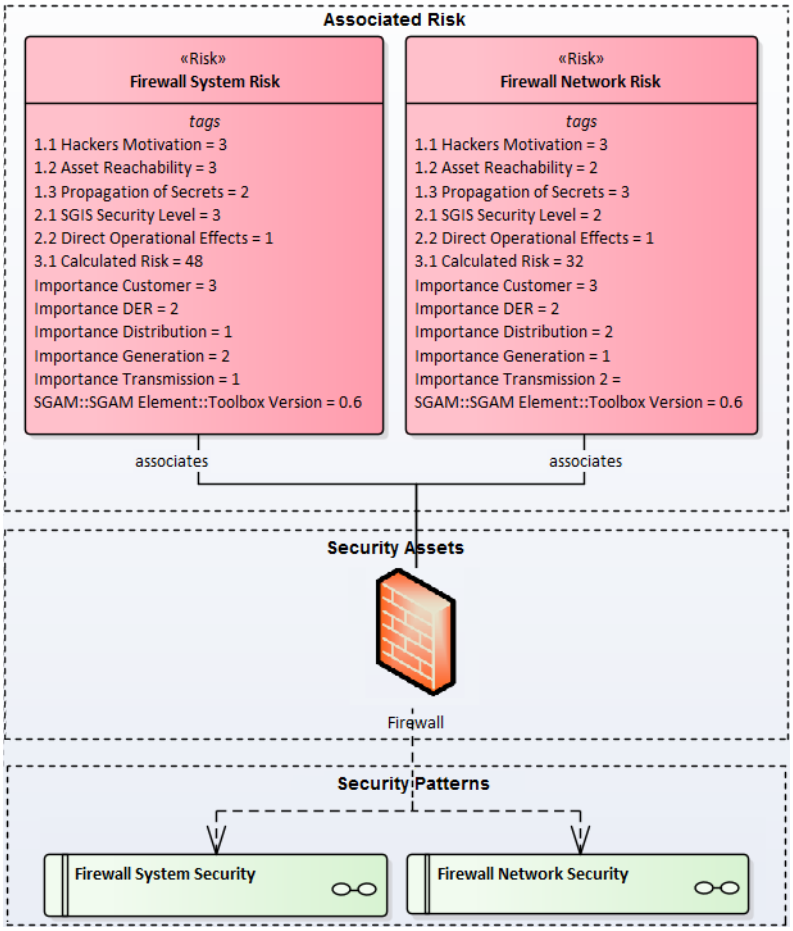



Abbildung 4.26: Screenshot einer erweiterten Risikoabschätzung und der Verbindung zugehöriger Elemente innerhalb der SGAM Toolbox [13].

In diesem Beispiel sind folgende Werte im Risiko-Element als *Tags* hinterlegt worden, die nach [95] wie folgt beschrieben sind:

1.1 Hackers Motivation: Schätzung der Attraktivität eines Ziels für Cyber-Angreifende (Hacker_innen).

1.2 Asset Reachability: Die Erreichbarkeit eines Assets (zu verstehen als Komponenten oder Systemzugangspunkte) spiegelt wider, ob ein Asset beispielsweise über das Internet, nur über das Unternehmensnetzwerk oder durch physische Präsenz in einem eingeschränkten Bereich wie zum Beispiel einem Kontrollraum erreichbar ist.

1.3 Propagation of Secrets: Es wird die Anzahl der Zugriffsberechtigten bestimmt, die den Zugang kennen, um auf ein bestimmtes Asset zuzugreifen.

2.1 SGIS Security Level [105]: Das Smart Grid Information Security - Security Level ist eine Einschätzung nach der Reichweite und Schwere eines möglichen Stromausfalls. Der Wert 5 wird verwendet, wenn es zu einem europaweiten Stromausfall kommen würde und 1 wenn nur die Nachbarschaft oder eine Stadt betroffen wäre. Die Autor_innen haben eine Tabelle [105, S. 10] geschaffen, in der die Abschätzung für Komponenten und Systeme bei der Verortung in die SGAM-Domänen und -Zonen gegeben ist.

2.2 Direct Operational Effects: Hier wird ein Wert zwischen 0 und 1 angegeben, der einen Faktor für die Einschränkung im Falle eines gehackten Assets widerspiegeln soll.

3.1 Calculated Risk: Eine Berechnung des Risikos ist ausführlich in [95] beschrieben.

Je höher das berechnete Risiko, desto intensiver muss die Komponente oder das System abgesichert werden. Die Motivation dieser Aufteilung liegt darin, die untersuchten Risiken vergleichbar zu machen und deren Prioritäten festzulegen [13].

Die SGAM Toolbox ermöglicht den Export dieser Risikoelemente, um in einer Microsoft Excel Tabelle die Risikoberechnungen durchführen zu können. Auch ein Import des Ergebnisses ist im Anschluss möglich. Die weiters dargestellten in den *Tags* definierten Werte, stellen Beispiele für die Demonstration von firmenspezifischen Erweiterungen dar. Der neu eingeführte *Importance*-Wert der fünf SGAM-Domänen ist ein Beispiel, nach dem die *Firewall* je nach Domänenzuordnung eine höhere oder geringere Wichtigkeit erhält um entsprechenden Einfluss auf die Risikoberechnung haben zu können.

Die SGAM Toolbox ermöglicht in der verwendeten Version die Erstellung von drei unterschiedlichen Security Patterns. Diese sind vorangefertigte Diagramme, die mit wenigen Klicks erstellt werden kann. In Abbildung 4.27 ist ein Beispiel für die Erstellung eines *Network Security Pattern* für das Element *Firewall* zu betrachten. Man kann darauf erkennen, dass unterschiedliche Maßnahmen nach der Legende getroffen werden sollten.

Die zur Verfügung gestellten Patterns befinden sich noch in der Entwicklung und werden in folgenden SGAM Toolbox Versionen weitere Informationen beinhalten.

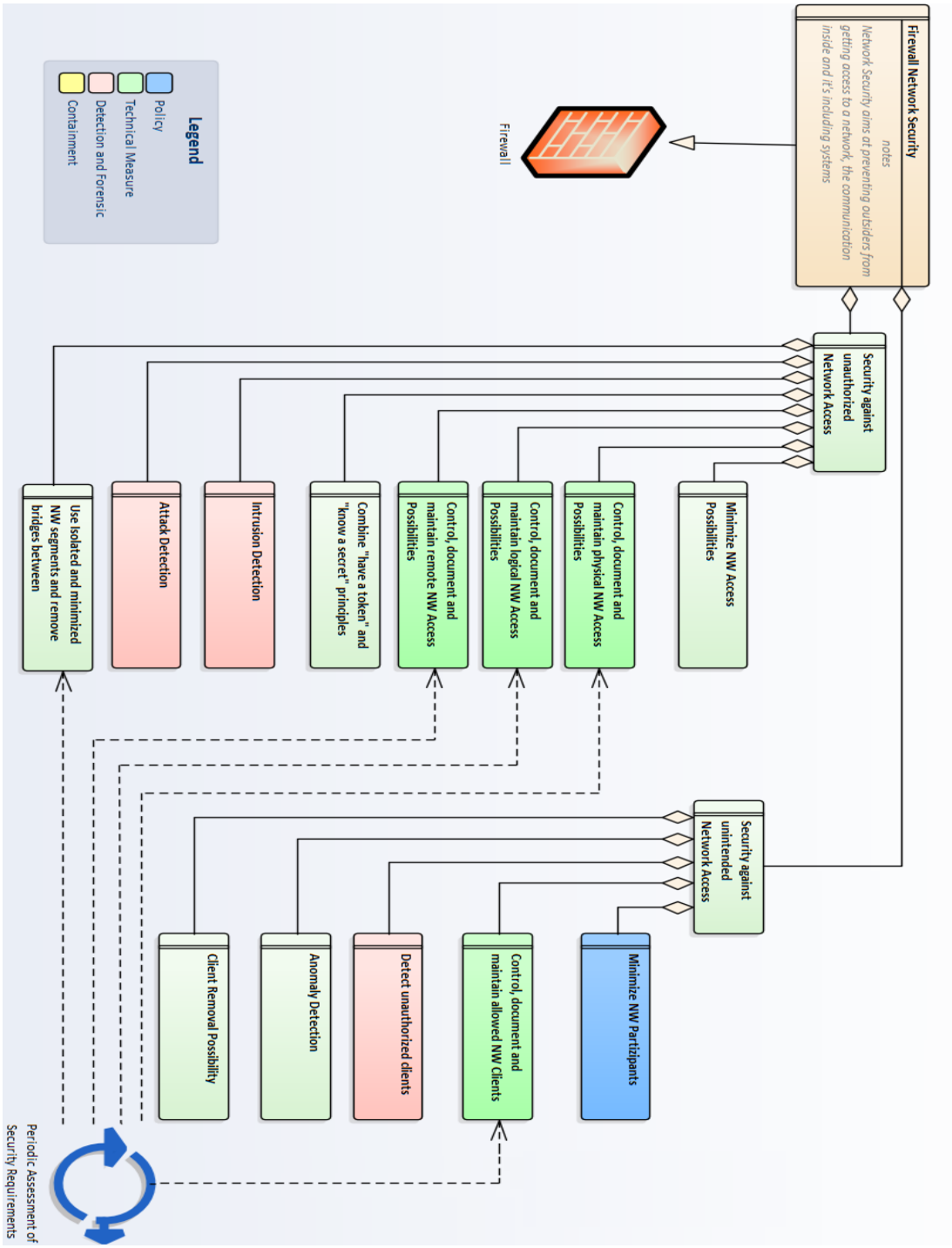



Abbildung 4.27: Screenshot eines erstellten *Network Security Pattern* für das Element *Firewall* [13].

Die Farbe der Kästchen aus Abbildung 4.27 gibt eine Unterscheidung für die empfohlene Maßnahme an. Richtlinien sind als blaue Rechtecke dargestellt, technische Maßnahmen grün, Erkennung und Forensik sind hellrot und Eindämmungsmaßnahmen sind gelb [13].

Um beispielsweise die Security gegen unbeabsichtigten Netzwerkzugang zu erhöhen, wird als Richtlinie empfohlen, die Anzahl der Netzwerkteilnehmer_innen klein zu halten. Im Gegenzug dazu wird für die Security gegen unautorisierten Netzwerkzugang empfohlen, die Möglichkeiten des Zugangs zum Netzwerk zu reduzieren. All die im Diagramm dargestellten Schritte sollten regelmäßig durchgeführt werden, eine Prozess der durch die zwei blauen Pfeile gekennzeichnet ist.

Ein Vorteil ergibt sich durch den schnellen Zugriff auf diese Patterns und die Wissensbasis die dadurch schnell für die Anwender_innen verfügbar ist. Die erstellten Diagramme lassen sich erweitern, auch das Erstellen von neuen (firmenspezifischen) Patterns ist technisch möglich.

Während die hier beschriebenen Ausführungen lediglich eine Einführung und Evaluierung bezüglich individueller Erweiterungsmöglichkeiten zu dem Thema geben können, wird in [95] das Thema der Risikoabschätzung und Berechnungsmöglichkeiten vertieft.

## 4.5 Evaluierung durch Stakeholder

Die Schaffung der RASSA-Referenzarchitektur benötigte die Zusammenarbeit von vielen Organisationen, Arbeitsgruppen und die Abstimmung und Diskussionen mit Stakeholdern. Ziel der Referenzarchitektur ist es, die unterschiedlichen Stakeholder für Smart-Grid-Lösungen dabei zu unterstützen, solche zu realisieren. Die Aufsplittung und Standardisierung mit den SGAM-Ebenen sollten von Anfang an die unterschiedlichen Sichtweisen im Entwicklungsprozess begleiten. So sollte eine gemeinsame Sprache für die Akteure, Komponenten und die Schnittstellen im Smart Grid geschaffen werden. Durch die in dieser Arbeit präsentierte Herangehensweise können international standardisierte Sicherheitsanforderungen in diversen Repräsentationen einer breiten Basis an Endanwender_innen zugänglich gemacht werden.

Dieses Kapitel evaluiert die Ergebnisse die auf Diskussionen und Vorstellungen mit Stakeholder zurückzuführen sind. Für detaillierte Ergebnisse wird auf [8] verwiesen.

### 4.5.1 Evaluierung durch Netzbetreiber

Die Integration von neuen Smart-Grid-Komponenten und der damit einhergehenden Security Requirements müssen bewältigt werden. Die Verwendung der RASSA Referenzarchitektur stellt eine Möglichkeit dar, wie diese durch Netzbetreiber unter Zuhilfenahme von Modellierung durchgeführt werden kann. Die Verwendung eines SGAM-Modells erfordert eine Zuordnung spezifisch für jede Ebene. Dadurch lässt sich die Kommunikation intern sowie extern vereinfachen, da der Verwendungszweck der SGAM-Ebene und der zwischen den Akteuren bestehenden Beziehungsarten vordefiniert ist. Um komplexe

Smart-Grid-Lösungen zu schaffen benötigt es die Fusion von Informations- und Kommunikationstechnologie mit den elektrischen (Steuerungs-)Systemen. Die für den ersten Schritt notwendige gemeinsame Sprache als auch das gemeinsame Verständnis konnte durch das Zusammentragen des Wissens der Stakeholder in der Referenzarchitektur erreicht werden.

Die Vorstellung der Bericht-Generierungsfunktion eröffnete beim Stakeholdertreffen mit den Netzbetreibern neue Möglichkeiten. Diese können bei einem abgestimmten Vorgehen als wichtiges Werkzeug für die Verwendung von zum Beispiel Ausschreibungsinhalten verwendet werden, anhand welcher auch besser mit den Herstellern kommuniziert werden kann. Durch die Ableitung von Anforderungen aus einem Referenzarchitektur-Modell kann die Erfüllung von gesetzlichen und technischen Umsetzungen geprüft werden, sofern die Datenbasis dafür gepflegt wird. Ein aktuelles Beispiel hierfür ist die Intelligente Messgeräte-Einführungsverordnung, welche auch IME-VO genannt wird. In dieser sind die Vorgaben zur Einführung von intelligenten Messgeräten (Smart Meter) aufgeführt, die aufgrund der technischen und rechtlichen Machbarkeit hinsichtlich ihres Zeitplans geändert wurde. Darin wurde zuerst ein Ausrollungsgrad (Austausch von konventionellen Messgeräten) von 95% bis Ende 2019 vorgeschrieben, der allerdings voraussichtlich nicht erreicht werden kann [106].

Die in 4.4 beschriebene Herangehensweise zeigt, dass die RASSA-Referenz-architektur als Grundlage für eine Risikoanalyse dienen kann. Wenn darüber hinaus Kenntnisse über Datenobjekte, physischen (verbauten) Komponenten und verwendeten Protokollen zur Verfügung stehen, können Auswirkungen von bekannten Angriffen so besser und schneller eingeschätzt werden. Darüber hinaus können die in dieser Arbeit beschriebene Methode und in den Stakeholder-Treffen präsentierten Funktionen zukünftige Anwender_innen bei der Dokumentationspflicht unterstützen. Die Dokumentationsfunktion müsste allerdings weitere Arbeiten und Anpassungen durchlaufen, um den Ansprüchen und gesetzlichen Auflagen zu entsprechen. Die Grundfunktion wurde allerdings schon als guter Ausgangspunkt erachtet [8].

### 4.5.2 Evaluierung durch Lieferanten und Stromhändler

Der auf den Technologiefortschritt und die Öffnung des regulierten Marktes zurückzuführende sich schnell entwickelnde Markt steht ähnlichen Herausforderungen, wie denen in 4.5.1, gegenüber. Die Anzahl der notwendigen Schnittstellen um am kompetitiven Marktgeschehen teilzuhaben steigt. Zudem werden gesetzliche Anforderungen für die neuen Smart-Grid-Lösungen definiert. Erste Änderungen können schon durch das Inkrafttreten der Datenschutzgrundverordnung beobachtet werden, da die unterschiedlichen Anbieter teilweise neue Geschäftsmodelle durch die Verarbeitung personenbezogener Daten verfolgen.

In den Stakeholder-Gesprächen wurde festgestellt, dass die Schnittstelle zwischen den Netzbetreibern und Lieferanten nicht als kritisch für den Betrieb des Stromnetzes einzustufen ist. Dennoch müssen geltende Security Requirements erfüllt werden. Bei einer Einigung auf eine gemeinsame Basis, die durch die Referenzarchitektur weitergegeben werden kann, kann diese dabei helfen, die bestehenden Schnittstellen besser abzusichern.

Große Herausforderungen entstehen durch die Digitalisierung und der damit einhergehenden Geschäftsmodelle. In 5.2 wird auf die Identifizierung eines neues Gefahrenfelds im Zuge der Digitalisierung näher eingegangen-

Energielieferanten und Stromhändler sollten daher ihre Anwendungen auf Basis der Referenzarchitektur modellieren, um über interoperable Schnittstellen zu Markt und Netzbetreiber zu verfügen. Die Durchführung einer Datenschutzfolgenabschätzung oder eine allfälligen Risikoanalyse wird durch vorhandene Modelle maßgeblich erleichtert.

Bei der Verwendung der Referenzarchitektur konnte unter anderem durch die Generalisierungsbeziehungen bereits modellierte Eigenschaften von den in 4.4 angeführten Programmen Datenschutzfolgenabschätzungen oder Risikoanalysen ohne zusätzliche Eingaben erfolgreich durchgeführt werden. So lässt sich eine mögliche neue Anbindung über Schnittstellen zum Markt oder Netzbetreiber auf Modellierungsebene abschätzen, bevor es eine prototypische oder echte Realisierung gibt. Aufgrund der Inklusionsmöglichkeit von Gefahrenkatalogen und Security Requirements, lassen sich der notwendige Aufwand und vor allem die erforderlichen Akteure im Vorhinein besser abschätzen.

### 4.5.3 Evaluierung durch Komponentenhersteller

Komponentenhersteller können durch die Verwendung der RASSA-Referenzarchitektur Vorteile erzielen. Durch die Verwendung von standardisierten und vordefinierten Schnittstellen lässt sich eine größere Interoperabilität zwischen den Systemen erreichen. Die Ansammlung von internationalen oder nationalen Security Requirements können den Entwicklungsprozess durch zielbewusste Entwicklung unterstützen. Wie in 4.2.5 gezeigt, können eigene firmeninternen Security Requirements durch eine eigene Modellierungsschicht realisiert und eigenen Produktreihen zugewiesen werden.

Als weiteren Vorteil sehen die Komponentenhersteller, dass sie sich einfacher auf die Ausschreibungen verschiedener Netzbetreiber beziehen können, wenn sie auf den gleichen Sicherheitsmaßnahmen basieren. Hierfür ist allerdings eine Einigung der Netzbetreiber auf die notwendigen Standards notwendig. Eine Referenzarchitektur kann durch die nachvollziehbaren Konzepte zu *Security by Design* die Herkunft der Anforderungen nachvollziehbar machen. Durch eine einheitliche mit wenigen Klicks durchführbare Dokumentationsmöglichkeit mittels Enterprise Architect und SGAM Toolbox können so Ausschreibungs- und Evaluierungsprozesse vereinfacht werden.

Allerdings wurden auch Hürden der Komponentenhersteller in den Stakeholder-Gesprächen genannt. Die größte Herausforderung sehen diese bei der Überführung und Einpflegung des Altbestands in ein solches System. Dafür werden individuelle Export- und Importfunktionen für die Verwaltungsprogramme notwendig, um einen nutzbaren Ist-Stand des breiten Komponentenangebots abbilden zu können.

### 4.5.4 Evaluierung durch Politik und Verbände

Zum Zeitpunkt des Verfassens dieser Arbeit ist der hier präsentierte Stand der Referenzarchitektur eine Momentaufnahme der sich immer weiter verändernden Umstände und

Anforderungen. So müssen Security Requirements überarbeitet werden, sobald neue Angriffswege und -techniken erkannt werden, und in die Referenzarchitektur aufgenommen werden. Wenn sich Gesetze und regulatorische Rahmenbedingungen ändern, muss eine entsprechende Abbildung vorgenommen werden. Neue Anwendungen oder Komponenten, wie sie innerhalb des iniGrid-Projekts entstanden sind, können die Definition von neuen Kategorien oder Schnittstellen erfordern. Nur wenn entsprechende Schutzmaßnahmen definiert angewandt werden, stellen neu(artig)e Komponenten und Anwendungen kein großes Risiko für die Security des Stromnetzes dar. Die Verwendung (und damit einhergehende Pflege) einer Referenzarchitektur kann so den Sicherheitsgrad potentiell erhöhen.

Da eine Umsetzung für den Schutz des Stromnetzes besonders wirksam ist, wenn diese flächendeckend ausgerollt wird, muss eine Referenzarchitektur für alle (Übertragungs-, Verteiler- und Telekom-)Netzbetreiber gepflegt werden und den aktuellen Stand der Technik repräsentieren können.

Bei den Gesprächen mit den Stakeholdern ist die vorherrschende Meinung, dass für die Validierung der notwendigen Security Requirements und die Pflege der Modelle eine zentrale Instanz in die Verantwortung genommen werden muss. Dabei sollte sich diese auch auf europäischer Ebene mit anderen Teilnehmern des Marktes abstimmen. Als Vorschlag für diese mögliche Rolle wurden Österreichs Energie oder Österreichischer Verband für Elektrotechnik genannt, welche diese Aufgabe übernehmen und repräsentieren könnten.

KAPITEL 5

# Diskussion

Die Schaffung einer Referenzarchitektur, wie sie durch die RASSA-Initiative angestrebt wurde, erfordert zahlreiche und vor allem unterschiedliche Kooperationspartner_innen, die mit ihrem Domänenwissen das Modell bereichern können. In diesem Kapitel werden unterschiedliche Sichtweisen und gesammelte Ergebnisse diskutiert, die über diese Arbeit gewonnen werden konnten.

## 5.1 Diskussion der vorgestellten Lösungen

Nachfolgend werden die vorgestellten Lösungen und Konzepte diskutiert. Es wird auf den in Kapitel 2 beschriebenen Stand der Technik eingegangen und die möglichen Vorzüge bei dem Einsatz der jeweiligen Lösung werden erörtert.

#### Bedeutung von Referenzarchitekturen

Speziell im Bereich Smart Grid werden neben der Definition und Anwendung von SGAM Lösungsansätze unternommen, die viele der Herausforderungen behandeln.

Wie bereits durch die in 2.2 angeführten Beschreibungen der verschiedenen Themengebieten von Referenzarchitekturen deutlich wird, bewegen sich aktuelle Bestrebungen bei komplexen Systemarchitekturen hin zu sicheren und übersichtlichen Lösungen.

Derzeitige Entwicklungen zeigen, dass die Herangehensweise, die durch SGAM ermöglicht und erprobt wurde, auch auf andere Domänen und Anwendungsfälle anwendbar ist. So kann die Schifffahrt profitieren, den Informationsaustausch von heterogenen Systemen zu harmonisieren [107] oder das SGAM-Prinzip für die immer stärker aufkommende Elektromobilität eingesetzt werden [108].

Projekte im Gesundheitswesen haben bereits erkannt, dass eine domänenspezifische Modellierung mit strikten Regeln keineswegs einfach ist. Nur durch die Zusammenarbeit

von Modellierungsexpertinnen und -experten mit Expertinnen und -experten vom jeweiligen Fach über mehrere Iterationen hinweg können korrekte und praktisch brauchbare Umsetzungen entstehen, wie zum Beispiel in [109] oder [110] beschrieben.

Um hierbei auch wirtschaftliche Relevanz zu erlangen, wird es für die Entwicklung von sicherheitskritischen Systemen einen Zertifizierungsprozess brauchen. Probleme bei der Umsetzung müssen hierbei beachtet [109] und für eine Lösung bearbeitet werden. Kombinationen von Projektergebnissen und Programmfunktionen werden nach und nach durch Forschung und Industrie ausgearbeitet. Das Ziel ist es, dass Neuentwicklungen oder Weiterentwicklungen in der alltäglichen Arbeitsumgebung von beispielsweise Verteilernetzbetreibern mithilfe von domänenspezifischen Tools [111], wie auch die SGAM Toolbox eines darstellt, verwendet werden können [96].

In dieser Arbeit liegt der Fokus auf SGAM und der SGAM Toolbox. Die in dieser Arbeit angeführten Ausarbeitungen bieten einen Überblick an die verschiedenen Anforderungen und Funktionalitäten. Durch die detaillierten Systembeschreibungen in Referenzarchitekturen, kann mittels Austausch von Modellierungsinformationen innerhalb von Softwarelösungen, wie zum Beispiel dem DPIA-Tool oder AURUM-Tool ohne großes Zusatzwissen nützliche Funktionen ausgeführt werden. Für AURUM beispielsweise, können Informationen aus SGAM in ein Ontologie-basiertes IT Risikomanagement-Tool importiert werden, um Informationssicherheitsrisikomanagement durchzuführen [71]. Die Definition von lösungs- oder herstellerspezifischen Qualititätskriterien, deren Extrahierung den Informationsaustausch zu Drittanbieterlösungen ermöglicht, bietet einen hohen Mehrwert für den Entwurf von Smart-Grid-Anwendungen.

Das Schaffen einer Referenzarchitektur benötigt allerdings, wie durch die RASSA-Initiative oder die Arbeiten zum NIST LRM klar wird, eine große Anzahl von Mitwirkenden und einen großen Einsatz finanzieller Ressourcen. Ohne den Einsatz von Forschungs- oder Fördergelder ist es darüber hinaus schwierig, unterschiedliche (oft konkurrierende) Unternehmen für die Zusammenarbeit an öffentlich zugänglichen Endresultaten zu bewegen. Das wird nochmals verdeutlicht, wenn man die notwendige Anzahl an 484 mitwirkenden Expert_innen betrachtet, die für die initiale Erstellung *NIST-IR 7628 Guidelines for Smart Grid Cyber Security* beteiligt waren.

#### Bedeutung der Use-Case-Management-Lösungen

Vor allem offen zugängliche Lösungen für das Use-Case-Management sind positiv zu betrachten. Sie unterstützen so die Verbreitung von standardisierten Kommunikationsformen und Inhalten, die für eine Domäne essentiell sind. Durch Einhaltung von definierten Standards können Programme von Drittanbietern leichter die Daten importieren, modifizieren und wieder exportieren. Ein Beispiel hierzu ist in 2.4.2 zu finden.

Eine Versionskontrolle, wie sie im UCMR gegeben ist, hilft den Nutzerinnen und Nutzern den Evolutionsverlauf eines Use Case nachvollziehen zu können. Funktionen in einem Statusfeld für die Freigabe der Use-Case-Versionsnummer geben weitere Informationen über den Bearbeitungsstatus.

Die in 2.3.4 erwähnte dreidimensionale Darstellung in Abbildung 2.7 bietet durch die Ansichtsmöglichkeiten mithilfe von Dreh- und Zoomfunktionen volle Freiheiten in der Darstellung des Use Cases im *SGAM-Würfel*. Durch die freie „Kamerasicht“ innerhalb der Visualisierung sind die Verbindungen zwischen Komponenten und Akteuren eines definierten Use Case leichter nachzuvollziehen. So bieten interaktive Anwendungen für Use-Case-Management wesentliche Vorteile gegenüber rein textuell basiertem Austausch von Use Cases. Diese Lösungen bieten eine Unterstützung bei dem Entwurf der komplexen Zusammenhänge eines Use Cases, nehmen die notwendige Arbeit einer genauen Ausarbeitung aber nicht ab. Durch vorgefertigte Felder lassen sich fehlende Informationen einfacher beim Sichern von Eingaben überprüfen und Programme die Nutzer_innen kontextbezogen darauf hinweisen.

Die in 2.3 vorgestellten Use-Case-Management-Lösungen konzentrieren sich auf die (Weiter-) Verwendbarkeit des jeweiligen Endergebnisses. Dies wird gefördert durch den Einsatz von Standards oder das Bereitstellen von Vorlagen und bearbeitbaren Dateien. Die Endanwender_innen können so auf Basiswissen und -abläufe zurückgreifen, um die eigene Arbeit in einem bekannten Format fortzuführen.

Durch den Zugriff mit einem herkömmlichen Webbrowser ist das UCMR für jede Nutzerin und jeden Nutzer ohne technische Barrieren möglich. Das erhöht die Chancen zur Kollaboration an den Use Cases, wodurch das (projektspezifische) Repository wachsen kann. In Bezug auf die Microsoft Visio-Vorlage von DISCERN kann gesagt werden, dass die Handhabung für neue Benutzer_innen nicht schwierig ist. Notwendige Schritte zur Modellierung sind im verfügbaren Handbuch [112] beschrieben. Unterstützt wird die Handhabung durch die hilfreichen Tooltips und Meldungen, die hier ebenfalls kontextbezogen erscheinen. So werden zum Beispiel Nutzer_innen mit einer Fehlermeldung gewarnt, wenn ein Element, das für den *Component Layer* gedacht ist, in einer anderen Schicht positioniert wird. Verbesserungsfähig wäre hier anzuführen, dass das Element wieder automatisch gelöscht werden sollte, nachdem die Fehlermeldung bestätigt wird, da dies bislang nach der fehlerhaften Positionierung manuell durchgeführt werden muss [13].

#### Bedeutung von Drittanbieterlösungen

AURUM und das DPIA Tool lassen sich beide in einem herkömmlichen Webbrowser ausführen. Die Tools wurden unabhängig voneinander entwickelt und konnten beweisen, unterschiedliche SGAM-Modelle erfolgreich zu importieren und für die RASSA-Initiative zu verwenden. In 4.4.3 wurde eine individuelle Erweiterung der Risikoberechnung der von Enterprise Architect und SGAM Toolbox bereitgestellten Funktion vorgestellt.

Das in 2.4.5 beschriebene Tool ist, sofern der oder die Endnutzer_in Zugang zu Microsoft Excel und Makrounterstützung hat, ein schnell einzusetzendes Tool für erste Informationen durch den *Basic*-Modus. Für eine intensivere Auseinandersetzung ist ein *Expert*-Modus verfügbar, der deutlich mehr Informationen von den Nutzer_innen erwartet. Allerdings ist durch die Gestaltung und Formularführung die Benutzung einfach gehalten. Die Hinweise und Umsetzungsempfehlungen variieren stark in einer hilfreichen Art und Weise, je nachdem, welche Antworten gegeben wurden. So wird zum Beispiel der Hinweis gegeben,

die Kosten der durchzuführenden Maßnahmen einzuschätzen und zu koordinieren, um die Bedrohungen und Auswirkungen zu behandeln, und auch Verantwortliche für die Ausführungen dieser Maßnahmen zu ernennen.

An den hier angeführten Programmen ist vorteilhaft, dass die Struktur-Unabhängigkeit oder die Kompatibilität mit gängiger Bürosoftware wie Microsoft Excel oder einem Webbrowser zur Verfügung gestellt wird. In den Stakeholder-Gesprächen stellte sich die Systemabhängigkeit als große Herausforderung dar, vor allem, da nicht von jedem oder jeder Nutzer_in verlangt werden kann, sich in neue Programme einzuarbeiten. Export- und Importfunktionen werden als überaus wichtig gesehen um mit dem betriebsinternen Datenbestand effizient umgehen zu können. Darüber hinaus wird der Prozess der Standardisierung unterstützt, wenn eine einheitliche Darstellungsform und Austauschformat von Daten und Modellen verfolgt wird.

Einschränkungen gibt es nach dem derzeitigen Stand der Technik zum Beispiel bei der verwendeten Softwarelösung von CRISAM®, da hier noch eine entsprechende Funktion für Import und Export zur Verfügung gestellt werden müsste, um so die SGAM-Modelle in eine vom Netzbetreiber bekannte Softwareumgebung zu überzuführen (oder umgekehrt).

## 5.2 Beurteilung der Anwendbarkeit

Die Ergebnisse lassen Spielraum zur Beurteilung der Anwendbarkeit der präsentierten Vorgehensweise. Im Folgenden werden unterschiedliche Aspekte dieser Arbeit hinsichtlich der Anwendbarkeit diskutiert und unter verschiedenen Gesichtspunkten näher betrachtet.

#### Diskussion um Definition neuer Akteure

In 4.2.3 wurde die Einführung der Rolle des Prosumers für die Referenzarchitektur erläutert. In dem Vortrag *Smart Networks for the Energy Transition – A European Technology and Innovation Platform to Implement the SET-Plan* von ENTSO-E Chief Innovation Officer & Chair of ETIP SNET Konstantin Stachus am 16. Mai 2017 wurde ebenso die rechtliche Rolle des Prosumers auf der *Smart Energy Systems Week Austria* diskutiert. Hier wurde die Ansicht vertreten, dass während des Netzbezugs der Prosumer als Konsument einzuordnen ist und während der Netzeinspeisung als Produzent (und den damit einhergehenden Auflagen). Für die Verwendung innerhalb einer Referenzarchitektur oder einem UML-Modell allgemein würde es bei der Use-Case-Definition und Ausarbeitung zu zeitintensiveren Mehraufwand für den oder die Nutzer_in kommen, da diese den Anwendungsfall skizzieren, formulieren und modellieren müssen, um beiden Betrachtungsseiten des Prosumers gerecht zu werden. Solange kein ersichtlicher Mehrwert aus der Unterscheidung der Prosumer-Teilrollen gezogen werden kann, empfiehlt sich daher für Modellierungen die Verwendung der neu geschaffenen Rolle.

**Diskussion der Nützlichkeit**

Ein Problem, welches sich während der Laufzeit von RASSA-Architektur herauskristallisiert hat, waren unterschiedliche Interessen und Erwartungen an das Projekt. Als wissenschaftlicher Partner im Forschungsprojekt lag die Aufgabe in der Erarbeitung der Grundlagen, der Methodik und dem Vorgehen, wie die angesprochenen Probleme der RASSA-Initiative gelöst werden können. Konkrete Ergebnisse, wie sie in den Abschnitten 4.3.1 und 4.3.2 angeführt sind, konnten erst in den letzten Konsortiumsmeetings präsentiert werden, da erst zu diesem Zeitpunkt das notwendige Vorwissen und die technischen Möglichkeiten entsprechend geschaffen wurden. In der vorliegenden Arbeit sind die Darstellungen noch einmal bezüglich ihrer Anwendbarkeit auf die iniGrid Use Cases überarbeitet worden.

Um den Nutzen der RASSA-Methode bestmöglich auch außerhalb der hier als Anwendungsbeispiel angeführten iniGrid Use Cases darzustellen, erfordert es die Präsentation des erwartbaren Ergebnisses aus unterschiedlichen Perspektiven, um auch die Diskussion und die Weiterentwicklung durch unterschiedliche Standpunkte weiter voranzutreiben.

Für diese Diskussionsbasis können mögliche Rollen in einem größeren Unternehmen herangezogen werden und die Vorteile für die Interaktion zu anderen Rollen, Funktionen oder Partner_innen wie folgt mit Hilfe von plakativen Beispielen erläutert werden:

- Projektplaner_in: Der oder die Projektplaner_in möchte ein neues Projekt *„X“* durchführen und entsprechende Use Cases definieren. Für das erforderliche Abstraktionslevel genügen die mit der SGAM Toolbox zur Verfügung gestellten Werkzeuge. Sie erleichtern die Ausformulierung und Visualisierung von Szenarien anhand der involvierten Komponenten.

- Behörden: Sofern Behörden für die Genehmigung der Projektdurchführung eine Dokumentation oder Risikoabschätzung für die Systeme im Einsatz benötigen, können diese (mit entsprechender Anpassung der Berichtsgenerierung oder Vorlagen) mit Enterprise Architect erstellt werden.

- Geldgeber, Investoren oder Förderstellen: Für diese Anlaufstellen ist eine detaillierte Abschätzung von (Investitions-)Kosten und dem damit zu erwarteten Ausmaß der Verbesserungen oder Einbußen bei der Integration oder dem Aussparen von (zusätzlichen) Security-Features.

- Security-Engineer: Im Rahmen der Tätigkeiten eines Security-Engineer kann eine Liste von Bedrohungen, auf die Komponenten überprüft werden sollen, den Arbeitsalltag vereinfachen. Auch für Dokumentationszwecke ist eine Liste der durchgeführten Überprüfungen für einen späteren Nachweis oder der Lückensuche vorteilhaft.

- Anwenderinnen und Anwender: Es soll sowohl für unausgebildeten als auch trainierten Nutzer_innen möglich sein, Informationen zu einem Thema zu finden. Ohne

Expertenwissen soll es beispielsweise möglich sein, Informationen zu Schnittstellen eines Smart Meters zu finden.

- Unternehmen möchten eigene firmenspezifische (Security) Requirements definieren und das vorhandene Modell um diese Stufe erweitern. Eine weitere Anforderung könnte die Corporate Identity auf Formularen, Listen und Dokumenten sein.

Die Möglichkeiten und positiven Nebeneffekte, die sich durch die Arbeit an einem Modell ergeben, sind besonders erwähnenswert. So kann an Modellen kollaborativ gearbeitet werden und dabei sehen alle Anwenderinnen und Anwender den letzten Stand des definierten Use Cases oder von definierten Anforderungen.

Sowohl innerhalb dieser Arbeit als auch während des RASSA-Architektur-Projekts wurde eine modellierungstechnische Abkürzung vorgenommen, um die Anzahl der unterschiedlichen Elemente gering zu halten. Das Framework der SGAM Toolbox [85] sieht keine *Physischen Komponenten* im *SGAM Function Layer* vor, um mit Use Cases in Verbindung gebracht zu werden. Für die Verwendung und Erstellung der möglichen Endprodukte wie den Checklisten und den Berichten ist diese Zuordnung allerdings unerheblich, sowohl für die Modellierungsarbeiten als auch für die Endanwender_innen hätte die zusätzliche Abstraktionsebene durch dezidierte *Logische Akteure* für die jeweiligen *physischen Komponenten* mehr Aufwand zur Folge gehabt.

Oft werden Versionen von Text- oder Tabellendokumenten zur Bearbeitung oder Sichtung an die entsprechenden zuständigen Personen über mehrere (Unternehmens-)Schichten hinweg geschickt. So werden Änderungen und Ergänzungen in der lokalen Dateiversion ergänzt und wiederum verschickt. Es gibt hierzu zwar technische Lösungen, gleichzeitig auf einem Dokument zu arbeiten oder mit einem Versionsverwaltungssystem dem Problem von unterschiedlichen Dateiversionen entgegen zu wirken. Diese Lösungen sind aber wenig verbreitet oder technisch aufwendig umzusetzen. Demnach werden aufgrund des Aufwands oder fehlendem Wissen diese Systeme oft nicht genutzt, insbesondere über mehrere Unternehmen hinweg. Bei der Kooperation mit vielen verschiedenen Partnern greift man so schnell zu der erstbesten und am meisten bekannten Variante, dem klassischen Austausch von Dateien mittels E-Mail. Bei einer Umsetzung mit einer Modellierungssoftware muss der Schritt zur Einrichtung eines Softwarezugangs für ein kollaboratives Modell geplant und ebenso vollzogen werden.

Die Verwendung einer Referenzarchitektur ersetzt keine gründlichen Komponententests oder Tiefenanalysen. Die in dieser Arbeit vorgestellte Methode ist im aktuellen Entwicklungsstand vor allem nützlich, um sich einen Überblick zu verschaffen, deren Fokus auf Kommunikationsschnittstellen und Protokollen liegt. Tiefenanalysen hingegen benötigen das entsprechende Fachwissen, Ressourcen (in Form von Zeit und Geld) und spezielle Gerätschaften, die in einem Hardware Security Labor vorzufinden sind [113]. Durch die ableitbaren Security Requirements gibt es allerdings für Überblicksanalysen einen informationsreichen Ausgangspunkt der sich, wie in 4.2.5 gezeigt wurde, durch die Anwender_innen jederzeit erweitern lässt. Durch die *Generalize*-Beziehung wird sichergestellt, dass bestehende Informationen bei den betroffenen neuen Elementen ankommen.

**Diskussion der Relevanz**

Andere internationale Forschungsgruppen abseits der RASSA-Initiative haben auch den Bedarf an einer anderweitigen Darstellungsmöglichkeit des NIST LRM identifiziert. Die Autoren von [114] haben beispielsweise eine HTML-Webseite erstellt, die eine Filterfunktion für die Kategorien bietet. Weiters haben sie eine dreidimensionale-MATLAB Anwendung geschaffen, um die Limitierungen der zweidimensionalen HTML-Version zu überwinden. Mittlerweile wurde hier ein kommerzieller Ableger [115] entwickelt, auf dessen Startseite gefragt wird, ob das Netzwerk (des Webseitenbesuchers) NIST-konform sei. Dieses Beispiel soll verdeutlichen, dass die Arbeiten des NIST nicht nur ein Spezialthema behandeln, sondern dass es sich um eine durchaus relevante Grundlage für eine Weiterführung handelt, wie sie sowohl innerhalb der RASSA-Initiative als auch in der vorliegenden Arbeit, durchgeführt wurde.

Die Referenzarchitektur kann sich allerdings in Zukunft nur durchsetzen, wenn die Datengrundlage an den rasanten Entwicklungen von neuartigen Bedrohungen oder Komponenten für das intelligente Stromnetz angepasst und gepflegt wird. Die Zuordnung der einzelnen Gefahren konnte für das Domänenmodell .AT nicht durchgeführt werden, da diese nicht öffentlich zugänglich ist. In der neuen Version von 2018 [116] sind die Informationen noch spärlicher. Die Elemente des Domänenmodells .AT gibt es nun für Strom mit 70 Akteuren, allerdings gibt es keine detaillierte Beschriftung, was einen Abgleich erschwert. Zusätzlich befindet sich in dem Bericht [116] ein Domänenmodell für Gas, welches ähnlich zu dem für Strom aufgebaut ist.

Für den Stromsektor konnte ein neues Gefahrenfeld identifiziert werden, sodass es nun insgesamt 16 sind. Dieses Gefahrenfeld lautet:

> »Gefahrenfeld Strom XVI: Gefahren, die sich aus der Nutzung von „Elektronischen Datenaustauschplattformen“ ableiten lassen« [116, S. 18]

Der Gefahrenkatalog wurde erweitert und inkludiert nun auch die Gas-Domäne. Allerdings liegen in der 2018-Version nicht einmal mehr die Beschreibungen der Einzelgefahren vor. Da es sich um sicherheitsrelevante Informationen handelt, ist der geringe öffentlichzugängliche Zugriff nachvollziehbar. Im Sinne der Referenzarchitektur bedeutet dies allerdings, dass nur eine zentrale Instanz an vertrauliche Partner_innen die eingepflegten Informationen und Risiken weitergeben dürfte, damit diese auch die aktuellen Security Standards ableiten könnten.

KAPITEL 6

# Weiterer Forschungsbedarf

Die intensive Arbeit bei der Erstellung der Referenzarchitektur RASSA zeigte die derzeitigen Grenzen auf. Diese sind teilweise bedingt durch Modellierungssoftware oder den Entwicklungsstand der SGAM Toolbox. Etliche Neuerungen und modellierungstechnische Abkürzungen sind während des Referenzarchitekturentwurfs für die SGAM Toolbox in enger Abstimmung mit den Entwicklern eingeführt worden.

Abbildung 6.1 zeigt ein Feature, welches vom Josef Ressel Center for User-Centric Privacy, Security and Control entwickelt wurde. Die Elemente für die Referenzarchitektur sind als Blaupausenelemente gedacht und sollten nicht für die Einbindung in Use Cases oder anderen Diagrammen verwendet werden. Durch das entwickelte Kontextmenü können Elemente als *Instanz* oder *Link* in ein Diagramm eingefügt werden.

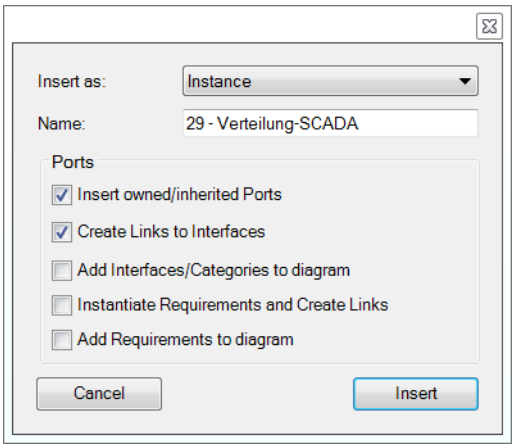



Abbildung 6.1: Screenshot eines entwickelten Komfort-Feature für Referenzarchitektur Modellierer_innen

In der Abbildung 6.1 sind Checkboxen dargestellt, mit deren Hilfe man die Security Requirements eines Elements in das aktuell geöffnete Diagramm einfügen kann. Danach

kann zum Beispiel die Generierung von Checklisten in nur wenigen Schritten durchgeführt werden. Einige Punkte liegen allerdings in der angesprochenen Struktur von Enterprise Architect und darin, wie die Modellierungsumgebung Funktionen für die Nutzer_innen zulässt. Eine Erweiterung und Entwicklung von neuen Funktionen könnte wesentliche Vorteile für die Endanwender_innen bedeuten.

In Abbildung 6.2 ist ein beispielhafter *Communication Layer* dargestellt. Der Kommunikationspfad, der zwischen den beiden Interfaces U117 von *29 - Verteilung-SCADA* zu einer physischen Komponente verläuft, ist mit der Beschriftung *Protokoll: Kommunikation Operation-Station* versehen, um die Verbindung über die Zonen des SGAM hinweg zu beschreiben. Die Linie kann mit Detailinformationen hinterlegt werden. Die

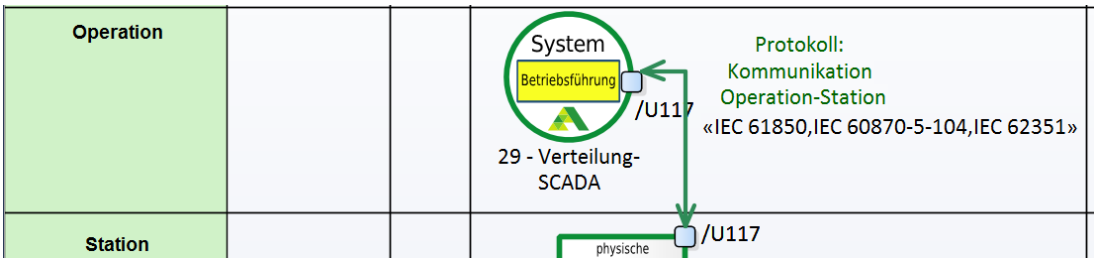



Abbildung 6.2: Screenshot einer beispielhaften Modellierung für Kommunikation und deren Verbindung über Ports [8]

Detailbeschreibung ermöglicht die Einbettung von Texten, Tags und Stereotypen. Im Beispiel des genannten *29 - Verteilung-SCADA* sind es die Kommunikationsstandards (IEC 61850, IEC 60870-5-104 sowie IEC 62351), die als ausgewählte Stereotypen in der Mitte der Abbildung 6.3 zu sehen sind. Durch die Zuweisung sind diese Beschriftungen auch in Abbildung 6.2 in schwarzer Schrift zu sehen.

Diese ausgewählten und eingegebenen Details und Eigenschaften erscheinen beim Export des Modells für externe Tools oder in der Dokumentengenerierung auf, sodass eine Analyse durch externe Lösungen möglich ist.

In Abbildung 6.4 ist ein Ausschnitt des zuvor angeführten RASSA Use Case im *Communication Layer*-Diagramm gezeigt. Auf der rechten Seite sieht man zwei Elemente die über das Interface U117 verbunden sind. Links ist die *Tag*-Detailansicht von dem unterem Element *15 - RTU/IED-Sensor/Datenempfang und Durchführung autonomer Steueraufgaben* zu sehen. In diesem sieht man die durch die SGAM Toolbox vordefinierten Felder *Domain from*, *Domain to*, *Zone from*, *Zone to*, *Zugehörigkeit*, *Interoperability Layer* und *Toolbox Version*. Die *Zugehörigkeit* ist in 3.4.3 beschrieben. Im unteren Teil der Tabelle sieht man die geerbten *Tags* von *15 Distribution RTUs or IEDs*, das aus dem NIST LRM stammt. Hier wurde die Domäne (*Distribution*) zugewiesen, aber nicht weitergegeben. Eine Funktion, die einen automatischen Werteabgleich für diese *Tags* aufgrund ihrer Position im Diagramm für die Domänen und Zonen erkennen könnte, würde die Eingabearbeit ersparen. Darüber hinaus könnten die daraus resultierenden Werte zum Beispiel in dem angesprochenen Smart Grid Information Security - Security Level in Unterkapitel 4.4.3 anhand der Position algorithmisch befüllt werden.

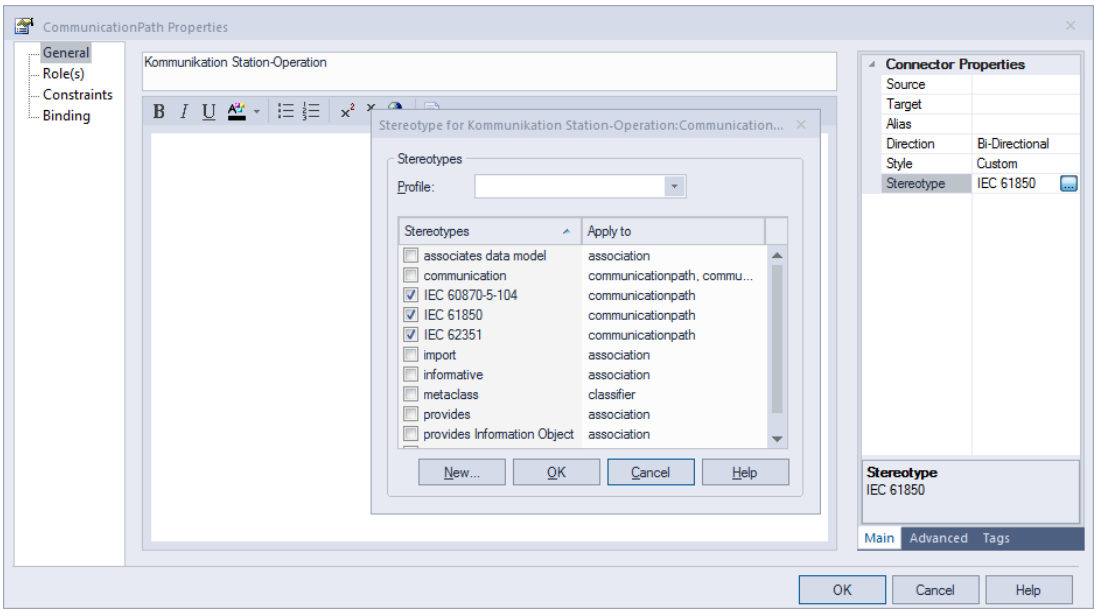



Abbildung 6.3: Detailansicht des modellierten Kommunikationspfades nach derzeitigen Stand der Software [8]

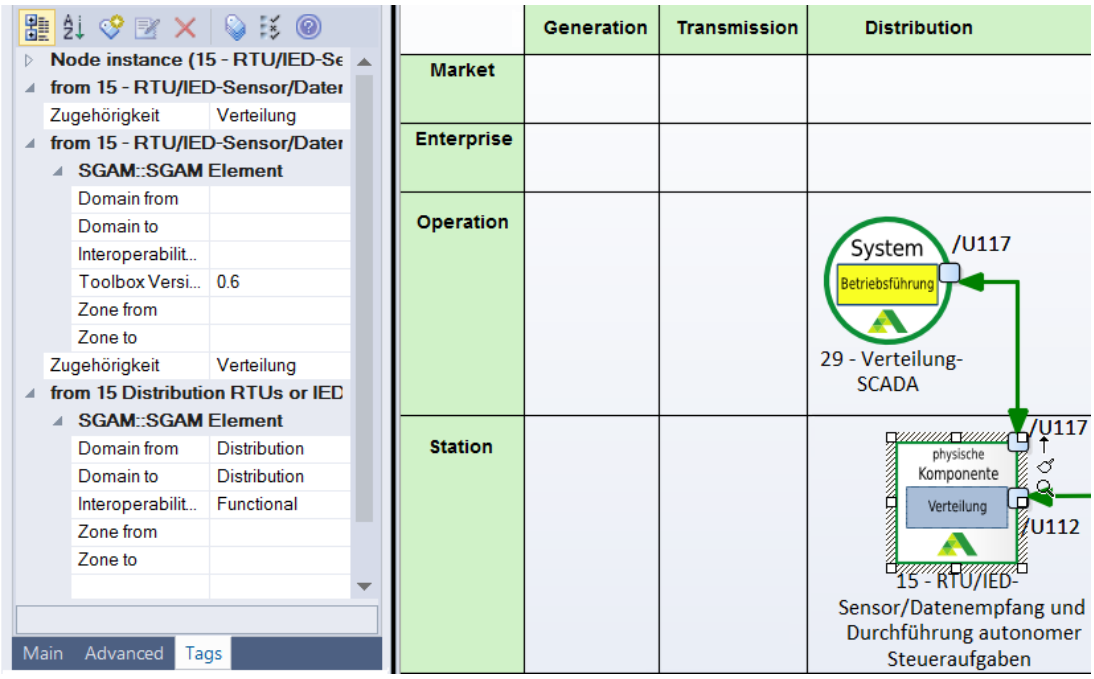



Abbildung 6.4: Screenshot eines Elements und dessen SGAM-Detailinformation in den *Tags*

Allerdings gibt es Einschränkungen im aktuellen Stand der Entwicklungstechnik von Enterprise Architect. Es ist für die Stereotypes der Kommunikationsverbindungen nicht möglich, dieselbe Art von Informationen wie bei der Modellierung von Elementen zu erreichen. Es sollte eine softwareseitige Lösung in Form eines Modifizierungsfensters oder -tools für die Kommunikationsverbindungen geschaffen werden, um Security Standards oder Security Requirements auch auf Ebene der Kommunikationsverbindungen einzubetten, wie es in dieser Arbeit durch die *Generalize*-Beziehung für die Elemente ermöglicht wird. Schließlich unterscheiden sich die Kommunikationsprotokolle untereinander und beinhalten mit unterschiedlichem Bekanntheitsgrad Risiken und Gegenmaßnahmen. Durch solch eine Zusatzfunktion könnte der Einsatz der Referenzarchitektur sowie auch der modellgetriebene Ansatz weitere Chancen für Standardisierung bringen.

KAPITEL 7

# Zusammenfassung und Ausblick

Diese Arbeit beschäftigt sich mit der Modellierung komplexer Smart-Grid-Lösungen mittels der Referenzarchitektur RASSA. Nach einer Begriffsklärung sind relevante Forschungsarbeiten zu diesem Thema am aktuellen Stand der Technik dargestellt. Es werden verschiedene Lösungen für Use Case Management beschrieben und eine Auswahl an Auswertungs- und Bewertungstools vorgestellt.

Es wird auf die Herausforderungen von Smart-Grid-Lösungen eingegangen und die verwendete Modellierungssoftware vorgestellt. Vorhandene Konzepte, die neu modelliert wurden, werden präsentiert. Anhand des iniGrid-Projekts wird ein Abriss über neu entwickelte Technologien für das Smart Grid und deren Anwendungsfälle beschrieben.

Im Anschluss wird die Modellierung der iniGrid-Use-Cases in der Referenzarchitektur evaluiert. Im ersten Schritt wird das europäische Marktrollenmodell vorgestellt und, wie die in iniGrid identifizierten neuen Akteure in Österreich aussehen könnten. Es werden die Use Cases von iniGrid konform zur Referenzarchitektur modelliert. Im Anschluss wird die Möglichkeit für die Berichtslegung aufgezeigt. Eine Vorstellung der möglichen Vorgehensweisen durch Analysetools rundet die technischen Möglichkeiten ab. Im Anschluss wird anhand von unterschiedlichen Stakeholdern die Verwendung und Anwendung der Referenzarchitektur RASSA evaluiert.

Abschließend werden die Ergebnisse diskutiert und es wird auf die Bedeutung der technischen Lösungen eingegangen und deren Anwendbarkeit beurteilt.

Das Feedback der Stakeholder hat neue Erkenntnisse über die Einsatzmöglichkeiten einer Referenzarchitektur gebracht. Die mögliche Verwendung als ein Werkzeug für (öffentliche) Ausschreibungen und der Anforderungsauflistung wird in der RASSA-Initiative weiter verfolgt werden. Für einen breitflächigen Einsatz fehlt es allerdings an weiterer Kompatibilität. Zu bestehenden Systemen und eingesetzten Lösungen wie *CRISAM*® müssen Import- und Exportfunktionen geschaffen werden, um den Bestandssystemen nutzen zu können.

Durch die Verwendung und Einbettung von Use Cases, die außerhalb der RASSA-Initiative entstanden sind, kann der Einsatz der Referenzarchitektur außerhalb der Initiative bestätigt werden. Eine fortführende Einpflegung neuer Daten oder die Entwicklung von Softwarefeatures kann die Basis der Referenzarchitektur weiter verbessern und die Kommunikation zwischen Stakeholdern in einer komplexen Themenwelt wie den Smart Grids unterstützen.

Die Referenzarchitektur für sichere Smart Grids in Österreich hat europaweit als erstes Projekt gezeigt, dass es möglich ist, nationale und internationale Konzepte auf eines derart großen Systems wie das derzeitige Stromnetz, miteinander zu verknüpfen. Es konnte so das Wissen aller beteiligten Stakeholder in einem Modell zusammengetragen werden.

Durch die in dieser Arbeit präsentierten Herangehensweise konnte gezeigt werden, wie komplexe Smart-Grid-Lösungen für ein gemeinsames Verständnis modelliert werden können. Anhand eines repräsentativen Beispiels der neu entwickelten *Smart Breaker* Komponente wurden neue Security Requirements exemplarisch in der Referenzarchitektur definiert und diese für verschiedene Interessensgruppen einsehbar gemacht.

Denkbar ist es, in zukünftigen Forschungsprojekten für unterschiedliche Bedarfsträger_innen die Basis der Referenzarchitektur als Service beziehungsweise Dienstleistung zugreifbar zu gestalten. Dies ist vor allem interessant, da zukünftig das *Common Grid Model*, ein gemeinsames Netzmodell der ENTSO-E, das zentrale Element für die Umsetzung von europäischen Vorgaben der Kapazitätsberechnung darstellen soll. Die Referenzarchitektur kann sich durch die in dieser Arbeit gezeigten Flexibilität und Erweiterbarkeit für eine Weiterentwicklung in diese Richtung eignen.

# Abbildungsverzeichnis

# Tabellenverzeichnis

# Literatur


[1] European Network of Transmission System Operators for Electricity ENTSO-E. *Frequency Deviations*. 2018. URL: https://www.entsoe.eu/news/2018/03/06/press-release-continuing-frequency-deviation-in-the-continental-european-power-system-originating-in-serbia-kosovo-political-solution-urgently-needed-in-addition-to-technical/ (besucht am 18. 07. 2018).

[2] European Network of Transmission System Operators for Electricity ENTSO-E. *Frequency deviations July 2018*. 2018. URL: https://www.entsoe.eu/news/2018/07/09/frequency-deviations-in-continental-europe-originating-from-kosovo-started-again-technical-measures-kicked-off-to-keep-time-delay-below-60-seconds/ (besucht am 18. 07. 2018).

[3] European Network of Transmission System Operators for Electricity ENTSO-E. *Frequency Deviations Restored*. 2018. URL: https://entsoe.eu/news/2018/04/03/frequency-deviations-continental-european-tsos-have-restored-the-situation-to-normal/ (besucht am 18. 07. 2018).

[4] AIT Austrian Institute of Technology. *iniGrid project webpage*. 2017. URL: http://www.inigrid.at/ (besucht am 28. 04. 2018).

[5] Technologieplattform Smart Grids Austria AIT Austrian Institute of Technology. *RASSA Initative*. 2017. URL: https://rassa.at/ (besucht am 01. 06. 2018).

[6] CEN/CENELEC/ETSI Joint Working Group on Standards for Smart Grids. *CEN-CENELEC-ETSI Smart Grid Coordination Group: Smart Grid Reference Architecture*. Techn. Ber. November. 2012, S. 107. URL: ftp://ftp.cen.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/Security.pdf.

[7] National Institute of Standards and Technology. *Guidelines for Smart Grid Cybersecurity*. Techn. Ber. 2014. DOI: http://dx.doi.org/10.6028/NIST.IR.7628r1.

[8] Oliver Jung, Petra Kölndorfer, Marcus Meisel, Friederich Kupzog, Dominik Engel, Peter Fröhlich, Marie-Theres Holzleitner, Johannes-Reichl, Kathrin de Bruyn und Angela Berger. *RASSA-Architektur Publizierbarer Endbericht*. Techn. Ber. 2018, S. 96. URL: https://rassa.at/.

[9] Hans-Jürgen Appelrath, Petra Beenken, Ludger Bischofs und Mathias Uslar. *IT-Architekturentwicklung im Smart Grid*. Springer-Verlag Berlin Heidelberg, 2012, S. 269. ISBN: 978-3-642-29207-1. DOI: 10.1007/978-3-642-29208-8. URL: https://www.springer.com/de/book/9783642292071.

[10] Christian Neureiter. *Vortragsfolien: Das SGAM Modell und seine praktische Anwendung*. 2015. URL: https://www.fh-salzburg.ac.at/fileadmin/fh/forschung/its/images/06072015_Vortrag_Christian.pdf (besucht am 05. 09. 2018).

[11] The British Library Board. *Vitruvius's theories of beauty*. URL: http://www.bl.uk/learning/cult/bodies/vitruvius/proportion.html (besucht am 12. 08. 2018).

[12] Schahram Dustdar, Harald Gall und Manfred Hauswirth. *Software-Architekturen für Verteilte Systeme*. 1. Aufl. Berlin: Springer-Verlag Berlin Heidelberg, 2003. ISBN: 978-3-540-43088-9. DOI: 10.1007/978-3-642-55599-2.

[13] Stefan Wilker, Marcus Meisel und Thilo Sauter. „Smart grid architecture model standardization and the applicability of domain language specific modeling tools". In: *IEEE International Symposium on Industrial Electronics* (2017), S. 152–157. DOI: 10.1109/ISIE.2017.8001239.

[14] Dieter Draxler. *Architekturentwicklung im Smart Grid*. Techn. Ber. Josef Ressel Center for User-Centric Smart Grid Privacy, Security und Control, 2017. URL: https://www.en-trust.at/papers/Draxler17a.pdf.

[15] Object Management Group. „Object Management Group, Model Driven Architecture (MDA) MDA Guide rev. 2.0". In: 2.0.June (2014), S. 1–15. URL: https://www.omg.org/cgi-bin/doc?ormsc/14-06-01.

[16] Christian Neureiter. *A Domain-Specific, Model Driven Engineering Approach for Systems Engineering in the Smart Grid*. MBSE4U, 2017, S. 1–272. ISBN: 978-3-9818529-2-9.

[17] Marco Brambilla, Jordi Cabot und Manuel Wimmer. *Model-Driven Software Engineering in Practice*. 2nd. Morgan & Claypool Publishers, 2017, S. 187. ISBN: 9781608458837. DOI: 10.2200/S00441ED1V01Y201208SWE001. URL: https://www.morganclaypool.com/doi/abs/10.2200/S00441ED1V01Y201208SWE001.

[18] Lukas Razik, Markus Mirz, Daniel Knibbe, Stefan Lankes und Antonello Monti. „Automated deserializer generation from CIM ontologies: CIM++ —an easy-to-use and automated adaptable open-source library for object deserialization in C++ from documents based on user-specified UML models following the Common Information Model (CIM) stand". In: *Computer Science - Research and Development* 33.1-2 (2018), S. 93–103. ISSN: 18652042. DOI: 10.1007/s00450-017-0350-y.

[19] Stuart Kent. „Model Driven Engineering“. In: *Integrated Formal Methods* 2335.2 (2002), S. 286–298. ISSN: 1083-351X. DOI: 10.1007/3-540-47884-1_16. URL: http://link.springer.com/10.1007/3-540-47884-1_16%5Cnhttp://dx.doi.org/10.1007/3-540-47884-1_16.

[20] Jean Bézivin. „Model Driven Engineering: An Emerging Technical Space“. In: *Generative and Transformational Techniques in Software Engineering: International Summer School, GTTSE 2005, Braga, Portugal, July 4-8, 2005. Revised Papers*. Hrsg. von Ralf Lämmel, João Saraiva und Joost Visser. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, S. 36–64. ISBN: 978-3-540-46235-4. DOI: 10.1007/11877028_2.

[21] Matthias (TÜV NORD GROUP) Springer. *Was ist der Unterschied zwischen Safety und Security?* 2016. URL: https://www.tuev-nord.de/explore/de/erklaert/was-ist-der-unterschied-zwischen-safety-und-security/ (besucht am 15. 08. 2018).

[22] Technologieplattform Smart Grids Austria TPSGA. *Technologieplattform Smart Grids Austria*. 2016. URL: https://www.smartgrids.at/ (besucht am 10. 09. 2018).

[23] FEEI Fachverband der Elektro und Elektronikindustrie. *FEEI Netzwerk -Technologieplattform Smartgrids Austria*. URL: https://www.feei.at/feei-netzwerk/technologieplattform-smartgrids-austria (besucht am 10. 09. 2018).

[24] Technologieplattform Smart Grids Austria TPSGA. *Technologieplattform Smart Grids Austria - Impressum*. 2016. URL: https://www.smartgrids.at/impressum.html (besucht am 10. 09. 2018).

[25] Angela Berger, Helfried Brunner, Michael Hübner, Friederich Kupzog, Andreas Lugmaier, Natalie Prüggler, Wolfgang Prüggler, Karl Scheida, Alexander Schenk und Ursula Tauschek. *Technologieroadmap Smart Grids Austria - Die Umsetzungsschritte zum Wandel des Stromsystems bis 2020*. Techn. Ber. 2015. URL: https://www.smartgrids.at/files/smartgrids/Dateien/Dokumente/05Technologieroadmap_web_final.pdf.

[26] Mathias Uslar, Andre Göring, Roland Heidel, Christian Neureiter und Dominik Engel. „An Open Source 3D Visualization for the RAMI 4.0 Reference Model“. In: *VDE Kongress 2016 – Internet der Dinge* (2016), S. 1–6. URL: https://www.entrust.at/papers/Uslar16a.pdf.

[27] Bauer Wilhelm, Schlund Sebastian, Marrenbach Dirk und Ganschar Oliver. *Studie: Industrie 4.0 - Volkswirtschaftliches Potenzial für Deutschland*. Techn. Ber. 2014. URL: https://www.ipa.fraunhofer.de/content/dam/ipa/de/documents/UeberUns/Leitthemen/Industrie40/Studie_Vokswirtschaftliches_Potenzial.pdf.

[28] Peter Adolphs, Heinz Bedenbender, Dagmar Dirzus, Martin Ehlich, Ulrich Epple, Martin Hankel, Roland Heidel, Michael Hoffmeister, Haimo Huhle, Bernd Kärcher, Heiko Koziolek, Reinhold Pichler, Stefan Pollmeier, Frank Schewe, Armin Walter, Bernd Waser und Martin Wollschlaeger. „Statusreport: Referenzarchitekturmodell Industrie 4.0 (RAMI 4.0)“. In: *VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik* April (2015), S. 1–32. URL: https://www.vdi.de/fileadmin/user_upload/VDI-GMA_Statusreport_Referenzarchitekturmodell-Industrie40.pdf.

[29] Christoph Binder. *Introduction to the „RAMI 4.0 Toolbox“*. Techn. Ber. Josef Ressel Center for User-Centric Smart Grid Privacy, Security und Control Salzburg University of Applied Sciences, 2017, S. 1–27. URL: https://www.en-trust.at/wp-content/uploads/Introduction-to-RAMI-Toolbox.pdf.

[30] Johannes Kalhoff, Ulrich Löwen, Tobias Manger und Karsten Schneider. *Open Source Projekt openAAS – mit offenen Standards Industrie 4.0 umsetzen*. Techn. Ber. 2017. URL: https://www.zvei.org/fileadmin/user_upload/Verband/Fachverbaende/Automation/Open-Source-Projekt-openAAS-mit-offenen-Standards-Industrie-4.0-umsetzen.pdf.

[31] Shi-Wan Lin (Thingswise/Intel), Bradford Miller (GE), Jacques Durand (Fujitsu), Graham Bleakley (IBM), Amine Chigani (GE), Robert Martin (MITRE), Brett Murphy (RTI) und Mark Crawford (SAP). *The Industrial Internet of Things Volume G1: Reference Architecture, Version 1.8*. Techn. Ber. Industrial Internet Consortium, 2017, S. 1 –7. URL: https://www.iiconsortium.org/IIC_PUB_G1_V1.80_2017-01-31.pdf.

[32] Industrial Internet Consortium. „Industrial Internet Consortium and Plattform Industrie 4.0 Collaboration for Interoperability“. 2016.

[33] Shi-Wan Lin, Murphy Brett, Erich Clauer, Ulrich Loewen, Ralf Neubert, Gerd Bachmann, Madhusudan Pai und Martin Hankel. *Architecture Alignment and Interoperability An Industrial Internet Consortium and Plattform Industrie 4.0 Joint Whitepaper*. Techn. Ber. 2018, S. 19. URL: http://www.iiconsortium.org/pdf/JTG2_Whitepaper_final_20171205.pdf.

[34] Cynthia K Veitch, Jordan M Henry, Bryan T Richardson und Derek H Hart. *Microgrid Cyber Security Reference Architecture - Version 1.0*. July. 2013. URL: https://prod.sandia.gov/techlib-noauth/access-control.cgi/2013/135472.pdf.

[35] AIT Austrian Institute of Technology, AISEC Fraunhofer, The Queen's of University Belfast, Energieinstitut an der Johannes Kepler Universität Linz, EMC Information Systems International Ltd, Kungliga Tekniska högskolan (KTH), Landis+Gyr AG, United Technologies Research Centre und SWW Wunsiedel GmBH. *White Paper – An Assessment of Smart Grid Reference Architectures*. 2015. URL: http://project-sparks.eu/wp-content/uploads/2014/04/SPARKS-Smart-Grid-Reference-Architecture-White-Paper.pdf.

[36] University of Maryland und Robert H Smith School of Business. *The ICT SCRM Community Framework Development Project Final Report (Whitepaper)*. 2011, S. 95. URL: https://csrc.nist.gov/publications/detail/white-paper/2011/12/01/ict-scrm-community-framework-development-project-final-report/final.

[37] GridWise Architecture Council. „GridWise Transactive Energy Framework Version 1.0“. In: *GridWise Architecture Council on Transactive Energy* 1 (2013), S. 1–23. URL: https://www.gridwiseac.org/pdfs/te_framework_report_pnnl-22946.pdf.

[38] Koen Kok und Steve Widergren. „A Society of Devices: Integrating Intelligent Distributed Resources with Transactive Energy“. In: *IEEE Power and Energy Magazine* 14.3 (2016), S. 34–45. ISSN: 15407977. DOI: 10.1109/MPE.2016.2524962.

[39] National Institute of Standards and Technology. *NIST Special Publication 1108r3: NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0*. Techn. Ber. 2014, S. 239. DOI: http://dx.doi.org/10.6028/NIST.SP.1108r3.

[40] GridWise Architecture Council. *Smart Grid Interoperability Maturity Model Summary*. 2011. URL: https://www.gridwiseac.org/pdfs/imm/sg_imm_beta_final_12_01_2011.pdf (besucht am 24. 07. 2018).

[41] Electric Power Research Institute. *EPRI Product Abstract: A Utility Application Implementation Strategy Using the EPRI IntelliGrid Methodology and the GridWise Architecture Council Stack as a Model*. 2011. URL: https://www.epri.com/#/pages/product/1024590/?lang=en (besucht am 01. 08. 2018).

[42] John J Simmins, Brian Green und Michael Tao. *Using the IntelliGrid (sm) Methodology and GWAC Stack in IT Smart Grid Project Management (Presentation)*. 2011. URL: https://www.gridwiseac.org/pdfs/forum_papers11/simmins_sgimm_pres_gi11.pdf.

[43] The Open Group. *The TOGAF® Standard, Version 9.2: Introduction*. 2018. URL: http://pubs.opengroup.org/architecture/togaf9-doc/arch/index.html (besucht am 06. 08. 2018).

[44] Ian Yosef Matheus Edward, Wervyan Shalannanda, Susmini Indriani Lestariningati und Aldo Agusdian. „E-Government Master Plan Design with TOGAF Framework Case Study: Payakumbuh City Government, Indonesia“. In: *2014 8th International Conference on Telecommunication Systems Services and Applications (TSSA)* (2014), S. 1–6. DOI: https://doi.org/10.1109/TSSA.2014.7065957.

[45] The Open Group. *The TOGAF® Standard, Version 9.2: Core Concepts*. 2018. URL: http://pubs.opengroup.org/architecture/togaf9-doc/arch/chap02.html (besucht am 06. 08. 2018).

[46] National Institute of Standards and Technology Smart Grid Interoperability Panel. *Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security*. Techn. Ber. September. 2010. URL: http://permanent.access.gpo.gov/gpo1900/nistir-7628_total.pdf.

[47] Angela Berger, Marcus Meisel, Lucie Langer, Markus Litzlbauer und Mathias Uslar. *RASSA-Stakeholderprozess*. Techn. Ber. Bundesministerium für Verkehr, Innovation und Technologie, 2015, S. 79. URL: https://publik.tuwien.ac.at/files/publik_257955.pdf.

[48] European Commission Directorate General for Energy. *Smart Grid Mandate M/490 EN*. 2011. URL: https://ec.europa.eu/energy/sites/ener/files/documents/2011_03_01_mandate_m490_en.pdf.

[49] CEN-CENELEC-ETSI Smart Grid Coordination Group. *SGAM User Manual - Applying, testing and refining the Smart Grid Architecture Model (SGAM)*. Techn. Ber. 2014, S. 67. URL: ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/SGCG_Methodology_SGAMUserManual.pdf.

[50] Florian Skopik und Paul Smith. *Smart Grid Security*. Amsterdam: Elsevier, 2015, S. 324. ISBN: 9780128021224.

[51] National Institute of Standards and Technology. „NIST Special Publication 1108 NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0“. In: *Nist Special Publication* 0 (2010), S. 1–145. URL: http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf.

[52] The Open Group. *ArchiMate 2.1 Spezifikation*. 2013. URL: http://pubs.opengroup.org/architecture/archimate2-doc/ (besucht am 04. 09. 2018).

[53] Bundesamt für Sicherheit in der Informationstechnik. *Zertifizierte Produkte - Intelligente Messsysteme*. URL: https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/ZertifizierungnachCC/ZertifizierteProdukte/Intelligente_Messsysteme/Intelligente_Messsysteme_node.html (besucht am 20. 11. 2018).

[54] Bundesamt für Sicherheit in der Informationstechnik. *Technische Richtlinie BSI TR-03109-2: Anhang : Smart Meter Gateway – Sicherheitsmodul – Use Cases V1.1*. Techn. Ber. 2014, S. 1–83. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03109/TR-03109-2-Sicherheitsmodul_Use_Cases.pdf?__blob=publicationFile&v=2.

[55] Oesterreichs Energie. *AMCS Lastenheft und Smart Meter-Use Cases*. 2015. URL: https://oesterreichsenergie.at/amcs-lastenheft-und-smart-meter-use-cases.html (besucht am 16. 08. 2018).

[56] Oesterreichs Energie. *Smart Metering Use-Cases für das Advanced Meter Communication System (AMCS) Version 1.1*. Techn. Ber. 5. 2015, S. 1–91. URL: https://oesterreichsenergie.at/files/DownloadsNetze/OesterreichUseCasesSmartMetering_14122015_Version_1-1.pdf.

[57] Electric Power Research Institute (EPRI). *EPRI Use Case Repository*. URL: http://smartgrid.epri.com/Repository/Repository.aspx (besucht am 17. 08. 2018).

[58] Electric Power Research Institute (EPRI). *Smart Grid Demonstration — Integration of Distributed Energy Resources*. URL: http://smartgrid.epri.com/Demo.aspx (besucht am 17. 08. 2018).

[59] Stephan Amsbary und Martin J. Burns. *IntelliGrid Use Case Template*. URL: http://smartgrid.epri.com/Repository/Repository.aspx (besucht am 17. 08. 2018).

[60] Electric Power Research Institute (EPRI). *EPRI Smart Grid Demonstration Initiative Final Update*. Techn. Ber. 2014, S. 104. URL: https://www.epri.com/#/pages/product/000000003002004652/?lang=en-US.

[61] International Electrotechnical Commission. *IEC - Smart Grids Standards Map*. URL: http://smartgridstandardsmap.com/ (besucht am 18. 08. 2018).

[62] Innogy. *DISCERN The Project*. 2016. URL: https://www.discern.eu/project.html (besucht am 02. 01. 2019).

[63] OFFIS. *DISCERN SGAM Visio Template*. 2016. URL: https://www.discern.eu/datas/DISCERN_SGAM_Visio_Template.zip (besucht am 02. 01. 2019).

[64] OFFIS. *Use Case Management Repository*. URL: http://ucmr.offis.de/#use-case-management-repository (besucht am 17. 08. 2018).

[65] *IEC 62559-2:2015 Use case methodology - Part 2: Definition of the templates for use cases, actor list and requirements list*. 2015. URL: https://webstore.iec.ch/publication/22349.

[66] Electric Power Research Institute (EPRI). *IEC PAS 62559:2008 Withdrawn IntelliGrid methodology for developing requirements for energy systems*. 2008. URL: https://webstore.iec.ch/publication/7564.

[67] M. Gottschalk und M. Uslar. „Ein Use Case Management Repository zur Unterstützung der Normungsarbeit“. In: *Mensch & Computer: Gemeinsam Altern erleben* (2015), S. 583–588.

[68] Ewa Piatkowska, Agron Bajraktari, Dharini Chhajed und Paul Smith. „Tool support for data protection impact assessment in the smart grid“. In: *e & i Elektrotechnik und Informationstechnik* 134.1 (2017), S. 26–29. ISSN: 0932-383X. DOI: 10.1007/s00502-017-0484-4. URL: http://link.springer.com/10.1007/s00502-017-0484-4.

[69] Stefan Wilker, Marcus Meisel, Ewa Piatkowska, Thilo Sauter und Oliver Jung. „Smart Grid Reference Architecture, an Approach on a Secure and Model-Driven Implementation“. In: *2018 IEEE 27th International Symposium on Industrial Electronics (ISIE)* (2018), S. 74–79. DOI: 10.1109/ISIE.2018.8433754. URL: https://ieeexplore.ieee.org/document/8433754/.

[70] Xylem Science GmbH und Technology Management. *AURUM Risiko- und Compliance-Management für Unternehmen*. URL: https://www.xylem-technologies.com/portfolio/aurum-risiko-und-compliance-management-fuer-unternehmen/ (besucht am 17. 12. 2018).

[71] Andreas Ekelhart, Stefan Fenz und Thomas Neubauer. *Ontologiebasiertes IT Risikomanagement*. Techn. Ber. SBA Research gGmbH, 2009, S. 1–12. URL: https://www.sba-research.org/wp-content/uploads/publications/2009-Ekelhart-OntologiebasiertesITRisikomanagement.pdf.

[72] Andreas Ekelhart, Stefan Fenz und Thomas Neubauer. „AURUM: A framework for information security risk management“. In: *Proceedings of the 42nd Annual Hawaii International Conference on System Sciences, HICSS* (2009), S. 1–10. ISSN: 1530-1605. DOI: 10.1109/HICSS.2009.82.

[73] Bundesamt für Sicherheit in der Informationstechnik. *IT-Grundschutz GSTOOL*. URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/GSTOOL/gstool_node.html (besucht am 17. 12. 2018).

[74] Manfred Stallinger. „IT-Governance im Kontext Risikomanagement“. In: (2007), S. 235. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Extern/IT-Governance_im_Kontext_Risikomanagement.pdf?__blob=publicationFile&v=1.

[75] CALPANA business consulting GmbH. *CRISAM ISO 27001 Knowledge Pack*. URL: https://www.crisam.net/de/crisam-iso-27001-knowledge-pack (besucht am 17. 12. 2018).

[76] CALPANA business consulting GmbH. *CRISAM ICS/SCADA Knowledge Pack*. URL: https://www.crisam.net/de/crisam-icsscada-knowledge-pack (besucht am 17. 12. 2018).

[77] SerNet GmbH. *verinice features*. URL: https://verinice.com/produkt/#_features (besucht am 17. 12. 2018).

[78] Bundesamt für Sicherheit in der Informationstechnik. *BSI - IT-Grundschutz-Kataloge*. 2018. URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html (besucht am 02. 01. 2019).

[79] European Union Agency for Network Security und Information. *ENISA Self Assessed Risk Management (SARM)*. URL: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/approaches-for-smes/self-assessed-risk-management-sarm (besucht am 16. 12. 2018).

[80] Ihor Blinov und Serhii Tankevych. „The harmonized role model of electricity market in Ukraine“. In: *2016 2nd International Conference on Intelligent Energy and Power Systems (IEPS)* (2016), S. 1–3. DOI: 10.1109/IEPS.2016.7521861. URL: http://ieeexplore.ieee.org/document/7521861/.

[81] Mathias Uslar, Christine Rosinger und Stefanie Schlegel. „Security by design for the smart grid: Combining the SGAM and NISTIR 7628“. In: *Proceedings - IEEE 38th Annual International Computers, Software and Applications Conference Workshops, COMPSACW 2014* (2014), S. 110–115. DOI: 10.1109/COMPSACW.2014.23.

[82] Jochen Ludewig und Horst Lichter. *Software Engineering: Grundlagen, Menschen, Prozesse, Techniken*. 3., korrig. dpunkt.verlag, 2013, S. 688. ISBN: 978-3-86490-092-1. URL: https://www.dpunkt.de/buecher/4439/software-engineering.html.

[83] SparxSystems Software GmbH. *Funktionsübersicht - Enterprise Architect*. 2018. URL: https://www.sparxsystems.de/uml/ea-function/?L=0 (besucht am 22. 11. 2018).

[84] Security Josef Ressel Center for User-Centric Privacy und Control. *SGAM Toolbox Webseite*. URL: https://sgam-toolbox.org/ (besucht am 22. 11. 2018).

[85] Christian Neureiter, Mathias Uslar, Dominik Engel und Goran Lastro. „A standards-based approach for domain specific modelling of smart grid system architectures“. In: *2016 11th System of Systems Engineering Conference (SoSE)*. IEEE, 2016, S. 1–6. ISBN: 978-1-4673-8727-9. DOI: 10.1109/SYSOSE.2016.7542888. URL: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7542888.

[86] Entso-E. *The Harmonised electricity role model, Version 2015-1*. Techn. Ber. 2015, S. 1–33. URL: https://docstore.entsoe.eu/Documents/EDI/Library/HRM/2015-September-Harmonised-role-model-2015-01.pdf.

[87] Object Management Group. *Unified Modeling Language Specification Version 2.5.1*. Techn. Ber. 2017, S. 796. URL: https://www.omg.org/spec/UML/.

[88] Security Josef Ressel Center for User-Centric Privacy und Control. *SGAM Toolbox - Example Model*. URL: https://sgam-toolbox.org/examples/ (besucht am 27. 11. 2018).

[89] Security Josef Ressel Center for User-Centric Privacy und Control. *Klickbares NIST LRM in SGAM Toolbox*. URL: https://sgam-toolbox.org/NISTLRM (besucht am 27. 11. 2018).

[90] European Network of Transmission System Operators for Electricity ENTSO-E. *Harmonised Electricity Role Model - Webseite*. 2018. URL: https://www.entsoe.eu/digital/cim/role-models/#harmonised-electricity-role-model (besucht am 26. 11. 2018).

[91] E-Control Austria. *Risikoanalyse für die Informationssysteme der Elektrizitätswirtschaft*. Techn. Ber. 2014, S. 1–80. URL: https://www.e-control.at/documents/20903/-/-/3f89d470-7d5e-433c-b307-a6443692d8f7.

[92] Security Josef Ressel Center for User-Centric Privacy und Control. *SGAM Toolbox Example Model*. URL: https://sgam-toolbox.org/examples/ (besucht am 27. 11. 2018).

[93] National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity Version 1.0*. Techn. Ber. 2014. URL: https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[94] Oesterreichs Energie. *Smart Metering Use-Cases für das Advanced Meter Communication System (AMCS)*. Techn. Ber. 2015, S. 1–91. URL: smartmeteringusecases.

[95] Christian Neureiter, Günther Eibl, Dominik Engel, Stefanie Schlegel und Mathias Uslar. „A concept for engineering smart grid security requirements based on SGAM models“. In: *Computer Science - Research and Development* 31.1-2 (2016), S. 65–71. ISSN: 18652042. DOI: 10.1007/s00450-014-0288-2. URL: http://dx.doi.org/10.1007/s00450-014-0288-2.

[96] Christian Dänekas, Christian Neureiter, Sebastian Rohjans, Mathias Uslar und Dominik Engel. „Towards a model-driven-architecture process for smart grid projects“. In: *Advances in Intelligent Systems and Computing* 261 (2014), S. 47–58. ISSN: 21945357. DOI: 10.1007/978-3-319-04313-5_5.

[97] Stefan Kollmann, Stefan Wilker, Marcus Meisel, Alexander Wendt, Andres Moreno, Khalil Hamad und Peter Zeller. *iniGrid Deliverable D6.1: System Functionality Validation*. Techn. Ber. Auf Anfrage., 2018.

[98] Lucie Langer, Marcus Meisel, Christian Neureiter, Wolfgang Kastner, Mathias Uslar, Angela Berger und Thomas Aichholzer. *RASSA-Architektur Deliverable AP 2 Methodik zur Referenzarchitekturentwicklung*. Techn. Ber. Auf Anfrage, 2016.

[99] European Network of Transmission System Operators for Electricity ENTSO-E. *The Harmonised electricity role model, Version 2018-01*. Techn. Ber. 2018. URL: https://docstore.entsoe.eu/Documents/EDI/Library/HRM/Harmonised_Role_Model_2018-01.pdf.

[100] European Network of Transmission System Operators for Electricity ENTSO-E. *HRM2018-01 XMI EA*. 2018. URL: https://www.entsoe.eu/Documents/EDI/Library/HRM/HRM2018-01_XMI_EA.zip (besucht am 30. 12. 2018).

[101] European Network of Transmission System Operators for Electricity ENTSO-E. *ENTSO-E Official Mandates: The Third Energy Package*. URL: https://www.entsoe.eu/about/inside-entsoe/official-mandates/ (besucht am 04. 12. 2018).

[102] Kaindl H.a B. „A design process based on a model combining scenarios with goals and functions“. In: *IEEE Transactions on Systems, Man, and Cybernetics Part A:Systems and Humans.* 30.5 (2000), S. 537–551. ISSN: 10834427. DOI: 10.1109/3468.867861. URL: http://www.scopus.com/inward/record.url?eid=2-s2.0-0034269939&partnerID=40&md5=cefb48f820011092ed9c504adaa74b13.

[103] Sparx Systems Pty Ltd. *Enterprise Architect User Guide 14.0 Trace.* 2018. URL: https://sparxsystems.com/enterprise_architect_user_guide/14.0/model_domains/trace.html (besucht am 29. 12. 2018).

[104] Lucie Langer. „Effective Security Guidance for Smart Grid Stakeholders“. In: Wien, Austria: Poster presented at: Smart Grid Weeks 2015, 2015. URL: http://www.smartgridsweek.com/docs/SGW15_Poster_WEB/Poster_Langer.pdf.

[105] CEN-CENELEC-ETSI Smart Grid Coordination Group. *Smart Grid Information Security.* Techn. Ber. November. 2012, S. 46. DOI: 10.1002/aur.1474.Replication. arXiv: 15334406. URL: ftp://ftp.cen.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/Security.pdf.

[106] E-Control Austria. *Bericht zur Einführung von intelligenten Messgeräten in Österreich.* Techn. Ber. 2018, S. 69. URL: https://www.e-control.at/documents/20903/388512/20181012_Monitoringbericht_Smartmeter.pdf/d28e5a28-4d03-f454-ea50-5161bb2db091.

[107] Benjamin Weinert, Mathias Uslar und Axel Hahn. „System-of-systems: How the maritime domain can learn from the Smart Grid“. In: *2017 International Symposium ELMAR.* 2017, S. 229–232. DOI: 10.23919/ELMAR.2017.8124474.

[108] Mathias Uslar und Marion Gottschalk. „Extending the SGAM for Electric Vehicles“. In: *International ETG Congress 2015; Die Energiewende - Blueprints for the new energy age.* 2015, S. 1–8.

[109] Technologieplattform Smart Grids Austria TPSGA. *IES - Integrating the Energy System.* 2016. URL: https://www.smartgrids.at/plattform-aktivitaeten/ies-integrating-the-energy-system-austria-eng.html (besucht am 01. 06. 2018).

[110] Hussein Gannud, Hao Wu und Joseph Timoney. „Applying a MDE approach to a healthcare environment: A case study of an AE dept“. In: *2017 28th Irish Signals and Systems Conference (ISSC).* 2017, S. 1–7. DOI: 10.1109/ISSC.2017.7983632.

[111] Rafael Santodomingo, Mathias Uslar, Marion Gottschalk, Andre Goering, L. Nordstrom und Georgii Valdenmaiier. „The discern tool support for knowledge sharing in large smart grid projects“. In: *CIRED Workshop 2016.* Institution of Engineering und Technology, 2016, 1–4, Paper 355. ISBN: 978-1-78561-202-2. DOI: 10.1049/cp.2016.0728.

[112] OFFIS. *DISCERN SGAM Visio Template User Guide*. Techn. Ber. 2016, S. 20. URL: https://www.discern.eu/datas/DISCERN_SGAM_Visio_Template_-_User_Guide.pdf.

[113] Oliver Jung, Stefan Fenz, Markus Kammerstetter und Aleksandar Hudic. „Eine Architektur für sichere Smart Grids in Österreich“. In: *D-A-CH Security 2016*. Klagenfurt, AT, 2016, S. 1–9.

[114] Matthew Harvey, Daniel Long und Karl Reinhard. „Visualizing NISTIR 7628, Guidelines for smart grid cyber security“. In: *2014 IEEE Power and Energy Conference at Illinois, PECI 2014* (2014), S. 1–8. DOI: 10.1109/PECI.2014.6804566.

[115] Network Perception. *Network Perception - About*. 2018. URL: https://www.network-perception.com/about/ (besucht am 10. 12. 2018).

[116] E-Control Austria und Infraprotect GmbH. *IKT-Risikoanalyse der Energiewirtschaft Version 3.0 WHITE-VERSION*. Techn. Ber. 2018, S. 30. URL: https://www.e-control.at/documents/20903/388512/IKT-Risikoanalyse+Strom-Gas+Endbericht_V_3_0_WHITE_2018-12-10.pdf/2184ddfd-5d8d-213b-ffdd-1c3d8502f5ac.

ANHANG A

# Abbildungen von Modellen

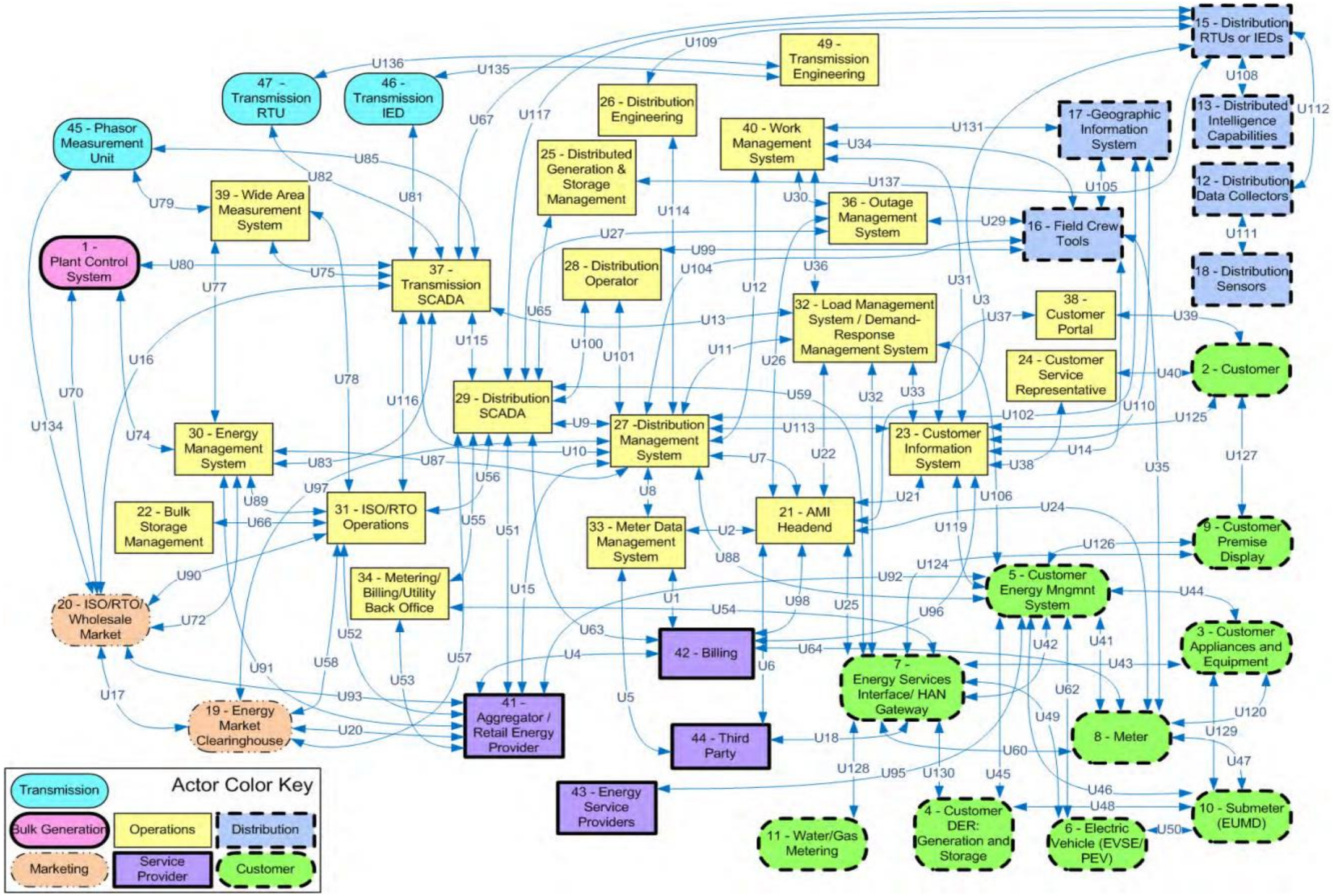
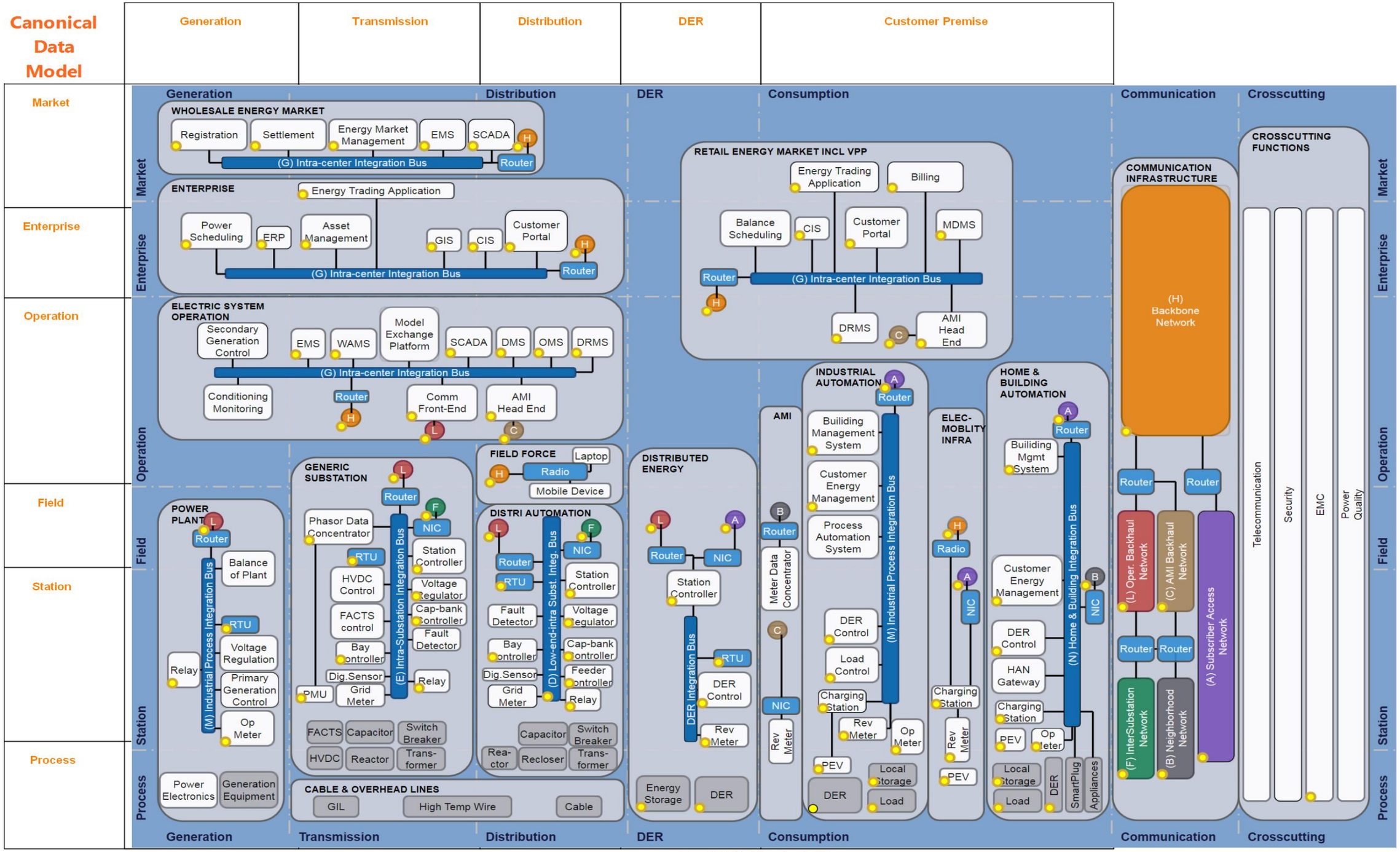



Abbildung A.1: Logical Reference Model [46] *Reprinted courtesy of the National Institute of Standards and Technology, U.S. Department of Commerce. Not copyrightable in the United States.*




**Double-Click the image to visit the IEC's Map of Smart Grid Standards at "http://smartgridstandardsmap.com/"**
**This is an interactive tool that delivers an overview about applicable standards in the Smart Grid**

Abbildung A.2: Abbildung der Smart Grids Standards Map in der RASSA-Referenzarchitektur [8, 61]

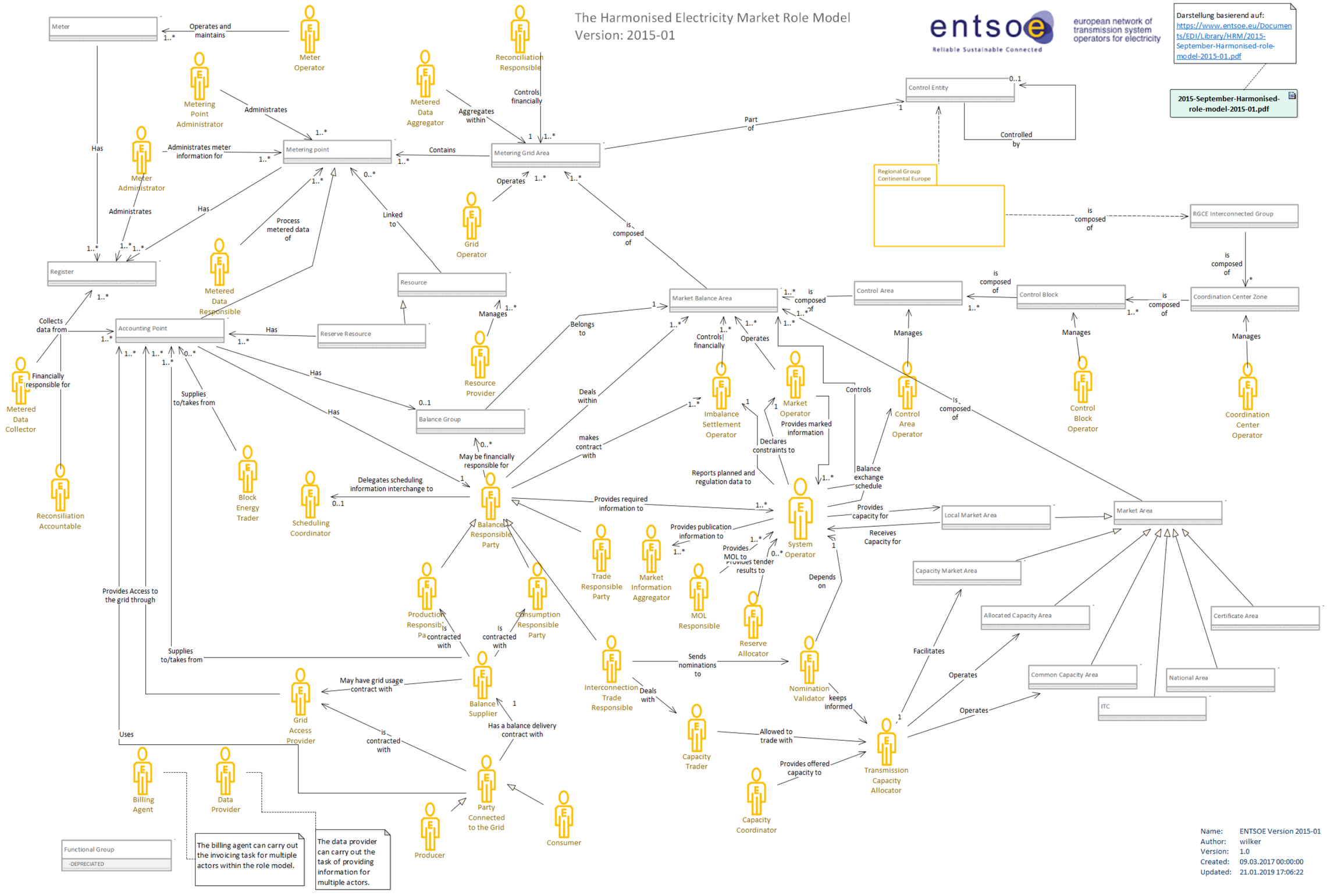



Abbildung A.3: Komplettes nachmodelliertes Harmonized Electricity Market Role Model (ENTSO-E) nach Version 2015-01

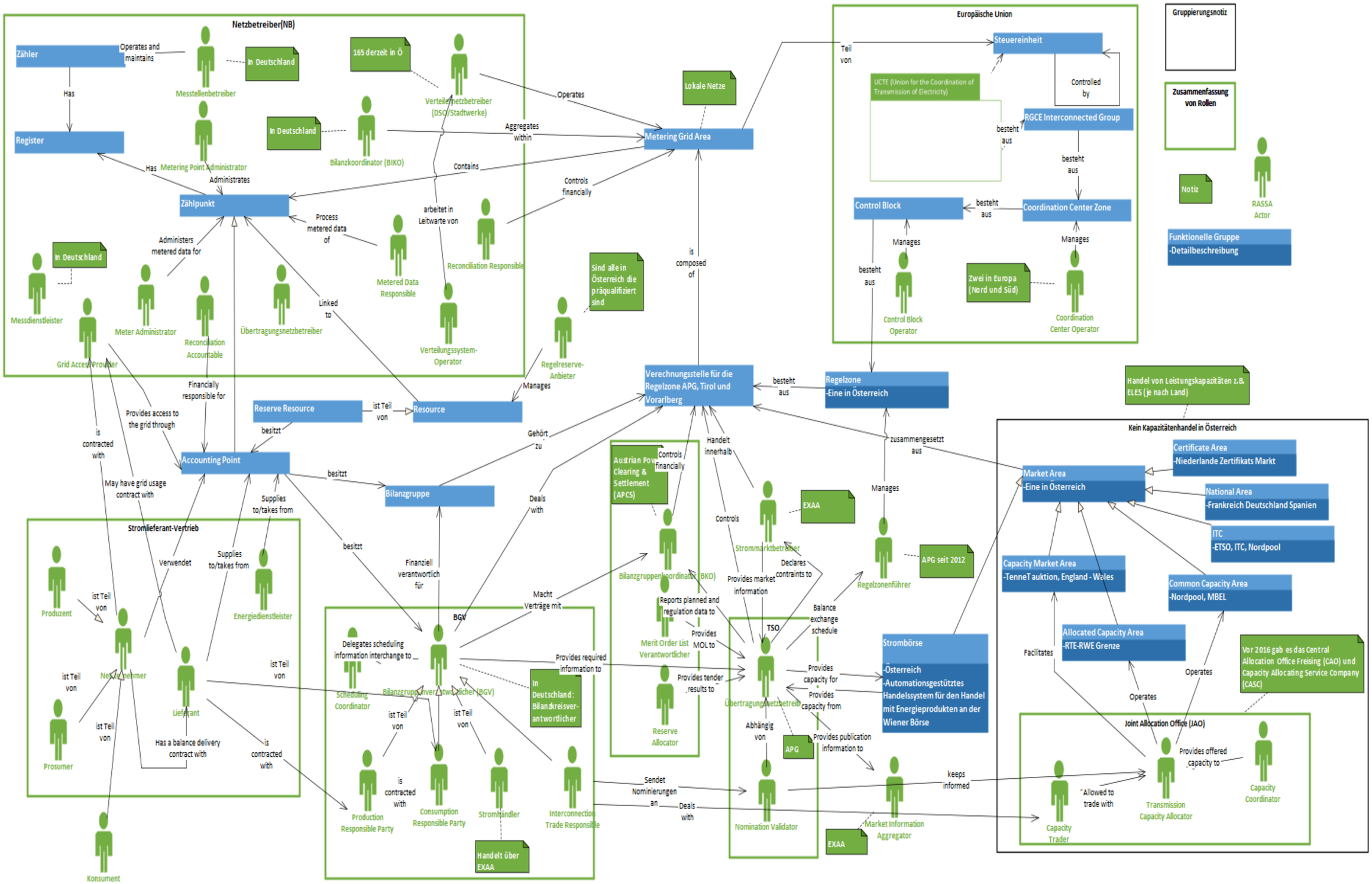



Abbildung A.4: Österreichisches Marktrollenmodell ohne Einführung eines neuen zusammenfassendes Elements

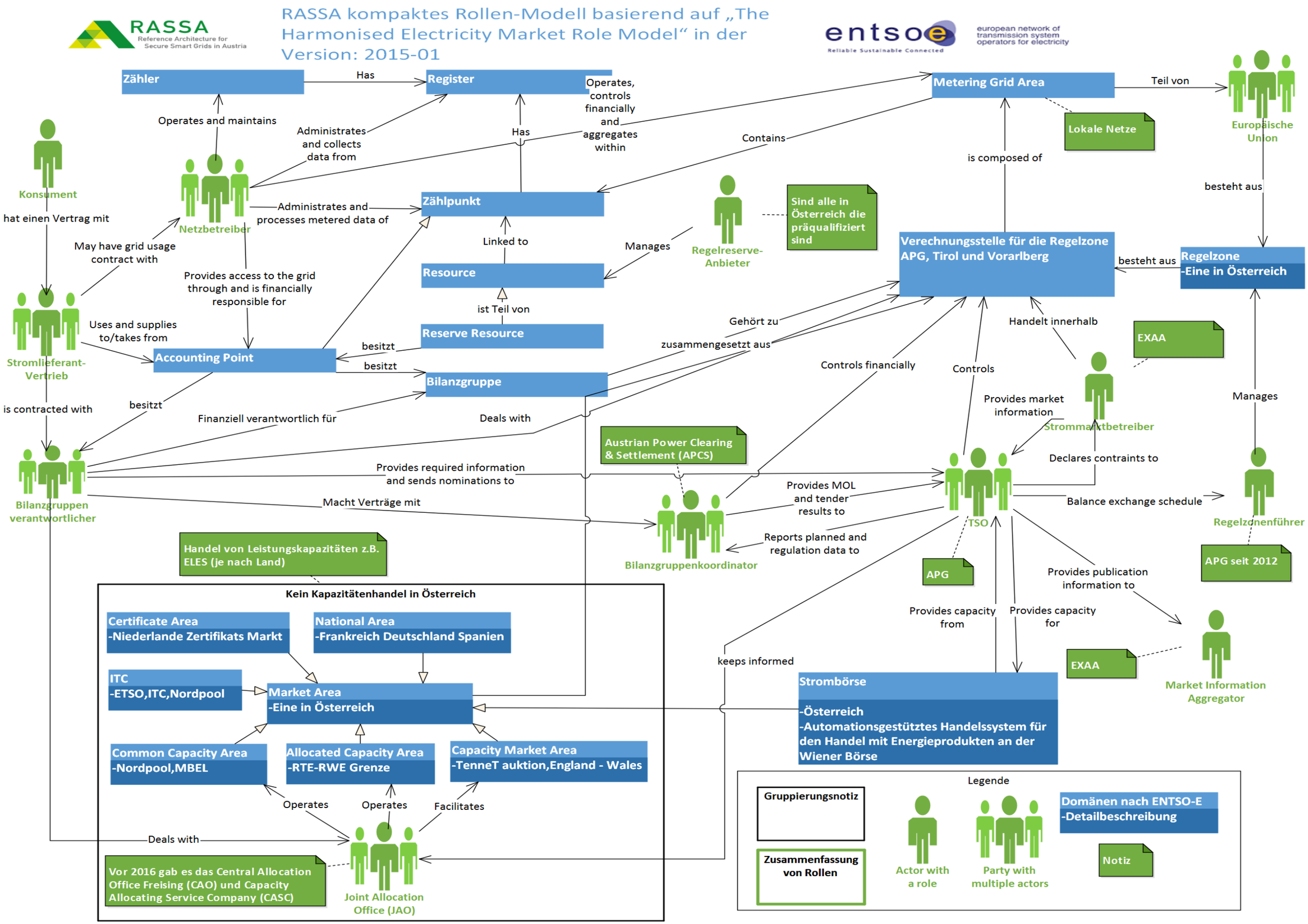



Abbildung A.5: Kompaktes RASSA Rollenmodell zur Darstellung des Österreichischen Marktes nach dem *Harmonized Electricity Market Role Model Version 2015-01*